Поиск malware на Server 2003/XP своими руками

Крис Касперски

Глобальных эпидемий не вспыхивало уже несколько лет, но локальные очаги заражения продолжают разрастаться, осваивая новые территории. Покажем, как обнаруживать свыше 90% заразы бесплатным ПО. Главным образом, мы будем говорить о Server 2003/XP, однако сказанное во многом справедливо и для Server 2008/Vista.

Антивирусы, изначально рассчитанные на борьбу с вирусами (то есть с саморазмножающимися программами, внедряющими свою, возможно, слегка измененную копию в другие файлы) к нашествию троянских коней оказались совершенно не готовы. Троянская программа никуда не внедряется, пишется (на основе готовых компонентов) чуть ли не за несколько минут, после чего обрабатывается упаковщиком/протектором и «сливается» в Сеть, например, путем широковещательной/избирательной почтовой рассылки. К тому времени, пока пользователи заподозрят что-то неладное и пошлют файл в антивирусный центр на исследование (если еще найдут его на диске!), вредоносное программное обеспечение (далее по тексту именуемое malware) уже сделает свое черное дело, например, разошлет спам, найдет и передаст конфиденциальную информацию, создаст новую учетную запись, допускающую удаленное подключение хакера и т. д. Грамотно спроектированное malware обычно уничтожает себя буквально через несколько минут, а то и секунд после запуска вредоносного файла.

Основную зацепку представляют готовые компоненты, используемые хакерами, чтобы не писать каждый экземпляр malware с нуля. Теоретически их можно занести в базу сигнатур, детектируя заразу на ранних стадиях внедрения. Практически же универсальный распаковщик, встроенный в антивирусы, справляется лишь с простейшими упаковщиками. Все, что посложнее, – распаковывается набором статических распаковщиков, запрограммированных вручную и «тупо» повторяющих алгоритм оригинального упаковщика. Проблема в том, что алгоритм упаковки может быть легко изменен прямо в hex-редакторе. Хакеру достаточно перенести оригинальную точку входа (OEP – Original Entry Point) в другое место, чтобы обхитрить антивирус или воткнуть в начало файла конструкцию, вызывающую у антивируса «несварение желудка».

Обычно это что-то из набора команд SSE/SSE2/SSE3 – в настоящий момент их не эмулирует ни один антивирус, а переменная длина x86-команд не позволяет продолжить декодирование инструкций после встречи с первой же неизвестной командой. То же самое относится и к самомодифицирующемуся коду (особенно выполняющемуся на стеке), структурным исключениям… Да что там говорить, хакеру достаточно «закрутить» цикл, исполняющийся секунду или около того, чтобы эмулятор антивируса «отвалился» по тайм-ауту. Никакой антивирус не эмулирует кодов ошибок, возвращаемых API-функциями, которые могут быть использованы для расшифровки остального тела файла (скажем, malware открывает заведомо несуществующий файл, но антивирус-то этого не знает! А «подобрать» правильный ключ расшифровки – выше его сил!).

Таким образом, хакеру достаточно взять широко распространенную зловредную программу, обработать ее новейшим упаковщиком/протектором, слегка изменив код последнего так, чтобы статический антивирусный распаковщик не смог справиться с ним – и все! Антивирус будет молчать как партизан! Что же касается C#-программ, то их элементарно декомпилировать штатным дизассемблером ildasm.exe, слегка модернизировать CLR-код и ассемблировать его заново штатным же ассемблером ilasm.exe – антивирусы вновь отдыхают, а хакеры размножаются со страшной силой – легкость программирования, большое количество готовых руководств, компонентов и библиотек вызывает активный приток «пионеров» всех мастей, в то время как еще буквально 5-10 лет назад написание вируса представляло собой нетривиальную задачу, требующую глубокого знания внутренностей операционной системы, ассемблера и… уймы свободного времени, которое нечем занять.

И хотя некоторые антивирусы (такие, например, как Norman) «прогоняют» подозреваемые файлы через своеобразную «песочницу» (sandbox), в грубом приближении представляющую собой эмулятор операционной системы, с тщательной проверкой изменений состояния реестра и файловой системы после завершения работы подопытной программы, они не панацея, а очередное «плацебо» для успокоения пользователей. Достаточно сказать, что экзотические API-функции типа NtSetLdtEntries() ни сам Norman, ни его «коллеги» не эмулируют, то же самое относится и к NtSystemDebugControl(), что позволяет

Укрепляем линию обороны

Чтобы затруднить атаку на систему, рекомендуется заблаговременно предпринять ряд несложных действий. Во-первых, переименовать ядро (файл ntoskrnl.exe) во что-то другое (например, nezumi.exe), а вместо ntoskrnl.exe положить ядро от другой версии системы (не забывая обновить его и в кэше SFC, иначе весь труд пойдет насмарку, и она тут же его восстановит). Фокус в том, что для определения адресов перехватываемых функций многие rootkit вызывают функцию LoadLibrary («ntoskrnl.exe»), даже не догадываясь о том, что ядро переименовано и полученные адреса весьма далеки от действительности! Корректно написанный rootkit в таком случае просто откажется от перехвата, некорректный (коих большинство) грохнет систему, что неприятно, но все-таки лучше заражения.

