Харлэн Карви

Криминалистическое исследование Windows

Глава 7

Руткиты и обнаружение руткитов

Содержание этой главы:

- Руткиты
- Обнаружение руткитов
  - Краткое изложение
  - Быстрое повторение
  - Часто задаваемые вопросы

Введение

На конференции RSA Conference в феврале 2005 года Майк Данселио (Mike Danseglio) и Курт Диллард (Kurt Dillard), оба из корпорации Microsoft, упомянули слово *руткит* (*rootkit*), и в последующие месяцы наблюдался всплеск активности, когда «эксперты» разглагольствовали о руткитах, а компании-разработчики выпускали инструменты для их обнаружения. Несмотря на то, что о руткитах, которые появились в мире UNIX, а затем перешли в мир Windows, было известно многие годы, эту проблему в основном недооценивали, а в некоторых случаях даже старались не замечать, закрывая на факты глаза. Но вскоре после этой конференции интерес к руткитам увеличился, и появились сообщения о разработке коммерческих средств обнаружения руткитов (некоторое время были доступны несколько бесплатных инструментов и методик обнаружения). По мере того как методы обнаружения улучшались, создатели руткитов разрабатывали новые способы изменения работы операционной системы и даже ядра, чтобы руткиты нельзя было обнаружить.

Нет никаких сомнений в том, что руткиты очень опасны. Они могут скрывать присутствие таких инструментов, как клавиатурные шпионы, анализаторы сетевых пакетов и программы несанкционированного удаленного администрирования, не только от пользователей, но и от операционной системы. Коварный принцип работы руткитов может быть источником проблем, когда руткиты действительно присутствуют в системе, а также когда их нет, но специалисты по расследованию инцидентов, из-за недостатка знаний и подготовки, предполагают, что они есть. Предположение (без основательных данных, подтверждающих эту теорию), что в системе или сети установлен руткит, может привести специалиста к неправильным действиям и решениям, основанным на неверной оценке инцидента. Значительные средства могут быть потрачены на реализацию ненужных мероприятий, или системы могут быть очищены от данных и переустановлены заново, а затем снова быть заражены после ввода в эксплуатацию, если основная причина инцидента не определена.

Руткиты

Итак, что такое руткит? В подкасте Sophos (www.sophos.com/pressoffice/news/articles/2006/08/rootkit-podcast.html) от 24 августа 2006 года говорится, что согласно опросу, проведенному компанией Sophos, 37 процентов респондентов не знали, что такое руткит. Википедия определяет руткит (http://en.Wikipedia.org/wiki/Rootkit) как «набор программных средств, предназначенных для сокрытия запущенных процессов, файлов или системных данных от операционной системы». В первой из трех статей о руткитах, опубликованной на сайте SecurityFocus,

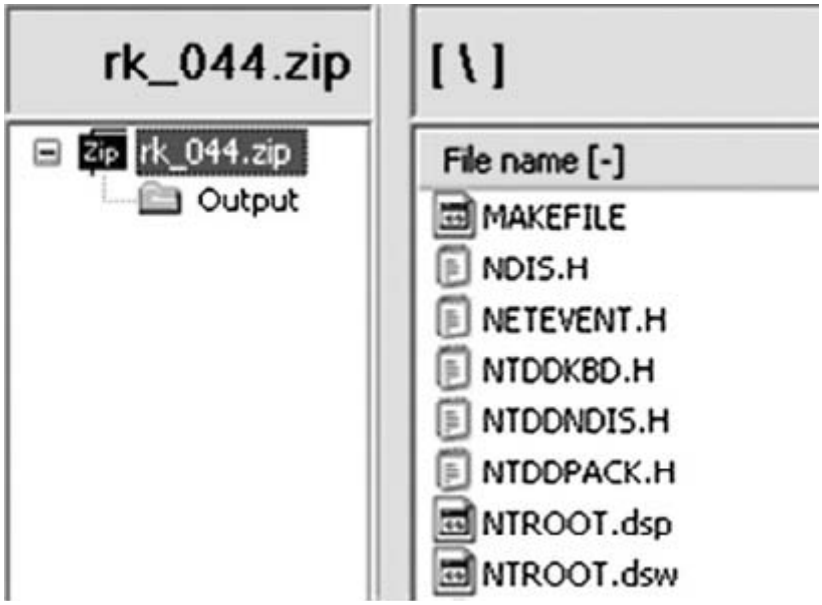
Джейми Батлер (Jamie Butler), авторитетный эксперт по технологиям руткитов, и Шерри Спаркс (Sherri Sparks) определяют руткит следующим образом (www.securityfocus.com/infocus/1850):

> Программа или ряд программ, которые использует злоумышленник, чтобы скрыть свое присутствие в компьютерной системе и предоставить доступ к этой компьютерной системе в будущем. Для того чтобы выполнить свою задачу, руткит изменяет процесс выполнения операционной системы или манипулирует набором данных, который операционная система использует для аудита и учета своих ресурсов.

Руткит можно также рассматривать как программное обеспечение, изменяющее операционную систему таким образом, чтобы скрыть себя или другие объекты от пользователей, администраторов и даже от самой операционной системы.

Руткиты используются для сокрытия процессов, сетевых соединений, разделов реестра, файлов и других объектов от операционной системы и, само собой разумеется, от администраторов. Термин *руткит* родом из мира UNIX, где такие инструменты часто использовались, чтобы получить и/или сохранить доступ к системе на уровне суперпользователя (англ. *root* – то же, что администратор в Windows). Когда похожие функциональные возможности были разработаны для вредоносных программ в Windows, то сами программы стали называть так же.

Одним из первых разработанных для Windows руткитов был NTRootkit, написанный Грегом Хоглундом (Greg Hoglund) и выпущенный в 1999 году. NTRootkit состоит из драйвера и до сих пор доступен с открытым исходным кодом, как показано на илл. 7.1.



Илл. 7.1. Архив руткита NTRootkit 0.44 с исходными файлами.

С тех пор было проведено множество исследований, касающихся разработки руткитов и руткитных технологий. Хоглунд и другие специалисты организовывают курсы по созданию руткитов на различных конференциях, например, BlackHat Security Conference, а на его веб-сайте Rootkit.com можно узнать о руткитах и их разработке, а также поделиться своей информацией с другими пользователями. Со временем появились другие руткиты, а разработка новых способов реализации руткитов продолжается без остановки. Кроме того, существует отличная книга о руткитах, способах их разработки и принципах их работы: «Руткиты: внедрение в ядро Windows» (***Rootkits: Subverting the Windows Kernel***). Эта книга написана Грегом Хоглундом и Джейми Батлером и доступна на сайте Amazon.com.

Сразу после конференции RSA Conference в феврале 2006 года возникла вспышка интереса к руткитам и обнаружению руткитов, а так как способы обнаружения становились более сложными, то же происходило и с самими руткитами. Рассматривайте эту тенденцию как постоянно обостряющуюся битву, где развитие одной области стимулирует дальнейшее развитие другой.

Существует несколько разных типов руткитов. Первые версии руткитов работали посредством замены утилит и приложений операционной системы версиями утилит и приложений, зараженными троянами, и эти зараженные версии были запрограммированы так, чтобы при запуске не показывать отдельные объекты. Например, зараженная команда *netstat* сначала удаляла сетевые соединения злоумышленника из списка, а затем показывала оставшиеся сетевые соединения как обычно.

Позднее появились руткиты, внедряющие DLL в адресное пространство процесса, или руткиты режима пользователя. Эти руткиты устанавливаются в контексте безопасности пользователя, вошедшего в данный момент в систему, и заменяют, перехватывают или исправляют различные вызовы операционной системы или DLL-функции. Например, вместо того чтобы заменять саму команду *netstat* из предыдущего примера, руткит режима пользователя перехватывает вызовы функций Windows API и обрабатывает их так, чтобы сами функции не возвращали полный список всех сетевых соединений. Затем команда *netstat* продолжает показывать информацию, полученную от функции, не зная, что ей были переданы неполные и неправильные данные. При перехвате указанных вызовов функций сетевые соединения будут также скрыты от любых других программ, использующих те же API-функции. Руткиты режима пользователя, скрывающие файлы, перехватывают вызовы функций *FindFirstFile()* и *FindNextFile()* и изменяют их так, чтобы ни одна программа, использующая вызовы этих функций, в том числе оболочка (т. е. проводник Windows), не увидела файлов, скрываемых руткитом.

