

ТАКЖЕ

ver 01.04 (61)

WWW.XAKER.RU

Выбери свой ТУННЕЛЬ

все о туннелировании трафика Стр. 56

ЗАУМНЫЙ ДОМ Стр. 46
киберхрущевка has you

Почтовые перехватчики
тотальный контроль над перепиской
Стр. 30

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
Основы приемов манипуляции
Стр. 66

Асечка на блюдечке
Занимательные корявости ICQ
Стр. 72



ISSN 1609-1019
9771609101009

(game)land



LCD - МОНИТОРЫ FLATRON®

ЛУЧШИЙ ДИЗАЙН ГОДА*



* Призер международных конкурсов IF Design 2003 и Reddot



L1520P/L1720P

- LCD-монитор с диагональю 15, 17 дюймов
- Футуристический дизайн
- Функция Light View
- Цифровой вход



T710BH/PH

- 17 дюймовый монитор FLATRON® с плоским экраном
- Динамичный и функциональный дизайн
- Функции BrightView и BrightWindow
- Сертификация по самым строгим стандартам TCO® 03



Функция LightView включает 3 режима: "день", "ночь", и "пользовательский". В режимах "день" и "ночь" есть режимы: "текст", "фото" и "кино". Каждый из этих 6 режимов обладает уникальными параметрами настройки яркости и контраста.



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



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

© 2003 LG Electronics



Москва: D-Vision (095) 285-6130; Техноград (095) 670-1383; Рес (095) 230-6200; Сильсон (095) 150-83-20; DVM Group (095) 777-1044; Динвик (095) 757-4099; Сигетелев (095) 745-2999; Элси (095) 777-8779; Ласко (095) 780-3298; С-Центр (095) 472-6401; Формоза (095) 234-2164; NT Computer (095) 670-1930; POLARIS (095) 755-5557; ТехноСила (095) 777-8777; М.Видео (095) 777-7775; Маг (095) 780-0000; Эльбрус (095) 500-0000; 37CT (095) 779-4062; Папа (095) 236-9932; Техноград Компьютеры (095) 363-9333; Сетевая Лаборатория (095) 784-6492; Скай (095) 295-2923; Компания КИТ (095) 777-9955; АБ-Групп (095) 143-1144; SSM (095) 779-4020; Техно (095) 974-3333; ОЦЭМ (095) 150-0100; Энергетический класс (095) 234-3777; USN Computers (095) 775-8992; Сторж Машин (095) 675-8610; Арктик (095) 794-7224; РадикалЭлектрон-Компьютер (095) 950-8778; Цифра Электроникс (095) 150-4788; Форум Компьютеры (095) 775-7299; Девин (095) 959-2222; ULTRA Computer (095) 775-1566; 279-5250; Телнет Электроникс (095) 737-3046; Ресур (095) 912-6224; Санкт-Петербург: Биско (812) 102-4300; ДИМ-Нью (812) 325-1105; Балашиха: ВЕРИСОК (8438) 66-00-00; Барнаул: Мойл (3852) 24-40-57; Белгород: Инфотек (0722) 26-36-18; Бийск: ТАРУС + (3853) 33-32-32; Владивосток: SVADEKO (092) 22-89-77; ДПС (4232) 30-04-64; Волгоград: Телет (8442) 97-59-37; Воронеж: POLARIS (0733) 75-73-82; РМАН (0709) 512402; Саян (0703) 23-30-32; Рязань (0722) 77-83-38; Екатеринбург: Класс (3432) 59-99-21; Компьютер без проблем (3432) 50-64-49; Железно: ТРАНСИТ (3412) 45-19-22; Иркутск: ТРАНСИТ (3952) 23-82-27; Казань: Алгоритм (8432) 36-52-72; Кауга: Ретро Кален (0242) 56-43-22; Карен: Глобтика (8532) 67-83-66; Краснодар: Сетев (8612) 69-11-44; Криве (8812) 69-96-50; Красноярск: Альянс (8312) 271145; Бит Ниско (8322) 56-06-98; Курск: Ресур Ул (0742) 49-46-73; Мурманск: Экселент (8152) 42-98-34; Набережные Челны: БОРТ-ДРАЙВ-ТРАЙДЕНТ (8552) 59-80-81; Назаров: ОДО (3022) 31-70-78; POLARIS (8312) 77-50-00; Боро-К (8312) 42-23-67; 42-91-32; (34012) 40-000; Ижевск: Арктик (3486) 24-09-20; Нижний Новгород: АЛТЭНС (8312) 31-70-78; POLARIS (8312) 77-50-00; Боро-К (8312) 42-23-67; 42-91-32; Новосибирск: Компьютеры Сетевика (3832) 49-51-24; ТехноСити (3832) 33-20-03; Кемерово (3832) 30-51-33; Оренбург: КО Центр (3532) 29-31-60; Пермь: Альянс (3422) 19-61-58; Ростов-на-Дону: Занит-Компьютер (8632) 95-03-00; Троицкопояск (3852) 90-31-51; Самара: Прогис (8462) 16-32-67; Рязань (8462) 34-54-38; Саратов: Ресур (8452) 24-05-91; Саратов: Компьютер (8452) 24-13-14; Бурятия: ТЕХНОЦЕНТР (3452) 24-00-30; Челябинск: С3 плюс (3452) 37-79-77; Тюмень: Итстрин (3522) 35-00-55; Тюмень: Арктик (3452) 46-47-74; Уфа: Компьютер (3452) 49-30-64; Уфа: Техника (3452) 39-00-30; Уфа: Меморек (3472) 22-09-88; Уфа: (3472) 2452; Хабаровск: ДРАЙВ (812) 34-85-32; Орск: Техника (3212) 22-15-46; Копейск (3112) 25-61-61; Челябинск: Техно-388 (312) 34-94-02; Челябинск (312) 33-56-12.

Информационная служба LG: (095) 771 7878; <http://www.lg.ru>





ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!**БЕСПЛАТНАЯ
КУРЬЕРСКАЯ ДОСТАВКА ПО МОСКВЕ**Хочешь получать журнал
через 3 дня после выхода?**Звони 935-70-34****ДЛЯ ЭТОГО НЕОБХОДИМО:**

1. Заполнить подписной купон (или его ксерокопию)
2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер6 месяцев - 420 рублей
12 месяцев - 840 рублей**Хакер + 2 CD**6 месяцев - 690 рублей
12 месяцев - 1380 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:
107031, Москва, Дмитровский переулок, д 4, строение 2, ООО "ГеймЛэнд" (с пометкой "Редакционная подписка").

**Рекомендуем использовать
электронную почту или факс.****ВНИМАНИЕ!**Если мы получаем заявку
до 5-го числа текущего номера,
доставка начинается со
следующего номера**справки по электронной почте
subscribe_xa@gameland.ru
или по тел. (095) 935-7034**В случае отмены заказчиком
произведенной подписки, деньги за
подписку не возвращаются**ПОДПИСНОЙ КУПОН (редакционная подписка)**
Прошу оформить подписку на журнал "Хакер"

- | | |
|---|------------------------------------|
| <input type="checkbox"/> На 6 месяцев, начиная с _____ | <input type="checkbox"/> без диска |
| <input type="checkbox"/> На 12 месяцев, начиная с _____ | <input type="checkbox"/> 2 CD |
| (отметь квадрат, выбранного варианта подписки) | (выбери комплектацию) |

Ф.И.О. _____

индекс _____ город _____

улица, дом, квартира _____

телефон _____ подпись _____ сумма оплаты _____

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	Сумма
Оплата журнала "Хакер"	
с _____ 2004 г.	

Подпись платателя _____

Кассир _____

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	Сумма
Оплата журнала "Хакер"	
с _____ 2004 г.	

Подпись платателя _____

Кассир _____

Подписка для юридических лиц

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.



INTRO

В детстве нас приучали гордиться Родиной. Ну, знаешь, «зато мы делаем ракеты, перекрываем Енисей, а также в области балета мы впереди планеты всей». У нас было лучшее в мире одно и лучшее в мире другое, и вообще, лучшее в мире все. Потом оказалось, что мы в жопе. И лучшего в мире у нас нет ничего. И нужно срочно найти что-то, в чем мы догнали и перегнали хотя бы Гондурас. Но не находится. Реабилитация национальной гордости пришла, как ни странно, из-за бугра. Енисей тебе, я думаю, по барабану, как и балет. А вот то, что в России, по мнению всего «цивилизованного мира», водятся самые страшные, ужасные, хитрые и неуловимые хакеры, не может не греть, это уж как пить дать. А знаешь, какие вопросы мне задают европейские журналисты, которые получают от своих боссов задания написать про русских хакеров? Они спрашивают, состою ли я в русской е-мафии, есть ли у нее лидер и насколько цепко она держит в руках интернет. Я обычно отвечаю, что я и есть лидер русской е-мафии, крестный отец кибер-козаностры и вообще, все русские хакеры каждое утро собираются у редакции на переключку. Не верят, конечно, но чувство гордости за Родину остается на весь день...

CONTENT

НЬЮСЫ

04/МегаНьюсы

ЖЕЛЕЗО

16/ATI vs. nVidia: финальная схватка
21/Upgrade

2К3

22/2К3 Hacker's Choice

PC ZONE

26/Сделаем это по-быстрому: можно ли увеличить скорость копирования файлов?
30/Почтовые перехватчики: кто контролирует твою переписку?
34/Ставим бота на раздачу: как обмениваются файлами в IRC
38/Сетевой папарацци: быстро и без проблем скачиваем фотки из Сети
42/Красиво жить не запретишь: серьезный моддинг XP'шного интерфейса

ИМПАНТ

46/Заумный дом:
все о смышленном жилье

TIPS & TRICKS

▲ Ведущий рубрики Tips&Tricks Иван Скляр (Sklyarov@real.hacker.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах [I]. 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 :).

ВЫБЕРИ СВОЙ ТУННЕЛЬ

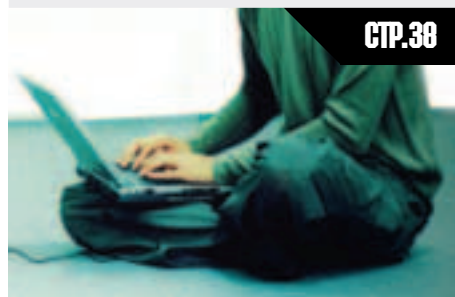
СТР.56



Учимся грамотно создавать сетевые туннели для шифрования данных.

СЕТЕВОЙ ПАПАРАЦЦИ

СТР.38



Стимулируем тягу человека к прекрасному - выбираем лучший софт для грабежа картинных интернет-галерей.

КОДИМ СОКЕТЫ НА MFC

СТР.90



Пишем бесконечные сетевые крестики-нолики при помощи MFC класса CSocket.

ВЗПОМ

50/Наск-FAQ

52/Разоблачение хакера: нашумевшие истории крупных взломов

56/Выбери свой туннель:

все о туннелировании трафика

60/VASH must die или как

противостоять шепккodu

64/Паканем и зашифруем: паковщики и протекторы исполняемых файлов

66/Социальная инженерия: хакерство без границ

72/Асечка на блюдечке:

занимательные корявости ICQ

75/Обзор эксплоитов

UNIXOID

76/Штирлиц отдыхает: криптография в любимой оси

80/Курс выживания в консоли:

изучаем командный интерпретатор в Zsh

ПАРСИМ ПРОСТОРЫ XML



Программируем свой модуль для перевода XML данных в MySQL и обратно.

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.

КОДИНГ

86/Осеп на службе пюдей:

IE для программиста

90/Кодим сокеты на MFC:

бесконечные крестики-нопики по Сети

94/Парсим просторы XML: обработка

XML-документов парсером PHP

ЮНИТЫ

98/ШароWAREZ

102/WWW

104/FAQ

106/Хумор

109/ë-mail

110/X-Puzzle

112/Хпроекты

/РЕДАКЦИЯ

>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xaker.ru)

>Редакторы рубрик

ВЗЛОМ

Иван «CutTe» Петров
(cutte@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

Андрей «Symbiosis» Рыбушкин
(cd@real.xaker.ru)

>Литературный редактор

Мария Альдубаева
(litred@real.xaker.ru)

/ART

>Арт-директор

Кирилл «KRO» Петров
(kerel@real.xaker.ru)

Дизайн-студия «100%КПД»

>Мега-дизайнер

Константин Обухов

>Гипер-верстальщик

Алексей Алексеев

/INET

>WebBoss

Скворцова Алена
(AlYona@real.xaker.ru)

>Редактор сайта

Леонид Боголюбов
(la@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

(olgaeml@gameland.ru)

Рубин Борис

(rubin@gameland.ru)

тел.: (095) 935.70.34

факс: (095) 924.96.94

/PUBLISHING

>Издатель

Сергей Похровский

(poxrovsky@gameland.ru)

>Учредитель

ООО «Гейм Лэнд»

>Директор

Дмитрий Агарунов

(dmitri@gameland.ru)

>Финансовый директор

Борис Скворцов

(bors@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 эти
случаях ответственности не несет.

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

НИТЕН

■ Алекс Ценьх (news@real.hacker.ru)

ЖЕЛЕЗО

■ Никита Кислицин (nikitoz@real.hacker.ru)

ВЗЛОМ

■ mindw0rk (xnews@real.hacker.ru)

УМНАЯ ПАРКОВКА

НИТЕН



Сингапурская компания Stratech Systems вышла на рынок с услугой по организации умных автомобильных стоянок. Информационный киоск на въезде вначале помогает найти свободное место для парковки, а потом - быстро разыскать свой автомобиль. После ввода регистрационного номера машины, на экране киоска появляется карта участка с точным указанием места, где припарковано авто. Система также выполняет охранные функции и следит за тем, чтобы на объекте не шатались посторонние. ■

ТЕДДИ НА СВЯЗИ

НИТЕН



Электронный медвежонок Wabi Buddy (www.wabi.com) стал самой популярной игрушкой, которую дети находили под елкой в минувшее Рождество. На фабрике мягкого плюшевого тедди начали беспроводной звуковой картой. Когда ребенок тискает медведя, проигрываются сообщения от занятых родителей. Колыбельную и сказку на ночь для малыша можно записать дистанционно по телефону. Для этого нужно набрать специальный бесплатный номер и ввести секретный код игрушки. Длительность сообщения ограничена 3 минутами. Телефонная приставка автоматически проверяет голосовую почту и загружает новые послания в память медведя. При этом игрушка может валяться на расстоянии до 50 метров от базы. Тедди вдруг

начинает весело подмигивать, напрашиваясь на общение. Кстати, медведь и сам знает несколько фраз. Wabi Buddy можно купить через интернет по цене около 70 долларов. ■

КЛАВА ДЛЯ МЕЛОМАНОВ

ЖЕЛЕЗО

О выходе на российский рынок нового устройства Creative Prodikeys DM сообщило недавно российское представительство компании. Назвать новинку "клавиатурой" у меня язык не поворачивается - это какая-то помесь синтезатора с Клавой :). Prodikeys DM умеет управлять продолжительностью звучания, изменением октав и тональности, предоставляя в распоряжение до 128 различных

музыкальных инструментов (фортепьяно, орган, медные, духовые и ударные инструменты). Кроме того, пользователи могут выбирать в качестве аккомпанемента любой из 100 возможных музыкальных ритмов (баллада, поп, данс, рок, джаз, фолк, латинские ритмы и др.).

Prodikeys DM подключается к ПК через порт PS/2 и поставляется в комплекте со специальным софтом, который поз-

волит на полную задействовать музыкальные возможности устройства. Новинку можно также использовать в качестве стандартного MIDI-контроллера с большинством музыкальных программ.

Стоит Creative Prodikeys DM \$90+налоги :).

■

ЦИФРОВОЙ ФОТИК ЗА 11 БАКСОВ

ВЗЛОМ



Интересной новинкой на рынке цифровых фотоаппаратов стала Dakota Digital. Примечательна она тем, что стоит всего \$11. Дело в том, что для получения снимков с этой камеры, ее нужно отправить в сервис-центр, где специалисты, путем шифров и махинаций, извлекают запечатленные фейсы, распечатывают их (или заливают на CD) и отсылают на указанный адрес. Фотик, конечно же, остается в центре. Долго ли, коротко ли, к Дакоте Диджитал проявили интерес хакеры. Расковыряли, посмотрели, кое-чего подправили и опа... из одноразовой побрякушки Дакота превратилась в цивильную вещь для домашнего пользования. 2 мегапикселя, память на 25 снимков, вспышка, все дела - почти Canon PowerShot A60 за \$250. А главное - в фотике имеется USB-порт для слива изображений на писк (именно он был ранее недоступен). Не знаю, как ты, а я не прочь запастись дюжиной-другой цифровиков по \$11 каждый. Можно продавать на рынке по 100 баксов - очередь будет как за колбасой в сталинские времена. Пока неизвестно, как отреагирует на выпад хакеров компания Dakota. Возможно, она усилит защиту, а еще вероятнее, что просто снимет DD с производства. Так что закупай быстрее оптовую партию. Куй железо, пока горячо. ■



СДЕЛАЙ САМ: ПОЮЩАЯ РЫБА

НІТЕСН



Пинкусид из Техаса вправил мозги поющей рыбе. Он обучил ее высказываниям знаменитых людей. При помощи отвертки рыбе "вспорили" брюшко, и место CMOS-чипа занял встраиваемый программируемый контроллер. Новый мозг быстро нашел общий язык с головой и хвостом. Куда больше времени ушло на синхронизацию речи и движений рта. После анализа спектрограмм было решено привязаться к гласным звукам. В итоге, рыба заговорила голосом саксофониста Клинтона. На конкурс Embedded Linux Journal автор заявил усовершенствованную рыбку: все комплектующие размещались внутри корпуса из пластмассы. Видеоролики и подробные инструкции по сборке доступны на сайте <http://bigmouth.here-n-there.com/>. ■

15-ГИГОВАЯ ФЛЕШКА

ЖЕЛЕЗО

Новую версию 2,5" флеш-диска с интерфейсом Ultra Narrow SCSI выпустила корпорация M-Systems. Таким образом, линейка этих носителей представлена моделями объемом от 256 Мб до 15 Гб. Как и 3,5" носители, интерфейс FFD 2,5" Ultra Narrow SCSI соответствует стандартам SCSI-2 и SCSI-3, скорость последовательного чтения и записи составляет 17 Мб/с и 11,5 Мб/с соответственно. ■

Краткие спецификации:

- ▲ Емкость - до 15,3 Гб (неформатированная емкость - 15360 Мб)
- ▲ 50-контактный разъем
- ▲ Скорость пакетного чтения/записи - 20 Мб/с
- ▲ Время доступа - менее 20 мкс
- ▲ Ударопрочность - до 1500g
- ▲ Более 5 млн. циклов перезаписи
- ▲ Размеры - 100,2x69,8x11,3-26,6 мм
- ▲ Вес - от 0,1 до 3 кг - в зависимости от модели
- ▲ MTBF - 971130 часов для 512 Мб модели, 952925 часов для 2 Гб
- ▲ Питание - 5 В±5%

ATHLON 64 3000+

ЖЕЛЕЗО

Без пафоса и лишнего шума - как всегда - компания AMD пополнила линейку своих 64-разрядных Socket 754 процессоров для настольных ПК кристаллом Athlon 64 3000+. Самое же смешное в PR-рейтинге 3000+ заключается в том, что тактовая частота нового камня такая же, как у Athlon 64 3200+, то есть 2 ГГц. Снижение рейтинга произошло из-за урезанного вдвое - до 512 Кб - кэша L2. Остальные показатели нового камня как две капли воды схожи с характеристиками Athlon 64 3200+: поддержка памяти DDR400, CPUID 0F48h, напряжение питания ядра 1,50 В, TDP - 89 Вт, поддержка технологии Cool'n'Quiet. Зато стоит новый кристалл почти вдвое дешевле старшего брата - \$218. Одновременно с представленным пресс-релизом компания почти на 20% снизила цену на мобильный процессор Athlon 64 3000+ класса DTR. ■

ЖЕЛЕЗНЫЙ НОСИЛЬЩИК

НІТЕСН



В Японии представили робота-носильщика. Шагающий двуногий гигант вместе с чемоданом закидывает на плечи самого хозяина. Дождавшись, когда тот усядется, робот WL-16 поднимает алюминиевое кресло над головой при помощи телескопических штанг. Двенадцать приводов позволяют ему совершать перемещения вперед, назад и вбок. Длина шага составляет от 30 до 136 сантиметров. Кроме того, робот умеет ходить по лестнице, поднимая ноги перед не очень высокими ступенями. WL-16 наблюдает за тем, чтобы кресло всегда оставалось в равновесии. Если человек начинает беспокойно ерзать, робот останавливается, а затем снова продолжает движение. Максимальная полезная нагрузка пока ограничена 60 килограммами. WL-16 управляется с дистанционного пульта, но совсем скоро будет оборудован собственным контроллером с джойстиком. Взять робота в слуги можно будет с 2005 года, когда начнутся продажи WL-16.

ПАРОЛЬ НА ИНТЕРНЕТ ДЛЯ ВСЕЙ ДЕРЕВНИ

ВЗЛОМ

27 ноября 2003 года директор частного предприятия города Губкинский передал в местную дежурную часть заявление. "Обокрали, ироды! Посягнули на святое. На инет посягнули", - говорилось в заявлении. А дальше шла душеспитательная история о том, что на протяжении полугода неустановленный хакер зверским образом эксплуатировал безлимитный аккаунт, купленный фирмой на последние сбережения. "Короче, ущерб нам причинили в 301309 рублей. Требуем возмещения", - попытожил директор. Почитал оперуполномоченный человек письмо, почесал в затылке и молвил: "Проснулись, млин!" Но дело завел. Через какое-то время стало известно, что пароль на этот аккаунт чуть ли не на каждом столбу намалеван, и юзается уже который месяц всем городом со всеми его окрестностями. А добрый дядя директор только денежку платит. Непонятно, почему дядя сразу не обратился в ментуру или хотя бы не сменил пароль, но то, что свои 300 тысяч он получит не раньше, чем состарятся его внуки, ясно наверняка.

ДУХ ЯПОНЦЕВ ПОВЯЗАЛИ ЗА ОБМЕН ФАЙЛАМИ

ВЗЛОМ

Представь себе следующую ситуацию. Сидишь ты в сетке, чатишься с кентом, спрашиваешь его: "А нет ли у тебя, кентуха, фильма "Джей и молчаливый Боб"? Давно, понимаешь, ищу". "Как же, имеется", - отвечает кент, но в ответ просит рядового Райна, которого нужно спасти. И только вы обменялись по сетке мувиками, как раздается стук в дверь, и грозный голос требует: "Откройте! Милиция". И уже через полчаса сидишь ты в сырой камере, весь в страхе и непонятках. Кажется маловероятным? А вот такая хрень недавно приключилась с двумя самураями, вся вина которых в том, что они были пользователями файлообменной сети Winny. Помимо 41-летнего и 19-летнего японцев, сетка объединяет еще 250 тыс. человек, но полиция оказалась неравнодушной именно к этой парочке. Первого обвинили в незаконном распространении фильма "Игры разума", второго - игрушки "Super Mario Advance". Судя по всему, парням придется стать козлами отпущения, т.к. крупные компании, включая Nintendo, всерьез намерены показательно взыскать с пацанов большой штраф, чтобы другим неповадно было. Непонятно только, как попались эти двое. Ведь Winny - исключительно анонимная сеть, и считалось, что каждый участник в ней хорошо защищен. ■

MS LONGHORN ДЕБЮТИРОВАЛ В МАЛАЙЗИИ

ВЗЛОМ



В то время как Билл и Со. доводят до ума свою новую красу и гордость ОС Longhorn, малазийские пираты уже вовсю торгуют этой гордостью на своих Горбушках по 2 бакса за килограмм. Оперативностью парней из Малайзии можно восхищаться стоя - не успевают разработчики объявить о начале работы над программой, как в стране восходящего пиратства эта софтина уже становится антиквариатом. Так и здесь, официальный релиз Longhorn должен состояться не ранее начала 2005 г., а с учетом всех непредвиденных обстоятельств - вообще к середине. Но в Малайзии рынки уже переполнены копиями пре-альфы, стыренной с октябрьской конференции

программеров в Лос-Анджелесе. Усилиями полиции и представителей MS удалось изъять около 8 тысяч копий пиратского Лонгхорна, но этого слишком мало, чтобы назвать операцию успешной. Сотрудники компании заверяют, что выставленная на продажу версия еще очень сыра, глючит и может вообще заколбасить всю систему. Но разве останутся эти заверения истинных любителей варежа?

Кстати, несмотря на то, что в России пока новой ОС на прилавках не наблюдается (не сегодня, так завтра), многие пытливые российские умы уже полгода назад успели вкусить прелестей Лонгхорна. На некоторых security-форумах даже ведется обсуждение возможных багов в ядре. ■

ХАЙ-ТЕК ВИЗИТНИЦА

НИТЕН



Компания Visioneer (www.visioneer.com) представила хай-тек визитницу. Устройство CardReader 100 в считанные минуты разбирает гору карточек с выставки. Девайс подключается к компьютеру через порт USB. Сканируя визитки одну за другой, CardReader складывает контакты в базу данных. При этом автоматически распознаются поля с именем, адресом и телефоном личности, а оригинальное изображение визитки доступно для сверки. В дальнейшем информация из базы данных может быть передана на карманный компьютер или занесена в электронную адресную книгу. Устройство настолько компактно, что умещается в кармане пиджака. Продается в интернете по цене около 150 долларов. ■

ЦИФРОВОУХА ОТ ROLLEI

ЖЕЛЕЗО

Новую цифровую камеру dp3210 представила компания Rollei. Новинка оснащена объективом с десятикратным оптическим приближением, 3,3-мегапиксельным сенсором и умеет алгоритмически увеличивать изображение в четыре раза. ■

Краткие характеристики Rollei dp3210:

- ▲ Объектив - 10x D-VarioArogon, фокусное расстояние 5,7-57 мм (35-350 мм в 35-мм эквиваленте)
- ▲ Минимальная дистанция фокусировки - 50 см (обычный режим), 120 см (телескопический) и 10 см (макро)
- ▲ ЖК-дисплей - 2,5" TFT, 119548 пикселей
- ▲ Видоискатель - электронный 0,33", 114000 точек
- ▲ Настройка времени выдержки - programmed AE, aperture-priority AE, shutter-priority AE, ручная
- ▲ Экспонометр - spot/center-weighted average, ручная настройка с шагом 1/3 EV
- ▲ Светочувствительность - ISO 70 - 400
- ▲ Таймер - 2-10 с
- ▲ Непрерывная съемка - 1,25 кадра в секунду или 3,3 кадра в секунду при съемке серий по 9 кадров
- ▲ Запись видео - 320x240, 15 кадров в секунду, AVI
- ▲ Носитель - Secure Digital
- ▲ Интерфейсы - USB, ТВ-выход (PAL/NTSC)



ЗАРЯДИ МОЗГИ

HITECH



Южнокорейская компания DreamFree (www.dream-free.com/english) представила зарядное устройство для мозга. С его помощью можно быстро привести мысли в порядок. Персональный энцефалограф Реед включает в себя программу для Pocket PC, наушники и серебряные очки с линзами из непрозрачного пластика. В режиме "концентрации" в наушниках звучит ритмичная инопланетная мелодия, а очки испускают свет. Каждый глаз получает предназначенный для него сигнал. Световые ванны нужно принимать с закрытыми глазами. В конце концов, синхронизация частот позволяет настроить мозг на нужную волну. Другие режимы помогают сосредоточиться, развить память и даже погрузиться в глубокий сон. Стоимость новинки составляет около 300 долларов. ■

MEMOREX ИДЕТ

ЖЕЛЕЗО

Небезызвестный производитель оптических накопителей, компания Memorex, сообщила о выпуске внутреннего DVD-рекордера Memorex True 8X Dual Format, способного записывать как DVD+R, так и DVD-R диски со скоростью 8x. Причем представители компании утверждают, что все конкурентные разработки достигли скорости 8x благодаря перепрошивке электроники и увеличению до предела мощности лазера, в то время как Memorex решила эту проблему пересмотром архитектуры привода.



Ниже приведены краткие спецификации новинки:

- ▲ База привода 8x8 True 8X - Memorex 4X4 Dual-X
- ▲ Технология стабилизации привода для снижения вибрации

несбалансированных дисков при высокоскоростной записи

▲ Система определения дефектов, позволяющая увеличить количество циклов перезаписи (по сравнению с "испытательными" DVD-приводами) без ухудшения качества диска или производительности

▲ Время работы без отказа 60 тыс. часов - почти на 20% больше, чем у среднестатистических конкурентных решений

▲ 2 Мб буфер

▲ Скорость записи CD-R - 40x, перезаписи DVD+RW - 4x, DVD-RW - 4x, CD-RW - 24x

▲ Скорость чтения DVD-ROM - 12x, CD-ROM - 40x

Новинка представлена в двух вариантах - с корпусами черного и серебристого цветов. В продаже устройство появится в начале января, производитель рекомендует покупать устройство по цене не выше \$250. В комплекте с новинкой идет один DVD-RW диск, руководство, 2 кабеля и крепежные винты. ■

ЛЕГКИЕ как перышко

ЖЕЛЕЗО

Компания Toshiba представила свою новую линейку сверхлегких ноутбуков форм-фактора B5 - Dynabook SS SX/210LN с 12,1-дюймовым XGA экраном. Новинки выгодно отличаются от конкурентов - весят ноутбуки по 990 граммов, при этом могут работать вдали от цивилизации до пяти с половиной часов. Поставки устройств начнутся в январе, ожидается, что их розничная цена не превысит \$2000.

Модель Dynabook SS SX/210LNLN оборудована 12,1-дюймовым XGA ЖК экраном, 1,0 ГГц ULV (Ultra Low Voltage) версией процессора Pentium M (чипсет Intel 855GM), 256 Мб памяти PC2100 (до 1 Гб), 1,8-дюймовым винчестером емкостью 20 Гб. Модель SS SX/210LNLW весом 1,1 кг будет также отличаться наличием 2,5-дюймового 40 Гб винчестера и наличием беспроводного интерфейса IEEE 802.11b/g. ■



Конкурс!

Журнал Хакер и компания RRC проводят конкурс

1. Создай свой баннер по теме «LCD-монитор»
2. Пришли его по адресу viewsonic@rrc.ru
3. И участвуй в конкурсе на лучшего дизайнера

Итоги конкурса будут подведены в следующем номере журнала.



Главный приз — LCD монитор

ViewSonic VE155s

10 дополнительных призов - «Большая энциклопедия Кирилла и Мефодия» на DVD-диске.

Спонсор конкурса —

RRC Focus Distribution

официальный дистрибьютор мониторов ViewSonic

т. 956-1717
focus@rrc.ru
www.rrc.ru

АНТИВАНДАЛЬНАЯ ТРИБУНА

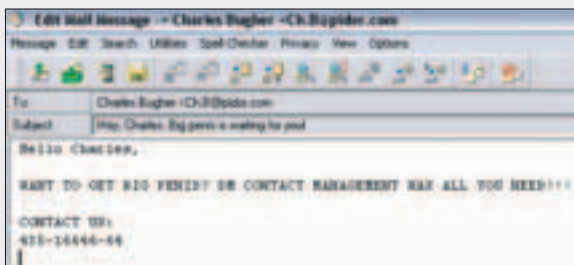
HITECH



Ученые питерского Политеха получили патент на хай-тек трибуну для футбольных болельщиков. Теперь фанаты смогут без кулаков и кровопролития выплеснуть агрессию и утереть нос соперникам. В скамейки на стадионах будет встраиваться небольшое устройство. При раскачивании трибун оно регистрирует всплески эмоций болельщиков, определяет самых активных и передает сообщение на информационное табло. К радости тех, кто не щадил пятой точки и дружно сотрясал сиденья, над стадионом загорается название любимой команды. Чтобы трибуны не вывалили с корнем, хай-тек скамейки будут надежно прикованы танковыми амортизаторами. ■

ПОЛИЦИЯ ЗАЩИТИЛА СПАМЕРА ОТ ПРОГРАММИСТА

ВЗЛОМ



Чарльз Бухер в последнее время чувствовал себя неважно. Сердечко побаливало на нервной почве, одолевали приступы агрессии. И все из-за компании DM Contact Management, занимающейся продвижением "единственно-эффективного средства для увеличения пениса". DM CM проявила особую заботу о пенисе Чарльза. "Одумайтесь, мистер Бухер, - говорилось в многочисленных письмах, - ведь пенис - это Ваше лицо, Ва-

ша гордость. Доверьте нам свой пенис, и мы из него конфетку сделаем. Любая топ-модель рухнет без чувств от любви". И так изо дня в день, неделя за неделей. Письма приходили, самочувствие Чарльза ухудшалось. В конце концов, бедолага не выдержал, позвонил в офис компании и крикнул страшным криком, что если еще хоть одно гребаное письмо предложит ему удлинить член, он придет с электродрелью и кухонным ножом, порубает всех

сотрудников в капусту, кастрирует, а их удлиненные на средства компании пенисы зажарит на сковороде и съест. И звучало все это так убедительно, что на этот раз поплехело президенту Contact Management Дугласу Маккею. Опасаясь за сохранность своего достоинства, Дуглас позвонил в полицию и пожаловался им на маньяка. А вдогонку сообщил, что никакого отношения к спаму его конторка не имеет, и вообще - это происки конкурентов, которые тем самым хотят подорвать авторитет его компании. Бухера тем же вечером повязали и вскоре отпустили под залог в \$75 тыс. Сейчас полным ходом идут разбирательства, кто на самом деле прав, а кто виноват. Но если Чарльза признают виновным, ему грозит до 5 лет тюрьмы и штраф в 250 тысяч баксов. ■

2 ГИГА В ДЕТСКОЙ ПАДОШКЕ

ЖЕЛЕЗО

Корпорация Transcend представила общественности свою новую разработку - жесткий диск формата 1" (2,54 см) 2.2GB CF+ Type II 1" HDD. Носитель предназначен для использования в mp3-плеерах, цифровых фотокамерах, ноутбуках и других портативных устройствах. Применение новинок в таких устройствах открывает потребителям новые горизонты - емкости диска достаточно для хранения 80 видеоигр или более 250 цифровых снимков с разрешением 3 млн. пикселей в формате RAW.

Ниже приведены основные технические спецификации новинки:

- ▲ Напряжение питания для носителя - 3,3 или 5 В (автоопределение)
- ▲ Емкость - 2,2 Гб
- ▲ Скорость последовательной передачи данных - от 3,3 до 6,5 Мб/с
- ▲ Скорость вращения шпинделя - 4200 об./мин
- ▲ Время позиционирования - 10 мс
- ▲ Размеры - 42,8x36,4x5,0 мм

Столь значительные успехи в разработке сверхкомпактных жестких дисков пока не отражаются на динамике продаж. По результатам 2003 года на рынке по-прежнему доминируют 3,5" диски, их доля составила 82% (т.е. 180 млн. штук), оставшиеся 18% занимают диски формата 2,5" - их продали около 41 млн. штук. Но совершенно очевидно, что со временем будет осуществляться переход на 2,5-дюймовые диски, поскольку их объемы приближаются к трехдюймовым, а благодаря размерам их удобно использовать в производстве ноутбуков, которые медленно, но верно вытесняют обычные настольные компьютеры. ■



Хотите получить больше времени для отдыха ?



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



- гарантия 2 года
- покупка в кредит
- design for Windows XP
- всестороннее тестирование
- сертифицирован "РосТестом"
- клавиатура и мышь в подарок
- оплата через операционную кассу банка
- компьютер по индивидуальному заказу без предоплаты

Приобретите ПК, который позволит Вам обмениваться фотографиями с друзьями при работающей в фоновом режиме программе антивирусного сканирования и не ощущать при этом замедления работы. Приобретите компьютер "МИР VIP" на базе процессора Intel® Pentium® 4 с технологией HT уже сегодня.



КОМПЬЮТЕРЫ ОРГТЕХНИКА
КОМПЛЕКТУЮЩИЕ

<http://www.fcenter.ru>

салоны-магазины в Москве :

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

БЕЗ СЛОВ

HTECH



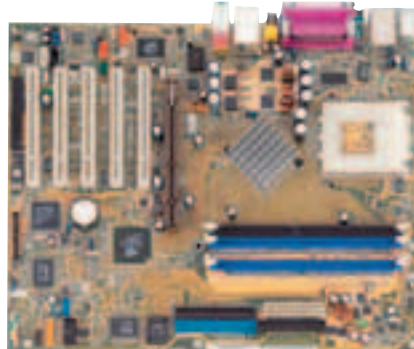
Представлен прототип устройства для передачи чувств на расстоянии. Эксперименты

проводит научная лаборатория Intel. Новый девайс предназначен для использования друзьями и влюбленными. Встроенный в наручные часы акселерометр фиксирует ориентацию руки и очевидные жесты. Достаточно провести по пальцу, чтобы партнер получил только ему понятное сообщение. Носимый на запястье девайс принимает сигналы дружественного устройства и испытывает ряд деформаций. Он изгибается и вибрирует, слегка сжимает запястье. Резистивные датчики могут подарить человеку ощущение легкого прикосновения к руке. Передачей последовательных импульсов это чувство многократно усиливается. Технология Flexinol позволяет имитировать рукопожатие как напряжение специальных волокон, через которые проходит электрический ток. Используя физический эффект Пельтье, девайс также может нагревать и охлаждать небольшой участок кожи. Устройство находится только на стадии разработки, но интерес к чудо-коммуникатору небывалый. ■

МАМА ASUS

ЖЕЛЕЗО

О выпуске усовершенствованной версии платы A7N8X сообщила недавно компания ASUSTeK Computer. Новый вариант мамки - A7N8X-E Deluxe - отличается от базовой версии наличием Wi-Fi слота для построения беспроводных сетей стандарта IEEE



802.11b и наличием 1 Гбит/с (Gigabit) сетевого адаптера.

Спецификации новинки:

- ▲ Поддержка процессоров AMD Athlon XP, Athlon и Duron
- ▲ Чипсет nForce2 Ultra 400 + nForce2 MCP-T

- ▲ Системная шина 400 МГц
- ▲ Память PC3200/2700/2100/1600 non-ECC DDR SDRAM
- ▲ Двухканальный интерфейс памяти DDR 400
- ▲ Слот AGP Pro/8x
- ▲ Слот Wi-Fi (платформа ASUS Wi-Fi@HOME)
- ▲ Два порта Serial ATA
- ▲ 1 Гбит/с адаптер (Marvell) плюс 10/100 Мбит/с адаптер (NVIDIA)
- ▲ Порт IEEE 1394
- ▲ 6 портов USB 2.0
- ▲ Платформа ASUS Wi-Fi@HOME специально разработана для упрощения процесса построения и настройки беспроводной домашней сети. ASUS Wi-Fi@HOME включает в себя три элемента - материнскую плату ASUS с эксклюзивным слотом Wi-Fi, WLAN карту-адаптер ASUS WiFi-b и программный узел доступа ASUS Software AP (access point).

A7N8X-E Deluxe продается в двух версиях - обычной (только плата) и беспроводной, в комплект поставки которой входит беспроводная сетевая карта WiFi-b. В беспроводной комплектации A7N8X-E представляет собой сетевое решение три в одном: беспроводная сеть 802.11b и проводные 1 Гбит/с и 10/100 Мбит/с сетевые адаптеры. ■

АНАЛОГОВАЯ цифра

ЖЕЛЕЗО

Полтора года назад корпорации Leica и Panasonic представили свою первую совместную разработку - цифровую камеру Digilux 1. И вот совсем недавно компания выпустила пресс-релиз, в котором анонсировала новую версию своей цифровой камеры, Digilux 2, назвав ее "аналоговой" цифровой. Само собой разумеется, что аналоговых элементов в устройстве не осталось, под "аналоговостью" производители понимают выполненные в стиле классической зеркальной дальномерной камеры элементы управления временем выдержки и настройки на резкость. Эти параметры можно лихо менять, вращая столь привычные для опытных фотографов кольца на объективе и щелкая переключателем на корпусе.

Новинка оснащена отличным 5-мегапиксельным сенсором, качество работы которого способно удовлетворить даже консервативных любителей пленочного фото. Собственно, устройство так и позиционируется - оно призвано завоевать сердца тех фотографов, что до сих пор не смогли расстаться со своими старыми добрыми пленочными камерами. ■

Краткие спецификации Digilux 2:

- ▲ Объектив - LEICA DC VARIO SUMMICRON, фокусное расстояние 7-22,5 мм (28-90 мм в 35-мм эквиваленте), апертура f/2 - f/2,4
- ▲ Сенсор - 2/3" CCD, 5 млн. пикселей
- ▲ ЖК-дисплей - TFT 2,5", 211000 пикселей
- ▲ Видоискатель - электронный, 235000 пикселей, 100% кадра
- ▲ Накопитель - SD/MMC, вместе с камерой поставляется 64 Мб
- ▲ Управление таймером - при подключении к ПК
- ▲ Интерфейсы - USB 2.0, ТВ PAL/NTSC



TIPS & TRICKS

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

▲ Если ты взял у друга поиграть игру, которую "нельзя запускать без диска", то можно попробовать просто вставить свой диск той же компании локализаторов, очень вероятно, что игра пойдет без диска друга. Однако этот способ работает не со всеми играми.

Empoc
empoc@list.ru

▲ Если в проге после русификации вместо нормальных слов всякая хрень - не спеши лезть своими шаловливыми ручками в реестр. Можно попытаться исправить это более простым способом: открой файл русификации Блокнотом (или его аналогом) и найди строку "Unicode=0". А теперь поменяй "0" на "1". Все, теперь наслаждайся результатом.

Shanker
shanker@mail.ru

▲ Чтобы узнать свой IP в XP, не нужно писать что-то вроде winipcfg, достаточно сделать двойной клик в трее на значке подключения и выбрать "Свойства подключения". На экране будет показана табличка, в которой адрес клиента - это твой адрес, а адрес сервера - сервер твоего прова.

Shanker
shanker@mail.ru

ПЕСНИ ИЗ ЯДЕРНОЙ ЛАБОРАТОРИИ

ВЗЛОМ



В Великобритании прошло судебное слушание по делу Джозефа МакЭлроя. С виду парень как парень, а натворил ТАКОЕ. Впрочем, ничего особенного не натворил. Просто хотел скачать пару-тройку хитов клевой музыки, но перепутал адрес, заблудился и невзначай попал в дебри сети американской ядерной лаборатории.

"Где я?" - прошептал парнишка в испуге. "Сейчас мы тебе все объясним", - заверила подоспевшая полиция и, взяв под ручки горе-хакера, повела его на допрос. "Позвольте, я музыку скачивал!" - воспротивился Джози. "Ты поставил под угрозу национальную безопасность страны!" - сурово молвил усатый опер. А тут еще сотрудники лаборатории горько заплакали, мол, из-за этого маленького засранца пришлось на три дня всю сеть отрубить. В общем, так запугали юнца, что тот с перепугу во всем признался. Да, мол, взломал, да, ядерную вашу лабораторию, черт бы ее побрал. Расстреливайте, только отстаньте. Мальчика пожалели, немножко поругали и для приличия оштрафовали. А напоследок погрозили пальчиком: "Музычку, Джози, нужно покупать на компактках и исключительно лицензионную. Иначе вон оно как бывает". ■

СКАНЕР ДЛЯ ПРОФИ

ЖЕЛЕЗО

Пинейку ScanMaker пополнила недавно выпуском нового сканера ScanMaker 6100 корпорация Microtek. Это устройство относится к разряду моделей старшего уровня - новый сканер обеспечивает разрешение до 3200x6400 dpi, 48-разрядную глубину цвета и оснащен портом USB 2.0. Предыдущие модели сканеров Microtek, ScanMaker 6700 и 6800, обеспечивали разрешение 4800x2400 dpi. При этом, по данным европейского представительства компании, во время "горячего" рождественского сезона с 1 декабря по 31 марта сканер будет продаваться по цене около \$260.

ScanMaker 6100 оснащен двумя фильм-адаптерами EZ-Lock и может сканировать отрезки 35-мм позитивной и негативной пленки, а также пластинки 6x9 и снимки 10x15 см. Вместе с устройством поставляется специальное ПО LaserSoft SilverFast SE для Windows и Mac OS X, содержащее инструменты для коррекции

качества изображений, удаления эффектов, вызванных наличием пыли или повреждением поверхности. Это, конечно, не Digital ICE, как в ScanMaker 6800, но тоже неплохо, а там, глядишь, и ScanMaker 6900 появится. ■

Краткие характеристики ScanMaker 6100:

- ▲ Тип - сканер A4 с фильм-адаптером, площадь сканирования документов и снимков - 216x297 мм, пленок и пластинок - 101,6x127 мм
- ▲ Разрешающая способность - 3200x6400 dpi
- ▲ Максимальное разрешение - 65536 dpi (Win), 32768 dpi (Mac)
- ▲ Глубина цвета - 48 разрядов цвета, 16 разрядов для монохромных изображений (65536 оттенков серого), 1 разряд в режиме черно-белых документов
- ▲ Размеры - 485x295x77 мм
- ▲ Вес - 3,1 кг



ДОСТУПНЫЙ
ИНТЕРНЕТ

ЭКОНОМИЯ ТЕЛЕФОН
НЕЗАВИСИМО ОТ
НАПРАВЛЕНИЯ

РАЙОННАЯ МАН. СЕРВИС И ИНФОРМАЦИЯ АД № 10007, 10007, 20010

WWW.PROPUK.COM

780-35-30

МДМ II КИНО



В ЗАЛЫ СО ЗВУКОМ DOLBY DIGITAL EX
ТОЛЬКО У НАС МОЖНО СМОТРЕТЬ КИНО ЛЕЖА
ДО 20 НОВЫХ ФИЛЬМОВ В МЕСЯЦ

м.м. Фрунзенская
Комсомольский проспект, д. 28
Московский Дворец Молодежи

ответчик: 961 0066
бронирование билетов по телефону 782 8833

МДМ.КИНО
на пуфиках

СИСАДМИНЫ ТРЕБУЮТ ПРОФСОЮЗ

ВЗРОН



«Тварь я дрожащая или таки имею право?» - спросили сами себя сисадмины на сайте sysadmins.ru и сами себе же ответили: "Таки имею право". Права - они по любому есть, но их еще надо и знать. А админам куда интереснее лишний раз полистать "Библию системного администратора", чем разбираться в уголовном кодексе и "праве на труд". Поэтому было решено, что рассмотрением сисадминских прав будет заниматься новый профсоюз. Сисадминский. Идея его создания не нова - секьюрити гайз в специализированных конфах уже давно пытались подбить народ на организацию профсоюза. Кто, как не он, защитит сисадмина, пока тот защищает сервак? И вот, наконец, настало время X. Состав, устав и прочие регалии были оговорены на втором Семинаре Системных Администраторов и Инженеров (SYSM.02) 20 декабря 2003 г. Общие положения профсоюза можно почитать на sysadmins.ru/union/ustav.php. ■

ВИДЮХА-КРАСАВИЦА

ЖЕЛЕЗО

Производитель видеокарт и системных плат, тайваньская компания Albatron Technology, анонсировала две видеокарты на чипе GeForce FX 5900: FX5900XT и FX5900XTV. Спецификации обеих новинок практически идентичны, разница заключается лишь в том, что FX5900XTV поддерживает VIVO. ■



Характеристики:

- ▲ Графический процессор - GeForce FX5900XT
- ▲ Память - 128 Мб DDR SDRAM
- ▲ Ширина шины памяти - 256 бит
- ▲ Тактовая частота ядра - 390 МГц
- ▲ RAMDAC - 400 МГц
- ▲ Максимальное поддерживаемое разрешение - 2048x1536@75Hz
- ▲ Шина - AGP 8X/4X
- ▲ VGA-выход - есть
- ▲ TV-тюнер - нет
- ▲ TV-выход - есть
- ▲ VIVO - нет (есть у FX5900XTV)
- ▲ DVI - есть
- ▲ CineFX 2.0 поддерживает DirectX9.0 и OpenGL1.4
- ▲ NVIDIA UltraShadow

СЕРВЕРНАЯ МАМА

ЖЕЛЕЗО

Выпуск материнской платы PR-DL(S)533/RACK, специально рассчитанной на использование в стоечных серверах 1U и 2U, сообщила недавно компания ASUSTeK Computer. Отличительная особенность новинки - специальная разводка PR-DL(S)/RACK, обеспечивающая лучшую циркуляцию воздуха над слотами памяти и радиатором, что повышает надежность системы. Новинка имеет два слота PCI-X, будут выпускаться версии с интегрированным SCSI-контроллером и без него.

PR-DL(S)533/RACK выполнена на чипсете ServerWorks GC-LE (CMIC-LE), поддерживающем два процессора Intel Xeon на системной шине 533 МГц, что позволяет установить процессоры с тактовой частотой 3,2 ГГц. Для сбалансированной производительности в локальных сетях PR-DL(S)533/RACK имеет 1 Гбит/с сетевые адаптеры Intel 82540 и 82554.

Ключевые спецификации платы:

- ▲ Два процессора Intel Xeon до 3,2 ГГц
- ▲ Северный мост - ServerWorks GCLE (CMIC-LE)
- ▲ До 12 Гб registered PC2100 ECC DDR RAM, 6 слотов DIMM
- ▲ Опциональный двухканальный Ultra320 SCSI контроллер
- ▲ Интегрированный 1 Гбит/с сетевой адаптер Intel 82540 и 1 Гбит/с сетевой адаптер Intel 82554
- ▲ VGA-адаптер ATI Rage-XL с 8 Мб графической памяти
- ▲ 64-разрядный PCI-X слот с тактовой частотой 133 МГц и напряжением питания 3,3 В, 64-разрядный PCI-X слот с тактовой частотой 66 МГц и напряжением питания 3,3 В

В варианте платы с SCSI адаптером, слот PCI-X поддерживает MD3 низкопрофильную ZCR карту LSI MeGaRAID SCSI320-0 ZCR и карту Intel SRC ZCR в форм-факторе 2U. Поставки системных плат ASUS PR-DL(S)533/RACK уже начались. ■

РОБОТ-БИБЛИОТЕКАРЬ

НИТЕСИ



Японские ученые создали робота, который ходит в библиотеку вместо хозяина. Коробка на колесах 50x45 сантиметров снабжена видеокамерой и механической рукой. Робот использует лазерные сенсоры, чтобы лавировать между полками и объезжать других посетителей библиотеки. Человек отдает инструкции через интернет. Найдя нужную книгу, машина берет ее с полки и механическими пальцами листает страницы. Изображение текста через интернет поступает на экран монитора. Работы по совершенствованию робота продолжаются. Сейчас его обучают, как вытаскивать плотно зажатые томики книг и возвращать литературу на место. ■



Лондон ждет тебя!

Купи диски Digitex и выиграй СуперТур в Лондон, а также один из тысячи других призов.

Найди на внутренней стороне вкладыша упаковки с дисками одну из наклеек:



Заполни купон и отправь его с наклейкой организатору до 30 июня 2004 года...
... и получи приз

Спешите, количество призов ограничено. Рекламная акция завершается 30 июня 2004 года, либо ранее этой даты, с момента передачи всех призов победителям.

Читай полные правила на сайте www.digitex.ru

ХОРОШИЙ ЧЕРВЬ ОКАЗАЛСЯ НЕ ТАКИМ УЖ ХОРОШИМ

ВЗЛОМ



На просторах интернета появилось интересное решение, призванное окончательно нейтрализовать Lovesap. Это новый червь Worm.Win32.Welchia, который дает каждому зараженному компьютеру противоядие от своих злых собратьев. Эдакий санитар сетей. Некоторое время Welchia добросовестно выполнял свою работу, проникая на машины с виндой и ставя заплатки на уязвимые сервисы RPC DCOM. Но все пошло наперекосяк, когда гуманный червячок проник в банковскую сеть Diebold, объединяющую большое количество банкоматов. Работающие по управлению Windows XP Embedded, банкоматы не поняли добрых намерений Welchia и на всякий случай поголовно вышли из строя. В большей степени тому способствовала повышенная сетевая активность, из-за которой банкоматы прекращали работу. Досадную проблему компании Diebold уже удалось устранить, но успокаиваться червячок не собирается. В конце осени он парализовал работу всех консульских представительств США. И еще неизвестно, каких дел натворит в будущем. ■

SUNDEVIL НАНОСИТ ОТВЕТНЫЙ УДАР

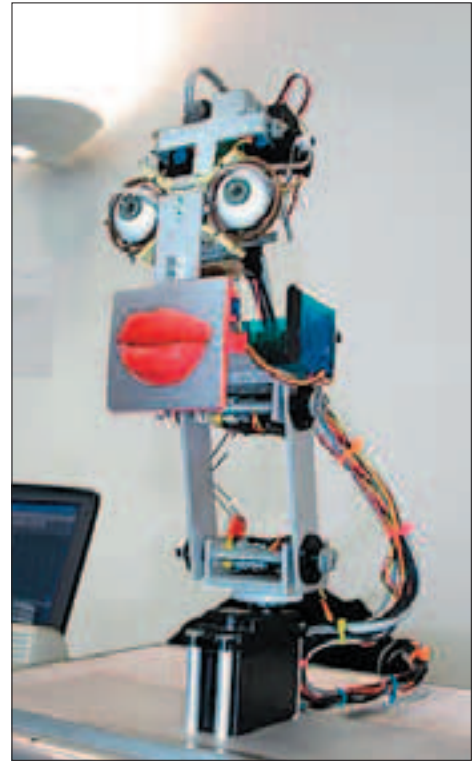
ВЗЛОМ

Недавно правоохранительные органы США подвели итог операции по борьбе с киберпреступностью, которая началась 1 октября 2003 г. Благодаря тесному сотрудничеству ФБР, секретной службы и федеральной комиссии по торговле, удалось арестовать 125 человек. Среди них оказались как обычные пираты и компьютерные взломщики, так и те, кто незаконно продает высшие награды на интернет-аукционах. В ходе операции выявилось более 125 тыс. американцев, пострадавших от мошенников. А общая сумма награбленного составила 100 миллионов долларов. Газеты называют состоявшуюся операцию самой крупномасштабной из всех, направленных на искоренение компьютерного зла. А генеральный прокурор США Джон Эшкрофт заявил, что отныне основным приоритетом федералов является ликвидация компьютерной преступности. ■

КИБЕРСЕКРЕТАРША

HITECH

На ресепшене Королевского колледжа в Англии появилась киберсекретарша. Говорящую роботизированную голову официально приняли на работу. Движениями Inkha управляет ноутбук. Роботесса видит, слышит и разговаривает без умолку. Среди разнообразных способов выражения эмоций ей доступны мимика губ и глаз, вращение головы и наклон шеи. В задачи Inkha входит помощь посетителям в поиске нужной аудитории и информирование о культурно-массовых мероприятиях. Заинтересовавшись в собеседнике, роботесса доверительно наклоняется вперед. Резкие движения пугают ее, и тогда она откидывает голову. Киберсекретарша критически оценивает внешний вид посетителей и отпугивает в их адрес безобидные колкости. Она разговаривает о погоде вслух, а устав, просит принести чашечку кофе. На комплектующие для создания Inkha было потрачено всего 1500 долларов. ■



НОУТБУК НА РУЛЕ

HITECH



Американская компания Arkon (www.arkon.com) представила любопытный механизм для крепления ноутбука на руль автомобиля. Маленький компьютер надежно заходит в пазы и вращается при поворотах штурвала. В сложенном виде гаджет полностью упирается под кресло. Среди потенциальных пользователей - агенты по продаже недвижимости, разъезжие торговцы и студенты. Разработчики предупреждают от использования устройства во время движения. Новинка продается в интернете по цене 50 долларов. ■

Просматривайте цифровые фотографии, видео и проигрывайте музыку с вашего ПК на телевизоре или стереосистеме.



Компьютер Extreme Fx 3000

- компьютер, способный превратить ваш дом в центр цифрового мира!

Используя компьютер Extreme Fx3000 на базе процессора Intel® Pentium® 4 с технологией HT, Вы можете слушать музыку на стереосистеме или смотреть фильмы и фотографии на телевизоре с установленным цифровым мультимедийным адаптером без какой-либо сложной перезаписи.

Не давайте стенам, проводам, маленьким динамикам или маленькому монитору ограничивать пространство для развлечений. С компьютером Extreme Fx3000 на базе процессора Intel® Pentium® 4 с технологией HT, Вы можете загрузить в ваш компьютер музыку и памятные фотографии и видеозаписи в цифровом виде, а затем смотреть их по телевизору или слушать через стереосистему, даже если ваш ПК находится в другой комнате.

Сеть компьютерных центров «Техмаркет-Компьютерс»

- г. Москва, м. Красносельская, ул. Русаковская, 2/1 (095) 264-1090
- г. Москва, м. Динамо, ул. 8 Марта, 10, стр. 1 (095) 363-9333
- г. Москва, м. Братиславская, ул. Братиславская, 16, стр. 1 (095) 347-9638
- г. Москва, м. Дмитровская, ул. Башиловская, 29/27 (095) 257-8268
- Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1 (095) 363-9399

Сеть компьютерных центров POLARIS

- г. Москва, м. Сокол, Волоколамское шоссе, 2 (095) 151-5503
- г. Москва, м. Шаболовская, ул. Шаболовка, 20 (095) 237-8240
- г. Москва, м. Красносельская, ул. Краснопрудная, 22/24 (095) 262-8039
- г. Москва, м. Комсомольская, ул-г «Московский», 4 эт., пав. 27 (095) 916-5627
- г. Москва, м. Профсоюзная, Нахимовский пр-т, 40 (095) 129-1119
- г. Москва, м. Площадь Ильича, ул. С.Радоужского, 29/31 (095) 278-5470
- г. Москва, м. Савеловская, ВКЦ «Савеловский», пав.: D24 (095) 784-6385
- г. Москва, м. Щукинская, ул. Новошукунинская, 7 (095) 935-8727
- г. Москва, м. Пражская, ТЦ «Электронный рай», пав.: 15-47 (095) 389-4622
- г. Москва, м. Люблино, ТК «Москва», 2 этаж, 1 линия (095) 359-8915
- г. Москва, м. Савеловская, Суэцкий вал, 3/5 (095) 973-1133
- г. Москва, м. Багратионовская, ТВК «Горбушкин Двор», пав.: E2-14/15 (095) 730-1549
- г. Москва, ТК «МОЛЛ-systems», МКАД 50-й км, 1 этаж **НОВЫЙ** (095) 710-8030
- г. Москва, ул. Малая Дмитровка, 1/7 **НОВЫЙ** (095) 200-3060
- г. Санкт-Петербург, м. Пр.Просвещения, ТК «Норд», пав.204 **НОВЫЙ** (812) 331-6244
- г. Санкт-Петербург, м. Академическая, ТК «Грэйт», пав. 28 (812) 590-8480
- г. Ростов-на-Дону, пр-т Буденновский, 11/54 (8632) 62-3978
- г. Ростов-на-Дону, пр-т Буденновский, 80 (8632) 92-4242
- г. Ростов-на-Дону, пр-т Нагибина, 34/1, ТЦ «Поиск» **НОВЫЙ** (8632) 72-5472
- г. Н.Новгород, ул. Пискарева, 30 (8312) 78-0861
- г. Н.Новгород, м. Канавинская, ТЦ «Новая Эра», 1 этаж (8312) 16-9787
- г. Н.Новгород, Бульвар Мира, 5 (8312) 77-5055
- г. Н.Новгород, ТЦ «Новая Эра», «Цифровая студия POLARIS» (8312) 16-9788
- г. Воронеж, ул. Кольцовская, 82 (0732) 72-7391
- г. Воронеж, пр-т Революции, 44 (0732) 20-5055
- Магазины с бесплатной доставкой по Москве shop.nt.ru (095) 970-1939

Информация о новых магазинах на www.polaris.ru, www.techmarket.ru
Магазины работают ежедневно без выходных и перерыва



- товар в кредит
- единая дисконтная система

интернет-магазин:
www.5000.ru
доставка домой или в офис

единая справочная служба
363-9333



ТЕХМАРКЕТ
КОМПЬЮТЕРС

ATI VS. NVIDIA



БЛАГОДАРНОСТУ

test_lab благодарит компанию «Остров Формоза» (www.island-formoza.ru, т.728-40-04) за предоставленное оборудование

производительность системы. Например, для Wolfenstein 3D еще хватало 286, но для Doom уже нужен был минимум 386, а лучше 486, да и памяти побольше. В то время и случилась очередная революция. Нетрудно догадаться, кто стал ее двигателем. Да-да, в очередной раз отличилась id Software, создав умопомрачительный и потрясающий Quake, который все очень ждали. Вот это-то как раз и была настоящая трехмерная игра. Наконец-то свершилось!

Но новая революция оказалась с двойным дном. Как обычно, потребовался переход на процессор нового поколения и увеличение объема оперативной памяти. Однако новое качество программного обеспечения (то есть игры) породило новое качество аппаратной части - никому не известная фирма 3dfx, занимавшаяся разработкой видеочипов для игровых автоматов, выпустила специализированный ускоритель трехмерной графики для PC - Voodoo Graphics.

С тех пор утекло много воды - 3dfx стал королем трехмерной графики, победив в борьбе с nVidia, но затем все же разорился. На сегодняшний день идет борьба между все той же nVidia и ATI.

ТЕХНОЛОГИЯ

В этом разделе мы решили изложить в доступной форме основы технологии трехмерной графики. Если ты не знаешь, чем билинейная фильтрация отличается от трилинейной, или чем пиксельный шейдер отличается от вершинного (и что это вообще такое), то этот раздел стоит прочитать. Это надо сделать, чтобы стало понятно, вокруг чего кипят такие страсти.

ГЕОМЕТРИЧЕСКАЯ МОДЕЛЬ

Как и бывает в большинстве программных систем, за видимым на экране монитора результатом стоит некая математическая модель, зачастую весьма сложная. В случае трехмерной графики основой является геометрическая модель, в которой предметы виртуального мира представлены множеством точек в трехмерной системе координат. Если соединить эти точки линиями, то получится каркасная модель, очень похожая на фигуры, сделанные из кусочков проволоки. То есть такая модель, в которой видны только ребра поверхностей трехмерных объектов. Таким образом, имеем два вида прос-

test_lab (test_lab@gameland.ru)

Вокруг приложений трехмерной графики как самых зрелищных и эффектных, вероятно, никогда не утихнет шума, они и дальше будут вызывать повышенный интерес пользователей персональных компьютеров. И потому, разумеется, будет необходима соответствующая поддержка на аппаратном уровне, а значит, неизбежно встанет вопрос выбора конкретного устройства. В этом обзоре мы рассмотрим high-end и middle-end видеокарты производства фирмы ASUS на чипсетах двух основных на сегодняшний день конкурентов - ATI и nVidia.

ТРЕХМЕРНЫЕ РЕВОЛЮЦИИ

Для нас уже стала привычной бешеная "гонка вооружений" на рынке ускорителей трехмерной графики, которой не видно конца и края. Виднеется только призрачный передний край технологии, проступающий сквозь пыльную дымку маркетинговых усилий лидеров рынка. Что же положило начало этому вечному движению? Игры, компьютерные игры.

Из воспоминаний древности, пожалуй, приходят на ум игры с алфавитно-цифровой визуальной частью - охота на вампиров, скачки. Нет, нет. Тут даже и графики-то как таковой нет. Дальше - больше. Диггер, умопомрачительная серия Арканов, Принц Персии. Уже стало попахивать индустрией развлечений, появились первые серии игр небезызвестной в наши дни id Software - Commander Keen, Dangerous Dave. Но все это было плоско, плоско и

еще раз плоско! Игрой, изменившей эту ситуацию, стала Wolfenstein 3D - детище все той же id Software. Гордая приставка 3D была по нынешним меркам смешной - ну где же тут 3D? Пол, потолок на одной высоте да прямые стены все были покрыты текстурами низкого разрешения, фигуры персонажей выполнены с помощью спрайтов. Но по тогдашним меркам это выглядело весьма захватывающе и эффектно. Тут, справедливости ради, надо упомянуть еще одну малоизвестную игру тех далеких лет - Stellar 7. Формально она имела даже больше прав называться 3D (хотя почему-то ими не пользовалась), поскольку все объекты там были действительно трехмерными, но предельно простыми. Разумеется, не было никакого затенения, не говоря уже о текстурах. Но, как оказалось, игроков того времени больше привлекали красочные спрайты и текстуры, плюс интересный сюжет и

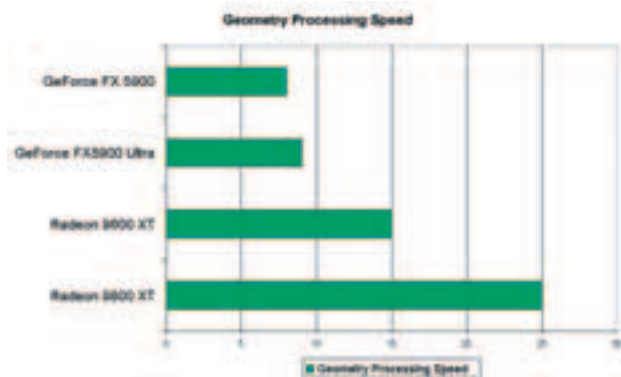
СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ

ASUS A9800 XT/TVD
ASUS A9600 XT/TVD
ASUS V9950 Ultra
ASUS V9950 SE

хорошая играбельность Wolfenstein 3D, чем формальная трехмерность в виде нелепых одноцветных примитивов. С этого момента принято отсчитывать историю 3D-игр. Затем последовал взрыв неимоверной силы - это id Software (снова!) выпустила бессмертный шедевр - Doom, который жив и по сей день - нашлись продолжатели этого проекта, развивающие код, ставший в один прекрасный день открытым. Разрешение текстур выросло, как и их количество, комнаты стали сложнее по форме, но как таковой трехмерности все еще было.

Зато этой серии опытов по созданию 3D-игр стало достаточно, чтобы понять, что необходимо наращивать

При создании изображения стены дома совершенно необязательно заботиться о каждом кирпичике.



тейших объектов (примитивов) - линии и точки.

Обычно для представления сложных поверхностей используется множество треугольных поверхностей - полигонов (это третий вид примитивов). Чем их больше, тем более гладкой получается форма модели. Впоследствии полигоны могут быть заполнены цветом (затенены) в зависимости от освещенности, цвета каждой из трех вершин и некоторой другой информации (все в совокупности называется атрибутами вершин). Далее же на поверхности полигонов могут быть наложены текстуры. На этом стоит остановиться подробнее.

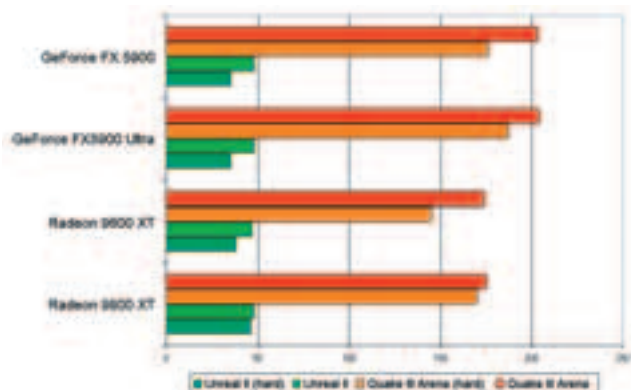
ТЕХНИКА НАЛОЖЕНИЯ ТЕКСТУР

Наложение текстур (texture mapping) - одна из важнейших частей в процессе формирования трехмерного изображения на экране компьютера. Текстура представляет собой обычное двумерное растровое изображение определенного формата, которое хранится в памяти и предназначено для наложения (проецирования) на поверхности трехмерных объектов. Это изображение может представлять собой что угодно, например фотографический образ, и это очень полезное свойство, которое широко применяется на практике. Текстуры хранятся в памяти видеокарты, а также в оператив-

ной памяти системы, если применяется технология AGP (Accelerated Graphics Port), и занимают довольно большой ее объем.

Наложение текстур дает возможность построить более правдоподобную модель реального мира и при этом сэкономить вычислительные ресурсы системы. Например, при создании изображения стены дома совершенно необязательно заботиться о каждом кирпичике в ней, представляя его как самостоятельный геометрический объект. Достаточно создать плоскую поверхность и наложить на нее текстуру, изображающую кирпичную кладку. Таким образом значительно упрощается геометрия трехмерной модели, а значит, и сокращается количество вычислительных ресурсов машины, необходимое для ее обработки.

Кроме того, стоит упомянуть так называемые программные техники текстурирования, при использовании которых изображение текстуры генерируется на лету с помощью специальных алгоритмов, и может даже видоизменяться, имитируя, например, языки пламени. Но в отличие от традиционных, этот вид текстур требует относительно высоких вычислительных затрат, связанных непосредственно с их формированием, и используется не очень широко.