А как же сообщить самой системе, где искать новое ядро? Очень просто – добавить в файл boot.ini «волшебный» ключик «/kernel=», после чего строка с описанием операционной системы будет выглядеть приблизительно так:

Листинг 1. Фрагмент «защищенного» файла boot.ini

```
multi(0)disk(0)rdisk(0) ↵
      partition(1)\WINNT= ↵
      "Server 2003" /fastdetect / ↵
      kernel=nezumi.exe
```

Только не забудьте перед установкой пакетов обновления вернуть прежнее ядро на место, иначе инсталлятор аварийно завершит свою работу, поскольку, он (как и rootkit) не догадывается о возможности переименования ядра.

Кстати, большинство создателей вредоносных программ свято верят в то, что Windows всегда стоит на диске «C:» и нагло используют абсолютные пути, даже не заглядывая в соответствующие переменные окружения. Следовательно, поставив систему на любой другой диск (например, «D:» или «F:»), мы отсечем часть зловредных программ еще на подлете. Windows Update, кстати говоря, обрабатывает такую ситуацию вполне адекватно.

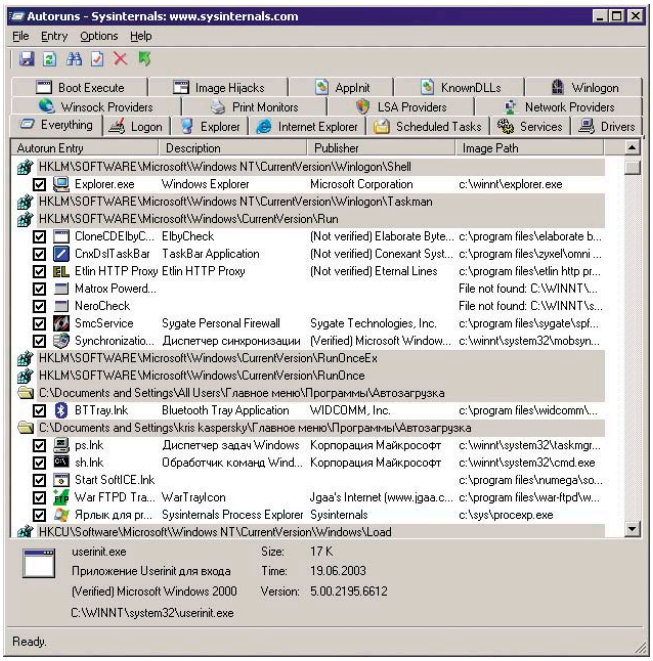

Рисунок 1. Внешний вид утилиты Autoruns от Марка Руссиновича

зловредному коду в лучшем случае остаться незамеченным, а в худшем – вырваться из-под контроля эмулятора, попав на живую машину со всеми вытекающими отсюда последствиями.

А чего вы хотели? Антивирус – тупая машина. Мыслит шаблонно, и всякий нормальный хакер обязательно проверяет созданный им вредоносный код на большой коллекции свежих антивирусов, совершенствуя алгоритмы маскировки до тех пор, пока они перестанут его обнаруживать.

Мораль: поиском заразы должен заниматься человек, чей живой и неординарный ум оперирует отнюдь не шаблонами, а логикой, размышлениями, интуицией. Близкое знакомство с malware показывает, что подавляющее большинство вредоносных программ элементарно обнаруживается буквально с первого взгляда. И не нужно платить никаких лицензионных отчислений, постоянно качать самые свежие базы, мириться с тормозами pro-активных технологий и прочих прелестей прогресса.

Мы будем рассматривать только бесплатные общедоступные утилиты и простые технологии обнаружения вредоносного ПО, не требующие глубокого знания внутренностей системы и умения читать дизассемблерный код. А раз так, чего мы сидим!

Вперед!

Закулисные игры автозагрузки

Чтобы «окопаться» на вражеском компьютере, вредоносная программа должна пустить корни, прописав себя в автозагрузку. Разумеется, термин «автозагрузка» в данном контексте очень условен – это может быть и сетевой фильтр, и сервисная служба, и расширение к Internet Explorer – в системе существуют сотни мест, в которые можно незаметно внедриться, получая управление сразу же после загрузки Windows или при наступлении определенных событий (запуска IE или другого приложения).

Просматривать все ключи реестра, прямо или косвенно связанные с автозапуском, не только утомительно, но и нецелесообразно, поскольку, «невооруженным глазом» очень трудно отличить легальные компоненты от нелегальных. Что делать?! И тут на помощь приходит бесплатная утилита Autoruns от Марка Руссиновича, показывающая огромное количество «злачных» мест, куда любит внедряться вредоносное программное обеспечение (см. **рис. 1**).

Для облегчения восприятия вся информация разбита на 16 вкладок (точнее – 15, 16-я включает содержимое остальных). Но даже такое изобилие отнюдь не гарантия полноты. Увы!

Существуют десятки мест, вполне подходящие для внедрения, которые Autoruns не показывает. Например, malware может вклиниться в цепочку ассоциаций расширений. Скажем, при открытии .doc-файлов управление получает не MS Word, а зловредный файл, делающий свое черное дело и запускающий оригинальный MS Word, так что с точки зрения пользователя не происходит ничего подозрительного. То же самое относится и к пунктам контекстного меню. Допустим, у нас есть пункт «Add to zip/rar», но вместо архиватора сначала запускается вредоносное ПО (подменившее эту ветвь в реестре) и только потом передающее управление оригинальной программе.