К руткитам режима пользователя относятся, помимо прочих, следующие:

- AFX Rootkit 2005 – руткит с открытым исходным кодом, написанный на Delphi (пользователем Aphex) и использующий внедрение DLL и перехват API-функций, чтобы скрыть файлы, разделы реестра и т. п.
- Hacker Defender (с сайта Hxdef.org, разработанный пользователем holy_father) был, возможно, самым популярным и распространенным из существующих руткитов. Hacker Defender на сайте F-Secure описывается как наиболее широко применяемый руткит в мире. Hacker Defender также использует перенаправление портов, чтобы с помощью традиционных способов обнаружения руткитов, таких как удаленное сканирование портов, нельзя было обнаружить утилиту скрытого удаленного администрирования, реализованную руткитом. Hacker Defender использует файл конфигурации, который можно найти в содержимом физической памяти, собранном с зараженной системы. В физической памяти можно найти части файла конфигурации, нельзя восстановить файл целиком. Кроме того, при исследовании физической памяти ее содержимое отображается в обход Hacker Defender; эксперт может увидеть все процессы, скрываемые руткитом. Эксперт должен сравнить активные процессы, найденные во время анализа памяти, со списком процессов, предоставляемым операционной системой, чтобы узнать, какие из них скрываются руткитом.
- NTIllusion (www.securiteam.com/securityreviews/5FP0E0AGAC.html) был разработан так, чтобы иметь возможность выполняться с минимально доступными привилегиями, внедряясь в процессы, запущенные от имени текущего пользователя.
- Vanquish – румынский руткит, внедряющий DLL и умеющий скрывать файлы, процессы, разделы реестра и другие объекты. Vanquish состоит из автозагрузчика (exe-файл) и DLL-файла, который в свою очередь состоит из шести подмодулей. Vanquish требует прав администратора для правильной установки и, согласно

файлу сведений, который идет в комплекте с дистрибутивом, не работает, если в системе присутствуют другие руткиты.

- Gromozon (www.Antirootkit.com/articles/gromozo/The-strange-case-of-DrRootkit-and-Mr-Adware.htm) – руткит режима пользователя, который заражает систему через объект модуля поддержки браузера (BHO) и использует различные приемы для поддержания сохраняемости в зараженной системе (скрывает код в EFS-файлах и альтернативных потоках данных NTFS, создает службу, создает ссылку в разделе реестра AppInit_DLLs и т. д.). Кроме того, руткит удаляет привилегию отладки из учетных записей пользователей, чтобы препятствовать нормальной работе средств обнаружения руткитов. В отчете на сайте Symantec (https://forums.symantec.com/syment/blog/article?message.uid=305212) этот руткит сравнивается со спагетти из-за различных способов сохраняемости, встроенных разработчиком в его код.

Совет
Многие руткиты можно загрузить из Интернета, в частности с сайта Rootkit.com.

Руткиты режима ядра обнаружить еще труднее, так как они изменяют работу самого ядра операционной системы. Они не только перехватывают вызов низкоуровневых API-функций, но и манипулируют структурами данных ядра. Пример руткита режима ядра – FU (разработанный Джейми Батлером), использующий прием, который называется *непосредственное манипулирование объектами ядра* (Direct Kernel Object Manipulation, DKOM), чтобы скрыто работать в системе. DKOM – это процесс манипулирования структурами данных уровня ядра, не используя функции Windows API. Например, ядро Windows содержит двусвязный циклический список всех выполняющихся процессов, а FU удаляет необходимые процессы из этого списка. Процессы по-прежнему находятся там, но ядро их не «видит». Квант времени в системе выделяется для потока, а не процесса, поэтому поток FU продолжает выполняться, в то время как процесс невидим для системы. FU использует драйвер, который по умолчанию называется «msdirectx.sys», чтобы получить доступ к системе и контроль над ней. Программа FU, «fu.exe», завершает свою работу после того, как загрузит драйвер в память.

Руткиты режима ядра могут также изменять другие структуры ядра. Руткит FUTo (www.uninformed.org/?v=3&a=7), разработанный как преемник FU, подробно рассматривается в третьем томе журнала *Uniformed Journal* (www.uninformed.org), выпущенном в январе 2006 года. FUTo расширяет возможности DKOM руткита FU, используя код на языке ассемблера (а не вызовы функций API), чтобы манипулировать переменной *PspCidTable*, которая является указателем на таблицу дескрипторов для клиентских идентификаторов процессов и потоков. Эта таблица дескрипторов используется для отслеживания всех идентификаторов процессов.

Shadow Walker – экспериментальный руткит режима ядра, обсуждавшийся на конференции BlackHat 2005. Shadow Walker основан на рутките FU и содержит дополнительный драйвер, манипулирующий диспетчером памяти, чтобы скрыть существование файлов руткита. Чтобы достичь этого, Shadow Walker проверяет, что все скрытые страницы находятся в невыгружаемой памяти, и перехватывает все обращения к этим страницам. Когда операционная страница выполняет запрос на чтение этих страниц, руткит возвращает страницы, заполненные нулями. Когда операционная система выполняет запрос на выполнение этих страниц, руткит возвращает вредоносный код. Помните эпизод из фильма «Звездные войны», когда Оби-Ван Кеноби говорит командиру штурмовиков: «Это не те дроиды, которых вы ищете»? Здесь происходит примерно то же самое.

Следует отметить, что руткиты режима ядра могут быть причиной критической системной ошибки, если они написаны неправильно. Часто сотрудники службы

поддержки Microsoft помогали пользователям решить проблему с повторяющимися ошибками BSoD (т. н. синий экран смерти – ***Blue Screen of Death***) и выясняли, что причиной является руткит режима ядра. Как упоминалось в главе 3, при сбое в системе или при возникновении ошибки BSoD создается аварийный дамп памяти на НЖМД, и сотрудники службы поддержки могут использовать этот файл, чтобы установить причину ошибки. Часто таким способом можно обнаружить известную или даже новую версию руткита в системе.

Иногда термин *руткит* употребляется в несколько другом смысле. Например, в сентябре 2006 года в веб-блоге Security Response компании Symantec была опубликована статья «The Poor Man's Rootkit». В этой статье автор описывает вредоносную программу Trojan.Zonebac, использующую способ маскировки, чтобы «скрыть» свое присутствие в системе. Вкратце, во время установки эта троянская программа сканирует содержимое раздела реестра Run и выбирает часто использующееся приложение. Она создает резервную копию исполняемого файла, указанного в параметре реестра, и записывает себя в файловую систему, используя имя исходного файла. При загрузке системы троянская программа запускается автоматически, а затем также выполняет резервную копию файла, поэтому кажется, что все в порядке. Более того, время ***LastWrite*** раздела Run не обновляется, так как в этот раздел не вносится фактических изменений.

Несмотря на то, что эта программа использует действительно новый и даже оригинальный способ сокрытия в системе, она не является руткитом. На самом деле, сокрытие вредоносной программы в обычном месте и присваивание ее исполняемому образу какого-нибудь безобидного имени является распространенным и эффективным способом. Его можно рассматривать скорее как способ сбить администратора или эксперта с толку, но не как способ взлома сервера.

Предупреждение

Не стоит полагаться только на имя файла при диагностировании проблемы, так это может ввести эксперта в заблуждение и помешать ему выявить истинную причину инцидента. Нередки случаи, когда администратор находит подозрительный файл и ищет в Google сведения о нем, используя имя файла. Затем он обнаруживает, что есть надежный файл Microsoft с таким именем и решает завершить расследование инцидента. Это касается не только администраторов; мне встречались случаи, когда то же самое делали специалисты по анализу вредоносных программ. Однако я также сталкивался с ситуациями, когда вредоносная программа устанавливалась в системе, используя имена надежных файлов Microsoft, например, «alg.exe» или «svchost.exe». В большинстве таких случаев администраторы выясняли, что эти файлы являются «надежными» и не проводили дальнейшего исследования. Например, никто не обращал внимания, что эти исполняемые файлы не были расположены в каталоге «system32». Дело в том, что нельзя полагаться только на имя файла в качестве средства для определения типа файла и воздействия, которое он может оказывать на систему или инфраструктуру.