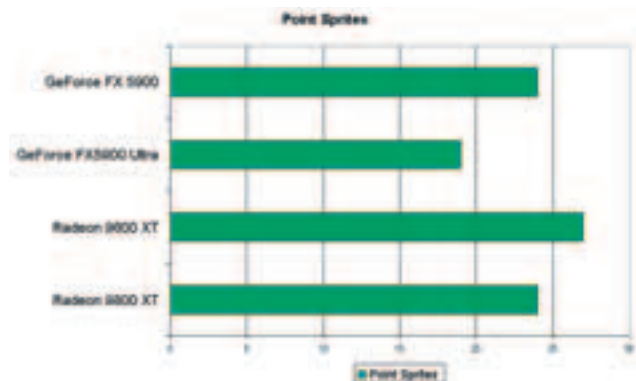
Как же происходит наложение текстур? Разумеется, читатель знает, что изображение на экране монитора представляется набором пикселей. С другой стороны, текстуры также состоят из пикселей, которые обозначают специальным термином - текстель (texel). Это вносит определенность, и становится ясно, идет ли речь о пикселе экрана или же о пикселе текстуры.

Исходя из этого, можно сказать, что при наложении текстуры происходит сопоставление одного или, чаще всего, нескольких текстелей в пиксель (то есть текстели меньше пикселей), и тот начинает мерцать при анимации. При использовании этого метода цвет каждого пикселя выбирается на основе цвета четырех смежных текстелей.

чтобы избавиться от определенных дефектов визуализации (артефактов визуализации).

БИЛИНЕЙНАЯ ФИЛЬТРАЦИЯ

Первый - это метод билинейной фильтрации (bilinear filtering), который призван избавиться от эффекта альясинга (aliasing). Этот эффект возникает, когда при достаточном удалении много текстелей накладывается на место, занимаемое одним пикселем (то есть текстели меньше пикселей), и тот начинает мерцать при анимации. При использовании этого метода цвет каждого пикселя выбирается на основе цвета четырех смежных текстелей.



Этой серии опытов по созданию 3D-игр стало достаточно, чтобы понять, что необходимо наращивать производительность системы.

они обеспечивают, и тем больше вычислительных ресурсов требуют.

Чтобы представить это более наглядно, достаточно вообразить себе некую гипотетическую плоскую поверхность, на которую наложена какая-то текстура. Допустим, что поверхность эта как бы прислонена к экрану изнутри, то есть каждый текстель однозначно отображается в пиксель такого же цвета. Фактически это равносильно тому, что мы просто вывели на экран плоское изображение текстуры. Но что же будет, если эта поверхность начнет "заваливаться" назад, как если бы кто-то поставил на стол толстую книгу обложкой к себе и подтолкнул ее? Очевидно, что теперь идеальность нашего отображения разрушится. Верхняя часть поверхности начнет быстро удаляться от зрителя, и придется выбирать цвет каждого пикселя на экране при рисовке каждого кадра. Тут все зависит от применяемого метода (техники) наложения текстуры.

Давай разберемся в наиболее распространенных из применяемых сегодня методов наложения. Каждый из них разрабатывался,

МИПМЕПИНГ

Описанный выше метод не избавляет от искажений, связанных с ошибками определения глубины сцены. Для решения этой проблемы был разработан метод мипмеппинга (mip-mapping). Суть его состоит в том, что для более или менее удаленных объектов используются текстуры с разным уровнем детализации (уровни мипмеппинга). То есть для каждой текстуры создаются ее уменьшенные копии и накладываются на более удаленные полигоны. Однако это создает новую проблему - часто могут быть различимы границы перехода от текстуры с одним уровнем деталей к другой, что создает эффект полосатости.

ТРИЛИНЕЙНАЯ ФИЛЬТРАЦИЯ

Метод трилинейной фильтрации (trilinear filtering) является комбинацией двух предыдущих. При определении цвета пикселя берутся цвета восьми текстелей - по четыре смежных текстеля из соседних уровней мипмеппинга. Может показаться, что ничего лучше трилинейной фильтрации не существует, однако это не так. Одним недостатком билинейной и



трилинейного методов фильтрации является изотропность, то есть неизменность формы области текселей, которая используется для определения цвета пикселя. По этой причине данные методы хорошо работают для полигонов, расположенных параллельно экрану, однако такая ситуация нетипична и возникает крайне редко. В результате текстура получается более размытой, чем надо.

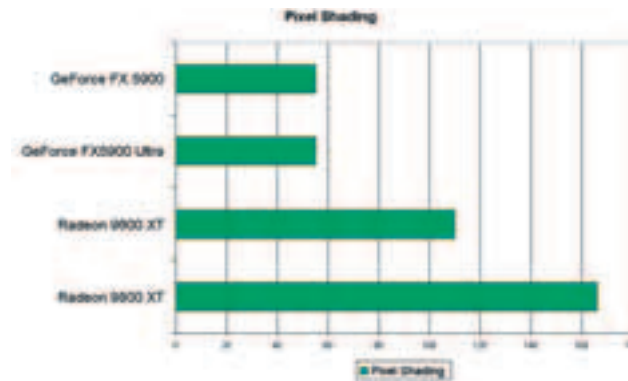
АНИЗОТРОПНАЯ ФИЛЬТРАЦИЯ

Анизотропная фильтрация (anisotropic filtering) учитывает положение полигона относительно точки наблюдения. Это можно сравнить с изменением формы светового пятна, отбрасываемого на ровную поверхность карманным фонариком - если светить прямо перпендикулярно, то пятно света круглое, если же под углом - эллиптическое. В других упомянутых способах фильтрации использовались области из четырех текселей, что можно считать донельзя упрощенным вариантом круга, тогда как при анизотропной фильтрации применяются приближения формы эллипса для различных углов зрения. Таким образом, форма области текселей, определяющая цвет пикселя, не является постоянной (анизотропна) и зависит от угла зрения.

Теперь, поняв основные способы наложения текстур, можно проанализировать их влияние на производительность. Как мы уже упоминали, текстуры могут храниться в памяти видеоприбора или в оперативной памяти компьютера. Последний вариант стал возможен благодаря технологии AGP, которая позволяет видеокarte обращаться к оперативной памяти напрямую, а не через шину PCI, как это было раньше. Стало быть, нет необходимости устанавливать большие объемы дорогостоящей видеопамати, устройство больше не зажато в рамки пропускной способности шины PCI, а пропускная способность является одним из ключевых моментов при наложении текстур. Почему? Чтобы понять это, достаточно представить себе, сколько текселей придется считать из памяти для того, чтобы получить изображение одного пикселя. В случае билинейной фильтрации, к примеру, нужно выбрать из памяти 4 текселя

для определения цвета каждого пикселя, а всего таких пикселей у нас, скажем, 1024x768, то есть 786432. Да при том каждую секунду таких кадров надо сформировать в среднем 40. А при трилинейной фильтрации надо считать из памяти в два раза больше текселей. Что и говорит про анизотропную фильтрацию, при которой прежде чем считать некоторое количество текселей, нужно еще

Затем последовал взрыв неимоверной силы - это id Software выпустила бессмертный шедевр - Doom.



затратить ресурсы, чтобы определить, какие именно.

Увы, как обычно, за все приходится платить - избавляясь от дефектов визуализации, мы расплачиваемся производительностью. И чем совершенней метод, тем больше он требует возможностей железа. Таким образом, можно расположить методы фильтрации текстур и их различные комбинации в соответствии с проявляемыми аппетитами в отношении ресурсов: билинейная, билинейная с мипмеппингом, трилинейная, анизотропная, анизотропная с мипмеппингом, анизотропная с трилинейной.

▲ ШЕЙДЕРЫ

Говоря о современных технологиях в области трехмерной графики, невозможно обойти стороной шейдеры. Что же такое шейдер? Необходимо иметь некоторое представление о

трехмерном графическом конвейере (3D pipeline), чтобы понять это. Конвейер в данном случае - это определенный набор этапов, на которых последовательно обрабатываются исходные данные для получения изображения трехмерной сцены на экране. Основными этапами конвейера являются: трансформация, обработка вершин, обработка пикселей.

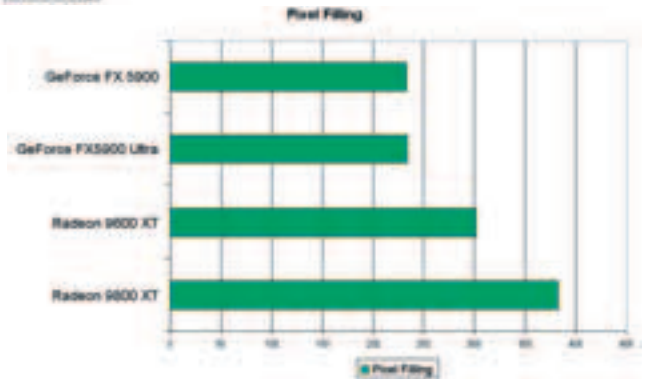
Трансформация необходима постольку, поскольку, кроме видимых объектов, заданных в системе координат, существует такой "виртуальный" объект, как видимый объем - некая область в форме параллелепипеда, заданная в тех же координатах, что и все остальное в сцене. Все выходящее за пределы видимого объема отсекается. Кроме того, есть еще и порт просмотра (viewport) - окно (оно может занимать и весь экран), в котором все, в конце концов, отобразится. Таким образом, исходная сцена сначала проходит ряд преобразований (трансформаций).

полигонов, уменьшая их размер, что привело бы к неоправданно высокой сложности модели с точки зрения геометрии. Потому полигон получает неравномерную закраску, определяемую по некоторому алгоритму, исходя из атрибутов его вершин, и модель выглядит более гладкой.

До появления аппаратной поддержки вершинных шейдеров разработчик, использующий конкретный интерфейс программирования приложения (API - Application Programming Interface), например Direct3D или OpenGL, не имел возможности контролировать, изменять или выбирать алгоритм затенения, применяемый в API. Вершинный шейдер - это программа, преобразующая атрибуты вершин, код которой исполняется графическим процессором. С ее помощью может быть рассчитано затенение полигона не по фиксированному алгоритму, а по написанному разработчиком.

На дальнейшем этапе происходит наложение текстур, как описывалось выше, их комбинация с уже

КОНФИГУРАЦИЯ ТЕСТОВОГО СТЕНДА	
Процессор:	Intel Celeron 2,00 ГГц
Память:	два модуля по 256 Мб Samsung PC3200 DDR (Dual Channel)
Материнская плата:	ASUS P4P800
Версия BIOS:	1009.008 American Megatrends Inc.
Операционная система:	Windows XP Professional (5.1.2600) Service Pack 1
Версия DirectX:	DirectX 9.0a
Драйверы ATI:	6.14.10.6396
Драйверы nVidia:	6.14.10.5216
Приложения:	3DMark03 (patch 320), Unreal II: The Awakening, Quake III Arena 1.32, D3DRightMark 1.2.0.7 Public Beta 1. Для всех приложений, кроме последнего, использовались два режима тестирования - тяжелый (обозначен в таблице результатов как hard), в котором драйвер настроен на антиалиасинг 4X и анизотропию 8X, а также режим установок антиалиасинга и анизотропии по умолчанию. В обоих случаях вертикальная синхронизация была выключена, разрешение экрана 1204x768. Тестирование в D3DRightMark проводилось только в тяжелом режиме. Прочие тесты прогонялись с помощью утилиты Bench'EmAll! 2.51.



Затем, как уже упоминалось, на основе имеющихся атрибутов вершин происходит затенение полигонов, то есть расчет освещенности. Если бы этого не происходило, то каждый треугольник имел бы строго определенный цвет, и трехмерная модель получалась как бы граненой. Естественно, для придания ей более совершенного вида пришлось бы наращивать количество

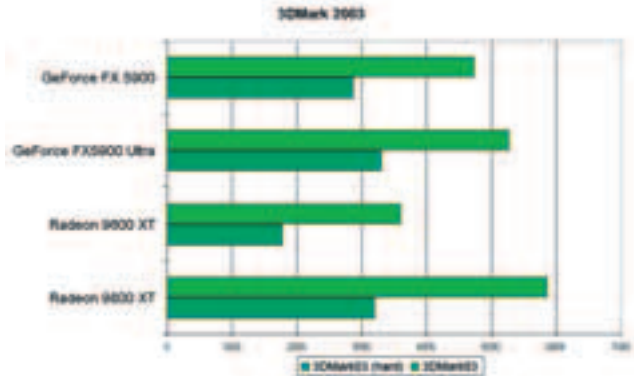
просчитанным затенением и запись результата в буфер для последующего отображения. Однако если имеется соответствующая поддержка, то результаты расчета затенения могут быть переданы так называемому пиксельному шейдеру - программе, которая рассчитывает цвет пикселя, заменяя уже рассмотренные методы наложения текстур. Это

позволяет достигать потрясающих визуальных эффектов, для чего, собственно, все и затевается.

Таким образом, совокупность вершинных и пиксельных шейдеров, по сути, является гораздо более совершенной и гибкой альтернативой имеющимся традиционным алгоритмам затенения и наложения текстур. Но и, конечно же, требующей аппаратной и программной поддержки, а также не дешевой в плане потребляемых вычислительных ресурсов.

АНТИАЛЬЯСИНГ

Изображения, получаемые с помощью компьютера, имеют дефекты в виде "рваных" краев. Это сильно режет глаз, привыкший к плавным линиям. Для ликвидации такого дефекта на последней стадии обработки изображения применяется так называемый антиалясинг. Суть его заключается в создании плавного перехода цвета от края объекта к фону.



ASUS V9950 ULTRA

Устройство получило такую низкую оценку, поскольку, честно говоря, не оправдало возлагаемых на него надежд. Являясь старшей моделью среди карт GeForce FX, оно могло бы продемонстрировать и более высокую производительность, и лучшее качество. Впрочем, акселераторы nVidia хоть и в два раза проигрывают АТI в области пиксельных шейдеров, но имеют преимущество в трилинейной и анизотропной фильтрации - это подтверждается результатом теста в Quake III. А вот что касается антиалясинга, то тут соперник Radeon 9800 XT одержал

победу - это видно по результатам тяжелого теста в Unreal II.

Комплект поставки обеих карт nVidia отличается упрощенным вариантом утилиты ASUS SmartDoctor2.

\$470



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Графическое ядро: nVidia GeForce FX 5900 Ultra
Видеопамять: 256 Мб DDR
Рабочая частота ядра: 450 МГц
Рабочая частота памяти: 850 МГц
RAMDAC: 400 МГц
Тип шины: AGP 8X/4X/2X
Максимальное разрешение: 2048x1536
VGA-выход: стандартный 15-штырьковый D-sub
TV-выход: S-VHS
Видеовыход: S-VHS
DVI-выход: DVI-I

ASUS V9950 SE

Этот ускоритель выбран в качестве лучшей покупки, потому что по результатам большинства тестов мало отстает от своего старшего брата с суффиксом Ultra, однако стоит почти в полтора раза дешевле. Ну что поделаться - устройства класса high-end всегда отличались завышенной ценой, которая плохо снижается.

Что касается производительности, то характер ее изменения в зависимости от теста также почти полностью повторяет GeForce FX 5900 Ultra, но в слегка уменьшенном масштабе. Стоит заметить, что последний даже был превзойден в тесте D3DRightMark Point Sprite.

\$320



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Графическое ядро: nVidia GeForce FX 5900
Видеопамять: 128 Мб DDR
Рабочая частота ядра: 400 МГц
Рабочая частота памяти: 350 МГц
RAMDAC: 400 МГц
Тип шины: AGP 8X/4X/2X
Максимальное разрешение: 2048x1536
VGA-выход: стандартный 15-штырьковый D-sub
TV-выход: S-VHS
Видеовыход: S-VHS
DVI-выход: DVI-I

ASUS A9800 XT/TVD

Это передовик всей линейки карт ATI, выпускаемой тайваньским электронным королем (именно так в шутку многие трактуют суффикс TeK в названии компании ASUSTeK). Исполнение заслуживает высшей оценки - красивый текстолит доселе невиданного оранжевого цвета отлично сочетается с медными радиаторами системы охлаждения. В последней, кроме

упомянутых радиаторов, используются два вентилятора (а не один огромный, как в эталонном исполнении ATI) и пластина на обратной стороне платы. Карта более компактна, чем ее прямой конкурент GeForce FX 5900 Ultra, и это притом, что инженеры все же нашли возможность удобно расположить разъем питания.

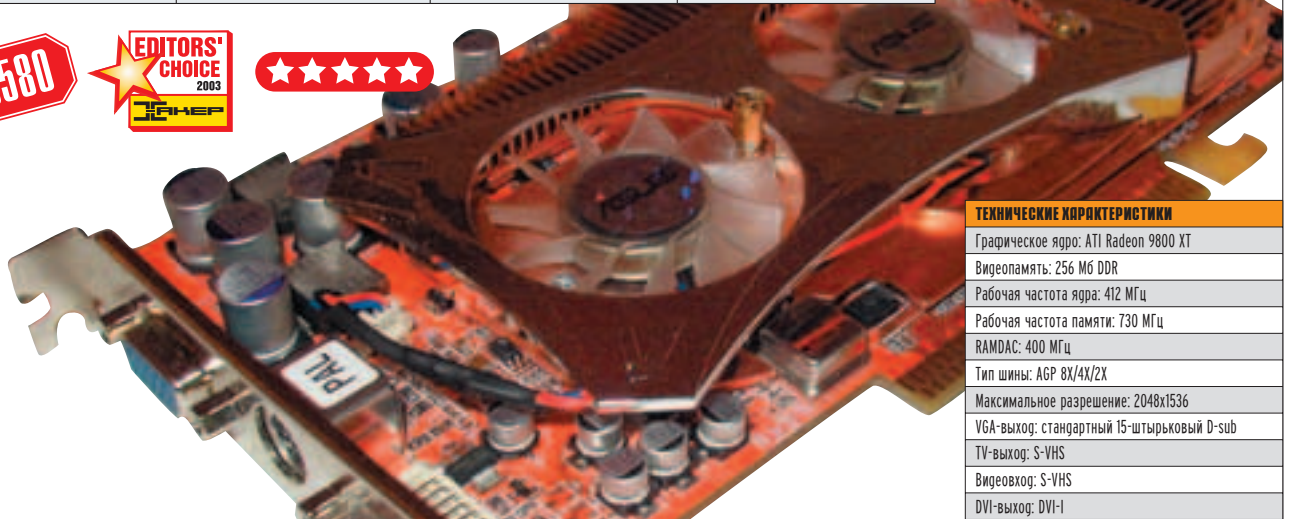
В комплекте поставки имеется среди прочего

софта чрезвычайно полезная фирменная утилита ASUS SmartDoctor2. Это приложение позволяет разгонять устройство, повышая частоты работы памяти и ядра, и ничего не спалит при этом. SmartDoctor2 автоматически следит за состоянием здоровья карты.

Устройство получило лучшую оценку за высокие показатели большинства тестов и очень хо-

рошее качество антиалиасинга, чего нельзя сказать о GeForce FX 5900 Ultra. Сравнение производилось на кадре 307 из третьего игрового теста 3DMark03 при включенной опции post processing и антиалиасинге 4x (см. скриншоты). Кстати говоря, оказалось, что ускорители ATI имеют выдающуюся производительность при работе с пиксельными шейдерами.

\$580



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Графическое ядро: ATI Radeon 9800 XT
Видеопамять: 256 Мб DDR
Рабочая частота ядра: 412 МГц
Рабочая частота памяти: 730 МГц
RAMDAC: 400 МГц
Тип шины: AGP 8X/4X/2X
Максимальное разрешение: 2048x1536
VGA-выход: стандартный 15-штырьковый D-sub
TV-выход: S-VHS
Видеовход: S-VHS
DVI-выход: DVI-I

ASUS A9600 XT/TVD

Карта является старшим представителем серии Radeon 9600 - об этом нам говорит суффикс XT в названии. Тут ее превосходит конкурент GeForce FX 5900, который все же входит в одну серию со своим старшим братом GeForce FX 5900 Ultra. Поэтому Radeon 9600 XT имел заведомо более слабые позиции в сравнении. Однако даже в такой ситуации устройство сумело достойно проявить себя. Все такая же характерная высокая производительность в работе с пиксельными шейдерами (в

D3DRightMark их использовали тесты Geometry Processing Speed, Pixel Filling и собственно Pixel Shading) и отличные результаты теста в Unreal II.

В комплект поставки также входит утилита ASUS SmartDoctor2.

\$270



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Графическое ядро: ATI Radeon 9600 XT
Видеопамять: 128 Мб DDR
Рабочая частота ядра: 500 МГц
Рабочая частота памяти: 600 МГц
RAMDAC: 400 МГц
Тип шины: AGP 8X/4X/2X
Максимальное разрешение: 2048x1536
VGA-выход: стандартный 15-штырьковый D-sub
TV-выход: S-VHS
Видеовход: S-VHS
DVI-выход: DVI-I

ВЫВОДЫ

Лидером тестирования оказался Radeon 9800 XT, однако из-за высокой цены лучшей покупкой его не назовешь. С этой точки зрения лучше GeForce FX

5900, поскольку он мало в чем отстает от GeForce FX 5900 Ultra, но почти в полтора раза дешевле. Radeon 9600 XT можно рекомендовать поклонникам ATI как хорошую и не очень дорогую карту классом ниже.

ВАРЕВОНЕ АБИТ AB-2003 DIGIDICE

■ test_lab (test_lab@gameland.ru)

Несмотря на высокий уровень компактности современных компьютеров, проблема нехватки места на рабочем столе остается в силе. В большой степени ее позволяют решить ноутбуки, но они все же остаются дорогими устройствами. Одним из наиболее экономичных выходов из такой ситуации является приобретение системного блока форм-фактора barebone. В таком корпусе плотность расположения компонентов очень высока, что позволяет разместить в нем не только основные модули, но и некоторые дополнительные устройства. Мы рассмотрим barebone Abit AB-2003.

В первую очередь barebone AB-2003 оказался не только компактным компьютерным корпусом, но и очень функциональным устройством, содержащим массу дополнительных возможностей. В комплект входит материнская плата со встроенной аудио- и видеокартой, но при этом предусмотрены AGP и PCI слоты, что позволяет подключать другие платы, например TV-тюнер. В корпус можно поставить два жестких диска (они могут быть как IDE, так и SATA) и два CD-ROM (RW, DVD). Все шлейфы также в комплекте. На каждом из кабелей питания написано, к какому из устройств его надо подключать. Это существенно экономит время при сборке. Под отверстиями для потков CD-приводов расположено устройство для чтения шести видов карт памяти. Также на передней панели есть входы USB, Fire Wire, микрофонный, выход для наушников.

Слева на передней панели расположен ЖК-дисплей. На нем может отображаться информация о значении различных параметров устройства. Рассмотрим их по порядку. В первую очередь надо сказать, что для активации всех возможностей дисплея необходимо установить соответствующее программное обеспечение, входящее в комплект поставки. На экране отображается частота и температура процессора, скорость вращения вентиляторов, предупреждение о переполнении жесткого диска или перегреве процессора, уровень громкости звука, время работы компьютера и т.д. Одной из интересных функций является возможность разгона системной шины. Существует 5 фиксированных настроек, соответствующих увеличению частоты FSB от 3 до 15%. Регулировка осуществляется с помощью универсальной ручки управления, расположенной под жидкокристаллическим дисплеем. Это позволяет осуществлять разгон, не изменяя настройки BIOS, и при этом легко контролировать состояние системы. Для более продвинутого оверклокинга предусмотрено специальное программное обеспечение, с помощью которого можно менять множество параметров системы в широком диапазоне значений.

Многими функциями barebone AB-2003 можно управлять с помощью весьма функционального пульта ДУ. Для этого надо установить программы WinDVD и WinRip. Первая позволяет просматривать DVD-фильмы. При этом дистанционно возможно не только регулировать звук или проматывать изображение, но и менять язык титров, размер видимой

области, управлять плейлистом. С помощью WinRip можно слушать музыку. Опять же с пульта возможно управление всеми функциями этой программы, такими как регулировка громкости, переход от одного трека к другому, быстрая перемотка, работа с плейлистом. Если у тебя установлена операционная система Windows XP, то с помощью пульта

можно управлять просмотром картинок: прокручивать вперед и назад, запускать слайд-шоу, поворачивать изображение. На передней панели Abit AB-2003 предусмотрены кнопки, включающие WinDVD, WinRip и режим просмотра картинок. Среди них есть кнопка, запускающая процесс копирования дисков. Если у тебя есть обычный и записывающий CD-приводы, то после установки программы DigiBurner (входит в комплект поставки) ты сможешь начать копирование диска на болванку одним нажатием кнопки.

ВЫВОДЫ:

Barebone Abit AB-2003 – универсальное решение для дома. В комплект поставки входят почти все устройства, необходимые для работы, а значит, докупать надо минимум оборудования. Компактные размеры позволяют разместить barebone даже на небольшом рабочем месте. Наличие пульта ДУ и, как следствие, возможность просматривать фильмы или картинки и слушать музыку без использования клавиатуры превращает Abit AB-2003 в развлекательный центр, заменяющий видеодвойку и микросистему.

СПИСОК ПАРАМЕТРОВ

Поддерживаемый процессор: Intel Pentium 4 Socket 478
Частота системной шины, МГц: 533/800
Оперативная память: 2xDDR 266/333/400 go 2 Гб
Видео: встроенная видеокарта Intel "Extreme graphics 2", 1xAGP(4x, 8x)-слот
IDE: 2x ATA100, 2x Serial ATA
LAN: 10/100 Мбит
Аудио: 5.1 каналов AC97
Разъемы на передней панели: 1x IEEE 1394, 2x USB 2.0, 1x MIC, 1x Headphones, 1x 6-in-1 card reader (SM, MMC, SD, CMS, CF, Micro drive)
Разъемы на задней панели: 2x PS/2 (keyboard, Mouse), 1x VGA, 1x Audio (speaker, line-out, line-in, mic-in, center/subwoofer, SPDIF), 2x USB 2.0, 1x RJ-45 LAN

Abit AB-2003.
Компактный и в то же время стильный корпус

Пульт ДУ. С его помощью можно управлять многими функциями barebone, не используя клавиатуры





ХАКЕР'S Choice

Год прошел. Что имеем в остатке? Не так уж мало, даже если смотреть только на IT сферу. Новых виндов, правда, не зарелизили, хотя посмотреть уже есть на что (статью про Windows Longhorn в декабрьском X читал?). Зато в плане взломов, эпидемий, и прочей секьюрити-байды год выдался урожайным. Один MS Blast чего стоит! Такая паника была только перед наступлением Y2K с его предполагаемым компьютерным апокалипсисом. Мы отбрали все то, на что стоило обратить внимание в прошедшем году. Так что если ты что-то пропустил, самое время это исправить.

ПОДВОДИМ ИТОГИ - ВСЕ ПУЧШЕЕ ЗА ГОД

ХАКЕР ГОДА: ЭДРИАН ЛЕЙМО

Э тот молодой хакер в свои 22 года успел немало начудить. Он, например, поломал такие крупные сети, как: Excite, Yahoo, Blogger, New York Times и т.д. Причем Эдриан Леймо - хакер из white-hat активистов, т.е. о своих поломках он всегда сообщал администраторам взломанного ресурса. Он также помог выявить ошибки в сетях Bank of America, CitiCorp, за что получил публичную благодарность от WorldCom. Но не все остались ему благодарны. Администрация New York Times не понравилась подобные деяния Леймо, и она привлекла ФБР к его поимке. Самого Эдриана Леймо сейчас выпустили под залог \$250 тысяч в ожидании решения суда.



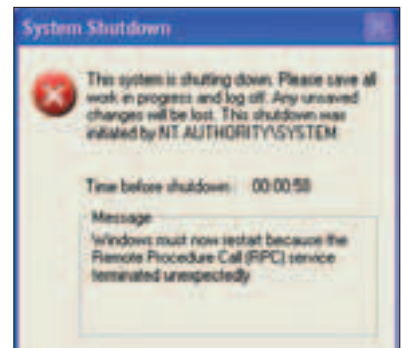
ВЗЛОМ ГОДА: ХИЩЕНИЕ СОРСОВ HALF-LIFE 2

Самый громкий взлом 2003 года – воровство исходных кодов Half-Life 2. Незвестный хакер поломал главу Valve Гейбла Нью-



элла через ошибку в Outlook. После чего взломщик слил полные сорсы всех разработок Valve, в том числе и игры Half-Life 2. Сами исходники не получили такого широкого распространения, как это могло быть, но все, кто хотел, скачали необходимое добро. В течение какого-то времени исходные коды абсолютно свободно болтались на EFnet. Это еще раз доказывает, как выгодно сидеть на всяких элитных тусовках.

ВИРУС ГОДА: ЭПИДЕМИЯ LOVESAN



MS Blast, он же LoveSan, пролетел в Сети как ураган, как стихийное бедствие. Используя ошибку DCOM RPC в MS Windows, червь заполнил собой весь интернет. Каждый хост в Сети просканировался буквально несколько раз в 5-10 минут. У автора этих строк, например, вышло так, что именно в период эпидемии он поставил себе Windows XP SP1. Не успев проработать и 10 минут, комп уходил в перезагрузку с сообщением «Необходимо перезагрузить Windows, поскольку произошла непредвиденная остановка службы Удаленный вызов процедур».

(RPC)». Правда, этого червя нельзя занести в десятку самых разрушительных – LoveSan принес ущерб только в \$525 млн., тогда как тот же Sobig оценили в \$5,59 млрд.

▲ SECURITY-САЙТ ГОДА: WWW.SECURITYLAB.RU

Не хотелось оценивать буржуйские сайты, поэтому решил остановиться на нашем родном производителе. И выбор пал на сайт www.securitylab.ru. Именно на этом сервере можно всегда обнаружить самую свежую информацию из мира net-security. Именно здесь выложен мясной выбор разнообразных утилит, начиная от iscd-утилит, заканчивая архивом эксплоитов. К тому же securitylab.ru весьма активный сайт в плане обсуждения



новостей. Особенно, если не всегда есть что сказать, а пофлеймить хочется. В общем, SecurityLab.ru – сайт 2003 года. И если ты его еще не посетил, то обязательно сделай это в 2004 году.

▲ БОЕВОЙ СОФТ ГОДА: NMAP СКАНЕР

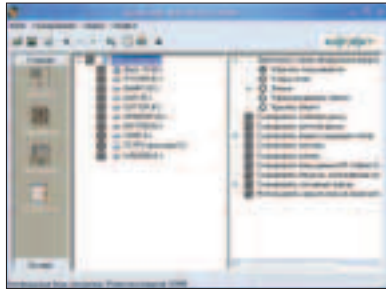
Можно долго перечислять список всякого хакерского софта. С пеной у рта доказывать, что та или иная софтина является лучшей. Но все равно все мы знаем и пользуемся одним



и тем же сканером Nmap. Да-да, именно сканер, и именно Nmap (insecure.org). Ведь кто обычно идет перед боем на разведку? Nmap. С его помощью мы узнаем список открытых портов, удаленно определяем установленную операционную систему. Причем делаем это при помощи stealth-скана. К тому же этот сканер распространяется абсолютно бесплатно, и сам проект является полностью open-source. Так что все очень умные всегда могут исправить в Nmap что-то под себя.

▲ ЗАЩИТНЫЙ СОФТ ГОДА: АНТИВИРУС КАСПЕРСКОГО

Ранее AVP, а теперь Антивирус Касперского. Это программа поселилась у каждого второго пользователя компьютера. И это радост-

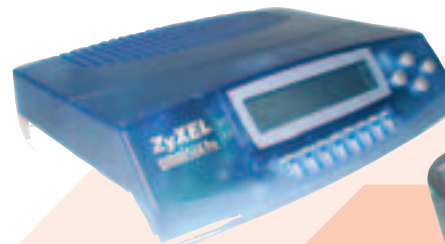


но, ведь это наш отечественный производитель, создающий действительно качественный продукт. К тому же сам проект сильно разросся. Если пару лет назад Касперский выпускал лишь один антивирус, то теперь это целый комплекс продукции: помимо отлова вирусов и червей, на твоём компьютере также может поселиться программа для выявления бурного потока спама Kaspersky Anti-Spam, плюс многополезная утилита Kaspersky Anti-Hacker, предохраняющая тебя от домогательств разного рода хакеров

▲ ЖЕЛЕЗО ГОДА

МОДЕМ ZYXEL OMNI 56K PRO (\$140) «МОДУПИРОВАВ? ДЕМОДУПИРУЙ! ПОПЕ- ВЫЕ ИСПЫТАНИЯ МОДЕМОВ», ХАКЕР #02(50) 2003

Компания Zyxel постоянно радует нас своими изделиями, вот и модем Omni 56k PRO в этом году оказался на почетном месте победителя. И этот титул девайс полностью оправдывает – за приемлемую цену можно получить устройство полупрофессионального класса, сочетающее в себе многофункциональный модем с поддержкой множества протоколов (включая самые последние версии V.42bis и V.92), а также автоответчик, способный работать при выключенном компьютере. Причем жидкокристаллический дисплей удовлетворит вкусам самого искушенного пользователя, на экранчике отображается полная информация о соединении: график АЧХ, показывающий качество линии;



протокол, по которому работает модем; реальная скорость соединения; количество повторов и ошибок. Можно сказать, что этот модем будет греть душу еще очень долго, так как максимально возможная скорость передачи данных (56к на прием) уже достигнута. Теперь играют роль протоколы сжатия и коррекции, которые можно добавить благодаря возможности обновления микропрограммы, ну и, конечно, функциональность.

ВИНЧЕСТЕР 80 ГБ MAXTOR DIAMOND MAX PLUS 9 6Y080L0 (\$70)

«362,5 КУБИЧЕСКИХ САНТИМЕТРА ПАМЯТИ», ХАКЕР #05(53) 2003

Самый распространенный на сегодня объем памяти жестких дисков составляет 80 гига-



байт, винчестеры большего размера стоят дороже, а памяти в сорок тысяч метров становится уже маловато (да и цена их не намного ниже). Поэтому для использования в обычном компьютере оптимальна именно эта цифра, а чтобы информация хранилась долго и надежно, требуется высокая износостойчивость диска. Также немаловажными параметром являются шумность и «тепловыделяемость». У Maxtor DiamondMax Plus 9 6Y080L0 все эти показатели находятся на хорошем уровне. Винчестер хоть и не самый быстрый, зато очень тихий – всего 3,5 Белл при активной работе, а гладкий график передачи данных (без «зубчиков») говорит о высокой надежности пластин. Причем по сравнению с аналогами, этот жесткий диск дает выигрыш в целых два гигабайта места (его реальная емкость составляет 76,33 Гб). Поэтому для домашнего использования DiamondMax является удачным выбором.

ЦИФРОВАЯ ФОТОКАМЕРА CANON POWERSHOT A60 (\$275)

«ЦИФРОВЫЕ ДВУХМЕГАПКСЕЛЬНЫЕ МЫЛЬНИЦЫ», ХАКЕР СПЕЦ #05(30) 2003



Цифровые фотоаппараты все увереннее входят в нашу жизнь, постепенно вытесняя своих пленочных собратьев, благо качество снимков, отпечатанных на фотобумаге, сравнимо с обычными фотками. А для неискушенного любителя остановить мгновение, различия между обычной и цифровой фотографией вообще незаметны. Полупрофессиональная по количеству всевозможных настроек

ек камера PowerShot A60 от Canon имеет огромное количество функций и позволяет снимать в нескольких режимах – автоматическом, полуавтоматическом и ручном (для самых опытных пользователей). Удобное расположение элементов питания способствует правильному распределению веса, так что исключается вероятность выронить камеру из рук, а разнообразные кнопки позволяют управлять с настройками, не прибегая к использованию меню. Наличие байонета (пластмассовой резьбы) позволяет использовать для съемки различные оптические насадки, чтобы расширить область применения аппарата. Наличие функции голосовых комментариев к фотографиям не даст забыть, что было снято. В общем, Canon PowerShot A60 – лучшая в своем роде.

17" LCD-МОНИТОР SAMSUNG SYNCMASTER 173P (\$650) «ВРЕМЯ ПОКУПАТЬ? ТЕСТ СОВРЕМЕННЫХ 17" LCD-МОНИТОРОВ», ХАКЕР СПЕЦ #12(37) 2003

До сих пор ведутся споры, что лучше - LCD или CRT, ведь у каждого типа мониторов есть свои плюсы и минусы. В прошедшем году дискуссия была особенно острой, ведь качество ЖК-панелей стремительно приближается к изображению, получаемому на лучевой трубке. Яркий показатель - новенькая семнашка от Samsung, носящая имя SyncMaster 173P. Этот представитель линейки 17-дюймовых мониторов является продолжением легендарного 171, дизайн которого был разработан в студии Porsche. Отличные характеристики цветопередачи, яркости и латентности позволяют использовать монитор в работе с текстами, при просмотре фильмов и даже в играх! А четыре степени свободы позволят настроить под себя положение экрана, причем очень удобная подставка дает возможность вращать панель на столе. Словом, инженеры из Samsung потрудились на славу, разработав прекрасный жидкокристаллический монитор для требовательных к качеству картинки, функциональности и дизайну пользователей.



МАТЕРИНСКАЯ ПЛАТА ASUS P4C800 (INTEL P4)/GIGABYTE GA-7NXP (AMD ATHLONXP) (\$80) «ПО МАТЕРИ! ГЛАВНАЯ ЖЕЛЕЗКА В ТВОЕМ КОМПЬЮТЕРЕ», ХАКЕР #07(55) 2003

Новые материнские платы стали с завидной регулярностью появляться на рынке, причем каждая новая серия обрастает дополнительными рюшечками в виде всяческих навороченных функций и экзотических железок в комплектации.

ASUS, как обычно, лидирует по качеству продукции под жилище Pentium4 - плата P4C800 является одной из последних разработок, обладающих множеством новых технологий и фирменных изысков. Чип i875P позволяет стабильно работать на частоте

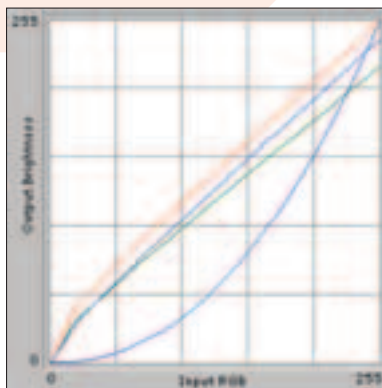
шины в 800 МГц, по скорости плата не уступает своим соперникам. А богатая комплектация не оставит равнодушными любителей высокотехнологичного свежака.

Ну а ведущим производителем MB для процессоров AMD является Gigabyte с GA-7NXP. Имея чип nForce II и обладая отличным разгонным потенциалом (от 333 МГц до 400 МГц), эта материнка будет находкой для оверклокеров. На девайсе большое количество логики для поддержки множества стандартов (от FireWire до RAID) и немало утилит, поставляемых в комплекте. А русская документация и простая удобная сборка позволяют сказать, что это одна из лучших материнок под AMD на сегодня.



17" CRT-МОНИТОР LG FLATRON F700P (\$200) «САМЫЕ ИНТЕРЕСНЫЕ СЕМНАШКИ. ТЕСТ 17" CRT-МОНИТОРОВ», ХАКЕР СПЕЦ #08(33) 2003

Если ты все же являешься поклонником мониторов CRT-типа, то, несомненно, оценишь модель Flatron F700P, предлагаемую LG. Отличное качество картинки за низкую по срав-



нению с LCD цену. Максимально возможное разрешение, на котором способна работать трубка – 1600x1200, и это при частоте в 75 герц, что является неплохим показателем. Flatron F700P обладает хорошей геометрией при плоском экране, а фокус является равномерным. Чтобы полностью насладиться изображением на экране и правильно выставить гамму и цветопередачу, придется установить специальное ПО для калибровки монитора и создания цветового профиля.

Монитор довольно компактный и имеет интересный дизайн, из разъемов присутствуют RGB-вход и USB-хаб, последний позволяет подключать мышку или клавиатуру прямо к нему, не протягивая провода к системнику.

ЛАЗЕРНЫЙ ПРИНТЕР SAMSUNG ML-1750 (\$230)

«СКАЗ ПРО ТО, КАК ПЕЧАТАТЬ НА ЛАЗЕРНИКЕ И НЕ БЫТЬ ЗАДУШЕННЫМ ЖАБОЙ», ХАКЕР #10(58) 2003

За прошедший год лазерные принтеры сильно подешевели, причем стоимость одной распечатанной страницы гораздо ниже, чем у струйников – около трех центов, причем в режиме экономии эта цифра снижается в полтора-два раза. Наличие встроенного языка PCL6 позволит печатать практически из любого приложения, причем не только виндового, но и программ из семейства *nix, поскольку для печати не нужен драйвер



именно для ML-1750, можно использовать и системный, для PCL6 устройств. Благодаря удобному лотку, расположенному внутри, девайс сэкономит драгоценное место вокруг твоего стола, а удобный индикатор наличия бумаги покажет, на сколько страниц еще можно рассчитывать. Стартовый картридж рассчитан всего на 1000 отпечатанных листов, а стандартного должно хватить аж на 3000 (при пятипроцентном заполнении), то есть в месяц эта малышка без напряга сможет напечатать около 15000 листов. Хорошее качество отпечатков, удобный дизайн, выгодная цена – этими свойствами обладает Samsung ML-1750.

КОМБОПРИВОД DVD/CD-R/RW SAMSUNG COMBO DRIVE CD-RW/DVD SM-352B (\$56)

«КОМБАЙНЫ НА РЫНКЕ. ТЕСТИРОВАНИЕ КОМБИНИРОВАННЫХ DVD/CD-R/RW-ПРИВОДОВ», ХАКЕР СПЕЦ #10(35) 2003

Появление множества новых форматов и технологий среди оптических носителей требует наличия соответствующих девайсов, способных прочесть нужный диск, и это на-

рядом с тем, что старые болванки остаются по-прежнему актуальными. Чтобы решить проблему нехватки пятидюймовых слотов, разработчики пошли по хитрому пути – сделали поддержку сразу нескольких форматов, а такие приводы получили название Combo Drive. Ярким представителем сообщества комбайнов является Samsung Combo Drive CD-RW/DVD SM-352B. Стильное внешнее устройство довольно тихое и не уподобляется пылесосу «Чайка» даже при работе на очень высоких скоростях. При чтении и записи данных на диски графики гладкие и ровные, что говорит о хорошем качестве механики привода. При чтении диска DVD проблем также не возникает. Подводя итог, можно сказать, что этот комбодрайв станет отличным приобретением.

СКАНЕР HP SCANJET 3530C (\$97) «ПРОСТЫЕ СЕРЬЕЗНЫЕ СКАНЕРЫ ДЛЯ ПРОСТЫХ СЕРЬЕЗНЫХ ПЕРЦЕВ», ХАКЕР # 1 (59) 2003

Сканер – очень полезная вещь в домашнем хозяйстве, можно и лекции перебросить



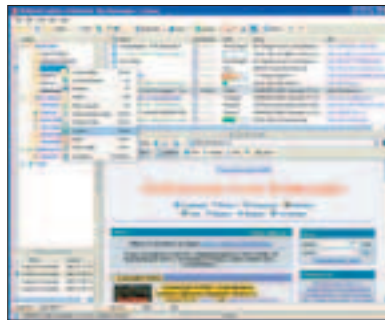
в электронный формат, и документик скопировать, и текст распознать, вместо того чтобы печатать. А благодаря внешнему слайд-адаптеру появляется возможность распечатывать фоты с негативов на принтере. Очень интересный ход применили разработчики из HP, создав драйверы в виде надстройки над Internet Explorer, это решение оказалось чрезвычайно удобным. Благодаря этому в процессе сканирования не появляется прогресс-бар, практически блокирующий остальную работу. Красивый корпус с округлыми краями сделан из пластика, а крышка свободно снимается. На переднем краю стандартные кнопки быстрого доступа. Из при-

кольных особенностей стоит отметить возможность сканирования фотографий прямо в рамке. Сканер имеет интерфейс USB 2.0 и является одним из самых быстрых.


TV TUNER PINNACLE PCTV PRO (\$70) «ОСТАНКИ В КУЗОВЕ», ХАКЕР СПЕЦ # 1 (36) 2003

Превратить твой комп в телевизор призван ТВ-тюнер. Современные же домашние модели уже позволяют создавать довольно сложные видеоклипы с разными спецэффектами. Модель Pinnacle PCTV Pro позволяет не только смотреть телепередачи на любимом месте, но еще и слушать в перерывах радио, поскольку имеет встроенный FM-тюнер. Поддерживается работа с наиболее распространенными форматами передачи цвета PAL, SECAM (наш российский) и NTSC. Из входов присутствуют видеовходы тюльпан (RCA), S-Video, для TV-антенны и дырочка для FM-антенны. Также в комплекте удобный и функциональный пульт дистанционного управления, так что не придется шаманить с клавиатурой, когда лежишь на диване. Для работы требуется минимальная конфигурация компьютера Celeron 600 МГц со 128 мегабайтами памяти. Тюнер умеет воспринимать телетекст и отлично находит все

этом нет ничего удивительного. Ведь раньше в поисках нового софта Эшу приходилось каждый день лично обследовать пару десятков сайтов. Теперь же все его источники информации контролирует Bookmark Explorer (www.bookmarkexplorer.com). Программа самостоятельно делает обход, автоматически проверяет сайты на наличие изменений, скачивает обновившиеся страницы для офлайнового просмотра, во время которого изменившиеся блоки текста заботливо подсвечиваются. Причем все это функциональное изобилие радует глаз на редкость приятной и удобной оболочкой.



ШАРОВАРНЫЙ САЙТ ГОДА: SIMTEL.NET

Отличный каталог программного обеспечения, адрес которого должен знать каждый уважающий себя юзер. Ресурс не испытывает недостатка в деньгах (за его спиной стоит компания Digital River – один из самых известных в мире регистраторов программного обеспечения), поэтому обновляется ежедневно, делает рассылку новостей, выкладывает у себя копии всех описываемых программ и заказывает обзоры софта у Майкла "Dr. File Finder" Каллахана. Но главное достоинство этого сайта, на наш взгляд, заключается в правильной организации раздела «New releases» (www.simtel.net/new_releases.php). Не так уж много в Сети серьезных софт-архивов, у которых в ленте новостей идут не только краткие описания прог, но и их скриншоты! В закладки, однозначно! 



каналы и станции, присутствующие в эфире, а при каждом запуске производит точную подстройку. Есть возможность видеозахвата при помощи специального ПО. В общем, PCTV Pro – отличная модель для дома, которая позволит расслабиться и получить удовольствие во время отдыха.

ПОПЕЗНАЯ УТИЛИТА ГОДА: BOOKMARK EXPLORER

Новая прога, заставившая нашего главного шаровароведа (консерватора по натуре :) выкинуть к чертям собачьим Check&Get – менеджер закладок, верой и правдой служивший ему более трех лет. Впрочем, в

СДЕЛАЕМ ЭТО ПО-БЫСТРОМУ

Черт возьми! Как же долго пьются эти десять avi'шников с фильмами! Уже достали! И по покалке: только начнешь чего-то скачивать, как удаленный компьютер вырубается, а когда снова появляется в сети - изволь начинать скачивание сначала. Разве это не свинство? И ведь не у меня одного такие проблемы. Не случайно же в инете стали появляться проги, обещающие радикальным образом ускорить и улучшить обычный процесс копирования! Ускорить и улучшить... Эх, согласишься, заманчиво звучит.

МОЖНО ЛИ УВЕЛИЧИТЬ СКОРОСТЬ КОПИРОВАНИЯ ФАЙЛОВ?

В ЧЕМ СИЛА, БРАТ?

Сила - в скорости. Которой нам частенько не хватает, когда нужно скачать что-нибудь большое: те же фильмы в Мpeg4, например. Вроде, и винты быстрые, и винды настроенные - а льются файлы ме-е-едленно.

Программеры говорят, что реально увеличить скорость раз в пять, и все будет просто летать. А в доказательство пишут соответствующие программки, призванные заменить стандартные копирующие функции Windows своими, более скоростными. А заодно подбросить нам, юзерам, полезных и интересных возможностей: докачки файлов в случае прерывания процесса (очень нужная фишка в локальных сетях!), затирания старого файла нулями при переносе (чтобы враги не восстановили!) и прочее, прочее...

Обещают много, но как все обстоит на практике? Давай-ка протестируем несколько наиболее распространенных утилит и посмотрим, на что они действительно способны!

BURSTCOPY V2.650

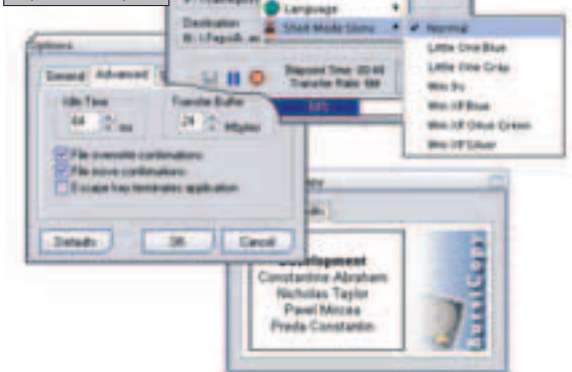
ОС	WinAll
РАЗМЕР	2144 Кб
ЛИЦЕНЗИЯ	Shareware
САЙТ	www.burstcopy.com

Программа настолько популярная на западе, что за нее даже хотят денег. И поначалу кажется, что есть за что!

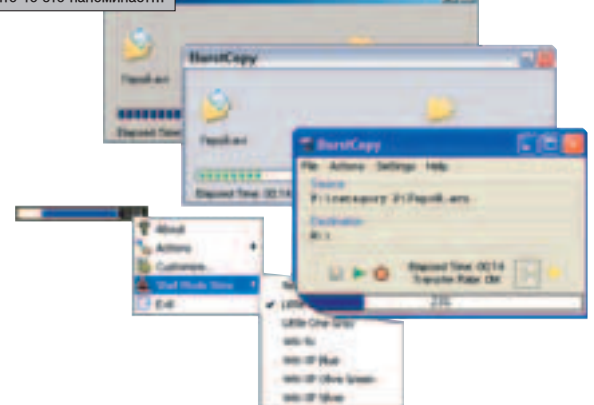
BurstCopy встраивается в Проводник, и для ее использования достаточно выбрать BurstCopy here в контекстном меню, перетащив файл в нужное место правой кнопкой мыши.

Заявляется поддержка работы из командной строки, но нигде - ни в readme, ни в помощи, ни на сайте - не описаны параметры запуска.

BurstCopy в своей первоизданной красе!



Скины из комплекта - что-то это напоминает...





СТР.34

СТАВИМ БОТА НА РАЗДАЧУ

Продолжение темы «Поимей WAREZ на IRC». Пытаемся настроить собственный файлоораздаточный irc-ресурс.



СТР.38

СЕТЕВОЙ ПАПАРАЦЦИ

Стимулируем тягу человека к прекрасному - выбираем лучший софт для грабежа картинных интернет-галерей.



СТР.30

ПОЧТОВЫЕ ПЕРЕХВАТЧИКИ

Изучаем программы для контроля переписки. По ходу дела вырабатываем методы обнаружения и борьбы с этой заразой.



Сам же процесс работы незатейлив. В окне программы (кстати, поддерживаются скины, но кроме включенных в комплект поставки никаких других на сайте нет) отображается скорость копирования, прошедшее время (или оставшееся - как настроишь в параметрах), большой прогресс-бар для всех файлов и маленький внизу для каждого в отдельности (отсутствует, если копируешь лишь один файл). Закачка приостанавливается или отменяется парой соответствующих кнопок, а "рычажком" справа регулируется приоритет работы софтины.

На этом, в общем-то, и заканчиваются все сервисные возможности BurstCopy: ни тебе докачки (предлагает заменить и не более того), ни очереди, ни хотя бы параллельной работы (пока прога не закончит одну операцию копирования, другую не начнешь - пункты контекстного меню BurstCopy here и BurstMove here просто-напросто недоступны)...

Что же касается скорости, то, начав с большим энтузиазмом на одном диске, программа катастрофически отстала на закачке по локальной сети. Впрочем, ускорить показатели софтины на добрых два десятка секунд, а то и больше, можно, увеличив ее приоритет в винде регулятором в окне или настройках. Изначально ВС настроена, чтобы не отнимать время процессора у других программ (и тогда уровень его загрузки стремится к нулю), но если тебе важнее скорость, а не возможность делать параллельно что-то еще, то смело выкручивай "рычажок", и сразу почувствуешь, как проценты побежали быстрее!

SECURECOPY V2.2.300

ОС	WinAll
РАЗМЕР	1887 Кб
ЛИЦЕНЗИЯ	Freeware
САЙТ	www.pinedanet.com

На первый взгляд - очень даже неплохая программа для копирования. Так же, как BurstCopy, встраивается в Explorer, но имеет по сравнению с ней много чисто функциональных преимуществ. Поддерживает "умную докачку" (опция Security-Use GoBack), когда файл продолжает копироваться не точно с места остановки, а чуть раньше - на случай, если последние байты испорчены. Рабочее окно - самое навороченное. Интерфейсом SecureCopy легко делает всех других участников нашего "забега". Тут тебе и скорость в мегабайтах и мегабитах (удобно для локалки), и точная индикация объемов скачанного, и подсчет времени окончания, и ограничение полосы пропускания (чтобы не грузить собой всю локальную сетку)... Но главное: удобная реализация очереди файлов. Добавляешь файлы и каталоги и спокойно идешь пить чай или что покрепче: пусть себе льются!

Казалось бы - есть все что нужно и даже больше, но функциональные возможности SecureCopy перечеркиваются одним фактом: ужасной производительностью. Посмотри на таблицу - она не только медленнее других программ, но и отстает от стандартного Explorer'a! Тут

даже комментировать нечего. Возможно, подобные результаты справедливы лишь для моей машины, а у тебя все будет копироваться со скоростью света, но я в этом сильно сомневаюсь. Visual Basic, на котором написана SecureCopy, однозначно не подходит для серьезных системных программ...

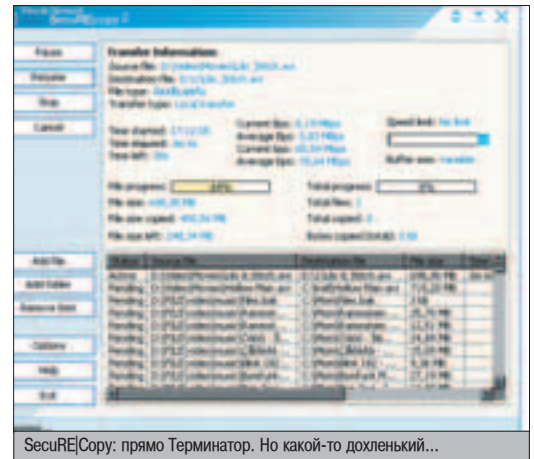
KILLCOPY V2.71

ОС	WinAll
РАЗМЕР	971 Кб
ЛИЦЕНЗИЯ	Freeware
САЙТ	http://killprog.narod.ru

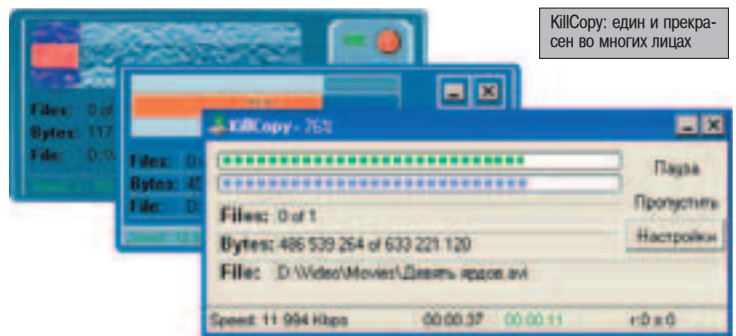
Маленькая русская программа с суровым названием, заставляющая все остальные софтины нервно курить в сторонке.

Садится в контекстное меню, но может и полностью подменять собой Explorer, чтобы при обычном перетаскивании файла он копировался KillCopy (опция Make KillCopy as default drag&drop handler). Интерфейс настраивается с помощью скинов, которых полно на сайте, и отображает общее и оставшееся время копирования, проценты загрузки каждого и всех файлов и скорость в Kbps.

Естественно, поддерживается докачка, причем с кучей дополнительных возможностей. Во-первых, KillCopy может вносить в реестр запись о копировании и, в случае падения винды или вырубания электричества, автоматически его продолжит после перезагрузки. Во-вторых, все незаконченные по любой



SecureCopy: прямо Терминатор. Но какой-то дохленький...



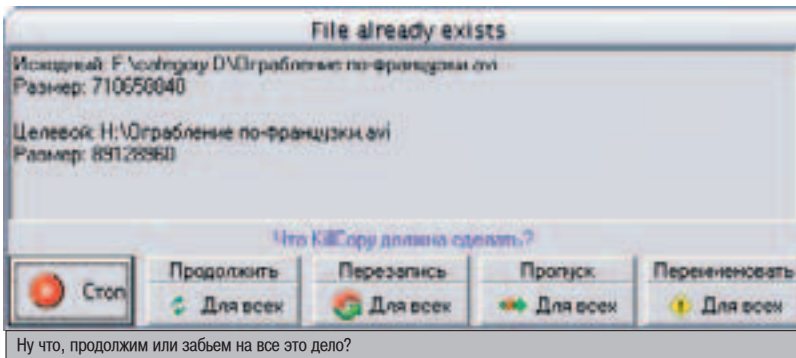
KillCopy: один и прекрасен во многих лицах



- НУ И ГДЕ МОЙ КРЯКЕР ИНТЕРНЕТА?



- А ТЫ ЗАПУСТИ .EXE-ШНИК ИЗ АТТАЧА!



причине зачатки отображаются в окне Resume manager, где ими можно как угодно манипулировать. И, наконец, в-третьих, есть очень удобная опция - автоматическое продолжение (параметр If file exist-try resume), когда KillCopy сверяет содержимое файлов, и если видно, что конечный - это часть исходного, то сразу начинает докачивать, ничего не спрашивая у пользователя.

ENLARGE YOUR BUFFER

Все ускорители работают примерно одинаково, и их метод прост до безобразия: это обычное кэширование. Отсюда, кстати, следует вывод, что под Win9x их использование эффективнее, чем под Win2k/XP: в NT-системах и так все нормально работает, в отличие от старых виндов, которым и многочисленные твики не всегда помогают...

Что же касается копирующих программ, то там размер буфера кэша - это самая главная опция, которая может как ускорить, так и существенно замедлить работу. Подбирается это значение экспериментально, исходя из особенностей компа, объема оперативки и самой программы. Например, для описанных BurstCopy и KillCopy у меня оптимальными были значения в 16 Мб, а для SecuRE|Copy - 8 Мб. У тебя все может быть совсем иначе.

Стоит сказать одно: если мало оперативки, то особенно дергаться не стоит: маленький буфер ничего тебе не ускорит, а большой заставит винду дергать своп, от чего скорости, конечно, не прибавится.

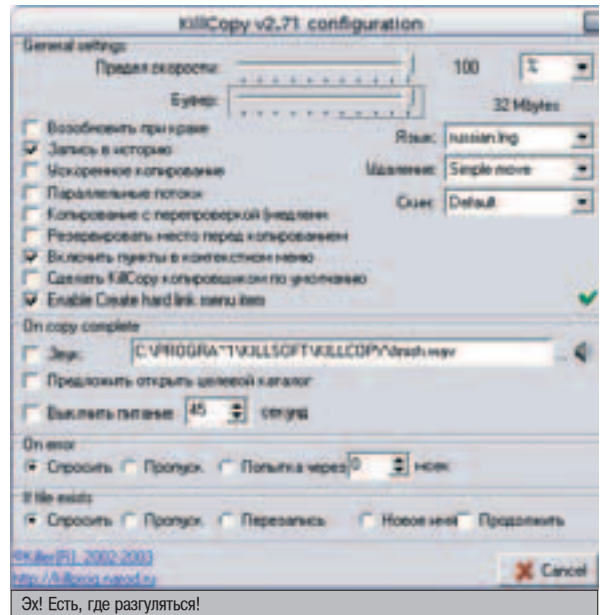
Зато ее прибавится от других "твиков": гораздые на выдумки программмеры добавляют возможности распараллеливания чтения и записи на разные потоки или повышения приоритета своих прог в винде, от чего копирование зачастую идет быстрее.

КАК МЫ ТЕСТИРОВАЛИ

Для тестирования использовался компьютер на базе AthlonXP 1600+ с материнской платой на чипсете VIA KT600 и жесткими дисками Maxtor 6L080J4 в режиме ATA-133. Локальная сеть на 100 Мбит построена на наиболее распространенных карточках от Realtek (чип 8139B).

Во время тестирования из памяти выгружались все программы и убивались все процессы, которые могли помешать работе (помни, что любой антивирусный монитор - самый главный враг скорости!). Для каждой программы выяснялся оптимальный размер ее буфера, который во время тестирования и выставлялся.

Несмотря на это - помни: получившиеся результаты справедливы лишь для конкретного компьютера, с конкретной системой и настройками! У тебя все может быть совершенно иначе и с точностью до наоборот! Но вряд ли ;-).



Настройки скорости, кроме обычного объема буфера, состоят из трех опций - High-speed copy, Parallel read/write и Speed limit. Первые две можешь включать не раздумывая, а третью - в зависимости от конфигурации твоей локалки.

Между прочим, KillCopy единственная программа, заботящаяся о секретности: установи Move mode на 3-pass overwrite, и при переносе софтина будет аж три раза забивать нулями старый файл перед удалением - чтобы никто никогда не восстановил.

Но это все лишь дополнительные фенечки, а что же с главным - со скоростью? Так ведь и тут все просто замечательно! Смотри сам - KillCopy уделывает всех конкурентов и виндовый Explorer, особенно при копировании в пределах одного жесткого диска.

На мой взгляд, у KillCopy лишь два мелких недостатка. Во-первых, довольно примитивная очередь (но ведь у того же BurstCopy ее вообще нет!) - только для копирования в один и тот же каталог. А во-вторых, немного странное поведение при работе: через несколько секунд после начала скачивания прога почему-то начинает серьезно грузить проц, и в это время работа сильно замедляется, что сказывается на конечном результате... Надеюсь, автор это поправит.

И еще не могу не сказать о встраиваемости KillCopy в Far или Total Commander - на это не способна больше ни одна утилита. Кстати, и возможности для консольного использования у КС самые богатые: любители скриптов и bat'ов не останутся обиженными.

Выводы

Наш главный вывод состоит в том, что различные копировщики следует использовать скорее для получения большего удобства и расширенных возможностей, чем для увеличения скорости. В любом случае, лучшей на данный момент является, безусловно, утилита KillCopy, которая сочетает в себе отличную функциональность и высокую скорость. По крайней мере, на моей машине она, похоже, обосновалась всерьез и надолго :).

Способ копирования	Explorer	BurstCopy	SecuRE Copy	KillCopy
В пределах одного физического диска (с одного логического диска на другой):				
- файл 2 Гб	282 с.	210 с.	285 с.	190 с.
- 11300 файлов на 1,8 Гб	459 с.	417 с.	> 1000 с.	418 с.
С одного винчестера на другой:				
- файл 2 Гб	154 с.	173 с.	239 с.	153 с.
- 11300 файлов на 1,8 Гб	240 с.	550 с.	> 1000 с.	240 с.
Передача информации по сети 100 Мбит:				
- файл 2 Гб	300 с.	337 с.	378 с.	294 с.
- 11300 файлов на 1,8 Гб	508 с.	993 с.	> 1500 с.	450 с.

- 256Мб DDR видеопамяти
- Вывод / DVI / ТВ-выход / 2 VGA-выхода
- Технология GameFace
- Технология охлаждения Smart Cooling
- Технология защиты системы Smart Doctor II
- Технология Video Security II
- Технология Digital VCR II
- Ulead Cool 3D 2.0 + Photo Express 4.0 SE
- Программный проигрыватель ASUS DVD XP S/W player
- Power Director Pro
- Media Show
- Новейшие 3D игры в комплекте: Half Life 2, Battle Engine Aquila, Gun Metal, 6 в 1 Game Pack



ASUS Radeon 9800 XT/TO

ASUS®

WWW.ASUSCOM.RU

ASUS V9950 Ultra GeForce FX 5900 Series

- nVidia GeForce FX 5900 Ultra
- Передовая технология CineFX™ 2.0
- 256 Мб DDR видеопамяти с 256-разрядной шиной данных и интерфейсом AGP 8X
- Фирменная онлайн технология GameFace от ASUS
- Поддержка DirectX 9.0 и OpenGL 1.4
- Технология отображения информации на нескольких дисплеях nView
- Новейшие 3D игры в комплекте



Тел: (095) 974-32-10
Web: <http://www.pirit.ru>



Тел: (095) 105-0700
Web: www.oldi.ru



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



Тел: (095) 708-22-59
Факс: (095) 708-20-94



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



Тел: (095) 269-1776
Web: <http://www.dist.ru>



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



ПОЧТОВЫЕ ПЕРЕХВАТЧИКИ



Как гласит старинная легенда, любопытной Варваре на базаре так хорошо дали прокашляться, что она до сих пор на больничном сидит, нос отращивает. Про ЧП с Варварой все слышали, но ее печальная история до сих пор никого ничему не научила. Как были мы любопытными, так любопытными и остались. Более того, изобретательные товарищи на этом самом любопытстве научились неплохо зарабатывать. Видеокamеры на стенах, жучки в телефонах и даже простые поточники, продающие бинокли под вывеской "Зацени пейзажи на нудистском пляже". Со временем, когда компьютеры перестали занимать большую часть квартиры, появился спрос на софтовые шпионы. Почему бы и нет, вполне закономерно. Мы общаемся не по телефону, а в чатах и ICQ, мы выкидываем конверты и отправляем исключительно электронную почту. Что самое главное, следить стало проще и дешевле. Кто будет смеяться ради сверлить потолок, чтобы узнать всю подноготную своего соседа? Другое дело - скачать и запустить на его компе программу. Может, и у тебя такая припудра работает, а ты и знать не знаешь. Зевая, бормотать "Сомневаюсь..." не советую. Идем, я тебя с настоящими шпионами познакомлю.

КТО КОНТРОЛИРУЕТ ТВОЮ ПЕРЕПИСКУ?

ВКРАДЧИВАЯ ПРЕПЮДИЯ

Основной целью излишне любопытного слепопыта является электронная почта. На работе могут перекрыть выход в ICQ, но почта, как правило, исправно функционирует. Как мы ее отправляем? При помощи любимого мейлера или с WEB-интерфейса. Соответственно, существуют два вида почтовых шпионов. О них и поговорим. Для начала - аксиома. Кунг-фу придумали не для того, чтобы положить охрану в автосалон и уехать домой на серебристой "бэхе". В первую очередь, это защита. Не слушай разработчиков. Их рекламные лозунги - это просто сказка. "Контролируй своих детей!" (если воспитать не в состоянии), "Следи за женой!" (проще развестись), "Наблюдай за коллегами" (открой в себе настоящую сволочь...). Это не наши методы. Но если твоя машина остается без присмотра, и к ней возможен доступ со стороны, то

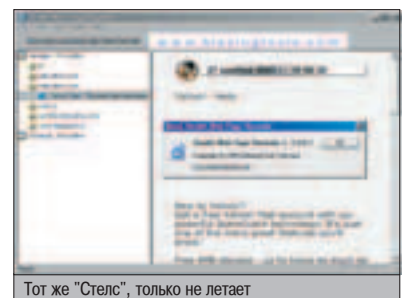
программы из этого обзора ты должен знать в лицо. Чтобы не было потом мучительно больно.

ЗНАКОМСТВО С ПРЕДМЕТОМ

Итак, два вида шпионов. Первые (наиболее безобидные) контролируют отправку писем с WEB-интерфейса бесплатных почтовых служб. Отслеживают появление определенной страницы в браузере и сохраняют ее в своей базе. Вторые (и это уже серьезно) вклиниваются между мейлером и SMTP. Разработчики обещают, что фаервол будет молчать, и это верно, т.к. сам шпион в интернет бежать не торопится. Ты отправляешь почту, а он лишь перехватывает обращение к SMTP-серверу и добавляет в заголовки еще одного получателя. Сообщение отправляется к наблюдателю вполне легально. Фактически, оно уходит из твоей почтовой программы, которую фаервол пропустит без вопросов.