Так вот, всего этого Autoruns не показывает! Это вовсе не призыв к отказу от его использования (более достойных утилит мне пока не попадалось), просто к полученным результатам следует относится со здоровой долей скептицизма, не забывая о необходимости ручной проверки системы.

Самым ценным свойством программы является возможность сохранять список элементов автозагрузки в текстовой файл, а затем в любой момент времени сравнивать его с текущим («File → Save As», «File → Compare»). «Новоявленные» элементы (см. **рис. 2**) помечаются зеленым цветом (хм, почему зеленым, а не красным?! ведь самое время бить тревогу!). Сравнение списков – очень мощное оружие, помогающее обезвреживать не только malware, но и некорректно написанные программы, лезущие своими грязными лапами туда, куда их не просят.

К минусам утилиты Autoruns можно отнести невозможность просмотра всех пользовательских профилей: даже будучи запущенной из-под администратора, она показывает только элементы автозагрузки текущего профиля, но никогда – всех профилей сразу. Правда, при запуске из-под администратора у нас появляется меню «User» со всеми пользователями, зарегистрированными в локальной системе, и для получения достоверного результата нам необходимо сохранить в log-файлы их все. Главное, потом не запутаться, какой log какому пользователю принадлежит, иначе можно получить очень неожиданный результат.

Рядом с каждым элементом автозагрузки находится галочка, сброс которой приводит к его отключению, причем программа хранит состояние всех элементов, и при желании отключенные элементы можно активировать вновь, если, конечно, их отключение не приведет к краху системы так, что нам вообще не удастся загрузиться, и тог-

да придется прибегнуть к танцам с бубном. Отключенные элементы автозапуска хранятся непосредственно в самом реестре, в частности, элементы из ветки \Software\Microsoft\Windows\CurrentVersion\Run\ попадают в подветку AutorunsDisabled, что необходимо помнить при запуске «Консоли восстановления» для подъема рухнувшей системы, а лучше – перед всякими экспериментами просто зарезервировать реестр любой из многочисленных утилит, коих за последнее время развелось…

Другая полезная функция – верификация цифровой подписи от Microsoft, для этого достаточно щелкнуть правой клавишей мыши по интересующему нас элементу автозагрузки и сказать «Verify». Если цифровая подпись совпадает, то рядом с именем программы появляется статус (Verified), означающий, что данному компоненту автозагрузки можно на 99% доверять. К сожалению, с компонентами от сторонних разработчиков верификация не работает, но, с другой стороны, в большинстве случаев ничего плохого не случится, если их временно отключить и посмотреть, что у нас упало. Ага, перестал работать прокси-сервер или ADSL-модем. Значит, все правильно, полет нормальный, и можно возвращать элемент автозагрузки на место. А вот если ничего не упало, то следует призадуматься, выбрав в том же контекстном меню пункт «Search Online» и поискать, что пишут о данном файле на WEB. До тех пор пока Sysinternals не продалась Microsoft, поиск работал через Google, теперь же он работает через MSN, то есть никак не работает (во всяком случае у меня) и приходится либо вбивать имя exe-файла в строку поиска Google вручную, либо изменять параметр «onlinesearchcommand» в ветке реестра программы Autoruns с MSN на Google и радоваться прогрессу, весне и автоматизации.

Обычно malware прописывает себя в фиксированные каталоги под фиксированными именами, и поиск на WEB оказывается довольно плодотворным, хотя и дает большое количество ложных срабатываний, от ложно-позитивных до ложно-негативных. Однако при возникновении подозрений файл можно немедленно отправить на www.virustotal.com – специальную on-line службу, собравшую под одной крышей пару десятков популярных антивирусов со свежими базами. Естественно, как мы уже говорили выше, верить антивирусу может только наивный, но дополнительная проверка никому не помешает.

Также стоит обратить внимание, что далеко не все элементы, причастные к автозагрузке, на самом деле являются таковыми. В частности, содержимое ветки реестра HKLM\System\CurrentControlSet\Services перечисляет драйверы, которые могут быть запущены вызовом ZwLoadDriver или каким-либо другим путем, однако их присутствие в данной ветке само по себе еще не приводит к автоматической загрузке драйвера, поэтому, ее следует

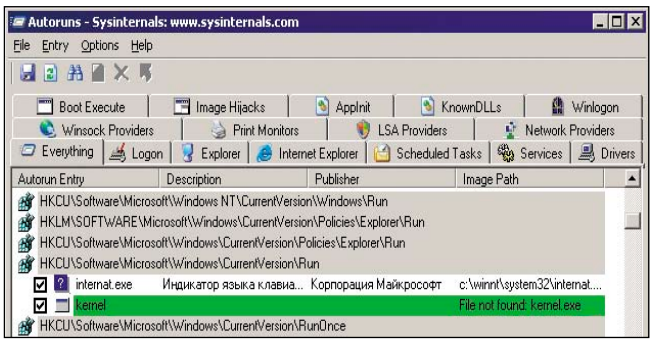

Рисунок 2. Сравнение логов элементов автозагрузки позволяет выявлять внедрение нового вредоносного ПО

рассматривать лишь как потенциальную угрозу. В той же самой ветке перечислены и активные сервисы (также называемые «службами»), при этом Autoruns показывает лишь запущенные сервисы, «забывая» упомянуть сервисы, загружаемые вручную или вызываемые из других служб при наступлении определенных обстоятельств.