Руткиты также используются в коммерческих целях. Помимо того, что некоторые разработчики создают руткиты на заказ для тех, кто желает за это заплатить, известны случаи, когда корпорации использовали руткиты, чтобы скрыть функциональные возможности своих продуктов. Тридцать первого октября 2005 года Марк Руссинович (известный по сайту SysInternals, а теперь работающий в Microsoft) сообщил в своем блоге о том, что обнаружил, что корпорация Sony использует руткит, чтобы воздействовать на средства управления цифровыми правами и защитить свою собственность (http://blogs.Technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx). В частности Марк указал не только то, что пользователь, купивший музыкальный компакт-диск и установивший программное обеспечение на свой компьютер, совершенно не знал об использовании руткита (пользователь не был в прямой

форме предупрежден об использовании руткита, и это не указывалось в лицензионном соглашении), но и то, что злоумышленник, обнаруживший это установленное программное обеспечение, мог использовать его в своих интересах и установить свои собственные инструменты, которые бы скрывались за ширмой Sony. После обнаружения этой проблемы и последующего фурора Марк получил должность в корпорации Microsoft. Архив статьи из блога Марка находится на сайте Virus Bulletin.

Записки из подполья…

Обмен информацией

В своей статье (которую можно найти на сайте Virus Bulletin) о проблеме с руткитом Sony Марк делает следующее заявление:

Несколько лет тому назад мы сделали исходный код программы Regmon общедоступным, что привело к использованию наших функций перехвата и процедур поддержки в экземпляре руткита NTRootkit, опубликованном на сайте www.rootkit.com. *Структура кода в Aries свидетельствует о том, что он, вероятно, был составлен на основе кода NTRootkit.*

Интересно наблюдать, как различные источники используются для дальнейшего развития приложений, в том числе вредоносных программ. В данном случае функции перехвата стали использоваться совершенно в других целях.

Марк Руссинович и другие специалисты провели исследование касательно того, как корпорации используют руткиты в своих программных продуктах, и 10 января 2006 года Symantec (www.symantec.com/avcenter/security/Content/2006.01.10.html) опубликовала информацию о том, что функция «Защищенная корзина Norton» (“Norton Protected Recycle Bin”) использует возможности руткита.

Обнаружение руткитов

Теперь, когда мы поняли, что такое руткиты и что они могут делать, нам нужно узнать, как обнаружить присутствие руткита в системе. Чтобы ответить на этот вопрос, давайте рассмотрим два способа обнаружения: на работающем компьютере и в образе данных. В первом случае у нас есть работающая система, и мы попытаемся определить, есть ли в ней руткит. Во втором случае мы работаем с образом данных, полученном из системы. Одно из преимуществ использования обоих способов обнаружения состоит в том, что для эффективного обнаружения руткитов требуется применение различных приемов, рассмотренных в других главах этой книги, таких как анализ памяти, исследование реестра и файловой системы, сканирование портов и анализ перехваченного сетевого трафика. Совместное использование всех этих приемов позволит получить более полное представление об инциденте, что поможет вам обнаружить руткиты.

Обнаружение руткитов на работающем компьютере

Обнаружение руткитов на работающем компьютере может быть довольно сложным делом, особенно если эксперт не разбирается в артефактах руткитов и не знает, какие данные в системе могут быть заражены руткитом. Часто это приводит к неверной оценке инцидента и неправильному дальнейшему расследованию.

Предупреждение

Не забывайте, что любой инструмент, предназначенный для обнаружения вредоносных программ, не должен автоматически удалять файлы или другие артефакты; вам нужно только, чтобы этот инструмент обнаружил присутствие вредоносной программы и предупредил вас. Удаление артефактов лишает анализ смысла.

Осенью 2006 года Джесси Корнблюм (Jesse Kornblum) опубликовал очень интересную статью «Exploiting the Rootkit Paradox with Windows Memory Analysis» в журнале *International Journal of Digital Evidence* (www.utica.edu/academic/institutes/ecii/publications/articles/EFE2FC4D-0B11-BC08AD2958256F5E68F1.pdf). В этой статье Джесси определил два принципа, которым пытаются следовать все руткиты: они хотят оставаться невидимыми, и они должны выполняться. Фактически, для того чтобы оставаться невидимым в системе, руткит должен свести к минимуму количество своих следов, взаимодействуя при этом с системой некоторым образом. Сама система, точнее операционная система, должна иметь возможность выполнять руткит, который пытается оставаться невидимым и сохранить свои функции после перезагрузки системы. Следовательно, Джесси предполагает, что если операционная система может найти руткит, то это же может и эксперт. Я бы добавил к этому «хорошо осведомленный эксперт», но уверен, что именно это Джесси и имел в виду.

Основной прием для обнаружения руткитов на работающем компьютере иногда называют *поведенческим* или *дифференциальным* анализом. Основная идея в том, что, выполняя два различных вида запросов к одной и той же информации и стараясь найти различия в откликах, можно обнаружить присутствие руткита или какого-нибудь объекта, скрываемого руткитом. Например, одним из первых инструментов для обнаружения руткитов был скрипт «rkdetect.vbs», написанный на Visual Basic и все еще доступный по адресу www.security.nnov.ru/files/rkdetect.zip; он мог обнаруживать популярный руткит Hacker Defender, выполняя удаленный запрос на перечисление служб с помощью «sc.exe», за которым следовал локальный запрос (с помощью «psexec.exe» или «sc.exe»), а затем выполняя поиск аномалий или различий между двумя результатами. В своей первой книге, *Windows Forensics and Incident Recovery*, я рассматривал Perl-скрипт «rkd.pl», который проводил дифференциальный анализ процессов, служб и некоторых разделов реестра. Скрипт обращал внимание на различия в результатах между удаленным и «локальным» запросами (инструменты запускались локально на удаленной системе с помощью «psexec.exe»), а также выполнял проверку некоторых сигнатур, то есть проверку на наличие отдельных руткитов. В книге я демонстрировал применение таких инструментов для анализа руткита AFX Rootkit 2003.

Примечание

Ленни Зельцер (Lenny Zeltser), специалист по расследованию инцидентов из центра SANS Internet Storm Center (ISC), 16 июля 2006 года опубликовал статью (http://isc.sans.org/diary.html?storyid=1487), которая называлась «Behavior Analysis of Rootkit Malware». В данной статье Ленни предоставляет снимки экрана и описания нескольких инструментов для обнаружения руткитов (а также ссылки на другие инструменты), которые тестировались на некоторых руткитах, упомянутых ранее в этой главе.

Со временем руткиты развивались, используя более сложные способы сокрытия и обеспечения невидимости объектов, а способы обнаружения руткитов должны были не отставать от этого развития. Дифференциальный анализ все еще является наилучшим подходом к обнаружению руткитов, но запросы к элементам данных становятся все более детализированными. Например, некоторые инструменты сканируют файловую систему, используя такие команды, как *dir /s* и *dir /s /ah*, а затем сравнивают результаты с содержимым главной файловой таблицы (MFT). Идея состоит в том, чтобы выполнить высокоуровневый запрос, а затем запрос (максимально) низкого уровня и найти различия в выходных данных двух запросов.

Существует несколько бесплатных и коммерческих инструментов обнаружения руткитов, но ни один из них не предоставляет подробностей о своем *способе* работы. Это

делается для того, чтобы создатели руткитов не имели легкой возможности определить, как работают инструменты обнаружения, и не могли затем добавить контрприемы в свои руткиты, чтобы те не были обнаружены этими инструментами. Однако это не мешает создателям руткитов загрузить эти инструменты и определить способ их работы самостоятельно.