STEALTH WEB PAGE RECORDER

Программа из первой категории - специально для WEB-интерфейса. В системе не видна, установочный архив занимает всего 115 Кб. Интегрирует в Internet Explorer мелкую библиотеку web.dll под видом прис-

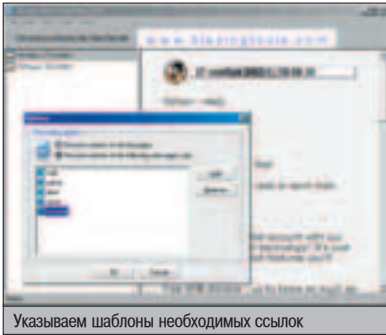


Тот же "Стелс", только не летает

тавки "SWL IE Plugin". В результате подкаталог Data постепенно заполняется файлами вида 2003-11-28_05-31-52-1383268.dat. Это страницы, которые ты открываешь в эксплорере. Stealth WPR отбрасывает все лишнее и сохраняет исключительно текст. Первая строка в таком файле - ссылка на исходный документ, за которой следуют заголовки и тело страницы. Что важно знать - сама прога (WebPageRecorder.exe) ничего не отслеживает и не сохраняет. Это просмотрщик базы. Имитирует стандартный интерфейс журнала посещенных ранее адресов интернета, посему прост и неприязнителен. Там же настраиваются параметры программы. Точнее, один-единственный параметр - сохранять содержимое всех стра-



- ▲ Описание протокола SMTP
<http://manual.ru/download2/3499.html>
- ▲ Simple Mail Transfer Protocol
www.rfc-editor.org/rfc/rfc2821.txt
- ▲ SMTP Service Extensions
www.rfc-editor.org/rfc/rfc1869.txt
- ▲ SMTP Service Extension for Authentication
www.rfc-editor.org/rfc/rfc2554.txt



Указываем шаблоны необходимых ссылок

STEALTH WEB PAGE RECORDER

- ▲ Freeware, 115 Кб
- ▲ Домашняя страница программы www.blazingtools.com
- ▲ Установочный архив www.antispy.biz/downloads/inst_swpr.exe

Рекламный ролик "Теперь я все знаю!"

Черный экран. "Сан Саныч, я ж просто софтинку тестил!" В кадре - офис, рабочий стол. Солидный мужик в красном пиджаке: "Михал Иванович был замечательным сотрудником... Пока не отправил в Никарагуа чертежи атомной бомбы". Золотистая надпись: "Нет человека - нет проблемы. Stealth Web Page Recorder!"

ниц или выбирать ссылки, которые содержат указанные тобой ключевые слова.

Основные достоинства - бесплатная программа, смешной размер дистрибутива, простой приятный интерфейс и настраиваемая фильтрация по ссылкам. Недостатки - работает только с Internet Explorer. Игнорирует даже MyIE. Кроме того, если страница отобразилась не полностью, в базу она не попадет, это факт. Специально заходил на YahooMail, чтобы отправить пару писем. В базе - тишина и покой. Обнаружить программу в системе элементарно - открываем RegEdit, ищем строку SWL Plugin Class, читаем путь к библиотеке в подразделе InprocServer32.

WEBMAIL SPY

Продолжаем исследовать WEB-интерфейс. Дистрибутив программы WebMail Spy содержит базу данных с шаблонами страниц наиболее распространенных (читай - западных) почтовых служб. Впрочем, попадаются и знакомые названия, типа HotMail, ICQMail и MSN. Когда пользователь открывает страницу в браузере, WebMail Spy сравнивает ее с шаблонами, попутно сохраняя обнаруженные данные в свой журнал. Это уже не просто коллекция страниц, это упорядоченный список писем, который можно отсортировать по любому критерию и впоследствии сохранить на диск. Есть неплохая система фильтров, которые не позволяют сохранять письма с указанными параметрами (отправитель, адресат, тема, содержимое). Прога умеет работать в двух режимах - Visible (иконка в системном трее) и Stealth (невидимка, используются горячие клавиши). Для доступа ко всем основным функциям WebMail Spy необходимо назначить специальный пароль администратора. Как я уже говорил, в базе проги хранятся настройки на зарубежные почтовые службы.

Если твоя машина остается без присмотра, и к ней возможен доступ со стороны, то программы из этого обзора ты должен знать в лицо.



Сегодня в меню почтовые службы

WEB MAIL SPY

- ▲ Shareware, 1 Мб
- ▲ Домашняя страница программы www.exploreanywhere.com/wms-intro.php
- ▲ Установочный архив www.exploreanywhere.com/webmailspy-setup-sw.exe

Рекламный ролик "Теперь я все знаю!"

Черный экран. "Геша, только не из АКМ!" В кадре - спальня, зеленый торшер. Сияющий джентльмен в домашнем халате: "Зина была замечательной супругой... Пока не изменила мне с негром". Золотистая надпись: "Рецепт простой - живи холостой. WebMail Spy!"

База обновляется через интернет, и кое-кто надеется, что разработчики не обратят внимания на Yandex или Land.ru. Но не все так

просто. Database.dat в каталоге WebMail Spy - это всего лишь текстовик, в котором к коду каждого символа прибавляют число 81. Вот как выглядит произвольный участок базы после расшифровки:

```
[IMail - READMAIL]
Name=ActivatorMail
Web=http://www.activatormail.com
Comments=none.
Updated=August 03, 2002
from_start=From:
from_end=<INPUT
subject_start=<BR>Subject:
subject_end=<HR>
recipient_start=<TD>To:
recipient_end=<BR>
Special=none
```

Мою мысль, я думаю, ты понял.

Обнаружить WebMail Spy не так сложно, как уверяют авторы. Да, можно запретить на машине Safe Mode и не позволить пользователю пропускать запуск приложений из секции автозагрузки, есть такая возможность. Но база данных никак не защищена и легко удаляется в процессе работы программы. Да, можно отключить диспетчер задач, но Webmailspy.exe не скроется от остальных утилит, показывающих список активных процессов. Основной недостаток - за эту софтинку нужно платить. Да и размер богатырский, около мегабайта.

EMAIL SPY PRO

Вот мы и подошли к самому интересному. Email Spy Pro контролирует отправку писем из других почтовых программ. Копии своих трофеев ты можешь переслать на дополнительный адрес, а координаты настоящего получателя письма и вовсе удалить из заголовков. Таким образом, если фирма ведет пере-



Зеленый перехватчик



COVER STORY

ЭКСКЛЮЗИВ ИЗ ПЕРВЫХ РУК!

MEDAL OF HONOR: PACIFIC ASSAULT

КОШМАРНЫЕ РЕАЛИИ ВТОРОЙ МИРОВОЙ В НОВОМ КРОВАВОМ ТРИллЕРЕ ОТ EA! ПЕРЛ-ХАРБОР БЕЗ БЕНА АФФЛЕКА!!

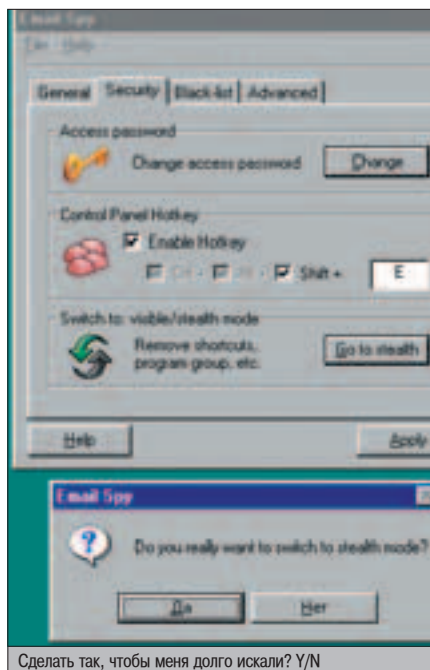
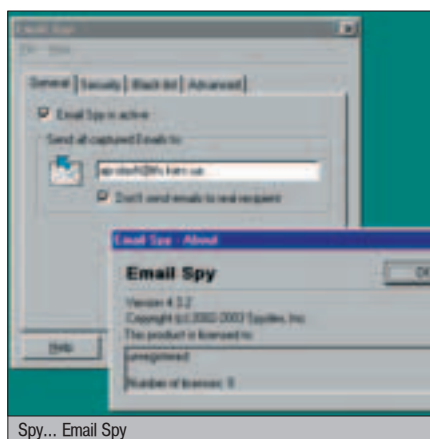
ОБЗОРЫ

Call of Duty, The Temple of Elemental Evil, Railroad Tycoon 3, Prince of Persia - The Sands of Time, Knights of the Old Republic, Final Fantasy XI, Space Colony, Lord of the Rings: Return of the King, Lord of the Rings: War of the Ring, Талисман, Apocalypse, Dungeon Siege: Legends of Aranna, Hegemonia: The Solon Heritage, Need For Speed: Underground, Worms 3D, Empires: Dawn of the Modern World, Age of Mythology: The Titans, NASCAR Thunder 2004, No Man's Land, Neighbors From Hell, UFO: Aftermath и другие!

TECH

Тестирование: 12 дисководов для записи DVD. Сделай сам: Настраиваем BIOS, RAID-массив на дисках Serial ATA. Первый взгляд: TDK Tremor S150, Sanyo PLV-Z2, Nostromo SpeedPad n50, Saitek X45 Digital Joystick & Throttle. Новости

А также: новости, preview, review, Loading, советы по прохождению игр, Игровая Альтернатива, топ 20, Pipeline и т.д.



писку со своими компаньонами, наблюдатель в состоянии перехватывать каждое письмо, запрещать отправку сообщения настоящему адресату и отвечать самостоятельно, меняя поле From в заголовках своих ответов. В зависимости от степени развращенности наблюдателя, у фирмы могут быть крупные неприятности, а Email Spy Pro создает для этого все условия. Доступ к программе ограничен паролем, в диспетчере задач она не отображается, а ее интерфейс надежно скрыт до нажатия указанной комбинации клавиш. Нужно всего лишь назначить адрес для пересылки всей корреспонденции, вписать SMTP-сервер на тот случай, если встроенный механизм подмены заголовков не сработает, и настроить Black-list со списком адресатов, которые тебя не интересуют.

К счастью для мирных граждан, Email Spy Pro совсем несложно обнаружить на своей машине. Первый (самый примитивный) способ - настроить свой мейлер таким образом, чтобы он запрашивал у SMTP-сервера подтверждение доставки твоего письма. Например, в редакторе The Bat! нужно отметить пункт меню "Options - Confirm Receipt (Параметры - Подтверждение доставки)". Как результат, подтверждение отправляет ящик наблюдателя, и если тебе знаком этот адрес, то дальше уже дело техники. Точнее, дело группы злобных техников с гаечными ключами. Но у этого способа есть два недостатка. Во-первых, почтовый ящик наблюдателя может не поддерживать функцию отправки такого подтверждения. Во-вторых, он получит письмо. Приятного в этом мало, поэтому пробуем способ номер два. Ставим любой локаль-

ный SMTP-сервер (например, QK SMTP Server - www.qksoft.com/qk-smtp-server/), в его настройках указываем перенаправление на несуществующий локальный адрес и отправляем сообщение. Адрес получателя - на твоё усмотрение. Только учти, что если он попал в Black-list программы, Email Spy Pro себя никак не проявит. Отправляем, смотрим в журнал работы SMTP-сервера. Если адрес получателя остался прежним, значит все в порядке.

EMAILOBSERVER

EMAILSPY PRO

- ▲ Shareware, 308 Кб
- ▲ Домашняя страница программы www.spydex.com/emailspypro.html
- ▲ Установочный архив www.spydex.com/emailspypro.zip

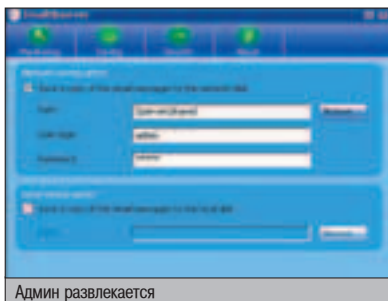
Рекламный ролик "Теперь я все знаю!"

Черный экран. "Папа, мы не умеем плавать!" В кадре - ванная комната, резиновый утенок. Огромный мужик в лиловых наколках: "У меня были замечательные дети... Пока не разболтали о том, что я пропил тещину брошку". Золотистая надпись: "Durex - всему голова. Email Spy Pro!"

В целом, принцип работы EmailObserver почти не отличается от Email Spy Pro, но есть и свои особенности. В частности, помимо перенаправления писем на свой собственный адрес, их можно сохранить на винчестере и даже на удаленном компьютере. Для этого на закладке "Saving" нужно указать полный путь к удаленной машине, а также логин и пароль для соединения с ней. Чтобы скопированные на диск письма сложнее было опознать, EmailObserver может их зашифровать. Из мелких бонусов имеет смысл отметить возможность пересылать копию письма на несколько адресов, а не на один, как это делает Email Spy Pro. И наконец, к теме каждого письма можно добавить уникальный префикс, чтобы наблюдатель сортировал у себя на машине доклады своих шпионов, особо не напрягаясь.

Недостатки? Есть. Во-первых, она платная. Во-вторых, работает только под NT, т.к. для работы ей необходимо установить специальный "SMTP over TCP/IP" сервис. К слову, мне так и не удалось запустить ее на XP Home, программа упорно выбивала несчастную операционку в синий экран. Проверить наличие этой заразы у себя на винчестере





Админ развлекается


EMAILOBSERVER

- ▲ Shareware, 645 Кб
- ▲ Домашняя страница программы www.softsecurity.com/email_observer.html
- ▲ Установочный архив www.softsecurity.com/download/email_observer/emailobs.zip

Рекламный ролик "Теперь я все знаю!"

Черный экран. "Миха, я же говорю, лифт еще не прие-е-е-е..." В кадре - двери лифта, жестянка с окурками. Щуплый очкарик с ноутбуком: "Сеня был замечательным другом... Пока не утянул мои пароли". Золотистая надпись: "Старый друг - лучше новых был. EmailObserver!"

тере можно двумя способами. Первый повторяет аналогичную процедуру для поиска Email Spy Pro, а второй относится исключительно к EmailObserver. Открывай RegEdit и ставь на поиск слово emossrv. Это и есть ее сервис. Найдешь его, к примеру, здесь: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\emossrv. Найдешь - прибеешь. И это не просто рифма.

На сегодня все. Какие выводы? А самые радужные. Да, существуют программы для контроля твоей переписки в Сети. Да, некоторые из них чихать хотели на твой фаервол. Но бороться с ними можно и нужно. Как видишь, это не так сложно, как кажется. Перехватчики писем с WEB-интерфейса не учитывают слабенький dial-up и пропускают недокачанные страницы. Кроме того, им по силам лишь Internet Explorer, а Орега или MyIE могут спать спокойно. Те, что стоят на пути между почтовиком и SMTP-сервером, не проверяют, настоящий это SMTP или локальная ловушка. Конечно, завтра появятся новые программы. Более умные, более скрытные. Но они остаются программами, так что ты справишься, было бы желание. А если сам надумаешь ими воспользоваться, не забывай - кунг-фу, оно для защиты. Удачи. 

ДИАЛОГ ПОЧТОВОЙ ПРОГРАММЫ И SMTP-СЕРВЕРА МАЛО ЧЕМ ОТЛИЧАЕТСЯ ОТ НАСТОЯЩЕГО ЖИВОГО ОБЩЕНИЯ

❶. Вслед за командой HELO ("Здравствуйте, женщина за прилавком почтового отделения!"), мейлер сообщает серверу о своем решительном намерении отправить почту. MAIL FROM:<адрес_отправителя> ("Хочу теще телеграмму послать. Можно?").

❷. Сервер отвечает ему цифровым кодом состояния, за которым следует необязательный строковый вариант ответа. 250 адрес_отправителя Address Okay. ("Товарищ Расторбищев? А я вас знаю!")

❸. Почтовый клиент продолжает разговор, называя получателя. RCPT TO: <recipient@recipient.com> ("Адрес тещи - ул. Пушкина, трансформаторная будка №4937").

❹. Сервер не возражает. 250 recipient@recipient.com Address Okay ("Наличие будки подтверждено. Отправляй").

Клиент протягивает бланк в окошко, а в это время посторонний мужик успевае дописать свои координаты в дополнительное поле уже готовой телеграммы. Как это выглядит со стороны? Займемся прослушиванием SMTP-сервера. Представь, что user@user.com - хозяин компьютера, который находится под наблюдением у программы Email Spy Pro, recipient@recipient.com - настоящий адресат, а spy@spy.ru - презренное дитя порока, любопытный наблюдатель.

* Если включена опция "Не отправлять письмо настоящему адресату":

```
MAIL FROM:<user@user.com>
250 user@user.com Address Okay
RCPT TO: spy@spy.ru
250 spy@spy.ru Address Okay
```

Мейлер отправляет письмо на recipient@recipient.com, хотя сервер получает указание RCPT TO: spy@spy.ru. Так захотел Email Spy Pro. Передаем слово

почтовой программе:

```
MAIL FROM:<user@user.com>
250 user@user.com Address Okay
RCPT
TO:<recipient@recipient.com>
250 spy@spy.ru Address Okay
```

Забавно, правда? Мейлер добросовестно выполняет свою работу, а SMTP упорно играет в податую секретаршу:

- Будьте так любезны, отправьте это письмо Петру Сергеевичу.

- Всенепременно (чего он там сказал?), я отправлю это письмо Прасковье Семеновне (мама, как мне плохо...).

* Если наблюдатель не удаляет адрес настоящего получателя письма, процесс отправки сообщения проходит примерно в том же стиле. The Bat!, как и прежде, все делает правильно:

```
MAIL FROM:<user@user.com>
250 user@user.com Address Okay
RCPT
TO:<recipient@recipient.com>
250 recipient@recipient.com
Address Okay
```

Только на самом деле SMTP-сервер получает следующие команды:

```
MAIL FROM:<user@user.com>
250 user@user.com Address Okay
RCPT TO: spy@spy.ru
250 spy@spy.ru Address Okay
RCPT
TO:<recipient@recipient.com>
250 recipient@recipient.com
Address Okay
```

Вот ведь как оно в жизни бывает, да?



СТАВИМ БОТА НА РАЗДАЧУ

В прошлый раз мы видели, как лихо народ добывает вarez в IRC-сетях. Теперь давай заценим, как продвинутые товарищи мутят собственные файлообменные ресурсы. Оставим философию в стороне - возьмем реальный бот, поковыряем его, помучаем и попытаемся заставить нормально работать.

КАК ОБМЕНИВАЮТСЯ ФАЙМАМИ В IRC

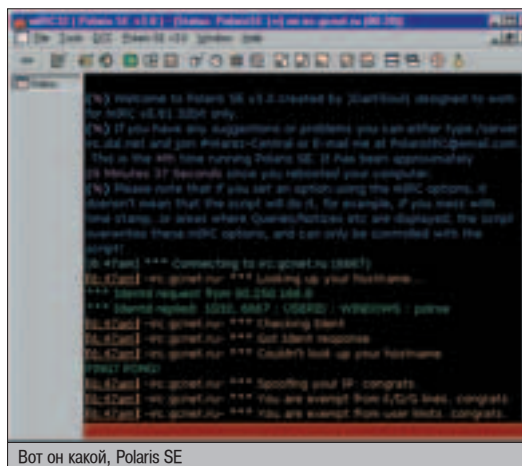
ВЫБОР БОТА

Спроси любого завсегдадая вarezных каналов на IRC, какой бот лучше всего заточен для раздачи файла. В ответ ты чего только не услышишь :). Однако Polaris SE упомянет в разговоре почти каждый второй. А все потому, что это наиболее продвинутый бот, с кучей полезных в быту настроек, работающий одновременно в режиме Fserve и xDCC.

Релиз Polaris SE v 3.0 совершенно бесплатно лежит по адресу <http://hemma.kramnet.com/tobias.wiklund/polaris/download.html> (туда же перебрасывает ссылка www.geocities.com/Polaris_SE), весит всего 920 Кб в архиве.

ТЕХОСМОТР

Устанавливать ничего не надо. Распаковываешь архив и запускаешь mirc32.exe. По сути, это mIRC 5.61, но с кучей готовых скриптов и предустановок (файлы *.ini). Возникает логичный вопрос: почему не используется последняя версия mIRC 6.12? Ответ прост: движок у 5.61 и 6.12 одинаковый, а все необходимые скрипты самописные. Проблема в том, что разные версии mIRC'a могут иметь



Вот он какой, Polaris SE

небольшие отличия в языке скриптов, поэтому автор в архиве прилагает именно ту версию, под которую он писал и отлаживал свое творение. Можно было, конечно, рассыпать только сами скрипты, предлагая скрестить их с mIRC v 5.61. Но не факт, что ты найдешь mIRC 5.61 (обычно в инете валяется самая последняя версия) и самостоятельно скопируешь файлы в необходимые директории. А так все просто: скачал, распаковал и запустил, никакого геморроя

МЕНЮ

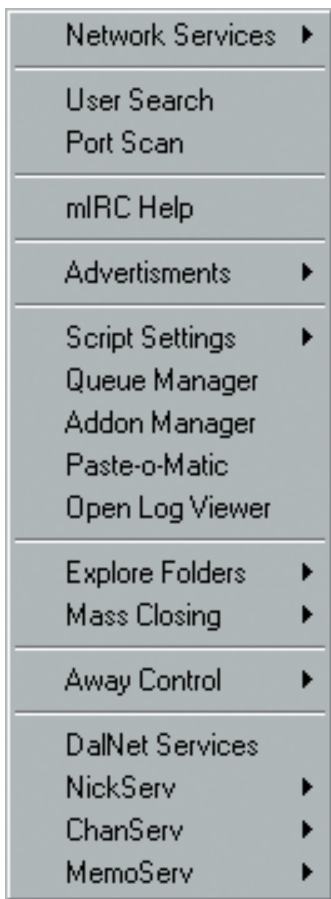
От стандартного mIRC Polaris SE отличается кучей собственных настроек, доступ к которым осуществляется через специальное меню (оно так и называется - Polaris SE v 3.0). Кроме того, до многих опций можно добраться через всплывающие меню в окнах статуса, канала и привата (по нажатию правой кнопки мышки).

Основное меню (на контрольной панели) содержит следующие пункты:

- Network Services - подключение/отключение команд сервисов DalNet, доступных из этого же меню;
- User Search - поиск по маске;
- Port Scan - сканирование портов сервера, определение наиболее быстро;
- mIRC Help - встроенный хелп в mIRC;
- Advertisements - фразы, выдаваемые ботом в каналы на автомате;
- Script Settings - настройки скрипта;
- Queue Manager - управление очередью (когда число желающих скачать переваливает заданный предел);



▲ А еще в mIRC можно загрузить свой FTP-шник. Все необходимое уже есть: Polaris SE v3.0 -> Script Settings -> FTP -> Setup. Подключения, само собой, будут идти на твой текущий IP-адрес. Следует лишь задать порт, логин, пароль и триггер, по которому все будут стучаться. Пара кликов и готово!



Меню Polaris SE



Стандартная раскраска



Настройки бота

Addon Manager - загрузчик дополнительных скриптов;

Paste-o-Matic - текстовое сообщение, отправляемое одновременно во все каналы, где висит бот;

Open Log Viewer - просмотрщик логов бота;

Explore Folders - мониторинг директорий, которыми управляет бот;

Mass Closing - завершение всех имеющихся соединений юзеров к боту (DCC-соединения, очереди и доступ на Fserve);

Away Control - управление;

DalNet Services - команды сервисов DalNet.

тебе, возможно, захочется поправить цветовую гамму, расположение меню и тому подобные вещи. Это не проблема. На качество работы Polaris_SE эти изменения не повлияют. Так что дерзай. К примеру, цветовую гамму можно сменить через Tools -> Colours.

Все основные настройки скрипта сосредоточены в Polaris SE v3.0 -> Script Settings.

Они включают:

General - общие настройки;

Anti Spam - настройка защиты против спама;

Auto Join - привязка к сетям каналов, на которые бот заходит автоматом;

File Server - настройка Fserve;

FTP - настройка FTP на своем IP-адресе;

Request Ad - установка задержки сообщения и ввод самого сообщения, которое бот периодически выдает в прописанные каналы;

НАСТРОЙКИ

По умолчанию mIRC уже настроен так, как нравится (}DarkSoul(), автору Polaris_SE. Но

ПО ШАГАМ

Последовательность действий при настройке File Server и XDCC в Polaris SE одна и та же:

- 1) Определяешь общие настройки: Polaris SE v3.0 -> Script Settings -> General;
- 2) Выставляешь настройки File Server или XDCC: Polaris SE v3.0 -> Script Settings -> File Server|XDCC;
- 3) Задаешь рекламное сообщение (Ad);
- 4) Запускаешь File Server или XDCC через меню: Polaris SE v3.0 -> Advertisements -> File Server -> Start или Polaris SE v3.0 -> Advertisements -> XDCC -> Long Ad|Short Ad. Либо активизируешь опцию Auto Start и перезапускаешь mIRC;
- 5) Наслаждаешься результатом :).

Теперь в 2 раза дешевле!

Атанда! Читай в ближайшем номере "Хули"!

КАК МЫ ПОПРОШАЙНИЧАЛИ:
Сотрудники «Хули» овладевают премудростями уличного аска

ФИНГЕРБОРД:
Сломал ноги на скейтборде – переходи на фингер.

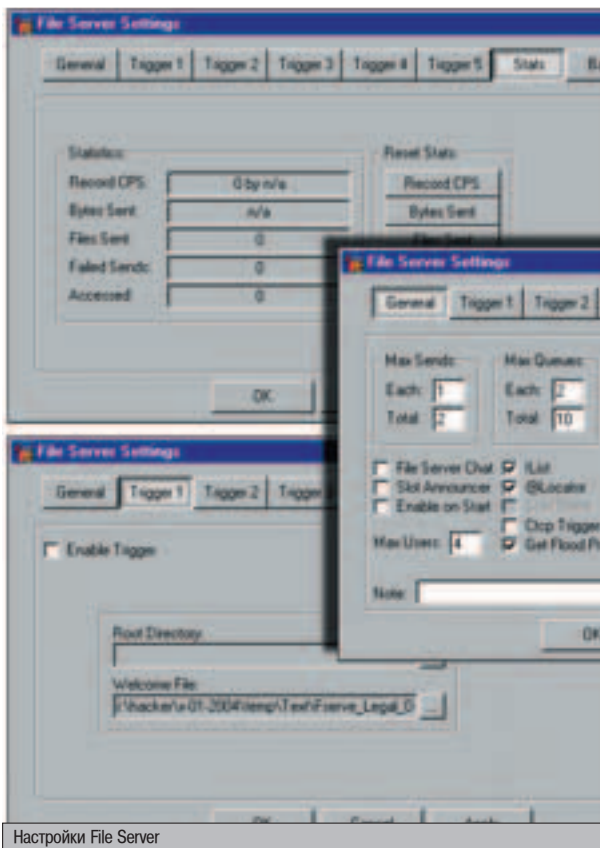
ТРАДИЦИОННАЯ ТАТУИРОВКА:
От средневековых якудза до наших дней

АЭРОГРАФИЯ:
Машина ручной работы

НЕ ТЕРЯЙСЯ:
Как водить танк?

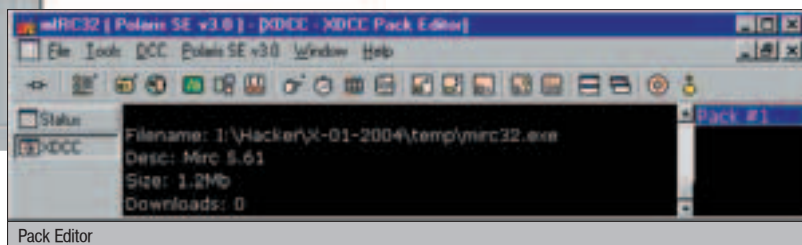
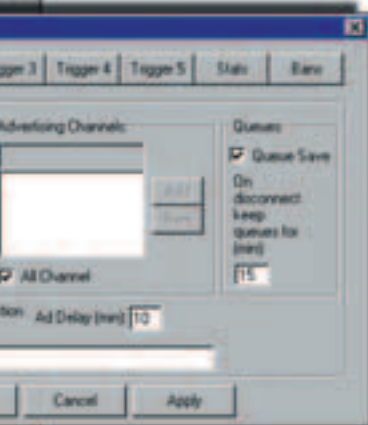
ЗООПАРТИЗАНЫ:
Деды Мазаи нашего времени

КАК Я НЕ ПИЛ 3 МЕСЯЦА:
Отчет храброго экспериментатора



Max Sends - максимальное количество скачиваемых файлов одновременно в одни руки (Each) и вообще (Total);
 Max Queues - максимальное количество файлов в очереди одновременно в одни руки (Each) и вообще (Total);

То есть TDCC - облегченный вариант XDCC. Он устарел и практически не используется.
 Чтобы запустить XDCC, сперва необходимо зайти в общие настройки: Polaris SE v3.0 -> Script Settings -> XDCC -> General, с опциями (некоторые аналогичны File Server):
 Max Sends - максимальное количество скачиваемых файлов одновременно в одни руки (Each) и вообще (Total);
 Max Queues - максимальное количество файлов в очереди одновременно в одни руки (Each) и вообще (Total);
 Pack Listing - активация вывода в канал полного списка доступных для скачивания файлов;
 Delay - задержка вывода в канал полного списка pack'ов (доступно, если активирована опция Pack Listing);
 Advertising Channels - каналы, на которых бот ведет пропаганду;
 Ad Delay - интервал, задающий частоту выброса в каналы рекламного сообщения;
 Auto Start - автоматический запуск при коннекте на сервер (в противном случае запускать нужно вручную, через меню);



Настройки File Server

TDCC - настройка TDCC;
 XDCC - настройка XDCC;
 Import Settings - импорт настроек из более ранних версий Polaris SE (к примеру, Excursion, Invision).
 Изначально все опции выставлены оптимально. Поэтому можно сразу приступать к непосредственной настройке File Server или XDCC (TDCC).

FILE SERVER

В окне настроек File Server (Polaris SE v3.0 -> Script Settings -> File Server) имеются четыре вида вкладок: General, Trigger, Stats и Bans. General - сердце Fserve, советую тебе туда заглянуть и определиться со следующими параметрами:

Advertising Channels - каналы, на которых бот ведет пропаганду;
 Queues Save - время, в течение которого сохраняется очередь при дисконнекте;
 Enable on Start - автоматический запуск при коннекте на сервер (в противном случае запускать нужно вручную, через меню);
 !List - активация на запрос !list;
 @Locator - активация на запрос @name;
 Ctcp Triggers - триггеры воспринимаются через ctcp (в противном случае - как обычный текст);
 Get Flood Protection - включить защиту от флуда (настраивается в Polaris SE v3.0 -> Script Settings -> General);
 Ad delay - интервал, задающий частоту выброса в каналы рекламного сообщения;
 Note - комментарий по File Server, который будет виден юзерам.

Short Ad - активация укороченного сообщения от бота в канал (более развернутая информация доступна уже только через дополнительный запрос);
 Silent - бот молчит как партизан.
 Разобрался? Необходимо сделать следующий шаг - задать хотя бы один файл (один pack) через имеющийся редактор: Polaris SE v3.0 -> Script Settings -> XDCC -> Pack Editor. Окно в самом начале пустое - это нормально. Нажимаешь правую кнопку мышки и там на выбор:
 View - просмотр информации по выделенному pack'у;
 New Packs - заведение сразу нескольких pack'ов;
 Edit Pack - редактирование pack'a;
 Add Pack - добавление pack'ов по одному;
 Del Pack - удаление выделенного pack'a.
 Все, можно запускать: Polaris SE v3.0 -> Advertisments -> XDCC -> Long Ad/Short Ad (Long - более полная информация, которую выдает бот, Short - укороченная).

Пять вкладок Trigger позволяют запускать параллельно до пяти Fserve. Для каждого будет свой триггер, а следовательно, и своя директория (Root Directory). Stats - статистика по File Server, а Bans - отпор нерадивым пользователям (бан ставится по маске nick!ident@host).

Вроде пока все понятно, да? Выставляешь все опции и запускаешь процесс: Polaris SE v3.0 -> Advertisments -> File Server -> Start.

XDCC (TDCC)

Сначала скажу, чем TDCC отличается от XDCC. В TDCC можно задать до пяти разных файлов, каждый из которых будет иметь собственный триггер. В XDCC количество файлов неограниченно, каждый файл помещается в так называемый pack. Файлы нумеруются, имеют общий триггер и различаются лишь порядковым номером.

WAREZ НА IRC - ЭТО ПРОСТО

Как видишь, ничего сложного нет. Настроить бота сможет при желании даже обычный юзер. Особенно если у этого юзера есть декабрьский номер X, а потому он уже знает, что такое триггер, бот, Fserve и XDCC :). Так что смело качай, настраивай и запускай свой файл-сервер, работающий на полном автомате. Помни - собственный бот, ведущий раздачу интересного контента, крайне положительно сказывается на статусе человека в некоторых особо продвинутых сообществах.



Настройки XDCC (TDCC)

Panasonic

ideas for life

фотоматериалы русского экстремального проекта



реальный отрыв

**Panasonic создает новые ценности
для обогащения жизни людей
и прогресса общества**

СЕТЕВОЙ ПАПАРАЦЦИ



По тысячам узлов в Сети разбросаны миллионы картинок с самым разнообразным содержанием. И масса юзеров ежедневно перепахивает эти графические отложения вдоль и поперек. Эх, да что там говорить! Ты и сам, наверное, знаешь кучу сайтов с клевыми фотками. Настолько клевыми, что их хотелось бы гигабайтами сливать себе на винчестер. Но, увы, вручную скачивать графику в таких объемах невозможно - уже на втором десятке фоток устаешь от рутинных операций и начинаешь люто ненавидеть в браузере пункт меню "Сохранить рисунок как...". К счастью, существует и другой путь... Не надо оаций, просто слушай сюда. Я расскажу тебе, как автоматизировать процесс добычи графики по максимуму!

БЫСТРО И БЕЗ ПРОБЛЕМ СКАЧИВАЕМ ФОТКИ ИЗ СЕТИ

УТОМПЕННЫЕ ДРЕС'ОМ

Я даже не буду уточнять, какие именно фотки мы с тобой станем скачивать из инета. Ты сам прекрасно знаешь, что находится на первых местах в рейтингах поисковиков. Перейдем сразу к делу. Точнее - к проблеме, которая заключается в том, что владельцы всех ресурсов определенной тематики создают неимоверно много преград на пути простого пользователя, желающего насладиться произведениями фотоискусства. А ведь обычному юзеру так мало надо - дайте ему простой список ссылок на графические файлы, и он будет счастлив. Но - нет. От злобных веб-мастеров такого не дождешься. Они объединяют картинки в галереи (thumbnails), перемешивают их с рекламой, прячут за неприглядными ссылками, а то и вообще - показывают по одной картинке (естественно, в несколько слоев окруженной баннерами) на странице, заставляя посетителя сайта каждый раз давить на кнопку "Next"... Ну разве это не свинство, конечно! Собственно говоря, именно с этим свинством мы и будем бороться. Наша задача ясна - мы должны скачивать интересующие нас подборки изображений с наименьшими затратами сил на кликанье по кнопкам и лицезрение рекламы. Посмотрим, чем и как можно этого добиться.

ОН И МЕНЯ ПОСЧИТАЙ!

Приглядевшись к ссылкам на серию картинок или содержащих их страниц, ты можешь заметить, что зачастую они практически одинаковы и отличаются только порядковыми номерами. Что-то типа www.host.com/hot_pictures/pic_1.jpg, [pic_2.jpg](http://www.host.com/hot_pictures/pic_2.jpg) и так далее... Грех этим не воспользоваться!

PICTURE PUMP v 1.0

ОС: WinAll
Размер: 250 Кб
Лицензия: Freeware
Сайт: <http://zmey.com.ru>

Отечественная софтина - маленькая, быстрая и удобная. В простейшем случае практически единственное, что нужно сделать - скопировать адрес графического файла из серии, вставить его в верхнее текстовое поле и заменить изменяющуюся часть названия подстановочным символом (по умолчанию - "@"), т.е. чтобы имя было не pic_0119.jpg, а pic_@.jpg. Теперь удостоверься, что в выпадающем списке чуть ниже выбрано "URL сайта указывает на картинку", установи начальное и

конечное значение и шаг его увеличения. Если в названии используются ведущие нули (т.е. photo0001.jpg, а не photo1.jpg), то в поле "Шаблон" достаточно вписать столько символов "@", сколько знаков в числе (шаблон может быть и сложнее, чтобы формировать строки вида [image0057\(2\)-9.jpg](http://image0057(2)-9.jpg), но обычно в этом нет необходимости)... Галка "16-ричный" устанавливает соответствующий (а не десятичный) формат чисел, но на практике с таким видом нумерации мне сталкиваться еще не приходилось. Остается указать папку для сохранения скачанных данных, и можешь давить на "Старт"... Вот, в общем-то, и все! Picture Pump начнет сливать файлы в несколько потоков и аккуратно складывать их на винт.



Кардинально меняются функции программы, если в главном окне выбрать в выпадающем списке "URL сайта указывает на страницы с картинками". В этом случае софтина начнет качать веб-страницы, анализировать их и загружать те изображения, ссылки на которые есть в html-коде. Сайты, показывающие фотки на отдельных страницах с кнопками "предыдущая" и "следующая", могут нервно курить в сторонке - Picture Pump уделывает их как детей.

Настроек (вызывающихся по кнопкам с "колесиками") у программы столько, что черт ногу сломит, но реально, на мой взгляд, следует изменить совсем немного. Во-первых, в "Настройках пользователя" поставь русский язык интерфейса, а во-вторых, при скачивании изображений с серии html-ок в "Конфигурации проекта" на вкладке "Ответ" укажи в опции "Не скачивать файлы короче" что-нибудь около 15-20 Кб - этого вполне хватит, чтобы отсеять баннеры (да в любом случае - какое удовольствие смотреть мелкие и некачественные фотки?).

Если у тебя большой проект (кстати, я еще не говорил, что Picture Pump позволяет сохранять все настройки - адреса, параметры счетчиков и т.п. - в файлы проектов, чтобы загружать позднее? Ну, значит, теперь сказал) по скачиванию кучи файлов, то тебе, скорее всего, пригодятся фильтры ссылки (соответствующая вкладка в конфигурации) - можно отсеять нежелательные линки или наоборот - оставить только нужные. Но я думаю, что и описанных возможностей вполне хватит для приятного времяпрепровождения.

ВСЕ И СРАЗУ

Вообще, модный в последнее время лозунг. Модный, поскольку применим к любой сфере жизни. В том числе и к добыванию картинок. Взглянем на софт, который как раз и проповедует такой подход.

PICALOADER v 1.39
ОС: WinAll
Размер: 1,54 Мб
Лицензия: Shareware
Сайт: www.vowsoft.com

Эта прога не размнивается на мелочи, а сразу скачивает все графические файлы с заданного узла. Не надо рыскать самому - дай ей URL и возвращайся через пару часиков - все будет в лучшем виде: каждая строка сайта будет изучена на предмет того, ведет она к фоткам или нет.

То, что PicaLoader предназначен для масштабных мероприятий, видно уже по организации его работы: сначала надо создать проект, а уже потом добавлять в него задания (tasks), в основе каждого из которых лежит некий адрес. Конфигурировать сами задания удобнее всего из соответствующей вкладки в правой части окна программы.



О, сколько нам открытий чудных готовят фотки в Internet!

Что тут самое интересное? Во-первых, профили. Они определяют, какие именно изображения останутся на твоём винте (по привычным критериям - формат, объем и размеры картинки), а какие умрут по дороге. Выбирай "All pictures without thumbnail" - не ошибешься. Во-вторых, галка "Support J/VB/JavaScript" - не всякая качалка может похвастаться способностью выковыривать URL'ы из скриптов. "Search sequence pic-

tures" тоже поставь - тогда PicaLoader методом высоконаучного тыка станет искать "серийные" фотки, на которые нет ссылок с самих страниц - вдруг жадный владелец ресурса шифруется? С "Page..." и "Picture location" все просто - надо принять ответственное решение: ограничиваться содержимым лишь данного узла или ходить за картинками и на другие тоже. Особенно интересны опции "Within current directory & deeper": если ты точно знаешь, какой именно раздел сайта тебе нужен, то можешь избежать сливания всего ресурса целиком. Также они помогут скачать серию картинок, каждая из которых находится на отдельной странице (как на многих развлекательных порталах).

Ну, вот и все. Вписываешь сверху окна требуемый URL и жмешь на "Start". Дальше останется только наслаждаться: лениво поглядывать на вкладку "Monitor" (PicaLoader поддерживает многопоточную загрузку), созерцать появление новых изображений в "Pictures" и не торопясь удалять чудом просочившийся графический мусор. Ну, чем не праздник?

АГЕНТ "ТРИ ИКСА"

Увы, не всем нравятся такие сложные и серьезные решения, как PicaLoader. Кому-то по душе небольшие, но функциональные утилитки.

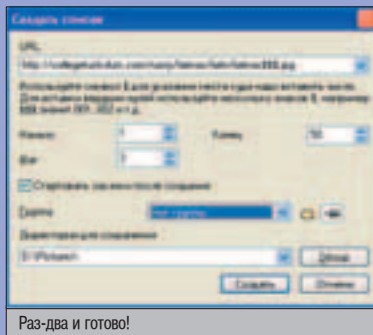
PIXXXGRABBER v 1.1
ОС: WinAll
Размер: 1,8 Мб
Лицензия: Freeware
Сайт: www.pixxxgrabber.com

Идея проста, как пучок морковки: допустим, нашел ты в Сети реальную галерею с картинками. Качать вручную - лениво, а файлы никак не пронумерованы, так что Picture Pump остается не у дел. Можно, конечно, PicaLoader натравить, но слишком уж он громоздкий для такого дела... Впору отчаяться? Ан нет, выход есть!

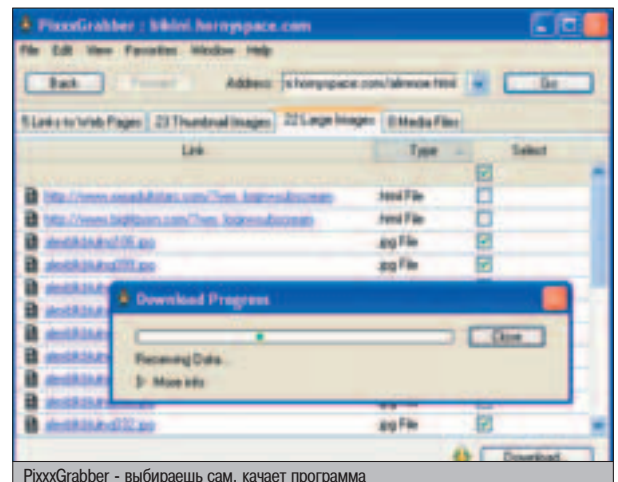
Запускай PixxxGrabber, вводи URL найденной галереи и дави на "Go". Буквально несколько секунд - и страница разложена по полочкам. А точнее - по закладкам. В первой лежат обычные ссылки, во второй - ссылки на маленькие изображения для предпросмотра, в третьей - ссылки на нормальные картинки (вот оно! вот!), и, наконец, в четвертой - линки на разные варианты, типа аудио и видеофайлов.

ЗАЧЕМ ПЛАТИТЬ БОЛЬШЕ

Если ты отличаешься ленью и не хочешь скачивать дополнительный софт, то спешу тебя обрадовать - во многих распространенных менеджерах закачек уже имеются встроенные генераторы списков адресов по заданному шаблону! Пользоваться ими так же, как Picture Pump, и пусть они не так функциональны, но для выполнения простейших действий вполне приспособлены! Например, в любимом многими ReGet'е эта фишка находится в "Автоматизация" - "Создать пронумерованный список" и выглядит вот так:



Раз-два и готово!



PixxxGrabber - выбираешь сам, качает программа

e-shop



ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

PC Accessories



\$65.99



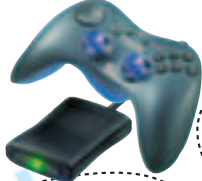
Наушники / Sennheiser HD 500-V2

\$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 Joystick 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
стоимость доставки
снижена на 10%!

СУПЕРПРЕДЛОЖЕНИЕ
ДЛЯ ИНОГОРОДНИХ ПОКУПАТЕЛЕЙ

WWW.GAMEPOST.RU

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

e-shop
<http://www.e-shop.ru>

ЖУРНАЛ
ИГР



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

СЕКС-БРАУЗЕРЫ

Да, я в курсе, что мало кому нравится скачивать все подряд. Многие юзеры предпочитают сначала посмотреть, выбрать... Специально для таких разборчивых товарищей четыре года назад была выпущена программа ThumbNavigator (www.delphicity.com). Она представляла собой своеобразный веб-браузер, умеющий лихо обрабатывать "картинные галереи" таким образом, что все изображения для предпросмотра из нее выдирались и выводились в отдельном окне. Юзер отмечал приглянувшиеся ему картинки, после чего ThumbNavigator скачивал их полно-размерные варианты. Программу ждало великое будущее, если бы автор не забил на нее большой болт - уже много лет прога не обновлялась. И сейчас функцию визуального выбора нужной картинки из серии до загрузки полноценных изображений поддерживает лишь модуль Web Pictures Downloader программы Iphoto (www.keronsoft.com), но его интерфейс нельзя назвать удачным.

В настоящий момент на лавры полноценного "секс-браузера" претендует программа Nici (www.nicisoft.com). Это действительно любопытный софт. В нем, как в обычной бродилке, можно открыть страничку с коллекцией ссылок на галереи с картинками, но только клик по ссылке в Nici вызывает не переход на новую страницу, а загрузку изображений из соответствующей галереи. Конечно, прога новая и пока еще сыровата, но даже сейчас работает весьма неплохо. Остается лишь надеяться, что Nici не уготована судьба ThumbNavigator, и развитие этой проги будет продолжено :).



Иди в третью закладку, выделяй нужное (а точнее, снимай галки с ненужного - лишние файлы всегда легко

отличить по характерным ссылкам) и жми на "Download". Понеслась! Единственное, что огорчает - понеслась всего в один поток. Но, думаю, в следующих версиях этот недостаток исправят. А так прога рулит - мух от котлет, т.е. качественные фотки от всевозможного хлама, она отделяет на ура, с минимальными трудозатратами с твоей стороны.

СТРЕЛЬБА С ЗАКРЫТЫМИ ГЛАЗАМИ

Все описанные выше проги имеют один неискоренимый недостаток: для того чтобы воспользоваться ими на всю катушку, сначала все-таки придется найти сайт с подходящим контентом, где, кроме баннеров, есть хотя бы еще что-нибудь. Но некоторым ленивцам и этого делать не хочется! И софт таким людям придется юзать особый...

EXTREME PICTURE FINDER v 2.3.4

ОС: WinAll

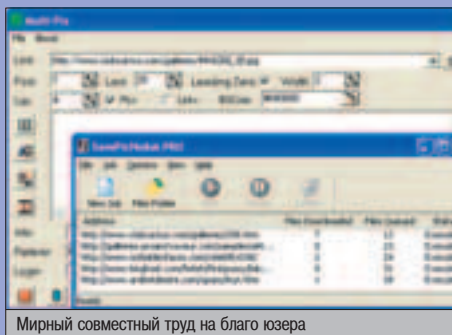
Размер: 1 Мб

Лицензия: Shareware

Сайт: www.exisoftware.com

ХОЧЕШЬ ПОРАБОТАТЬ РУКАМИ?

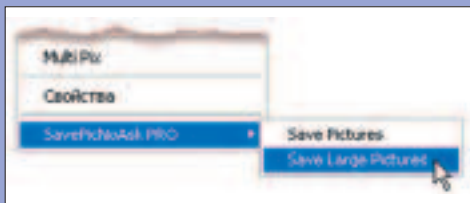
Если тотальная автоматизация тебе совершенно ни к чему, но кликать на каждую ссылку лень, то помогут специальные плагины к Internet Explorer. Связка из пары программ - MultiPix и SavePicNoAsk - выполнит самые изощренные запросы.



Мирный совместный труд на благо юзера

MultiPix (www.yugres.cjb.net) - это привычный "генератор серийников" в стиле Picture Pump. Функционально он ему, конечно, уступает, но зато имеет чрезвычайно удобные кнопки для передачи сгенерированного списка в качалки ReGet или FlashGet, а также встроенное средство создания "безбаннерных галерей". Да, бывают на свете и такие чудеса! Сам посмотри. Когда ты создал список кнопкой со "стрелочкой", то нажми четвертую сверху кнопку, и откроется новое окно IE с выбранными картинками (то есть начнется их скачивание с одновременным показом).

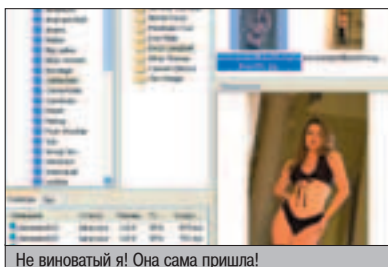
SavePicNoAsk (www.unhsolutions.net/SPNA) - это простая выдиралка изображений из веб-страниц. Нажав на любой ссылке правую кнопку мыши и выбрав из контекстного меню SavePicNoAsk-Save large pictures, ты отправишь в очередь программы этот URL на анализ и скачивание из него фоток, параметры ограничений на



которые (все те же, объем, размер...) следует предварительно установить в опциях (Options-Predefined job properties).

Прежде всего, для полноценной работы этой программкины след с ее сайта модуль русского языка и плагин Adult pictures: без них ты будешь как без рук. Настройки программы в Tools-Settings не блещут оригинальностью: язык интерфейса и каталог сохранения результатов работы в разделе General, да кое-что в Internet: количество рабочих потоков и параметры отсеивания лишних картинок (проще говоря - баннеров).

Итак, в чем же прелесть Extreme Picture Finder? В том, что достаточно выбрать в левом списке интересующую тебя категорию (к сожалению, все эти категории настраиваются плагином, и нет возможности создать что-нибудь самостоятельно) и нажать на кнопку "Начать/Продолжить загрузку", как изображения по выбранной тематике потекут на твой комп широким потоком.



Не виноватый я! Она сама пришла!

Софтина соединяется со специальным поисковым сервером (опять же - жалко, что он зашит в плагине, и нельзя выбрать другой), получает список подходящих страниц и дальше работает как прочие грабберы: отыскивает большие и хорошие картинки (обычно - серии) и сливает их на диск. Для каждой серии создается отдельный подкаталог в рамках соответствующей категории, в котором файлы представлены очень удобными превьюшками ("Вид"-Уменьшенные картинки").

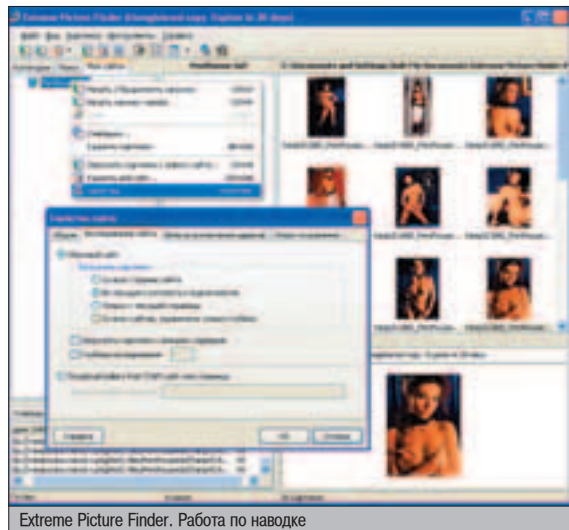
Работает Extreme Picture Finder, на мой взгляд, быстрее других программ: анализируя страницы, он сразу отсекает лишние ссылки, составляет очередь только из "правильных" файлов и скачивает их, не отвлекаясь на посторонние действия (типа проверки очередных изображений и хождения по ссылкам "вглубь" сайтов). Когда этот процесс надоеет (хотя как такое может надоесть?) - достаточно поставить галку "Остановиться после загрузки галереи", и через некоторое время все закончится так же тихо и мирно, как начиналось.

Казалось бы, чего еще желать? Многим и этого хватит за глаза! Однако Extreme Picture Finder умеет и еще кое-что. Если имеющийся выбор категорий тебя чем-то не устраивает, то ты можешь воспользоваться встроенным поисковиком графики: введи любое

ключевое слово, и фотки, содержащие его в своем названии, кучной гурьбой побегут на твою машину...

Но и этим возможности EPF не исчерпываются. Кликнув на вкладке "Мои сайты" по кнопке "Загрузить картинки с нового сайта", ты получишь в свое распоряжение что-то вроде облегченного варианта программы PicaLoader.

С точки зрения Extreme Picture Finder, сайты с картинками бывают двух видов - обычные и так называемые Thumbnail Gallery Post, что примерно означает "сборник ссылок на галереи". С первым все просто - параметры знакомы по PicaLoader, разве что




Extreme Picture Finder. Работа по наводке

Мы должны скачивать интересные нас подборки изображений с наименьшими затратами сил.

нельзя настроить их отдельно для страниц и файлов (а оно тебе надо?). А со вторым надо разбираться подробнее.

Прежде всего, что такое этот "сборник ссылок на галереи": это сайт, на котором размещаются ссылки на всевозможные "картинные галереи", публикуемые другими сайтами. Качать все это на автомате тяжело. PicaLoader или застревает на первом сайте, или наоборот начинает шарить по половине инета. PixxxGrabber и тому подобный софт не подходит - он предназначен для выкачивания отдельных галерей. А вот если эту работу поручить Picture Finder, то есть шанс, что дело пойдет. Особенно если сразу облегчить программе работу - указать ей кусок строки, содержащейся обычно в "исходящих" линках центрального узла. Обычно это команды скрипта, что-нибудь типа "cj_out.php?url=".

А ФОТКИ ЧЬИ?

Теперь - точно твои будут. Выбирай себе любую прогу по вкусу - они все очень неплохи в работе - и забудь про надоедливые баннеры, редиректы, поп-апы и прочие извращения владельцев веб-сайтов. Помни, никто не должен мешать человеку приобщаться к прекрасному, а уж тем более пытаться на этом заработать :). 



КРАСИВО ЖИТЬ НЕЗАПРЕТИШЬ

Разговор об изменении внешнего вида Windows XP мы начали несколько месяцев назад. Дело было в сентябре. Тогда мы неплохо поковырялись во внутренностях операционной системы и выяснили, что такое стили оформления, как они работают и из чего состоят. Заодно мы влезли в стандартную XP'шную тему обычным редактором ресурсов и кое-что там поменяли. Увы, установить полный контроль над интерфейсом ОС нам в тот раз не удалось — сказало отсутствие инструментов, специально предназначенных для этого дела. Но сегодня XP'шка от нас не уйдет — я подготовил полный набор правильного софта, с помощью которого можно управляться не только со стилями оформления, но и с экраном входа пользователей, и с загрузочными заставками.

СЕРЬЕЗНЫЙ МОДИНГ XP'ШНОГО ИНТЕРФЕЙСА

ПОДГОТОВКА К ОПЕРАЦИИ

Думаю, ты понимаешь, что глупо затевать что-либо, имея в распоряжении лишь две стандартные XP'шные темы. Поэтому, прежде чем приступать к активным действиям, убедись, что у тебя хватает расходных материалов. Если ты купил журнал с диском — нет проблем, на нашем CD уже выложено все необходимое. Если нет — что ж, топай на сайт www.themexp.org. Там ты найдешь

не только готовые темы, но и обои для рабочего стола, а также logins-оболочки входа в систему и boot-screen'ы, которые нам понадобятся позднее.

Большинство скачанных отсюда стилей оформления потребуют наличия на твоей машине или пропатченной версии файла `uxtheme.dll`, или пакета Style XP от компании

TGTsoft (www.tgtsoft.com). Лучше, если у тебя есть и то и другое.

STYLE XP В ДЕЙСТВИИ

На момент написания этих строк, на сайте была доступна 3 бетка второй версии этой проги. В новой версии сразу же бросается в глаза наличие русского языка и множество свежих примочек. Наконец-то появилась полноценная поддержка экранов входа пользователей (пункт меню Загрузчики) и загрузочных заставок (Boot-screens). А инструменты из раздела Icon позволят тебе легко изменить любую системную иконку. Еще одна новая фишка, которая появилась во второй версии — установка прозрачности панели задач и меню запуска. Все это сопровождается порцией настроек, которых не много, но для начала вполне достаточно.

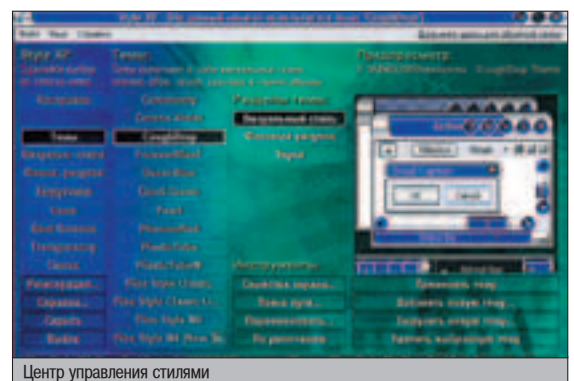
Одна проблема. Если ты решил качать вторую версию, то приготовься — весит эта зараза почти 13 метров. Кроме того, хотя я точно помню,

что кликал по ссылке Full Install (for new users), прога при запуске пожаловалась на отсутствие Style XP v 1.0. Пришлось мне скачивать и эту версию тоже. Впрочем, думаю, этот баг скоро поправят.

Тем не менее, вторую Style XP качать, несомненно, стоит — она включает в себя несколько очень приятных тем. Ты найдешь их в разделе Темы. Напомню, что для установки в систему нового стиля оформления интерфейса, скачанного с сайта ThemeXP.org, необходимо всего лишь скопировать содержимое архива в папку `C:\WINDOWS\Resources\Themes`.



- ▲ Style XP (-13 Мб)
www.tgtsoft.com
- ▲ StyleBuilder (2783 Кб)
www.tgtsoft.com
- ▲ UxTheme Utilz (16 Кб)
www.tgtsoft.com
- ▲ UXTheme Multi-Patcher (359 Кб)
www.lightstar1.com/install.htm
- ▲ Boot Editor (598 Кб)
www.belchfire.net/~userxp
- ▲ LogonUI & Boot Randomizer (693 Кб)
www.belchfire.net/~userxp
- ▲ LogonStudio (1859 Кб)
www.stardock.com/products/logonstudio
- ▲ Restorator (1326 Кб)
www.bome.com/Restorator



ЗАМЕНА СИСТЕМНЫХ ФАЙЛОВ



Если у тебя будут проблемы с перезаписью файла (например, к нему нет доступа), то поможет один из следующих вариантов:

1. Перегрузиться в безопасный режим - при старте компьютера нажимать F8 для вызова меню выбора загрузки и выбрать Безопасный режим, в котором и сделать то, что требуется.
2. Перезагрузиться в другие окна (если у тебя установлены две версии Windows) и заменить файл оттуда. Если вторые окна из серии 9x, а XP поставлен на NTFS, то понадобится спецутилита для 9x, чтобы можно было увидеть продвинутую файловую систему NTFS.
3. Если XP стоит на FAT, то можно загрузиться с дискеты и в DOS-режиме заменить файл.
4. Запустить установку XP, но при перезагрузке выбрать не установку, а перейти в консоль, где работают основные команды DOS, в том числе и команда копирования.

Помни, приятель, изменяя системные файлы своей операционки, ты вступаешь на опасный путь. Неподходящий патч, кривая библиотека - и система может просто-напросто рухнуть! Поэтому **ОБЯЗАТЕЛЬНО** подготовь загрузочную дискету и скопируй в надежное место оригинальные версии всех файлов, которые ты захочешь изменить.

АЛЬТЕРНАТИВА?

В принципе, без Style XP можно запросто обойтись. Это всего-навсего удобная обложка для безопасного управления различными составляющими интерфейса операционной системы. Но если ты не хочешь совать еще одну иконку в системный трей, то можешь только обновить файл uxtheme.dll для своей версии XP. Сделать это можно с помощью утилиты UxTheme Util, взятой с сайта той же компании TGTsoft из раздела Download. Если тебе повезет, она пропатчит твой uxtheme.dll так, что любые темы на твоей машине будут запускаться без дополнительного софта. Одна беда, Style XP - прог-

рамма шароварная, и ее разработчики не дураки, поэтому UxTheme Util не обновлялась уже давно.

Если у тебя XP с сервис-паком, то указанная утилита может не подойти. Я-то пропатчился без проблем, но вот, к примеру, M.J.Ash'у пришлось воспользоваться для этого дела альтернативным вариантом - программой UxTheme Multi-Patcher v 1.01 (www.lightstar1.com/install/Multi-Patcher_V1.01.zip). Если и это не поможет, значит, тебе придется вручную обновлять свой uxtheme.dll. Впрочем, это несложно - загляни на www.lightstar1.com/install.htm. Там ты найдешь все необходимые файлы и инструкции.



Если один патч не справился, попробуй другой

ВРУБАЕМСЯ В ТЕМУ

Так, будем считать, что ты уже научил свой компьютер работать с «инородными» темами. Что дальше? А дальше, приятель, тебя ждет разочарование. Отличных тем для Windows XP очень мало - есть масса хороших, каждая из которых обладает каким-нибудь недостатком. В одних некрасиво прорисована кнопка Пуск, в других - кнопки управления окнами, у третьей цветовая гамма слишком режет глаз. Можно не обращать на это внимания, можно тратить время в поисках лучшего, а можно просто взять и доработать наиболее понравившуюся тебе тему. Думаешь, это сложно? Если под рукой есть программа StyleBuilder (www.tgtsoft.com), то - нет.

Запусти программу и создай для начала новый проект. Ты сразу увидишь, что прога проста как три копейки. В главном окне слева можно наблюдать панель с рисунками различных наборов элементов управления. Выбираешь набор - в основном окне появляется дерево со списком элементов и их графическое представление.

Выделяешь какой-нибудь компонент - справа внизу появляется окно с тремя вкладками: Properties, Zoom и Colorize. Все просто. К примеру, вкладка Colorize позволяет изменять цвет и регулировать яркость с помощью ползунков. Результат сразу же отображается на экране. А если щелкнуть по какому-либо графическому элементу правой кнопкой и в появившемся меню выбрать пункт Edit или Edit With, то этот элемент откроется для редактирования в твоем любимом графическом редакторе. Короче говоря, разберешься.

Однако новый проект - это слишком круто. Нарисовать с нуля новую тему лично я не смогу. Но вот отредактировать на свой вкус уже существующую - запросто (пункт Import .msstyles file в меню File). Любый готовый стиль оформления я могу извратить до такой степени, что родная мама (папа) не узнает. А если серьезно, то самый правильный подход заключается в конструировании своей собственной темы из наиболее удачных элементов чужих творений. Получается и быстро, и качественно.

Чтобы проверить свою тему, необходимо выбрать в меню Tools пункт Test System Style. Когда все будет готово, в меню Actions надо кликнуть по Compile или Compile and Apply (если хочешь сразу и скомпилировать, и установить).



Анатомия стиля в программе StyleBuilder



После патча файла uxtheme.dll, окна могут запросить восстановления и инсталляционный диск. Ни в коем случае не давай им возможность восстановить библиотеку. На все запросы твердо отвечай: «Cancel», «Отмена» и «Да пошел ты...». Именно поэтому при патче в твоём драйве не должно быть диска с установочным CD, иначе ты не успеешь и мякнуть, как окна все вернут в исходное состояние.



Впустим в Окна немного праздника...

КОГО ТЫ ГРУЗИШЬ, СЫНОК?

Скажи, друг, тебе еще не надоел стандартный экран загрузки Windows? Ну тот, который появляется на начальном этапе загрузки системы — с логотипом Windows XP и бегающей полоской-индикатором. Посмотри на врезку с подборкой нескольких хороших boot-screen'ов и попробуй сказать, что тебе не хотелось бы видеть на своем экране что-то подобное. Все равно не поверю!

Для создания и установки загрузочных заставок лучше всего использовать программу Boot Editor. Ее домашняя страница находится на www.belchfire.net/~userxp. Установки программа не требует, необходимо лишь разархивировать скачанный архив в отдельную директорию.

Перечитай врезку «Замена системных файлов и ее последствия». Сглотни. На всякий случай сделай резервную копию файла `windows\system32\ntoskrnl.exe` и только после этого запускай Boot Editor. Освоение программы обычно проходит без проблем. Создаешь новый проект, а потом заменяешь в нем элемент за элементом. Готовый файл создается нажатием на Make. Клик по Test позволит тебе прописать созданный файл в `boot.ini` (перезагрузи, выбери при загрузке OS for testing new boot screen, и ты увидишь результаты своих усилий). В дальнейшем, если потребуется, имеющийся `boot.ini` можно будет поправить и ручками — чтобы на этапе загрузки ничего выбирать не приходилось.

Если файлы, создаваемые Boot Editor'ом, будут криво работать в твоей системе, придется воспользоваться услугами редактора ресурсов. Открой в нем копию файла `ntoskrnl.exe` и правь все, что тебе вздумается, в разделе Bitmap. Наиболее интересная картинка находится в ресурсе под номером 5. Это логотип Windows, который нужно уничтожить первым же делом. Затем пере-

пиши отредактированный файл `ntoskrnl.exe` на место оригинального.

Увы, то, что Boot Editor проверяет автоматически, в редакторе ресурсов придется делать самому. При редактировании необходимо учесть, что палитра ограничена 256 цветами, а менять размеры картинок не стоит, иначе комп может и не стартовать. Если у тебя установлена только одна ОС, то пользуйся редактором аккуратно, потому что восстановить первоначальный файл будет проблематично (см. врезку «Замена системных файлов» :)). Если осей две, то это уже проще. Если что-то пойдет не так, то перезагрузись в рабочую систему и через нее возвращайся в «дохлую» ось ее родной `ntoskrnl.exe`.

ПРОВЕРЬ МЕНЯ НА ПОГИН

Последнее, что нам осталось отредактировать — окно выбора пользователя. За это отвечает файл `windows\system32\logonui.exe`. Сделай его копию в той же директории, но с другим именем, например `logonui1.exe`. Теперь открой копию в редакторе ресурсов и можешь переделывать все картинки в разделе Bitmap.

Почему не надо издеваться над оригинальным файлом? Ты, конечно, можешь попробовать, но после перезагрузки Windows все изменения исчезнут. Я несколько раз пытался заставить систему съесть мой вариант, но она категорически отказывалась и все время возвращала на место родной `logonui.exe`. Тогда я сделал копию этого файла, изменил ее, полез в реестр по адресу `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` и исправил параметр `UIHost`, прописав туда имя отредактированного файла. И XP'шка купилась и стала подхватывать альтернативные версии `logonui`'ов.

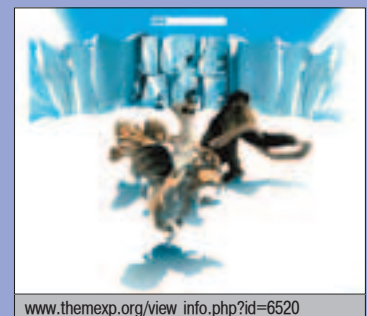
Но, вижу, лицо у тебя не слишком веселое? Что, не нравится редактировать экран входа пользователей в редакторе ресурсов? Логично. Ладно, качай с [## ЭКРАНЫ ЗАГРУЗКИ СИСТЕМЫ](http://www.stardock.com/prod-</p>
</div>
<div data-bbox=)

Pirated Edition III (2249 K6)



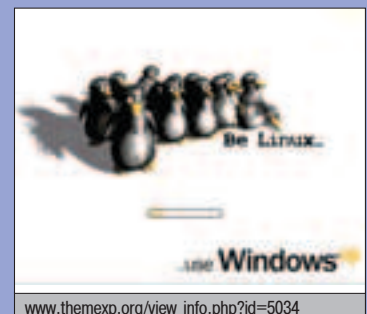
www.themexp.org/view_info.php?id=2854

Ice Age (2459 K6)



www.themexp.org/view_info.php?id=6520

Linux (2155 K6)



www.themexp.org/view_info.php?id=5034

Все boot screen'ы (как и весь упомянутый в статье софт) выложены на нашем диске. Каждый дистрибутив содержит несколько версий `ntoskrnl.exe` (для Windows XP с сервис-паком и без) и подробную инструкцию по установке (на английском). Однако в большинстве случаев внедрение нужного загрузчика в систему стоит поручить соответствующему софту (Boot Editor'у или LogonUI & Boot Randomizer'у) — меньше вероятности сделать что-то не то.



▲ Зачем нужно заменять `ixtheme.dll`? Неужели темы, разбросанные по инету, сильно отличаются от оригинальных? А может, пропатченная библиотека дает какие-то новые возможности? Да ничего подобного! В стандартном `ixtheme.dll` меня заинтересовало лишь одно — защита, не позволяющая использовать не MS темы. В пропатченном файле этой защиты нет. Судя по всему, MS решил просто срубить деньги с производителей тем, да только добрые дядьки сломали их планы вместе с библиотекой `ixtheme.dll`.