Наведя курсор на любой файл и нажав <ALT+ENTER>, мы получим стандартное диалоговое окно со свойствами, среди которых иногда можно обнаружить цифровую подпись (если она есть), а также имя производителя и прочие данные, содержащиеся в секции ресурсов исполняемого файла/динамической библиотеки и, естественно, подверженных угрозе фальсификации. Если цифровой подписи нет (а чаще всего ее нет), то кто угодно может написать здесь что угодно, однако, как показывает практика, хакеры крайне редко утруждают себя подделками, а если и пытаются выдать malware за продукцию известной компании, то подделывают ее имя столь неумело, что тут же разоблачают себя.

А вот что действительно важно – из диалога «свойств» можно извлечь дату создания исполняемого файла/динамической библиотеки на диске. Если, допустим, вы никаких программ уже полгода как не устанавливали, и тут вдруг появляется файл, созданный совсем недавно, это наводит на размышления (естественно, вредоносный файл может изменить дату своего создания, но пока с такими «умными»

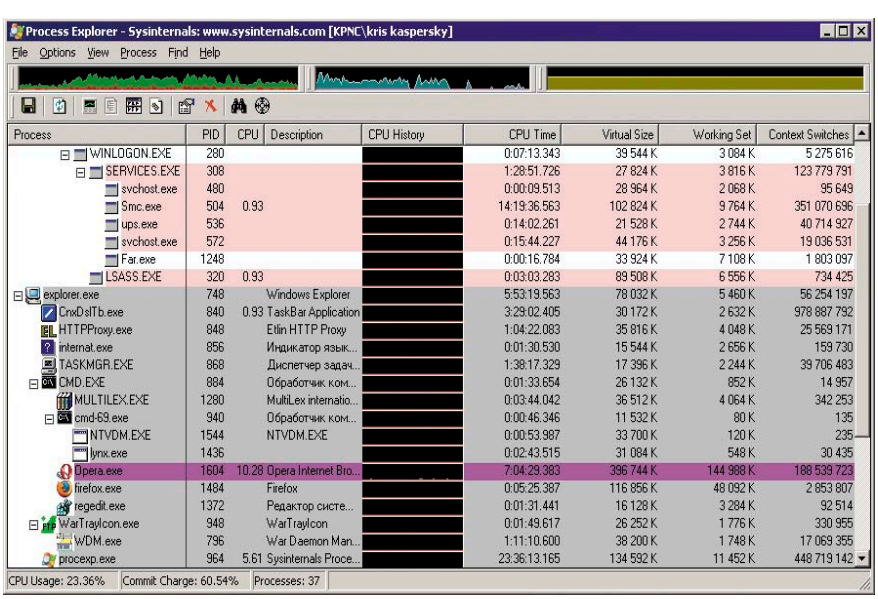

Рисунок 3. Внешний вид утилиты Process Explorer

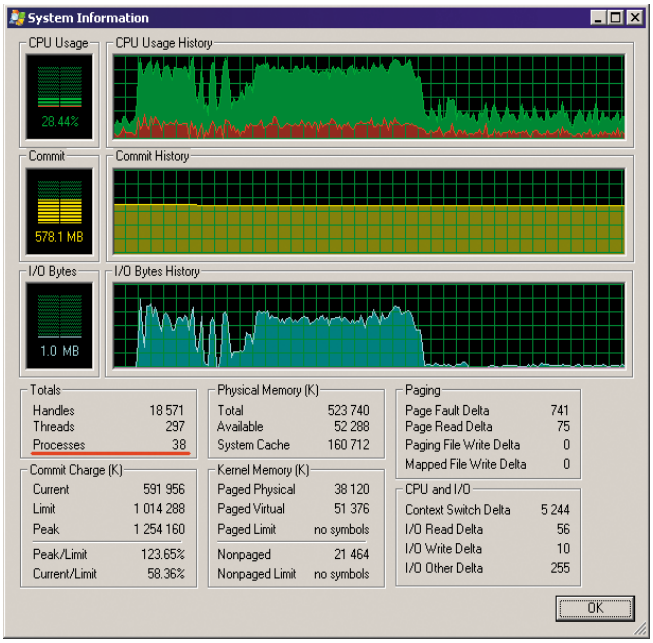

Рисунок 4. Счетчики производительности в окне «System Information» – еще один источник данных о количестве процессов в системе

вирусами мне сталкиваться еще не приходилось) и чтобы исследовать его свойства, достаточно вызвать «Process Explorer» из контекстного меню. Это еще одна утилита от Марка Руссиновича, очень мощная и очень полезная в плане поиска malware. И на этой ноте мы заканчиваем описание Autoruns и переходим к Process Explorer.