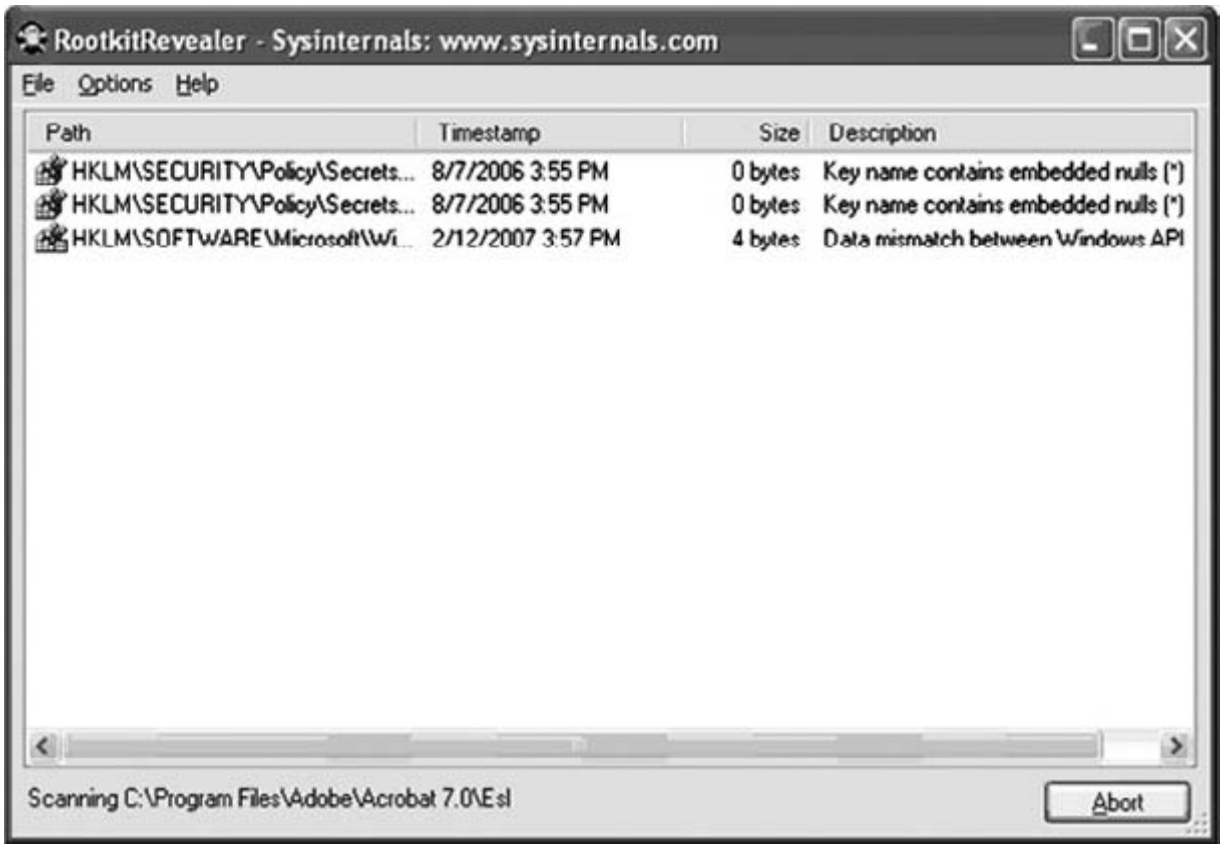
RootkitRevealer

RootkitRevealer (http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, см. илл. 7.2) – это средство обнаружения руткитов, которое появилось весной 2005 года. (Сведения о RootkitRevealer были опубликованы на веб-сайте Slashdot.org (http://it.slashdot.org/it/05/02/23/1353258.shtml?tid=172&tid=218) 23 февраля 2005 года.) С момента своего первого выпуска средство претерпело ряд изменений, чтобы не отставать от изменений в области создания руткитов. Как только разрабатываются руткиты, содержащие способы, препятствующие их обнаружению, в состав таких инструментов, как RootkitRevealer, включаются приемы противодействия этим способам.

В описании RootkitRevealer автор специально указывает, что, хотя утилита предназначена для обнаружения руткитов, скрывающих файлы и разделы реестра, и умеет это делать, она не находит руткиты (такие как FU), изменяющие структуры ядра.

Предупреждение

При запуске любого инструмента нужно знать, как он работает и что он делает; это также относится к средствам обнаружения руткитов. Однажды я столкнулся со случаем, когда действия по расследованию инцидента, предпринятые клиентом, были плохо организованы и несогласованны. В то время как одним администраторам были даны указания выполнять специальные задачи, другие администраторы решили самостоятельно провести разрушающие проверки систем на наличие вирусов, а также запустить RootkitRevealer. Для выполнения своих проверок средство RootkitRevealer устанавливается как служба, а исполняемому файлу присваивается случайное имя, хотя сам исполняемый файл имеет случайное заполнение (чтобы хэш-значение файла никогда не совпадало). Это один из способов, не позволяющий руткитам обнаружить это средство. На определенном этапе расследования администратор сообщил мне, что обнаружил «сильно зараженную» систему, в которой выполнялось восемь странных служб, а средство RootkitRevealer не определяло их как руткиты. Во-первых, если администратор мог «видеть» эти службы в списке, то, вероятно, они не были скрыты руткитом. Во-вторых, все исполняемые файлы имели одинаковый значок. В-третьих, все исполняемые файлы были средством RootkitRevealer. Из-за отсутствия согласованности в действиях и недостатка знаний используемых инструментов, расследование инцидента привело к обнаружению якобы зараженной системы.



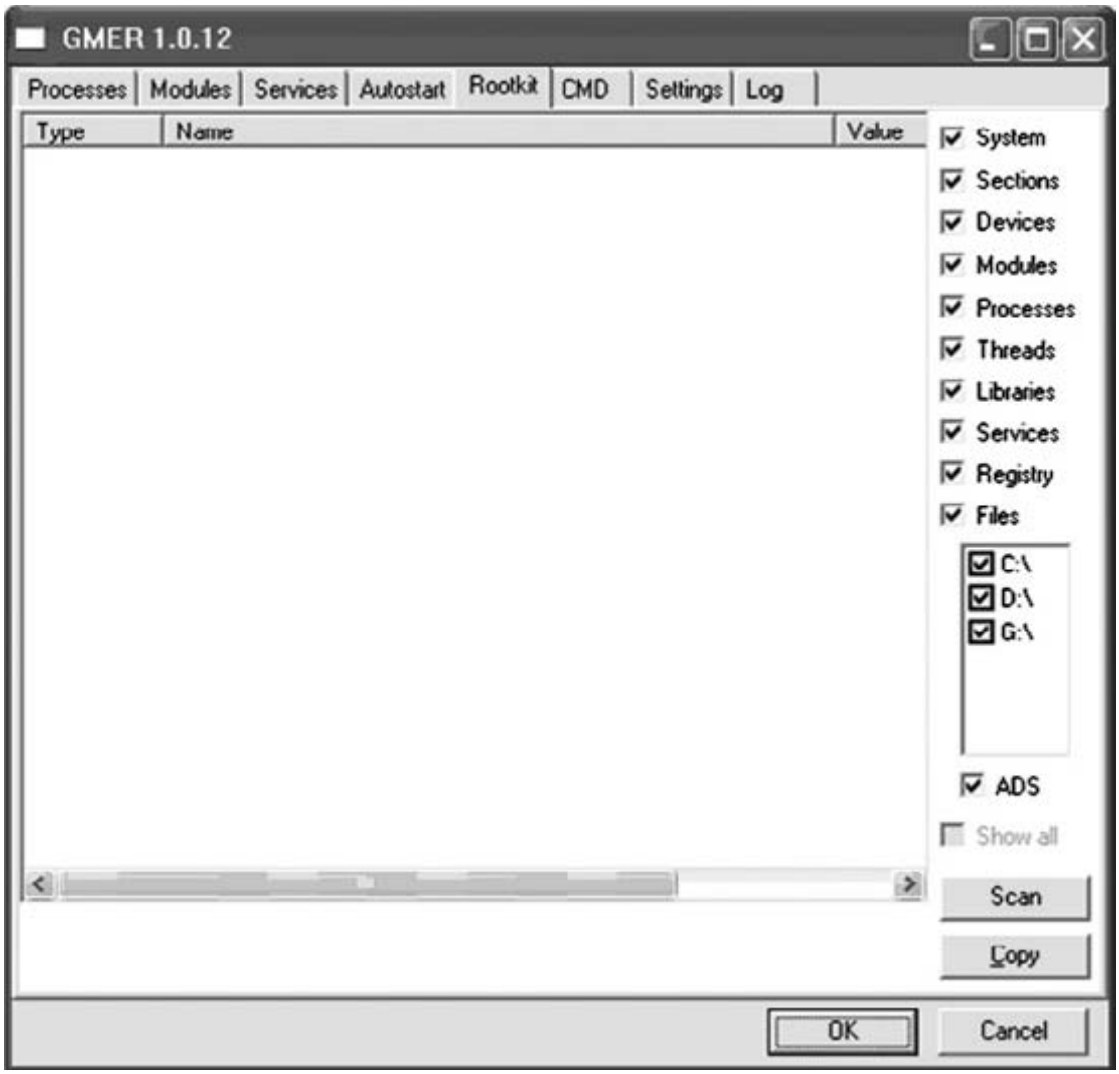
Илл. 7.2. Графический интерфейс программы RootkitRevealer.

GMER

GMER (www2.gmer.net/) – это бесплатное приложение (на основе графического интерфейса) для обнаружения руткитов, которое пытается найти:

- скрытые процессы, файлы, службы, разделы реестра и драйверы;
- драйверы, перехватывающие таблицу дескрипторов системных служб (System Service Descriptor Table, SSDT), таблицу дескрипторов прерываний (Interrupt Descriptor Table, IDT) или вызовы пакетов запроса ввода/вывода (IO Request Packet, IRP).