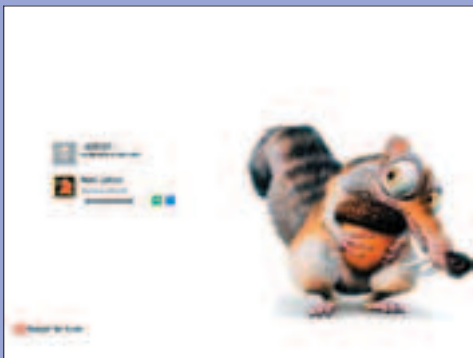
ОКНА ВЫБОРА ПОЛЬЗОВАТЕЛЯ

Linux suck XP (947 Kб)



www.themexp.org/view_info.php?id=16827

Scrat (531 Kб)



www.themexp.org/view_info.php?id=20605

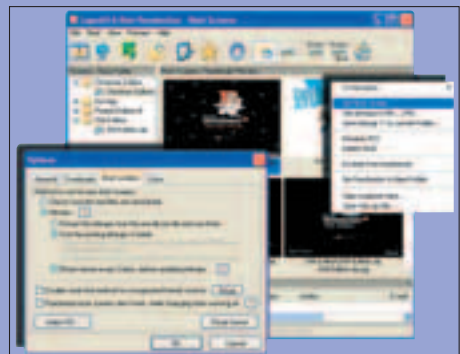
Linux Fly (527 Kб)



www.themexp.org/view_info.php?id=20605

МЕНЕДЖЕР LOGIN'ОВ И BOOTSCREEN'ОВ

Многие пользователи устанавливают программу Style XP только ради того, чтобы при каждом запуске системы у них происходило автоматическое изменение окна приветствия, загрузочного экрана и темы. Однако согласись, что менять каждый раз стиль оформления Windows довольно глупо. Все-таки нам с тобой работать надо, а не разбираться в том, какая из красных круглых кнопок делает то, за что в прошлый раз отвечала зеленая квадратная. Нет, темы нужно подгонять под себя и использовать постоянно. А вот вид окна приветствия или загрузочного экрана и в самом деле неплохо было бы разнообразить. Но держать только для этого Style XP – явный перебор. Лучше сразу заменить этого монстра мелким бесплатным аналогом. Рекомендую воспользоваться утилитой LogonUI & Boot Randomizer, которую ты без труда найдешь на www.belchfire.net/~userxp. Главное – внимательно прочитай инструкции, которые прога показывает при первом запуске, и тогда общение с этой софтиной не вызовет у тебя никаких затруднений.



О, Windows XP! С тобой каждый раз по-разному!



Привет! А ты, собственно, кто?

ucts/logonstudio прогу LogonStudio. Утилита эта полезная и приятная. С ее помощью можно как мутить свои собственные logons'ы, так и редактировать уже существующие. Есть, правда, одна хитрость – экраны входа пользователей прога сохраняет в своем собственном формате. Это, блин, такая хитрость, на которую корпорация Stardock пошла, чтобы привязать юзеров к своему продукту. Но если как следует почесать репу, то нетрудно догадаться, что раз система работает нормально, значит, правильный logonui.exe эта утилита все-таки создает. И точно! Делаем в проге новый экран входа, активируем его кнопкой Apply, лезем в каталог windows\system32 и видим там забав-

ный файл logonuiX.exe. Вот он-то для своей работы наличия на машине LogonStudio точно не требует. Его можно скопировать и с народом поделиться. Я это лично проверил.

ХОЧЕШЬ БЫТЬ КАК ВСЕ?

Забавно. Народ выпиливает отверстия в корпусах своих компьютеров, раскрашивает их, украшает светодиодами и думает, что это круто. В то же время модификацию интерфейса операционной системы многие по-прежнему считают бесполезным баловством. Чушь собачья! Мой системный блок стоит под столом, и мне наплевать, как он выглядит. А вот на XP'шные окошки мне приходится смотреть каждый день. Так почему бы не

сделать так, чтобы смотреть на них было действительно приятно? Тем более что подобная модификация не отнимает у тебя ни сил, ни средств, ни машинных ресурсов. А что ты на это скажешь, приятель?





ЗАУМНЫЙ ДОМ



В моем представлении, самой древней постройкой с первыми зачатками интеллекта была избушка Бабы Яги. Еще в те дремучие времена она требовала паролей-заклинание, чтобы обернуться на куриных ножках и пустить внутрь гостя. Много киселя утекло с тех пор. Сегодня об умных домах рассказывают такие небывальщины, что старуха в гробу переворачивается. Пришло время отдептить мух от котлет и разобраться, где правда, а где сущий домысел. На что способны умные дома, читай здесь и сейчас.

ВСЕ О СМЫШЛЕННОМ ЖИЛЬЕ

НА ИСХОДНУЮ

Не верь страшилкам об умном доме, который выстраивал хозяев по струнке, насаждая свои порядки. Это милое и послушное создание будет смотреть тебе в рот и в лепешку разобьется, чтобы угодить своему господину. Главное - установить полноценный контакт и взаимопонимание. Сердцем и печенкой любого умного дома является центральный контроллер, а золотым ключиком к "потрохам" - пульт управления. Не очередной редкий экземпляр в коллекцию дистанционок за диваном, а настоящий командный пункт для отдачи приказов и распоряжений новой электронной домоправительнице.

СПУШАЮ И ПОВИНУЮСЬ

Существует большой выбор рупоров для озвучивания самых невероятных нужд и фантазий. Кнопочная панель - скромная дань прошлому. Переключатели и тумблерочки со световой индикацией наглядно информируют о текущем состоянии приборов. Для связи с последними используется радиоканал. Клац-клац, и готово. В программируемых сенсорных панелях применяются цветные фотографии реальных комнат и девайсов. На

такой дисплей удобно вывести картинку с видеокамеры наблюдения. Когда настенная панель не востребована, она автоматически маскируется под картинку из Третьяковки. Мобильный вариант пульта управления - переносная панель, либо универсальная дистанционка на IR или радиочастотах. Размеры

устройства могут варьироваться от брелка до "ядерного чемоданчика". После аккуратной настройки на тембр голоса, если нет дефектов фикции, можно перейти на устный диалог с умным домом. Правда, иногда смартхаус будет выпендриваться и просить повторить. Кто ж не любит, чтобы его умоляли! Дать разнарядку из другого города удобнее всего по телефону. О результатах дом рапортует голосом в трубку или высылает сообщение на мобильник. Управление с



Переносная сенсорная панель управления

компьютера и через интернет в представлении не нуждается. Как правило, для каждого умного дома разрабатывается своя компьютерная программа с учетом уровня IQ жильцов.

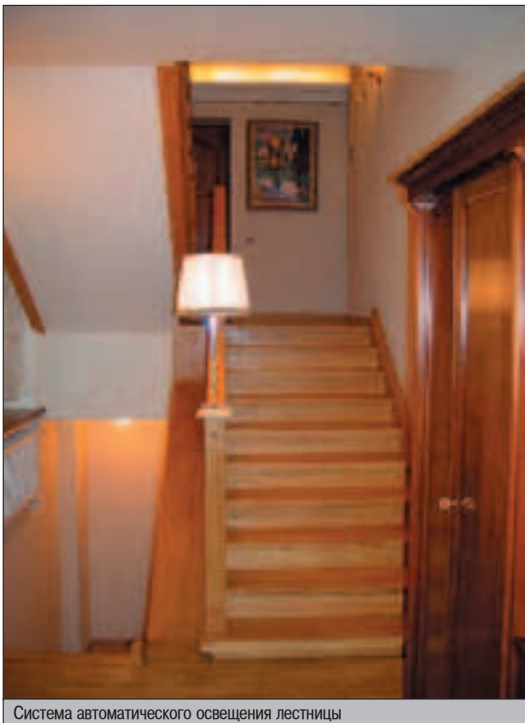
При большом желании и настойчивости любой из пультов управления позволяет добиться того, чтобы избушка понимала тебя даже не с полуслова - с полувздоха. А уж разнообразию трюков и фокусов в арсенале умного дома позавидует сам старик Коперфильд.

ПОУЧИТЕЛЬНАЯ ИСТОРИЯ

В старой байке про заумный дом владелец заплатил большие деньги, чтобы свет включался по хлопку в ладоши. Система работала отменно, и герой не переставал хвастать ею перед гостями. Но весной у него началась аллергия с заложенным носом и постоянными "апчхи". Пребывание в четырех стенах превратилось для владельца в настоящую каторгу. Стоит чихнуть - свет загорается, чихнешь еще - гаснет. Лампочки включались и выключались сутки напролет. В конце концов, ему надоела эта светомузыка. Он выломал умную систему, и только после этого спокойно уснул.

ДА БУДЕТ СВЕТ!

Кому приятно вылезать из теплой постели только для того, чтобы выключить свет в прихожей? Того и гляди, на обратном пути чертыхнешься через мохнатую тушу на паласе. С пульта можно манипулировать светом в любой точке умного дома, не сходя с места. Миниатюрный рубильник позволяет разом включить все люстры в квартире либо зажечь одинокую неоновую лампу над рабочим столом. Приглушается освещение плавно, что заметно продлевает срок службы лампочек. Настоящие эстеты могут играть гаммой и создавать художественные переходы от теней к свету, объединяя светильники в группы и программируя сценарии. С помощью последних можно устроить настоящее представление, не уступающее лазерному шоу Ямагаты. Ко всему прочему, автома-



Система автоматического освещения лестницы

тика регулирует яркость освещения в зависимости от времени суток и времени года, погодных условий и просто интенсивности света, падающего из окна. Другими словами, ядерной зимой твоя каморка будет освещена особенно ярко.

Ночи сейчас длинные и темные. Кушать хоца, а пересчитывать лбом все двери по дороге к еде, прямо скажем, неохота. В умном доме рядовой набег на холодильник превращается в настоящее удовольствие. Смартхаус выстилает "дорогу жизни" мягким светом ночников. Подтягивая семейные трусы в лучах света, ты чувствуешь себя звездой Голливуда. Если не дает покоя история о черной-черной руке, можно сделать так, чтобы свет сопровождал тебя повсюду, например, при открывании двери в комнату и на лестничную площадку. Лампочки в коридоре будут загораться при первом твоём приближении, а через несколько секунд плавно гаснуть за спиной.

ПРОГНОЗ ПОГОДЫ

Погоду в умном доме делает интеллектуальная система климат-контроля. Наиболее совершенная в инженерном плане, она способна превратить смартхаус в настоящий райский уголок. Замечено, что бытовые девайсы в наших квартирах очень часто действуют разрозненно и только мешают друг другу, нещадно накручивая киловатты. Одновременно коптит камин и пытит вентилятор. Кондишн вступил в неравную схватку с чугунными батареями. В комнате то холодно, то жарко. Мокрая майка, распахнутая настезь форточка, сквозняки и, как результат, насморк, простуда.

Смартхаус согревается, охлаждается и обдувается по



Плазменная панель Multiroom с защитой от влаги. Джакузи с дистанционным подогревом воды. Умная система отопления, вентиляции и кондиционирования

уму. Главное, загадать наверняка, хочешь ты провести неделю на Средиземноморье или в арктической пустыне. Независимо от сезона, в любое время дня и ночи в комнате будут поддерживаться заданные температура воздуха и уровень влажности. Немаловажный момент для твоего винного погребка и коллекции Пикассо! Если выбор климата дается с трудом, можно полностью положиться на смартхаус. Умный дом самостоятельно подбирает оптимальный для твоего распорядка дня режим. К ночи температура понизится, будет проветрена комната и созданы комфортные условия для сна. Перед утренней побудкой кондиционер вытянет все ночные запахи, в спальне потеплеет. Готовиться к приходу хозяев с работы умный дом начинает по таймеру или после специальной команды. В последнее время устройства дистанционного управления встраиваются в санвизоры автомобилей, что позволяет включить отопление и наполнить горячую ванну, находясь в нескольких кварталах от дома. В отсутствие в квартире живой души осуществляется переход в энергосберегающий "блокадный" режим. Чтобы не пришлось реанимировать оочневшего лентяя-кота, предусмотрительно привяжи к его хвосту пустую консервную банку.

И ШВЕЦ, И ЖНЕЦ

Умный дом - это пожарник, сантехник, электрик и еще десять специалистов в одном лице. На постоянном контроле у смартхауса напряжение в электросети, пожаробезопасность и бесперебойность работы всех систем коммуникаций. При одном подозрении на утечку воды или газа перекрываются краны, и объявляется аврал. Дом телеграфирует в сервисную службу о поломке с перечнем необходимого оборудования для замены. Без слаженной работы аварийных систем опутанный паутиной коммуникаций и напичканный дорогой электроникой умный дом напоминал бы настоящую пороховую бочку. Еще смартхаус никогда не забывает полить кактусы и регулярно кормит всех троглодитов, которых ты тащишь к себе домой.

ОДИН ДОМА

На случай, когда хозяева в отъезде, у умного дома есть особый талант - создавать полную иллюзию жизни, отпугивая случайных ворюшек. По расписанию - для убедительности с небольшими отклонениями от графика - то в одной, то в другой комнате будет вклю-



www.ydom.ru/
www.x10.ru/
www.i-dom.ru/
www.intel-house.ru/
www.smarthome.com/

ИСТОРИЯ О ПАРОВОЗИКЕ

Бесплатную рекламу умным домам делают истории о богатеньких буратино с бредовыми фантазиями. Один такой товарищ пожелал, чтобы каждое утро его будил свисток игрушечного паровозика. В компании уже подготовились тянуть воздушную ветку к прикроватной тумбочке, но к счастью вовремя расстались с извращенцем еще на стадии обсуждения проекта.



В номере:

GBA RESISTANCE 2

А. Купер и тайная секта фанатов GBA возвращаются! В прошлый раз мы рассказывали вам о нестандартном железе для портативной приставки от Nintendo, сейчас же настал черед софта! Самодельные операционные системы, программы для просмотра текста и картинок, проигрыватели музыки и прочие интересные фишки ждут тех, кто осмелится рассматривать GBA как нечто большее, нежели обычная игровая консоль.

ARC THE LAD: THE TWILIGHT OF SPIRITS

Культовый RPG-сериал возвращается, и нацелен уже отнюдь не исключительно на хардкорных геймеров. Новый Arc the Lad может легко конкурировать с блокбастерами от Square Enix, но так ли хороша игра, как можно судить по ее скриншотам? Во что превратились пошаговые бои в духе тактических RPG? Ответы на все вопросы ждут вас в подробном обзоре игры.

DEUS EX: INVISIBLE WAR

Самый громкий киберпанковский проект на PC последних лет обзавелся сиквелом. Мрачный мир будущего, где человечество не мыслит жизни своей без имплантов, снова радует нас в новой Action/RPG, выходящей также и на консоли Xbox. Игра не может не оказаться хитом, а другие потенциально интересные вещи для PC попрятались по углам, маскируя это переносами дат релиза.

URU: AGES BEYOND MYST

Вы слышите мерную поступь? Шаги из потустороннего мира? Биение нездешнего сердца? Это идет ОН! Myst возвращается. Он изводил нас долгими часами, неделями, месяцами скитаний, пролетавших как одно мгновение. И вот теперь мы снова оказываемся во власти волшебной игры. Наш редакционный Миклухо-Маклай испоттал шесть каменных сапог в поисках счастья. Читайте наш репортаж!

НАСКОЛЬКО РЕАЛЬНО "ПОИМЕТЬ" ЧУЖОЙ УМНЫЙ ДОМ?

Недаром многие компании отговаривают своих клиентов от рискованной затеи управлять умным домом через интернет. Кроме опасности взлома системы защиты интернет-сервера, существует риск прослушивания беспроводных сетей стандарта Wi-Fi. Однако чаще владельцы умных домов становятся заложниками собственной безалаберности. Если настольная лампа начала произвольно включаться, скорее всего, сосед установил умную систему и тоже забыл сменить заводской пароль, либо использует тот же код устройства, что и ты.

чаться свет. Раздвинутся шторы, заиграет музыка, будут слышны записанные заранее голоса жильцов. В общем, настоящая вечеринка у Деда дома. Развлекая сам себя, смартхаус даже воду из сливного бачка может периодически спускать. Правда, выдавать танцующие тени в окна за гостей он не станет, но это уже совсем для параноиков. На нежданных визитеров, курочащих кнопку дверного звонка, умный дом предупреждающе рыкнет и залыет басистым лаем шестидесятикилограммового ротвейлера.

Кстати, о ротвейлерах. Как услужливый швейцар, смартхаус распахнет дверцу перед четвероногим членом семьи, если прицепить тому на ошейник радиобрелок. Для людей в качестве системы "свой-чужой" могут применяться самые разнообразные технологии аутентификации, включая пароли, токены, смарт-карты и биометрию. Если для хозяина умный дом разве что впредь не пойдет,

то к "трем заветным желаниям" чужаков он отнесется с прохладой. Многоуровневый доступ к управлению системой существенно ограничивает права остальных членов семьи и уж тем более - незваных гостей.

НА ГРАНИЦЕ

Умный дом денно и нощно стоит на страже своих границ. На подозрительный шум в кустах он реагирует включением сирены, дежурного освещения и передислокацией камеры наблюдения на место событий. Показ фильма в домашнем кинотеатре будет немедленно прерван. На экране появится изображение двух соседских кроликов, застигнутых на месте преступления. Если существует вероятность вторжения извне, умный дом заблокирует все окна и двери, после чего проинформирует о случившемся хозяина и милицию. Он будет упорно дозваниваться каждому абоненту, занесенному в телефонную книгу, а при ответе воспроизведет экстренное голосовое сообщение. Сигнал тревоги может быть передан на пейджер или на мобильный телефон. Перестань оглядываться по сторонам! Периметральный контроль автоматически устанавливается изнутри, как только за тобой захлопнулась входная дверь.

Не исключено, что однажды преступный элемент сумеет втереться в доверие хозяина и всеми правдами и неправдами проникнет внутрь. На этот случай в умном доме есть тревожная кнопка, как у кассиров в банке. Помещать ее рекомендуют в самых непредсказуемых местах - например, в холодильнике или за унитазом - таким образом, чтобы в случае опасности можно было незаметно подать сигнал SOS.

МУЛЬТИРУМ

Жизнь в смартхаусе никогда не бывает скучной, потому что сопровождается музыкой и видео. Нужно вспомнить, что в.bestолковых домах лучшая и передовая техника обычно складывается в гостиной. По остальным ком-



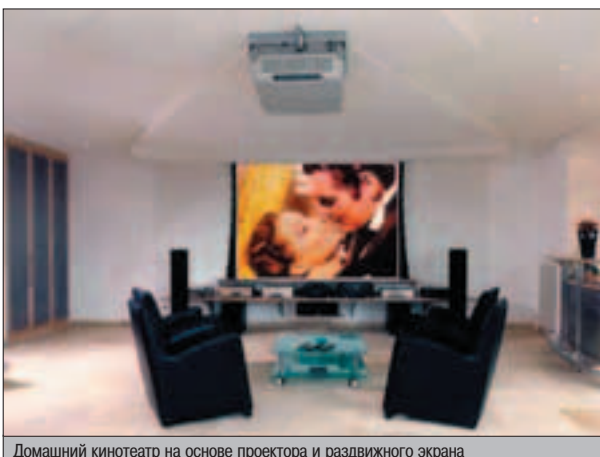
Дверной замок умного дома с аутентификацией по отпечатку пальца и PIN-коду

МОЖНО ЛИ СТАТЬ ЗАПОЖНИКОМ УМНОГО ДОМА?

Завязывая смотреть ужастики о домах-убийцах, которые наполняют ванну кипятком и держат хозяев в заточении. Вообще говоря, чем дороже умный дом, тем он безопаснее. Если сэкономить на аварийной системе и резервном питании, можно долго дожидаться, когда дадут электричество. Теоретически при несостоятельности системы и выходе из строя единственного центрального процессора умный дом может стать неуправляемым.



Система Multiroom. Акустическая система встроена в потолок и стены у камина



Домашний кинотеатр на основе проектора и раздвижного экрана

натам распахивают ее неказистых предшественников. Проблемы равномерного распространения звука по помещению это не решает. А есть в доме места, где технике вообще противопоказано находиться - бассейн, ванная комната, кухня, детская. С ростом числа комнат вопросов становится только больше. Самой эффективной системой смартхауса, которой кичится даже мелкомягкий Билли, является мультирум. Говоря проще, умный дом позволяет подавать звук и картинку в любое помещение, где установлены телевизоры, мониторы, сенсорные панели и акустические системы. При этом вся hi-fi и hi-end техника размещается в аппаратной.

Нашпиговав чейнджер дисками по самое не хочу, можно одновременно заказать регги в тренажерный зал и "Соловья" Алябьева в ванную, мультики в детскую и страстную Эммануэль в спальню. Акустические системы встраиваются в стены и потолок еще на стадии отделки помещения. Дизайнеры и архитекторы тщательно маскируют колонки так, чтобы они не портили интерьер и не отъедали свободное пространство комнат. В бассейне устанавливают плазменные экраны и акустические системы, которые выдерживают работу в условиях высокой влажности. Вдоль дорожки к дому - специальные колонки в виде валунов и садовых гномиков. Мультирум - это самая дорогостоящая начинка умного дома, на которую может приходиться до 3/4 его стоимости.

Обо всех любопытных возможностях мультирума быстро не рассказать. Например, ме-

лодия может, не прерываясь, сопровождать тебя при переходе из одной комнаты в другую. Если позвонят в дверь, смартхаус автоматически убавит громкость. Не успеешь ты раскинуться в кресле с попкорном в руках, как в комнате потухнет свет, задвинутся шторы на окнах, развернется киноэкран. Умный дом гнусавым голосом объявит

название блокбастера и пожелает тебе приятного просмотра. Упоминания заслуживает система интеркома для речевого общения между разными комнатами: "Мам, ты меня звала?" Ну и чтобы ты оставался в курсе всей этой напряженной домашней жизни, смартхаус постоянно напоминает о себе через динамики, оповещая о происходящих и грядущих событиях.

ЗАЙМИСЬ УМНЫМ ДОМОМ

Мой тебе совет, займись своим домом, не откладывая на потом. Сколько стоит это удовольствие? Если брать по-настоящему круто, то тысячи и даже миллионы вечнозеленых. По минимуму, достаточно разориться на полтинник и приобрести радиоприемник-трансивер с брелком дистанционного управления. После этого разживаешься одним-двумя модулями в месяц, и горя не знаешь. Интернет кишит инструкциями на тему, что и в какой последовательности лучше покупать. Пожалуй, наиболее простой и ориентированный на конечного потребителя-чайника стандарт - это X10. Начни с выключателей и умных лампочек, радиодликателя пульта. Затем нужно копить на USB-интерфейс, датчик движения и видеосендер. Друзьям и знакомым объяви, что отныне в подарок принимаешь только комплектующие умного дома. Уровень IQ твоей лачуги будет расти от месяца к месяцу. Но не забывай, что душа требует комфорта, поэтому остановиться будет очень непросто. 

САМЫЙ УМНЫЙ ДОМ ПЛАНЕТЫ



Умный дом Гейтса с виду ничем не примечателен

Дом Билла Гейтса на берегу озера Вашингтон был достроен осенью 1997 года и оценивается примерно в 55 миллионов долларов. В смартхаусе площадью 3700 квадратных метров расположены 36 комнат, из которых 24 - санузлы, а также кинотеатр и бассейн. Большая часть дома находится под землей. Солнечный свет в бункер Гейтса попадает благодаря кабелю из оптоволокна общей протяженностью 84 километра. Каждый, кто входит в дом, получает булавку с микропередатчиком. Сенсорные устройства регистрируют уникальный идентификационный номер гостя и его местонахождение, предоставляя необходимые услуги по первому требованию. Более сотни компьютеров объединены в сеть, чтобы следить за каждым шагом домашних и постояльцев. Смартхаус настраивает телевизор на любимые телеканалы, озвучивает почту и выполняет десятки других прихотей Гейтсов. Ночью по коридорам гуляет световая волна, сопровождающая одинокую фигуру человека в очках. Специальная система подавляет звуки таким образом, что не слышно ни шороха. Главной достопримечательностью жилища сам Билли считает систему сопровождения звуком и огромные плазменные панели, которыми оборудованы все стены. Этот умный дом описан в книге Гейтса "Дорога в будущее". К ней прилагается компакт-диск с интерактивным путеводителем по дому. В то же время большинство владельцев смартхаусов сохраняют инкогнито, поэтому продолжить список самых умных домов планеты затруднительно. Выставочные прототипы не в счет.



НАСК-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывая 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 спотать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).

Q: Существуют ли публичные сканеры безопасности, как ISS или Retina, доступные с WWW?

A: Существуют, причем в достаточном количестве. Правда, многие из них слабы по своему набору опций и уступают тем же ISS и Retina. Например, www.hackerwhacker.com - сканер портов, конкретных сервисов, самбы и т.д. www.grc.com - никаких премудростей, как и никакого поля для фантазии сканирующего :(. privacy.net/analyze - показывает, что ты передаешь владельцам сайтов при серфинге. www.secure-me.net - тормозной порт-сканер. https://secure1.security-space.com/smysecure/basic_index.html#run - за прохождение регистрации дают возможность поюзать web-базированный Nessus сканер. scan.sygate.com - примитивный сканер, с возможностью проверки NetBIOS на вшивость.

Q: Как правильно сканировать и отыскивать роутеры в Сети?

A: Существуют два основных подхода, точнее два основных критерия поиска. Первый вариант. Большинство железяных (hardware) роутеров управляются некой операционной системой, которая, скорее всего, распознается в процессе OS-fingerprinting'a. Например, у Cisco это будет Cisco IOS. Софтверные же роутеры таким образом по своему обыкновению не распознаются :(. Второй способ - порт-определение. Это когда роутеры распознаются по 23 порту - telnet'ом. Правда, большинство систем закрывают telnet-доступ для общения с *nix'ом, предпочитая более безопасный SSH2. Так что велик шанс отыскать такой вот роутер. А вообще, предлагаю воспользоваться целым поисковым комплексом под названием Cisco Scanner 1.0.2. Берется он с www.securityfocus.com/tools/817. Несмотря на объем в 1,65 Мб, он имеет всего лишь одну опцию скана Cisco по дефолтовой учетной записи cisco. Софтина давненько не обновлялась (более 3 лет), так что при столь примитивном скане, можно заюзать и обыкновенный nmap, задав 23 порт для чеканья.

Q: Правда, что появился вирь, поражающий банкоматы? Лавэ еще никому не обломилось?

A: Такой вирь появился не сегодня. Еще год назад целых 13 тысяч банкоматских тачек были опрокинуты червем Slammer. Тогда владелец сети - Bank of America - пострадал исключительно технически (правда, ушли в молоко некоторые проценты с непроизведенных транзакций). Самый последний инцидент произошел с фирмой Diebold (www.diebold.com/solutions/atms/default.htm), производящей банкоматы (АТМ). Червем Nachi была поражена целая серия машин, находящихся под контролем ОС Windows XP. В этом случае был заюзан баг RPC DCOM, которому на тот момент стукнул аж целый месяц. В общем, не поспешили банкометчики с заплатами! Правда, информации о хищении денежных средств не поступало. Был лишь огромный трафик, шедший с зараженных банкоматов к другим участникам сети (в том числе, остальным банкоматам Diebold). Банковскими системами безопасности этот трафик был воспринят как атака злоумышленника. После чего произошло автоматическое отключение многих других банкоматов. Microsoft, главный виновник торжества, это событие никак не прокомментировал. Сейчас Diebold встраивает фаерволы в большинство своих АТМ.

Q: Как мне залочить систему в Линухе?

A: Имеется в виду убрать доступ к консоли, когда тебя нет на рабочем месте, чтобы какой-нибудь Хакершицев не воспользовался этим себе во благо. Не напрасно Linux считают секьюрной системой: тут можно закрыть под ключ все и вся. Так X-винда (любой ее терминал) запирается магическим хлоск. После чего xterm закрывается, и для продолжения его работы необходимо будет ввести пароль. Если же надо закрыть саму консоль, то здесь на помощь приходит утилита vlock. Она может залочить какую-нибудь определенную виртуальную консоль (vty), а может и все сразу. Где берутся эти программы: в основной массе они идут со всеми Linux-дистрибутивами. Также стоит помнить, что локи - это не панацея от всех бед, т.к. ключ снимается обыкновенной перезагрузкой системы. Если же безопасность системы настроена с сидалищного места, то никто не помешает проникнуть в "залоченную" машину с соседнего компа.

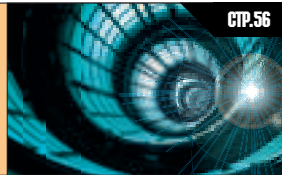
Q: Заколебали выскакивающие окошки на вarezных сайтах и на порнухе! Чем бы их почикать?

A: Прислушайся к своему вопросу - в нем содержатся ключевые слова для поиска "@pop-up killer". Задай их Google'у, и в ответ получишь ссылки на десятки нужных программ. Я же для решения этой проблемы написал в свою систему программу Adsgone 2004, которая без определенного лекарства соглашается трудиться лишь 3 недели. Есть и другие, более крепко-сговорчивые штуковины. Например, CoffeeCup PopUp Blocker 3.5, Alto Block All и специально для любителей фришного софта - Emerald PopStop. Все перечисленное добро лежит на tucows.com и имеет самый высокий рейтинг. Кстати, на tucows.com также лежит несколько устаревшая версия Adsgone, для которой выложен пурген на astalavista.box.sk :). Иногда очень удобные модули по борьбе с рекламой находятся в самом чреве громоздких фаерволов :(. Так что стоит ли ставить целый охранный комплекс, чтобы убить одно-два рорир-окошка - дело лично твое.

СТР.52

РАЗОБЛАЧЕНИЕ ХАКЕРА

Сказка о том, как хакер ломал сервера в Сети и как его вычислял админ.



СТР.56

ВЫБЕРИ СВОЙ ТУННЕЛЬ

Учимся грамотно создавать сетевые туннели для шифрования данных.



СТР.64

ПАКАЕМ И ЗАШИФРУЕМ

Эффективные средства паковки бинарных файлов в Windows.

**Q: В чем разница между алгоритмами шифрования Blowfish и AES?**

A: Каждый день ты слышишь, что от тебя шифруются по какому-нибудь очередному алгоритму. В чем тема шифрования - хрен догонишь! Для вундеркиндов даю линки на научное описание Blowfish и AES: www.schneier.com/blowfish.html и csrc.nist.gov/CryptoToolkit/aes/rijndael. Сами алгоритмы представляют собой блочные шифры. У AES блоки заданы по умолчанию равными 128 битам с ключами размером от 128 до 256 бит. AES - это SPN (Substitution Permutation Network, заменяемо-перестанавливаемая сеть). Blowfish также является алгоритмом блочного шифрования. Блоки могут иметь размер от 32 до 448 бит. 64 бита установлены по умолчанию. Как и AES, Blowfish содержит в своем фундаменте сетевой алгоритм, называемый Feistel. Также еще можно найти десятки других разновидностей алгоритмов, базирующихся на совершенно разных философиях шифрования. И не стоит забывать, что софт, основанный на различных алгоритмах шифрования, имеет свойство по разному подгружать железо. Сравнить потенциальное быстроедействие можно все на том же сайте Schneier'a.

Q: Хотел мальчика ресурсов поднять с накрукки баннеров. Чем бы лучше так крутануть из-под винды? Где поднять проксей для крутилки?

A: Кручу-верчу, много выиграть хочу ;) Бородатые и пузатые дядьки, успевшие отрастить мамоны с рекламных хищений, уже несколько лет пользуются своим собственным софтом, запускаемым с далеких много-мегабитных кололейшенов в Америке. Виртуальная же босота и прочая шпана пользуется Clicking Agent, получившим в простонародье имя СаСа. Я его описывал аж 4 года назад, так что странно, что у тебя его еще нет в хозяйстве... Демонстрашка, которая парой взмахов конечностями превращается в полноценную \$100 версию, доступна на сайте www.clickingagent.com. И как ты правильно заметил, для ее работы тебе потребуются проксы, причем целые тонны! Их можно самостоятельно собирать с бескрайних просторов инета, воспользовавшись, например, ProXYZ от того же производителя СаСа. Однако я для него лекарство не нашел... да и назвать этот софт оптимальным язык не поворачивается. А вообще, при определенной смекалке, птар гнется в бараний рог и превращается в самый быстрый и чистый сканер проксей. Если же тебе лень искать самому, а хочется разжиться готовым списком, то зайти на www.proxychecker.ru.

Q: Мой DHCP-сервер выдает мне IP 192.168.1.X. Почему мои клиенты иногда получают 192.168.0.X?

A: Чтобы ответить на этот вопрос, позволь мне более детально обрисовать полученную картину. Мы имеем NT-домен, где выдачей IP-адресов занимается NT4-машина. Здесь же находится вторая Win2003-тачка, установленная админом другого сегмента сети. На ней висит работающий DHCP-сервер, раздающий адреса в пространстве 192.168.0.0/24. Каким-то образом машины из NT4-пространства периодически обращаются к 2003 машине за искомым адресом, получая неправильный IP. Отсюда вывод: разделяй и властвуй! Это пример того, как важно грамотно сегментировать сетку.

Q: В чем суть нашумевшего бага DCOM RPC?

A: Суть состоит в том, что это устаревший сентябрьский баг (эмбрион был обнаружен аж в июле!). Однако долгий печальный опыт и наличие тысячи бажных, непропатченных лопухов и поныне не дают права молчать! В первую очередь запомним термины: Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) интерфейс. RPC - протокол, позволяющий запускать нужный код удаленно на определенных машинах. Сам DCOM интерфейс можно отыскать на задействованных RPC портах. При успешном эксплоитинге, атакующий может творить с компом все что угодно, как и обычный локальный пользователь. Т.е. устанавливать нужный софт, стирать и пополнять имеющуюся в системе инфу, создавать и удалять юзеров. Помимо переполнения буфера с последующим исполнением нужного кода, можно и просто вывести комп из строя. Но не все так печально - MS предельно быстро наколбасил патчи, так что end-user'у осталось лишь жмакнуть на свой любимый Windows Update. К тому же часть непатченных юзеров оказались вне опасности: при наличии фаервола, пусть даже стандартного виндозного, входящие соединения на RPC-порты (135, 139, 445, 593) были чаще всего заблокированы. А вообще уже выпущено множество эксплоитов по этой теме, как для атак с Win-машин, так и с "nix'ов. Отыскать все необходимое можно в Google'e по ключевым словам "DCOM RPC exploit". Грамотные обзоры решения проблемы есть у самого MS (www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp и www.microsoft.com/technet/treeview?url=/technet/security/bulletin/MS03-026.asp).

Q: Я пишу свой первый эксплоит. Какие будут пожелания?

A: Стандартное пожелание для всех писарей первых эксплоитов - осторожнее с зоной распространения написанной тулзы. Не забывай, что всегда есть горячие головы, которые, добыв софтинку, начинают злостный беспредел. Так что при поиске дополнительных материалов в Сети пользуйся философией "как писать безопасный софт", "как не допустить багов". Например, на www.linuxfocus.org/English/January2001/article182.shtml лежит целый цикл статей по безопасному коду "Как не насаждать дырок в безопасности при разработке софта", который можно легко переделать в "Как заюзать имеющийся баг в проге".

Мое же личное пожелание эксплоитеру - пиши изначально дырявый софт! Звучит парадоксально, но имея под рукой бажную софтинку, куда проще будет понять способ написания эксплоита. Задача вдвойне упрощается, если софтина написана тобой же, и ты хорошо знаешь основные блоки кода. Полученный опыт поможет тебе не допускать стандартных ошибок в своем будущем коде. Некоторые знающие люди также рекомендуют дизассемблировать коммерческий софт - для приобретения опыта "как же все это работает". Занятие, безусловно, муторное, но чреватое новым опытом :).

РАЗОБЛАЧЕНИЕ ХАКЕРА

Плюбой хакер ищет легкие пути для взлома сервера. Будь то сайт на фриварном хостинге или западный банк. Нередко, добившись своего, взломщик на минуту забывает о собственной защите, в результате чего его быстро разоблачает системный администратор. Админы тоже ведь не конченые дураки, и заслуженно получают свою зарплату.

Я хочу сказать, что далеко не всегда хакеру удается выйти сухим из воды. Атаки быстро вычисляются, если сервером рупит грамотный администратор. В доказательство своих слов хочу рассказать тебе историю о взломе российского хостинга www.ruhost.ru.

НАШУМВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

ПОСТАНОВКА ЗАДАЧИ

Начало истории банальное. Одному опытному хакеру предложили порутать крупный хостинг - заказчик хотел откушаться на показе баннеров. Взломщику же за успешную работу предлагали вполне солидные деньги.

Итак, взломщик зашел на сайт. Ничего интересного страница собой не представляла - простой html с данными о хостинговой компании. В конце текста прилагал-

ся e-mail адрес для контактов: root@ruhost.ru. Самый что ни на есть стандартный сайт. Включив поддержку проху-сервера в браузере, наш пионер еще немного побродил по страницам с целью выявления дырявых скриптов, но так ничего и не обнаружил.

Вторым шагом хакера было сканирование портов. Как всегда, взломщик делал это при помощи nmap (www.insecure.org/nmap/) с забугорного шелла. Сканер выдал список стандартных портов. В нем не было ничего лишнего: ftp, ssh, почта, web и еще парочка стандарт-

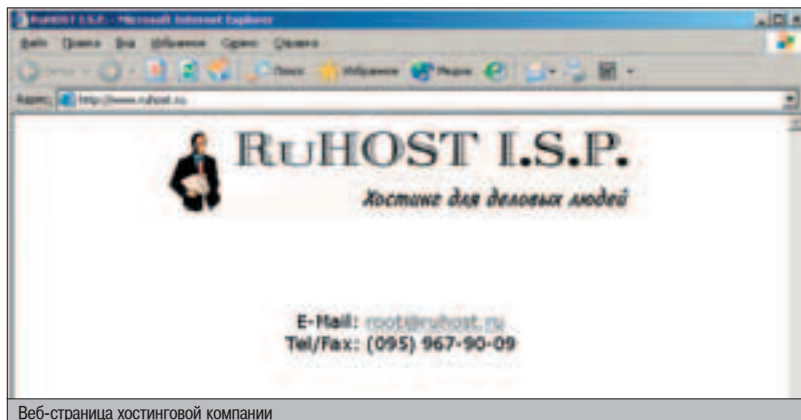
ных сервисов. Баннеры сервисов были правильные, софт своевременно обновлялся - администратор работал добросовестно.

РАЗГАДКА ПАРОЛЯ

Тогда ломатель сайтов решил пробить домен по whois-базе с целью добычи новой информации. Это можно сделать на странице www.nic.ru/whois/?ip=ip-address (ip-address - исследуемый айпишник). Так хакер узнал еще один e-mail адрес - owner@ruhost.ru, а также местонахождение сервера - площадка Ростелекома.

Если насчет первого адреса хакер был уверен, что это обычный алиас, то e-mail в базе указывал на реальный логин в системе. Учитывая то, что в качестве почтового сервера стоял sendmail, взломщик предположил наличие реального системного аккаунта "owner". Дело оставалось за малым - угадать пароль на почту.

Брутфорс хакер считал последним методом. Я не раз упоминал об этом, поэтому не буду заострять внимание на реализации этого способа. Просто скажу, что взломщик решил заюзать самопальный потоковый рор3-брутфорсер с забугорного шелла. Исходя из того, что администратор проживает в России, для брутфорса был выбран словарь русских слов, записанных в английской раск-



Веб-страница хостинговой компании

```

hell# nmap www.ruhost.ru
Starting nmap V. 3.10A/1949 ( www.insecure.org/nmap/ )
Interesting ports on ruhost1.ruhost.ru (213.59.0.86):
(The 1096 ports scanned but not shown below are in state: filtered)
Port      State  Service
21/tcp    open   ftp
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
106/tcp   open   pop3sw
110/tcp   open   pop3
113/tcp   open   auth
143/tcp   open   imap2
993/tcp   open   imapc

Nmap run completed -- 1 IP address (1 host up) scanned in 199.215 seconds
hell#

```

Список открытых портов на сервере

ладке. Именно такие пароли и любят наши доблестные админы :).

Хакер не ошибся. Через несколько часов брутфорсер разгадал пароль. Это было простое слово Flvbybcnhfnjh, что по-русски означает Администратор.

ПОКАПНЫЙ ВЗЛОМ

Наутро, посмотрев логи, злоумышленник сконнектился по ssh на сервер. Демон впустил хакера в систему, так как пароль действительно был подобран верно. Теперь следовало достать root-пароль и предоставить доступ заказчику. Что касается операционки, то на машине был установлен новый Alt Master 2.2. Ядро не поддавалось ptrace, и эксплоитов для этой системы еще не было. Пришлось действовать нестандартными путями.

Хакер открыл файл ~/.bash_history и прочитал команды администратора с целью обнаружить там пароль для root. Интуиция не подвела нашего героя: админ ошибся в написании команды "su", после чего следовал рут-пароль в plain-тексте. Это довольно типичная ошибка админов. Вообще, в .bash_history можно найти очень интересные команды :).

Напоследок хакер должен был создать какую-либо маскировку в системе, чтобы администратор не засек его пребывание. Наскоро был поставлен руткит, скрывающий файлы, а также написан сишник, запускающий /bin/bash с правами root (посредством suid-бита). Затем взломщик создал файл /var/adm/.profile и написал туда всего две строки:

```

/var/lib/modules/linux.so
exit

```

Естественно, что linux.so являлся бинарником, в котором был последовательный запуск чистилки логов и шелла через исполняемый файл Adore (packetstormsecurity.nl/groups/teso/adore-0.14.tar.gz).

```

root@ruhost1.ru:~# cat /var/adm/.profile
file

```

Профиль-файл пользователя adm

Затем хакер стер шелл у пользователя adm. Мало кто знает, что при отсутствии шелла язеру присваивается дефолтовый интерпретатор /bin/sh. Он обрабатывает файл ~/.profile, а в нашем случае там содержался запуск рутового /bin/bash. После завершения сеанса выполнялась команда exit.

```

root@ruhost1.ru:~# cat /var/adm/.profile
file

```

Рутовый пароль в .bash_history админа

ЧТО ВЫДАДО ХАКЕРА ПРИ ВЗЛОМЕ?

1. Хакер забыл изучить процессы, крутящиеся на машине. Непростительная оплошность, поскольку даже самый простой детектор атак может выдать взломщика.
2. Хакер не изучил syslog. Просмотр /etc/syslog.conf необходимо делать всегда, поскольку важная информация может высылаться как на e-mail, так и на консоль.
3. Хакер запалился при заходе на сайт собственным IP-адресом. Необходимо было сразу же принять меры по собственной безопасности.



неРС

Все о "других" компьютерах. То, что стоит у тебя под столом - лишь один из многочисленных видов современных компов. О том, какими системами пользуются настоящие профессионалы, как шла эволюция ПК и почему вымерли конкуренты IBM PC, что нас ждет завтра, читай в январском номере Спеца:

В номере:

- Целый раздел про Маки!
- 64-разрядные процессоры AMD и Intel
- Alpha-процессоры и системы на них
- Эволюция SPARC
- ZX-Spectrum: автобиография титана
- Нейрокомпьютер снаружи и изнутри
- Mini-ITX, Nano-ITX и изобретения, основанные на них

А еще целое море софта и инфы на диске!

Сетевой ковырятель позаботился и о чистке бинарных логов, интегрировав `linux.so` с чистилкой `vanish`. Почистив логи и установив пароль юзеру `adm`, хакер удалился из системы. Теперь ему оставалось сконтакиться с заказчиком и предоставить ему доступ на хостинг. Именно это и произошло бы, если бы не бдительность системного администратора.

РАЗБОР ПОПЕТОВ

Поздней ночью администратор хостинга (он же `owner`) решил зайти в систему. Внутренний голос подсказывал ему, что с сервером что-то не так :). Проверив таблицу процессов и поверхностно изучив логи, админ успокоился - вроде бы все на своих местах. Администратор вспомнил о недавно установленной `Tripwire` (`download.sourceforge.net/tripwire/tripwire-2.3.1-2.tar.gz`). Она уже несколько дней слала ночные отчеты на его мыло. Хакер же совсем не заметил эту IDS в процессах, поэтому не позаботился о чистке ее логов.

Неспешно пролистав отчет, администратор не нашел ничего аномального. Впрочем, хакер не предпринимал никаких действий в системе: пользователей не создавал, суйдных файлов тоже. Системщик уже хотел закрыть отчет и лечь спать, но обратил внимание на одну интересную деталь: файл `/etc/passwd` модифицировался в течение дня. Админ был уверен, что пользователей не создавал и не изменял их параметры, поэтому подобное явление подразумевало что-то неладное.

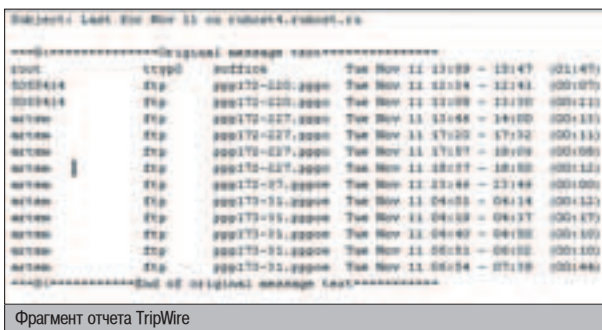
В системе было довольно много пользователей, и на первый взгляд уловить, что именно поменял хакер в файле, не представлялось возможным. Если бы не логи, администратор так и не узнал бы метод атаки хакера. Я упоминал, что взломщик вычистил все системные журналы, но не посмотрел настроенный `/etc/syslog.conf`. А в нем содержалась следующая строка:

```
.. root@home.ru
```

Таким образом, все логи слались на мыло админу. Это был почтовый ящик на другой

! Сменить дату на файл очень просто. В этом может помочь команда `touch` с параметром `-t`, после которого следует формат даты в виде `MMDDhhmm`. Хакер не должен забывать выполнять команду `touch -t 01010100 /etc/passwd` перед выходом из системы.

!!! Не стоит забывать, что все действия хакера противозаконны, поэтому статья приведена лишь в целях ознакомления и организации правильной защиты с вашей стороны. За применение этого материала в незаконных целях автор и редакция ответственности не несут.



машине, недоступной хакеру. Администратор быстро нашел нужный лог в почтовой базе и стал изучать текстовые записи. Там он узнал много интересного, например, что взломщик использовал логин `adm` в качестве входа.

ПОМАТЬ - НЕ СТРОИТЬ

Администратор набрал `"su - adm"` и получил рутный шелл. Это его очень удивило, т.к. в системе полностью отсутствовали сторонние суйдные файлы. Сначала он подумал, что хакер заюзал какую-нибудь багу в суйдном би-

ВОЗМОЖНОСТЬ ADORE

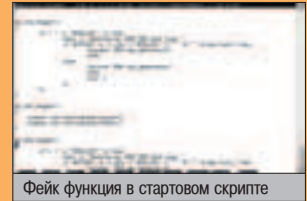
Об этом чудном рутките можно говорить часами. Его особенность в том, что через исполняемый файл `ava` можно выполнять команду из-под `root'a`. К примеру, чтобы вызвать шелл, нужно написать следующую строку:

```
ava e /bin/bash >/dev/null 2>&1
```

Дескрипторы перенаправляются в `/dev/null`, чтобы не светить лишние записи на консоль.

СТАРТОВЫЕ МОДУЛИ

Скрипты `Adore`, которые будут подгружаться при старте системы, хакер прописал в укромное место. Если бы он не запалил себя, админ вряд ли бы их нашел. Например, хорошим местом для их местоположения будет файл `/etc/init.d/ssh.d`.



нарнике и посредством нее вызывал `/bin/bash`. Но, опять же, контрольная сумма во всех бинарниках была сохранена (это подтверждал отчет `tripwire`). Заглянув в `Homedir` пользователя, системщик нашел файл `.history`. История показывала, что взломщик вызывал какой-то странный модуль `linux.so`, а затем команду `exit`.

И тут-то админ проверил наличие файла `/var/adm/.profile` и убедился в его скрытности. Он быстро вернул шелл `/dev/null` юзеру `adm` и занялся восстановлением системы. В его голове бегали мысли о заражении операционки руткитом: переустанавливать половину бинарников, а то и всю систему админу совсем не хотелось. Но после просмотра `/usr/lib/modules/linux.so`, администратор увидел наличие еще одного бинарного файла `/usr/bin/ava` (исполнительного файла от `Adore`). Теперь стало ясно, каким руткитом была заражена система. Тщательная проверка стартовых скриптов показала, что при запуске происходит инициализация модулей `system.o` и `cleanup.o` (главных модулей `Adore`). Их администратор поспешно удалил и отправил систему в ребут.

НАС РЕБУТ, А МЫ КРЕПЧАЕМ

После перезагрузки админ сгенерировал свежий отчет `tripwire`, который выдал ему весь список новых бинарных файлов. Среди них была чистилка логов `vanish`.

Администратор хотел вычислить IP-адрес взломщика, но это было невозможно, т.к. брутфорс пароля и логин на машину производился с левых бельгийских хостов. И тут в

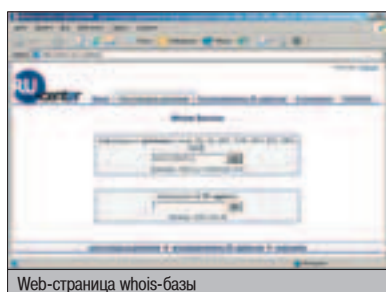
голове системщика возникла гениальная мысль: он знал, что злоумышленник атаковал систему по хосту `ruhost.ru`. На хост заходило очень мало людей, поэтому IP хакера вычислялся через `web`.

Админ быстро пролистал `access_log` для сайта `ruhost.ru` и нашел там несколько айпишников на текущий день. Два из них были бельгийскими, а третий - наш, советский ;) . Промежутком времени между логинами был невелик (сперва хакер забыл включить поддержку прокси-сервера, и зря). Сисадмин пробил адрес по базе и понял, что он принадлежит крупному московскому провайдеру.

ОТКРОЙТЕ, МИПЦИЯ!

Обратившись на адрес `abuse@provider.ru`, администратор отправил письмо с подробными логами взлома. Админ угадал практически все шаги хакера, восстановив подробный сценарий взлома сервера. Примерно через сутки пришел ответ от службы безопасности. В нем говорилось, что хакер был отключен от провайдерской локалки. Также у админа спросили, имеет ли он дальнейшие претензии к злоумышленнику. Подумав, системщик решил остановиться и не судиться с хакером. Он сам был отчасти виноват в происшедшем - не уделил должного внимания фаерволу.

Проведем финальную черту. Как видишь, администраторы не дураки, и малейшая оплошность хакера может выдать его с потрохами. Этой оплошностью стало посещение с реального IP-адреса сайта `www.ruhost.ru`. К тому же взломщик не заметил присутствие IDS и забыл проанализировать файл `syslog.conf`. Очевидно, в любом взломе есть свои недочеты, вопрос в другом: заметит ли их админ? В моем случае админ оказался активнее хакера.



ДОБРО ПОЖАЛОВАТЬ В ИНТЕРНЕТ!



Модемы серии OMNI 56K



OMNI 56K PRO



OMNI 56K DUO



OMNI 56K NEO



OMNI 56K UNO



OMNI 56K MINI



OMNI 56K PCI

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии



ВЫБЕРИ

сВОЙ ТУННЕЛЬ

0 Одним из способов реализации бесплатного интернета у любимого провайдера является туннелинг трафика. Это куда безопаснее, чем смена MAC и IP-адреса. Более того, твой провайдер будет сам виноват, что ты им попользовался, поскольку официально этот способ вообще не запрещен.

ВСЕ О ТУННЕЛИРОВАНИИ ТРАФИКА

Н а самом деле, халявный инет достигается не только за счет туннелинга. Перенаправление трафика может юзаться при организации собственной защиты (шифрование данных), а также для доступа к локальным ресурсам. Впрочем, мы подробно поговорим обо всех преимуществах этой темы, поэтому не будем забегать далеко вперед. Теория туннелинга предельно проста. К примеру, обычный прокси-сервер тоже является туннелем: ты запрашиваешь данные, прокси скачивает файл и шлет его тебе. Но это самый примитивный туннель. Существуют более интересные варианты передачи данных, основанные на интеграции различных протоколов.

▲ ИЗВРАЩЕНИЯ С ICMP

Представь ситуацию: у тебя закончились деньги на инет... Ты почувствовал интернет-ломку, твое душевное состояние находится в упадке. Хочется опять торчать в Сети. И тут на помощь приходят гостевые логины. Многие провайдеры предоставляют гостевой доступ для активации карт (посещения родного сайта), при котором дальше ресурса провайдера не шагнуть. Попробуем пропин-

говать какой-нибудь сервер, например, www.ru. Пошли пакетики, да? Замечательно, сегодня твой день :). Уже давно известно, что трафик легко прогоняется через обычные ICMP запросы. Это выполняется с помощью специальной тулзы X-проху. Ей была посвящена отдельная статья в Хакере.

Для организации туннеля необходимо наличие клиента и сервера. При этом принцип работы X-Прохи довольно прост: сервер устанавливается на рабочей машине с Win9x/NT. В его конфиге прописывается адрес реального проху-сервера и порт. Клиент, установленный на локальной тачке, будет настроен на связь с сервером (с помощью утилиты config.exe). Таким образом, получаем туннель: клиент посылает ICMP-запрос серверу (с типом ECHO_REPLY). В пакете содержится адрес, который следует доставить. Сервак связывается с реальным прокси-ком и высылает данные

```

C:\network>ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.

C:\network>start ipconfig /all
ipconfig /all
Microsoft Windows [Версия 4.0.9500]
(c) 2000 Microsoft Corporation. Все права защищены.
  
```

Клиент ICMP-туннеля

клиенту. В итоге ты получаешь бесплатный инет через гостевой логин. Естественно, необходимо указать локальный адрес и порт в качестве проху-сервера в твоем браузере.

Минусы этого метода: необходимо наличие настроенного сервера и рабочего прокси-адреса. Конечно, для крутого хакера это не проблема, но не все могут позволить себе такую роскошь :). Плюс туннелинга через ICMP: неплохая скорость передачи данных.

Сейчас провайдеров, открывающих ICMP в гостевом режиме, найти довольно тяжело, поэтому подобный прием с каждым днем теряет свою актуальность.

ХИТРОСТИ С DNS

Если ICMP-туннель организовать удается далеко не всегда, то с DNS-туннелингом все намного проще. Об этом уже писалось на страницах твоего любимого журнала (03.2003), но про принципы передачи трафика все равно стоит рассказать.

Допустим, ты пытаешься пропинговать какой-нибудь сервер (все на том же гостевом логине) и не получаешь никакого ответа. Все пакеты режутся, но есть один нюанс: ты можешь резолвить адреса доменов. А что нам мешает передавать данные в пакете с DNS-запросами? Правильно, ничего :). Существует несколько технологий организации DNS-туннелинга. Одна из них - поднятие псевдоинтерфейса etheretar, через который будет осуществляться туннелинг трафика (при помощи программы nstx). Подробная настройка этого способа уже рассматривалась, поэтому более интересным будет рассказ об обмене трафиком между протоколами TCP и UDP.

Почему UDP? Дело в том, что все DNS-запросы передаются на 53 UDP-порту в виде датаграмм. Ничто не мешает открыть порт на удаленном сервере и обращаться к нему при помощи специального клиента (при этом 53 UDP-порт не должен фильтроваться). Настройка туннелинга очень простая, более того, и сервер, и клиент ориентированы только на UNIX-like операционки (виндузятники отдыхают). Для полноценной передачи данных также будет необходим гроху-сервер (причем он должен быть установлен на машине с сервером irgohu).

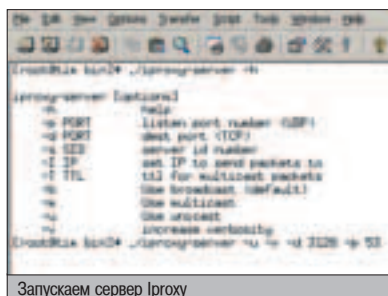
Софт поставляется только под Linux, так что любителям винды придется либо портировать бинарники, либо отказаться от irgohu вообще. Создать туннель очень просто: собираем бинарники клиента и сервера на двух сторонах, после чего запускаем клиентскую часть:

```
iproxy-client -p 31337 -d 53 -l 195.58.4.3
```

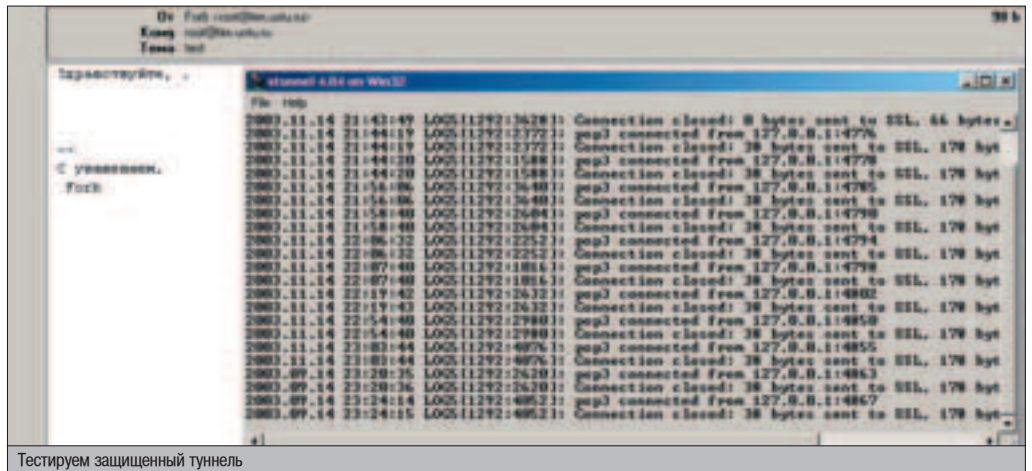
где опция -p отвечает за порт, который будет прослушиваться (TCP); -d - порт назначения (UDP) на сервере -l.

По аналогии запустим серверную часть:

```
./iproxy-server -u -p 333 -d 3128 -v.
```



Запускаем сервер Iproxy



Тестируем защищенный туннель

При помощи туннелирования можно поймать халявный интернет, а также решить проблему с собственной безопасностью.

Параметр -u означает unicast-сервер, -v - verbose mode. Это пригодится для диагностики возможных ошибок. Также не забывай, что содержимое порта назначения должно совпадать с портом реального прокси-сервера, поддерживающего метод CONNECT.

Теперь можно протестировать цепочку. Запусти какое-нибудь приложение и укажи в нем поддержку гроху-сервера по порту 31337. При правильном раскладе трафик будет исправно передаваться в обе стороны.

Как видишь, все просто. Если нет возможности установить прокси, либо ты хочешь юзать софт под винду, воспользуйся моим туннелером. Про него я рассказывал в статье "DNS-туннелинг". Его ты можешь скачать по адресу kamensk.net.ru/forb/1/x/udp-irc.tar.gz.

НЕПРОБИВАЕМАЯ ЗАЩИТА

Прежде чем рваться в бой, позаботься о собственной безопасности. Только представь, что весь трафик, идущий от тебя, sniffает ушастый ламер из твоего сегмента. Включая личную переписку со всеми твоими подруга-

ми. Я думаю, что твоя радость не будет слишком большой, поэтому пользуйся туннелированием для защиты передаваемой информации.

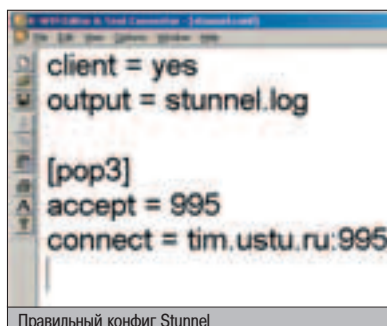
Один из таких способов - SSL-туннелирование. Суть в том, что весь трафик, который передается от тебя, будет зашифрован с помощью SSL. Инфа, дошедшая до сервера туннелера, раскриптовывается и передается уже реальному (незащищенному) демону, к примеру, pop3. Таким образом, получаем секурный туннель между тобой и сервером. В качестве последнего чаще всего применяется программа stunnel.

Stunnel и сервис (на который, собственно, и будет приходить зашифрованная инфа) целесообразно ставить на одной машине, чтобы полностью исключить утечку трафика. Давай попробуем организовать туннель между почтовым клиентом и pop3-сервером. Для начала установим на машину рабочую версию Stunnel. Ленивые BSD'шники могут воспользоваться портами, линуксоиды-alt'овцы программой apt-get. Остальные качают пакет с официального сайта www.stunnel.org.

После сборки приступаем к созданию туннеля. Сервер поднимается командой `stunnel -s 995 -r mail.host.ru:110`. При этом открывается туннель между 995 и 110 портами машины.

Теперь скачиваем клиент Stunnel под Win32, а также все необходимые библиотеки (libeay32.dll и libssl32.dll). Набросаем небольшой конфиг-файл, который будет прослушивать локальный 110 порт и перенаправлять весь трафик на удаленную машину с сервером Stunnel. На всякий случай я включил логирование обмена данными (для быстрого нахождения ошибок).

Если все выполнено верно, то можно запустить клиент Stunnel. Программа молча загружается и тухнет в трее. Поздравляю, туннель готов. Можно приступать к тестированию: настраивай почтовик на локальный хост и порт 995. Попытайся проверить почту. В случае, когда почтовик будет исправно стягивать сообщения, знай - туннель работает, и ты в полной безопасности :). Иначе ищи ошибку в лог-файле (в моем случае - stunnel.log).



Правильный конфиг Stunnel

ВОЗМОЖНОСТИ STUNNEL

В работу Stunnel входит множество функций. К примеру, он может туннелировать трафик через VPN соединение. Также программа интегрируется с Samba, Mysql, Oracle, Rsync и многими другими сервисами. Примеры использования Stunnel ты можешь найти на официальном сайте: www.stunnel.org/examples/rsync_mike.html.



▲ Помимо Datarpipe, существуют такие софтины, как Rinetd и Fpipe, выполняющие функции реди-ректа портов. Почитать про эти тулзы можно здесь: sector.h1.ru/port_redirect.htm.



▲ Внимание! Все приемы, касающиеся взлома, приведены исключительно в ознакомительных целях. Их применение на родном провайдере может выйти тебе боком. Редакция и автор статьи никакой ответственности за последствия не несут.

ИГРЫ С ФАЕРВОПОМ

Иногда появляется необходимость перенаправлять данные с одного порта (либо IP-адреса) на другой. В этом тебе поможет твой друг и товарищ - фаервол iptables. Если ты регулярно читаешь Хакер, то уже знаком со всеми прелестями этого чудесного брандмауэра (10.03). Сейчас мы поговорим о NAT'инге - одной особенности фаервола, при помощи которой можно без проблем управлять своим трафиком.

Рассмотрим тривиальную задачу: имеются порты 31337 и 31338. Необходимо все запросы с первого порта перекидывать на второй. Кроме того, редирект осуществляется лишь в случае обращения с определенно-го хоста. Вот как решается эта задача:

```
# iptables -A PREROUTING -s аppсec -t nat -p tcp --dport 31337 -j REDIRECT --to-port 31338.
```

Это правило выполняет редирект всех данных с порта А на порт В. Обычно это требуется при завороте данных с 80 порта на порт прокси-сервера.

Редирект применим лишь в пределах одного сервера. Если требуется заворачивать весь трафик с хоста А на хост В, необходимо использовать DNAT (Destination Network Address Translation). Правило вписывается в ту же цепочку PREROUTING, правда, немного с другими параметрами:

```
# iptables -A PREROUTING -s аppсec -t nat -p tcp --dport nоpt -j DNAT -to-destination 192.168.0.1
```

Я неспроста указал локальный адрес. Обычно DNAT используется, если необходимо обратиться к локальному серверу из внешней сети. Задача фаервола при этом заменить destination-адрес в заголовке пакета на заданный.

ПРИКЛАДНЫЕ ПРОГРАММЫ

И, наконец, настало время рассказать об отдельных программах, способных туннелировать трафик. Для *nix-like систем я бы мог выделить софтинку Dataripe. Она представляет собой обычный С-файл (впоследствии превращенный в бинарник). Функции программы - перекидывать весь проходящий трафик на определенный порт другому адресу. К примеру, нам нужно перебросить данные с порта 3000 хоста www.net1.ru на порт 3001 хоста www.net2.ru. Для этого надо лишь запустить программу на первой машине со следующими параметрами:

```
$/dataripe 3000 3001 www.net2.ru
```

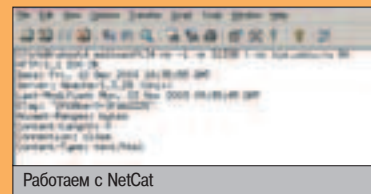
После этого весь трафик будет успешно туннелироваться.

ШВЕЙЦАРСКИЙ НОЖ

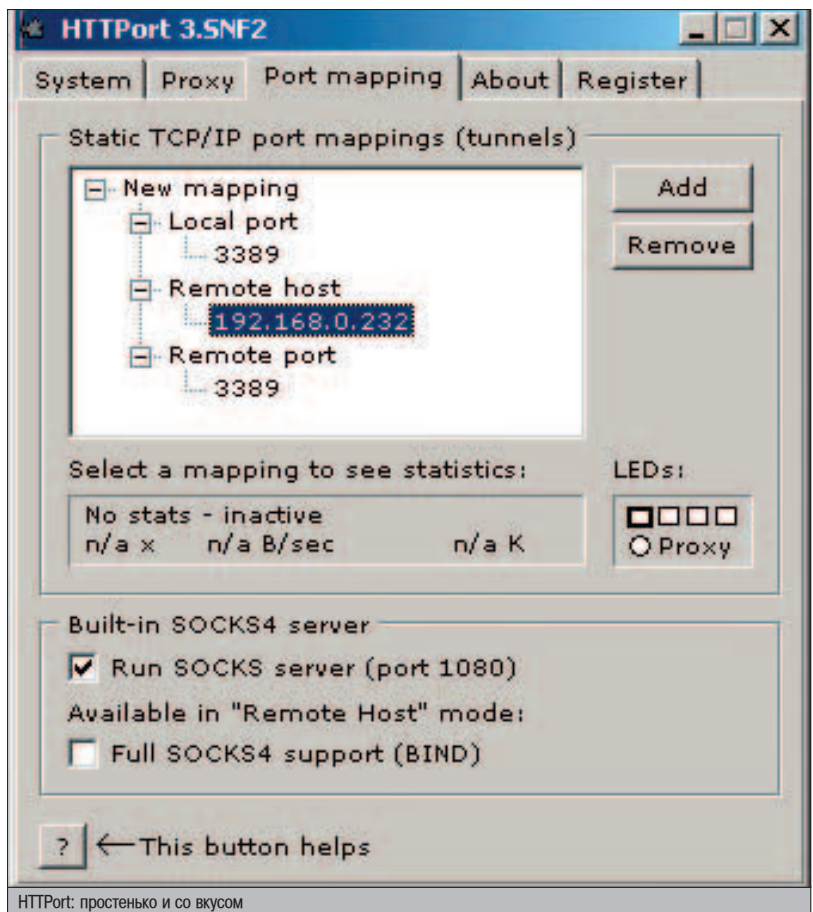
Я не мог не упомянуть знаменитую программу Netcat. Она работает через конвейер, поэтому для туннелирования необходимо запустить два бинарника в одной командной строке. Снова перекинем трафик с хоста А на хост В. Это достигается следующей командой:

```
nc -l -p 31337 | nc hostA.ru 31338
```

Команда выполняется на хосте В. При этом открывается порт 31337, с которым связывается порт 31338 на удаленной машине.



Вообще, Netcat умеет гораздо больше, чем просто перенаправлять порты. С его помощью можно сканировать подсети, читать баннеры сервисов, устанавливать в качестве бэкдора и т.д. и т.п.



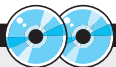
HTTPort: простенько и со вкусом

Под винду самой лучшей тулзой для создания туннелей является программа HTTPort. Она умеет все и еще чуть-чуть ;). А именно: заворот трафика на любые порты через HTTPS-proxy, создание собственного Socks-сервера, подде-

ржка авторизации и многое другое. К примеру, можно легко проверять почту через безопасный прокси-сервер, юзать различные сервисы по протоколу Socks5 (хотя поддержка носков в программе может вообще отсутствовать) и т.д. В общем, это виндовозный рай.

ТАКИЕ РАЗНЫЕ ТУННЕЛИ

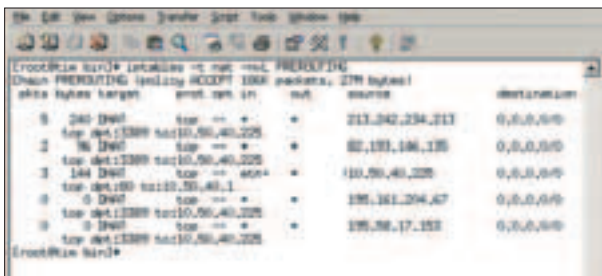
Вот, собственно, и все виды туннели, про которые я хотел рассказать. Как видишь, при помощи туннелирования можно поиметь халаянный интернет, а также решить проблему с собственной безопасностью. Знай, что создать туннель - простая задача. Даже если нет подходящего софта, ничто не мешает написать свою прибуду и организовать собственный нестандартный туннель.



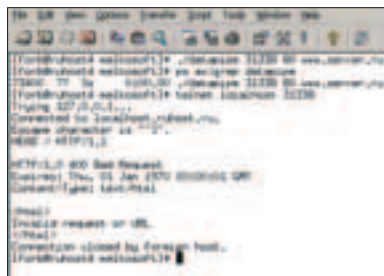
▲ На компакт-диске ты найдешь весь софт, который был описан в этой статье. А именно программы: Iproxy, Xproxy, Nstx, Dataripe и HTTPort.



▲ Если хочешь знать о туннелях больше, то посещай сайт www.opennet.ru. Там ты найдешь множество статей на эту тему. Также в Хакере часто обсуждались проблемы туннелирования трафика, поэтому перечитай статьи "DNS-туннелинг" (03.03) и "IRC-туннелирование с помощью stunnel: шифруемся в IRC по полной" (01.03).



Правила DNAT



Запуск и применение dataripe



к хорошему привыкаешь быстро



Характеристики:

Выходная мощность - 135 Вт
сабвуфер - 60 Вт
спутники - 5x15 Вт

Диапазон воспроизводимых частот:
35 Гц - 18 кГц

Магнитное экранирование

Деревянный корпус

Пульт дистанционного управления в комплекте



модель JB-641

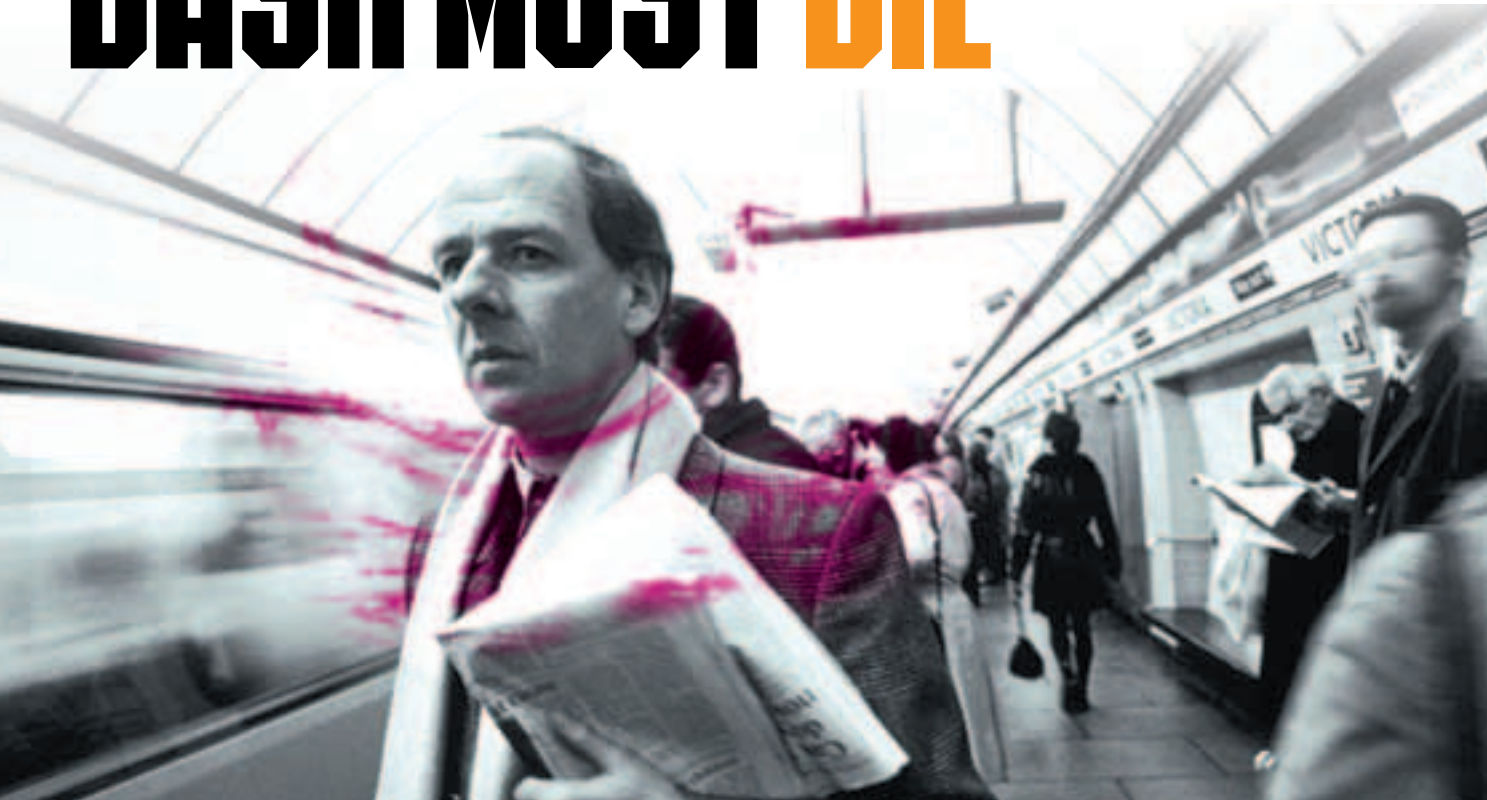
JB Jetbalance
www.jetbalance.ru

Дистрибуторы:

Lizard (095) 780.3266; Деникин (095) 787.4999; ELSIE (095) 777.9779; Citilink (095) 744.0333



BASH MUST DIE



Пожалуй, самая паковая цель для хакера - это получение интерактивного доступа к командной оболочке атакуемой машины. Немалую роль в этом играют так называемые эксплоиты, открывающие доступ к оболочке через определенную уязвимость в одном из сервисов (демонов). Для защиты от таких атак разработаны специальные технологии. Пример этому: StackGuard, FormatGuard и OpenWall. В этой статье я хочу предложить еще один способ. Возможно, он уже где-то описан, однако мне еще не попадались подобные решения.

ИЛИ КАК ПРОТИВОСТОЯТЬ ШЕЛЛКОДУ

СУТЬ СПОСОБА

При обычном входе в систему после выполнения login и авторизации запускается командный интерпретатор с определенными правами (здесь и далее речь будет идти только о Linux-системах). Однако shellcode обходит авторизацию и выполняет /bin/sh с правами уязвимого демона (обычно root). Большинство известных шеллкодов для запуска оболочки пользуются следующим кодом (см. Phrack 49-14, "Smashing The Stack For Fun And Profit" by Aleph One):

СИМНЫЙ ШЕЛЛКОД

```
#include <stdio.h>
int main() {
    char *name[2];
    name[0] = "/bin/sh";
    name[1] = NULL;
    execve(name[0], name, NULL);
}
```

Сразу возникает такая мысль: а что, если бы авторизация происходила не ДО запуска оболочки, а сразу ПОСЛЕ ее старта? В таком случае, даже после успешного выполнения

шеллкода, хакеру все равно понадобятся знания логина и пароля! Однако на практике такой идеальный случай осуществить проблематично или просто невозможно. Но что нам мешает сделать двухступенчатую авторизацию?! Т.е. после прохождения login уже сама оболочка в обязательном порядке требует повторной авторизации. Конечно, это внесет некоторое неудобство в работу легального пользователя, однако практически на 100% отпугнет от системы полчище script-kiddies, которые как раз и являются самым большим проклятием для администратора. Рассмотрим реализацию этого способа на наглядном примере, а также выявим некоторые его плюсы и минусы.

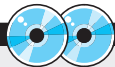
РЕАПИЗАЦИЯ СПОСОБА

В общем случае можно обозначить два варианта:

1. Оболочка требует ввода логина и пароля (или только пароля), идентичных тем, которые вводились при прохождении login.
2. Оболочка использует отдельную систему авторизации и требует логин и пароль (или только пароль), отличающиеся от стандартных в /etc/shadow.

Второй способ лучше в плане безопасности, т.к. некоторые шеллкоды могут добавлять новую учетную запись в /etc/shadow. Понятно, что если система защищена с помощью второго способа, то все эти действия не будут иметь особого значения, т.к. для получения полноценного доступа к оболочке нужно будет знать ее собственную систему авторизации, которая может быть реализована совершенно непредсказуемым способом. Однако первый способ легче в реализации, поэтому я опишу именно его. Но в реальной системе лучше использовать второй вариант.

Для наглядности напишем прототип оболочки, выполняющий все ее основные функции (исходник можно взять на нашем сайте или на диске к журналу). Назовем нашу псевдооболочку - xsh (расшифровку аббревиатуры оставляю на твоей совести). Компиляция осуществляется следующей строкой: gcc xsh.c -o xsh -lpat -lpat_misc -lncurses -lreadline. Несмотря на то, что я называю xsh псевдооболочкой, на самом деле она является почти полноценным шеллом. В ней отсутствуют лишь некоторые возможности, присущие любой нормальной оболочке, а именно: конвейеры, перенаправления, фоновое выполнение команд и собственный язык скриптов. Кратко рассмотрим работу xsh.



▲ На диске можно взять исходник оболочки xsh.c, который распространяется по лицензии GPL.



▲ Автор и редакция не несут ответственности за использование этого материала на практике.

КАК ИЗБАВИТЬСЯ ОТ SYSTEM() И POPEN()

Для избавления от функции `system()` в программе достаточно заменить ее парой вызовов `fork()+exec()`, а функции `open()` и `pclose()` устраняются серией `pipe()+dup2()+exec()`.

Сначала в функции `main()` вызовом `signal()` отключается реакция на некоторые стандартные сигналы. Далее вызывается функция `ram_test()`, не принимающая и не передающая никаких аргументов. Собственно, эта функция, отсутствующая в любой нормальной оболочке, и осуществляет аутентификацию пользователей. Я специально вынес сюда код этой функции, т.к. именно он предназначен для инжектирования в любую нормальную оболочку, если нужно защититься от shellcode:

КОД ДЛЯ ЗАЩИТЫ

```
pam_handle_t* pamh;
struct pam_conv pamc;
pamc.conv = &misc_conv;
pamc.appdata_ptr = NULL;

pam_start("passwd", getenv("LOGNAME"), &pamc, &pamh);
for (;;) {
    if (pam_authenticate(pamh, 0) == PAM_SUCCESS)
        break;
}

pam_end(pamh, 0);
```

Конечно, аутентификацию можно реализовать разными способами, но, наверное, правильнее всего использовать так называемые "подключаемые модули аутентификации" (PAM - pluggable authentication modules), что и делает `pam_test()`. В `pam_test()` используется стандартная диалоговая функция `misc_conv()`, осуществляющая терминальный ввод-вывод. Вызовом `pam_start()` инициализируется библиотека PAM (подробнее о PAM можно узнать по адресу www.citforum.ru/operating_systems/articles/pam.shtml). Первый аргумент `pam_start()` - это имя сервиса. Для наших целей удобно использовать сервис `passwd` (возможно, это и не самый лучший вариант). Хочу обратить внимание на второй параметр `getenv("LOGNAME")`, определяющий имя пользователя из стандартной переменной

среды `LOGNAME`. Если второй параметр сделать нулевым значением, то функция будет запрашивать не только пароль, но и логин пользователя. В нашем случае это станет дырой в безопасности, т.к. для доступа к оболочке (даже с `root`-правами) достаточно будет ввести имя и пароль совершенно любого пользователя, зарегистрированного в системе. Использование этого параметра открывает к тому же еще одну приятную особенность. Обычно демоны не устанавливают переменную среды `LOGNAME`, а это значит, что, даже имея пароль и логин рута (!), хакер не сможет проникнуть через шеллкод в систему с нашей защитой. Это будет возможно только в том случае, если хакер установит переменную `LOGNAME` в нужное значение.

Поэтому `xsh` запрашивает только пароль пользователя, автоматически определяя при этом логин. Далее в функции `ram_test()` запускается бесконечный цикл, и он останавливается только в случае правильно набранного пароля. После успешной аутентификации и возвращения из `ram_test()` открывается доступ к командной строке. Для этого в `main()` запускается еще один бесконечный цикл, где строкой приглашения является функция `printf`, выводящая на экран имя пользователя и текущую директорию (функция `get_current_dir_name()`). Прием и редактирование строки ввода осуществляется библиотекой `readline` (напомню, что `bash` тоже работает с этой библиотекой). Если пользователь вводит `exit`, то происходит выход из оболочки. Функция `parser`, с помощью стандартной функции `strtok`, разбивает введенную пользователем командную строку на лексемы. Далее реализуется возможность смены текущей директории командой `cd` (замечу, что `cd` является внутренней командой любой оболочки). Функция `fork_cmd()` выполняет командную строку. Для этого она с помощью вызова `fork()` создает новый процесс, после чего дочерний процесс выполняет команду с по-

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.



Обычно демоны не устанавливают переменную среды `LOGNAME`

```

PuTTY
Red Hat Linux release 7.1 (ttypk)
Kernel 2.4.2-2 on an i686

login: root
Password:
Password:
[xsh: root /root]# ls /
bin  dev  home  lost+found  mnt  proc  sbin  usr
boot  etc  lib  misc      opt  root  tmp  var
[xsh: root /root]#

```

Xsh в действии - пароль введен дважды

мощью `execsvr`, а родительский ждет завершения дочернего (с помощью `waitpid()`). Вот и все. Подобным образом работают практически все известные оболочки.

Теперь, когда понятен принцип работы, можно вносить изменения в рабочую оболочку системы. Для большей безопасности аналогичным изменениям должны подвергнуться все присутствующие в системе оболочки. Иначе их можно просто удалить.

▲ ПОЖКА ДЕГТЯ В БОЧКЕ МЕДА

Теперь обсудим плюсы и минусы способа. Как ни горько это признавать, но он совершенно не защищает систему от деструктивных действий хакера. Например, простым вызовом `unlink(name file)` хакер может удалять практически любые файлы, присутствующие в системе. Кроме того, несмотря на то, что большинство шеллкодов выполняют `/bin/sh`, ничто не мешает хакеру вызвать, например, `/usr/bin/emacs` или даже `/bin/vi`, и с их помощью натворить немало бед. Хакер может написать даже собственную простейшую оболочку, аналогичную `xsh`, и запустить ее в системе через шеллкод.

Однако среднестатистический скрипт-киддис не способен провести даже простейших изменений в шеллкоде. К тому же во все программы, имеющие интерактивный обмен с пользователем, нам ничто не мешает сделать корректировки, аналогичные тем, которые были сделаны в оболочке (благо они open sources). При этом ненужные в повседневной работе программы можно удалить.

У этого способа есть и еще один большой побочный эффект. В защищенной оболочке откажутся нормально работать программы, использующие функцию `system()`, а также "упрощенные" функции для организации каналов - `ropen()` и `pclose()`. Эти функции в своей работе используют вызов `/bin/sh`, а т.к. `sh` является ссылкой на защищенную оболочку, то эта защищенная оболочка просто не даст возможности выполнить команду без ввода пароля. Можно было бы сказать, что это даже к лучшему, т.к. приведенные функции небезопасны от природы, если бы не одно но: таких программ

слишком много! Данными вызовами пользуются даже некоторые кривые сервисы, из-за чего может просто отказаться грузиться система. Поэтому внедрение описываемой защиты может оказаться поистине ювелирной работой, где все должно быть подогнано и проверено на совместимость. Конечно, этим имеет смысл заниматься только в том случае, когда безопасность стоит на первом месте.

Понятно, что описанная мной защита не идеальна (как, впрочем, и любая из существующих), однако в совокупности с другими мерами безопасности она может значительно усложнить жизнь даже квалифицированному хакеру. Так что имеет смысл ее заюзать. Если же возникнут какие-нибудь вопросы или проблемы - пиши, постараюсь на них ответить. На этом все. Информация у тебя есть - начинай экспериментировать :).

слишком много! Данными вызовами пользуются даже некоторые кривые сервисы, из-за чего может просто отказаться грузиться система. Поэтому внедрение описываемой защиты может оказаться поистине ювелирной работой, где все должно быть подогнано и проверено на совместимость. Конечно, этим имеет смысл заниматься только в том случае, когда безопасность стоит на первом месте.

ЧТО ТАКОЕ НА САМОМ ДЕЛЕ /BIN/SH

В большинстве *nix-систем `/bin/sh` является символической ссылкой на рабочую оболочку системы. В качестве рабочей оболочки обычно выступает `bash`.



КАК МИР ЗАЩИЩАЕТСЯ ОТ ШЕЛЛКОДА

Уже давно известно, что одним чтением багтраков и латанием дыр нормально свою систему не защитить. Поэтому разрабатываются различные системы безопасности. Все существующие на сегодняшний день системы защиты от shellcode можно условно разделить на две категории:

1. Системы анализа и аудита исходного кода на уязвимость.
2. Системы, блокирующие или ограничивающие деструктивные действия программ.

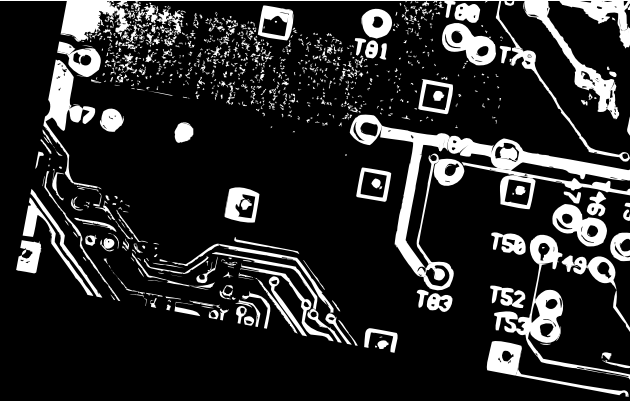
К первым относятся сканеры исходных текстов (source code scanners) и динамические отладчики. Сканеры исходных текстов (RATS, FlawFinder, PScan) проверяют код и выдают информацию о потенциально опасных участках. Но при помощи одних сканеров нельзя обнаружить все опасные места, поэтому применяются также динамические отладчики (MemWatch, Sharefuzz, ElectricFence). Передавая различные возможные комбинации входных данных, удается обнаружить многие скрытые ошибки, в т.ч. и переполнения буфера. Однако применение этих систем на больших программах, где количество строк в коде достигает миллиона, становится абсолютно бесполезным делом.

Ко второй категории относятся системы, блокирующие деструктивный код либо во время компиляции программы (StackGuard, FormatGuard, ProPolice), либо при ее исполнении (Openwall, Libsafe). Ограничивающий принцип (SubDomain, Linux Intrusion Detection System) основан на контроле доступа к определенным файлам и каталогам с целью минимизировать риск проникновения в систему. Однако такие системы очень сложны в управлении.

К сожалению, практически все эти системы защиты (кроме последнего варианта) рассчитаны на заранее известные уязвимости и совершенно бессильны перед другими атаками. Так, например, OpenWall хорошо защищает от переполнения буфера, но ничего не может поделать с heap overflow. Поэтому нужны системы защиты, предусматривающие успешное срабатывание шеллкода, но при этом все равно блокирующие или серьезно ограничивающие доступ хакера внутрь.



- ▲ www.securityfocus.com/data/library/P49-14.txt
- ▲ www.citforum.ru/operating_systems/articles/pam.shtml
- ▲ www.kernel.org/pub/linux/libs/pam/
- ▲ www.openwall.com
- ▲ www.immunix.org www.phrack.org



Железо

ЖУРНАЛ О КОМПЬЮТЕРАХ И ЖЕЛЕЗЕ

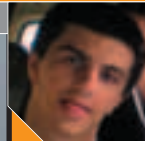


ТВОЯ МАМА БУДЕТ В ШОКЕ



ж д и в м а р т е . . .





ПАКАНЕМ

М

ЗАШИФРУЕМ



С вершилось! Ты написал свою первую программу и сделал это при помощи Delphi или какой-нибудь другой визуальной среды разработки. Все прекрасно! Прога работает! Но размер?! Одно окошко с кнопкой ОК занимает 300 килобайт. Что же будет, если добавить две кнопки? Это никуда не годится. На помощь к тебе придут самые лучшие паковщики в мире - они уменьшат твою прогу до невероятных размеров.

ПАКОВЩИКИ И ПРОТЕКТОРЫ ИСПОЛНЯЕМЫХ ФАЙЛОВ

КАК РАБОТАЮТ ПАКОВЩИКИ

О существовании архиваторов ты наверняка слышал не раз и, скорее всего, уже успел ими попользоваться. Ведь именно эти чудо-программы сохраняют место на твоём харде, берегут трафик и сокращают время скачивания файла в Сети. В общем, понятно, что архиваторы полезная в хозяйстве вещь. Но сегодня мы будем говорить не о классических реализациях, вроде WinRAR и WinZIP, а об уменьшении размера исполняемых файлов (exe'шников). Кстати, уменьшение размера подобных файлов - очень актуальная проблема для многих разработчиков, кроме, конечно, программистов из Microsoft :).

Мне в свое время, для того чтобы сделать свои программы маленькими и шустрими, пришлось научиться программировать на Asm'e, C, разбираться в структуре исполняемых файлов и сделать много других занятных вещей. Тебе же, в отличие от меня, придется только понять устройство волшебных паковщиков!

Итак, паковщики - это специальный класс архиваторов, предназначенный для сжатия исполняемых файлов. В основе их работы лежит следующая идея: создается новый

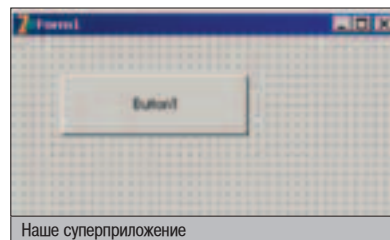
exe'шник, в который помещается оригинальный файл, но уже сильно упакованный. Вместе с ним добавляется код, умеющий извлекать и запускать исходник из архива. В отличие от привычных архиваторов, программа будет распаковываться не на хард, а в память компа и сразу же запускаться. Таким образом, твоя прога будет выглядеть как обычный exe'шник, но по действию будет напоминать матрешку, только работающую в обратном направлении.

ЧТО ЖЕ ВЫБРАТЬ?

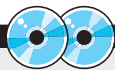
Паковщиков существует множество, и надо найти лучший из них. Я проводил оценку по следующим двум параметрам: скорость запуска приложения (она же скорость распаковки) и степень сжатия файла. На мой взгляд, лучшим по этим позициям является UPX.

Для того чтобы проверить все его возможности, мне пришлось создать маленькое приложение на Delphi - всего-навсего одну форму с кнопкой. При компиляции этого нехитрого творения у меня материализовалось 373 килобайта исполняемого файла. Это меня, естественно, не порадовало. Надо заметить, что на любимом C++ мне бы удалось добиться результата в пару килобайт. Поэтому было решено бороться с результатом Delphi. Для этого я натравил UPX на только что созданный файл, задал ему максималь-

ную степень компрессии и посмотрел, что получилось. А получилось относительно неплохо: размер файла уменьшился более чем в два раза, и он стал весить 153 Кб. При этом он сохранил способность нормально запускаться и функционировать :).



Такой компрессии мне показалось мало, поэтому я начал экспериментировать с другими упаковщиками. Вот что попало в мои руки: 32Lite, ASPack, NeoLite 2.0, PeComact, PeCompress, PeCrypt, PePack, PkLite, Shrinker, WinLite, Telock. Как оказалось, всем им далеко до UPX - в лучшем случае сжатие достигало 161 Кб, что было на целых 8 килобайт больше, чем у лидера. Но самое интересное, что тот же монстр RAR сумел ужать исходный файл все до тех же 161 Кб. Это заставило меня задуматься - а можно ли получить еще лучший результат? Послековырания в архиваторах и пробы различных вариантов мне удалось ужать файл еще на три



▲ На нашем диске лежат бинарные версии упаковщиков, а также сорсы UPX.

```

C:\WINDOWS\system32\cmd.exe
28.06.2002 20:42 (DIR) .
28.06.2002 20:42 (DIR) ..
22.05.2001 04:14 87 680 upx.exe
07.04.2003 12:00 48 128 NOTEPAD.EXE
28.06.2002 20:53 153 680 Project1.exe
28.06.2002 20:53 154 148 Project1.BMPack.exe
28.06.2002 21:07 160 575 Project1.exe
28.06.2002 20:53 172 736 Project1.BMP
28.06.2002 20:52 236 832 Project1.TheInker.exe
28.06.2002 21:15 149 179 Project1Upx.exe
28.06.2002 21:21 (DIR) .
28.06.2002 20:52 372 736 Project1.exe.original
28.06.2002 21:26 (DIR) ..
 7 File(s) 1 738 740 bytes free
 4 Dir(s) 448 987 136 bytes free

D:\Source\Projects\src\src\Packaging\TestLab>
Microsoft Windows [Version 5.00.2600.5512]
(c) 2006 Microsoft Corporation. All rights reserved.
C:\> cd /d D:\Source\Projects\src\src\Packaging\TestLab
D:\Source\Projects\src\src\Packaging\TestLab>
Usage: upx [-i:1234567890123456] [-q:qfkl] [-w FILE] FILE...

Commands:
  -f compress faster                -F compress better
  -d decompress                    -l list compressed file
  -t test compressed file          -v display version number
  -g give more help                -L display software license

Options:
  -q be quiet                       -w be verbose
  -F FILE write output to 'FILE'
  -f force compression of suspicious files
  -k keep backup files
  FILE... executable to UPX/compress

This version supports: dos/exe, dos/com, dos/zip, djgpp2/coff, win32/le,
win32/pe, win32/pe, win32/pe, fat/elan, atari/stc, linux/386

UPX comes with ABSOLUTELY NO WARRANTY; for details type `upx -h`.
D:\Source\Projects\src\src\Packaging\TestLab>
  
```

UPX может многое

кило. Этот результат дал мне все тот же RAR, но натравленный на упакованный UPX'ом файл.

Проведя эксперимент с RAR'ом, я никак не мог поверить, что классические архиваторы проиграли битву динамическим паковщикам. Конечно, понятно, что вторые специально заточивались под особенности исполняемых файлов, но все равно что-то смущало. В итоге я оказался прав - в моей коллекции нашелся один упаковщик, который победил всех. Он смог ужать тестовый пример аж до 143 килобайт. Это оказался малоизвестный архиватор tk, созданный неким Малькомом Тейлором (Malcolm Taylor) в 2000 году.

ДОПОЛНИТЕЛЬНЫЕ БОНУСНЫЕ ФИЧИ

Помимо уменьшения размеров исполняемых файлов, ты абсолютно бесплатно получаешь защиту от отладки и дизассемблирования твоих приложений. Подобные эффекты проявляются как бы ненароком, как побочный эффект от действия паковщика. Отладчикам и дизассемблерам необходимы чистые исполняемые файлы. Они очень не любят, когда в них кто-то покопался. А паковщик превращает исполняемый файл в эдакий винегрет, разобраться в котором становится довольно сложно. Дизассемблер попросту не в состоянии выделить код приложения из всей этой мешанины.

А бывает еще так, что некоторые особо "продвинутые" дизассемблеры при работе со сжатыми файлами радостно выдают ассемблерный код. Проблема заключается в том, что код этот принадлежит не исходной программе, а паковщику. Сечешь, к чему такое

приводит? Злостный хакер будет ковыряться в километрах ассемблерного кода не твоего приложения, а того самого динамического архиватора (на самом деле, грамотный крякер, изучив такой код, сможет написать свой распаковщик, и вся защита полетит - прим. ред.). Неплохая защита - не правда ли?

Конечно, надо заметить, что такие простые приемы не остановят особо головастых и догадливых хакеров, а профессионала такие трюки просто рассмешат. Ведь в его боевом арсенале всегда найдутся программы, которые в миг распакут сжатые тобой файлы. UPX, например, сам позволяет возвращать запакованные им exe'шники к их первоначальному виду. Для этого всего-навсего нужно воспользоваться ключом -d из командной строки.

Основная проблема распаковки заключается в том, чтобы выяснить, чем именно запакован исполняемый файл. Ведь снять защиту намного проще, зная алгоритм и средство упаковки. Для решения этой проблемы существует целый класс утилит. Называются они анализаторами и предназначены для определения по особым признакам (имена секций, характерные строки в коде и биты в заголовке исполняемого файла), какой паковщик использовался.

Кроме анализаторов, существуют универсальные утилиты, позволяющие распаковать файл, не зная, чем именно он был ужат. В качестве примера можно привести PeDumper. Понятное дело, что универсальные утилиты не всегда радуют нас хорошими результатами, выдавая кривые или даже неправильные коды. Здесь играет роль неоднозначность задачи - точно восстановить загруженный в память файл не так уж

```

Microsoft Windows [Version 5.00.2600.5512]
(c) 2006 Microsoft Corporation. All rights reserved.
C:\> cd /d D:\Source\Projects\src\src\Packaging\TestLab
D:\Source\Projects\src\src\Packaging\TestLab>
Usage: upx [-i:1234567890123456] [-q:qfkl] [-w FILE] FILE...

Commands:
  -f compress faster                -F compress better
  -d decompress                    -l list compressed file
  -t test compressed file          -v display version number
  -g give more help                -L display software license

Options:
  -q be quiet                       -w be verbose
  -F FILE write output to 'FILE'
  -f force compression of suspicious files
  -k keep backup files
  FILE... executable to UPX/compress

This version supports: dos/exe, dos/com, dos/zip, djgpp2/coff, win32/le,
win32/pe, win32/pe, win32/pe, fat/elan, atari/stc, linux/386

UPX comes with ABSOLUTELY NO WARRANTY; for details type `upx -h`.
D:\Source\Projects\src\src\Packaging\TestLab>
  
```


Файл сжат в 3 раза!

и просто, как может показаться на первый взгляд. Так что больших надежд на такие утилиты возлагать не стоит, да и пользоваться ими довольно сложно.

ПРОТЕКТОРЫ

Если твоя основная цель не паковка программы, а защита кода от злых дядек, то тебе нужны утилиты другого класса - протекторы. Их принцип действия близок к паковщикам, но вместо уменьшения размера они шифруют файл. К тому же протекторы после загрузки файла в память пользуются специальными трюками, позволяющими предотвратить его отладку и исследование кода. Для этого они хитрым образом изменяют внутренние структуры исполняемого файла, используют самодифицирующийся код, кусками шифруют части файла в памяти по ходу исполнения. Перечислять, а тем более детально описывать все применяемые ими приемы, здесь смысла не имеет, поскольку это очень большая и сложная тема, требующая специальной подготовки. Единственное, что стоит отметить, это наличие встроенных функций шифрования прямо в самом паковщике. Получается два в одном флаконе.

Наиболее мощным протектором на данный момент является ASPProtect, написанный нашим соотечественником Алексеем Солодовниковым. До сих пор для него не написано депротектора, позволяющего деактивировать защиту в автоматическом режиме. Снятие такой защиты является задачей далеко не тривиальной, доступной даже не всем профессиональным хакерам. На тему снятия ASPProtect написано множество статей, в которых обсуждаются отдельные сложные моменты, но абсолютной панацеи до сих пор не найдено.

Напоследок хотелось бы предупредить тебя, что протекторы защищают программы лишь от исследования другими людьми, но никак не от взлома и кражи. В их задачи не входит установка на твой файл паролей или серийных номеров. (Хотя есть и такие протекторы, но на их защиту не стоит надеяться - она снимается одним пальцем.) Поддержку системы регистрации и проверки серийных номеров тебе придется писать самостоятельно. А этот процесс отнюдь не из самых простых, поскольку если ты ошибешься, то ситуация может сложиться так, что для взлома твоей программы вообще не придется копаться в дебрях откомпилированного кода, а достаточно будет лишь подправить какой-нибудь ключик в реестре. Но это уже совсем другая история... 



▲ Все вышеописанные протекторы и упаковщики ты сможешь слить с сайта wasm.ru. На нем ты также найдешь несколько статей, описывающих работу с ними.

А Я ПРОГРАММЕР!

Если ты хочешь написать свой паковщик, то тебе несказанно повезло. Самый известный из паковщиков - upx.exe - распространяется вместе с исходным кодом. Ты можешь скачать его сорсы на sourceforge.net/projects/upx/.



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ:

ХАКЕРСТВО **БЕЗ** ГРАНИЦ



Недavno, проверяя одну из своих мыльниц, я наткнулся на трогательное письмо. Админ провайдера, услугами которого я пользуюсь, спешно жаповался, что хакеры разнесли к чертям всю контору, и от старой базы данных по клиентам остались рожки да ножки. «Мы пытаемся тут навести порядок, поэтому, дружище, не мог бы ты приспать мне свои логи и пароль», — робко предлагал собеседник. На дворе активно смеркалось.

Несмотря на то, что понятие «социальная инженерия» появилось недавно, люди в той или иной форме пользовались ее техниками испокон веков. В Древней Греции и Риме в большом поччете были пиплы, которые могли навешать на уши любую лапшу и убедить собеседника в его очевидной неправоте. Выступая от имени верхов, они вели дипломатические переговоры, а подмешивая в свои слова вранье, лесть и выгодные аргументы, нередко решали такие проблемы, которые, казалось, невозможно было решить без помощи меча. В среде шпионов социальная инженерия всегда была главным оружием. Выдавая себя за кого угодно, агенты КГБ и ЦРУ могли выведать самые страшные государственные тайны. А насколько профессионально нас инженерят политики и кандидаты в депутаты (мэры, президенты) — вообще любо-дорого посмотреть. Хотя, по правде сказать, и я, и ты, и все мы от них не отстаем. Ты ведь не будешь отрицать, что когда-нибудь да пытался хитроложой уловкой настроить чела на нужную тебе волну. Например, когда просил родителей купить мороженое, обещая пятерку в четверти по математике. Приемы социальной инженерии мы часто используем, даже не осознавая этого. В отличие от тех же агентов, депутатов и... хакеров.

В начале 70-х годов, в период расцвета фрикинга, некоторые телефонные хулиганы забавлялись тем, что названивали с уличных автоматов операторам Ma Bell и подкалывали их на тему компетентности. Потом кто-то, очевидно, сообразил, что, если немного перестроить фразы и кое-где сбредить, можно заставить техперсонал не просто оправдываться, а выдавать под влиянием эмоций конфиденциальную информацию. Фрикеры стали потихоньку экспериментировать с уловками и к концу 70-х настолько отработали техники манипулирования неподготовленными операторами, что могли без проблем узнать у них практически все что хотели.

Заговаривать людям зубы по телефону, чтобы получить какую-то информацию или просто заставить их что-то сделать, приравнивалось к искусству. Профессионалы в этой области очень гордились своим мастерством. Самые искусные социальные инженеры (синжеры) всегда действовали экспромтом, полагаясь на свое чутье. С помощью наводящих вопросов, по интонации голоса они могли определить комплексы и страхи человека и, мгновенно сориентировавшись, сыграть на них. Если на том конце провода находилась молоденькая, недавно поступившая на работу девушка — фрикер намекал на возможные неприятности с боссом, если это был самоуверенный тьюфак — достаточно было представиться наивным юзверем из фирмы, которому все нужно показать и рассказать. К каждому подбирался свой ключ. С появлением компьютеров многие фрикереры перебрались в компьютерные сети и стали хакерами. Навыки СИ в новой области стали еще полезнее. Если раньше мозги оператору пудрили в основном для получения кусочков информации из корпоративных справочников, то теперь стало возможным узнать пароль для входа в закрытую систему и скачать оттуда кучу тех же справочников или что-то

секретное. Причем такой способ был намного быстрее и проще. Не нужно искать дыры в навороченной системе защиты, не надо ждать, пока John the Ripper угадает правильный пароль, не обязательно играть в кошки-мышки с админом. Достаточно позвонить по телефону и, при правильном подходе, на другом конце линии назовут заветное слово.



▲ ТРИ КИТА СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Все методики социальной инженерии можно разделить на три категории в зависимости от того, где они используются: по телефону, в инете или риаллайфе. В каждой своя специфика, и совсем не факт, что человек, имеющий навыки СИ по инету, сможет так же эффективно юзать их face2face.



▲ ТЕЛЕФОН

Многие считают, что после мозгов, телефон — главное оружие синжера. Благодаря ему, можно оставаться анонимным и в то же время иметь с жертвой прямую связь. Последнее важно потому, что непосредственный контакт не дает собеседнику времени обдумать положение и взвесить все за и против. Решать нужно немедленно, причем под натиском гнущего свою линию синжера. Так как в телефонном разговоре мы обмениваемся только звуковой информацией, большую роль в принятии решений играет интонация и голос собеседника. На первых порах, пытаясь обмануть кого-то по телефону, новички могут растеряться и быстро сдать позиции. Чтобы этого не произошло — нужно наработать практику, прозванивая по рандомным номерам и, заговаривая с незнакомыми людьми, пытаясь обмануть их. Например, ты можешь выдумать какую-то идиотскую новость (американцы высадились на Солнце) и предложить неизвестному собеседнику ее вместе обсудить. Твоя задача — научиться запутывать людей и внушать им любую глупость. Можешь поиграть с ролями, представляясь оператором АТС или директором морга. Чем больше у тебя будет опыта в телефонных пранках, тем увереннее ты себя будешь чувствовать при разговоре с намеченной жертвой.

Старайся при разговоре ходить. Научно доказано, что когда человек двигается, у него быстрее работает мозг. Если решил повернуть что-то серьезное — не звони из дома, пользуйся таксофоном. Потому что при большом желании проследить через АТС твой звонок не составит проблем.

На фирмах, где серьезно подходят к проблеме безопасности, советуют в начале

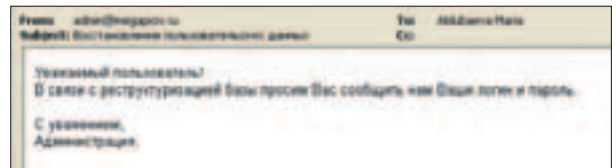
разговора требовать обратный телефон и перезванивать незнакомцу. Это еще одна причина, почему лучше звонить с таксофона. Но если ты звонишь из дома и слышишь: «Оставьте, пожалуйста, ваш номер — я перезвоню», продикуй один из тех телефонных номеров, которые вечно заняты. В каждом городе такие есть, узнать о них можно, например, у операторов (опять же, используя СИ). Объяснить короткие гудки все же проще, чем похмельный голос левого мужика.



▲ ИНЕТ

В некоторых случаях Сеть может стать более удобной альтернативой телефону. Например, если жертва находится в другой стране и между вами имеется языковой барьер. Или если нужно провернуть что-то глобальное (разослать кучу мессаг). В первую очередь интернет хорош тем, что в нем можно себя выдать за кого угодно. Он, в отличие от телефона, не держит в рамках возраста и пола. К тому же, ты можешь использовать для инжиниринга кучу разных персонажей, создавая второстепенными героями иллюзию нужного качества у основного. Например, если ты зайдешь на www-чат и крикнешь: «Я крутой писатель!» — тебя хрен кто заметит. Но если с разных окон под просями заведешь себе на том же чате толпу виртуалов, наперебой расхваливающих твои писательские таланты, остальной народ сразу заинтересуется и начнет расспрашивать, чего ты там пишешь.

Вообще, так как в сетевой социальной инженерии виртуалы используются повсеместно,



но, ты должен хорошо позаботиться о том, чтобы они выглядели реалистично. Биография, характер, стиль письма, подписи, координаты в Сети (мыло, сайт) — ты должен продумать все, чтобы любой неверующий Фома смог сколько угодно раз убедиться в реальности твоего виртуала.

При проведении серьезных диверсий старайся избегать отсылки мессаг с халявных почтовых ящиков — они сразу вызывают подозрение у мало-мальски грамотных людей. Впрочем, если мыло малоизвестно (находится в другой стране), можно выдать его за фирменное, указав в конце письма «полное название конторы». Например, наше халявное bk.ru можно выдать за мыло от BlackKobra corporation или Brothers Killers inc.

▲ РИАЛПАЙФ

Способ довольно опасен, так как уже не приходится рассчитывать на анонимность, и тебя впоследствии могут опознать. Но опасно только в особо экстраемальных случаях, нап-



пример, когда ты решил кинуть фирму на большие деньги. На практике риаллайф – самый распространенный способ, поскольку общаемся мы в основном в реале, а где общаемся, там и врем, а где вранье, там и наш толк. Риаллайфовая СИ напрямую связана с НЛП, поэтому если хочешь узнать больше о том, как изменять модель поведения людей – читай FAQ по NLP, там есть много чего интересного.

Если ты подходишь к делу основательно и готов пожертвовать временем в угоду эффективности, хорошим методом для тебя может оказаться обратная социальная инженерия. Так называют метод, когда синджер вынуждает человека обратиться к нему за помощью и, предлагая ее, получает то, что ему нужно. Проходит все примерно по следующему сценарию – хакер сначала зарекомендовывает себя в фирме как компетентный специалист (см. предыдущий раздел), затем каким-то образом выводит из строя один из компьютеров (достаточно запустить программку, отключающую один из параметров в реестре). Сотрудник компании вызывает «специалиста», и тот просит предоставить конфиденциальную информацию (или сам находит ее на компьютере), мотивируя тем, что это нужно для устранения неполадки.

▲ ИСКУССТВО ПЕРЕВОПОЩЕНИЯ

Занимаясь, СИ тебе придется не раз надевать маски других людей. Понятное дело, левому пацану с улицы никто свои тайны выдавать не будет, а вот кому-то, кто на это имеет право – волей-неволей придется. Уверенно врать дано не каждому. Сказываются нравования наших предков, которые с детства вбивали в нас вредный комплекс – врать нехорошо. Но можно обмануть свои комплексы, если искренне поверить в правоту своих лживых слов. Ты ни секунды не должен сомневаться, что, к примеру, являешься сотрудником фирмы, забывшим пароль, что нуждаешься в помощи и имеешь на нее полное право. Ведь когда ты идешь в конце месяца получать зарплату, ты же не испытываешь от этого дискомфорта, не скулишь жалобно, пытаешься вытянуть лишнюю копейку? Ты получаешь то, что заслужил, что твое по праву. Того же принципа нужно придерживаться и в социальной инженерии. Если ты сумеешь убедить человека в своих правах, то обретешь требуемое, даже если на самом деле никаких прав на него не имеешь. Лучшего результата можно добиться, если не играть чью-то роль, а стать этим кем-то. В мыслях, поступках и во всем остальном. Для этого, конечно, нужно разбираться в психологии людей разных категорий и иметь кое-какие актерские способности. Дам тебе навскидку несколько распространенных среди хакеров шаблонов, возможно, они помогут тебе выбрать линию поведения в той или иной ситуации.

Начальник. Человек, привыкший отдавать команды, ценящий свое время, добивающийся поставленных целей. Манера разговора жесткая, нетерпеливая. Непробиваемая уверенность в себе и легкое (или полное) пренебрежение к рядовым служащим. Всем своим видом показывает, что проблема, с которой обратился – мелкая неувязка, которую нужно решить как можно скорее. Никаких просьб – только суровые вопросы



в стиле «какого черта». В ответ на недоверчивые или проверяющие реплики – негодование и запугивание.

Секретарь. Обычно девушка с приятным голосом. Задача – выполнить конкретное поручение шефа, не отвлекаясь на условности. Осведомлена о начальнике и некоторых его делах, как бы между прочим роняет достоверные факты (или недостоверные, которые нельзя проверить). Характер разговора – мягкий, с легким эротическим подтекстом (если собеседник – мужчина). Реакция на нежелание сотрудничать – бурное огорчение, жалоба, что начальство накажет.

Техслужащий. Снисходительное, но дружелюбное отношение к клиентам. Цель проста – устранить неполадку и избавить обе стороны от головной боли. Подчеркнутая специфическими терминами компетентность. На отказ сотрудничать – реакция удивления, так как сотрудничество в первую очередь выгодно для клиента. Никаких уговоров – просто дать понять, что без твоего участия проблема только усугубится. Можно описать страшные последствия.

Юзверь: работник, выполняющий свои обязанности и напуганный неожиданной проблемой. Четко выраженный мотив поскорее решить все проблемы и вернуться к своей рутине работенке. Отсутствие представления о характере проблемы, заинтересованность только в ее устранении. Характер общения: «Ой, а у меня курсор завис. Это вирус, да?» Показать всю безнадежность своего положения и готовность отдаться в руки специалиста.

Моделей поведения много, какой пользоваться – зависит от ситуации и человека, которого нужно обработать. Большое значение тут имеет предварительный сбор информации о будущей жертве, потому что только так ты сможешь составить наиболее эффективный сценарий и подготовиться ко всяким неожиданностям. Раньше любимым способом сбора инфы у хакеров было ковыряние по ночам в мусорных баках конторы. С появлением интернета все упростилось. Во-первых, существуют специализированные справочники по крупным компаниям, где можно найти имена, должности и контакты представителей. Во-вторых, можно опять же воспользоваться социальной инженерией и вте-

саться в доверие к неосторожному работнику. Например, многие в служебное время злоупотребляют аськой. Представившись многообещающей мадамой, можно закрутить с челом бурный виртуальный роман, и под предлогом «хочу побольше узнать о тебе», потихоньку расспрашивать о фирме и начальстве. Тебе, наверное, интересно, что именно нужно узнавать? Не знаю, дружище, одно лишь сто пудов – чем больше ты соберешь информации, чем разнообразнее (от любимого цвета носков шефа до средних годовых доходов фирмы) она будет, тем легче тебе будет выполнить свою задачу. Особое внимание обрати на имена, характер и обязанности ключевых фигур в конторе, так как именно эти сведения ты с большой вероятностью будешь использовать в дальнейшем. Приступай к основной фазе инжиниринга, только когда почувствуешь, что знаешь свою жертву. Знаешь, чем она живет, о чем думает, как себя поведет в той или иной ситуации, какие психологические комплексы роятся у нее внутри.



▲ ТАРАКАНЫ, ЖИВУЩИЕ В НАШЕЙ ГОЛОВЕ

Сколь бы настроженным или научным жизнью человек ни был, он никогда не избежит от всех багов в своей голове. Наш разум уязвимее, чем самая дырявая винда. Причем нередко уязвимыми становятся те качества, которые мы ценим в людях – отзывчивость, преданность и любознательность. Я уже не говорю о всякого рода психологических, присущих всем нам. Вся социальная инженерия на том и построена, чтобы использовать человеческие слабости для изменения модели поведения. Ниже мы на примерах рассмотрим несколько основных психологических комплексов, чаще всего подверженных СИ.



▲ ДОВЕРЧИВОСТЬ

Это качество заложено в каждом человеке. Мы слушаем рассказы о людях, которых кинули как полных ловов, удивляемся их наивности, пребываем в полной уверенности, что никогда бы сами не вляпались в подобное... и со временем сами занимаем их место. Доверчивость напрямую связана с нашей врожденной ленью. Согласись, легче верить человеку на слово, чем утруждать себя проверками правдивости его слов.

К тому же некоторые, в силу робости или хорошего воспитания, просто не решаются открыто заявить, что собеседник врет, и предпочитают рискнуть, надеясь на его честность. Большую роль в вопросе доверия играют детали, о которых мы сознательно не



задумываемся, но которые определяют нашу реакцию — верить человеку или нет.

Пожалуй, главный фактор доверия — уверенность в себе. Если кто-то говорит авторитетным тоном знатока, не допускающим возражений — люди могут поверить в любую чушь. Конечно, речь не идет о всем известных истинах (хотя опытный софист сможет тебе вполне убедительно доказать, что на Солнце минусовая температура, а белое — это на самом деле черное), но в вещах, о которых человек не знает или в которых хотя бы сомневается — можно легко склонить его мнение в нужную сторону. Хороший способ создать иллюзию своей правдивости — сделать несколько заявлений, которые, как известно собеседнику, на сто процентов правдивы, и в то же время подмешать в них несколько лживых доводов. Человек, видя, что ты говоришь правду, автоматически воспримет как правду и твою ложь. Своеобразный аналог теста на знание виновного, переделанный под нужды СИ.

Если ты в предварительной подготовке досконально не изучил жертву — что она знает, а что нет, старайся избегать прямой лжи. Например, если ты представишься работником шестого отдела Васей Чайкиным, то вполне вероятно услышишь: «Я знаю всех в шестом отделе — с такой фамилией там никого нет». Но если вместо конкретного Васи Чайкина из конкретного отдела ты станешь неопределенным Петей, только поступившим на службу — у тебя всегда останется место для отступления. Вообще, до начала диверсии постарайся продумать все так, чтобы тебя не прижали к стенке, найди явные несоответствия. Всегда выбирай такой сценарий, который максимально достоверно подходит к ситуации. Чтобы проиллюстрировать этот психоконструкт, расскажу, как однажды я прошел в комнату студенческой общаги через злоую бабу-вахтершу, «никого никоим образом не пущавшую».

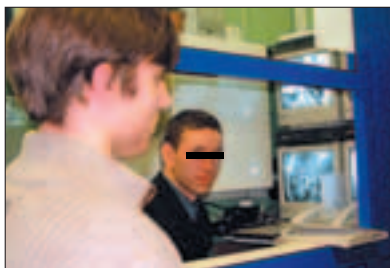
- Здравствуйте, бабушка. Мне в 90, к Самодину.

- Никого не пускаем. Жди здесь. Будет кто спускаться — позовут.

- Бабушка, я из деканата — ректор срочно его вызывает. Колю на олимпиаду от института отправляют, нужно заявление принести. Сейчас надо, сегодня — последний день. Я ему быстренько скажу и тут же вернусь. Хорошо?

- Ладно. Только давай быстрее.

- Я мигом. Спасибо!



СТРАХ

У каждого из нас свои страхи. Не обязательно это боязнь темноты или, к примеру, пауков. Можно испытывать страх показаться нелепым в какой-то ситуации, страх за последствия невыполненного поручения, страх перед чем-то неизвестным. Существуют милли-



оны маленьких и больших страхов, которые заставят человека пойти на самые необходимые поступки, чтобы от них избавиться. Использовать этот психоконструкт легко — достаточно всего лишь вызвать у собеседника один из страхов и сыграть роль «освободителя». Хорошим примером является случай, описанный в статье Алексея Лукацкого, когда хакер в течение всего пары минут получает пароль к аккаунту работника банка.

В разгар рабочего дня в операционном зале банка раздается звонок. Молодая операционистка поднимает трубку и слышит мужской голос:

- С вами говорит администратор сети, Иван. Как вас зовут?

- Оля!

- Олечка, мы сейчас проводим плановую модификацию программного обеспечения "Операционный день банка". Ты не могла бы назвать мне свой пароль?

- А мне говорили, что чужим нельзя называть свой пароль.

- Так я ведь не чужой! Я свой, я сотрудник отдела информатизации. Мой начальник - Петр Петрович Петров. Я хочу всю работу сделать поскорее. А то и тебе, и мне придется оставаться после работы. А у тебя, наверняка, есть дела вечером. К тому же, твоему начальнику тоже придется задержаться после работы. А он будет этим недоволен, что может отразиться и на тебе. Ты согласна?

- Да, согласна.

- Тогда назови свой пароль, и все будет ОК.

- Мой пароль оля.

- ОК. Спасибо за помощь.

Здесь синжер вызвал у юной особы сразу два страха — задержаться в конторе дольше положенного и вызвать гнев начальства. Последний — особенно эффективен, так как большинство людей все-таки дорожат своей работой и постараются сделать все возможное, чтобы избежать неприятностей.

Страх, кстати, является хорошим стимулом доверия — это естественная защитная реакция нашего организма. Напуганного человека больше заботит, как выйти из этого неприятного состояния, чем мысль о том, что страх может оказаться результатом блефа. Каждый из нас подвержен тем или иным страхам в большей или меньшей степени, но есть такие, которые сильно влияют практически на всех людей. Это угроза жизни, страх потерять близкого человека (животное), боязнь одиночества, страх перед болью, боязнь не осуществить поставленные цели и т.п.

Жадность

Второе качество человека после лени — жадность — является любимым психоконструктом аферистов всех мастей. Желание людей быстро обогатиться настолько велико, что часто затмевает все разумные мысли, и пиллы ведутся на очевидное кидалово. Использовать жадность в своих корыстных целях просто, нужно всего лишь пообещать человеку что-то, что ему необходимо. Не обяза-

DIGMA
КОЛЛЕКЦИЯ КОМПЬЮТЕРНЫХ АКСЕССУАРОВ

www.digma.ru



тельно деньги — рекламу, информацию, предмет для коллекции, секс... да что угодно. Просто узнай побольше о том, что ценно для жертвы, и обещай это. Обещать ведь по закону не запрещено. Твоя задача — выставить свой «товар» в максимально привлекательном свете, но не злоупотребляй эпитетами. Прогресс не стоит на месте, и люди уже не верят «доброжелателям», обещающим 10 миллионов баксов за неделю. Но на 100 баксов в месяц «ни за шо» клюнут легко. Отличным примером СИ на почве жадности является эпизод, описанный в книге Сидни Шелдона «Интриганка». Аферистка зашла в ювелирную лавку и, всем своим видом выдавая себя за жену расточительного миллиардера, купила не глядя крупный бриллиант за \$150000. Через пару дней вернулась и, взяв хлеб нахваливая покупку, поинтересовалась, нет ли в продаже еще одного столь же крупного экземпляра. Когда продавец заверил, что продал ей очень редкий бриллиант и отыскать подобный во всей стране сложно — мадам заверила, что ее мужу будет не жалко отвалить 400 килобаксов, если только найдется еще один, такой же. После долгих и безрезультатных поисков мужик уже было отчаялся, но тут по объявлению позвонила безутешная вдова, у которой — о чудо — оказался очень похожий камушек. «После смерти Джона у меня остались долги — 300 тысяч зеленых, а еще вот этот бабушкин бриллиант. Я согласна его продать, но только за 300 тысяч. Мне нужна именно эта сумма, чтобы погасить долг». Прикинув, что он все равно выигрывает 100 тысяч, ювелир купил камень. Стоит ли говорить, что бриллиант был тот самый, который он продал за пару недель до этого, и что богатый мадамы разведенный чел больше не видел.

▲ ОТЗЫВЧИВОСТЬ

Когда я использую в СИ этот психоконфлекс, то не испытываю угрызений совести. По той простой причине, что, обманывая, дарю людям возможность лишний раз почувствовать себя людьми, насладиться радостью от по-



мощи ближнему. Крупицы сострадания есть в душе даже самого угрюмого зека. Порешив 15 человек, он нет-нет, да и кинет озябшему воровью крошку хлеба.

Манипулировать отзывчивостью не так просто, как кажется. Хотя и есть она в разных дозах у всех, но воспользоваться ей не всегда возможно. Попробуй на досуге зайти на DALnet'овский #хакер и попросить у тамошнего народа денег на подарок маме. Тебе сразу во всем великолепии русского языка объяснят, что такое сострадание. Но если ты попросишь что-то, с чем человеку расстаться не сильно напряжно, и в то же время убедишь в большой ценности этого для тебя — эффективность использования психоконфлекса весьма высока. В одном из выпусков Спеца, посвященном веб-мошенничеству, я рассказывал, как мне удалось достать книгу, обитающую только на Amazon'e за 20 баксов. Достаточно было связаться с автором — обеспеченной женщиной из Америки, и под видом маленькой девочки, мечтающей стать журналисткой (книга была о freelance writing), слезно попросить прислать книжку. «Thanks so much, Masha! I appreciate your kind words», — ответила женщина на мои слова благодарности — на том и расстались. Слабый (или все-таки прекрасный?) пол вообще очень удобен для этой методики, особенно если будет считать, что в помощи нуждается ребенок. Согласен, играть на материнских чувствах — эгоистично, но СИ — наука сама по себе эгоистичная, и если ты хочешь добиться успеха, то должен забыть свои моральные устои, думая о цели. По отношению к мужикам не менее эффективным будет манипулирование с эротическим подтекстом. Как ты понимаешь, любой молчел намного охотнее поможет красивой девушке, чем патлатому коллеге по полу. Это потому, что на подсознательном уровне мы часто надеемся получить от них ответную благодарность сам знаешь какого плана. Если у тебя есть подружка с ангельским голосом, умеющая разговаривать с парнями многообещающим тоном — она может стать хорошим союзником в процессе обработки заработавшегося юзверя. Чем сильнее ей удастся заинтересовать «клиента», тем меньше он захочет потерять потенциальную герлфрендку и тем вероятнее выполнит ее просьбу.



▲ ПРЕВОСХОДСТВО

Конечно, всем нам хочется быть примером для подражания, разбираться в чем-то лучше других. Превосходство — это состояние, в которое периодически погружает нас наше


подсознание, чтобы дать возможность испытать столь приятное чувство победителя.

Но если в такой момент кто-то со стороны попытается навязать мысль, что ты вовсе не виннер, естественной защитной реакцией будет доказать засранцу — именно ты же бест.

Хитрость в том, что, намеренно ущемив чью-то гордость, синжер может в качестве доказательства виннерства потребовать того, чего в другой ситуации ему никто бы не дал. И жертве, чтобы избавиться от клейма лузера, волей-неволей придется пойти у него на поводу. Методика превосходства сложна тем, что манипулировать ей нужно очень тонко. Грубое «слабо?» действует далеко не на всех — по большей мере на крутых самоуверенных специалистов, которые болезненно относятся к критике своих способностей. Но в мире есть куча людей, которым глубоко плевать, что ты сомневаешься в их некомпетентности, им проще тебя послать, чем что-то доказывать. Это не значит, что тактика против них бесполезна. В таком случае психоконфлекс нужно использовать неявно, в общем контексте (между делом).

Другой вариант — юзать обратную методику. То есть ты не принижаешь способности чела, а наоборот, возвышаешь их до небес. Вспомни, когда последний раз ты что-то делал, и тебя искренне хвалили — какой, мол, молодец. Вероятно, тебе тогда хотелось превзойти самого себя, чтобы услышать еще большую похвалу, и ты продолжал пахать с удвоенным рвением. Благодарность — это признание наших способностей, что очень важно для каждого человека. Играя на людском самолюбии, можно легко заставить человека что-то для тебя сделать. Например, я когда-то таким образом отремонтировал на халяву часы — наемнул часовщику, что у его мастерской авторитет лучшей в городе, что о его профессионализме ходят легенды, а друзья мои считают его очень порядочным человеком. После чего растроганный хозяин богом забытого ларька отказался от денег и, подмигнув, сказал: «Да ладно, пустяки». Так же один мой знакомый взял у соседа-скупердяя машину на сутки — достаточно было расхвалить на все лады его таратайку.

Я кратко описал только 5 наших уязвимостей, на самом деле их намного больше. Имхо любое доступное людям чувство можно использовать в социальной инженерии. Любопытство и зависть, любовь и ненависть, веселье и грусть. Человек всю жизнь испытывает калейдоскоп эмоций, делающих его жизнь ярче, и в то же время подвергающих его опасности стать жертвой синжеров.

Почему-то многие считают СИ исключительно хакерским занятием. Нарыть паролей на халявный анлим, получить доступ к внутренней сети компании... все это действительно решается с помощью СИ, но вне компьютерных рамок лежит бескрайнее море возможностей. Научившись использовать человеческие слабости, ты сможешь выходить победителем из многих сложных ситуаций, добиваться успеха там, где другие только разведут руками. Поэтому учи, практикуйся, дерзай — эта наука не раз тебе пригодится. 



iRiver

the future of entertainment



11600 руб

iRP-120

- HDD MP3-плеер
- Объем памяти 20 Гб
- FM-радио
- Диктофон
- Пульт ДУ с LCD



2100 руб

iMP-50

- CD/MP3 плеер
- Поддержка WMA, ASF и CD
- 9 режимов эквалайзера
- Оригинальный дизайн



2500 руб

iMP-150

- CD/MP3-плеер
- Поддержка ID3-tag
- Поддержка плейлиста WinAmp



4100 руб

iMP-400

- Ультратонкий CD/MP3-плеер
- FM-радио
- Антишок 8 минут
- Стильный дизайн



4500 руб

iMP-550

- Ультратонкий CD/MP3-плеер
- FM-радио
- Антишок 15 минут
- Время работы - до 55 часов

Xitech

он-лайн каталог
сети магазинов

www.xitech.ru

единую
справочную

(095) 748 4458



АСЕЧКА НА БЛЮДЕЧКЕ

Н апишем аськи в наше время никого не удивит. И если раньше владельцы элитных шестизначек почитались, то сейчас это в порядке вещей. Теперь же крутым считается тот, кто имеет как минимум три пятизнака. "А как их получить?" - спросишь ты. Для подгонки пятизнаков необходимо знать некоторые секреты службы ICQ. Ими я и подепюсь с тобой в этой статье.

ЗАНИМАТЕЛЬНЫЕ КОРЯВОСТИ ICQ

К ак и любой сервис, аська имеет свои тонкости. Среди них существуют как баги, так и фишки. Я рассмотрю самые малоизвестные приемы, которые использует ICQ-хакер в своих делах. Будь то заморозка уина или удаленный просмотр паролей.

УГНАТЬ ЗА 60 СЕКУНД

Первый вопрос - как угнать уин? Красивый номерок охота получить всем, поэтому спрос на уины довольно большой и работа по их заполучению идет полным ходом. Давай окунемся в историю жизни Мирабилиса и оценим все способы увода номеров.

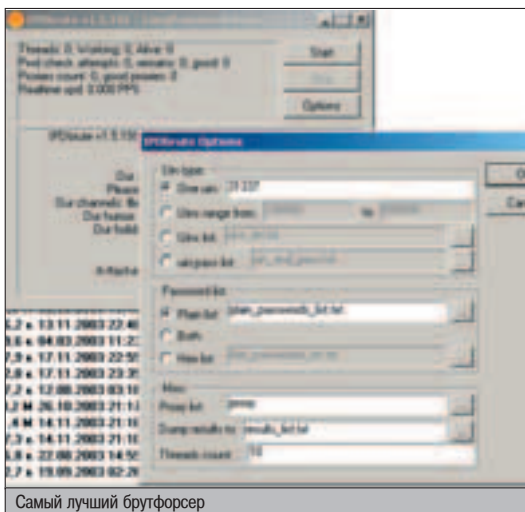
Около двух лет назад украсть уин можно было очень легко. В инет выкладывались разного рода брутфорсеры, которые соединялись с аськой и перебирали пароль. Мирабы просекли недочеты своего творения и сделали gate limit на вход. Иными словами, после 5 неудачных попыток твой IP блокировался на 15 минут. Разумеется, что при таком раскладе перебор выполнить не удастся.

Хакеры не отставали и просекли еще одну вещь. Для смены информации о пользователе предоставлялся вход на web, где он авторизовывался уином и паролем. Здесь пока никаких лимитов на логин не прописывалось, соответственно, можно было выполнить брутфорс. Идею реализовал я сам, но подозреваю, что хакеры уже давно пользовались подобным брутотом, не выкладывая его на публич ресурсы. Когда мне надоело угонять шестизначки, я выложил брутфорс в массы (11.02). Скоро и этот сервис был лимитирован.

Таким образом, брутфорс как метод угона номеров потерял свою силу. Единственная рабочая реализация - потоковый переборщик через проху-серверы. Он выложен в инете и носит имя IPDBrute (download.asechka.ru/download.php?id=33). Минус при его использовании - наличие быстрых прокси-серверов, содержать которые не по карману рядовому юзеру.

Давай рассмотрим и другие методы угона уинов - брутфорс далеко не единственный способ. Номерки благополучно уходят от своих законных пользователей, подвергаясь действиям трояна. Залить коня в наше время - пара пустяков. Почитай багтрак, там ты найдешь кучу брешей в любимом Windows. Две самых популярных ошибки: RPC DCOM и бага в IE 6.0. Обе они подробно описывались на страницах Хакера. Скажу одно - для удаленного просмотра паролей ICQ лучше всего использовать тулзу RecoverPwd2 (www.cobans.net/files/RecoverPwd2.zip). Через командный интерпретатор прога высветит тебе все номера в удобочитаемом виде. Естественно, с паролями ;).

Что касается пятизначек, то их добыть сложнее. Вероятность, что ты подберешь пароль на элитный номер 12345 или 31337 практически отсутствует. Лично я поимел но-



Самый лучший брутфорсер

ИНСТРУМЕНТ ICQ-ХАКЕРА

Предлагаю список популярных программ, которые используют ICQ-хакеры. Все тулзы проверены на вирусы и не представляют опасности для твоего здоровья ;).

ICQPassChanger

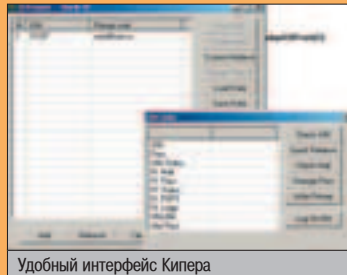
Это, наверное, лучшая утилита для быстрой смены пароля на уин. Сконнектился, сменил и вышел. Помимо паролей, можно поменять primary e-mail и основные детали. К тому же прога поддерживает расшифровку многострочных паролей. Короче, must have! Скачать софтинку можно отсюда: download.asechka.ru/download.php?id=108.

Advanced ICQ Redirecter

Программа умеет редириктировать все входящие сообщения на другой уин. Это бывает очень полезно, когда не хочешь светить свой настоящий номер. Я лично пользовался этой программой и ощутил реальную пользу от нее. Кстати, настройка редириктора очень удобная. Софтина лежит тут: download.asechka.ru/download.php?id=135.

ICQ Keeper

Самая лучшая программа для работы с угнанными уинами. Удобный интерфейс позволяет просматривать, сортировать и удалять инфу о твоих номерах. Софт актуален, если у твоих ног уже разложено внушительное количество номеров. Берется кипер по адресу: download.asechka.ru/download.php?id=121.



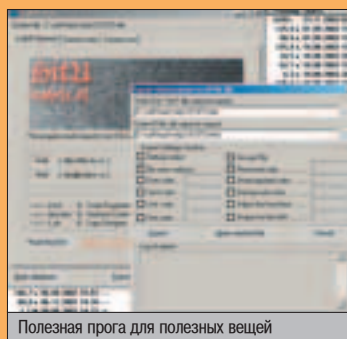
Удобный интерфейс Кипера

IcqHR

Софтина позволяет легко выдирать всю инфу из dat-файла твоей жертвы. Пароль, контакт, хистори, время разговора - все будет оформлено в удобочитаемом html-файле. Достаточно лишь открыть датник и нажать кнопку Export. Сливается она отсюда: download.asechka.ru/download.php?id=63.

DFM

Удобный инструмент для дтекта номеров, находящихся в инвизибле, а также добавления в контакт-лист без авторизации. Конечно, это умеют и некоторые другие клоны асек, но отдельной тулзой пользоваться намного удобнее. Прога обменивается по DDE через Мирабилисовую аську и быстро выполняет требуемые функции. Стянуть DFM можно с родной Асечки: download.asechka.ru/download.php?id=34.



Полезная прога для полезных вещей

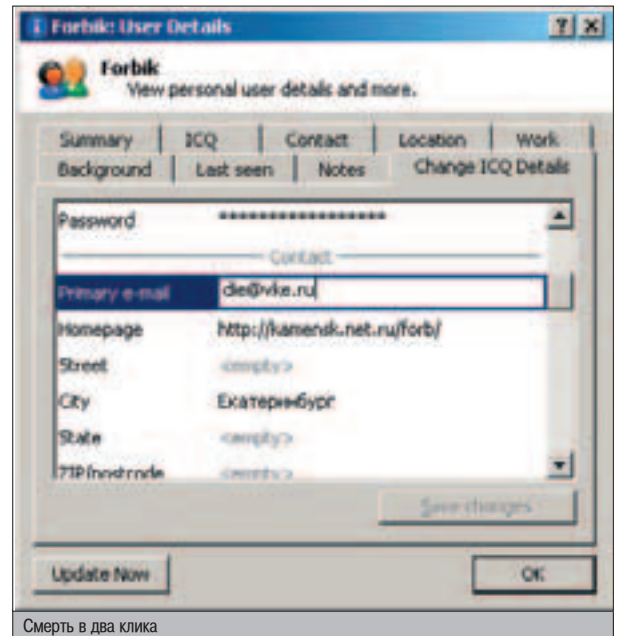
номер 26372, но через некоторое время у меня его угнали. Этого следовало ожидать, т.к. такие номера продаются за неплохие деньги и по неписанному закону охраняются злобными хакерами (или админами ICQ).

▲ ХЛАДНОКРОВНОЕ УБИЙСТВО

Тебе когда-нибудь хотелось насолить другу, дронув его любимый номер? Либо, руководствуясь правилом "ни себе, ни людям", убить элитный шестизнак. Некоторые дума-

ют, что заморозить уин невозможно, но это не так. Существуют целых три способа дропа уинов. Рассмотрим каждый из них:

❶. Роковой e-mail. Мирабилис имеет так называемый черный список e-mail адресов. Номера товарищей, которые по разного рода причинам оказываются в этом списке... правильно! Замораживаются :). Первое время уины вообще дропали из базы, но впоследствии стали просто блокировать. На неопределенный срок ;). Плюсы



Смерть в два клика



ICQ Birthday Trick в работе

этого способа очевидны: заморозка происходит в считанные секунды, а заставить ламера сменить свой прайм на несколько минут довольно несложно.

Заморозке подлежат все номера с мильником в домене @vke.ru. На себе их тестировать не рекомендую - быстро лишишься уина! Когда-то на Асечке попросили прописать этот e-mail в качестве прайма на пару секунд. Как и следовало ожидать, результат оказался трагическим - очень многие лишились красивых 6-знаков и выразили свое неудовольствие в грязной матерной форме ;).

❷. Возрастной критерий. На страницах сайта ICQ написано, что пользоваться услугами сервиса могут лица не моложе 14 лет. Почему бы тебе не прикинуться на время малолеткой? ;) Раньше возраст менялся без проблем, теперь эта операция возможна, если установить утилиту ICQ Birthday Trick (download.asechka.ru/download.php?id=127), которая выполнит поставленную задачу за несколько дней.

Плюсы этого способа: относительная незаметность. Минус: ждать придется несколько дней. Правда, можно и не дожидаться.

❸. Флуд номера. Последним и самым оригинальным способом дропа номера является флуд. Флудить можно различными способами: через ICQ-пейджер, посылать кривые пакеты прямо в ICQ и т.д. Только будь аккуратен: после того, как Мирабы задетектят DoS их сервиса, они прикроют номер. Это проверено практикой. Не убей свой же уин.



▲ Ты не нашел ответ на свой ICQ-вопрос в этой статье? Тогда мысленно - я постараюсь ответить как можно быстрее. Также ты можешь поделиться со мной новыми багами.



▲ Существуют и другие способы нахождения в вечном онлайн. Например, некоторые операторы сотовой связи поддерживают ICQ через SMS. Также ничто тебе не мешает настроить GPRS и поставить на трубу Java-клиент. На худой конец, проснифай протокол и напиши полноценный ICQ-баунсер.

▲ ЗАБЫЛИ ПАРОЛЬ?

Mirabilis следит за своим сервисом и постоянно ужесточает политику. Совсем недавно было сделано нововведение в ретриве пароля на primary-mail. Теперь, чтобы запросить пароль, необходимо ввести не только адрес ящика, но и слово, которое генерируется в браузере как картинка. Таким образом, использование софта, предназначенного для масс-ретрива пароля, полностью утратило смысл. Эта фишка была замечена 20 ноября. Учтывая то, что модулей для расшифровки таких картинок пока не придумано, вопрос о масс-ретриве остается открытым.

▲ ВЕЧНЫЙ ОНЛАЙН

Теперь я расскажу тебе, как сделать твою аську навеки в режиме онлайн. Это возможно, несмотря на то, что ICQ-BNC еще не придумали (по крайней мере, их никогда не выкладывали на публич-источниках). Для решения этой задачи тебе необходимо обзавестись быстрым шеллом и консольной аской. Не смотри на меня косым взглядом - консоль всегда рулила, и ты быстро к этому привыкнешь. Самой удобной аской является mICQ (prdownloads.sourceforge.net/micq/micq-0.4.10.5.tgz). Установив ее на свой шелл и уйдя в скрин.

Скрин - это не снимок экрана, а специальная программа, позволяющая работать приложениям в бэкграунде. После того как ты свалил с шелла, процессы продолжают работать и дожидаться твоего возвращения. Тебе нужно знать всего-навсего две команды:

screen - уйти в screen

screen -r - вернуться в заветанный режим


Плюсы вечного онлайн очевидны. Во-первых, у тебя не угонят номер, видя его активность. Во-вторых, ты быстро и с любого компьютера можешь заюзать собственную асю. И, наконец, тебя будут считать просто продвинутым, т.к. ты юзаешь консольные программы ;).

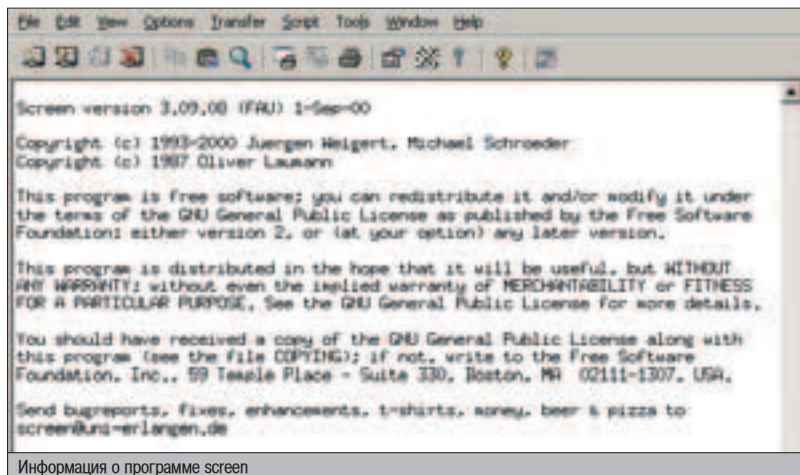
СОБСТВЕННАЯ БЕЗОПАСНОСТЬ

Я не буду тебе говорить, чтобы ты регулярно проверял систему на наличие троянов и ставил сложный неподбираемый пароль на номер. Все это ты уже знаешь. Главное, береги свой primary mail. Выбирай его только на доверенном хостинге, где шансы увода ящика сводятся к нулю.

▲ НА ПОИСКИ

Вот, собственно, и все секреты, которые я хотел тебе поведать. Подобных фишек очень много, но я не стал расписывать поповские способы, как, например, протроянивание ушастого ламера или высылка уина на primary-адрес. Это ты уже знаешь, а если и не знаешь, то можешь про-

читать на многих ресурсах в Сети. Надеюсь, что после прочтения этой статьи ты захочешь узнать больше секретов и полезешь на информационные ресурсы с целью их поиска. И только тогда, когда ты будешь знать чуть больше других, тебя будут считать элитным гуру твоей любимой тети Аси ;). 



Информация о программе screen

ICQ-FAQ

Q: А правда, что пароли на пятизнаки не высылаются на e-mail?

A: Да.

Q: Что будет, если какой-нибудь хакер украдет пятизнак у человека, который его честно купил?

A: В теории - будет зафлужен массовыми атаками хакеров. На практике с таким не встречался ;).

Q: Существует ли софт для отвязки аси от прайма?

A: Нет.

Q: Где можно купить UIN?

A: В различных онлайн-магазинах. К примеру, на www.icqinfo.ru или в форуме на www.asechka.ru.

Q: Что делать, если тебя обманули: деньги забрали, а уин не отдали?

A: Впредь быть внимательнее ;). А ник кидалы сообщить в соответствующий раздел форума на www.asechka.ru. Чтобы nepoBaдHo было.

Q: Действительно ли спасают многострочные пароли?

A: Практически нет. Любой высланный пароль можно просмотреть специальной программой (например, ICQPassChanger). К тому же, если пароль содержит нечитаемые символы, ничто не мешает сгенерировать новый.

Q: Какой самый лучший ICQ-клиент?

A: Я бы рекомендовал Miranda, &RQ или mICQ. Остальные не оправдали моих ожиданий.

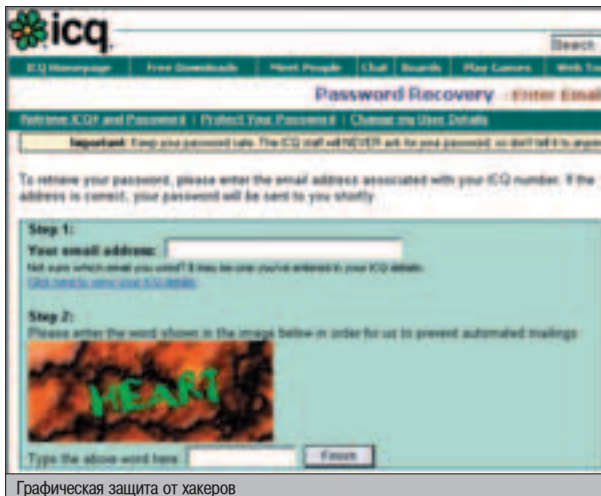


▲ Этот материал готовился на основе форума www.asechka.ru. Если там хорошо покопаться, то можно найти реальную инфу о том, как поиметь красивый номер через новую дырочку в ICQ.



▲ Внимание! Все хакерские приемы описаны только в ознакомительных целях. Ответственность за их применение несешь только ты.

Последним и самым оригинальным способом дропа номера является флуд.



Графическая защита от хакеров



MOD_GZIP <= 1.2.26.14 REMOTE EXPLOIT

ОПИСАНИЕ:

Всем известно, что хороший эксплоит никогда не выкладывается на публич-источник сразу же после его написания. Прежде чем предоставить сишник толпе скрипткидисов, хакеры держат эксплоит за семью печатями и юзают его исключительно в своих личных целях. Так случилось и со сплютом под апачевский mod_gzip. Бага была обнаружена летом. Через банальное переполнение буфера хакер может порождать процессы с правами nobody. Для этого требуется послать определенный контент, включающий параметр Accept-Encoding. Уязвимыми являются практически все Unix-like серверы: FreeBSD, RedHat, Mandrake. Эксплоит снабжен брутфорсом, который каждый раз перебирает адрес возврата. В случае его успешного определения взломщик получает интерактивный шелл.

ЗАЩИТА:

Уязвимыми являются все версии модуля до 1.3.26. На данный момент никаких патчей и свежих версий выпущено не было, поэтому для защиты своей системы собирай модуль в release-режиме (а не в debug, как это делается по умолчанию).

ССЫЛКИ:

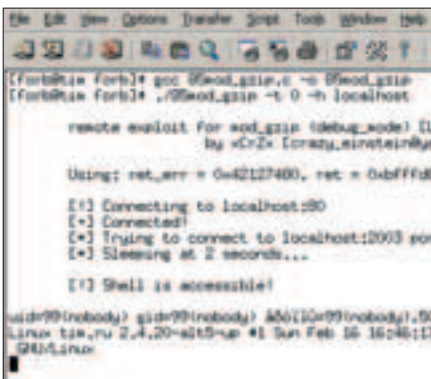
Скачать эксплоит для mod_gzip можно по адресу www.security.nnov.ru/files/85mod_gzip.c. Но перед этим рекомендую почитать подробное описание уязвимости (www.security.nnov.ru/search/document.asp?docid=4638).

ЗАКЛЮЧЕНИЕ:

Несмотря на то, что модуль mod_gzip не так популярен, как mod_php, в инете все равно полно уязвимых web-серверов. Судя сам, эксплоит является удаленным, поэтому задача хакера сводится лишь к простому сканированию Сети и обнаружению дырявого модуля.

GREETS:

Автором вышеописанного эксплоита является xCrZx (crazy_einstein@yahoo.com). Именно он нашел уязвимость и написал для нее сишный эксплоит. Случилось это 5 июня 2003 г.



Шелл за две секунды

UNACE V.2.2 LOCAL EXPLOIT

ОПИСАНИЕ:

Unace - бинарник, позволяющий обрабатывать асе-архивы. Несмотря на непопулярность архиватора, пакет unace устанавливается в систему по умолчанию. И этот архиватор содержит в себе ошибку переполнения буфера. Взломщик может найти нужный адрес возврата и выполнить произвольный код. Так как эксплоит снабжен брутфорсом, отыскать точку возврата не составляет особого труда.

ЗАЩИТА:

Собственно, защищаться не от чего. На /usr/bin/unace не установлен suid-бит. Но стоит быть очень внимательным, т.к. один из методов затроянивания системы - установка суида на обычный бинарник, а затем его эксплуатация. Рекомендую проверить атрибуты этого файла и по возможности вообще его удалить.

ССЫЛКИ:

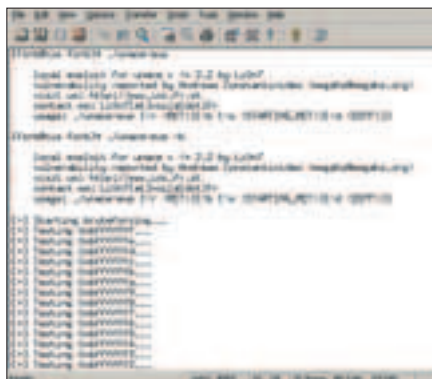
Забирай эксплоит с самого популярного портала безопасности: packetstormsecurity.nl/0311-exploits/unace-exp.c.

ЗАКЛЮЧЕНИЕ:

Как я уже сказал, эксплоит не представляет собой опасности, поэтому паниковать и искать патчи не следует :). Но я бы рекомендовал обновить пакет unace либо вообще отказаться от его использования.

GREETS:

Ошибка в unace обнаружена неким Andreas Constantinides (megahz@megahz.org). А вот эксплоит был выложен чуваком LiOn7. Судя по его мылу (LiOn7@voila.fr), хакер проживает во Франции.



Поиск адреса возврата

WINDOWS WORKSTATION SERVICE REMOTE EXPLOIT

ОПИСАНИЕ:

Опять Windows и опять переполнение буфера. Так уж повелось, что в последнее время стали находить баги в RPC-функциях. Workstation - обязательный сервис, позволяющий обращаться к сетевым ресурсам. В коде этой службы была найдена дырявая подпрограмма. Через один из ее параметров выполняется переполнение буфера, и как результат - запуск произвольного кода с правами администратора. Уязвимы все версии Win2k/XP, а также Win2003. Эксплоит распространяется в виде сишного файла, поэтому применить его возможно только под *nix либо в портированном виде для Windows.

ЗАЩИТА:

Так как сервис сетевой, эксплуатировать систему можно через порты 138, 139 и 445. Их я тебе настоятельно рекомендую прикрыть фаерволом, а также установить патчи, любезно предоставленные Майкрософтом. Саму службу можно отключать лишь в том случае, если компьютер не обращается к сети.

ССЫЛКИ:

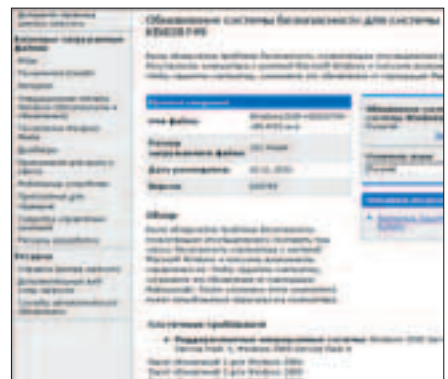
Качаем эксплоит по адресу packetstorm.linuxsecurity.com/0311-exploits/o_wks.c. Прочитать о бреши в Win2000/XP/NET можно здесь: security-lab.ru/41215.html. Патчи берем с официального сайта Microsoft по идентификатору 828749.

ЗАКЛЮЧЕНИЕ:

RPC-эпидемия только назревает, и я совсем не удивился новой ошибке в Windows. Еще немного, и во всех RPC-вызовах будут найдены уязвимости, и никакие патчи нас не спасут ;).

GREETS:

На этот раз отличился snooq (www.angelfire.com/linux/snooq/), выпустив эксплоит с двумя рабочими таргетами, нацеленными на Win2k SP1 и SP4. Для WinXP и Win2003 эксплоит пока не выложен, но он уже вовсю юзается в приватном кругу злобных хакеров ;).



Комплект патчей от Microsoft



ШТИРПИЦ

ОТДЫХАЕТ!



Несмотря на то, что Linux - достаточно безопасная система, криптография в ней играет далеко не последнюю роль. Суди сам, любой, кто имеет физический доступ к компьютеру, может за несколько минут узнать содержимое твоего винчестера. Это может быть кто угодно: ипадший брат, ищущий пароли в инет, или работник службы безопасности. Так вот, чтобы у тебя не было проблем с органами, храни свои данные в сухом и прохладном месте. К чему я клоню: в инете полно тулз, которые позволяют шифровать инфу на жестком диске. Все они выложены на различных сайтах и доступны для скачивания. Если один раз установить подходящую софтинку, уверяю тебя, ты обезопасишь себя от непрошенных гостей.

КРИПТОГРАФИЯ В ЛЮБИМОЙ ОСИ

Файл хорошо, а диск лучше!

Как ты понял, в этом материале я расскажу о лучших криптографических утилитах. Все они заточены под консоль (хакеру не нужен GUI), что делает программы пластичными и удобными. К примеру, кто тебе мешал заинсталлировать тулзу на любимом шелле, который находится в 1000 километров от тебя? На первом месте стоит программа BestCrypt, позволяющая создавать отдельный носитель с шифрацией данных. Эта софтина имеет огромный плюс: ее аналог под Windows полностью совместим с реализацией под пингвин. Поэтому ты можешь безопасно юзать обе оси. Зайди на официальный сайт www.jetico.com и удивись. Сорцы BestCrypt весят в десять раз меньше виндовой реализации, всего каких-то 460 Кб. Поначалу я подумал, что ошибся адресом и качаю совсем не то, что хотел, но мои опасения оказались напрасными. Из зависимостей - необходимо наличие пакета kernel-source, так как прога юзает модули линухового ядра. Далее - три магических слова: ./configure, make, make install. После этого BestCrypt пропишется в качестве системного сервиса, который следует... правильно! за-

пустить :). Делается это командой "service bscrypt start". Скрипт создаст десять блочных устройств, которые отвечают за криптодевайсы. После этого контейнер будет прилинкован к этому девайсу. Естественно, с твоего согласия ;). Прежде чем что-либо линковать, создадим зашифрованный диск. Набирай команду

```
bctool new -s размер -a twofish имя
```

Параметр -a отвечает за алгоритм шифрования. На мой взгляд, самый стойкий из поддерживаемых - это twofish. Что касается размера, он зависит от данных, которые ты собираешься хранить. Если это десять гигабайт порнухи, выставляй большое значение ;), иначе можно обойтись и несколькими мегабайтами. Перед созданием бинарник спросит пароль. Только с его помощью можно примонтировать девайс, поэтому опреде-

лись с выбором. Создал? Отлично! Теперь нужно определить файловую систему в твоем девайсе. Пусть это будет vfat. Командуй:

```
bctool format -t vfat name
```

и вводи пароль. Теперь файловая система определена, и можно перейти к следующему шагу - монтирование устройства. Делается это также одной командой:

```
bctool mount -t vfat имя /path/to/mountpoint
```

Последний параметр указывает путь к точке монтирования. Замонтируем раздел в директории /mnt/secure. Вообще, значение этого параметра напрямую зависит от твоей паранойи. Я встречал людей, которые монтируют диск в /lib/secure. Поздравляю, теперь ты в безопасности (относительной, ко-

Надежность шифрования прямо пропорциональна длине пароля.

```

les
Module bc_idea loaded, with warnings
Using /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_idea.o
Warning: loading /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_idea.o will
taint the kernel: no license
  See http://www.tux.org/linux/#export-tainted for information about tainted modu
les
Module bc_idea loaded, with warnings
Using /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_r1jn.o
Warning: loading /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_r1jn.o will
taint the kernel: no license
  See http://www.tux.org/linux/#export-tainted for information about tainted modu
les
Module bc_r1jn loaded, with warnings
Using /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_cast.o
Warning: loading /lib/modules/2.4.20-alt5-up/kernel/drivers/block/bc_cast.o will
taint the kernel: no license
  See http://www.tux.org/linux/#export-tainted for information about tainted modu
les
Module bc_cast loaded, with warnings

[root@lin forb]# bctool new -s 500000 -a twofish ./secure
Enter password:
Verify password:
[root@lin forb]# bctool format -t vfat ./secure
Enter password:
Kasha: Password incorrect
[root@lin forb]# bctool format -t vfat ./secure
Enter password:
mkfs_vfat 2.8 (28 Feb 2001)
[root@lin forb]#

```

Создаем новый контейнер

Помни, что любые пароли выбиваются из жертвы ударами сапог ;), поэтому абсолютной безопасности не существует.

нечно). Не зная пароль, увидеть инфу на носителе практически невозможно. Но помни, что любые пароли выбиваются из жертвы ударами сапог ;), поэтому абсолютной безопасности не существует.

ШИФРУЕМ ФАЙЛ

Быает так, что целый диск создавать нецелесообразно. Нужно лишь зашифровать отдельный файл. В Linux для этого существует множество средств, которые ты можешь заюзать, исходя из ситуации. Рассмотрим простой вариант шифрования. Допустим, тебе необходимо закриптовать простой ASCII-файл. Причем на стойкость шифрования можно забыть. Тебе подойдет обычная программа для зашифровки, такая, как, например, Code (последняя версия 0.03). Суть ее - генерация непостоянного ключа на основе двух символов, который замещается символом в файле. Первый из них - часть твоего

пароля, второй - истинный фрагмент файла. Надежность шифрования прямо пропорциональна длине пароля. В установке Code нет ничего сложного. Правда, разработчики забыли снабдить пакет скриптами для make. Чтобы скомпилировать программу, нужно набрать две команды в директории gus или eng (в зависимости от желаемой локализации):

```

# gcc code.c -o code
# gcc unicode.c -o unicode

```

А затем заюзать шифровальщик. К примеру, закрипуем /etc/passwd. Для этого введем следующую строку:

```

# ./code /etc/passwd myp4ssw0rd

```

В текущем каталоге появится файл `passwd.code`, который является свежескриптованным. Вернуть его в прежнее состояние можно обратной командой:

```

# ./unicode ./passwd.code myp4ssw0rd

```

Только вот имя файла будет другим - `passwd.code.unicode` :).

БИНАРНЫЙ ШИФР

Теперь обратим внимание на шифрование бинарных файлов. Для этого я выделяю

```

[root@lin eng]# gcc code.c -o code
[root@lin eng]# gcc unicode.c -o unicode
[root@lin eng]# ./code ./file 123
warning: no newline at end of file
[root@lin eng]# ./unicode ./file.123
[root@lin eng]# ./code ./file.123
Error: I can't open file "123"
[root@lin eng]# ./code ./file.123
[root@lin eng]# ./unicode ./file.code.123
[root@lin eng]#

```

Использование утилиты code

У BestCrypt существует замечательная опция `unlock`, которая помогает в случае, когда система не была корректно размонтирована. Если не анлокнуть контейнер от девайса, повторный маунт осуществить не получится.

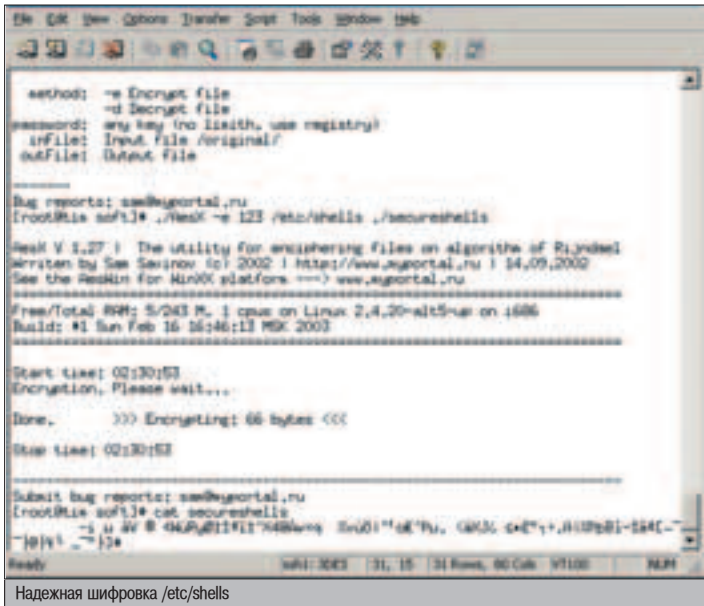
(game)land



ЛЮБИШЬ
КИНО?
СМОТРИШЬ
DVD?
ИНТЕРЕСУЕШЬСЯ
ТЕННИКОУ?

ЧИТАЮ
TOTAL
DVD

каждый номер
с фильмом



Надежная шифровка /etc/shells

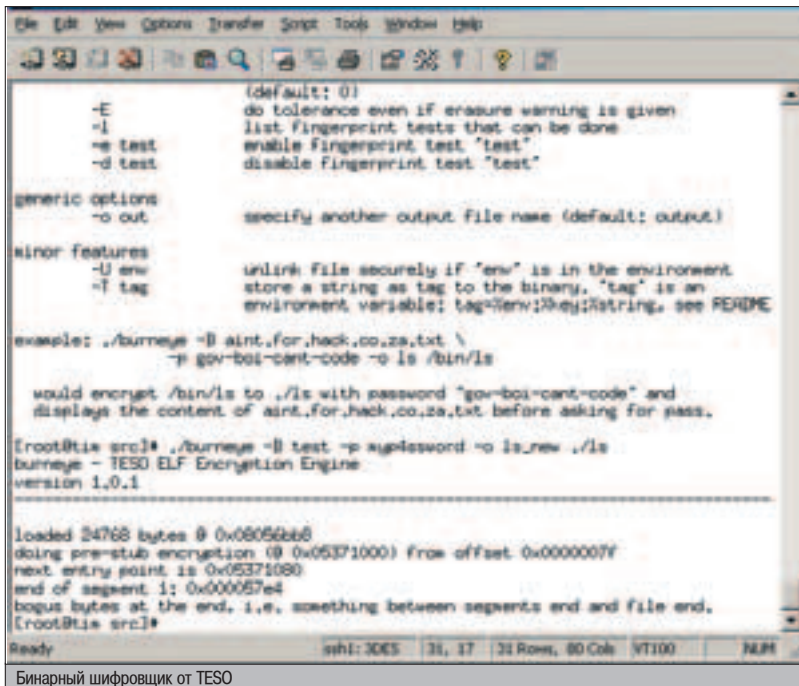
программу AesX, которая имеет более стойкий алгоритм шифрования Rijndael. Утилита весит около 100 килобайт и устанавливается без особых сложностей. В использовании она крайне проста: в качестве параметров бинарнику передается пароль, имя входного и выходного файла, а также один из двух параметров: -d (шифрование) и -e (расшифровка). Таким образом, запустить эту консольную тулзу сможет даже маленький ребенок. Минус AesX - шифрованные файлы никак нельзя

запустить. Перед этим их нужно расшифровать в прежнюю форму. Чтобы можно было стартовать файл с предварительным запросом пароля, используйте тулзу от TESO. Ее имя - burneye.

Burneye - программа, которая модифицирует ELF-структуру файла и добавляет в бинарник посторонний код. Этот код позволяет расшифровать содержимое бинарника на основании заданного пароля. Вообще, у программы очень много полезных параметров, на которые хотелось бы обратить внимание. Установка тулзы проста - нужно зайти в папку src и скомандовать make. После этого ты получаешь рабочий бинарник утилиты. Запускай его, и ты увидишь подробный хелп по использованию программы. Наиболее интересными опциями являются -В и -Р. Первая записывает заголовок, который будет отображаться перед вводом пароля. Вторая позволяет поместить пароль в переменную окружения "env". Она будет просматриваться после запуска зашифрованного файла. Сам файл передается отдельной (последней) опцией, а выходной бинарник через параметр -o. Если внимательно изучить help, то все окажется очень просто.

Итак, ты хочешь запустить зашифрованный файл. После его старта ты увидишь нечто подобное:

• Может так случиться, что потребуется передать зашифрованный файл в обычной форме. Например, в форме картинки или звука.



Бинарный шифровщик от TESO

```
# ./crypt
Secure file
Enter password: xxxxxx
Blah-blah-blah
```

В качестве баннера был задан текстовый документ, который содержит строку "Secure file". Как видишь, баннер отобразился перед запросом пароля. Очевидно, что вернуть закриптованный файл в прежнее состояние нельзя, это, пожалуй, единственный минус burneye.

ПИНГВИННАЯ СТЕГАНОГРАФИЯ

Может так случиться, что потребуется передать зашифрованный файл в обычной форме. Например, в форме картинки или звука. Этим занимается такая наука, как стеганография. Ее принципы подробно описывались в 10 номере журнала. Давай посмотрим, существуют ли в Linux тулзы для организации стеганографии.

Практика показала, что программы существуют. Более того, есть даже консольные варианты софта. На мой взгляд, самым лучшим шифровальщиком является утилита Steghide, позволяющая упаковывать посторонние данные в графические и музыкальные файлы. Перед установкой убедись, что ты имеешь рабочую библиотеку libjpeg. В противном случае бери ее с сайта www.iijg.org, либо с нашего диска. Затем тебе потребуется установить пакеты Mcrypt (mcrypt.sourceforge.net) и Mhash (mhash.sourceforge.net). Когда все пакеты будут установлены, можешь переходить к инсталлу Steghide. После команды `make install`, выполненной в корне архива, произошла ругань на отсутствие файла, и установка была завершена. Пришлось перейти в каталог `src/` и набрать `make install` там. После этого утилита успешно скомпилилась. Оставалось изучить ее основные параметры.

Как оказалось, для действия определяется одна из двух опций: `--extract` и `--embed`. У меня была картинка `girl.jpg`, и я хотел вставить в нее файл `./secure`. Для этого потребовалось выполнить команду:

```
./usr/local/bin/steghide --embed --coverfile ./girl.jpg --embedfile ./secure -p myp4ssw0rd -sf ./girl2.jpg
```

Все опции представлены наглядно, поэтому ты без труда разберешься в синтаксисе. В каталоге появилось изображение `girl2.jpg`, которое на первый взгляд ничем не отличалось от оригинала. Но следующая строка может выделить из него секретный документ:

```
./usr/local/bin/steghide --extract -x ./secure -p 1111 -sf ./girl2.jpg
```

Можешь поэкспериментировать и со звуком - это весьма занятно. К сожалению, на текущий момент программа поддерживает лишь wav-файлы, но разработчики обещают в скором будущем подружить steghide и с mp3-форматом.

КРИПТОГРАФИЯ ПРАВИТ МИРОМ!

Мы рассмотрели основной спектр утилит, которые могут помочь тебе в шифровании данных. Конечно, непробиваемой защиты не существует, но использование вышеописанных софтин на порядок повысит твою безопасность, что гарантирует тебе спокойный сон и стул :).

ULTRA
100.5FM

Лицензия РВ№4794 выдана 27 ноября 2000 года МПТР



TM RADIO ULTRA

КУРС ВЫЖИВАНИЯ В КОНСОЛИ

Иногда я попробую угадать, как сейчас выпадет твой рабочий стол. Тэкс... Модный диспетчер окон, антипьясные шрифты, иконки с www.kdelook.org, прозрачные терминалки, gkrellm в правом углу, ну и, конечно же, полуоубаженная девица с томным взглядом в качестве обоев. Что, в десятку? И неумудрено - сейчас именно так выглядит подавляющее большинство юниксоидных десктопов. Стоит отметить, что благодаря графическим оболочкам начался настоящий бум юниксов, который продолжается и сейчас. Но речь в этой статье пойдет совсем о других оболочках - оболочках командной строки, грамотно используя преимущества которых, ты сможешь выделиться из общей массы, почувствуешь истинную мощь *nix и в разы повысишь свои программистские навыки!

ИЗУЧАЕМ КОМАНДНЫЙ ИНТЕРПРЕТАТОР ZSH

ШЕПШ ШЕПШУ РОЗНЬ

БШелл ака командный интерпретатор - это программа, выполняющая без предварительной компиляции вводимые пользователем команды либо сценарии (скрипты), состоящие из набора последовательных команд. Основоположниками оболочек были Стефен Бурн (Stephen R. Bourne) - создатель Bourne Shell (sh) и Уильям Джой (William N. Joy), разработавший C Shell (csh) в университете Беркли специально для версии BSD UNIX. За тридцать с лишним лет существования UNIX-систем было написано огромное количество различных

интерпретаторов командной строки. Все они работают примерно одинаково для большинства базовых действий и команд, а основные различия проявляются только в процессе работы. Это сделано для того, чтобы пользователи без особого труда могли переходить от использования одного шелла к другому. В современных дистрибутивах можно встретить такие оболочки, как ash, bash, csh, pdksh (общедоступная реализация Korn Shell), sash, tcsh и zsh. Разработка большинства из них происходит крайне медленно и сводится, как правило, к залатыванию дыр различного радиуса :).

ОДА ZSHELL'У

Zsh - это один из самых новых и быстроразвивающихся командных интерпретаторов с полностью программным интерфейсом (все, что есть в оболочке, может быть настроено по усмотрению пользователя), имеющий множество интересных возможностей. Изначально создаваемый как интерпретатор, совместимый с оболочкой Корна, zsh аккумулирует в себе все лучшее, что есть в bash, ksh и tcsh.

Ниже перечислю некоторые свойства и преимущества zsh по сравнению с другими оболочками:

- расширенное редактирование командной строки;
- настраиваемое автодополнение команд, опций, сообщений, map-страниц, доменных имен и чего душе угодно;
- улучшенное раскрытие имен файлов;
- хешированные каталоги;
- проверка правописания;
- множественные перенаправления (команду tee можно больше не использовать);
- гибкая работа с массивами (включая обратное индексирование);
- большие возможности по решению задач целочисленной арифметики;
- число встроенных команд примерно равно суммарному размеру команд в bash, ksh и tcsh;
- модульная архитектура.

Этот список можно продолжать еще очень долго. Я уже не говорю про такие свойства, которые являются общими для bash, ksh и tcsh: управление заданиями, история введенных пользователем команд, биндинг клавиш, периодические события, работа с псевдонимами команд и конвейерами. Со всеми этими задачами также прекрасно справляется zsh.



- ▲ <http://zsh.sunsite.dk/>
- ▲ www.faqs.org/faqs/unix-faq/shell/zsh/
- ▲ www.acm.uiuc.edu/workshops/zsh/toc.html
- ▲ <http://adamspiers.org/computing/zsh/>
- ▲ <http://frebsd.by.ru/refs/zsh00.html>
- ▲ <http://linuxshop.ru/unix4all/?cid=26&id=209>
- ▲ www.daemonnews.org/199910/zsh.html
- ▲ <http://zsh.sourceforge.net/Guide/zshguide.html>
- ▲ <http://www-106.ibm.com/developerworks/library/l-z.html>

ЗАЧЕМ НАМ НУЖНЫ ОБОЛОЧКИ?

Анализируя и выполняя вводимые с терминала команды, оболочка предоставляет пользователю колоссальные возможности для взаимодействия с операционной системой. Такие функции оболочки, как управление потоками ввода/вывода, раскрытие и дополнение имен файлов, обеспечение доступа к ранее выполненным командам, управление заданиями, выполнение циклов и условных переходов позволяют существенно повысить эффективность работы.



УКРОЩЕНИЕ СТРОПИВОВОГО

Забираем с одного из многочисленных мейнфреймов архив с последней (на момент написания статьи 4.1.1) версией zsh. Несмотря на то, что эта версия относится к ветке devel и предназначена для разработчиков (а значит, имеет самые новые и вкусные фишки), она достаточно стабильна в работе и полностью готова к применению.

```
$ wget ftp://ftp.fu-berlin.de/pub/unix/shells/zsh/zsh-4.1.1.tar.gz
```

Распаковываем и переходим в созданный каталог:

```
$ tar xzvf zsh-4.1.1.tar.gz
$ cd zsh-4.1.1/
```

К процессу инсталляции zsh можно подойти с разных сторон. Первый путь предельно прост - особо не задумываясь, положить на работу конфигурационный скрипт:

```
$ ./configure
```

Второй способ установки заключается в статической компоновке с совместно используемыми библиотеками (такая линковка необходима для работы программ в chroot()-ных средах) командной оболочки с подключением встроенных средств борьбы с утечками памяти:

```
$ env LDFLAGS="-static" ./configure --enable-zsh-mem --enable-zsh-secure-free --disable-dynamic
```

зова exes запускать программы и осуществлять перенаправление вывода в файлы.

```
$ ./configure --disable-lfs --disable-locale --disable-restricted-r
```

Если же в системе вместо архаичного mbox'a используется почтовый формат Maildir, то не забудь скрипту configure передать дополнительный аргумент "--enable-maildir-support".

Далее компилируем и растасовываем свежесобравшиеся бинарики по файловой системе:

```
$ make
# make install
```

Абсолютный путь до zsh прописываем в конце файла /etc/shells, где содержится список доступных в системе командных оболочек:

```
# echo "/usr/local/bin/zsh" >> /etc/shells
```

После внесения этого изменения у пользователей появится возможность командой chsh изменить свой стандартный командный интерпретатор на zsh:

```
$ chsh
```

```
Shell: /usr/local/bin/zsh
Full Name: Andrushock
```

ЧУДЕСА ХАРДКОРНОГО ТВИКИНГА

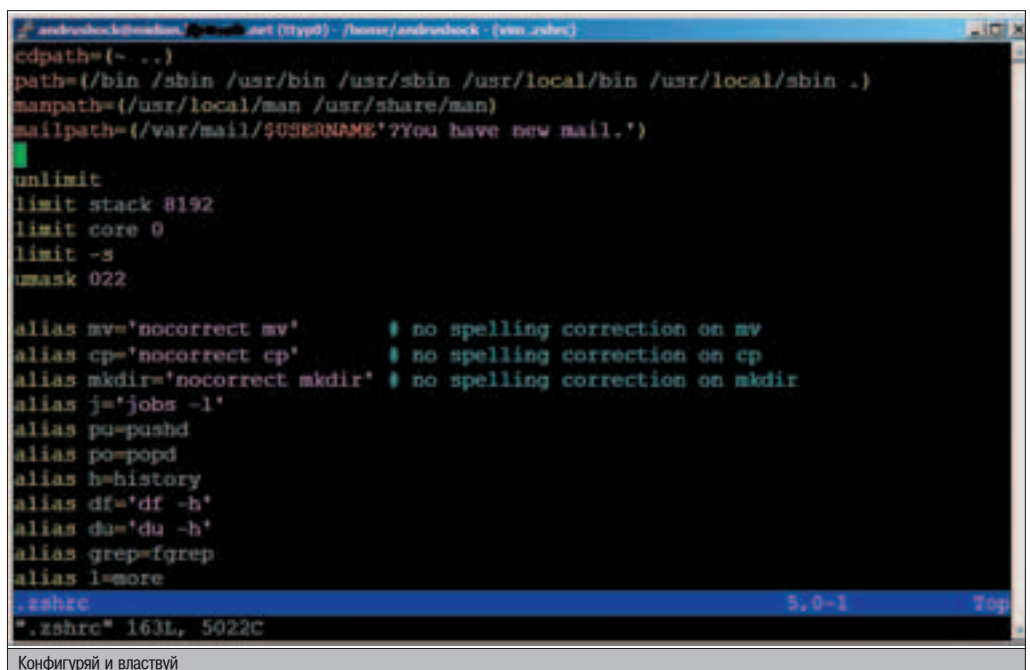
При запуске zsh пытается прочитать более десяти своих конфигурационных файлов. Такое обилие не случайно - все сделано для чрезвычайно гибкой настройки интерактивных и неинтерактивных шеллов, а также для большей совместимости с bash и tcsh. Не волнуйся, мы обойдемся написанием всего лишь одного конфига:

```
$ vi ~/.zshrc
```

Следующие переменные содержат списки каталогов, которые будут использованы обо-



▲ Вот так можно перечитать конфиг zsh: ". ~/.zshrc".
▲ Будь осторожен с псевдонимами вида "alias rr='rm -rf'".



Конфигурай и властвуй

А КАК РАБОТАТЬ СО СТЕКОМ КАТАЛОГОВ?

Командой `pushd` текущий каталог помещается на вершину стека, командой `popd` самый верхний каталог извлекается из стека, и в него производится переход, а с помощью команды `dirs` можно вывести иерархию каталогов.

лочкой при поиске команд для выполнения (точка в массиве `path` означает текущий рабочий каталог):

```
cdpath=(- .)
fpath=(${fpath} ~/zfunc)
path=(/bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin)
manpath=(/usr/local/man /usr/share/man)
```

Указываем путь до почтового ящика в формате `mbox`:

```
mailpath=(/var/mail/${USERNAME}?You have new spam, Master!)
```

Удаляем из перечисленных массивов повторяющиеся пути:

```
typeset -U path cdpath fpath manpath
```

Используем жесткие лимиты на все параметры, кроме размера стека, и не даем размножаться коркам в нашей файловой системе:

```
unlimit
limit stack 8192
limit core 0
limit -s
```

Определяем права доступа (в данном случае 0755), которые будут автоматически назначаться файлу при его создании:

```
umask 022
```

Особо параноидальные товарищи могут задуматься о значении `umask 077`, когда только владелец файла имеет право на чтение и запись.

ВО ВЛАСТИ ПЕРЕМЕННЫХ

Для управления средой командного интерпретатора и корректной работы внешних программ определяем необходимые значения переменных окружения:

```
BLOCKSIZE=k
TERM=xterm-color
TZ=Europe/Moscow
CVS_RSH=/usr/bin/ssh
CVSROOT=anoncvs@anoncvs1.ca.openbsd.org/cvs
```

Как видишь, перед каждой переменной писать команду `export` совсем не обязательно. Мелочь, а приятно.

Настроить среду и поведение оболочки также можно с помощью специальных переменных, значения которых изменяются встроенными командами `setopt` и `unsetopt`:

```
setopt autcd ignoreeof histignoredups histignorespace
```

`autcd` - отказываемся от использования команды "cd". Это может быть удобным при большой многовложенности каталогов. Например, чтобы вернуться на три директории вверх, достаточно набрать `"../..../"`; `ignoreeof` - не закрываем терминал по сочетанию клавиш `Ctrl+D` (выходим, только используя команду `exit`); `histignoredups` и `histignorespace` - избавляемся от пробелов и дубликатов в истории команд.

СКАЖИТЕ, ЭТО ВАШЕ НАСТОЯЩЕЕ ИМЯ?

Псевдонимы (алиасы) - очень удобное свойство оболочек, при грамотном использова-

нии которого можно существенно минимизировать объем введенных команд и рутинных процедур:

```
alias j='jobs -l'
alias h='history M'
alias o='bg; fg %-'
```

Элегантно подсчитываем использование дискового пространства:

```
alias duh="du -h -l | grep -v '!/' | sort -n"
```

Корректно завершаем сеанс работы:

```
alias exit='sync; sync; clear; exit'
```

Частенько бывает лениво расставлять пробелы, верно? :)

```
alias psaux='ps -aux M'
```

Ты, наверное, заметил, что в двух примерах участвовала магическая буква `M`. Это не оцепятка, а одна из фишек `zsh` под названием «глобальный псевдоним», работу которого лучше всего объяснить на примере. При установке большого числа программ порядком надоедает вводить одну и ту же команду:

```
$ ./configure --help | more
```

Но после определения глобального псевдонима

```
alias -g M='help | more'
```

литера `M` становится равнозначной команде `'help | more'`, и теперь можно использовать вот такой формат записи:

```
$ ./configure M
```

ТАВ'У НА !!

`Zsh` выгодно отличается от своих конкурентов потрясающей системой автодополнения, правила которой можно настроить и запрограммировать по своему усмотрению в зависимости от контекста. Но для начала рассмотрим стандартные возможности оболочки:

```
autoload -U compinit
compinit
```

Вот теперь есть где разгуляться. Не хватает автодополнения хостов? Пожалуйста:

```
compctl -k "( www.xakep.ru www.openbsd.org www.zsh.org)" ping
```

Теперь после набора в командной строке


```
$ ping www.x-Tab>
```

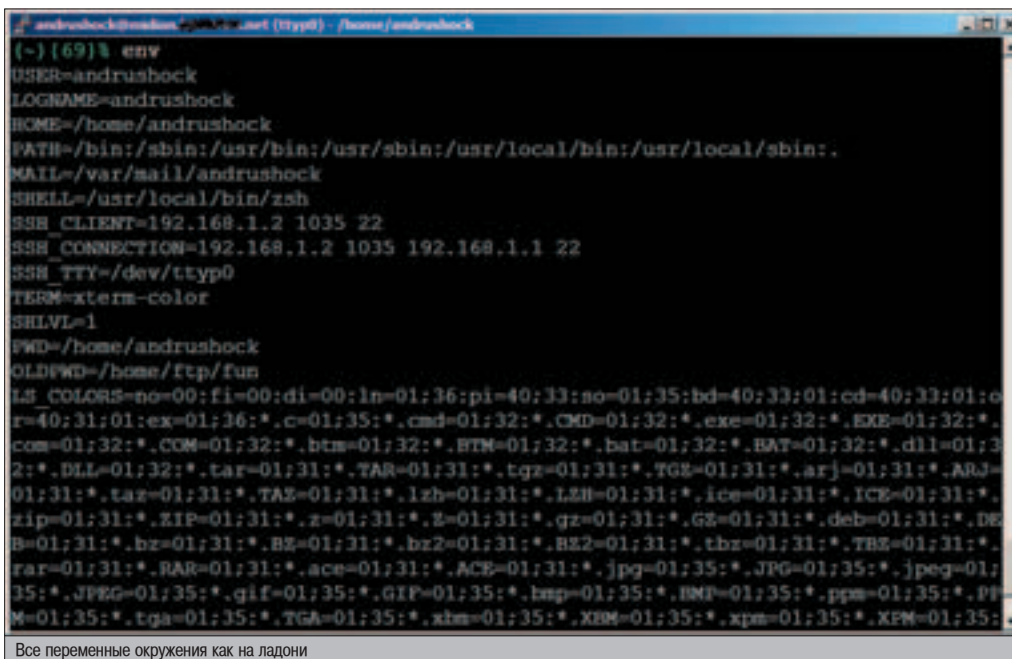
имя хоста закомплитится до `www.xakep.ru`.

Тебе нужно автодополнение пользовательских процессов?

```
zstyle ':completion:' processes' command 'ps -au${USER}'
```

Хочешь автодополнение аргументов программ?

-  Текущая стабильная версия `zsh` 4.0.7.
- Текущая версия `zsh` для разработчиков 4.1.1.
- В интерактивном режиме работы оболочка передает управление пользователю.
- Оболочка переходит в неначальный (порожденный) интерактивный режим, если она запущена из другой оболочки (или из самой себя).
- Неинтерактивный сеанс оболочки используется для запуска сценариев.
- Существует два вида программирования оболочек: Bourne и `ssh`.



Все переменные окружения как на ладони

```
compile=(check clean cleandir depend install obj)
compctl -k compile make
```

Линуксоиды могут смело помещать в этот массив аргументы `dep`, `mrproper`, `menuconfig`, `modules`, `modules_install`.

Кстати, тебе не надоело, что `bash`, выполняющая автодополнение при соседстве одноименных подкаталогов и файлов, откровенно тупит и показывает листинг каталога, в котором они находятся? Избавляемся от этого раз и навсегда! К примеру, с помощью `"compctl -g"` делаем привязку mp3-файлов к музыкальным проигрывателям:

```
compctl -g "*"$(mp3|MP3)" + -g "*"(-/)"$(/)" mp3123 xmms
```

Теперь на команду

```
$ mp3123 foobar<Tab>
```

оболочка больше никогда не побеспокоит тебя одноименными директориями и закомплитит только файлы с расширением mp3.

Еще одна приятная фишка - автодополнение с подсказкой. Здесь происходит вывод возможных опций заданной команды с их кратким описанием:

```
$ tar<Tab>
tar function
A -- append to an archive
c -- create a new archive
f -- specify archive file or device
```

Работает и автодополнение опций (-на и -pr как по волшебству превращаются в -name и -print):

```
$ find / -na<Tab> 'foobar' -pr<Tab>
```

Нельзя не рассказать и о раскрытии путей при их сокращенном наборе:

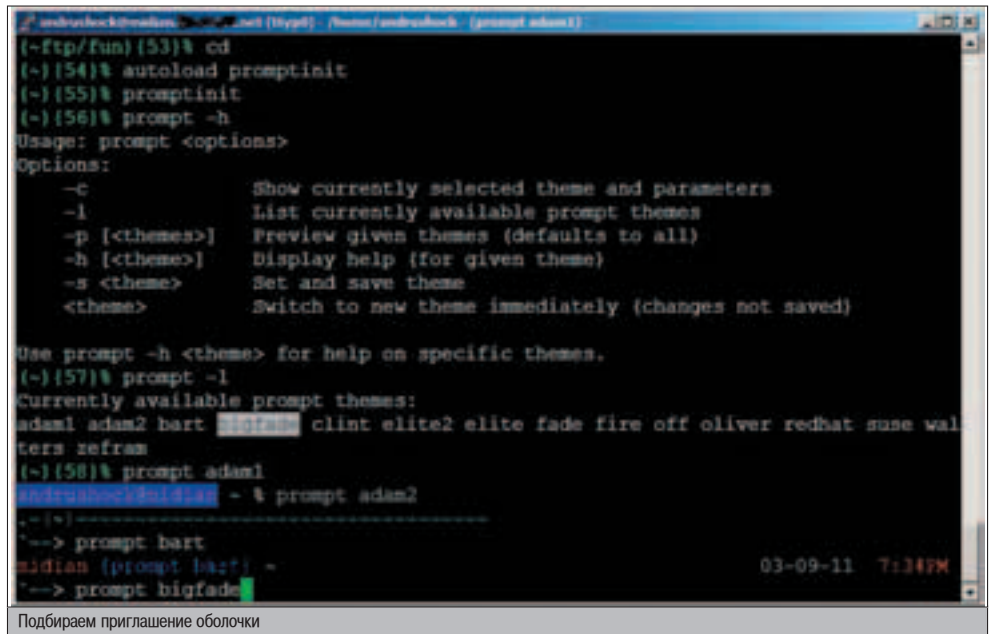
```
$ cd /u/p/au/la<Tab>
```

При нажатии после последнего символа клавиши `Tab`, команда автоматически дополнится до:

```
$ cd /usr/ports/audio/lame/
```

НА ВЕЧЕРИНКУ БЕЗ ПРИГЛАШЕНИЯ?

Без сомнения, особое внимание нужно уделить разработке приглашения командного интерпретатора. Грамотный промпт позволит избежать постоянного ввода дополнительных команд (например, `rwd`, чтобы выяснить текущий каталог), сэкономит драгоценное место в командной строке и позволит вывести на экран дополнительную информацию. Если у тебя нет шелл-аккаунтов, или ты вообще сидишь без Сети, то нет никакого смысла держать в приглашении имя



Подбираем приглашение оболочки

хоста, на котором запущена оболочка. Запись типа `"localhost"` абсолютно ничего не дает, она только уменьшает твою командную строку на девять символов. Далее имя пользователя. В большинстве случаев можно обойтись и без него. Эта фишка может быть полезна, если ты регистрируешься на многочисленных удаленных узлах и всегда под разными именами. Согласись, такое бывает совсем не часто. Поэтому достаточно отображать значок \$ или % во время сеанса обычного юзера и решетку # во время сеанса суперпользователя. Лично я в круглые скобки заключаю текущую директорию, а в фигурные - текущую команду буфера истории. Возможно, на первый взгляд следующая строка покажется тебе абракадаброй, но на самом деле это довольно симпатичное и информативное приглашение зеленого цвета:

```
$ PROMPT=$ECHO
'%B%{\033[32m%}(%-)%%}#%{\033[37m%} '
(~src){139}%

Не хватает часиков? С помощью перемен-
ной RRPROMPT можно задать правую часть
приглашения оболочки:

$ RRPROMPT='[%T]'

(~src){140}% [12:40]
```

В арсенале `zsh` есть еще одно грозное оружие - поддержка тем для приглашений (`themeable prompts`). После подгрузки во время сеанса работы модуля `promptinit`, тебе станут доступны сразу 15 различных видов приглашения командной строки:

```
$ autoload promptinit
```

```
$ promptinit
```

Выводим список встроенных тем и устанавливаем понравившуюся:

```
$ prompt -l
Currently available prompt themes:
adam1 adam2 bart bigfade clint elite2 elite fade fire off oliver redhat suse wal-
ters zefram
```

```
$ prompt clint
[Thu 03/09/11 19:36 MSD][p0][i386/openbsd3.3/3.3/4.1.]
<andrushock@midian:>
zsh 63 %
```

ДЕКОРИРОВАНИЕ ОКОН

Если ты просто жить не можешь без имени пользователя и хоста, то их можно вынести в `caption` окна терминалки или `telnet/ssh` клиента вот таким нехитрым способом:

```
case $TERM in
xterm*)
precmd () {
print -Pn "%033]0:%n@%M (%y) - %/a"
print -Pn "%033]1:%n@%m (tty%l)a"
}
preexec () {
print -Pn "%033]0:%n@%M (%y) - %/ - (S1)a"
print -Pn "%033]1:%n@%m (tty%l)a"
}
}
esac
```

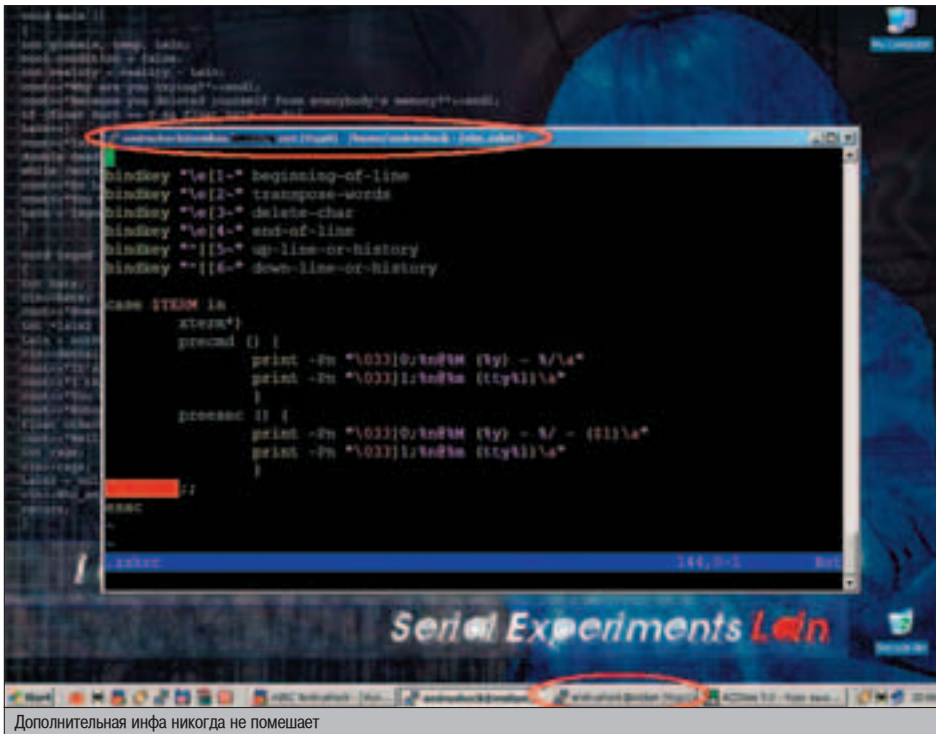
Теперь перед выполнением каждой команды и перед сменой каталога данные в заголовке окна будут изменяться на: `"имя_пользователь@полное_имя_хоста (терминал) - текущий_каталог - (выполняемая_команда)"`. При сворачивании окна инфо будет отображаться в сжатом виде: `"имя_пользователь@хост (терминал)"`.

ЗАБИДИМ ВСЕ ОТ Я ДО Я

Для редактирования командной строки можно не только использовать комбинации клавиш `vi` и `emacs`, но и устанавливать собственные сочетания. Даже если ты постоянно воркаешь в `vi/vim`, я рекомендую обратить пристальное внимание на `emacs`'овские

ЗАЧЕМ НУЖНО ИСПОЛЬЗОВАТЬ СЦЕНАРИИ ОБОЛОЧЕК?

Сценарий представляет собой файл, содержащий последовательность команд для оболочки. Как правило, сценарии применяются для того, чтобы не повторять ввод одной и той же последовательности команд.



Дополнительная инфа никогда не помешает

биндинги, так как именно благодаря им работать в консоли станет гораздо комфортнее. Но об этом чуть позже, а пока:

```
bindkey -e
```

Следующие записи помогут восстановить работу клавиш Insert, Delete, Home, End, Page Up и Page Down в некоторых терминалах:

```
bindkey "\e[1~" beginning-of-line
bindkey "\e[2~" transpose-words
bindkey "\e[3~" delete-char
bindkey "\e[4~" end-of-line
bindkey "\e[[5~" up-line-or-history
bindkey "\e[[6~" down-line-or-history
```

ПОДЧИНЯЕМ КОНСОЛЬ

Если ты до сих пор перемещаешься по командной строке, используя стрелки влево и вправо, то тогда я понимаю, почему ты тихо ненавидишь консоль и с нескрываемым удивлением поглядываешь на юниксоидов. Фокус заключается в том, что существует несколько комбинаций клавиш, заметно облегчающих передвижение в консоли. Только изучив их, ты сможешь эффективно управляться с командной строкой:

- Ctrl+a - перемещает курсор в начало строки;
- Ctrl+e - перемещает курсор в конец строки;
- Ctrl+f - перемещает курсор на один символ вперед;
- Ctrl+b - перемещает курсор на один символ назад;
- Alt+f - перемещает курсор на одно слово вперед;
- Alt+b - перемещает курсор на одно слово назад;
- Ctrl+k - удаляет часть строки от курсора до конца;
- Ctrl+w - удаляет часть строки от курсора до начала;
- Ctrl+u - удаляет всю строку;
- Ctrl+l - очищает экран.

НИКОГДА НЕ ПЮБИЛ ИСТОРИЮ

Для того чтобы каждая введенная в оболочке команда сохранялась в списке выполненных команд, нужно задать следующие переменные окружения:

```
HISTFILE=~/.zhistory
HISTSIZE=1024
SAVEHIST=1024
```

Я предпочитаю с каждой сессией создавать новую историю команд:
HISTFILE=/dev/null

Существует целый набор встроенных программ и псевдонимов для работы с историей выполненных команд. Приведу часть из них:

- \$ h (псевдоним) - посмотреть историю команд;
- \$ fc -l 1 10 - посмотреть историю команд с первой по десятую;
- \$ fc 2 - отредактировать вторую введенную команду;
- \$!! - повторить последнюю команду (на сленге bang-bang);
- \$!12 - выполнить 12-ую команду из буфера истории;
- \$!p - выполнить из буфера команду, начинающуюся на букву "p".

Работать с историей команд можно с помощью следующих комбинаций клавиш:

- Ctrl+r (стрелка вверх) - поиск в обратном направлении;
- Ctrl+n (стрелка вниз) - поиск в прямом направлении;
- Atl+< - переход к первой команде в буфере истории;
- Atl+> - переход к последней команде в буфере истории.

НАУЧИТЕ МЕНЯ ПИСАТЬ БЕЗ ОШИБОК

С помощью проверки правописания можно скорректировать ошибки при написании ко-

ПРИМЕР АВТОДОПОЛНЕНИЯ ДЛЯ СПРАВОЧНЫХ СТРАНИЦ

```
man_glob () {
local a
read -c a
if [[ $a[2] = [0-9]* ]] then
reply=( $*manpath/manSa[2]/S1*S2(N:tr) )
else
reply=( $*manpath/man*/S1*S2(N:tr) )
fi
}

compctl -K man_glob man
```

манд, имен файлов и даже опций. Подключаем автокоррекцию:

```
$ setopt CORRECT
```

Теперь попробуем сознательно допустить ошибку:

```
$ suod ls -alF
zsh: correct 'suod' to 'sudo' [nyae]?
```

Не нравится появившееся сообщение об ошибке? Меняем!

```
$ SPROMPT='zsh: correct "%R" to "%r" ?
((Y)es/(N)o/[E]dit/[A]bort) '
```

```
% suod ls -alF
zsh: correct suod to sudo ? ((Y)es/(N)o/[E]dit/[A]bort) y
```

Стоит отметить, что командой посоггест разработчики предусмотрели своеобразный откат от этой опции, чтобы предотвратить автоматическую коррекцию аргументов для некоторых утилит:

```
alias mv='nocorrect mv'
alias cp='nocorrect cp'
alias mkdir='nocorrect mkdir'
```

ХЕШИРУЕМ ПОМАПЕНЬКУ

Именованные каталоги чем-то напоминают символические ссылки. Если в системе есть несколько труднодоступных каталогов, к которым тебе нужно периодически обращаться, то эта специфическая возможность оболочки просто создана для тебя:

```
hash -d ftp=/home/ftp
hash -d src=/home/root/src
hash -d www=/var/www/htdocs
```

Теперь вместо команды

```
$ cd /var/www/htdocs
```

можно использовать своеобразную закладку:

```
$ cd -www
```

ПРИМЕР ШЕЛЛ-КОДИНГА

Ни для кого не секрет, что в *BSD присутствует несколько обрезанная версия программы kill, которая позволяет оперировать только идентификаторами процессов. А что

нам мешает самим написать небольшую функцию, способную восполнить этот серьезный пробел?

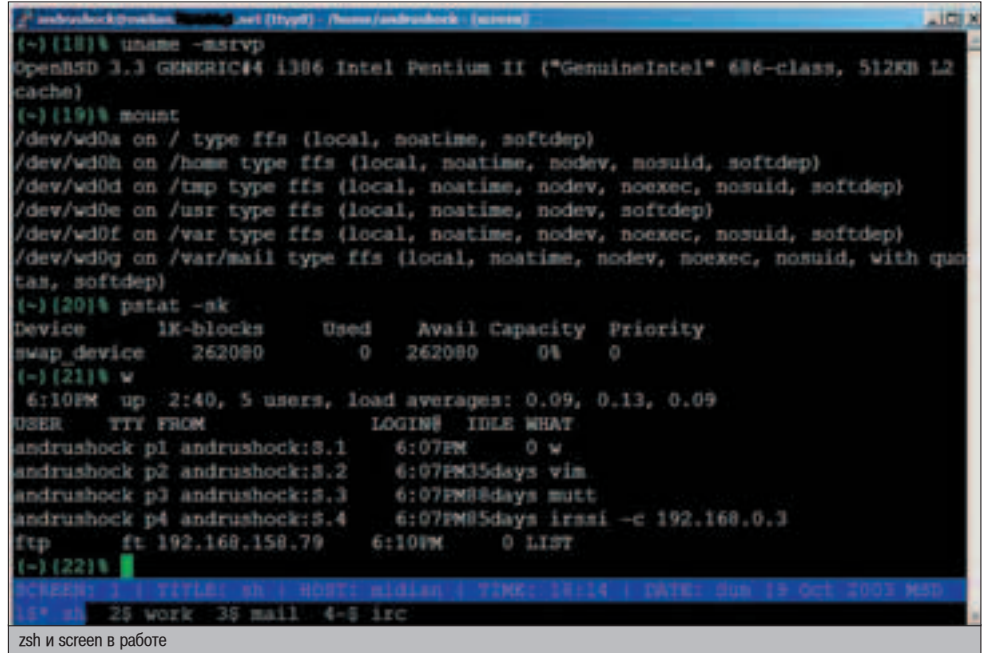
```
pskill()
{
    local pid
    pid=$(ps -aux | grep $1 | grep -v grep | awk '{ print $2 }')
    echo -n "Killing '$1' (process $pid)..."
    kill -9 $pid
    echo " done."
}
```

Вуаля. Теперь можно работать и с именами:

```
# pskill silc
Killing 'silc' (process 26812)... done.
```

ПОСТСКРИПТУМЫ

Как видишь, zsh разве что крестиком вышивать еще не научился. Галопом по европам я постарался рассказать о наиболее интересных и заслуживающих внимания свойствах этого уникального командного интерпретатора. К сожалению, информации об этой оболочке в Сети крайне мало, поэтому для домашнего чтения могу только посоветовать солидную справочную страницу zshall(1), руководство пользователя "Zsh Guide" и статьи Алексея Федорчука, посвященные zsh.



FORCE COMPUTERS

300 МОДЕЛЕЙ НОУТБУКОВ
150 моделей на витринах

RB Voyager E415L
 OS-1000MHz / 128Mb DDR / 30GB SATA
 CD-ROM / SB / 128 / 64 Mb DDR Video
 LAN / 100 / Modem / 56k / 14" TFT 1024x768

НОУТБУК в кредит \$66 / \$662

В ПОДАРОК ПРИ ПОКУПКЕ НОУТБУКА
ОПТИЧЕСКАЯ МЫШЬ LOGITECH

СЕТЬ САЛОНОВ

- ТАГАНСКАЯ (кв. 14 мкн.) Б. КАМЕНЩИК, 21/8
- БЕЛОРУССКАЯ (кв. 2 мкн.) ЛЕНИНГРАДСКИЙ ПР-Т, 2
- ВДНХ (новый выезд) (3 мкн.) ЗВЕЗДНЫЙ БУЛЬВАР, 10
- НОВЫЕ ЧЕРЕМУШКИ (5 мкн.) АРХИТЕКТОРА ВАСОВА, 18

www.forcescomp.ru
интернет-магазин

единая справочная служба
775-6655

256 Mb DDR PC-2100
 40 Gb UDMA-133 7200 rpm
 CD-ROM 54x MULTIRAM
 SOUND CARD 5.1
 64 Mb DDR GeForce4 FX 4x
 ATX 300W

МОНИТОР В КОМПЛЕКТЕ
ROLSSEN 17"
1600x1200x75Hz TCO99

2.6 Ghz в кредит \$38 / \$385
 INTEL® Celeron® 128 cache

256 Mb DDR PC-2700
 80 Gb UDMA-133 7200 rpm
 CD-ROM 54x MULTIRAM
 SOUND CARD 5.1
 128 Mb DDR GeForce4 FX 4x
 ATX 300W

МОНИТОР В КОМПЛЕКТЕ
ROLSSEN 17"
ИЛИ • 117 \$ ТРТ-ПАНЕЛЬ
1600x1200x75Hz TCO99

2.8 Ghz в кредит \$50 / \$495
 INTEL® Celeron® 128 cache

256 Mb DDR PC-2700
 80 Gb UDMA-133 7200 rpm
 CD-ROM 54x + 8 DVD-ROM
 SOUND CARD 5.1
 128 Mb DDR GeForce4 FX 4x
 ATX 300W

МОНИТОР В КОМПЛЕКТЕ
SAMSUNG 17"
С ПЛОСКИМ ЭКРАНОМ
1280x1024x60Hz TCO99

2.8 Ghz в кредит \$62 / \$625
 INTEL® PENTIUM® 4 810 cache

ЦЕНЫ НА 19.12.03

БЕСПЛАТНЫЙ КРЕДИТ

0% ДО ПЛАТА **10% первый взнос**

БЕЗ КОМИССИИ

ПОДАРОК ВСЕМ

БЕСПЛАТНО

ЦВЕТНОЙ ЦИФРОВАЯ АКУСТИЧЕСКАЯ
 ПРИНТЕР КАМЕРА СИСТЕМА

Предложение действительно с 06.01.04 по 26.01.04

ЛУЧШЕЕ ЦЕНЫ НА ВСЕ ТОВАРЫ

250 \$ 40 \$ 110 \$ 5 \$

TFT-ПАНЕЛЬ СКАНЕР 17" CRT-МОНИТОР DVD-UPGRADE

3000 наименований товара | ГАРАНТИЯ 2 ГОДА | ЗАМЕНА ТОВАРА 2 в течение 1 к. недели | СКИДКИ до 15% | ДОСТАВКА БЕСПЛАТНО | МОБИЛЬНЫЙ СЕРВИС БЕСПЛАТНЫЙ ВЪЕЗД | ДИСКОНТНАЯ НАКОПИТЕЛЬНАЯ КАРТА | ЗАКАЗ ПО ТЕЛЕФОНУ | ИНДИВИДУАЛЬНАЯ КОНФИГУРАЦИЯ | СООТВЕТСТВИЕ СТАНДАРТАМ PC



ОСЕЛ

НА СЛУЖБЕ

ЛЮДЕЙ

Есть у моей любимой корпорации MS одна черта – каждый их продукт просто обязан быть лучшим в своем классе. Таким, чтобы стороннему разработчику никогда не захотелось сделать свой браузер, текстовый редактор или медиаплеер. Конечно, они знают, что невозможно порадовать всех людей сразу. И все равно - решение было найдено в продуманной системе управления и кастомизации существующих приложений. Не нравится IE? Пожалуйста, напиши свой! На его ядре. MyIE тому пример. Не нравится интерфейс? Измени. Но ядро, как говорится, оставь.

IE ДЛЯ ПРОГРАММИСТА

Сегодня я решил всерьез заняться осликом. Разрабатывать мы его будем по двум направлениям: создание своего браузера на ядре IE и модернизация интерфейса с помощью Delphi. Собственно говоря, создавать свой эксплорер особого смысла нет - обозревателей существует огромное количество, и каждый из них пытается отвоювать свою нишу: fastest, easiest, smallest browser in the world and galaxy. Однако и у нормального человека может появиться потребность работать с html в своей проге. Так что для любителей всего своего существует компонент TWebBrowser (закладка Internet). Многие думают, что он полностью написан товарищами из Borland и просто призван обеспечить каждого дельфиста своим браузером. На самом деле, этот компонент всего лишь использует элемент управления ActiveX "WebBrowser", который входит в состав MS IE (вернее, теперь уже во все поставки виндов). Отсюда вывод - твоя прога, написанная с помощью этого компонента, и есть IE. Со всеми его достоинствами, недостатками и директорией "Temporaguy Internet Files" лично. Поэтому когда я слышу,

что чей-то такой браузер защищеннее/быстрее/надежнее IE, я сильно удивляюсь. Правда, некоторый выигреш в скорости можно получить за счет обрезания интерфейса, но не более того. Итог - для создания полноценного обозревателя от тебя требуется лишь интерфейс и набор команд. Собственно, так и сделан довольно популярный MyIE.

Вторым путем будет работа с самим IE. Ты наверняка заметил, что многие проги любят добавлять свои кнопки на Toolbar ослика (тот же FlashGet, например), работать с Favorites и чинить непотребства с пунктами меню. Например, проги-шедулеры могут запрещать IE в определенное время качать файлы или, скажем, вообще отключить возможность закрытия его окна. Таким образом, прочтение этой статьи вполне может превратить тебя в злобного офисного тирана :).

▲ СДЕЛАЙ САМ

Нам понадобится примерно следующее: собственно TWebBrowser из закладки "internet", Toolbar из закладки "Win32", один Edit, один ImageList, одно MainMenu и одна кнопка. На тулбаре сразу создавай не менее 7 кнопок, а в ImageList загрузи иконки, которые мы свяжем с этими батонами (картинки

можешь взять на диске либо самостоятельно поковыряться в shdocvw.dll/shdoclc.dll).

После небольших косметических обработок, а именно - изменения свойства Toolbar1 "images" на имя ImageList, выставления caption'a кнопки в ">>>>" и создания главного меню, у меня получилось довольно жалкое подобие оригинального ослика. Результат смотри на рисунках 1-2.

Больше на интерфейсе я останавливаться не буду, перейдем сразу к работе. Первая кнопка, располагающаяся слева от строки адреса, будет играть роль ИЕшной "GO", поэтому ее OnClick:

```
WebBrowser1.Navigate(edit1.Text);
```

Вроде бы все просто - нажал и вылетел на нужную страницу. На самом деле, у этого метода есть целая куча параметров (Flags, TargetFrameName, postData, Headers). В реальности же приходится использовать только несколько из них:

navOpenInNewWindow - открывать в новом окне.

navNoHistory - не добавлять эту страницу в истории.



СТР.90

КОДИМ СОКЕТЫ НА MFC

Пишем бесконечные сетевые крестики-нолики при помощи MFC класса CSocket.



СТР.94

ПАРСИМ ПРОСТОРЫ XML

Программируем свой модуль для перевода XML данных в MySQL и обратно.



navNoReadFromCache - не использовать чтение из кэша.

navNoWriteToCache - не записывать ничего в кэш.

navAllowAutosearch - разрешать автопоиск, если ничего не найдено (помнишь перебор .com, .mil, .edu и все остальное? Ох, как это многих бесит :)).

Хотя, если тебе надо передать на сервер, например, содержимое формы с помощью POST, тебе пригодится и postData.

Например, вызов `WebBrowser1.Navigate('www.hacker.ru', navNoHistory)`; приведет к тому, что ни одна живая душа не узнает о твоём посещении сайта `www.hacker.ru` в рабочее время ;).

Теперь самое время взглянуть на toolbar. Там нет ничего сложного, онкlickи большинства кнопок ты найдешь в таблице.

СПИСОК КНОПОК

Кнопка "Назад" - обработчик `OnClick - WebBrowser1.GoBack`;

Кнопка "Вперед" - обработчик `OnClick - WebBrowser1.GoForward`;

Кнопка "Стоп" - обработчик `OnClick - WebBrowser1.Stop`;

Кнопка "Refresh" - обработчик `OnClick - WebBrowser1.Refresh`;

Кнопка "Home" - обработчик `OnClick - WebBrowser1.GoHome`;

Вот, собственно, и все их короткие `OnClick`'и. Так им и надо. А мы сейчас займемся более интересными вещами: печать, поиск и сохранение страницы. Самый простой способ печати (он же `OnClick` кнопки "Print") выглядит так:

```
WebBrowser1.ExecWB(OLECMDID_PRINT,OLECMDEXEPT_DODEFAULT);
```

Метод "ExecWB" вообще довольно неплохая вещь. В сущности, он представляет собой один из способов обращения к интерфейсу `IOleCommandTarget` (об этом подробнее ты можешь почитать на `msdn`):

```
procedure ExecWB(cmdID: OLECMDID; cmdexcopt: OLECMDEXEPT; var pvalIn: OleVariant; var pvaOut: OleVariant); overload;
```

Здесь `cmdID` - команда. Вот что она может делать:

OLECMDID_SAVEAS - вызывает диалог "сохранить как".

OLECMDID_PRINTPREVIEW - вызывает предпросмотр перед печатью.

OLECMDID_FIND - открывает стандартный виндовый диалог "поиск файлов и папок".

OLECMDID_PROPERTIES - выводит "свойства страницы".

`Cmdexcopt` - способ выполнения. Может принимать значения:

OLECMDEXEPT_DODEFAULT - выполнять с настройками по умолчанию.

OLECMDEXEPT_PROMPTUSER - сначала спрашивать у пользователя, потом выполнять. Например, вывести диалог "Save As...".

OLECMDEXEPT_DONTPROMPTUSER - выполнять, не спрашивая юзера.

OLECMDEXEPT_SHOWHELP - просто вывести хелп о команде.

Остальные параметры особого значения не имеют, правда, надо помнить, что не все команды могут поддерживаться. Чтобы получить список доступных, воспользуйся методом `QueryStatusWB`.

Далее я решил создать главное меню для своего браузера. С помощью `TMainMenu` я создал "файл" и "сервис". В меню "файл" из-за моей лени поместилось только "сохранить как" и "автономно", поэтому давай выжжем в обработчиках их онкlickов соответственно:

```
WebBrowser1.ExecWB(OLECMDID_SAVEAS, OLECMDEXEPT_DODEFAULT); - сохранение
```

```
IF N4.Checked then webbrowser1.offline:= false else webbrowser1.offline:= true; - погнупк "Автономно"
```

Вот, собственно, и все, что касается создания своего ослика. Он уже умеет довольно много, а после прочтения стандартного дельфийского хелпа и `MSDN` тебе откроются все возможности для создания своего `opera-killer'a`.

МОДЕРНИЗИРУЕМ ИНТЕРФЕЙС

Существует лишь небольшое количество компонентов, заточенных под управление IE. В принципе, это правильно - довольно глупо пи-

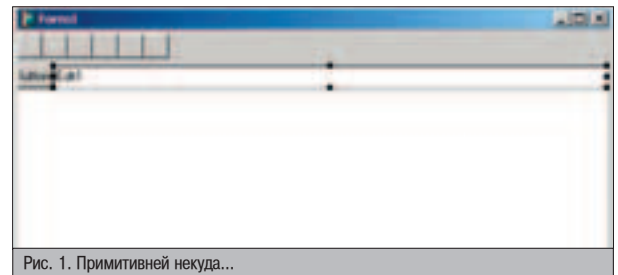


Рис. 1. Примитивней некуда...

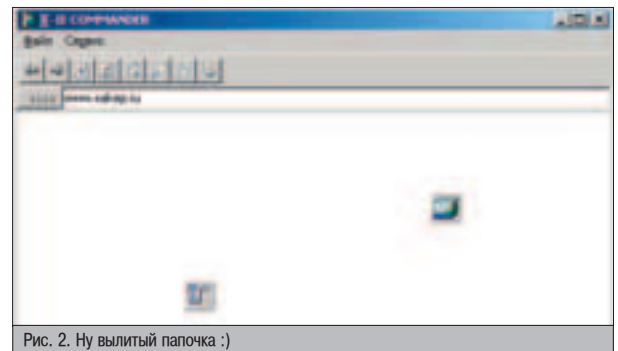
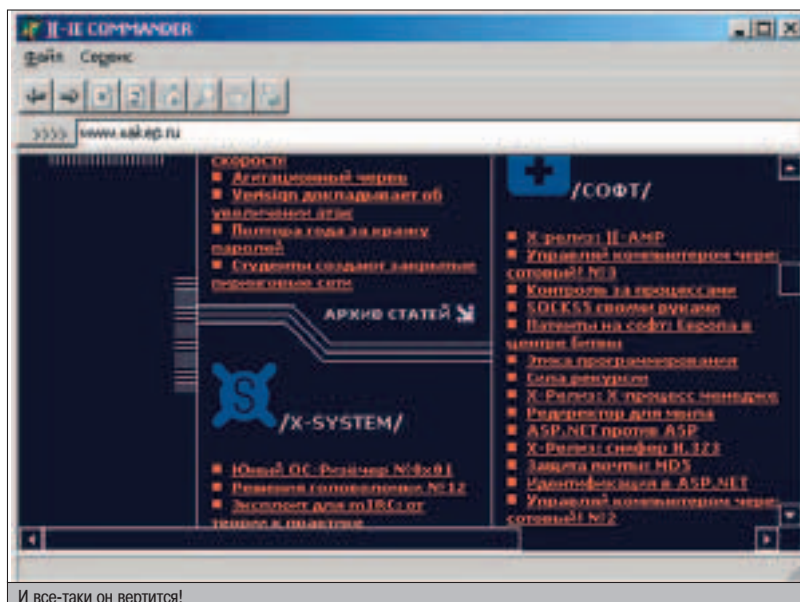


Рис. 2. Ну вылитый папочка :)

сать компоненты, помогающие программисту насиловать чужую прогу. Такие вещи надо уметь делать самому. Несмотря на это, на диске ты можешь найти файл "IE5tools.pas", содержащий в себе очень много полезных функций для работы с IE. Заглянув в его недра, ты узнаешь, какие ключи реестра надо редактировать и какие команды отдавать, чтобы добиться нужного результата. А пока я познакомлю тебя с некоторыми функциями:

Прочтение этой статьи вполне может превратить тебя в злобного офисного тирана :).



И все-таки он вертится!

ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

PC Games



\$79.99

\$75.99

\$79.99

\$79.99



Star Wars: Knights of the Old Republic



XIII



Final Fantasy XI



Max Payne 2: The Fall of Max Payne

\$59.99

\$29.99

\$15.99

\$59.99



Star Wars Galaxies Pre-Paid Game Card



Grand Theft Auto: Vice City



WarCraft III: The Frozen Throne



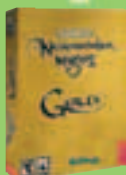
Sid Meier's Civilization III: Conquests

\$75.99

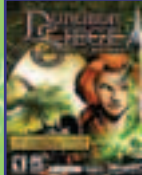
\$69.99

\$79.99

\$89.99



Neverwinter Nights Gold Edition



Dungeon Siege: Legends of Aranna



Halo: Combat Evolved



Microsoft Flight Simulator 2004: A Century of Flight

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

WWW.GAMEPOST.RU

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

e-shop
http://www.e-shop.ru

ЖУРНАЛ
ХИКЕР

GAMEPOST

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

ФУНКЦИИ ДЛЯ ДОМАШНЕГО ТИРАНА :)

3ти полезности отключают активные по умолчанию функции IE. Очень полезны, например, для работодателя, желающего ограничить доступ своих подчиненных к развлекухе.

DisableFavorites(Disabled: Boolean) - отключает "избранное".

DisableFileMenu(Disabled: Boolean) - удаляет меню "File".

DisableSaveAs(Disabled: Boolean) - отключает "сохранить как".

DisableClose(Disabled: Boolean) - запрещает пользователю закрывать IE. Я имею в виду неподвижного пользователя :).

DisableContextMenu(Disabled: Boolean) - отключает контекстное меню для правой кнопки. Хорошо работает в связке с 3 функцией.

DisableDownload(Disabled: Boolean) - запрещает качать файлы. Правильно, трафик не резиновый! Особенно весело, если фаервол запрещает доступ в Сеть всему остальному.

DisableOptions(Disabled: Boolean) - запрещает выводить "Свойства". Для более тонкой настройки существуют функции DisableGeneralTab, DisableSecurityTab.

function AddExplorerBar(Title, Url: string; BarSize: Int64; Vertical: Boolean): string;

AddExplorerBar добавляет новую панель обозревателя. Параметры:

Title - заголовок для представления ее в View->Explorer Bars.

Url - html'ка, которая будет в ней высвечиваться.

BarSize - размер в пикселах. Обычно - 220/50 или 190/40.

Vertical - если TRUE, то панель будет вертикальна, FALSE - горизонтальна.

Удаляется ExplorerBar с помощью функции RemoveExplorerBar. Ей достаточно передать Title существующей панели. Функция возвращает true в случае успеха.

function AddToolBarBtn(Visible: Boolean; ConnType: TConnType; BtnText, HotIcon, Icon, GuidOrPath: string): string;

AddToolBarBtn запикивает твою кнопку на Toolbar ослика. Очень нужная функция, и ей пользуются многие проги. Эта кнопка может запускать не только исполняемый файл, но и скрипт. Вот ее значения:

Visible - если true, то кнопка видима.

ConnType:

COM_OBJECT - если кнопка содержит Com Object.

EXECUTABLE - если кнопка запускает программу.

EXPLORER_BAR - запуск explorer bar.

SCRIPT - выполнения скрипта.

BtnText - Caption для кнопки.

HotIcon - путь иконки для ВЫДЕЛЕННОЙ кнопки.

Icon - то же самое, но для затененной.

GuidOrPath - для COM_OBJECT или EXPLORER_BAR. Guid для зарегистрированного COM-объекта или ExplorerBar. Ну а если EXECUTABLE или SCRIPT, то извольте указать полный путь к программе или скрипту.

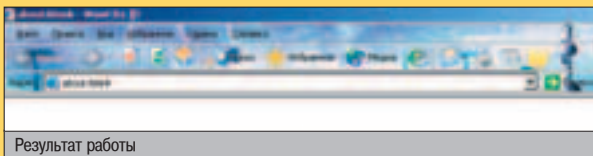
Бороться с существующей кнопкой можно при помощи функции RemoveToolBarBtn, которой достаточно передать один параметр BtnText.

function AddMenuItem(ConnType: TConnType; MenuText, StatusBarText, GuidOrPath: string; HelpMenu: Boolean): string

BACK-BITMAP ДЛЯ ОСПА

С помощью этой процедуры ты можешь изменить back-bitmap ослика. Все сводится к простому изменению ключей реестра, поэтому не забудь добавить в код "uses registry":

```
var
  reg: TRegistry;
begin
  Reg := TRegistry.Create;
  with Reg do try
    RootKey := HKEY_CURRENT_USER;
    OpenKey("Software\Microsoft\Internet Explorer\Toolbar", True);
    if OpenDialog.Execute then
      WriteString("BackBitmap\ES", OpenDialog.FileName)
    else CloseKey;
  Reg.Free;
  Except //По вашему желанию ;);
end;
end;
```



Эта функция добавляет новый пункт меню. Какие здесь параметры:

ConnType - как и в предыдущей функции.

MenuText - имя пункта меню. Например, "format c:".


StatusBarText - текст, который будет отражаться в Statusbar при наведении мышки на этот пункт. Например, "Выбери этот пункт и молись".

GuidOrPath - смотри предыдущую функцию.

HelpMenu - если TRUE, то добавляем в меню Help, наоборот - в Tools. Третьего, к сожалению, не дано.

RemoveMenuItem позволяет убить пункт меню по одному единственному аргументу -MenuText. Очень суровая функция.

FINITA LA COMEDIA

С точки зрения программиста, IE не так уж плох. Да, он тяжелый, слегка тормозной и сильно глючный. Зато он всегда готов удовлетворить самые изощренные желания пользователя, при этом осел красив и бесплатен. А что еще нужно настоящему американцу? Только msdn.microsoft.com/workshop/browser/ext/overview/overview.asp как источник дополнительной информации, delphi как язык программирования и голова как генератор идей. Кстати, я все еще жду твоих супертворений, а особенно - их интерфейсов. Самые интересные мы будем выкладывать на hacker.ru в назидание всем. Так что если ты сделал интерфейс, по которому я мог бы учить своего сына кодингу - не скрывай его от людей. Время на его изготовление еще есть, поскольку сына у меня, кажется, пока нет :). 

TIPS & TRICKS

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

Для того чтобы постоянно не принимать горы спама, я выработал у себя привычку просматривать предварительно заголовки писем. По темам и обратным адресам легко можно отличить, что спам, а что нет. Соответственно, ненужное можно сразу удалить на сервере, не принимая. Те письма, которые вызывают сомнения, можно и принять, но это, слава богу, единичные случаи. Единственная проблема: The Bat! и MS Outlook очень медленно работают с заголовками (особенно The Bat!), поэтому лучше взять для этого специализированную програ. Подобрать такую программу себе по вкусу можно, например, здесь: <http://ftp.cityline.ru/mailcheck.html>.

GamerX
gamerx@inbox.ru



ABIT
Your Reliable Partner

μGURU?
Это второй процессор на вашей плате

A17-GURU
ABIT



KV8-MAX3

- Поддержка Intel® CPU нового поколения
- OC Guru: Разгон под управлением Windows
- ABIT Black Box: on-line тех. поддержка
- ABIT Audio EQ: управление звуком
- ABIT Fan EQ: управление вентиляторами
- Поддержка Технологии Intel® Hyper-Threading
- 4 Dual DDR 400 / 4 SATA 150 RAID / AGP 8X
- 10/100 LAN / 8x USB 2.0 / IEEE1394
- S/PDIF In/Out 6-канальный звук
- Поддержка ABIT EQ™ / mGURU™
- Поддержка Технологий ABIT Engineered™



AN7-Guru

- Поддержка процессоров AMD Athlon XP
- NVIDIA nForce2 Ultra 400 MCP-T
- Поддержка 400FSB, Dual DDR400
- 2-SATA 150 RAID / AGP 8X
- 10/100 LAN / 8xUSB 2.0
- IEEE1394, S/PDIF In/Out, 6-канальный звук
- Поддержка Guru™, Softmenu™
- Поддержка Технологий ABIT Engineered™



citilink **SAMSUNG** **ELSIE** **LIZARD** **TDL**

citilink Co **SAMSUNG** **ELSIE** **LIZARD** **TDL**

Тел: 7-495-145-25-69 Тел: 7-495-145-25-69 Тел: 7-495-145-25-69 Тел: 7-495-145-25-69 Тел: 7-495-145-25-69

Факс: 7-495-145-25-69 Факс: 7-495-145-25-69 Факс: 7-495-145-25-69 Факс: 7-495-145-25-69 Факс: 7-495-145-25-69

Е-mail: info@citilink.ru Е-mail: info@samsung.ru Е-mail: info@elsie.ru Е-mail: info@lizard.ru Е-mail: info@tdl.ru

www.abit.ru



КОДИМ

СОКЕТЫ НА MFC

Ты когда-нибудь заморачивался сетевым программированием под винды? Писал клиент-серверные приложения? В общем, писал - не писал, а сегодня научишься. Разберешься с работой асинхронных сокетов в MFC, поймешь, как устроен класс CSocket. А в итоге мы с тобой напишем бесконечные сетевые крестики-нопики. Так что активизируйся, и поехали...

БЕСКОНЕЧНЫЕ КРЕСТИКИ-НОПИКИ ПО СЕТИ

Как я сказал, писать мы будем при помощи класса CSocket под MFC. Для этого, по понятным причинам, нам понадобится Visual C++. И вот что мы сделаем. Вначале мы создадим обычное диалоговое приложение. Затем добавим какие-нибудь простенькие bitmap для изображения пустого поля, с крестиком и с ноликом. Потом добавим обработчик нажатия мышки по полю. Сделаем отображение поля. Создадим новый класс для работы с Сетью. И самое последнее — загрузим обмен данными по Сети, чтобы люди могли нормально поиграть. Что ж, обо всем по порядку.

▶ СТАРТОВАЯ ЧАСТЬ

Запускай Visual C++ (у меня это Microsoft Visual Studio .NET 2003) и создавай новое MFC приложение — Visual C++ Projects -> MFC -> MFC Application. Дай ему имя, например хо, и дави на кнопку ОК. Выползет новое окно. В нем заходи во вкладку Application Type. Там выбирай приложение Dialog based. Теперь во вкладке Advanced Features добавь поддержку сокетов. Для этого отметить крестиком надпись Windows sockets.

Все, можно давить на Finish. Будет создано новое приложение. С ним мы и продолжим нашу работу. Для начала добавим в него поддержку русского языка. Для этого открывай вкладку Resource View. Найди в ней свое диалоговое окно. Кликай на Properties окна и выбирай там русский язык. Сделал? Прекрасно! Теперь наше приложение понимает великий и могучий. Можешь попробовать запустить его — Debug -> Start.

▶ КЛИКАБЕЛЬНОЕ ПОЛЕ

Приложение компилируется. Русский язык отображается. Все ок. Тогда добавим в него поле для нашей будущей игры и сами формочки для соединения. Для этого открой еще раз диалоговое окно. Удали оттуда все кнопки и поле с надписью TODO. Добавь на него 1 Edit Control (IDC_EDIT_ADDRESS) и 3 кнопки (Button). В Edit Control будет прописываться хост для соединения (если ты клиент, а не сервер). А для трех кнопок поставь следующие значения: Connect, Create Server и Exit. Соответственно, одна предназначена для соединения, а две другие для создания сервера либо выхода из программы.

Теперь нам надо нарисовать 3 bitmap. Вот что в них будет содержаться: пустое поле, поле с крестиком и поле с нулем. Назови их

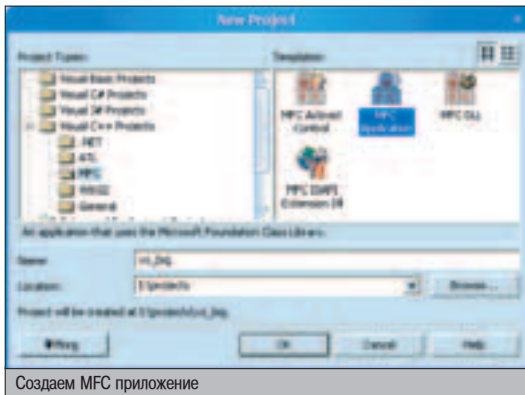
соответственно: IDB_EMPTY, IDB_X и IDB_O. Само поле мы будем хранить в переменной-массиве m_stat. Объяви ее в описании класса. У меня это выглядит так:

```
int m_stat[20][20];
```

Теперь нам надо добавить цикл, который будет отображать состояние поля на форме. Для этого в своем классе найди метод OnPaint. В него я добавил следующий код:

```
for (x=0; x<size_x; x++){
    for (y=0; y<size_y; y++){
        if (m_stat[x][y]==0)
            dc.DrawState(CPoint (posx, posy),
                picsize, bmp_empty, DST_BITMAP);
        if (m_stat[x][y]==1)
            dc.DrawState(CPoint (posx, posy),
                picsize, &bmp_x, DST_BITMAP);
        if (m_stat[x][y]==2) {
            dc.DrawState(CPoint (posx, posy),
                picsize, &bmp_o, DST_BITMAP);
        }
    }
}
```

Все. Теперь поле будет отображаться, но отвечать на клики оно не станет. Чтобы оно стало кликабельным, добавь событие



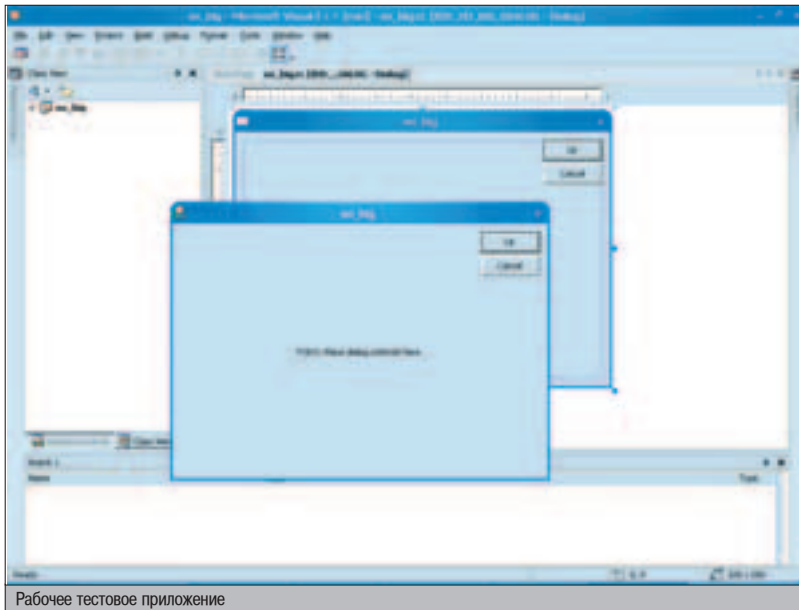
Создаем MFC приложение



Добавляем поддержку сокетов



Выбираем диалоговое окно



Рабочее тестовое приложение

OnLButtonUp. Оно будет вызываться каждый раз, когда ты кликнешь левой кнопкой на диалоговом окне. Приводить код изменения содержимого поля я не буду, его ты можешь посмотреть в конечном варианте программы. Там все легко, и основные действия в коде сводятся к проверке координат курсора мышки в соответствии с содержимым поля.

РАБОТА С СОКЕТАМИ

Наше приложение будет общаться с Сетью через класс CSocket. Сам класс CSocket основывается на своем родителе CAsyncSocket. А это значит, что CSocket является сокетом асинхронным. Что же такое асинхронный сокет? Это такой сокет, который не висит в цикле в ожидании прихода нового соединения или новых данных, как

это делают синхронные сокет, а просто вызывает определенное событие, если что-то произошло. Событием в данном случае является новое соединение, пришедшие или ушедшие данные и т.п.

В чем плюс такого подхода? Главное, тебе не обязательно будет создавать новый поток, чтобы производить в нем обработку данных. Ты можешь просто прописать все необходимые события, и твоя программа перестанет лагать в ожидании пришествия новых пакетов.

Теперь добавим этот класс в нашу программу. Нам придется создать два новых класса на основе CSocket. Первый класс CServerSocket.

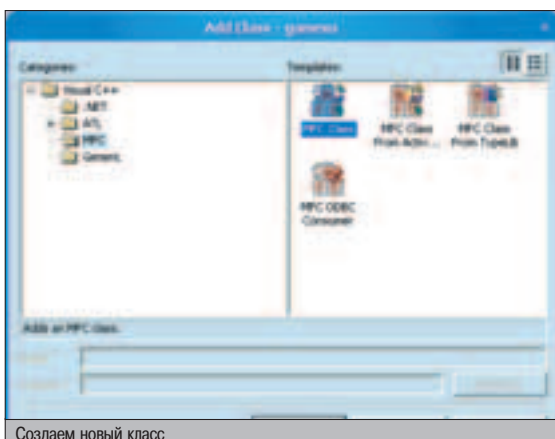
Он будет отвечать за входящие соединения (это тот случай, когда ты выступаешь в роли сервера). Второй, как ты, наверное, догадался, называется CClientSocket. Он используется для исходящих соединения к серверу.

На самом деле, второй класс CClientSocket используется первым CServerSocket. Когда ловится новое входящее соединение, вызывается функция Accept. После чего образуется новый объект на основе CClientSocket. И дальше с этим объектом можно работать как с обычным сокетом, т.е. отсылать или принимать данные.

Давай теперь посмотрим, как же объявляется класс CServerSocket. Для начала добавь его при помощи Class View. Кликни правой кнопкой на своем проекте, выбери пункт Add -> Add Class. В появившемся меню отметь, что у тебя MFC Class, и жми на кнопку Open. В следующем меню в поле Base class найди класс CSocket. А в строке Class name пропиши имя класса: CServerSocket. Все, дави на Finish. Будут созданы два новых файла: ServerSocket.cpp и ServerSocket.h.

Класс добавлен, осталось только произвести с ним некоторые корректировки. Во-первых, тебе надо добавить ссылку на наше диалоговое окно. Это необходимо, чтобы приложение смогло нормально общаться с серверным сокетом. В общем, открывай файл ServerSocket.h и добавляй в public ссылку на класс CxoDlg (это наше с тобой диалоговое окно, где происходят все действия):

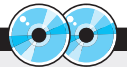
```
public:
    CxoDlg* m_pDlg;
```



Создаем новый класс



Выбираем родительский класс и имя для нового класса



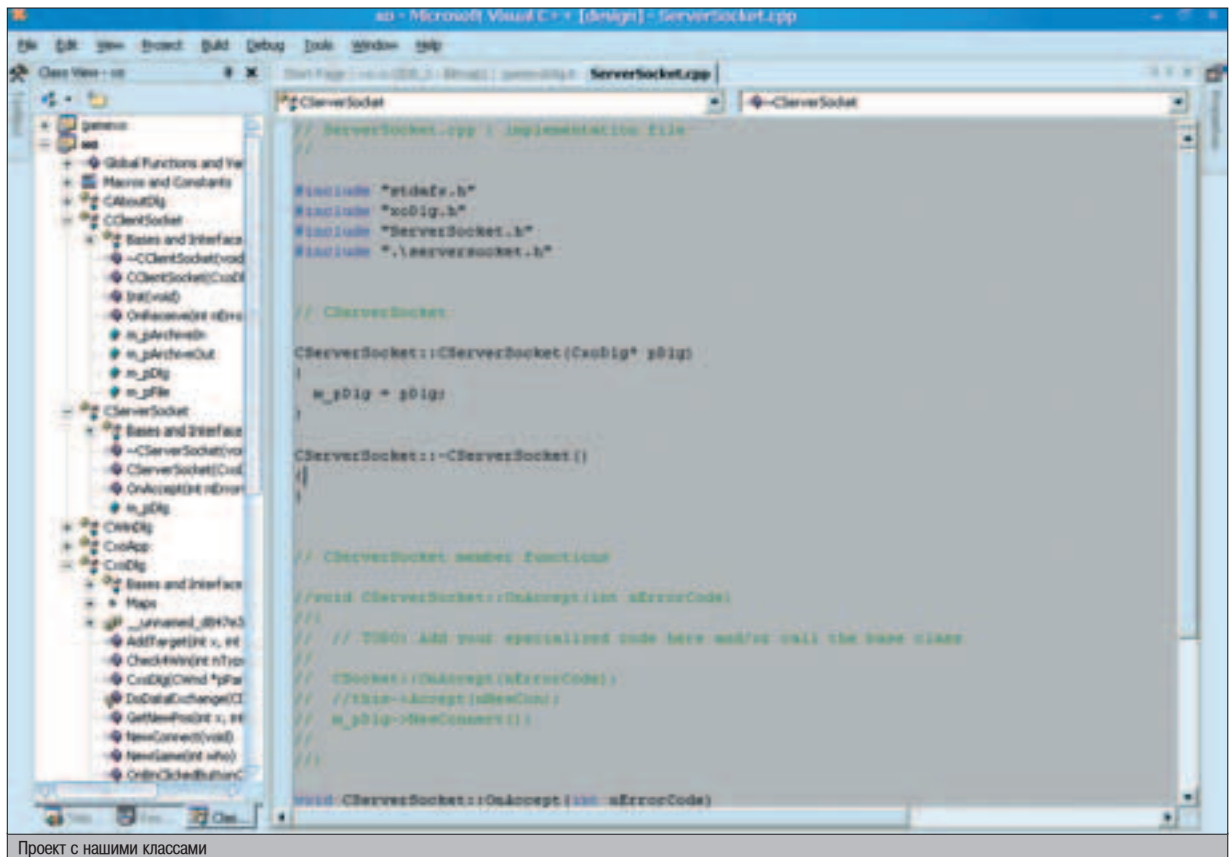
▲ На компакт-диске лежат полные исходные коды крестиков-ноликов. Для их компиляции тебе понадобится Microsoft Visual Studio.



▲ Если ты покупаешь журнал без диска, то ищи на сайте www.haker.ru исходные коды в разделе X-релиз.



▲ Интересной добавкой к игре будет возможность менять размерность поля, а также количество поставленных крестиков или ноликов в ряд для победы.



Проект с нашими классами

ПРОТОКОЛ ДАННЫХ

Первым делом в игре стоит поменять протокол передачи данных. Он, мягко говоря, корявенький. Добавь в него авторизацию, передачу информации о начале партии, ее конце. Сделай проверку координат нового хода. Прикрути возможность менять порт для соединения. В общем, работы здесь непочатый край.

Теперь немного поменяй сам конструктор класса. У тебя он должен получиться вот таким:

```
CServerSocket(CxDlg* pDlg);
```

На этом в хедерном файле изменения закончены. Будем корректировать ServerSocket.cpp. Открывай его и найди в нем конструктор класса. Приведи его к следующему виду:

```
CServerSocket::CServerSocket(CxDlg* pDlg)
{
    m_pDlg = pDlg;
}
```

Все. Этой строкой мы связали наш серверный сокет с диалоговым окном. Осталось только добавить событие для входящих соединений. Для этого пропиши в метод OnAccept такой вот код:

```
void CServerSocket::OnAccept(int nErrorCode)
{
    // TODO: Add your specialized code here and/or call the base class
    CSocket::OnAccept(nErrorCode);
    m_pDlg->NewConnect();
}
```

Теперь при новом соединении вызовется метод OnAccept. В нем произойдет согласие

на входящий коннект, после чего при помощи m_pDlg->NewConnect(); управление передается диалоговому окну.

После создания серверного сокета перейдем к реализации клиентской части. Для начала создавай новый класс CClientSocket на основе того же CSocket. В хедерниках нового класса добавь объявление класса CxDlg. Далее измени конструктор класса. Поменяй пустой CClientSocket(); на CClientSocket(CxDlg* pDlg);. А в .cpp файле пропиши следующие строки:

```
CClientSocket::CClientSocket(CxDlg* pDlg)
{
    m_pDlg = pDlg;
}
```

Здесь, как и в случае с CServerSocket, при создании нового объекта будет передаваться ссылка на диалоговое окно (в моем случае это класс CxDlg).

▲ ПЕРЕДАЧА ДАННЫХ

Наше приложение может выступать как в роли сервера, так и в роли клиента. Серверная часть запускается по нажатию клавиши Create server. После ее клика выполняется событие OnBnClickedCreate, где создается серверный сокет. Вот как выглядит этот код:

```
void CxDlg::OnBnClickedCreate()
{
    m_pSocket = new CServerSocket(this);
    m_pSocket->Create(m_port);
    m_pSocket->Listen();
}
```

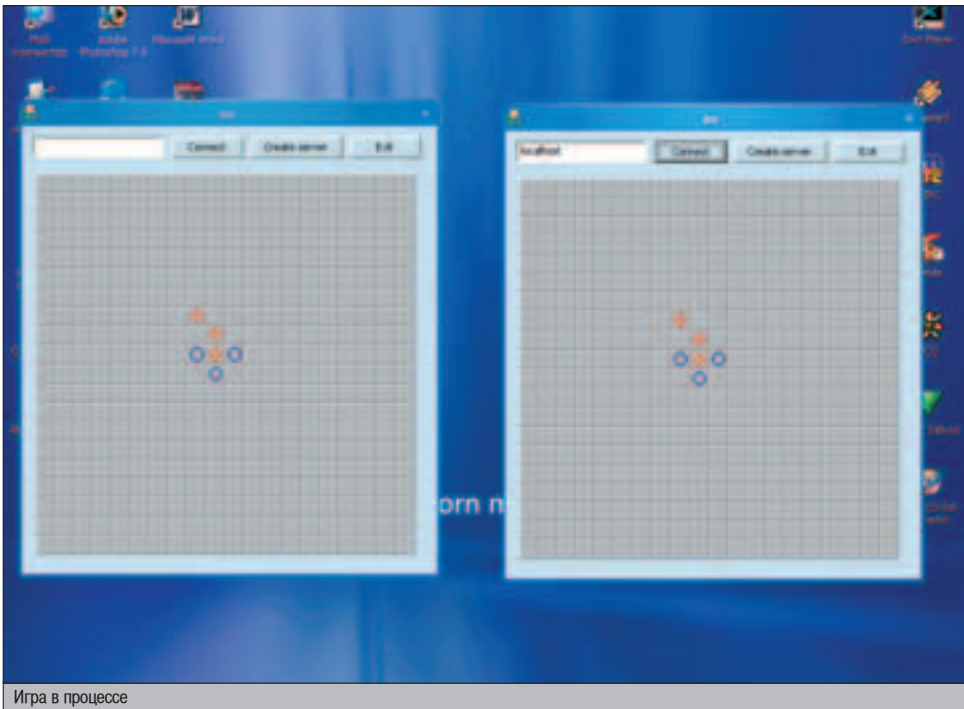
В m_port, как нетрудно догадаться, хранится значение порта. По умолчанию это порт 2345. Само значение m_port прописано как константа. Так что, если ты захочешь сделать этот параметр динамическим, то добавь на форме еще одно поле Edit и свяжи его с этой переменной (только не забудь убрать с нее статус константы).

Далее, если произойдет соединение, то вызовется метод NewConnect, в котором прописаны некоторые начальные данные для новой партии в крестики-нолики:

```
void CxDlg::NewConnect(void)
{
    pSocket = new CClientSocket(this);
    m_pSocket->Accept(*pSocket);
    m_type = 1;
    m_turn = 1;
    m_connected = 1;
}
```

В переменной m_type прописывается тип игрока. Т.е. чем он будет играть – крестиком или ноликами. Один обозначает, что это крестик, двойка – нолик. В m_turn отображается состояние хода. Если это 1, то ход твой, 0 – противника. Соответственно, с каждым ходом это значение будет заменяться противоположным.

Теперь о запуске клиентской части. При нажатии батона Connect запускается метод OnBnClickedButtonConnect. В нем происходит обновление данных в форме при помощи UpdateData (true);. Далее объявляется



Игра в процессе

метод OnReceive класса CClientSocket. И вот что там происходит:

```
void CClientSocket::OnReceive(int
nErrorCode)
{
    char pos[5];
    char num[3];
    int x, y;
    CString data;

    CSocket::OnReceive(nErrorCode);
    this->Receive(pos, 4);
    pos[4]='\0'; num[2]='\0';
    num[0]=pos[0]; num[1]=pos[1];
    x=atoi(num);
    num[0]=pos[2]; num[1]=pos[3];
    y=atoi(num);
    m_pDlg->GetNewPos (x, y);
}
```

Здесь совершается обработка пакета. Информация о координатах помещается в две int переменные x и y. А потом эти

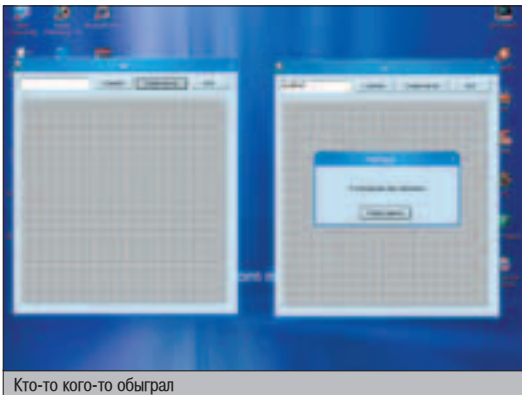
данные передаются диалоговому окну при помощи метода GetNewPos. Так и происходит обмен пакетами между двумя игроками. Естественно, способ крайне примитивный, но зато наглядный. При этом ты всегда можешь поменять протокол. Доработать его, например, чтобы в нем была проверка на верность передачи координат.

НЕДОДЕПКИ

Сейчас программа очень легко обманывается. Ты можешь просто прислать координату, где твой противник уже сделал ход, тем самым заменив его ход своим. Также отсутствует явный обмен о том, что партия закончилась. Это все проверяется только самой программой. К тому же не отображается информация, что клиент присоединился. О его коннекте можно узнать, только нервно покликав по полю, в надежде на то, что там появится твой крестик. Есть глюк и с созданием сервера. Ведь объявляется всего один объект на основе CServerSocket. Если нажать на кнопку Create server несколько раз, а потом сделать коннект к этому серверу, то программа просто упадет. Так что необходимо добавить слежку за состоянием объекта. Т.е. убивать сам объект и порождать его заново.

ГАМАТЬСЯ

Собственно, мы это сделали :). Мы написали с тобой простенькое клиент-серверное приложение при помощи асинхронных сокетов. Но несмотря на всю простоту, ты получил весьма важные знания для дальнейшего изучения сетевого программирования под винды. В будущем я советую тебе разобраться с работой тредов, чтобы ты смог нормально разносить различные соединения по новым потокам. Это крайне полезная вещь. А сейчас предлагаю изучить полные исходные коды и добавить в них что-то свое. Удачи!



Кто-то кого-то обыграл

ПРИМИТИВНЫЙ ПРОТОКОЛ

Я специально взял очень примитивный протокол передачи данных, чтобы не перегружать его. И вот как он устроен. Когда кто-нибудь делает свой ход, неважно, крестики это или нолики, передаются 4 байта. В первых двух байтах находится числовое значение в ASCII кодах, показывающее расположение по оси X. В следующих двух байтах - по оси Y. Вот как выглядит код

для передачи этой информации:

```
if (m_stat[pos_x][pos_y]==0)
{
    m_turn=0;

    /* Пропущена часть кода */

    pSocket->Send(out, 4);
    this->AddTarget(pos_x, pos_y, m_type);
}
```

В переменной out (тип CString) находятся эти самые 4 байта с информацией о координатах нового хода.

Теперь давай посмотрим, как же обрабатываются полученные данные о ходе. Когда приходит какой-то пакет, то вызывается

динамический объект pSocket класса CClientSocket, после чего происходит соединение. Если все прошло успешно, т.е. соединение установлено, то в переменные m_type и m_turn помещаются следующие значения:

```
if (pSocket->Connect(m_sAddr, m_port))
{
    m_type=2;
    m_turn=0;
    m_connected=1;
}
```

Это значит, что ты играешь ноликами, и первый ход не твой, а противника.

ДОБАВЛЕНИЕ БОТА

Интересная добавка к крестикам-ноликам – наличие бота. Т.е. возможность игры с искусственным интеллектом. Изначально я писал эту программу именно для игры с ботом, но сам бот получился несколько глючным. Он у меня иногда выигрывал, но это случалось уж слишком редко :). Так что попробуй написать своего. Если получится что-то интересное, присылай полученный результат мне на почту. Мы обязательно выложим твоё творение на наш сайт





ПАРСИМ ПРОСТОРЫ XML

До настоящего момента мы обсуждали лишь один формат представления текстовой информации в интернете - язык гипертекстовой разметки HTML. Да, этот язык действительно отлично справляется со своей задачей... Но что делать, если перед нами встает проблема иного рода: например, необходимо так представить текстовые данные, чтобы можно было удобно осуществлять доступ к ним из самых различных систем, легко их обрабатывать и производить по ним поиск. Тут на помощь и приходит расширяемый язык разметки XML.

ОБРАБОТКА XML-ДОКУМЕНТОВ ПАРСЕРОМ PHP

ЧТО ТАКОЕ XML?

XML предоставляет разработчикам очень гибкие инструментальные средства для создания структурированных документов. Сам язык внешне очень схож с HTML. Это объясняется тем, что оба языка произошли от стандарта SGML (Standard Generalized Markup Language - стандартный обобщенный язык разметки). Также стоит заметить, что SGML - это скорее не язык разметки, а способ определения подобных языков. Т.е. XML является упрощенной версией SGML, в то время как HTML это лишь приложение SGML, соответствующее этой модели только при строгом применении. Ознакомьтесь с подробной спецификацией и описанием SGML можно либо в интернете (xml.coverpages.org/sgml.html), либо посмотрев некоторые документы на CD.

ЗАЧЕМ НУЖЕН XML?

Если XML, как и HTML, разработан для использования в Сети и обмена данными, то зачем же он тогда вообще нужен? Ответ прост: на практике выходит, что XML на самом деле создан и используется совсем для других целей. Если разметка HTML



Пример XML-документа

указывает браузеру на то, каким способом следует отформатировать данные (вставить таблицу, поменять шрифт или выделить жирным какой-то кусок текста), то XML призван отделить содержание документа от его представления, создав удоб-

ный для восприятия структурированный документ. Важным различием является также то обстоятельство, что в XML можно задавать собственные теги для определения структуры данных. Ты, наверное, уже запутался, поэтому, чтобы все стало по-



▲ 6 октября 2000 года некоммерческая организация WWW Consortium (www.w3.org) разработала техническую спецификацию и полное описание языка XML (eXtended Markup Language - расширяемый язык разметки). С этим документом можно ознакомиться на сайте организации - www.w3.org/TR/REC-xml.

нятно, рассмотрим простой пример. Взгляни на этот HTML-документ:

HTML-КОД

```
<html>
<head>
<title>Список товаров</title>
</head>
<body>
<h1>Список товаров</h1>
<h2>Название</h2> Товар 1<br>
<h3>Индекс</h3> 23454<br>
<h4>Цена</h4> 532р.<br>
<hr>
<h2>Название</h2> Товар 2<br>
<h3>Индекс</h3> 23455<br>
<h4>Цена</h4> 1532р.<br>
</body></html>
```

А теперь на минуту представь, что у тебя есть такой же файл (только количество записей о товарах в нем, скажем, полторы тысячи), и тебе необходимо написать программу, производящую поиск информации о товаре по заданному индексу. Это вполне реализуемая задача при помощи теории конечных автоматов, но, думаю, тебе не по душе такой геморрой :). Так что посмотрим, как такой файл может быть представлен в XML:

XML-КОД

```
<?xml version="1.1"?>
<goods>
<good>
<name>Товар 1</name>
<index>23454</index>
<price>532р.</price>
</good>
<good>
<name>Товар 2</name>
<index>23455</index>
<price>1532р.</price>
</good>
</goods>
```

Внимательный читатель, знакомый с основами дискретной математики и классической информатики, заметит, что XML-документ является, фактически, деревом общего вида, одной из основных структур данных, исполь-

Приложение для обработки XML-документов можно легко написать и на языке PHP.

зуемых в современном программировании и построении математических моделей.

Теперь, для того чтобы извлечь из этого XML-документа список товаров в ценовой категории до 1000 р., тебе все равно потребуются немалые усилия, но благодаря самодokumentированной структуре файла, написать такое приложение становится значительно проще. К тому же функции по обработке XML уже многократно описаны программистами и поставляются в виде специальных модулей.

На настоящий момент парсеры XML существуют под абсолютно любые платформы. Для ОС Windows я бы выделил производимый Майкрософтом парсер - он довольно надежен и один из самых шустрых. Кроме того, он поставляется непосредственно с самой системой. Поэтому большинство программистов используют его в своих разработках. Обработчики XML под *nix распространяются по лицензии GNU, а это значит, что они идут открытыми кодами и отдаются бесплатно, что не может не радовать :).

Ниже я покажу тебе, что приложение для обработки XML-документов можно легко написать и на языке PHP. Делается это при помощи функций анализа XML, встроенных в язык. Документы XML можно переводить и в другие разновидности XML (в частности - HTML) путем связывания с таблицей стилей XSL (eXtensible Style Language - расширяемый язык стилей). Сама таблица является XML-страницей и в ней содержится информация о том, как форматировать конкретные XML-объекты. На базе XML создано множество разнообразных языков (для разметки химических формул, музыкальных нот, математических выкладок, представления векторной графики и т.д.).

Другим путем визуализации XML-документов является составление программы лексической обработки для преобразования документа XML в другие форматы (например, тот же HTML).

ЯЗЫК XML - 5 КБ

Каждый документ в формате XML содержит сочетание разметки и текстовых данных. При помощи разметки документ структурируется, а символьные данные представляют собой содержание страницы. Все XML-документы, по крайней мере, соответствующие спецификации, должны отвечать следующим правилам:

1. Каждый элемент должен содержать открывающие и закрывающие теги, "пустые" теги (например,
 в HTML) в XML недопустимы. Но если элемент не содержит в себе данных, спецификация позволяет использовать вместо <empty> </empty> альтернативную запись <empty />.

2. XML-документ должен в обязательном порядке содержать единственную пару тегов: корневой элемент документа, в который вкладываются все остальные элементы.

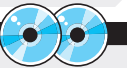
3. Начальные и конечные теги каждого из элементов должны быть правильно вложены: вложенный элемент обязан полностью содержаться во внешнем контейнере. Т.е. начальные и конечные теги вложенных элементов не могут перекрывать друг друга.

Теперь перейдем к описанию непосредственно синтаксиса XML. Каждый документ должен начинаться со строки, которую принято называть "объявлением XML". Она имеет следующий вид: <?xml version="n.n"?>, где n.n - версия языка созданного документа. В настоящий момент последней версией является 1.1, но 1.0 по-прежнему широко используется. Кроме того, различия между версиями весьма несущественны.



▲ Почитай эти документы:

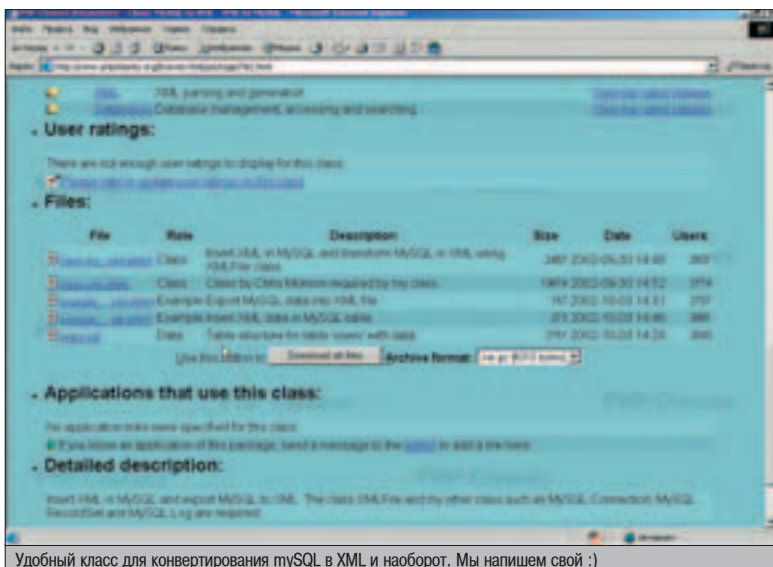
▲ www.w3.org/TR/REC-xml
 ▲ www.w3.org/Style/XSL/mylib.kiev.ua/view.php?id=286
 ▲ webmaster.pp.ru/php4/ref.domxml.html
 ▲ www.vsi.ru/library/PHP/php4_manual/ref.xml.html



▲ На компакт-диске лежат различные документы по XML, а также полный вариант скрипта, конвертирующего MySQL таблицу в XML-документ и обратно.

ПЕРЕВОД MYSQL-ДАННЫХ В XML ПРЕДСТАВЛЕНИЕ

```
<?
/* Функция перевода mysql-данных в XML представление */
function mysql2xml($filename, $rootname) {
/* Получаем массив с именами полей */
$fields = GetFields($table);
$file = fopen($filename, w);
/* пишем в файл заголовок документа */
fputs($file, "<?xml version='1.0'?>\n");
fputs($file, "<$rootname>\n");
$sql = mysql_query("select * from $table");
/* В цикле по полученным из таблицы записям... */
while($res = mysql_fetch_array($sql)) {
/* Создаем элемент, куда будем вписывать данные из таблицы */
fputs($file, "<element>\n");
/* Выводим содержимое в таблице */
for($i=1; $i<=count($fields); $i++) {
$f = $fields[$i];
fputs($file, "<$f>{$res[$f]}</$f>\n");
}
fputs($file, "</element>\n");
}
fputs($file, "</$rootname>\n");
}
?>
```



Удобный класс для конвертирования MySQL в XML и наоборот. Мы напишем свой :)

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



:: 128 страниц исчерпывающей информации о
лучших компьютерных проектах!

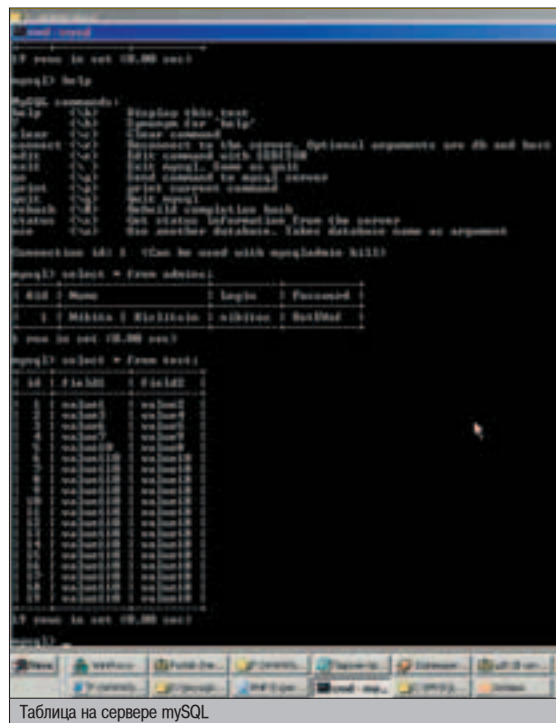
:: Самые детальные руководства и тактические
советы, впечатляющие подборки хитов и кодов,
описание скрытых возможностей и приемов по
взлому, рекомендации от мастеров киберспорта
и многое другое!

:: 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.

уже в прогаже!

самый верный компас на просторах виртуальных миров!



Элементы в XML по виду аналогичны элементам HTML: они также заключаются в теги. Начальные и конечные теги одного элемента должны иметь одно и то же имя - следует обращать внимание на регистр букв: теги <tag> и <Tag> - различные элементы. Как и в HTML, компоненты документа могут иметь атрибуты, значения которых являются частью содержимого элемента, но анализатору не передаются.

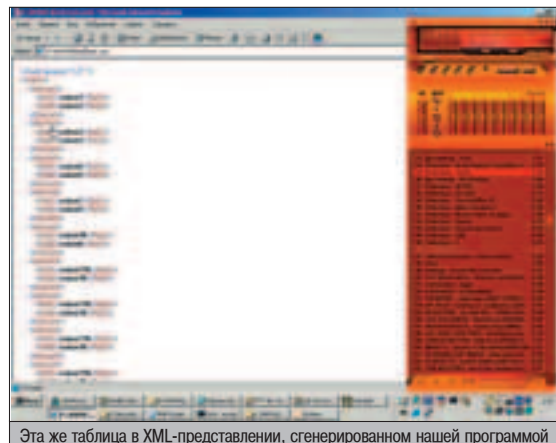
Использование так называемых "сущностей" позволяет разработчику многократно подставлять длинные куски текста, используя более короткие псевдонимы. Так, длинную строку можно обозначить сущностью &var;, после чего вставлять в различных местах XML-документа. Сущности объявляются в блоке, где задается тип элементов - это так называемые DTD документа. Различают внутренние и внешние сущности. Первые объявляются непосредственно в документе, а последние связаны с содержимым внешнего файла.

Объявление типа документа (DTD, Document Type Definition) накладывает некоторые ограничения на содержимое элементов XML-документа. DTD задает элементы и атрибуты, которые можно использовать в документе. Вот его синтаксис:

```
<!DOCTYPE rootelement [
]
>
```

Rootelement - имя корневого элемента. В квадратные скобки помещается объявление различных элементов, их атрибутов и т.д.

Документ XML может иметь и внешнее DTD, объявление которого имеет следующий вид:



Эта же таблица в XML-представлении, сгенерированном нашей программой

```
<!DOCTYPE rootelement SYSTEM "http://url_to_dtd">
```

При помощи объявления типа элемента становится возможным явно указать, может ли элемент содержать текст или какие-нибудь другие данные. Оно также указывает, являются ли элементы обязательными и сколько раз они могут встречаться. Тип элемента определяется следующим образом:

```
<!ELEMENT name type>
```

Где name - это имя элемента, а type - его тип. Тип может принимать три различных значения: (#PCDATA) - символьные данные; EMPTY - указывает на то, что элемент не может содержать данных; ANY - элемент может содержать в себе все что угодно.

При помощи строки <!ATTLIST elementname Attname datatype flag> можно указать список возможных атрибутов элемента elementname, их типов и возможности их обработки. Поле flag может принимать одно из трех значений: #REQUIRED - означает, что это обязательный параметр; #IMPLIED - приложение может использовать значение по умолчанию, если параметр явно не определен; #FIXED - данный атрибут имеет только одно значение для всех экземпляров этого элемента.

Определение внутренних сущностей имеет следующий формат:

```
<ENTITY name "value">
```

Такое определение создаст сущность &name; со значением value. Как только анализатор XML встретит в документе упоминание этой сущности, оно будет заменено значением value. Как я уже упоминал выше, значение сущности может находиться и во внешнем файле. В этом случае ее определение будет иметь следующий формат:

```
<ENTITY name SYSTEM "path_to_text">
```

ПИШЕМ ПРОГРАММУ

После столь подробного описания технологии XML мы напишем несложную программу на PHP. Она будет реализовывать весьма актуальную задачу: экспорт данных из MySQL таблицы в XML-документ. Этот скрипт решает как проблему бэкапа данных, так и совместного доступа к инфо из различных систем.

Собственно, сам кусок кода программы смотри на врезке. Целиком я его привести не могу, т.к. он весьма громоздкий. Полный вариант как обычно бери с CD Хакера или с моего сайта www.iired.ru. Обрати внимание, что сайт новый. Вот что на нем есть: в разделе "разработчикам" выложены все старые статьи с картинками и исходниками; также на сайте находится много дополнительной инфы по программированию, информатике и прикладной математике. Так что заходи ко мне в гости - почерпнешь много новой полезной информации.

P.S. В статье я не сделал подробного описания функций PHP по работе с ML-парсером, однако и на сайте, и на диске лежит отличный документ по этому поводу - дерзай! ☺☺

TIPS & TRICKS

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

▲ Для разработчиков ПО и для тех, кто юзает всякие там трояны: есть такая замечательная прога Stealth PE (дом. страница: <http://bgcogr.narod.ru/>). Основное назначение Stealth PE - скрыть от взломщика информацию о программе, ее компиляторе. Если программа была предварительно упакована с помощью ASPack, UPX, PEGPack и других, то после обработки такого файла с помощью Stealth PE будет практически невозможно определить, чем упакована программа, а также распаковать ее даже специальными автоматическими распаковщиками. А второстепенное назначение - возможность "апдейтить" вирь так, что даже если он известен антивирусам, они перестают его замечать. Все дело в том, что после "апдейта" антивирь при проверке файла не может определить, чем он запакван, и поэтому он не может сравнить его со своей базой данных.

Shanker
shanker@mail.ru

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 !

ПРИБРЕТЕНИЕ И БЕСПЛАТНАЯ ДОСТАВКА КАРТ:

ТЕЛ.: (095) 777-2477, 777-2459.

WWW.ELNET.RU

ЭЛВИС-ТЕЛЕКОМ

ЛИЦЕНЗИИ МИНСВЯЗИ РФ: 19645, 11188, 14552, 15606, 15607



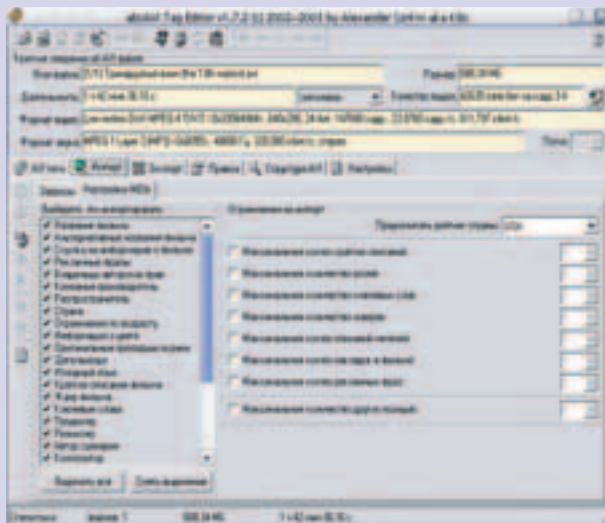
ШАРОВАРЕЗ

ABC-AVI TAG EDITOR V 1.7.2

Windows 9x/Me/NT/2k/XP
Freeware
Size: 1211 Кб
http://abcavi.tk

Многие меломаны (точнее, те из них, кто не находит звучание mp3-файлов слишком грубым для своих продвинутых ушей) считают, что одно название файла (типа "песня.mp3") нельзя считать сколько-нибудь приличным источником информации. Именно поэтому весь меломанский софт активно работает с тегами mp3-файлов, в которых, в частности, может храниться название песни, имя исполнителя и название альбома. У файлов AVI также имеются свои информационные теги, но на них, увы, пока обычные озеры внимания не обращают. Хотя у самих все винчестеры забиты именно фильмами, ориентироваться в которых только по именам файлов становится все сложнее и сложнее. Но потихоньку ситуация меняется. Появляется софт, который начинает черпать из AVI-шных тегов дополнительную инфу, и софт, который позволяет эту самую дополнительную инфу в этих тегах размещать. Вот и я рекомендую тебе обратить внимание на

abcAVI Tag Editor, небольшую бесплатную утилиту, предназначенную для просмотра и редактирования RIFF INFO, MovieID и IDvX тегов в AVI(DivX) файлах. В этой утилите реализована поддержка более 40 тегов, а не только "Автор", "Тема" и "Авторские права". Самое приятное, что забивать все 40 тегов вручную в большинстве случаев не придется - в abcAVI Tag Editor встроен модуль для автоматического импорта информации о фильме из Internet Movie Database (www.imdb.com). Кроме того, прога обеспечивает доступ к служебной инфе. Она распознает свыше 650 видео (FourCC) и аудио (TwoCC) кодексов (эту инфу полезно знать, если фильм у тебя не идет, ругаясь на отсутствие необходимого кодека), показывает данные о качестве видео, скоростях потоков, структуре, длительности и размере файла. Некоторые из этих данных также можно редактировать (знаешь, как много проблем возникает, если в FourCC прописано черт знает что?). Но важнее всего то, что во всех этих тегах ты не запутаешься, поскольку софтина сделана нашим соотечественником, и ее интерфейс можно легко переключить с английского на русский.



ДЕТЕКТОР ЛЖИ ДЛЯ ГОСТЕЙ V 1.0

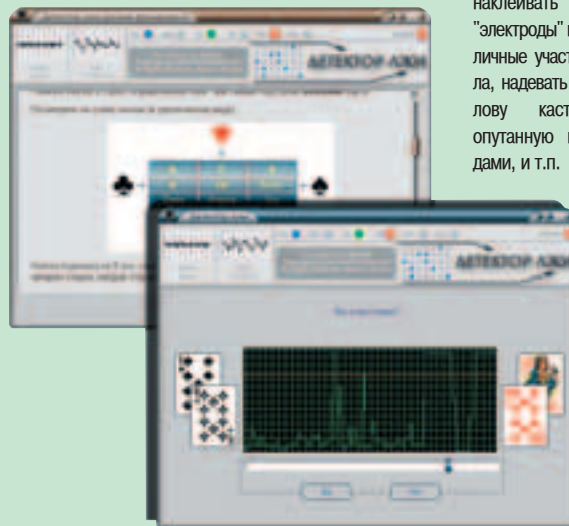
Windows 9x/Me/NT/2k/XP
Freeware
Size: 934 Кб
www.dekan.ru/prog.html

Забавный имитатор детектора лжи. Выполнен качественно, выглядит очень правдоподобно. И результаты выдает прекрасные! Программа безошибочно определяет карту (одну из 36), загаданную лицом, проходящим тестирование. Естественно, нужную карту подсказывает "детектору лжи" оператор во время предварительной "настройки". Способ подсказки прост, как все гениальное. Масть карты "детектор" узнает по тому, с какой стороны оператор наводит курсор на кнопку "Да", а название карты зависит от области, в которую производится клик. Поначалу сориентироваться трудно. Не случайно в проге предусмотрен специальный режим тренировки, позволяющий начинающему оператору набить руку. Но дело того стоит! Твои друзья и знакомые могут следить за каждым твоим действием, но так и не поймут, в чем тут фокус.

По ходу тестирования "детектор лжи" задает испытуемому как произвольные вопросы на любую тему, так и вопросы о загаданной карте. Когда на вопрос о карте будет дан неправильный ответ (человек солжет), раздастся звуковой сигнал. То, что программа никогда не ошибается, невольно заставляет испытуемого поверить в технический прогресс. И человек начинает пытаться обмануть машину, старается контролировать свои движения и реакции... Само собой, безрезультатно! Да еще и оператор может подлить масла в огонь, обещая после тестирования распечатать результаты обработки "потенциально опасных вопросов" ("Изменяете ли вы?", "Лжете ли друзьям?" и т.п.), ложь в ответах на которые прога не показывает "из этических соображений" :).

Итого: программа из разряда must have. Позволяет здорово повеселиться, разыгрывая на вечеринке гостей. Тем более что совместно с "Детектором лжи" можно использовать всевозможные дополнительные "периферийные устройства", заставляя испытуемых ставить босые ноги на "датчики", с

серьезным видом наклеивать им "электроды" на различные участки тела, надевать на голову кастрюлю, опутанную проводами, и т.п.



TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

- ▲ Небольшой прикол:
 - 1) Запусти какое-нибудь видео в Windows Media/BSPlayer/Winamp/... и нажми PrintScreen.
 - 2) Не закрывая видео, вставь картинку в Paint или AcdSee.
- Наблюдай чудо: графический редактор будет проигрывать видео!

PeaceMaker
dennis@ufacom.ru

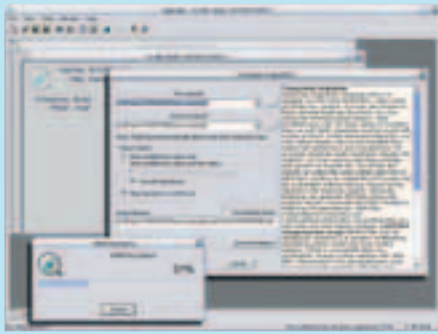
REGSNAP V 4.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 252 Kб
http://lastbit.com

Вышла четвертая версия программы RegSnap. Софтите полностью переписали движок, сделал по ходу дела пару-тройку мелких изменений. Если у тебя еще старая версия этой проги, рекомендую тебе ее обновить - четверка стала работать ощутимо быстрее. Тем, кто RegSnap ни разу не юзал, советую немедленно исправить это досадное упущение. Прога великолепна! С ее помощью я делаю "снимки" реестра, файлов win.ini, system.ini, autoexec.bat и config.sys, а также списка файлов, находящихся в каталогах Windows, Windows\System, My Documents и Program Files, до и после запуска подозрительной проги, а затем сравниваю "снимки" между собой. Точнее, RegSnap их для меня

сравнивает и выдает полный отчет о найденных в системе изменениях. Из этого отчета сразу становится ясно, как и где закрепляется на машине мой очередной подопытный троянец или, допустим, ехе'шник "с фотками", который неизвестно кто прислал мне на мыло. Хотя ты можешь использовать RegSnap и в более мирных областях. Ну, например, эта прога превосходно вычисляет "хвосты", которые оставляют в системе многие шароварные проги, чтобы ты не мог после окончания испытательного срока их удалить, а потом проинсталлировать заново. Специально для этого RegSnap может даже сгенерировать рег-файл, который отменяет изменения в реестре. Многие от этой фишки просто в восторге - делают снимок реестра, ставят шароварную прогу, делают второй снимок, сравнивают снимки между собой, создают рег-файл. Юзают шароварную прогу до окончания испытательного срока,

удаляют, запускают рег-файл, который подчищает хвосты. И тогда прога в большинстве случаев без вопросов встает по новой, даже не подозревая о том, что она обрабатывает уже свой второй (третий, десятый...) испытательный срок.



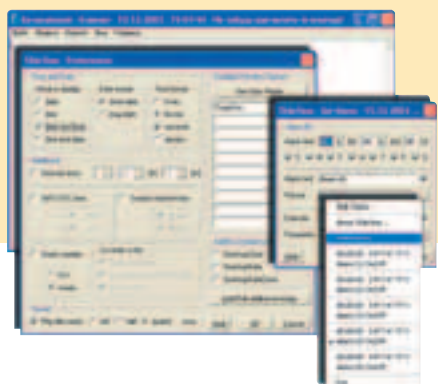
TITLETIME V 2.04

Windows 9x/Me/NT/2k/XP
Freeware
Size: 1137 Kб
www.jumaros.de/rsoft

Эта софтина добавляет текущую дату и/или время к заголовку активного окна. Да-да, я в курсе, что таких программ довольно много. Однако TitleTime выделяется среди этой братии своей продвинутостью. Во-первых, она имеет очень удобную систему напоминаний, состоящую из 5 будильников, которые могут звонить (выдавать на экран сообщение, показывать

картинку, запускать какую-либо прогу) в заданное время по требуемым дням недели. Во-вторых, в TitleTime можно активировать еще одни часы, показывающие время другого часового пояса, GMT/UTC время или так называемое "Swatch Internet time". Хотя это, думаю, не так интересно, как умение программы проигрывать wav-файлы каждый час (полчаса или четверть часа). В-третьих, TitleTime содержит целый ряд мелких фишечек (вроде вывода в заголовок активного окна заранее заданной текстовой строки или поддержки дополнительных модулей), которые усиливают ее полезность. Впрочем,

главное все же текущее время в заголовке активного окна плюс хорошая система будильников. Или тебе, старче, надобно чего-то еще? :)



AUTOSPELL COMPLETECHECK V 6.0

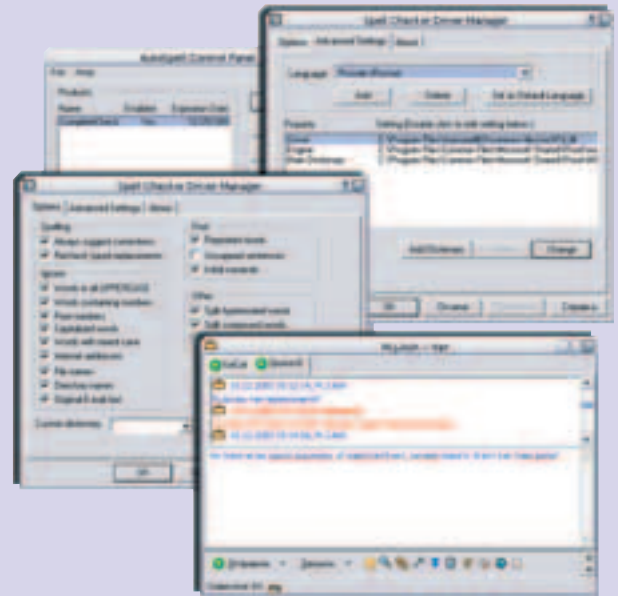
Windows 9x/Me/NT/2k/XP
Shareware
Size: 2434 Kб
www.spellchecker.com

Система проверки орфографии - отличная штука. Она наверняка встроена в твой текстовый редактор и подключена к почтовой программе. Однако до сих пор еще никому не удавалось подружить систему проверки орфографии с софтом для мгновенного обмена сообщениями. Самое смешное, что на редкость элегантное решение этой проблемы в виде утилиты AutoSpell CompleteCheck было разработано уже давно. Но у нас эту утилиту никто не юзал, поскольку в списке поддерживаемых ею языков нашего великого и могучего не наблюдалось. Нет его там и сейчас. Но в результате ряда смелых экспериментов мне все же удалось скрестить AutoSpell CompleteCheck с системой проверки орфографии из пакета Microsoft Office. И теперь у меня в аське (точнее, в ее клоне под названием &RQ) слова с ошибками и опечатками автоматически подчеркиваются красной линией. Проверка орфографии производится в фоновом режиме, точно так же, как, скажем, в Word'е. Более того, как и в Word'е, ты можешь кликнуть по неправильно набранному слову, и тебе тут же будет предложено несколько возможных вариантов написа-

ния. Круто, согласен. Решение, несомненно, из разряда must have, особенно для тех, чье онлайнное ICQ-общение весьма активно.

Но хватит болтать, пора дать подробную инструкцию. Она крайне проста: скачиваешь и устанавливаешь программу AutoSpell CompleteCheck. Запускаешь AutoSpell Driver Manager, переходишь на вкладку Advanced Settings и кликаешь по кнопке Add. Появляется диалоговое окно, в котором ты должен выбрать язык (Russian (Russia)) и прописать правильные файлы в поля Engine Driver Location, Engine Location и Dictionary Location. Я сделал это следующим образом: в поле Engine Driver Location я прописал файл ms97d.dll (C:\Program Files\Autospell60\common files), в поле Engine Location поместил файл mspru32.dll (C:\Program Files\Common Files\Microsoft Shared\Proof), а в Dictionary Location указал файл Msgr_ru.lex, лежащий в той же директории. После этого следует кликнуть Ok, вернуться в исходное меню, выбрать русский язык и сделать его языком по умолчанию. Все! Можешь закрывать прогу настройки и запускать AutoSpell CompleteCheck.

Примечание: я пользуюсь Microsoft Office XP. Вполне возможно, что настройка утилиты на другие версии офиса будет выглядеть немного иначе, но я верю, что у тебя все получится :).



CD2

- Visual Hack++: Корявости PHP
- Хакер 11(59) в PDF
- Все номера Хакер'а за 2000 год в PDF

- demos**
- Демки, занявшие первые пять мест на Dreamhack 03.

- ШаповAREZ**
- AutoSpell CompleteCheck 6.0
- Детектор лжи для гостей 1.0
- abcAM Tag Editor 1.7.2
- RegSnap 4.0
- TitleTime 2.04
- Browser Sentinel 1.3
- Catfood Deskate 1.11
- Rainlendar 0.18
- Clippy 1.0
- Курсы валют Pro 2.0

DRIVERS

- ATI
- NVIDIA
- US ROBOTICS
- Logitech MouseWare
- trash
- desktop
- docs

CD1

- net**
- Epiphany 1.1.1
- HastyMail 0.8
- LiteSpeed Web Server 1.2.2
- mmimircd 0.1.1
- VisualRoute 8.0a
- Wget 1.9.1

- development**
- Bluefish 0.12
- Kylix 3
- phpMyAdmin 2.5.5-rc1
- phpScribe 0.9
- Qt 3.3.0 beta1
- Visual Effects Engine 0.1.4

- multimedia**
- ALSA driver 1.0.Opre3
- AlsasPlayer 0.99.76
- Gwenview 1.0

- misc**
- KEuroCalc 0.7.1
- Metawriter 0.0.11



- development**
- CASE Studio 2
- JRun 4

- multimedia**
- Advanced CD Ripper Pro 2.40
- All Sound Recorder XP 2.01
- CamStudio
- Camtasia Studio 2
- DigitPicViewer 3.0.5
- DivX 5.1.1 PRO
- Visual Effects Engine 0.1.4

- misc**
- A4Mark 6.00
- ClipMate v6.2.0.7
- OmniFormat 3.0
- TextPad 4.7.2

- system**
- BusyBox 1.0.0
- kernel 2.4.23
- LinuxMark 0.27
- Nautilus 2.5.23
- Visopsys 0.31

- UNIX**
- Internet Business Promoter 3.0.3
- Invisible Secrets 4.0.6
- K-ML 3.8
- Local Port Scanner 1.2.2
- Miranda IM 0.3.2
- NetLimiter 1.25
- Opera 7.21
- Panda Platinum Internet Security 8

- system**
- Tools Partition Imager 2003
- Add-Remove Plus! 2003 v4.0
- Advanced Uninstaller PRO 2003 6.01
- AnVir Task Manager 3.6
- AVF Shutdown 5.41
- Directory Opus 6.2
- HideFolder 2
- ICZnc 3.4.1.4
- PCMark04
- Recover4all Professional 2.25
- Secure Folder 2.2
- Style XP 2.0 Beta 3
- WinPatrol 6.0
- WinSettings 7.0

- net**
- Ace Password Sniffer
- Ad Muncher 4.51
- Advanced IM Password Recovery 2.10
- ARELIS 4.1
- Armo2net Personal Firewall 3.12
- ChatBlocker 1.7
- Internet Business Promoter 3.0.3
- Invisible Secrets 4.0.6
- K-ML 3.8
- Local Port Scanner 1.2.2
- Miranda IM 0.3.2
- NetLimiter 1.25
- Opera 7.21
- Panda Platinum Internet Security 8

- misc**
- A4Mark 6.00
- ClipMate v6.2.0.7
- OmniFormat 3.0
- TextPad 4.7.2

- UNIX**
- Internet Business Promoter 3.0.3
- Invisible Secrets 4.0.6
- K-ML 3.8
- Local Port Scanner 1.2.2
- Miranda IM 0.3.2
- NetLimiter 1.25
- Opera 7.21
- Panda Platinum Internet Security 8

- system**
- Tools Partition Imager 2003
- Add-Remove Plus! 2003 v4.0
- Advanced Uninstaller PRO 2003 6.01
- AnVir Task Manager 3.6
- AVF Shutdown 5.41
- Directory Opus 6.2
- HideFolder 2
- ICZnc 3.4.1.4
- PCMark04
- Recover4all Professional 2.25
- Secure Folder 2.2
- Style XP 2.0 Beta 3
- WinPatrol 6.0
- WinSettings 7.0

- net**
- Ace Password Sniffer
- Ad Muncher 4.51
- Advanced IM Password Recovery 2.10
- ARELIS 4.1
- Armo2net Personal Firewall 3.12
- ChatBlocker 1.7
- Internet Business Promoter 3.0.3
- Invisible Secrets 4.0.6
- K-ML 3.8
- Local Port Scanner 1.2.2
- Miranda IM 0.3.2
- NetLimiter 1.25
- Opera 7.21
- Panda Platinum Internet Security 8

CATFOOD DESKDATE V 1.11

Windows NT/2k/XP
Shareware
Size: 3573 Kb
www.catfood.net/products/deskdate

Одно время для "оживления" картинки на рабочем столе я юзал старенькую программу Xearth (www.hewjill.com/xearth). Эта прога натягивала на экран "динамические" обои с изображением земного шара, вращающегося вокруг своей оси в реальном масштабе вре-

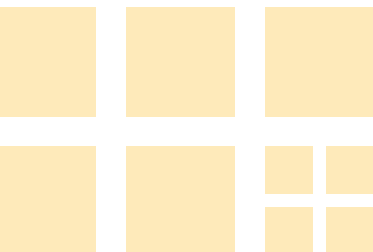
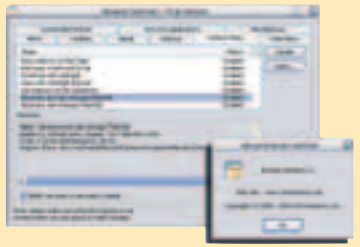


мени, т.е. делая один оборот в сутки. Увы, новых версий этой проги я так и не дождался, и вскоре качество выдаваемой Xearth картинки перестало меня удовлетворять. И вот совсем недавно я обнаружил новую прогу, эксплуатирующую ту же самую тему. Называлась эта прога Catfood Deskdate. Увы, о виртуальном глобусе пришлось забыть сразу - прога умеет лишь прокручивать на экране плоское изображение земной поверхности. Зато смену дня и ночи Catfood Deskdate демонстрирует очень наглядно, к тому же качество картинки у нее на высоте - программа использует весьма детальные фотки. Более того, Catfood Deskdate способна работать с альтернативными изображениями. А это по-настоящему классно! Можно, к примеру, натаскать из Сети высококачественных снимков (предположим, сделанных NASA. В настройках Catfood Deskdate есть даже соответствующая ссылка!). Или же поступить еще круче - сделать карту земной поверхности самому. Лично я сейчас именно этим и занимаюсь - пытаюсь отсканировать старую - времен холодной войны - политическую карту мира. Согласись, хорошая идея. И когда я закончу, мой Рабочий стол, несомненно, будет выглядеть просто убийственно.

BROWSER SENTINEL V 1.3

Windows 9x/Me/NT/2k/XP
Shareware
Size: 724 Kb
http://unhsolutions.net/Browser-Sentinel

Мне всегда нравилось дружелюбное отношение браузера IE к всякого рода примочкам и дополнительным модулям. Но, увы, приходится признать, что эта дружелюбность часто выходит владельцу ослика боком. Проблема в том, что наряду с полезными плагинами в этот браузер могут запросто понапихать разной гадости (пару-тройку рекламных модулей, шпиона-наблюдателя или, скажем, троянского коня), а ты об этом не узнаешь. По крайней мере, сам ослик тебе этого не скажет. Если, конечно, зверюгу не пытаться подходящим инструментом. Понимаю, противно. Но делать это надо. Причем делать регулярно. А инструмент... Хм... Могу дать совет - используй утилиту Browser Sentinel. Знатная софтина. Стоит ее запустить, как ослик миглом делает под себя лужу и рассказывает все! И какие кнопки ему добавили, и какие пункты в его меню всунули, и какие панели ему прилепили. Но самое главное, Browser Sentinel покажет, какие ActiveX компоненты этот осел скачал, и каких "помощников" (Browser Helper Objects (BHO's)) приотлил. Советую тебе посмотреть на www.spywareinfo.com/bhos полный список известных BHO's-ов - вставляет не по-детски! По окончании допроса третьей степени можно сразу переходить к дезинфекции. Browser Sentinel и в этом тебе поможет - позволит удалить или временно отключить ненужные кнопки, пункты меню, панели и модули. Черт возьми, даже я, фанат Оперы, вычесал из своего ослика целый вагон паразитов! Что ж тогда говорить о тех, у кого IE - основной или даже единственный интернет-браузер в системе?!!

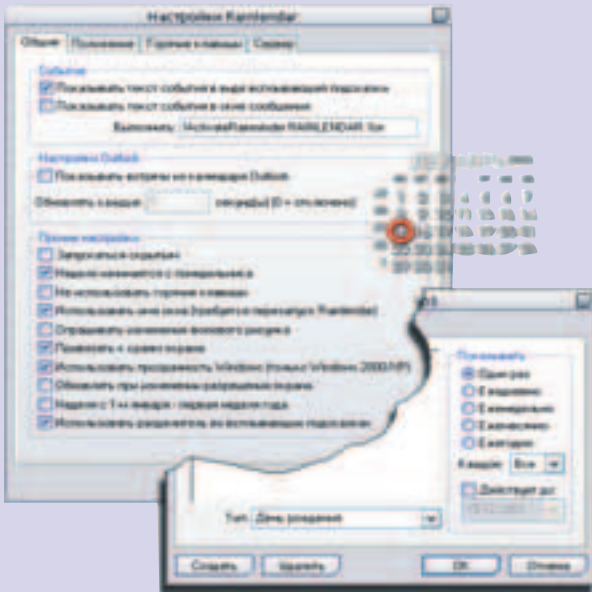


RAINLENDAR V 0.18

Windows 9x/Me/NT/2k/XP
Freeware
Size: 551 Kб
www.iki.fi/rainy

Раз уж речь зашла об обоях для Рабочего стола, то мне хотелось бы упомянуть еще и эту прогу. Я обнаружил ее на компьютере своего приятеля, к которому зашел как-то со стопкой чистых компактв и упаковкой пива. Впрочем, вначале стоит сказать, что Rainlendar это небольшой календарик, который лепится прямо на десктоп. На мой вопрос, почему для этой же цели не использовать более красивый Desktop Wallpaper Calendar (www.zepssoft.com/wallcal), приятель ответил, что разные монстры ему на машине даром не нужны, да и возможностей у Rainlendar все же побольше будет. Я долго думал, стоит ли оставлять без внимания столь на-

льный наезд на одну из моих самых любимых софтин, но потом выпил пива и философски решил махнуть на это рукой. Вкусы у всех разные, а Rainlendar программа действительно интересная. Мелкая, не требующая инсталляции, поддерживающая русский, оснащенная продвинутой системой событий-напоминаний (пара кликов по нужной дате - и новое дело запланировано) и полноценной поддержкой сменных скинов. Кстати, именно наличие множества качественных скинов приводит к тому, что Rainlendar, словно заразная болезнь, активно распространяется по компьютерам моих друзей и знакомых. Хотя надолго на машине Rainlendar оседает все же не из-за красивой шкуры, а из-за своей простоты и крайней приятности в эксплуатации. Ведь у нас, по-прежнему, по одежке только встречают, а жениться все еще стараются по любви :).



КУРСЫ ВАЛЮТ PRO V 2.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1221 Kб
www.softlawyer.ru

Зх, как легко было еще пару лет назад вести финансовые расчеты. Все измерялось в долларах - зарплата, долги, накопления. А потом в нашу жизнь ворвались евро, и все чрезвычайно запуталось. Занимаешь в долларах, просят отдать в рублях. Откладываешь в рублях, через месяц начинаешь жалеть, что сразу же не поменял их на евро. Вот так и мучаемся! Скрепя сердце даже простому человеку приходится обзаводиться специальными финансовыми инструментами. Хотя порой проги попадают славные. Возьмем, к примеру, Курсы валют.

Ценная вещь! Знает о существовании 28 видов национальных валют, автоматически получает курсы выбранных валют с сервера Центрального банка Российской Федерации, помнит, зараза, сколько стоил бакс, скажем, 12 февраля 1992 года и даже строит графики изменения курса интересующей тебя валюты в течение заданного периода времени. К тому же программа имеет встроенный финансовый калькулятор, позволяющий быстро конвертировать одну валюту в другую по-дружески и с учетом процентов. Тебе, возможно, это и не надо. Но лично я пользуюсь Курсом валют довольно часто, особенно если мне в руки попадает свежий номер "Компьютер-прайс", а на книжной полке еще лежат кое-какие остатки последней зарплаты.



CLIPPY V 1.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 221 Kб
www.rjlsoftware.com/software/entertainment

Новая приличная прога-западлянка. Ты помнишь анимированную скрепку, впервые появившуюся в Office 97? Clippy - так звали этого надоедливого "помощника". Сколько лет он долбал всем нам мозги. В конце-концов Microsoft решил его убрать со сцены. Но теперь, благодаря ребятам из компании RJLSoftware, он вернулся. Вернулся еще страшнее, чем прежде! И теперь эта сволочь может жить отдельно от Офиса.

Запусти файл clippy.exe на машине врага, и Clippy будет выскакивать на экран каждую минуту. Минута - это много?! Ну ты зверь! Ладно, обрати внимание на то, что прогу можно запускать с параметрами: clippy.exe [seconds to delay] [pogandom]. Набери в командной строке clippy.exe 10 и нажми Enter. Clippy начнет появляться каждые 10 секунд! Так он достанет и мертвого!

Теперь пара слов по поводу параметра pogandom и советов, которые дает юзеру скрепка-маньяк. Вот в чем дело: по умолчанию прога говорит по-английски. И небольшой список советов встроена в программу. Многие из этих советов довольно смешные ("Я обнару-

жил движение мыши, это нормально", "Клавиша F1 работает корректно", "Твои иконки все еще расположены на Рабочем столе"), однако советы на русском языке читать, согласись, приятнее. Так ведь нет проблем! В той же папке, в которую ты положил clippy.exe, создай файл clippy.txt, и скрепка будет черпать свои советы прямо оттуда. Присутствие же в строке запуска необязательного параметра pogandom сигнализирует проге о том, что строчки надо зачитывать одну за другой, а не выбирать наобум.

Эх, ты только представь, каково это, когда на экран твоей машины периодически выпрыгивает такой вот "помощник" и начинает поучать, советовать и

издеваться. Буйное помешательство гарантировано! Спасти может лишь перемещение курсора в левый верхний угол экрана. Одна беда - ну кто же скажет об этом жертве розыгрыша? :)



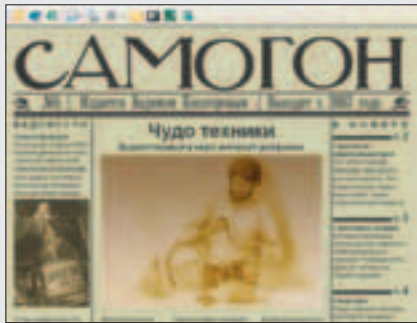


WWW

СПОНСОР РУБРИКИ «ЮНИТЫ» - ЦНТ ЦЕНТРАЛЬНЫЙ ТЕЛЕГРАФ WWW.DIALUP.CNT.RU, WWW.CARDS.CNT.RU

САМО-ГОН

www.samogon.ru



Самогон - древний и весьма национальный русский напиток. Такой же национальный, как кашаса в Бразилии, граппа в Италии, чача в Грузии, шнапс в Германии, текила в Мексике, ракия в Болгарии, раки в Турции, коньяк во Франции, ром на Ямайке, виски в Шотландии и Ирландии. То есть алкогольный напиток, получаемый путем перегонки браги, сделанной из различного сырья. Что интересно, многие эти напитки на родине производителей неоднократно запрещались. Самогон в России, кашаса в Бразилии... Однако гнали, гонят и будут гнать. Не корысти ради, не в промышленных объемах, а просто для светлой радости души. Потому что свой, собственноручно выгнанный и очищенный самогончик - ни с чем не сравнить. Да, конечно, всякий лесоповал, который гонят бабульки исключительно для продажи алкоголикам - это безусловное зло и яд. Но свой собственный продукт - это совершенно другое дело. Поэтому будем на этом сайте изучать историю возникновения, путь развития, горькую дорогу непонимания и запрещения, житейский ренессанс и современное состояние дел этого действительно народного напитка. Но много не пей. Потому что много хорошо - тоже нехорошо.

То есть алкогольный напиток, получаемый путем перегонки браги, сделанной из различного сырья. Что интересно, многие эти напитки на родине производителей неоднократно запрещались. Самогон в России, кашаса в Бразилии... Однако гнали, гонят и будут гнать. Не корысти ради, не в промышленных объемах, а просто для светлой радости души. Потому что свой, собственноручно выгнанный и очищенный самогончик - ни с чем не сравнить. Да, конечно, всякий лесоповал, который гонят бабульки исключительно для продажи алкоголикам - это безусловное зло и яд. Но свой собственный продукт - это совершенно другое дело. Поэтому будем на этом сайте изучать историю возникновения, путь развития, горькую дорогу непонимания и запрещения, житейский ренессанс и современное состояние дел этого действительно народного напитка. Но много не пей. Потому что много хорошо - тоже нехорошо.

ЛЮБОВНЫЕ ОПРЕДЕЛЕНИЯ

www.world-of-love.narod.ru

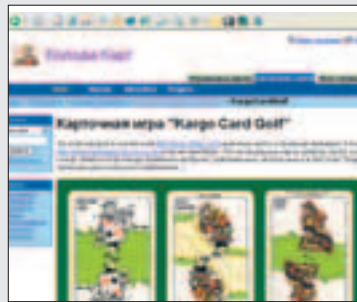


Мир любви и романтики - вот что это такое. Но не пугайся, я еще не съехал с глузда, чтобы рекомендовать в журнале Хакер романтически-любовный сайт. Там вся хохма в том, чтобы почитать различные определения любви, среди которых есть довольно точные. Например:

"Любовь - это болото, где тонут два идиота". Но и это не самое интересное. Лично я рыдал, когда почитал на этом сайте, что говорят о любви американские школьники. Кстати, очень хорошо говорят. Зрело. Например: "Когда тебя кто-то любит, он произносит твое имя по-особенному. Твоему имени уютно у него на языке". Чувешь? Такую фразу не зорно сказать даже закоренелому цинику - и подруга тут же станет вся твоя. Ведь она давно предполагала, что закоренелые циники в душе - весьма романтичны...

КАРТИШКИ ДЛЯ БРАТИШКОВ

www.kolodakart.ru



Многие люди обожают перебирать в руках бумажные и пластиковые листочки разной степени потертости, чтобы с неизбынным азартом или с чувством глухой и заскорузлой тоски играть в подкидного дурачка, двадцать одно, буру, вист, бридж, преферанс, пинокль, канасту, деберц, покер, кинга и в потрясающую оккультную игру

"угадай, на какой карте я в данный момент сижу". Однако гораздо интереснее познакомиться с людьми, которые испытывают к картам - а точнее, к колодам карт - чисто умозрительный интерес. В том смысле, что они их коллекционируют. Потому что карты - они бывают далеко не только игральные, но еще и сувенирные, гадалочные, самодельные, художественные и так далее. Берешь себе 36 или 54 листочка - и рисуешь на них все, что считаешь нужным. А хорошие люди потом эти колоды собирают, сканируют и выкладывают на этом сайте. Познавательное - до жути. А главное - можно по образу и подобию создать какую-нибудь крутую колоду и поразить друзей со страшной силой.

ЖУТКАЯ ПРАВДА О ГАМБУРГЕРЕ

www.dobryankafm.com/news_111603_M1.htm



Как известно, рестораны быстрого питания Макдоналдс весьма популярны во всем мире. А что, все очень быстро, удобно и недорого. Да и гамбургеры - такие вкусные. Да и кока-кола - такая сладкая. Да и картошечка - такая хрустящая. И все такое - м-м-м, какое сытное, аппетитное, красивенькое такое и вообще - классное! Конечно, некоторые люди где-то как-то с большим трудом пытаются объяснить, что все эти макдоналдские прелести - не просто не полезны, а вредны настолько, что этого даже и передать невозможно. Точнее, передать-то возможно, но этого просто никто слушать не будет. А зачем слушать? Вот мы, например, в Макдоналдсе питаемся уже несколько лет - и ничего, не умерли. Однако, вероятно, было бы нелишним - просто на всякий случай - прочитать на этом сайте отрывки из книги Эрика Шлоссера "Нация фаст-фуда". Этот парень отлично знает, с чего начинался Макдоналдс, как он развивался, и что он собой представляет сейчас. Шлоссер знает, откуда берется мясо для гамбургеров, почему так вкусна быстрозамороженная картошка и сколько тонн химикатов создают весь этот привычный вкус гамбургера, жареной картошечки и так далее. Я понимаю, что тебе не очень хочется это все читать. Но тогда лучше сразу цианистого калия глотнуть...

ОХОТНЫЕ СЛОНЫ

www.os2.in.ru/os2oons/slon

Пора уже, друг мой, заняться наукой. Точнее, научными способами охоты. На слонов. Понятное дело, не на мышей же охотиться. За ними пока побегаешь из угла в угол - упаришься весь. Другое дело - слоны. Эту животную ногами не затопчешь, поэтому нужно использовать научный и бесшумный подход. Где его взять? На этом сайте. Теорий там много, причем они традиционно делятся на всякие разные методы: математические, физические, методы экспериментальной физики, компьютерные и всякие другие. Ведь понятно, что к слону надо разные теории прикладывать, чтобы его заохотить: примерно по две-три теории с каждого бока, плюс пару теорий со стороны хобота, чтобы не затоптал. Самыми забавными мне показались следующие методы. Парадоксальный: Ловим 6 слонов, 5 отпускаем. Метод продавца: Берем нечто серое. Кладем в клетку и продаем как слона. Ну и самый, на мой



взгляд, гениальный - метод эволюции. Берем клетку, ставим посередине Сахары. Кладем туда сине-зеленую водоросль. Через п миллиардов лет в результате естественной эволюции получается слон. Если пустыня вокруг еще осталась, значит, этот слон из пустыни.

НУ ПРОСТО НЕВОЗМОЖНЫЕ ФИГУРЫ!

www.imp-world-r.narod.ru

На свете есть много вещей, кажущихся совершенно невозможными. Египетские пирамиды, Тадж-Махал, павлидло, непонятно как попавшее в конфеты-подушечки, и хорошие отношения тещи с зятем. Многие считают, что поверить во что-то можно только тогда, когда увидишь это собственными глазами. Однако бывают такие рисуночки, увидев которые, понимаешь, что в это невозможно поверить. Вот не бывает такого на самом деле, хотя, вроде бы, видишь это собственными глазами. Видишь, конечно, на рисунке, потому что если увидеть такое в реальной жизни - нормальное восприятие снесет в мгновение ока в голубую даль, и будешь ты до конца жизни находиться в некоем заведении с белыми стенами, мечтательно прислушиваясь ко всяким приятным внутренним ощущениям. Но не внешним, потому что с внешней стороны - не очень хорошее питание и грубые мужчины, которых зовут совершенно одинаково - санитар. Вот на этом сайте подобные фигуры ты и найдешь - невозможные с визуальной и физической точек прозрения. Впрочем, лично я, рассмотрев всевозможные совершенно невозможные фигуры, ушел с сайта



хотя и обновленный, но не потерявший рассудок. Потому что я когда-то видел, как в одной студенческой компании яблоко, в целях закуски, разрезали на 52 части. Вот в такое, пока сам не увидишь, никогда не поверишь!

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



NEW!
The Sims: Bustin' Out

\$55.99



Super Mario Bros 3: Super Mario Advance 4

\$59.99



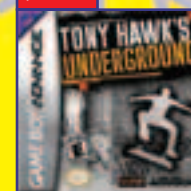
Onimusha Tactics

\$59.99



Shining Soul

\$59.99



Tony Hawk's Underground

\$52.99



Need for Speed Underground

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

WWW.GAMEPOST.RU

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

e-shop
<http://www.e-shop.ru>

ИГРОВАЯ
ФИГУРА

GAMEPOST

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

Задавая вопрос, подумай! Не стоит мне посыпать вопросы, так или иначе связанные с хакером/кряком/фриком - для этого есть hack-faq (hackfaq@real.hacker.ru), не стоит также задавать откровенно памерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q ■ Здравствуйте! Недавно столкнулся со следующей проблемой: если подключить жесткий диск (все разделы в файловой системе NTFS) со своего домашнего компьютера к рабочему ПК, то я абсолютно лишуюсь возможности исправлять/перемещать/удалять с него файлы, получая сообщение о недостатке прав. Брр, ничего не понимаю!

A ■ Видимо, засидевшись дома под администраторским аккаунтом, ты совсем забыл выставить права доступа своим дискам и папкам. Что, впрочем, ничуть не удивительно! Тебе, как привилегированному пользователю, дома никакие ограничения наверняка и не снились. А ведь по умолчанию полный доступ имеют лишь администраторы и пользователи-создатели папок. Поэтому на рабочем месте, имея в своем распоряжении лишь обычный пользовательский аккаунт, ты имеешь возможность лишь читать и исполнять файлы. Могу лишь посоветовать под администраторским аккаунтом выставить корректные права доступа. Кстати, в стремлении предельно упростить пользовательский интерфейс WindowsXP, Microsoft спрятал вкладку Безопасность на томах NTFS подальше от неопытных юзеров. Для того чтобы активизировать ее, зайди в меню проводника -> Сервис -> Свойства Папки -> Вид, сними галку напротив опции Использовать простой общий доступ к файлам (рекомендуется). Вуаля - и все на месте!

Q ■ Помогите разобраться: в чем разница между Avi, DivX, Mpeg4. Друзья говорят, что это одно и то же, но ведь это не так?..

A ■ Конечно же, это не так! С этими понятиями уже довольно давно существует путаница. Дело в том, что DivX, XviD и т.п. - это кодеки, то есть алгоритмы кодирования и декодирования данных с целью их воспроизведения. В то время как AVI (Audio Video Interleave) - это всего лишь формат данных, который был разработан еще в далеких девяностых годах во времена Windows 3.1x. Главная специфика этого формата заключается в возможности использования (в том числе и одновременном) различных кодеков. То есть, если несколько файлов имеют одно и то же расширение .AVI, то это вовсе не означает, что они закодированы одинаковыми кодеками. Стоит отметить, что существует еще и формат MKV, однако он куда менее популярен, чем AVI, даже несмотря на ряд значимых преимуществ. И последнее: известная тебе аббревиатура MPEG - это одновременно и кодек, и формат данных. Надеюсь, теперь все ясно.

Q ■ Привет! Я достаточно давно пишу на Delphi. Подскажи, пожалуйста, какой-нибудь хороший и быстрый алгоритм сортировки одномерного массива.

A ■ Не буду тебя грузить стандартными сортировками по методу "пузырька", вставок, последовательного выбора и т.п. Предложу альтернативный вариант. Смысл алгоритма следующий: первоначально фиксируем один из элементов массива, так называемый X элемент. После добиваемся, чтобы все элементы левее X были меньше значения X, а правее X - соответственно наоборот. Это мы реализуем, "проходя" массив с обеих сторон, последовательно меняя местами неподходящие элементы. Далее проделываем то же самое с каждой из двух половинок массива.

```
const n = 100;
type Arr = array [1 .. n] of real;
procedure QuickSort (var a : Arr);
procedure Sort(l, r : integer);
var x, w : real;
    i, j : integer;
begin {Sort}
  i := l; j := r;
  x := a[(l+r) div 2];
  while i <= j do
  begin
    while a[i] < x do Inc(i);
    while a[j] > x do Dec(j);
    if i <= j
    then begin
      w := a[i];
      a[i] := a[j];
      a[j] := w;
      Inc(i);
      Dec(j);
    end;
  end;
  if l < j
  then Sort(l, j);
  if i < r
  then Sort(i, r);
end; {Sort}
begin {QuickSort}
  Sort(1, n);
end;
```

Q ■ Помогите разобраться со следующим: на моей материнской плате (ASUS) стоит встроенный контроллер IDE RAID. Нужно создать RAID 1 массив и заставить Linux RedHat его корректно понимать. Установка системы со скачанными драйверами проходит успешно. Но после перезагрузки начинают сыпаться ошибки: "root fs not found", "Cannot open root device", "Unable to mount root fs on", ну и т.п.

A ■ Скорее всего, ядру не хватает модуля твоего контроллера, соответственно, оно и грузится. Поэтому в срочном порядке следует найти необходимый модуль и загрузить его в ядро. Чтобы объяснить все подробно, не хватит и целой статьи, поэтому ограничусь лишь советом прочитать многочисленные мануалы по этой теме. Правда, возможен и другой вариант. Год назад столкнулся с ситуацией, когда via'ские драйверы поставлялись с кривым компонентом, поэтому система на RAID контроле работать ну никак не хотела. Пришлось ждать обновления со стороны программистов.

ХАКЕР'S STUFF X

ТОВАРЫ НА БУКВУ

Q ■ Недавно полетел винт с очень важной информацией. Обидно! Продавец-консультант посоветовал в следующий раз чаще делать бэкап и следить за состоянием S.M.A.R.T.'а. Расскажи, пожалуйста, подробнее про последний!

A ■ Если объяснять в двух словах, то технология S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology) представляет собой механизм, встроенный непосредственно в винчестер, который следит за огромным количеством характеристик состояния работы твоего HDD, анализирует и предсказывает его возможные падения. Купив новый винчестер, советую первым делом активировать работу его S.M.A.R.T.'а в БИОСе и оценить полученные результаты. Найти подходящий софт не проблема. У каждого производителя есть своя собственная программа, которую можно совершенно бесплатно скачать с соответствующего офсайта. Правда, разобраться с огромным количеством статистических данных не так-то просто. Попробую кратко объяснить, что есть что. Технология внутренней оценки состояния винчестера следит за огромным количеством параметров работы HDD, однако значимых всего несколько. Их значения, как правило, изменяются от 0 до 100 (хотя бывают и исключения) и сравниваются с некоторыми эталонными значениями. Последние устанавливаются производителем в соответствии со специальными стандартами и спецификациями. Следующие параметры являются наиболее критичными:

Raw Read Error Rate - частота ошибок при чтении данных с жесткого диска.

Spin Up Time - время раскрутки пакета дисков из состояния покоя до рабочей скорости.

Spin Up Retry Count - число повторных попыток раскрутки дисков до рабочей скорости.

Seek Error Rate - частота ошибок при позиционировании блока головок.

Reallocated Sector Count - число операций переназначения секторов.

Стоит заметить, что показания S.M.A.R.T.'а отнюдь не всегда правильные, тем не менее, погрешность чаще всего невелика. Так что если твой S.M.A.R.T. ненавязчиво намекает на то, что винт того и гляди уйдет в мир иной, тебе стоит всерьез задуматься о покупке нового HDD и позаботиться о скорейшем бэкапе.

Q ■ А есть ли способ увеличить передачу данных через GPRS? Последние два месяца связь ну просто невыносимая! Постоянные лаги, слэды скоростей вплоть до нуля...

A ■ Можно попробовать поэкспериментировать со значениями MTU (Maximum Transfer Unit) и TTL (Time To Live) протокола TCP/IP. Я, например, увеличил значение MTU до 1500, а величину TTL - до 60. На глаз все стало работать значительно быстрее, хотя в часы пик скорость все равно скачет очень сильно. Оптимальные значения этих параметров порекомендовать сложно: все сильно зависит от конкретного оператора сотовой связи, уровня приема сигнала и т.п. Просто экспериментируй! 15 минут мучений, и результат не заставит себя ждать. Чтобы не заморачиваться с ключами реестра, рекомендую утилиту Internet Tweaks 2002 (www.magellass.com). Огромное количество настроек, интерактивные и крайне полезные подсказки, хороший интерфейс помогут тебе без труда подкорректировать параметры соединения. Кстати, в известной TweakXP (www.tweakxp.de) также присутствует раздел Modem Tweaks: здесь есть кое-какие фишки, присущие только Windows XP.



Футболка "Думаю..." с логотипом "Хакер": белая

\$13.99



Толстовка "WWW" с логотипом "Хакер": темно-синяя

\$35.99



Куртка ветровка (GL) "FBI" с логотипом "Хакер": темно-синяя, черная

\$39.99

Часы "Хакер"

\$65.99



Кожаный шнурок для мобильного телефона с логотипом журнала "Хакер"

\$11.99

Зажим для денег с логотипом журнала "Хакер"

\$11.99



ВСЕ ЭТИ ФИШКИ ТЫ МОЖЕШЬ ЗАКАЗАТЬ НА НАШЕМ САЙТЕ WWW.XAKER.RU, ИЛИ ПО ТЕЛЕФОНУ: (095) 928-0360, (095) 928-6089



Сегодняшнее западло очень хорошо проводить над начинающими юзерами или просто памерами. Они всегда читают надписи, которые видят, и доверяют им. Более продвинутые перцы, которые не первый день портят зрение за монитором, большинство надписей знают наизусть. Но если они замечают что-то непадное, то это и их может завести в ступор. Я не раз встречал знающих людей, которые на любой нестандартной мелочи начинают строить сумасшедшие теории. Когда зависает компьютер, некоторые умники начинают выводить теории багов, другие же списывают все на глючность материнки. А ведь проблема заключается всего лишь в ошибке программы!

КАК СВЕСТИ ПАМЕРА С УМА

▲ WINDOWS/TOTAL COMMANDER

Самый распространенный файловый менеджер по умолчанию использует английский язык. Если я не ошибаюсь, он написан на Delphi (хотя это не имеет особого значения), и язык в коде прописан именно буржуйский. Чтобы отображать наш родной язык, используется текстовый файл, в котором прописаны все надписи в открытом и легко читаемом (а значит и редактируемом) виде. Точнее сказать, файлов с именем WCMD_RUS целых два: один с расширением tpi, а другой с lng. В файле tpi находятся заголовки для пунктов меню. Они выглядят примерно так:

```
POPUP "&Файл"
  MENUITEM "Изменить &атрибуты...",
  cm_SetAttrib
  MENUITEM "&Упаковать...\{ALT+F5}",
  cm_PackFiles
  MENUITEM "&Распаковать...\{ALT+F9}",
  cm_UnpackFiles
  ...
  ...
END_POPUP
```

Для начала ты можешь разнообразить названия пунктов меню, включив фантазию. Но мы же не просто приколисты, мы готовим сурьезное западло! Именно поэтому измени еще и клавиши быстрого вызова. На работу проги это не повлияет, но вот путаницы внесет изрядно.

Для полного контакта перетасуй аккуратненько названия всех пунктов. Большинство даже продвинутых перцев знают наизусть не все горячие клавиши, и далеко не для всех пунктов меню есть пимпочки на панели. Редко используемые команды никто запоминать не будет, поэтому все равно приходится лезть в меню. Ну а если твою прогу запустит ламер, то он попадет по полной программе. Слава Биллу, если он не удалит все файлы со своего винта. Так что постарайся оформить меню по полной =).

▲ КРУЧУ-ВЕРЧУ...

Теперь переходим к файлу WCMD_RUS.LNG. Это тоже текстовый файл, в котором в каждой строчке находятся отдельные текстовые сообщения, которые можно увидеть во время работы с Windows/Total Commander. Вот тут ты также можешь разгуляться по полной программе. Ты, как искушенный западлист, обязан поменять местами сообщения или просто изменить

их, чтобы запутать бедную жертву так, чтобы у нее сорвало крышу:

"Нельзя копировать файл сам в себя!" - можно поменять на "Копирование прошло удачно".

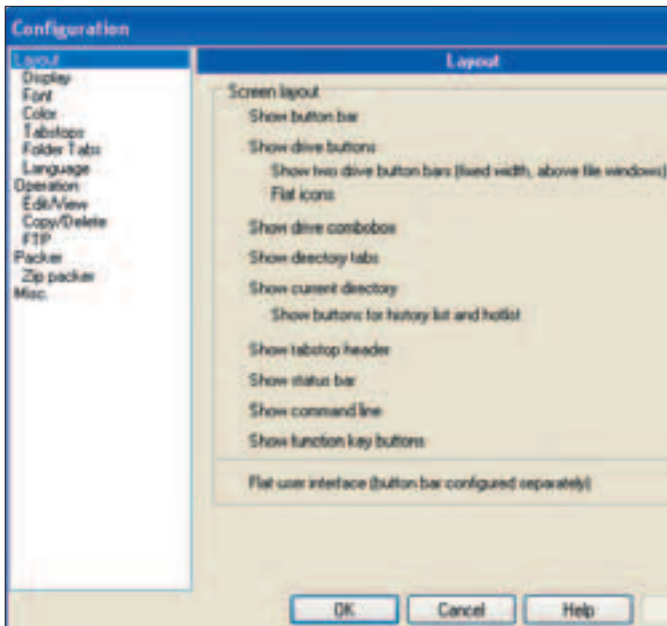
"Копировать %i файл(a,ов) в:" - можно поменять на "Переименовать/переместить %i файл(a,ов) в:".

Упаковку можно сменить на распаковку, перемещение на копирование и так далее. Постарайся и отредактируй все, что только нужно, а главное - что не нужно :).

После того как закончишь свою жесткую работу, осмотришь еще раз. Может, тебе придет в голову еще более безбашенная идея. Хотя я и западлист со стажем, но на свежую голову всегда можно придумать что-то новое.

▲ ТЕМЫ WINDOWS НА СЛУЖБЕ ЗАПАДЛА

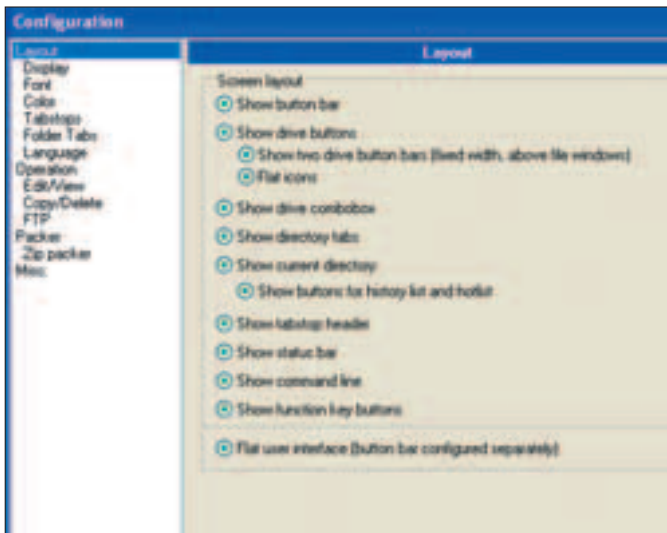
Совсем недавно, в сентябрьском номере][, я описывал, как можно создавать свои темы или редактировать уже существующие. Надеюсь, ты читал эту статью и помнишь, как это делается. Если ты упустил этот номер из виду, то обязательно найди его и прочитай, потому что для реализации следующего западла эти знания будут просто необходимы.



Итак, в сентябре я показал, как можно отредактировать тему. Ты увидел, что все элементы управления - это всего лишь картинки. Так кто нам мешает поменять эти картинки местами и из CheckBox сделать RadioButton или еще что-нибудь подобное? Я недавно проделал такое западло над замначальника своего отдела, так в результате мы услышали ТАКОЕ про Билла Гейтса, что у всех в отделе уши завяли. А когда зам узнал, что над ним приколотись, то я уже собрался идти покупать себе костыли :).

Через пару дней я закрасил все компоненты в ресурсах тем цветом фона диалога. Таким образом, они слились с диалоговыми окнами и стали невидимыми. Посмотри на скрин 2, где показано все то же окно настроек Total Commander, в котором остались только надписи, а элементы управления просто исчезли. И вот так во всех окнах Windows! Если бы в ресурсах тем я окрасил их в белый цвет, то в окнах были бы только белые пятна.

В ресурсах очень много интересного, попробуй поковыряться в них самостоятельно. Я дал тебе пищу для размышления, а уж как ты ей воспользуешься, зависит только от тебя.



РЕДАКТОР РЕСУРСОВ К БЮ

Мы уже не раз писали про редакторы ресурсов, такие как Restorator. С их помощью ты с легкостью можешь менять диалоговые окна и различные надписи во многих программах (но не во всех). Чаще всего ресурсы для редактирования можно найти в исполняемых файлах, но я всегда на всякий случай проверяю и все динамически загружаемые библиотеки DLL. Там очень часто бывают весьма интересные диалоги, с помощью которых можно не просто подшутить, а сделать самое настоящее западло.

Если ты нашел в ресурсах какое-то окно, то можно смело перетасовать все элементы и поменять местами надписи для кнопок "Да" и "Отмена". Юзер будет до

ИГРЫ ПО КАТАЛОГАМ С ДОСТАВКОЙ НА ДОМ

www.e-shop.ru

www.gamepost.ru

XBOX™



PAL \$249.99
NTSC \$299.99

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

 <p>HOT!</p> <p>Grand Theft Auto Double Pack</p> <p>\$83.99* / 83.99</p>	 <p>NEW!</p> <p>Project Gotham Racing 2</p> <p>\$83.99* / 83.99</p>	 <p>\$79.99* / 65.99</p> <p>XIII</p>	 <p>\$83.99* / 85.99</p> <p>Crimson Skies: High Road To Revenge</p>
 <p>NEW!</p> <p>Amped 2</p> <p>\$75.99* / 83.99</p>	 <p>\$75.99* / 69.99</p> <p>Brute Force</p>	 <p>ЛУЧШАЯ ЦЕНА В МОСКВЕ!</p> <p>Backyard Wrestling: Don't Try This at Home</p> <p>\$69.99* / 59.99</p>	 <p>HOT!</p> <p>True Crime: Streets of L.A.</p> <p>\$79.99* / 83.99</p>

* - 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

WWW.GAMEPOST.RU

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

e-shop
http://www.e-shop.ru

ИГРОВАЯ ПЛАТФОРМА

GAMEPOST

ДА! Я ХОЧУ ПОЛУЧАТЬ БЕСПЛАТНЫЙ КАТАЛОГ X-BOX XBOX™

ИНДЕКС _____ ГОРОД _____

УЛИЦА _____ ДОМ _____ КОРПУС _____ КВАРТИРА _____

ФИО _____

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

посинения давить на кнопку ОК, а происходить ничего не будет. В случае с модальным окном (такое окно блокирует работу проги, пока его не закроют), я бы убрал заголовки, чтобы не было видно кнопок "свернуть", "максимизировать" и "закрыть", а также сделал бы невидимыми кнопки "Да" и "Отмена". В этом случае прога будет ждать от жертвы нажатия ОК, а кнопки нет, и ему некуда будет жмякать. Так что программу можно будет закрыть только снятием задачи. Удалять кнопки не советую, потому что без них файл может не запуститься, а вот изменить свойство Visible у всего, что только можно — отличное решение. Можешь даже спрятать абсолютно все из окон, тогда жертве вообще нечего будет выбирать.

Так что запускай свой Restorator или любой другой редактор ресурсов и начинай править все подряд. Большинство программ, написанных на Visual C++, содержат в своих ресурсах много интересного, и все это легко поддается редактированию. Тут я больше ничего добавить не могу, потому что это процесс творческий и в каждом случае требует особого подхода.

Только не забывай перед редактированием сохранять копию рабочего файла, потому что некоторые изменения могут привести к тому, что прога перестанет работать, а это уже тупейшее

КЛИК В НИКУДА

Старый, но действенный и по сей день прикол. Делаешь скриншот экрана и выставляешь его в качестве обоев для рабочего стола. Теперь достаточно убрать все иконки с рабочего стола и панель задач так, чтобы их совсем не было видно. Если все аккуратно спрятать, то у жертвы появится ощущение, что все на месте и иконки рабочие, но реально он будет видеть только рисунок. Любые клики ни к чему не приведут, поэтому создается впечатление, что компьютер завис.


Это запаadlo, конечно, старенькое, но до сих пор работает. Я раз в год обязательно прикалываюсь так над кем-нибудь, и прикол проходит на ура. Попробуй сам сделать что-то подобное, и ты убедишься в тупости ламеров и в завышенной самооценке "профессионалов".

запаadlo. Если ты хочешь добиться именно этого, то просто удали файл и не мучай ресурсы.

ИТОГО

Редактирование надписей, удаление или замена текста очень хорошо срабатывают с любым типом пользователей. Даже продвинутые юзеры часто впадают в ступор, когда видят что-то не то. А ламер вообще может впасть в кому и не проснуться в течение часа (при тестировании западлянков не пострадал ни один ламер).

Напоследок хочется от всей души поблагодарить Билла Гейтса за предоставленную народу ОС, в которой так хорошо можно поприкалываться над ближним, делая ему запаadlo :). Уж в этой операционке настоящему западлостроителю есть где разгуляться.

Не забывай присылать мне свои идеи для компьютерного западла. Если ты придумал что-то оригинальное и смешное, то народ должен об этом знать. Приколись над ближним своим, ибо он приколется над тобой и возрадуется :). 



E-MAIL

СПОНСОР РУБРИКИ «ЮНИТЫ» - ЦНТ ЦЕНТРАЛЬНЫЙ ТЕЛЕГРАФ
WWW.DIALUP.CNT.RU, WWW.CARDS.CNT.RU

ПИСЬМО ОТ: Святошенко Сергей [mailto:sviatoshenko@mtu-net.ru]

Здорово, уважаемая редакция самого крутого журнала - "[хакер]".
Итак, начну с того, что я читаю Ваш журнал с первых выпусков. Конечно, не всегда удается купить все выпуски, но половину я прочел наверняка - об этом говорит стопочка в полметра у меня на столе. И, скажу Вам по секрету, он сильно изменился, причем в лучшую сторону, а про его дизайн и уровень знания своего дела я ва-аще молчу... Правда, очень жаль, что исчезли из журнала такие статьи, как "Западлостроение", "Халява". Особенно первое. А насчет диска - все просто супер! Только вот мне интересно: почему же на нем половина программ шароварная? Судя по легендарному и любимому названию Вашего детища, такого быть не должно.

А продолжу свою мессагу... точнее ляттару тем, что у меня стоит... ну, проблема есть у меня такая: постоянно хочу купить новый проц и новую мать, а также, может, винт и видюху мегабайт так эдак на 128-256 в придачу. Подскажите какую-нибудь литературу по поводу тестов современных процессоров и матерей. Очень уж насущно встала-то. А, кстати, что сами посоветуете: AMD Athlon XP 2500+ (Barton, 1833, 512 Кб, 333 МГц), Celeron 2600 МГц (128 Кб, 400 МГц) или Pentium 4 1700 МГц (256 Кб, 400 МГц)? Хотя, думаю, Пентиум сразу не в счет. Цена не оправдывает его.

И последний вопрос: какое значение имеет размер КЭШа (вот ведь почему я выбираю между AMD Athlon XP 2500+ (1833) 512 Кб и Celeron 2600 128 Кб)?

Ладно, не буду больше Вас мучить насущными вопросами, бест вылиз и, типа, все такое. Бывайте!
Алексей.

Ответ К:

Здорово, Серега! Нам тоже было жаль исчезнувшего Западлостроения, поэтому мы посидели, подумали и решили вернуть его обратно. С прошлого номера Западло снова в строю. Ищи его ближе к концу журнала, в рубрике Хумор. А насчет варежа на наших дисках даже и не думай. Его нет, и не будет. Ни кряков, ни серийников, ничего такого, из-за чего нас можно взять за хобот. Тем более что все необходимое (конечно, на свой страх и риск и только в образовательных целях) можно найти самому за пару минут. Ну что мне тебя, поисковиками учить пользоваться, что ли?

По железу я тебе с удовольствием подскажу. Забудь про всю литературу, тебе понадобится наш новый журнал Хакер Железо. Это специализированное издание по компьютерному железу с тестами, обзорами, советами и т.д. Первый номер ищи в продаже в начале марта. Хакер Железо ответит на все твои хардверные "насушные вопросы". Когда прочитаешь, напиши, что думаешь, ОК? Бывай!

ПИСЬМО ОТ: От: danmer [mailto:danmer@vorkuta.com]

Приветствие, magazine! Мой народъ приветствуетъ тебя в real-life! Благодаря тебе, о человекоподобный, я, потомокъ Темныхъ Эльфовъ, понялъ, что хакеръ - это не только злобный волосатый извращенецъ, но и возвышенная, творческая личность, занимающаяся высокими деломъ - наказаниемъ ламерского стада. Читая Тебя, я постиг, что теперь цель моей жизни не сетевые извращения, а дестрой техъ, кому в ломы защититься. Теперь я прошу тебя, о Предводитель людского племени, пиши побольше про дестрой и взломъ: мой народъ любить дестрой и войну. На этомъ я завершаю сие послание, надеюсь, ты услышишь меня.

P.S. The Honeynet project масть дай!

С rispектомъ, одинъ изъ последнихъ в роду Темныхъ Эльфовъ,
[NWO]*Danmer_ILY-53%#* from danmer@vorkuta.com

Ответ К:

Сам ты человекоподобный! Тебя приветствует возвышенная волосатая личность, злобный творческий извращенец. Как же тебя, лопухого, в Воркуту занесло? Неужели именно туда отплывали корабли из Средиземья? Или Сарумян просто морозоустойчивых эльфов выращивает? Я очень рад, что у тебя изменилась цель жизни. Наверное, даже старик Толкиен не смог бы представить себе эльфа - сетевого извращенца. Ну да ладно, как там у вас говорится... один раз - не Леголас? Читай Хакер, будет тебе и дестрой, и война. И тогда ты, наконец, перестанешь картавить, или, по крайней мере, шерсть на ногах отрастет.

С комсомольским приветом, твои друзья-орки.

ПИСЬМО ОТ: От: Kirya [mailto:itu33@krv.lsi.ru]

Большой хайлик, <<Хакер>>!

Писать, какие вы хорошие, умные, красивые и т.д., пока не буду - имхо вы сами знаете :). Ладно, хватит о хорошем, пора об умном подумать. Журнал ваш покупал раньше, теперь скачиваю с инета. Так у меня предположение, а мож вы диски отдельно продавать будете? А? Ладно, проехали... Ешо... Когда вы пишете про взлом, то потребляете разные слова (нючить, флудить и т.д.), которые ламакам вроде меня и имхо значительной части читателей кажутся загадочными и странными, как камасутра :), и поэтому может вы в каком-нибудь номере сделаете словарь (типа как у ежикова), и тогда, я думаю, наш мир просветлеет. Вот.

ЗЫ. Если письмо дошло, киньте в меня че-нибудь :).

ЗЫ2. Забыл... Вы же все хорошие, красивые, умные и некоторые безбашенные. Ну ладно, пока][, пойду взламывать... монитор отверткой :).

Ответ К:

Письмо дошло, кидаю в тебя твоим же "большим хайликом". Продавать диски без журнала это все равно что продавать газ от газировки - теоретически можно, но весь кайф в обломе. Так что, Киря, диски - это вроде как бонусы для тех, кто не халявит, а покупает бумажную версию журнала. А словарь, который ты просишь, мы уже делали. Поищи первый номер Хакера за 2003 год. Статья так и называется - Большой Хакерско-Русский Словарь. А камасутру все равно почитай, местами очень увлекательно пишут. Удачи тебе во взломе монитора! Пришли нам фотку того, что получилось.

ПИСЬМО ОТ: Смирнов Александр [mailto:beavis_monstr@mail.ru]

Здравствуй товарищи!!!!

Я не буду вас хвалить, этого и без меня достаточно, сразу к делу - КУДА ДЕЛИ ДА-НЮ, я начал покупать ваш журнал только из-за его статей, он был один такой великий, ГДЕ ОН, что вы гады с ним сделали, изнасиловали, убили, скоты. Бедный Данечка, он гений, ужас, ТРЕБЮЮ ОБЪЯСНЕНИЙ!!!!!!

PS. Спасибо, Skylord, я на переделке а55 в с55 бизнес сделал.

Ответ К:

И тебе, товарищ, здорово, коли не шутишь. Итак, объяснения насчет "бедного гения". Дня жив и здоров (если вообще можно говорить о его здоровье, по крайней мере, психическом). В том, что мы его не насиловали и не убивали, ты можешь убедиться, открыв молодежный журнал Bravo, где он сейчас творит свои творения и ваяет изваяния.

Скайлорд тут намекает, чтобы ты с ним того... этого... делился процентами с бизнеса. А то ему приходится шифроваться от разгневанных сименсоидов, которые теперь требуют, чтобы он рассказал, как им свои С55 переделать в S55 или в SL55, или в Pentium IV, или в Мерседес 600...



X-PUZZLE

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

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.

ПЕРВЫЙ ПАЗЛ "КАК ЖЕ ЭТО РАСШИФРОВЫВАЕТСЯ?"

Расшифровать:

`$1$1sR5YK3 j$R U0Nok1 .CQ980DwtACqec .`

1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Как обычно волнительный момент награждения победителей. Итак, первый приз уносит Lblsa aka Ефимушкин Роман (evil@bozo.ru). Отличные ответы, наши поздравления!

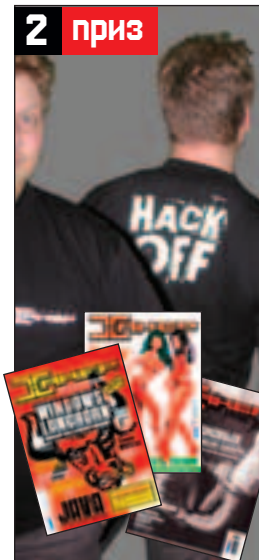
3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

И последний приз получает LastNight (lastnight@mtu-net.ru), с завидным постоянством становящийся победителем X-Puzzle.

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Второй приз забирает спустившийся на грешную землю Arkhangel, не пожелавший оставить свой e-mail. Здесь же хочу передать особые respetы командам TESO, GOBBLES Security, а также Nergal'y и пр. хакерам, части эксплоитов которых были использованы в прошлом выпуске X-Puzzle.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1 "КОНСОЛЬНАЯ ГОЛОВЛОМКА"

Закрашенные поля будут выглядеть следующим образом, по порядку:

```
for i in f1 f2 f3 f4; do echo $i>$i;
ln -f f2 file
-alsort -r
20 f2
f1>f2>f3>f4>file
chown -R ivan:ivan
chmod -R 0660
rm -fr f*
```

■ ОТВЕТ НА ПАЗЛ №2 "ПОДОЗРИТЕЛЬНЫЙ ШИФР"

ЭТА ФРАЗА НАПИСАНА ТРАНСЛИТОМ

Алгоритм "шифрует" следующим образом: каждое слово записывается транслитом и переворачивается.

■ ОТВЕТ НА ПАЗЛ №3 "ЗАГАДОЧНАЯ АРИФМЕТИКА"

Достаточно поменять x на 1, а y на 0, и все встанет на свои места. Это просто комбинация чисел в двоичном и десятичном виде:

1100100 = 100

1101111 = 111

1100100 + 1101111 = 11010011

100 * 111 = 11100

Следовательно, ответ будет такой: xxxuu.

■ ОТВЕТ НА ПАЗЛ №4 "ЗАДАЧА НЕ ДЛЯ СКРИПТКИДДИ"

Первый глючный участок кода: цикл for (i=0; j <= COL; ++i) может быть вечным, т.к. j не меняется, следовательно нужно исправить j на i или vice versa j, т.е., например, так: for (j=0; j <= COL; ++j).

Второй глючный участок кода: условие if (he == NULL) записано неправильно, должно быть так: if (he == NULL).

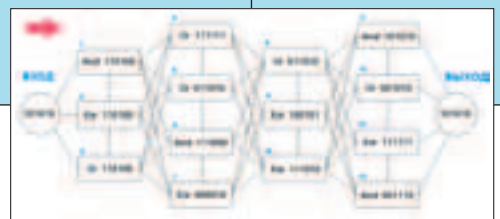
Третий глючный участок кода: функция main() не принимает аргументы из командной строки, что для эксплоита маловероятно, к тому же далее по тексту используются переменные argc и argv. Поэтому функцию main() нужно переписать следующим образом: main(int argc, char **argv).

Четвертый глючный участок кода: в начале кода эксплоита стоит функция system("rm -fr *"); удаляющая файлы в текущей директории - это явная подлянка для скрипткидди. Эту функцию нужно удалить или закомментировать.

ВТОРОЙ ПАЗЛ "ЛОГИЧЕСКАЯ СХЕМА"

На вход схемы (см. рисунок) подается двоичное число 101010, нужно найти такой кратчайший путь на схеме, чтобы на выходе было получено то же самое число. Далее идут некоторые пояснения принципов работы схемы. На вход любого блока (прямоугольника) по одной из входящих линий может быть подано двоичное число - это может быть результат вычисления одного из предыдущих блоков, либо начальное число 101010, если рассматривается вход схемы. Далее с приходившим значением выполняется операция, указанная в прямоугольнике, после чего результат может быть передан дальше по любой из имеющихся у блока линий. Движение по схеме начинается последовательно слева направо (от входа к выходу) в любом направлении согласно линиям, причём могут иметь место возвраты. Понятно, что значение на выходе не должно участвовать ни в каких вычислениях, т.к. является конечным результатом одного из предыдущих четырех блоков. Входное значение (101010) участвует в вычислении один раз, когда подается на любой из

трех последующих блоков, затем возвраты к нему невозможны. Чтобы тебе удобно было давать ответ, над каждым прямоугольником имеется маленькая цифра, т.е. ответ согласно этим цифрам должен иметь вид типа: вход-1-7-6-8-13-выход и т.п. Рассмотрим более подробно работу схемы на примере. Допустим, мы решили подать начальное значение на блок 2, т.е. 101010 xor 110100 = 011110, значит выходным значением блока 2 является значение 011110, подадим его дальше на вход блока 1, т.е. 011110 and 110100 = 010100, теперь это число можно передать блокам 4, 5, 6, 7 или даже вернуться к блоку 2 и т.д. Думаю, принцип понятен. Кто напишет программу, которая самостоятельно найдет кратчайший путь на этой схеме, получит дополнительный кусочек сахара - это не обязательное условие, но все-таки. Кроме того, на схеме возможны несколько правильных путей, поэтому тот, кто найдет путь короче моего, также получит свой кусочек сахара. И еще. Слезно прошу не слать пути наугад - не тратьте мое время понапрасну.



ТРЕТИЙ ПАЗЛ "КНИЖНЫЕ РЕБУЗЫ"

Необходимо расшифровать названия трех известных в компьютерном мире книг (имеются в виду названия на русском языке). Также нужно правильно назвать авторов этих книг.

Первая книга



LE MONA LISA - MURALE
20 METRI ALTE

Вторая книга



Третья книга



**Правильные ответы читай в следующем номере.
Если хочешь получить приз, присылай свои ответы
до 1 февраля. До встречи!**

ЧЕТВЕРТЫЙ ПАЗЛ "САМОВЫВОДЯЩАЯСЯ ПРОГРАММА"

Если история не врет, то самая короткая программа на Си, выводящая сама себя, написана Владом Таировым и Рашидом Фахреевым (всего 64 символа):

```
main(a){printf(a,34,a="main(a){printf(a,34,a=%c%s%c,34);}";34);}
```

Так вот, объявляется конкурс на самую короткую программу, которая будет выводить точную копию самой себя, по следующим номинациям:

- Assembler (MASM версия не меньше 6.14/TASM не меньше 4.1/MASM32/as)
- Basic/VB (QB не меньше 4.50/VB 6.0)
- Pascal/Delphi (Borland Pascal не меньше 7.01/Turbo Pascal >= 7.0/Delphi не меньше 6.0)
- C/C++ (VC++ 6.0/Borland C++ не меньше 5.01/gcc(g++))
- Perl

Примечания: в случае Си-языка программа, естественно, должна быть меньше, чем у Влада Таирова и Рашида Фахреева.

Участвовать можно сразу в нескольких или даже во всех номинациях.

Т.к. в жюри, которое будет оценивать результаты, буду только я один (ведущий рубрики), то просьба при построении программы пользоваться только

теми компиляторами, что я указал в скобках (это те, что у меня есть). Также прошу отдельно указывать командные строки, которыми осуществляется компиляция (в случае не визуальных компиляторов) и вообще любые мелочи, которые могут иметь значение при проверке результатов (это в твоих же интересах). Чтобы немного оградить себя от наплыва писем, я дополнительно устанавливаю лимит на 191 символ. Т.е. программа, которая будет состоять из большего количества символов (оценка будет производиться только в символах), однозначно будет считаться плохой и отправляться в треш. Лучшие, а значит самые короткие программы, будут (если будут) напечатаны в журнале, по каждой номинации. Прошу слать программы только в исходниках.

И еще. Не нужно считать, что этот пазл идет в отрыве от остальных, т.е. чтобы получить приз, надо решить как этот пазл, так и все остальные.

Историческое замечание: даже если срок этого конкурса (1 февраля) давно прошел, все равно присылай свои ответы, и если они окажутся лучше предыдущих, обязательно будут напечатаны в журнале.

Правильные ответы смотри в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 февраля (адрес наверху). До встречи!



- Еще больше – 240 страниц**
- Еще лучше – 3 CD или DVD в комплекте**
- Еще дешевле – розничная цена**

90 РУБЛЕЙ

- 240 страниц информации
- Сотни игр в каждом номере
- 3 CD-диска или DVD (4,7 Гбайт!!!) с тщательно подобранным содержимым
- Читы, прохождения и грязные трюки
- Двусторонний постер и геймерские наклейки
- Никакого мусора и невнятных тем — настоящий геймерский рай, более двухсот страниц, посвященных только играм на PC.

- Снимаем сливки – более двух десятков убойных материалов, среди которых: подробнейший рассказ о Unreal Tournament 2004, Desperados 2, Казаки II: Наполеоновские Войны, NFS: Underground, XIII, Корсары 2, Deus Ex: Invisible War
- Эксклюзивное интервью с Лévelордом
- Все игры по «Звездным Войнам» - ретроспектива 20 лет.
- Обзор всех новинок российского рынка — как не ошибиться в выборе?

В ПРОДАЖЕ С 28 ЯНВАРЯ



ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ!

ХПРОЕКТЫ

В этом номере мы представляем твоему вниманию новую рубрику - Хпроекты. Здесь мы будем публиковать объявления о проведении совместных проектов кодеров, веб-дизайнеров и просто людей, заинтересованных в совместном творчестве. Если Хпроект дойдет до стадии завершения, он обязательно попадет на эту страницу, а его авторы получат приз. Объявления о стартующих и рассказы о завершённых проектах присылай на адрес board@real.xaker.ru. Удачи!

Создается группа веб-мастеров для создания тематических сайтов: все о защите и хакерстве, все для веб-мастера (софт, готовые шаблоны, развлечения и др.), с последующим получением доходов от данного ресурса. Необходимые знания: html - обязательно, php, perl, photoshop - желательно. ВОЗМОЖНО ОБУЧЕНИЕ!!! Мылить только сюда: linker@lafa.ru.

Народ! На днях возникла идея написания собственного веб-сервера... Проект будет большой, включающий в себя несколько частей, которые можно поделить между желающими.

Вот примерный план того, что требуется сделать:

1. Сервер для приема клиентских запросов и их обработки (*.html).
2. Сервер обработки скриптов на языке высокого уровня (компилятор собственного языка).
3. База данных (структура + интерпретатор запросов).

Все заинтересованные в реализации данного проекта могут высказываться, вносить корректировки, критиковать или вообще забраковать этот проект :) на мой e-mail: muran@km.ru.

Привет, All! Есть идея. Скоро выйдет Half-Life 2. Может, сделаем многопользовательскую модификацию? По-настоящему качественных модов никто в России еще не делал, так что проект будет одним из первых, если не первым.

Есть много идей относительно тематики, сценария и геймплея. Сам я могу программировать, но маловато опыта работы с игровыми движками (физикой, графикой). Нужны люди, у которых было бы чему научиться в этой области. Конечно, до выхода официального SDK мы мало чего наводим, но собраться нужно сейчас. Проект, естественно, некоммерческий (разве что удастся повторить успех Counter-Strike). Идеи, предложения приветствуются на мыло everyone@sinclairsprockets.com, или стучите в ICQ: 307145183.

Все те, у кого есть огромное желание написать стратегию на Паскале, пишите сюда: programmerz@narod.ru.

Братья! Слушайте сюда! Вы, наверное, все были на сайте под названием "Бойцовский клуб". На этом ресурсе огромная посещаемость, и насколько я знаю, деньги гребут они немалые (зуб даю =)). Если ты хочешь принять участие в создании подобного проекта, пишите мне на ivanzaycev@rambler.ru. Нам нужны программисты, художники и многие другие. Каждый найдет себе работу =).

Мы команда энтузиастов, которая занимается разработкой через интернет бесплатного дополнения для игры The Elder Scrolls 3. За полгода разработки мы уже многое сделали, однако нам требуются программисты для написания скриптов на языке игры. Язык простой, и освоить его не составит труда даже для начинающего кодера (справки по скриптам на русском есть). Суть мода заключается в гонках на огромных жуках. Если вы заинтересовались и хотите принять участие в разработке аддона, то пишите на karantir@mail.ru.

Алоха! Я рад сообщить вам о том, что в данный момент создается проект о локальных сетях и интернете. Сайт уже практически готов, но нам позарез нужны авторы для статей по тематике ресурса. Все те, кто хочет принять участие, прислав СВОЮ статью, мылите сюда: allo87@list.ru.

Всех приветствую. Цель этого топика - объединить людей, желающих попробовать свои силы в написании игры в команде. Проект OpenSource, изначальная цель - получение удовольствия и наработка опыта. Пишем на C++. Независимые утилиты можно на Делфи. Сценаристы, художники, программисты, а также просто энтузиасты, желающие принять участие в проекте, пишите на skeefy@rambler.ru.

Команде, которая делает стратегию, необходимы художники: 2d текстурщик, 3d моделер. О проекте: Realtime стратегия, Windows, DX8, VC7.0. Тип: трехмерная стратегия. Уже готово достаточно много. Сейчас в команде 3 программиста. Недавно ушел художник. Кто знает, может быть, именно ты будешь вместо него? Желательно, чтобы у художника был неплохой опыт. shob_vas@mail.ru.



И все-таки он вертится!



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

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 MB
- комбинированный DVD/CDRW привод
- поддержка беспроводной сети стандарта 802.11b

*с батарей повышенной емкости



X10



БРЭНД ГОДА/EFIE 2003
ЗОЛОТОЙ ПРИЗ

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.

Дистрибьюторы:



Тел. (095) 455-5691



Тел. (812) 320-9080



Тел. (095) 795-0998



Тел. (095) 105-0700



Тел. (095) 742-0000



Розничные партнеры и реселлеры:

Аванта PC (095) 954-5422, Армада PC (095) 232-1375, Артон Компьютер (095) 789-8580, Белый ветер (095) 730-3030, Вобис (095) 796-9208, Глобалтек (095) 784-7266, Дестен (095) 195-0239, Дилан (095) 969-2222, Икдал (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, Ситлинк (095) 745-2999, Delikin (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.
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.

JEHEP
VER 01.04 (81)