Process Explorer

Грубо говоря, «Process Explorer» – это аналог «Диспетчера Задач», только намного более мощный (см. **рис. 3**). Искать malware с его помощью – одно удовольствие. Первое, что мы видим при запуске, – это список процессов (включая процессы, не отображаемые в «Диспетчере Задач»). Многие rootkit предпринимают неслабые усилия для удаления себя из списка процессов, и в этом плане доверять Process Explorer нельзя. Эх, взять бы отладчик Soft-Ice, напрямую работающий с низкоуровневыми структурами ядра и не оставляющий rootkit никакого шанса, но… Soft-Ice – это платный продукт, да к тому же еще и мертвый. Старые версии не работают под Server 2008/Vista, а новых не предвидится…

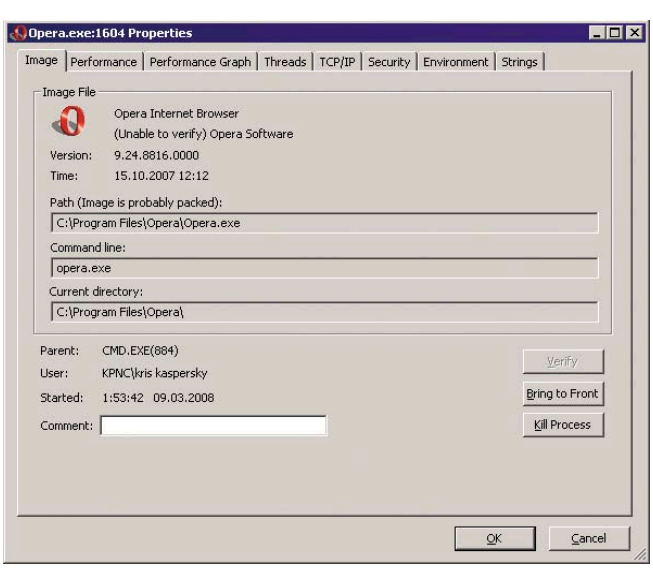

Рисунок 5. Вкладка «Image» – основные свойства процесса

Тем не менее здесь есть один очень хитрый трюк, способный разоблачить большое количество rootkit. Дело в том, что операционные системы семейства NT поддерживают два различных механизма перечисления процессов – средства TOOLHELP32, выдающие информацию по каждому процессу, и счетчики производительности (performance counters), подсчитывающие общее количество процессов в системе, обмануть которые намного сложнее, да и существующие rootkit даже не пытаются это делать (наверное, просто не знают, что есть такая лазейка).

Жмем <CTRL+I> для вызова диалогового окна «System Information» (см. **рис. 4**), где и видим показания счетчиков производительности: «Processes: 38», в то время как статусная строка Process Explorer насчитывает всего 37 процессов, то есть на один процесс меньше! Кто не верит – может сосчитать процессы вручную!

Расхождение в показаниях указывает на наличие Rootkit, который в данном случае действительно имеет место быть (причем ни KAV, ни DrWEB, ни NOD32 с самыми свежими базами его так и не обнаружили, хотя он был выловлен в дикой Сети более полугода назад – вот и верь после этого антивирусам). Но хватит лирики. Ближе к делу. Как же поймать этот неуловимый rootkit? Исходя из самых общих рассуждений: раз rootkit поселился в системе, то, вероятно, он нашел способ получать управление при загрузке, и, с определенной степенью вероятности, один из элементов автозапуска (о которых мы говорили выше) и есть наш rootkit, так что просмотрим представленный список еще раз. И внимательнее! Исключение составляют rootkit, проникающие через дыры в системе и обитающие исключительно в оперативной памяти, умирая сразу же после перезагрузки, кстати говоря, это довольно распространенное исключение, и количество таких rootkit неуклонно растет, особенно на серверах, которые не «перезагружаются» неделями или даже месяцами (личный рекорд моего домашнего сервера – полгода без перезагрузки). У Руссиновича на этот счет есть специальная утилита Rootkit Revealer (о ней мы поговорим чуть позже), которая может помочь. А может… и не помочь. К сожалению, очень трудно порекомендовать рецепт универсального противоядия против всех rootkit и остается только радоваться, что 90% – 96% malware ловится буквально голыми руками.

Наведя курсор на процесс и вызвав контекстное меню, мы можем:

- «убить» процесс (иногда это требует, чтобы Process Explorer был запущен с правами Администратора);
- приостановить процесс, вогнав его в сон, – кстати, не совсем безопасная операция, многие честные программы после пробуждения отказываются работать, а зловредное программное обеспечение зачастую держит «теневой» процесс-монитор, отслеживающий остановку/смерть основного и автоматически перезапускающий его вновь, что немедленно разоблачает вредоносную сущность последнего;

Удаленная проверка системы

Администратор должен заботиться не только о здоровье сервера, но и всего «зоопарка» вверенных ему машин (основных рассадников вредоносного ПО), но скакать по всем этажам, отвлекая пользователей от текущих дел, – это же какую выдержку нужно иметь! Спортивная подготовка также не помешает. Если же всего этого нет – вероятно, стоит задействовать возможности удаленного администрирования, выполняя «медосмотр» узлов локальной сети, не покидая пределов своего любимого кресла и попивая кофе (чай, квас) из огромной черной кружки с надписью «root».

Существует множество путей решения задачи. Во-первых, это штатный telnet-сервис, входящий в комплект поставки начиная с W2K, а, быть может, и раньше. Telnet (с некоторыми ограничениями) поддерживает работу консольных приложений, но это еще ничего. Хуже другое – он должен быть изначально запущен на всех рабочих станциях (что отличается от его состояния по умолчанию). То же самое относится к многочисленным утилитам сторонних разработчиков, многие из которых поддерживают и графические приложения (неожиданное появление которых на экране страшно нервирует пользователей) и ни одна из известных мне утилит не позволяет запустить заданную программу на всех узлах локальной сети, не делая никаких дополнительных телодвижений.

PsExec от Марка Руссиновича (входящая в комплект PsTools) относится к тем приятным исключениям, которые поддерживают удаленный запуск программ на всех (или заданных) узлах, при необходимости автоматически копируя программу на удаленный узел.