GMER также может отображать альтернативные потоки данных NTFS, как показано на илл. 7.3.



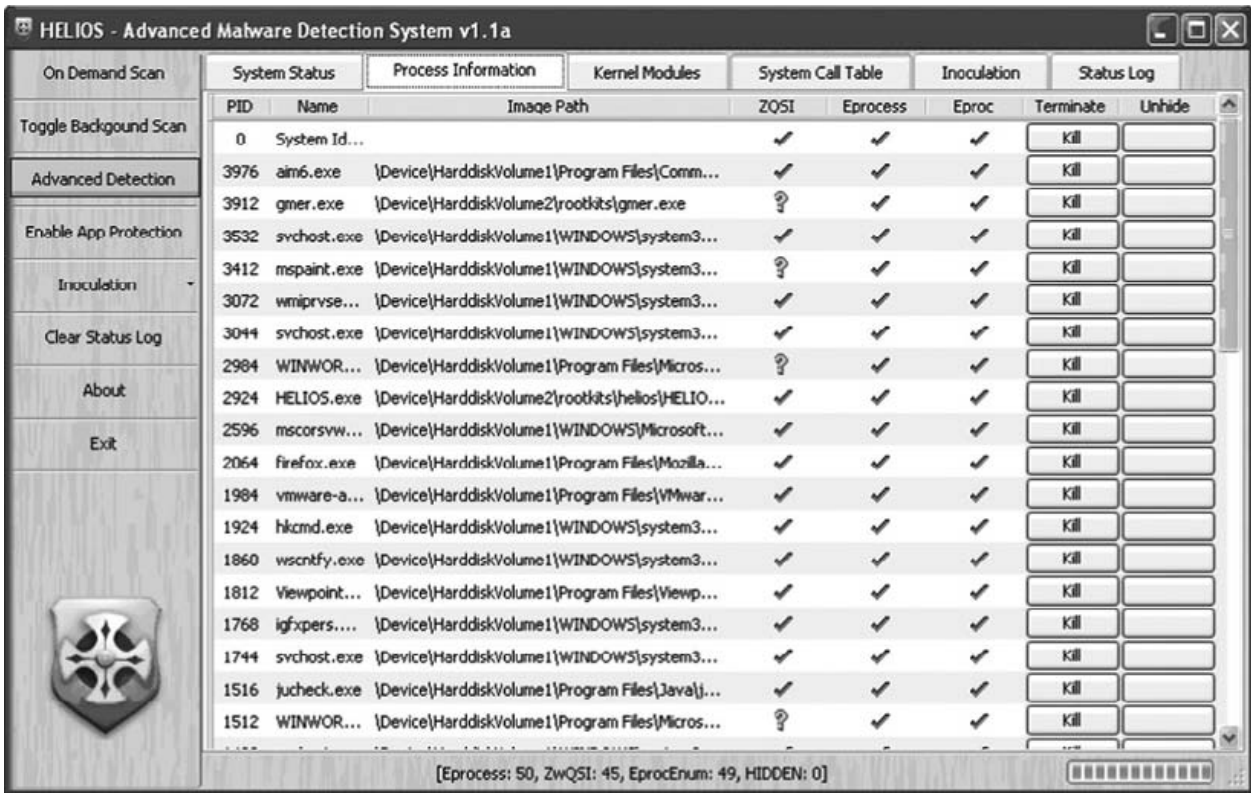
Илл. 7.3. Графический интерфейс программы GMER.

На веб-сайте GMER также доступно небольшое приложение ***catchme*** на основе командной строки, которое может обнаруживать руткиты режима пользователя, такие как Gromozon, Hacker Defender, aFX и Vanquish. С веб-сайта GMER можно загрузить не только приложение для поиска руткитов, но и несколько видеороликов об обнаружении руткитов и несколько файлов журналов проверок, во время которых были найдены руткиты. GMER также находит руткиты, изменяющие главную загрузочную запись (MBR), и позволяет добавить в свой интерфейс ваше любимое антивирусное приложение.

Helios

Helios (www.mielesecurity.com/) описывается как «усовершенствованная система обнаружения вредоносных программ», применяющая поведенческий анализ и не использующая сигнатуры в качестве механизма обнаружения. Хотя программа Helios позиционируется как система обнаружения вредоносных программ, она также может находить руткиты. Helios не является программой с открытым исходным кодом, но она бесплатна и (согласно веб-сайту www.Antirootkit.com/software/Helios.htm) имеет интерфейс API, предоставляющий доступ к ее основным функциональным возможностям. Helios не только обнаруживает руткиты, но и предохраняет систему от установки руткитов. Графический интерфейс программы Helios показан на илл. 7.4.

Совет
Если вы собираетесь загрузить и установить Helios, не забудьте установить платформу .NET Framework 2.0. Ссылка на необходимые файлы доступна на странице загрузки программы Helios.



Илл. 7.4. Графический интерфейс программы Helios.

На веб-сайте Helios также содержится несколько видеороликов (которые можно загрузить или посмотреть онлайн), демонстрирующих применение и возможности программы.

Совет
Многие бесплатные программы обнаружения руткитов, представленные в этой главе, можно легко загрузить и запустить из отдельного каталога. Для того чтобы развернуть эти инструменты во время расследования инцидента, можно просто копировать их на USB флеш-накопитель, а затем активировать переключатель защиты от записи (если таковой имеется) и вставить флеш-накопитель в компьютер, который вы хотите проверить. Однако не забывайте о зависимостях и требованиях, как например в программе Helios, которая требует установки Microsoft .NET Framework 2.0.

MS Strider GhostBuster

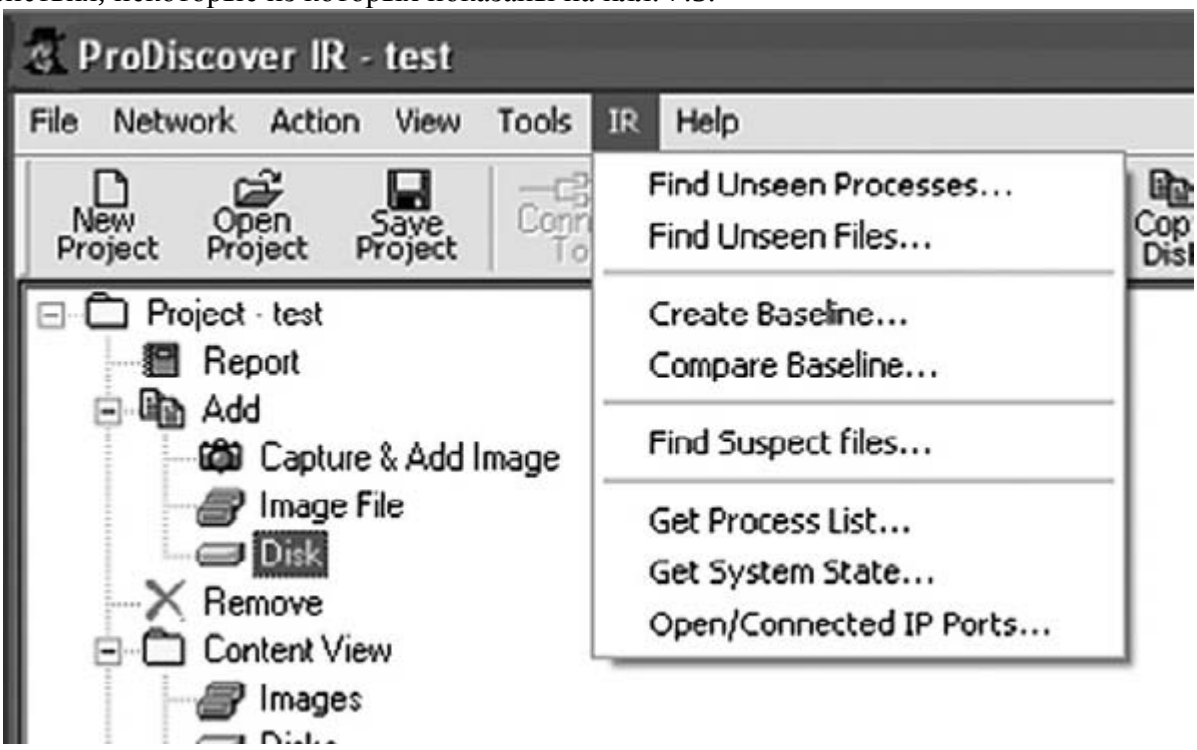
Научно-исследовательский центр Microsoft Research Center потратил значительные средства на изучение вопросов обнаружения руткитов в ОС Windows, результатом чего стал инструмент Strider GhostBuster (http://research.microsoft.com/rootkit/), предназначенный для поиска руткитов, перехватывающих и изменяющих функции Windows API. GhostBuster использует метод обнаружения различий при сравнении (“cross-view diff”), который похож на поведенческий или дифференциальный анализ. Выполнив запрос в «зараженной» системе, а затем загрузившись с «чистого» носителя (незараженного загрузочного компакт-диска Windows) и выполнив тот же запрос, вы можете провести сравнение двух результатов и определить скрытые объекты. Этот способ

особенно полезен в отношении файлов, но, так как вся система (включая приложения и исправления) должна храниться на загрузочном CD/DVD-диске, он не очень эффективен в отношении процессов. Для того чтобы найти скрытые процессы, используя этот способ (загружая систему с отдельного, незараженного носителя), администратору потребовалось бы сохранить весь набор приложений, а также исправления и параметры конфигурации операционной системы и приложений на чистом носителе. Любое, даже минимальное, изменение нужно было бы повторить на отдельном носителе. Этот способ является, возможно, слишком трудоемким для большинства инфраструктур и расследований.

