борьба с инсайдерами снаружи и изнутри: утечки информации через USB/Ethernet-порты советы по воздвижению защитной системы с нуля /* 1я полоса */

крис касперски, no-email

воздвигая все новые и новые системы защиты, многие администраторы даже и не подозревают, что враги находятся не только снаружи, но также и изнутри корпоративной сети. это обычные сотрудники, копирующие конфиденциальные файлы через USB\Ethernet порты и выносящие их за пределы охраняемого периметра. давайте обсудим возможные каналы утечки информации и покажем как защититься от них используя только _штатные_ средства операционной системы семейства Windows NT

введение или постановка проблемы
*/*2я полоса, 1 колонка */*

Повсеместное распространение "флэшек" и ноутбуков сделало кражу корпоративной информации тривиальной операцией: просто воткнул карту памяти, скопировал нужные файлы и унес их с собой. Для защиты от "несунов" создано множество сторожевых комплексов (как правило, дорогостоящих и неэффективных), но в ряде случаев предотвратить хищение можно с помощью скрытых возможностей Windows XP/2000.

Рассмотрим типичный офисный компьютер с демонтированным floppy-дисководом, без CD/DVD-R/RWприводов, без интегрированных беспроводных устройств (типа BlueTooth, WLAN) и подключенный к локальный сети, имеющей выход в Интернет через proxy-сервер/NAT. Из всех портов имеется только USB и еще, возможно, COM/LPT.

За компьютером сидит продвинутый пользователь, который намеревается скопировать конфиденциальную информацию на свой домашний компьютер или же передать ее третьим лицам (за определенное вознаграждение). И в том, и в другом случае мы сталкивается с утечкой данных, которую администратор обязан предотвратить.

Договоримся, что мы будем ориентироваться исключительно на _пользователей_ разной степени "продвинутости", но не хакеров, поскольку хакера никакая защита не остановит. Существует множество дыр в Windows, позволяющих локальному пользователю поднять уровень своих привилегий до администратора, причем такие дыры не считаются критическими, т. к. они "нечувствительны" к удаленным атакам и затыкаются в последнюю очередь. К тому же, процент хакеров относительно невелик и львиная доля информации утекает через обычных пользователей. Следовательно, разработка антихакерской защиты экономически не оправдана.

Другой немаловажный момент. Механизмы разграничения доступа, реализованные в Windows XP/2000, позволяет скрыть от пользователя те файлы, которые ему по статусу видеть не положено. Однако, такая защита не всесильна и даже будучи правильно настроенной не может решить рядовую задачу: открыть пользователю доступ к файлам (с которыми он должен работать в силу производственной необходимости), но предотвратить их "вынос". Вот и приходится прибегать к дополнительным оборонительным средствам, используя аппаратно-программные комплексы сторонних производителей или же обходиться собственными силами.

>>> врезка как возникала эта статья
*/*2я полоса, 2 колонка, врезка */*

Собственного говоря, эта статья возникла в результате исследования, заказанного одной достаточно крупной компаний, страдающей хроническими утечками информации, перепробовавшей все имеющиеся на рынке средства защиты данных (которые, между прочим, денег стоят!), но оставшаяся недовольной достигнутым результатом.

Анализ, проведенный автором вместе с сотрудниками данной компании (кстати говоря, весьма компетентными специалистами, с которыми было приятно работать), панацеи, естественно, не открыл и серебренной пули не изготовил, но, по крайней мере, выявил основные каналы утечек (между прочем, плохо согласующиеся с данными, предоставленными весьма

уважаемыми агентствами такими как InfoWatch так и Symantec). После чего обнаруженные бреши в системе защиты были заблокированы штатными средствами операционной системы без каких бы то ни было переделок существующего программного обеспечения и с минимальной перестройкой сетевой инфраструктуры, то есть, говоря другими словами, за вычетом расходов на исследование практически даром.

Имя компании автор разглашать не имеет права (таковы, увы, условия подписанного с ней "джентльменского" договора, плюс имеется ряд других соображений политического характера), однако, результатами исследования может поделиться вполне, сразу же обращая внимание читателя, что это вовсе не "серебренная пуля", а всего _частный_ случай решения _частной_ проблемы. Кому-то она может пригодится, а кому-то и нет. Но в любом случае, автор надеется, что приведенная информация окажется небесполезной.

>>> врезка исследуем свои тылы
*/*2я полоса, 2я колонка */*

На задней стенке компьютера типичного офисного компьютера находится много чего интересного (в качестве наглядно-учебного пособия рассматриваться компьютер автора). Это, в первую очередь Ethernet-порт (на рисунке 1 подсвеченный желтым и зеленым светодиодами, первый из которых сигнализирует о передаче данных, а второй — указывает на наличие Ethernet-соединения) Кабель можно вытащить и вставить, например, в ноутбук (или карманный компьютер), получив возможность "сливать" на свой диск любую конфиденциальную информацию, к которой мы только имеем доступ, причем сливать с очень высокой скоростью — вплоть до 1 Гигабита в секунду. Развернув принцип на 180 градусов, мы втыкаем шнурок от ноутбука в офисный компьютер, забрасывая туда вредоносные программы, позволяющие шпионить за сетью и повышать уровень локальных привилегий до администратора.

Здесь же, на задней стенке, находятся USB-порты, позволяющие подключать различные устройства, приводящие к утечкам данным: карты FLASH-памяти, беспроводные адаптеры (типа Голубого Зуба или Wi-Fi).

Для передачи небольшого объема данных сойдут низкоскоростные и COM/LPT-порты (кстати говоря, некоторые модели современных материнских плат уже выпускаются без них). А вот цифровой звуковой выход (красный огонек на рисунке 1) и цифровой видеовыход это пока что экзотика, однако, уже существуют хакерские программы и оконечные устройства использующие их для передачи данных, естественно, при условии, что хакерское программное обеспечение уже установлено на офисном компьютере.

Рисунок 1 задняя стенка компьютера

/* 2я полоса, 3я колонка, вертикальный рисунок на всю колонку */

источник утечки — USB
/ 3я полоса, колонка 1 */*

USB-порты, перекочевавшие на лицевые панели ПК (и даже на корпуса USB-клавиатур!) значительно упростили обмен файлами между компьютерами. Существует огромное количество USB-устройств: от FLASH-карт до PDA и ноутбуков. Правда, ноутбуки, в силу своих габаритов, менее популярны среди инсайдеров, но все-таки их нельзя списывать со счетов.

Как защититься от кражи? Самое простое (но и самое радикальное) — отключить USB-разъемы от "мамы", опечатав корпус или воткнуть в них заглушки, обильно смазанные "суперклеем". Смешно? Скорее грустно, поскольку к таким мерам администраторы прибегают достаточно часто. Офисный компьютер может работать и без USB. Ему не нужны никакие периферийные устройства, к нему не нужно подключать принтер (для этого есть локальная сеть). Поэтому, такое решение вполне жизнеспособно, вот только… в некоторых случаях без USB приходится очень туго.

ОК, устанавливаем на компьютер систему защиты типа ZLock или любую другую. Их много, но принцип один. Специальный драйвер перехватывает запросы на запись к USB и в зависимости от политики доступа либо разрешает запись, либо выдает сообщение об ошибке. USB с полностью закрытым доступом равносилен USB с заглушкой, только заглушка стоит порядка на два дешевле и, кстати говоря, совершенно необязательно сажать ее на клей. Достаточно закрыть разъемы специальным щитком с замком, который изготовит любой слесарь или даже сам администратор при минимальных навыках работы с металлом.

Поэтому, на практике защитные средства ал-я ZLock ограничиваются блокировкой записи определенных файлов, список которых формируется администратором. На первый взгляд все выглядит просто замечательно, однако, при ближайшем рассмотрении в защите обнаруживается огромная дыра.

Допустим, у нас имеется документ MS-Word. Что помещает пользователю сохранить ее под другим именем или скопировать в буфер обмена и вставить в файл, который не внесен в "охраняемый" список?! Даже если список включает в себя расширения или защита анализирует типы файлов, основываясь на их содержимом, пользователь может сжать файл малоизвестным архиватором или замаскировать его каким-нибудь другим способом. Как ни крути, а защита на основе списков, не способна остановить даже человека с именем Анастасия, не говоря за всех остальных мужчин.

источник утечки — Ethernet
/ 3я полоса, колонка 2 */*

Кабели локальной сети — это артерии и вены любой организации, имеющей более одного компьютера и это основной источник утечек, который, в отличии от USB, уже нельзя закрыть заглушкой, поскольку, даже если физически приклеить Ethernet-разъем к компьютеру, все равно остается достаточное количество хабов со свободными портами (см. рис. 4), в которые можно воткнуть шнурок от ноутбука или мини-файлового севера, которые уже давно появились в продаже и некоторые из них легко умещаются в кармане.

Злоумышленнику достаточно всего лишь подключить свое устройство к свободному Ethernet-порту и вот он уже в локальной сети и ему подвластны все файлы, к которым он только имеет доступ. Остается скопировать их и убраться восвояси.

Как от этого защищаться?! Прежде всего необходимо настроить маршртутизаторы, привязав локальные IP-адреса к MAC-адресам, и закрыть на брандмауэре все незанятые Ethernet-порты. Это намного проще и надежнее, чем помещать хабы в железный сейф, стоимость которого (помноженная на количество хабов в сети) весьма значительна.

Естественно, прописывание MAC-адресов в настройках брандмауэра/маршртутизатора занятие довольно утомительное, к тому же не существует никакой возможности отличить настоящий MAC-адрес от поддельного (не говоря уже о том, что в большинстве сетевых устройств MAC-адрес хранится во FLASH-памяти и может быть изменен), однако, для осуществления подобной атаки злоумышленник должен обладать хакерскими навыками, а мы уже договорились, что от хакеров мы не защищаемся.

источник утечки — COM/LPT
/ 3я полоса, колонка 2 (продолжение) */*

Некоторые модели современных компьютеров вообще не имеют COM/LPT портов и с точки зрения безопасности это очень хорошо, поскольку, используя ноутбук, злоумышленник может установить "прямое кабельное соединение" и скачать все необходимые файлы, правда, через COM большой файл за пару минут не скачаешь, да и у LPT пропускная способность находится на очень низком (по современным меркам!) уровне.

Но все-таки, угроза утечки есть и эти порты лучше сразу же закрыть заглушками, а на заглушки повесить печать или соорудить какой-нибудь примитивный замок. Кстати, если LPT-порт используется для подключения принтера, то без замка тут однозначно не обойтись, поскольку в противном случае, злоумышленник сможет запросто воспользоваться этим разъемом для своих нужд. Впрочем, принтеры на LPT постепенно отживают свое и производители активно переходят на USB и Ethernet. Естественно, с точки зрения безопасности, Ethernet самый предпочтительный, поскольку администратор можно заблокировать подключения любых других Ethernet-устройств на этот порт, простой проверкой MAC-адресов.

>>> иллюстрации
/ 3 полоса, колонка 3 */*

Рисунок 2 USB-порты на лицевой панели так и просят, чтобы в них воткнули FLASH-карту

Рисунок 3 адаптер "Голубого Зуба" (такой зеленый прямоугольник), несанкционированно подключенный к USB-порту нечестным на руку сотрудником и обнаруженный лишь спустя длительное время

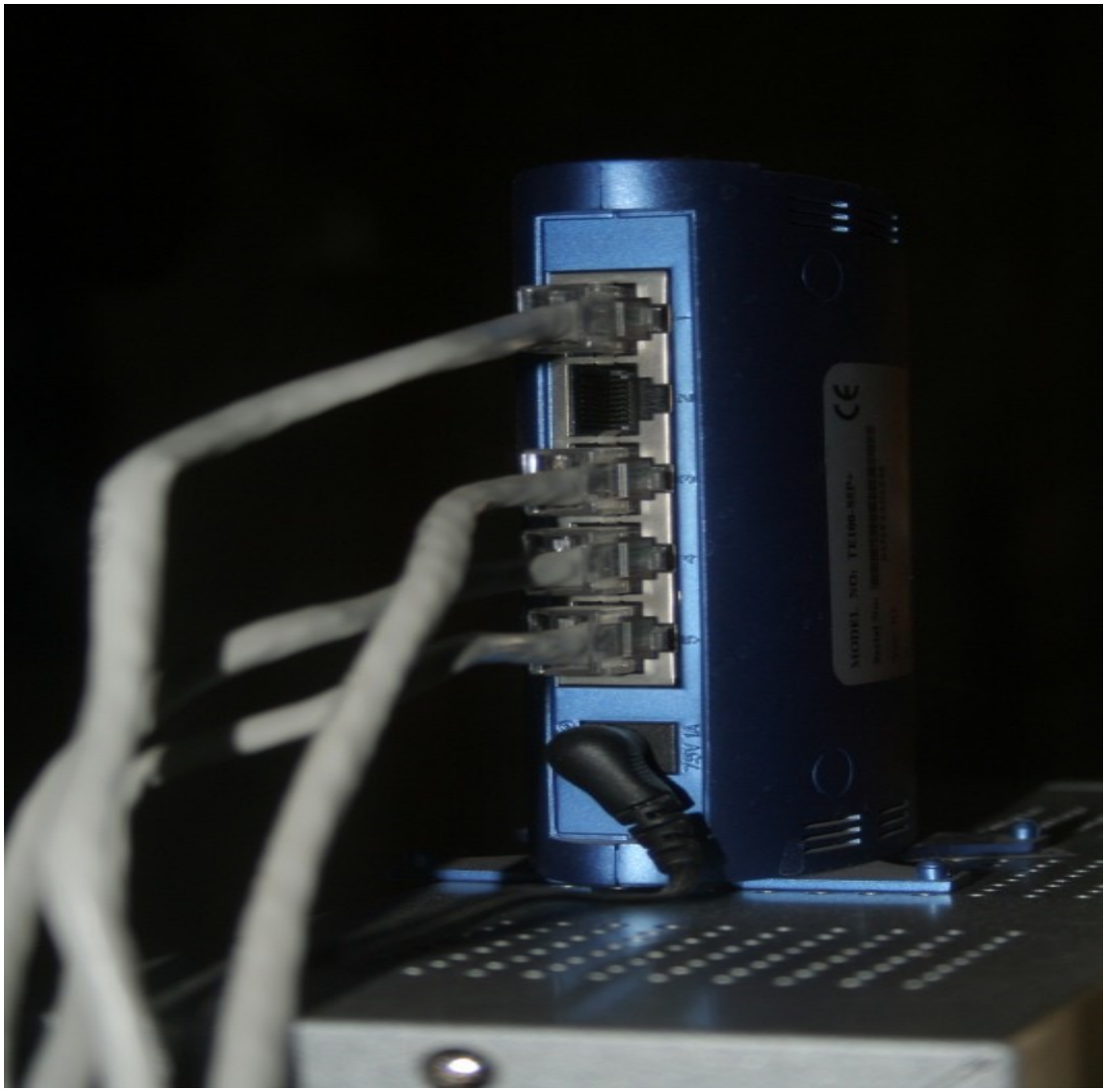

Рисунок 4 маршутизатор со свободными портами — прямая угроза атаки

методы защиты, основанные на NTFS-потоках
/ 4я полоса, колонки 1, 2 */*

Файловая система NTFS выгодно отличается от FAT16/32 тем, что поддерживает несколько потоков (streams) в рамках одного файла, так же называемых атрибутами (attributes), только не путайте их с атрибутами типа "только на чтение" или атрибутами времени создания/доступа/последней модификации — это совершенно различные сущности.

Каждый файл от рождения имеет один безымянный поток, и именно с этим потоком мы работаем, при открытии/закрытии файла, и именно его размер берется за основу при подсчете размера файла. Однако, мы можем создавать и другие потоки, отделяя их названия от имени файла символом ":", например, X:\my_file:my_stream1, X:\my_file:my_stream2. Естественно, полный путь указывать необязательно и X:\my_file:my_stream1 работает так же хорошо, как и my_file:my_stream1 (если, конечно, my_file:my_stream1 находится в текущем каталоге).

Проведем простой эксперимент. Возьмем FAR и, нажав <Shift-F4> (создание нового файла), введем "kpnc:nezumi", после чего в отрывшемся окне редактора наберем что-нибудь наподобие "hello, world!" или любой другой лозунг. Сохраняем изменения по <F2> и выходим. Смотрим — FAR (и "Проводник" Windows) показывают нулевой размер файла. Странно, не правда ли?! Нажимаем <F4> и видим, что файл действительно пуст. Но если нажать <Shift-F4> + "kpnc:nezumi", то наше приветствие "hello, world!" вновь появится на экране.

Если нет FAR'a, тот же самый фокус можно проделать и со штатным "Блокнотом", только… в силу ограниченных умственных способностей его создателей, он требует, чтобы имя

файла и имя потока оканчивалось обязательным расширением ".txt", иначе ничего не получится! ОК, окажем ему услугу. Пишем в командной строке "notepad kpnc.txt:nezumi.txt", утвердительно отвечая на запрос о создании нового файла. Вводим что-нибудь, сохраняемся. Выходим. Теперь, если попытаться открыть файл двойным щелчком, мы ничего не увидим (безымянный поток остается пустым) и "Проводник" отрапортует о нулевом размере файла, но стоит набрать "notepad kpnc.txt:nezumi.txt", как… содержимое потока nezumi.txt немедленно появляется на экране!!! Ну прямо чудеса на виражах!!!

Теперь поговорим как эти "чудеса" можно использовать на практике. При копировании на файловую систему, отличную от NTFS (например, на лазерный диск или FLASH'ку, размеченную под FAT), копируется _только_ безымянный поток, а все остальные игнорируются. При передаче по локальной сети все потоки сохраняются (и это хорошо!), однако, ни FAR, ни Проводник не позволяют выбирать какие именно потоки копировать, а какие нет. Утилита командной строки "copy" с этим так же не справляется, обвиняя нас в неправильном синтаксисе, хотя он правильный. Некоторые утилиты (например, RAR) поддерживаю сохранение всех потоков файла, чтобы полученный архив было можно записать на не-NTFS носитель, а при последующей распаковке на NTFS разделе получить все потоки обратно.

Потоки — идеальное средство для защиты от несанкционированного копирования файлов. Создаем файл с тремя потоками. Первый — безымянный и может содержать все, что угодно (или же не содержать ничего). Второй — именованный. Именно он хранит тело документа/электронной таблицы/базы данных с которым необходимо работать. Третий (именованный) поток выполняет роль своеобразного балласта и несет на своем борту несколько гигабайт мусора, сгенерированного произвольным образом и желательно очень трудно сжимаемого архиваторами.

Допустим, злоумышленник захотел скопировать этот файл на FLASH'ку, размеченную под FAT. Тогда он получит только первый (безымянный) поток, не содержащий ничего или содержащий грозное предупреждение с пожеланием немедленно явится к начальнику с повинной. Если же это FLASH'ка отформатирована под NTFS, то "Проводник" попытается скопировать все три потока, но третий поток туда ни за что не влезет (правда, с учетом порядка копирования потоков, поток-балласт, должен следовать вторым, а поток с полезной нагрузкой - идти последним, но это уже детали).

Аналогичным образом обстоят дела и с передачей файла по сети. Незаметно передать несколько гигабайт злоумышленнику не удастся, особенно если на исходящий трафик установлен жесткий лимит.

Единственная возможность — передать файл по сети на ноутбук, подключенный через Ethernet, но о защите Ethernet-портов от подключения "левых" устройств мы уже говорили, так что злоумышленник остается с носом. Не такая уж плохая защита, особенно с учетом того, что ее создание не требует никаких дополнительных затрат и реализуется штатными средствами операционной системы.

>>> врезка недостатки предложенной защиты
/ 4я полоса, колонка 3 */*

- открыв файл в Word'е/Excel'е и скопировав его в буфер обмена, злоумышленник сможет записать его через USB, если USB-порт открыт на запись, а так же передать по сети через тот же Skype;
- квалифицированный программист сможет написать программу для выборочного копирования отдельных потоков (впрочем, этой угрозой можно пренебречь, мы же сразу договорились, что защищается только против пользователей);
- потоки-балласты занимают достаточно много места, уменьшая полезную емкость жесткого диска (хотя, при современных объемах жестких дисков несколько дополнительных гигабайт на каждый секретный файл — вполне посильная ноша и приобретение более емких винчестеров обойдется дешевле специализированных защитных комплексов от сторонних разработчиков);

>>> врезка источник утечки — Skype
/ 4я полоса, колонка 3 */*

Среди прочих средств голосовой связи, Skype выделятся тем, что шифрует свой трафик и виртуозно обходит NAT'ы всесте с брандмауэрами, используя протоколы **STUN** и **TURN,** а

если они не срабатывают — гонит трафик через http-proxy, автоматически определяя настройки браузера. Другими словами, Skype представляет собой идеальное средство для передачи файлов из локальной сети в "дикий" Интернет, причем кому был передан файл определить невозможно, поскольку Skype использует распределенную сеть, каждый из узлов которой может использоваться для обслуживания всех остальных абонентов. Максимум, администратор "вычислит" Skype-имя пользователя, получившего уворованный файл, но, поскольку Skype выдает имена, не требуя предъявления никаких документов, то для установления личности оно, естественно, не подходит.

К сожалению, программ для детектирования и блокирования Skype-трафика не существует и единственное, что может администратор — периодически сканировать клиентские компьютеры на предмет наличия этого самого Skype и тут же удалять его как зловредную программу.

Естественно, помимо Skype конфиденциальная информация может быть передана через электронную почту или любой файло-обменный сервер, типа http://rapidshare.com/, но они в отличии от Skype по крайней мере оставляют следы в логах proxy-серверов и брандмауэров, позволяя вывести нечестного сотрудника компании на чистую воду, но… только пользы от этого будет немного. Ведь секретный файл уже ушел и назад его не вернешь.

>>> врезка возможные каналы утечки информации / 4я полоса, колонка 3 */*

Вот три основных источника угрозы: USB\Ethernet-порты и средство голосового общения Skype, поддерживающее режим передачи файлом.

COM\LPT-порты используются значительно реже, но все-таки представляют достаточный интерес как для злоумышленников, так для тех, кто от них защищается. Цифровые выходы звуковой карты и монитора — это уже из области экзотики, которой занимаются только хакеры-электронщики.

Остальные способы требуют либо вскрытия компьютера, либо чрезвычайно высокой квалификации злоумышленника, а потому здесь не рассматриваются.

методы защиты, основанные на запуске программ от имени спец пользователя / 5 полоса, колонки 1, 2 */*

Допустим, мы имеем "оператора архива", который должен резервировать все файлы, но при этом не должен иметь к ним доступа, чтобы не утащить налево. Возможно ли это?! Здравый смыл шепчет, что нет, в то время как операционные системы семейства NT (и UNIX в том числе) утверждают, что да. Все очень просто. Пользователь запускает программу, от имени другого пользователя, обладающего правами доступа ко всем файлам, которая выполняет архивацию и записывает результат в указанный оператором архива файл, но доступа к этому файлу оператор не имеет!!! Чтобы злоумышленник не подсунул программе резервирования сменный носитель, который потом будет подключен к другой машине, на которой он обладает правами администратора (например, к своему домашнему компьютеру), следует использовать атрибут шифрования файла, тогда для его открытия одних лишь прав администратора окажется недостаточно и еще потребуется заполучить ключ, хранящейся в учетной записи того пользователя, от имени которого запускается программа архивации, и эта учетная запись оператору архива, естественно, недоступна. Подобная практика защиты очень широко распространена и соответствующие профили даже встроены в Windows NT, однако, ничто не мешает нам использовать ее не только для архивации, но и для повседневной работы с секретными файлами.

Рассмотрим, например, MS Word, запускаемый от имени специального пользователя с тщательно настроенными правами доступа к секретным файлам. Как следствие, обычный пользователь сможет открывать/сохранять файлы только через MS Word, но не сможет скопировать их через "сохранить как…" То есть, скопировать-то он их сможет, но вот открыть сохраненный файл — нет, даже если он записан на FLASH'ку, КПК или другое устройство. К сожалению, по умолчанию буфер обмена одного пользователя доступен всем остальным, что позволяет "перетягивать" секретные файлы через copy/paste, однако, изменив настройки политики безопасности можно (и нужно!) сделать буфер обмена спец. пользователя невидимым для всех остальных.

Перспективы просто фантастические, и самое главное — никому не нужно ничего платить. Достаточно приобрести операционную систему семейства Windows NT (но только не Windows Vista, в которой по умолчанию выставляются довольно "демократичные" права доступа, позволяющие инсайдерам повышать уровни своих привилегий вплоть до администратора) и… опс! Разработчики Windows NT забыли доделать запуск программ от имени других пользователей с автоматическим вводом пароля, запрашивая его явным образом в специальном диалоговым окне, а это значит, что секретный пароль придется сообщать всем простым пользователям, иначе они не смогут запустить ни Word, ни другое защищаемое нами приложения, но зная пароль…

Здесь возможны два выхода из ситуации. Первое — Word запускает администратор, и оставляет его открытым, не позволяя пользователям его закрывать. Глупо конечно и утомительно, зато бесплатно. Второе — пишем свой собственный загрузчик, запускающий программы от имени других пользователей и автоматически передающий им пароль, жестко прошитый в его теле, а, чтобы пароль не бросался в глаза при просмотре файла в hex-редакторе, зашифруем загрузчик любым exe-упаковщиком.

Кстати, поскольку проблема необходимости явного ввода пароля (кстати говоря, отсутствующая в UNIX-подобных операционных системах) возникла не вчера и даже не позавчера, в сети можно найти множество готовых загрузчиков, в том числе и бесплатных, однако, по соображениям безопасности, лучше не доверять чужому коду и нанять программиста, который напишет несколько сотен строк на Си самостоятельно, предоставив вам исходный код, чтобы у него не возникло соблазна встроить туда закладку.

заключение
/ 5 полоса, колонка 2 */*

Описанные методики были опробованы на нескольких компаниях и дали положительный результат (более подробный отчет о проделанной работе автор планирует выкладывать на свой собственный сервер http://nezumi.org.ru, доступный как по протоколу ftp, так и по http).

Утечки информации в "подопытных" компаниях практически полностью прекратились, и заказчики остались весьма довольны тем, что им не пришлось платить за кота в мешке, которым являются решения конкурентов, не раскрывающие ни исходных текстов, ни даже технических подробностей алгоритмов работы своих аппаратно-программных комплексов.

Гавриленко Иван Борисович
научный редактор,
архитектор систем предотвращения вторжения
краткая рецензия на статью, демонстрирующая
уровень его компетентности
/* 6 полоса, колонка 1 */

Рисунок 5 Гавриленко Иван Борисович собственной персоной

> Договоримся, что мы будем ориентироваться исключительно
> на _пользователей_ разной степени "продвинутости ",
> но не хакеров (и не на программистов), поскольку хакера
> никакая защита не остановит
Пессимистично звучит. Означает - просто сложить ручки???
Нет ничего не возможного. Фраза только подчеркивает "неопытность" автора.

> Существует множество дыр в Windows, позволяющих

> локальному пользователю поднять уровень своих
> привилегий до администратора, а то и до уровня ядра
Используется термин Администратор. Уровень ядра - это пользователь System (0)

> К тому же, процент хакеров относительно невелик и львиная доля
> информации утекает через обычных пользователей. Следовательно,
> с экономической точки зрения, разработка абсолютно надежной
> защиты (а таких защит вообще не существует в природе!)
Как собственник компании я тогда спрошу - а зачем мне тогда все это надо?
Зачем статья?

> Вот три основных источника угрозы: USB\Ethernet-порты
> и средство голосового общения Skype , поддерживающее
> режим передачи файлом.
Откровенно говоря, неправильно.
USB - это коммуникационный порт.
Ethernet - это сетевой интерфейс, либо протокол.
ПО Skype - это всего лишь ПО для приема-передачи VoIP трафика и чата.
На порядки большую угрозу несут электронная почта и браузер.

> Прежде всего необходимо настроить маршртутизаторы,
> привязав локальные IP-адреса к MAC-адресам, и закрыть
> на брандмауэре все незанятые Ethernet -порты.
> Это намного проще и надежнее, чем помещать хабы в
> железный сейф, стоимость которого (помноженная
>на количество хабов в сети) весьма значительна
Абсолютно неэффективно и невыгодно.
У меня на работе даже секретарша может сменить mac адрес за 2 мин.
ответный комментарий автора
ну тут я уже не удержался. эх!!! где бы мне таких если не секретарш
то хотя бы секретарей раздобыть

> Среди прочих средств голосовой связи,
> Skype выделятся тем, что шифрует свой трафик
> и виртуозно обходит NAT'ы всесте с брандмауэрами,
> используя протоколы STUN и TURN
Ничего подобного. Абсурд и бред.
Если обходит - значит надо не искать способы блокирования приложения,
а новых системных администраторов (либо администраторов безопасности),
отвечаючих за прокси и межсетевые экраны.

> К сожалению, программ для детектирования
> и блокирования Skype-трафика не существует
Ничего подобного! В заголовках сетевых пакетов
пишется информация о получателе. Она - не шифруется.

/ 6я полоса, колонка 2, 3 — иллюстрации */*

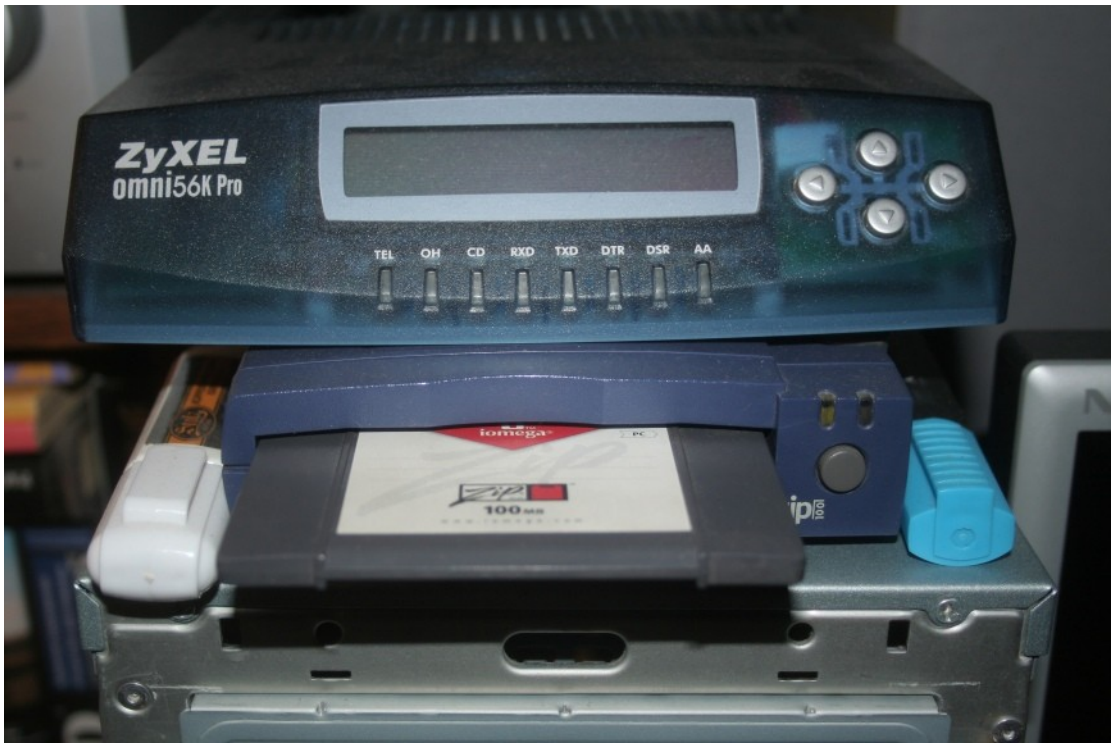

Рисунок 6 ZIP-дискеты еще не раритет, и кое-где они все-таки используются, так что не нужно забывать, что инсайдер может утащить в кармане сотни мегабайт

Рисунок 7 сотовый телефон с ИК-портом или прямым кабельным соединением — хорошее оружие инсайдера, особенно учитывая количество гигабайт памяти, способной поместиться внутри него

Рисунок 8 CD/DVD-R/RW приводы вкупе с мини-дисками представляют собой отличное средство для выноса информации

Рисунок 9 мини-диск, свободно помещающийся в кармане