Однако в ее использовании немало скрытых подводных камней. Запускающий ее пользователь должен принадлежать к группе администраторов, и, что самое важное, на удаленной машине необходимо заранее создать пользователя из группы администраторов с тем же самым именем и паролем, в противном случае удаленный запуск не получится. Также необходимо держать запущенной службу удаленного доступа к реестру (Remote Registry service) и открыть на брандмауэре все порты, ответственные за RPC-доступ (после памятных атак червя MSBlast эти порты очень часто закрываются, хотя Windows Firewall в конфигурации по умолчанию держит их открытыми).

Другой подводный камень намного более серьезен. Это даже не камень, а прямо айсберг какой-то (чей собрат, по всей видимости, потопил «Титаник», а все потому, что никто не хочет думать головой). Попытка удаленного запуска утилиты autorunsc.exe (консольной версии утилиты autoruns.exe) «подвешивает» консоль, не давая никакого полезного выхлопа. Пляски с бубном (типа перенаправления вывода и все такое) не помогают! «Диспетчер задач» показывает, что процесс висит, но… не выполняется, то есть очень даже хорошо выполняется! После того как компания Microsoft приобрела фирму Sysinternals, она обязала Марка Руссиновича добавить ко всем утилитам NAG-screen с текстом лицензионного соглашения (EULA), вспыхивающий при первом запуске (см. **рис. 6**).

Экран, конечно, графический с кнопочками «согласен»/«не согласен». Они-то и подвешивают «консоль» при удаленном запуске, и, чтобы все прошло успешно, все утилиты Марка Руссиновича хотя бы однажды должны быть запущены на каждой машине от имени Администратора (точнее, пользователя, входящего в группу администраторов на данной машине). Естественно, это ужасно напрягает, сводя все преимущества удаленного запуска на нет. К счастью, если добавить специальный ключик в реестр (что можно сделать и удаленно), никакого NAG-screen больше не будет. Короче, открываем (удаленно, конечно) ветку: HKCU\Software\Sysinternals\<имя_программы>, где <имя программы> – название утилиты, например, в нашем случае – «AutoRuns», создаем параметр EulaAccepted типа DWORD и устанавливаем его в 1 (см. **рис. 7**).

Все! Теперь можно запускать утилиту autorunsc.exe на удаленной машине с помощью утилиты psexec.exe, и все будет работать (ключ -c – копировать программу на удаленный узел перед запуском, автоматически удаляя ее после завершения работы, если вместо имени узла – в данном случае \\S2K3VM\ – указать «*», то программа будет запущена на всех узлах локальной сети, естественно, за исключением текущего! Ну разве не красота?!).

Листинг 2. Пример удаленного запуска утилиты autorunsc.exe на узле \\S2K3VM

```
$L:\>psexec.exe \\S2K3VM\ -c autorunsc.exe -b

PsExec v1.94 - Execute processes remotely
Copyright (C) 2001-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

Sysinternals Autoruns v9.13 - Autostart program viewer
Copyright (C) 2002-2008 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute
       autocheck autochk *
           autocheck autochk *
           Auto Check Utility
           Microsoft Corporation
           5.02.3790.1830
           c:\windows\system32\autochk.exe
           d18fa3530aa4124a9d64f97162b1e3df                                (MD5)
           08052f92587247180835b8ad13ddd79b33587864                        (SHA-1)
           d49e8d367e1d9f1b9b0a05ef6a3d1188a83eb540086b8dbe78ea1688447 (SHA-256)
autorunsc.exe exited on S2K3VM\ with error code 0.
```

- можно перезапустить процесс, вызывать JIT-отладчик (если он установлен в системе и если вы разбираетесь в ассемблере), повысить/понизить приоритет процесса, найти главное окно приложения, автоматически переключившись на него, поискать имя процесса на WEB и… наконец вызывать пункт «Properties» (Свойства), в котором, кстати говоря, и собрано большое количество инструментов, полезных для поисков malware (см. **рис. 5**).

На первой (слева) вкладке «Image» перечислены основные свойства образа исполняемого файла: название (взятое из ресурсов – если оно там есть), путь к исполняемому файлу, процесс-родитель, пользователь, запустивший этот файл на выполнение, и т. д. Если же всех этих параметров нет, значит, у Process Explorer не хватает прав для их получения – запустите его под Администратором, а в некоторых случаях и пользователем типа System, для чего

Рисунок 6. NAG-Screen, вспыхивающий при первом запуске всех утилит Руссиновича, в том числе и консольных

можно воспользоваться системным планировщиком, вызываемым утилитой at.exe, входящей в штатный комплект поставки. Если же и под System данные о файле получить не удается – кто-то очень сильно постарался, чтобы скрыть их от нас. Кто бы это мог быть? Явно не пингвин (кстати, пингвины очень больно кусаются), а нечто более воинственное типа malware.

Другой тонкий момент. Допустим, обнаружили мы подозрительный файл, определив путь запуска, заглянули туда FAR, а там… нет ничего такого!!! Вариантов два: либо это rootkit, скрывающий свое присутствие на диске, и тогда попытка создания exe-файла с заданным именем в заданном месте вернет ошибку. Либо же… активный процесс не может удалить себя (система блокирует файл от записи и удаления), но разрешает его переименование, следовательно, зловредная программа могла переименовать себя во что-то другое, причем переименование действует в пределах всего дискового тома, а не только текущего каталога! Другими словами, подлинный путь запуска зловредной программы определить непросто, а без этого мы не можем ни удалить ее с диска, ни отослать на www.virustotal.com для проверки! К сожалению, универсального решения данной проблемы нет. Отсутствие файла по указанному пути – верный признак вредоносного ПО, но вот где его искать – это хороший вопрос!