Несмотря на то, что сайт GhostBuster действительно содержит ссылки на информацию и статьи о различных аспектах руткитных технологий, на момент написания этой книги сам инструмент GhostBuster не был доступен для загрузки и использования. Тем не менее, некоторые статьи на сайте чрезвычайно полезны, и специалистам будет интересно их прочитать. Например, статья «Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management», представленная на конференции Usenix LISA в 2004 году, дает отличное представление о местах автозапуска в реестре.

ProDiscover

Версия Incident Response (IR) программы ProDiscover, от компании Technology Pathways (www.Techpathways.com), содержит функциональные возможности, которые должны помочь эксперту проверить системы на предмет наличия руткитов во время расследования инцидентов. Установив серверное приложение ProDiscover (PDServer.exe) в системе (либо запустив его с компакт-диска или флеш-накопителя, либо установив его удаленно по сети), эксперт затем может подключиться к серверу и выполнить различные действия, некоторые из которых показаны на илл. 7.5.



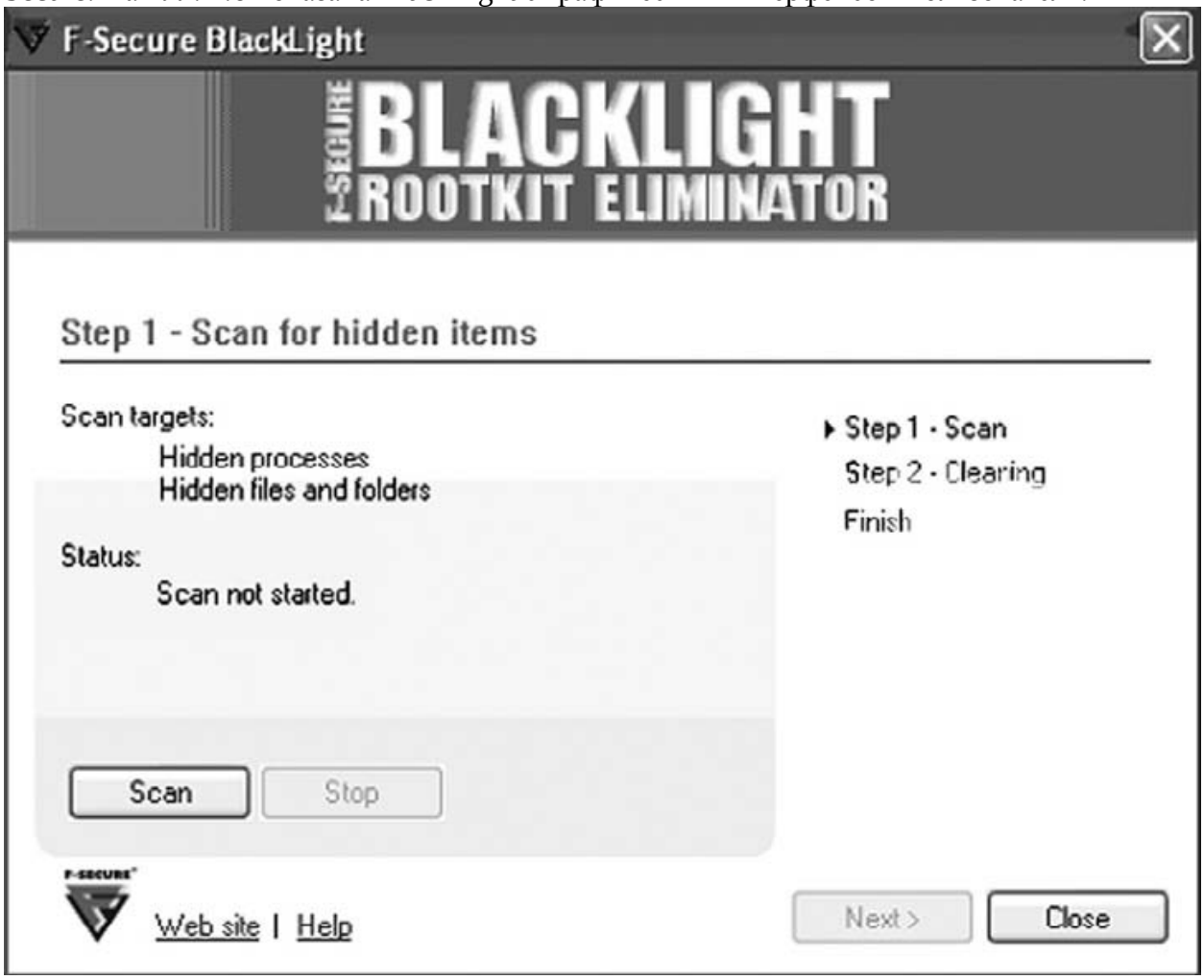
Илл. 7.5. Функции программы ProDiscover для обнаружения руткитов.

Как показано на илл. 7.5, эксперт может попытаться найти невидимые процессы и файлы, а также собрать информацию о списке активных процессов и состоянии системы через меню программы ProDiscover IR. Интерфейс ProScript API предоставляет больший уровень детализации и выбора относительно информации, которую можно собрать, а также относительно способа управления этой информацией. Поиск невидимых процессов и файлов может помочь эксперту обнаружить руткиты в системе.

F-Secure BlackLight

F-Secure – финская компания, выпускающая антивирусное программное обеспечение (согласно блогу компании, ее антивирусная программа была недавно включена в состав веб-сервиса VirusTotal.com, проверяющего подозрительные файлы), а также программу удаления руткитов, которая называется BlackLight (www.f-secure.com/blacklight). BlackLight обнаруживает объекты, скрываемые руткитами, и предоставляет пользователю возможность удалить проблемную программу.

Пробную версию программы BlackLight, которая выпускается как с графическим интерфейсом, так и с интерфейсом командной строки, можно загрузить с веб-сайта F-Secure. На илл. 7.6 показана BlackLight с графическим интерфейсом пользователя.



Илл. 7.6. Графический интерфейс программы BlackLight.

Как и многие другие приложения для обнаружения руткитов, BlackLight предоставляется в виде исполняемого файла и не содержит программу установки (т. е. msi-файла); приложение можно запускать сразу после загрузки исполняемого файла любой из выбранной вами версии.

Предупреждение

При работе с инструментами для поиска руткитов или других вредоносных программ, следует отказаться от использования средств, которые автоматически выполняют действия за вас, например, удаляют файлы или прочие артефакты. Основная цель проведения этого вида исследования состоит в обнаружении таких артефактов, чтобы вы могли составить профиль действий и характеристик руткита и по возможности найти этот руткит в других системах. Автоматическое удаление файлов сразу после их обнаружения значительно усложнит вашу задачу, так как в таком случае вам нужно

определить, какие другие действия были выполнены автоматически, и какие другие артефакты, возможно, были удалены.

Sophos Anti-Rootkit

Sophos – еще один производитель антивирусных программ, который также предоставляет антируткитное программное обеспечение. Программу Sophos Anti-Rootkit (www.sophos.com/support/knowledgebase/article/17004.html) можно бесплатно загрузить и использовать, и, как F-Secure BlackLight, она выпускается в виде версий с графическим интерфейсом (см. илл. 7.7) и интерфейсом командной строки. Sophos Anti-Rootkit можно использовать для проверки отдельных компьютеров и сетевой инфраструктуры на предмет наличия руткитов, а также для удаления руткитов. Программа выполняет поиск скрытых процессов, разделов реестра и файлов на локальных НЖМД.

Илл. 7.7. Графический интерфейс программы Sophos Anti-Rootkit.

Совет

Последняя из трех статей Джейми Батлера (Jamie Butler) и Шерри Спаркса (Sherri Sparks), «Windows Rootkits of 2005», была опубликована на сайте SecurityFocus.com 5 марта 2006 года. Рекомендуется прочитать эту статью (www.securityfocus.com/infocus/1854), в которой рассматриваются пять способов обнаружения руткитов и описываются особенности девяти руткитов.

AntiRootkit.com

F-Secure и Sophos, компании-производители антивирусных приложений, – не единственные, кто предоставляет программы обнаружения и/или удаления руткитов. Другие производители выпускают средства обнаружения руткитов либо в виде отдельных продуктов, либо в виде компонентов, включенных в состав антивирусных приложений. Программа McAfee Rootkit Detective, как и RootkitBuster от компании Trend Micro, выполняет поиск скрытых файлов, процессов, разделов и параметров реестра в потенциально зараженных системах.

Возможно, самый лучший сайт с информацией о способах и программах обнаружения руткитов – это AntiRootkit.com. На сайте есть блог, список бесплатных и коммерческих программ обнаружения/удаления руткитов (перечисленные программы предназначены главным образом для Windows, но кроме того указаны продукты для Linux, BSD и даже Mac OS X), а также список антируткитных приложений, которые можно использовать в первую очередь для того, чтобы предотвратить или блокировать установку руткитов. Новости и статьи, публикуемые на сайте, предоставляют доступ к еще большему количеству информации.

На других веб-сайтах и в блогах можно найти дополнительные сведения об инструментах, например:

- статья об антируткитных инструментах для Windows в блоге RaDaJo (http://radajo.blogspot.com/2007/11/anti-rootkit-windows-tools-searching.html);
- обзор антируткитных инструментов в блоге GrandStreamDreams (http://grandstreamdreams.blogspot.com/2008/01/anti-rootkit-tools-roundup-revisited.html).

Обнаружение руткитов в образе данных

Способы обнаружения руткитов в образе данных имеют собственный набор проблем. Вероятно, вы думаете: «Насколько сложно это реализовать?». Ведь вы имеете дело с образом данных, а не с работающей системой … что же можно там найти? Учитывая различные способы, доступные создателям вредоносных программ, в том числе антикриминалистические инструменты, имеющиеся в открытом доступе (на веб-сайте MetaSploit Project есть целый раздел, посвященный антикриминалистическим приемам), поиск вредоносных программ, даже в образе, может быть сложной задачей. Однако если вы знаете, что и где искать, вы, вероятнее всего, добьетесь успеха в своем исследовании.

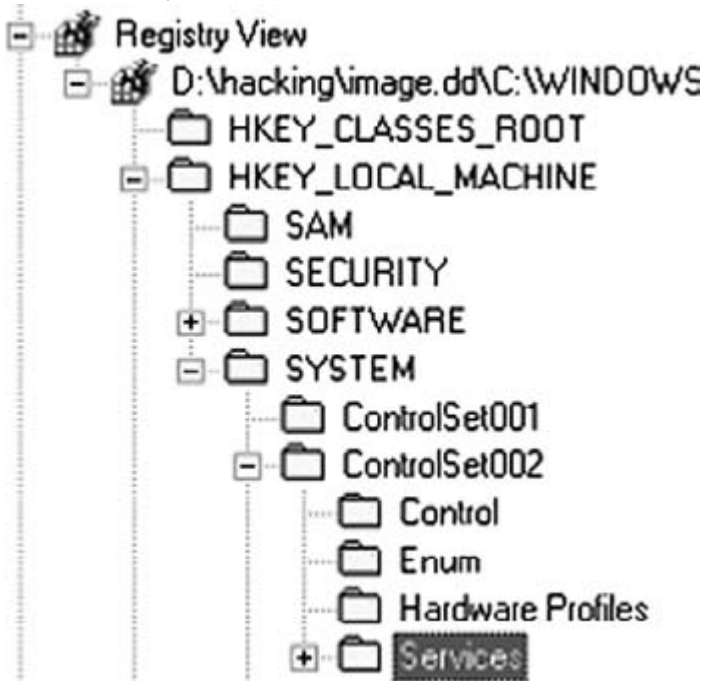
Один из способов обнаружить руткиты в образе данных – монтировать образ как виртуальную файловую систему на компьютере для анализа данных с помощью таких инструментов, как SmartMount (www.Asrdata.com/SmartMount/) или Mount Image Pro (www.mountimage.com), разрешив чтение файлов, не активируя для этого операционную систему из образа. Оба инструмента могут монтировать образ в режиме только для чтения, чтобы в файлы нельзя было внести изменения. После этого можно запускать любое количество антивирусных инструментов для проверки файлов в образе. Файлы в образе отображаются как обычные файлы. Ни процессы, ни службы в образе не выполняются, поэтому руткит не будет функционировать, а ядро системы для анализа данных не будет изменено.

Предупреждение
Использование SmartMount, чтобы получить доступ к образу данных как к структуре каталогов, поможет вам, если вы хотите проверить образ с помощью антивирусных и антишпионских приложений, но средства обнаружения руткитов будут вам не очень полезны. Причина состоит в том, что эти средства выполняют поиск скрытых объектов (файлов, разделов реестра, процессов и т. д.), а когда образ клонированных данных монтируется как накопитель, ни один из этих элементов

информации не скрыт.

Вы также можете загрузить образ в программе VMware с помощью LiveView (http://liveview.sourceforge.net) и проверить работающую систему на наличие руткитов, используя любой из инструментов, предназначенных для работающих систем. Это предполагает, конечно, что у вас есть имя пользователя и пароль, чтобы войти в систему после того, как будет загружен образ. В главе 6 я говорил, что некоторые вредоносные программы используют программные средства, чтобы выявить наличие виртуальной среды, и если вредоносная программа определяет, что она выполняется в такой среде, например, в VMware, она может изменить свое поведения, чтобы избежать обнаружения. Конечно, некоторые руткиты тоже могут это делать, а это вторичное поведение может быть причиной проблем в системе (например, не давать компонентам операционной системы работать правильно или просто вызывать ошибку BSoD). Можно также проверить виртуальную систему с помощью сканера портов (например, Nmap), а затем сравнить результаты проверки с выходными данными утилиты «netstat.exe» или «openports.exe». Если, используя Nmap, вы найдете открытые порты, но не увидите этих портов в выходных данных утилиты «netstat.exe», то, возможно, в системе работает руткит.

Для того чтобы быстро проверить образ данных на наличие руткитов, я открываю Registry Viewer в программе ProDiscover и перехожу в раздел Services в каждом из имеющихся разделов ControlSet, как показано на илл. 7.8.



Илл. 7.8. Фрагмент данных реестра из программы ProDiscover.

Совет

Чтобы определить раздел *ControlSet*, который отмечен как «текущий» (“current”) или загружается как *CurrentControlSet* при начальной загрузке системы, найдите параметр *Current* в разделе System\Select. Данные представляют собой параметр *DWORD* и указывают, какой из имеющихся разделов *ControlSet* отмечен как «текущий».

Найдя этот раздел, я сортирую записи в правой панели по времени *LastWrite* каждого раздела. Большинство записей в этом списке соответствуют времени первоначальной установки системы. Иногда несколько разделов могут иметь одинаковое время *LastWrite* в результате обновления программы, которое затронуло все записи, часто

в один и тот же день. Однако когда установлен драйвер руткита режима ядра, этот раздел будет отличаться от остальных одной или двумя записями, сделанными в один день. Отметки времени *LastWrite* не всегда соответствуют датам, указанным в отчете об инциденте, но в большинстве случаев эти записи будут видны невооруженным глазом. Кроме того, они предоставят вам дату, на которую следуют ориентироваться при составлении временной шкалы действий в системе. Так как, похоже, что не существует общедоступного интерфейса Windows API для изменения отметок времени *LastWrite* в разделах реестра из приложений режима пользователя, можно быть уверенным, что время *LastWrite* раздела соответствует времени установки руткита и его драйвера.

Инструменты и ловушки…

Применение RegRipper для поиска руткитов

Еще один способ выполнить такой же анализ без загрузки файла-образа в файл дела в любимом приложении для судебного анализа данных – использовать программу RegRipper (рассмотренную в главе 4) или связанный с ней инструмент «rip.exe» на основе командной строки (вместе с соответствующими подключаемыми модулями), чтобы проанализировать раздел Services в файле куста «System» и сортировать его подразделы по времени *LastWrite*. Это довольно легко сделать посредством монтирования образа с помощью SmartMount и использования пакетного файла для запуска соответствующих команд. Но если у вас нет образа данных и вы вынуждены иметь дело с работающей системой, вам доступен еще один вариант – запустить RegRipper посредством F-Response (www.f-response.com) Блогер под псевдонимом «Hogfly» разместил на сайте YouTube видеоролик, в котором демонстрируется, как он использовал F-Response и RegRipper (http://forensicir.blogspot.com/2008/04/ripping-registry-live.html), чтобы извлечь данные из реестра работающей системы.

Еще один способ поиска руткитов, который представляет собой что-то среднее между обнаружением руткитов в образе и обнаружением руткитов на работающем компьютере, был рассмотрен в главе 3. Если эксперт создаст дамп содержимого физической памяти и быстро проанализирует его, то система может все еще работать, но фактически будет выполняться анализ снимка ОЗУ. Как отмечает Джесси Корнблюм в своей статье «Exploiting the Rootkit Paradox with Windows Memory Analysis», «умный» руткит не будет вмешиваться в процесс создания дампа памяти, так как этим он может обнаружить свое присутствие. В конце концов, руткит, который вызывает создание аварийного дампа памяти операционной системой (что заканчивается ошибкой BSoD), выводит систему из строя как для администратора, так и для злоумышленника. Список инструментов для сбора и анализа содержимого физической памяти из ОС Windows можно найти в главе 3.

Если бы руткит вызвал создание системой аварийного дампа памяти, полученный файл аварийного дампа можно было бы проанализировать и обнаружить существование руткита. Собрав содержимое ОЗУ и выполнив поиск блоков PROCESS (дополнительные сведения о поиске информации о процессе в дампе ОЗУ см. в главе 3), можно сравнить процессы, которые не завершили свою работу, с процессами, отображаемыми в списке активных процессов, чтобы определить, какие из них скрываются руткитом, если это имеет место.

Предотвращение установки руткитов

Мы много говорили об обнаружении руткитов, но ничего не сказали о том, как фактически предотвратить установку руткитов в ОС Windows. Первый шаг к обнаружению руткитов – предотвращение их установки, что реализовывается посредством настройки и усиления защиты системы, тестирования уязвимостей и других

мер, но все они выходят за рамки этой книги. Однако достаточно сказать, что минималистский подход к конфигурации системы (например, предоставление пользователю прав доступа уровня администратора только в тех случаях, когда они ему действительно нужны) может значительно способствовать предотвращению или блокировке установки руткитов. Если установка руткита блокируется, руткит не будет работать нормально, и вы сможете обнаружить его присутствие; фактически, вследствие появления сообщений об ошибках или просто из-за чрезвычайно необычного поведения системы у вас не возникнет никаких сомнений, что в системе была предпринята попытка установить руткит.

Предупреждение

Некоторые пользователи не придерживаются минималистского подхода к конфигурации системы. Главная проблема состоит в том, что пользователи имеют в системе права доступа уровня администратора, и им разрешено устанавливать любые программы, которые они могут найти. В моей практике был случай, когда я обнаружил систему, в которой выполнялось в общей сложности четыре службы удаленного рабочего стола, и я определил, что злоумышленник использовал одну из них, чтобы получить доступ к системе. Сначала я подумал, что злоумышленник установил какую-нибудь программу для удаленного доступа, но системный администратор позднее сказал мне, что все четыре приложения были надежными и были установлены сотрудниками ИТ-отдела; каждое приложение удаленного доступа было резервной копией для других. Ни у одного из системных администраторов не было времени или навыков, чтобы управлять всеми приложениями удаленного доступа, а злоумышленник смог использовать одно из них, чтобы получить доступ к системе.

Краткое изложение

Хотя о руткитах было известно довольно давно как в мире Linux, так и в мире Windows, интерес к руткитам резко увеличился в феврале 2005 года, когда это слово было упомянуто сотрудниками Microsoft на конференции RSA Conference. Существуют книги («Руткиты: внедрение в ядро Windows» (*Rootkits: Subverting the Windows Kernel*) Хоглунда и даже *Rootkits for Dummies* на Amazon.com) и проводятся учебные курсы (Хоглунд читает лекции о технологиях руткитов во время обучающих семинаров на конференциях BlackHat) по разработке руткитов, а кроме того доступны образцы работающих (хотя в некоторых случаях экспериментальных) руткитов.

Руткиты представляют значительную угрозу системам и инфраструктурам, но самой серьезной проблемой является недостаток образования и знаний со стороны администраторов и экспертов относительно того, что такое руткит, что он может сделать, и как он работает. Имея более прочные знания в этих областях, эксперты будут лучше подготовлены, чтобы справиться с проблемой руткитов как при исследовании работающего компьютера, так и во время анализа образа данных.

Быстрое повторение

Руткиты

- Руткиты могут скрывать файлы, разделы реестра, процессы, сетевые соединения и другие объекты не только от администратора, но и от операционной системы.
- Руткиты и руткитные технологии все чаще используются во вредоносных программах и при совершении киберпреступлений.
- Лучшее понимание функций и возможностей руткитов поможет эксперту справиться с ситуациями, связанными с руткитами.

Обнаружение руткитов

- Для того чтобы обнаружить руткиты на работающем компьютере, необходимо использовать дифференциальный анализ.
- Для того чтобы обнаружить руткиты в образе системы, можно проверить образ (монтированный с помощью Mount Image Pro), используя антивирусное ПО, или даже отсортировать разделы Services в реестре по значениям времени *LastWrite*.
- Руткиты можно обнаружить в работающей системе, собрав содержимое физической памяти и проанализировав его на наличие процессов, которые являются активными, но отсутствуют в списке активных процессов.

Часто задаваемые вопросы

Вопрос: В журнале брандмауэра я обнаружил записи о странной сетевой активности, которая, судя по отметкам времени, имела место четыре часа назад. Похоже, что система в моей сети пытался установить соединение с Интернетом, используя необычный порт. Я исследовал данную систему и не нашел активных сетевых соединений, которые могли бы вызвать эту активность. Я имею дело с руткитом?
Ответ: Короткий ответ – возможно, нет. Любые данные, возникающие в системе, особенно данные, передаваемые по сети, должны иметь процесс или поток, отвечающий за их создание. Службы, как правило, выполняются в течение всего периода работы системы, а процессы могут быть недолговечными. Если вы больше не видите подобные записи в журнале брандмауэра, вероятно, процесс завершил свою работу, и поэтому вы не можете найти его в системе.

Вопрос: Что нужно сделать в первую очередь, чтобы предотвратить установку руткитов в системе?
Ответ: Управление конфигурацией имеет большое значение для предотвращения или блокировки заражений руткитами. Если вы будете придерживаться минималистского подхода, например, активировать минимум служб и уровней доступа, необходимых для функционирования системы, то значительно уменьшите вероятность атаки. В частности, если пользователям нельзя устанавливать любые программы, у них не будет возможности установить шпионские приложения, руткиты и т. п. Сокращение количества служб, выполняющихся в системе, уменьшает возможности злоумышленника получить доступ к системе и установить в ней свои инструменты и руткиты.

Вопрос: Я обнаружил руткит в одной из служб; что мне делать дальше? Мне сказали, что нет способа, чтобы определить, что произошло, и что я должен стереть данные с НЖМД и полностью переустановить операционную систему с незараженного носителя, а затем восстановить данные из незараженных резервных копий.
Ответ: Так очень часто поступает большинство администраторов, когда они имеют дело с руткитом. Однако у такого подхода есть несколько особенностей. Во-первых, вам нужно провести тщательное исследование системы (или нанять для этого специалистов), так как, возможно, вы сможете определить, что произошло (например, кража данных). Затем вам нужно как можно точнее установить, каким образом руткит попал в систему; проведите анализ первопричины. Без такого исследования вы поместите систему назад в сеть, которая может быть снова взломана или заражена. Наконец, если ваша организация подлежит проверке на соответствие нормативным требованиям (Visa PCI, HIPAA, FISMA

и т. п.), от вас могут потребовать (неявно или явно) провести расследование инцидента и предоставить как можно более подробный отчет.

Содержание

http://computer-forensics-lab.org

Перевод:
Бочков Д.С.
Капинус О.В.
Михайлов И.Ю.