Вкладка «Performance» содержит данные о памяти, потоках и операциях ввода/вывода, выполняемых процессом, что позволяет (приблизительно) определить его род занятий. В частности, интенсивный ввод/вывод программы, замаскированной под русификатор, наводит на размышления, и эти размышления отнюдь не в пользу программы.

«Performance Graph» – основные данные счетчиков производительности, представленные в графической форме. Нас, главным образом, интересует нижняя диаграмма, отображающая ввод/вывод, без которого не обходится практически ни одно malware, сканирующее диск в поисках конфиденциальной информации или рассылающая спам от нашего имени, или… что бы она ни делала, без ввода/вывода ей не обойтись.

Вкладка «Threads» перечисляет потоки процесса вместе с базовыми адресами их создания, позволяя «убивать» или «замораживать» ненужные нам потоки. Malware активно использует потоки для внедрения в адресное пространство «доверенных» процессов, таких, например, как Opera.exe, Firefox.exe, чтобы получить беспрепятственный доступ в Сеть и не создавать еще один процесс, привлекающий к себе внимание. Теоретически, можно было бы запомнить, сколько потоков имеет тот или иной процесс, а при появлении новых – карать их нещадно, но, к сожалению, многие приложения создают потоки динамически, по мере надобности. То же самое относится к драйверам (в том числе и драйверам звуковых карт), поскольку создание потока в контексте процесса – один из немногих способов взаимодействия ядерного кода драйвера с прикладным кодом и API (прямой вызов диалоговых окон из драйвера невозможен, и ему волей-неволей приходится пробивать «тоннель» в адресное пространство прикладных процессов, впрочем, мы отклонились от темы).

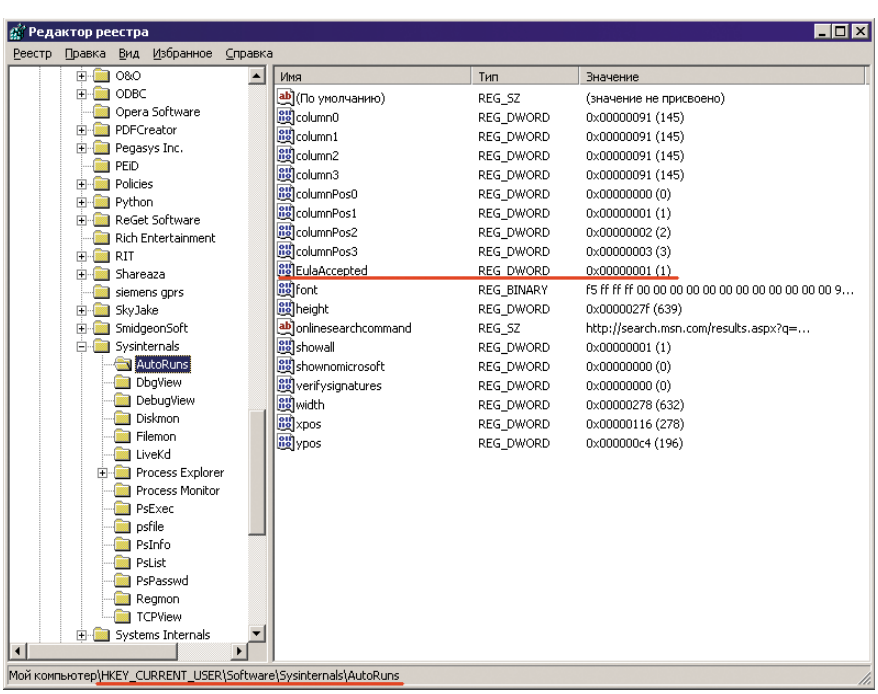

Рисунок 7. Обход NAG-Screen при помощи удаленного редактирования реестра

Потоки, созданные malware, которые мы ищем, в 96-99% случаев располагаются в области динамической памяти (также называемой кучей), в то время как легальные потоки – в тех же 99% дислоцируются внутри страничных образов динамических библиотек или самого исполняемого файла. Главное – это правильно определить стартовый адрес потока, чего Process Explorer делать не умеет, и хотя я указал Марку Руссиновичу на данную ошибку больше года назад, выслав демонстрационный «вирусоподобный» код вместе с кодом для определения подлинных стартовых адресов, Руссинович оставил все как есть, чем существенно затруднил поиск вредоносного программного обеспечения (см. **рис. 8**).

Но кое-какие зацепки у нас все-таки есть. Потоки, созданные с помощью функции CreateRemote Thread (а в большинстве случаев используется именно она), согласно Руссиновичу, имеют стартовый адрес KERNEL32.DLL+0xB700 (где 0xB700 – смещение кода, лежащего внутри API-функции CreateRemoteThread, и, естественно, слегка отличающееся в зависимости от версии Windows). Самое противное, что многие «честные» программы также используют CreateRemoteThread, причем на вполне легальных основаниях. Так в чем же все-таки разница?! Наводим курсор на поток и нажимаем кнопку «Stack» – у честных программ там будет куча вызовов, ведущая к RPCRT и другим библиотекам, а вот у malware стек обычно пуст. Описанный метод, конечно, не самый надежный, но… имея под рукой только Process Explorer без всяких отладчиков, лучшего, пожалуй, и не придумаешь. Прибив зловредный поток кнопкой «Kill» или заморозив его по «Suspend», смотрим на реакцию приложения – ее отсутствие вкупе с нормальным продолжением работоспособности укрепляет нашу уверенность, что мы имеем дело именно с malware.

Вкладка «TCP/IP» содержит список активных сетевых соединений, легко выдающий примитивные зловредные программы. Действительно, если мы установили игрушку типа «Тетрис», а она внезапно слушает какой-то порт, ожидая подключений, – это же back-door, причем явный. Естественно, продвинутые вредносные программы не дадут себя обнаружить так просто, и остается утешаться только тем, что их количество относительно невелико.

Вкладки «Security» и «Environment» мы пропускаем как не содержащие ничего интересного, а вот на String задержимся надолго. Казалось бы, что можно найти в списке ANSI-строк?! Ничего интересного… А вот и нет! Во-первых, список берется не из исполняемого файла (в случае malware, как правило, упакованного), а из его распакованного образа в памяти. Практически никто из современных хакеров не утруждает себя шифрованием строк в runtime, и эти самые строки содержат не только имена API-функций, с которыми работает программа, не только ключи реестра, но и различные высказывания (как правило, оскорбительного характера), адреса серверов, на которые следует отсылать добытую информацию – да много еще чего! Строки – верный ключ к выявлению malware. Исключение составляют, пожалуй, лишь зловредные программы, упакованные сложными протекторами с динамической распаковкой, но таких не так уж и много.

Rootkit Revealer

Никому не нужная игрушка, которая реально ничего не ловит, а только создает видимость спокойствия. Марк Руссинович утверждает, что Rootkit Revealer обнаруживает все rootkit, выложенные на www.rootkit.com, что не соответствует истине, поскольку на www.rootkit.com имеется множество rootkit, успешно борющихся с Rootkit Revealer теми или иными способами, о существовании которых Руссинович наверняка знает, но делает вид, что все идет по плану. К тому же на www.rootkit.com выкладываются преимущественно «сырые» proof-of-concept-программы, полноценные версии которых распространяются на коммерческой основе или же используются для целенаправленных атак.

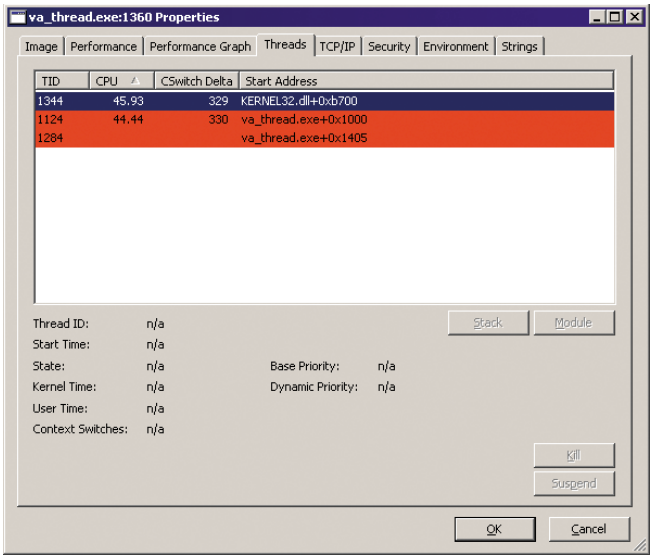

Рисунок 8. Process Explorer до сих пор неправильно определяет истинные стартовые адреса потоков

Что делает Rootkit Revealer? Он сравнивает результаты сканирования компьютера через высококровные API-функции и через низкоуровневые native-API. Rootkit, работающие «посередине», естественно, обнаруживаются за счет разницы в «показаниях», однако существует множество rootkit, которые трудно поймать даже на уровне ядра, не говоря уже о том, что львиная доля malware даже не пытается маскироваться, а потому Rootkit Revealer принципиально не в состоянии ее обнаружить. Тем не менее, учитывая бесплатность данной утилиты, высокую скорость сканирования (с поддержкой удаленной работы по сети), почему бы ее и не попробовать? А вдруг случится чудо и она поможет?!

Заключение

Список достойных утилит для поиска malware этим не ограничивается, их можно найти как на сайте Марка Руссиновича (www.sysinternals.com, автоматически переправляющего нас на сайт Microsoft), так и взять из других источников. В конце концов, всякая утилита – это всего лишь инструмент, возможности которого напрямую зависят от мастерства его обладателя. Опытный администратор обнаружит вредоносное ПО и голыми руками, начинающего не спасет и набор дорогостоящих защитных комплексов.

1. AutoRuns for Windows v9.13 – консольная и графическая версии утилиты AutoRuns (490 Кб), показывающая большинство объектов автозагрузки, а также предоставляющая дополнительный сервис по их версификации и выявлению новых объектов: http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx;
2. Process Explorer v11.11 – усовершенствованный аналог штатного «Диспетчера Задач» (1,6 Мб): http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx;
3. PsTool – набор утилит для удаленного запуска программ (1 Мб): http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx;
4. Rootkit Revealer – забавная игрушка, иногда ловит rootkit, но чаще – нет (231 Кб): http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx.