Харлэн Карви

Криминалистическое исследование Windows

Глава 8

Практические примеры

Содержание этой главы:

- Изучение конкретных примеров
- Начало работы
- Расширенный анализ временной шкалы
  - Краткое изложение
  - Быстрое повторение
  - Часто задаваемые вопросы

Введение

На протяжении всей книги мы рассмотрели большое количество технической информации, но, в каждом случае, эта информация была актуальна только для одной области: оперативная память, системный реестр, файлы и т. д. Однако, большинство расследований инцидентов, которые требуется провести специалисту, или судебных экспертиз, которые требуется провести эксперту, связаны с несколькими из этих областей. Например, причиной подозрительного сетевого трафика или процесса может быть файл в системе, связанный с механизмом сохраняемости, для вредоносной программы, которым, возможно, является раздел реестра. Представление о связи между этими различными компонентами и умение понять и распознать необходимость переходить от одного компонента к другому может означать различие между пониманием и непониманием того, как произошел инцидент.

Судебная экспертиза не должна основываться только на анализе файловой системы, особенно когда эксперт исследует образ данных. В реестре, а также в других различных файлах, доступно слишком много информации, поэтому не следует опираться исключительно на основные процедуры и способы анализа.

В этой главе я расскажу о сценариях и проведенных экспертизах – назовем их «практическими примерами» – в которых применяется несколько приемов, представленных ранее в этой книге, чтобы достичь цели. В каждом случае я попытаюсь быть настолько точен с технической точки зрения, насколько позволяет ситуация, хотя понимаю, что многие отдельные подробности придется либо упростить, либо опустить. В некоторых случаях примеры могут состоять из нескольких инцидентов или исследований, но основная цель остается той же – показать, как информацию из разных глав этой книги можно связать и сопоставить с другой информацией, чтобы получить наиболее полное представление об произошедшем инциденте.

Изучение конкретных примеров

Пример 1: Документальный след

Мне было поручено провести экспертизу нескольких НЖМД. У каждого накопителя был отдельный основной пользователь, и на каждом накопителе была установлена ОС Windows XP с пакетом обновлений (SP2). В основе инцидента лежали мошеннические действия, совершенные со счетами, имеющимися у организации клиента. После собственного расследования клиент предполагал, что мошенничество было делом рук одного недобросовестного служащего.

Первым делом я попытался определить, что мне нужно искать. Для этого я связался с клиентом и ознакомился с подробностями его собственного расследования. С точки зрения клиента, дело было связано с самими счетами, а в частности с номерами, используемыми для отслеживания счетов.

Получив информацию о номерах счетов, я достаточно быстро понял, что попытка найти любые цифры, соответствующие структуре номеров счетов (используя поиск регулярных выражений), будет трудной задачей и, вероятно, приведет к большому количеству ошибочных результатов. Мне нужен был какой-нибудь способ уменьшить количество данных, которые я должен буду проанализировать.

Клиент согласился прислать мне список номеров счетов, которые, как было установлено, использовались при мошенничестве. Используя эти номера как список ключевых слов, я выполнил поиск в каждом образе НЖМД и обнаружил совпадения только в одном из них, который был связан с профилем отдельного пользователя. В действительности совпадения были найдены главным образом в одном файле, который, согласно статье из базы знаний Microsoft, находился в каталоге, используемом программой Outlook для хранения файлов, открываемых из вложений электронной почты. Затем, я извлек для анализа копию этого файла (электронная таблица) из образа. Открыв эту таблицу на своем компьютере, используемом для анализа данных, я смог просмотреть ее содержимое, но не имел ни малейшего представления о том, что она собой представляет, за исключением того, что таблица содержала информацию о счетах, и что, учитывая совпадения поиска, номера счетов соответствовали счетам, по отношению к которым были совершены подозрительные действия.

Так как я уже извлек файлы кустов реестра из соответствующих мест в образе (см. главу 4), я проанализировал информацию из пользовательского раздела реестра RecentDocs, а также из раздела, в котором перечислены электронные таблицы Excel, открывавшиеся пользователем. Я обнаружил ссылку на таблицу из каталога временного хранилища Outlook (пользовательский файл Outlook.pst отсутствовал в системе), а также ссылки на другие таблицы, одна из которых, по-видимому, была расположена на файловом сервере, возможно, в каталоге документов пользователя (во многих организациях документы следует хранить на файловом сервере, чтобы их можно было использовать при стандартном резервном копировании данных). Я не смог найти ссылки на другие таблицы, расположенные в системе пользователя, и ни одно из совпадений поиска не было найдено в свободном пространстве накопителя, что свидетельствовало о том, что файлы, содержащие поисковые термины, недавно не удалялись.

На следующем этапе я извлек метаданные из электронной таблицы Excel. Документы Microsoft Office (документы Word, таблицы Excel и даже презентации PowerPoint) используют составную структуру («файловая система в файле») для хранения данных. Поэтому большое количество метаданных может храниться (и хранится) в структуре документа, и их можно извлечь для анализа и использования. Используя Perl-скрипт «oledmp.pl», находящийся на носителе, который идет в комплекте с этой книгой, я смог извлечь метаданные и увидеть, что пользователь открывал, редактировал и распечатывал эту электронную таблицу. Поля метаданных в электронной таблице содержали даты и время выполнения этих действий. Эти даты и время также соотносились с отметками даты и времени в файловой системе и реестре.

После того как я собрал всю эту информацию в понятную временную шкалу, я предоставил ее в виде отчета клиенту. Как и многие эксперты, я часто не знаю, чем заканчивается дело после того, как я отдаю клиенту итоговый отчет, и это еще один пример такой ситуации. Однако, этот пример показывает, как можно использовать несколько способов анализа, чтобы провести тщательное исследование и получить много сведений об инциденте. В данном случае, поиск по ключевым словам помог значительно сократить объем обрабатываемых данных и привел к отдельному документу, местонахождение которого указывало на вероятный источник документа (вложение

электронной почты Outlook). Затем анализ реестра показал, что, во-первых, пользователь получал доступ не только к этому документу, но и к другим документам с похожими названиями, а во-вторых, что как минимум один из этих документов был расположен на файловом сервере. Наконец, анализ метаданных, извлеченных из документа, показал, что кто бы ни получал доступ к этой учетной записи пользователя, он изменял и распечатывал файл, о чем свидетельствовали отметки времени этих действий. Все эти сведения помогли клиенту определить источник мошеннических действий.

Пример 2: Вторжение

Данный пример связан с вторжением в корпоративную сетевую инфраструктуру, которое началось со взлома домашнего компьютера сотрудника. Этот тип инцидентов встречается, возможно, чаще, чем многие думают. Домашние ПК, вдобавок к компьютерам, используемым обычными пользователями (ноутбуки студентов, настольные и переносные компьютеры сотрудников корпораций и т. д.), очень часто подвержены взлому, так как они рассматриваются как легкие цели: они достаточно распространены и, как правило, плохо защищены. Многие пользователи не понимают, насколько ценные данные хранятся на их домашних ПК. Они пользуются услугами интернет-банкинга и каждый год заполняют налоговые декларации через Интернет со своих компьютеров. Геймеры получают доступ к онлайн-играм, и, хотите верьте, хотите нет, существует целый рынок игровых персонажей. Поэтому домашние компьютеры, помимо того что они могут быть добавлены в ботнет, предлагают злоумышленнику множество других ценных данных.

Инструменты и ловушки…

Ценность компьютера

Один из нескольких факторов, приемлемый или понятный для многих пользователей, – это ценность, которую их компьютер (настольный ПК дома, ноутбук, используемый студентом для занятий, и т. д.) может представлять для злоумышленника. Несколько лет тому назад в Техасском университете в Остине я читал курс по расследованию инцидентов в ОС Windows 2000 и заметил удивление на лице одной из студенток в группе. Я попросил ее поделиться с группой своими мыслями, и она выпалила: «С какой стати кому-нибудь может понадобиться мой компьютер?!». Подумайте о том, что ваш компьютер, или любой компьютер, может предложить кому-нибудь. Во-первых, для чего вы используете свой компьютер? Вы заполняете каждый год налоговую декларацию на компьютере? Пользуетесь услугами интернет-банкинга или совершаете покупки в Интернете с помощью компьютера? Загрузив регистратор работы клавиатуры на вашем компьютере, злоумышленник может легко получить эту информацию. Помимо доступа к вашим личным данным, ваш компьютер предлагает злоумышленнику другие ресурсы. Например, злоумышленник может установить в вашей системе бот и добавить ваш компьютер в свой ботнет или сдавать его в аренду другим для рассылки спама или проведения атак типа «отказ в обслуживании» (DoS).

В данном случае, злоумышленник получил доступ к домашнему компьютеру сотрудника и установил регистратор работы клавиатуры (позднее это было подтверждено посредством отдельного анализа этого домашнего ПК). Таким образом злоумышленник узнал, что сотрудник входит в корпоративную сеть через клиентское приложение удаленного рабочего стола Windows, а так как все нажатия клавиш фиксировались, злоумышленник получил имя пользователя и пароль сотрудника для входа в сеть. Затем ему ничего не стоило открыть свое клиентское приложение удаленного рабочего стола, указать в нем правильный IP-адрес и ввести только что полученные учетные данные пользователя, чтобы войти в корпоративную сеть фактически под видом сотрудника.

Оказалось, что злоумышленника легко отследить. Войдя в сеть через клиентское приложение удаленного рабочего стола, злоумышленник получил доступ к оболочке, то есть при выполнении своих действий он взаимодействовал с проводником Windows так же, как обычный пользователь, работающий на компьютере. Вследствие этого многие из действий злоумышленника были зарегистрированы в реестре. Кроме того, злоумышленник имел достаточно высокий уровень доступа из-за того, что украденные учетные данные принадлежали сотруднику, который управлял учетными записями пользователей. Более того, злоумышленник активировал учетную запись администратора домена, которая была создана ранее, но никогда не использовалась. Это означало, что каждый раз, когда злоумышленник получал доступ к другому компьютеру в корпоративной сети, на этом компьютере создавался профиль для этой учетной записи администратора домена. Это позволило достаточно легко отследить действия злоумышленника в сети, по крайней мере на начальной стадии расследования (т. е. мы не хотели совершить ошибку, предполагая, что это было все, что сделал злоумышленник).

Вместе с сотрудниками ИТ-отдела клиента мы создали скрипт, который выполнял во всех компьютерах домена поиск признаков данного профиля пользователя. Сначала мы определили компьютеры, на которых существовал этот профиль, что позволило нам предварительно узнать, к скольким компьютерам получал доступ злоумышленник. Клонировав данные каждого из этих компьютеров, мы начали разрабатывать временную шкалу действий, используя дату создания каталога профиля как время, когда злоумышленник получил доступ к системе первый раз, а время последнего изменения файла куста «NTUSER.DAT» профиля как время, когда злоумышленник получил доступ к системе последний раз. Эти интервалы времени позднее были подтверждены во время исследования содержимого разделов UserAssist.

Совет

Это отличный пример дела, в котором можно было бы получить множество подтверждающих данных, если бы клиент сохранял журналы регистрации событий в центральном хранилище журналов. Хотя это было совсем не обязательно (так как дата создания файлов «NTUSER.DAT» в профиле пользователя указала нам на время первого входа злоумышленника в каждую систему, а артефакты реестра указали на интервалы действий злоумышленника), мы могли бы намного быстрее сузить список компьютеров, к которым получал доступ злоумышленник, если бы конфигурация аудита была задана правильно, а записи журналов регистрации событий собирались и архивировались в одном месте.

После того как нам удалось отследить действия злоумышленника в сети, нам нужно было установить, что злоумышленник сделал или пытался сделать на каждом компьютере. И снова тот факт, что злоумышленник получал доступ к каждому компьютеру через проводник Windows, предоставил нам много очень ценной информации. Этот клиент уже потратил много времени и усилий, чтобы составить список конфиденциальных данных в сети и указал, где эти находятся эти данные (как определено законами штатов, например, законом SB-1386 штата Калифорния, а также стандартом защиты информации в индустрии платежных карт Visa (Payment Card Industry Data Security Standard)). Приступив к анализу реестра, мы сосредоточились на файле «NTUSER.DAT» профиля пользователя, проверив раздел RecentDocs, списки недавно использованных файлов (например, электронные таблицы Excel и документы Word) и другие данные. Мы проверили разделы RecentDocs, чтобы увидеть, к каким типам файлов (xls, .doc, .jpg и т. д.) выполнялись обращения, а затем исследовали списки недавно использованных документов, чтобы узнать, какие приложения применялись для открытия этих файлов. Интересно, что обращения выполнялись к небольшому количеству файлов, возможно, частично из-за того, что мы обнаружили в разделе реестра ACMru. Было

похоже, что злоумышленник проводил поиск, открыв меню **«Пуск» (“Start”) | «Поиск» (“Search”) | «Файлы и паки» (“For Files and Folders”)**, и пытался найти файлы с определенными ключевыми словами. Вероятно, этого не заметили сотрудники ИТ-отдела, потому что несколько компьютеров было размещено в центре обработки данных, но информация, которую искал злоумышленник, используя ключевые слова, не хранилась на самом деле в этой организации. Однако, судя по признакам в некоторых системах, было ясно, что злоумышленник искал и нашел электронную таблицу, содержащую пароли, и были приняты соответствующие меры, чтобы решить проблему относительно этой раскрытой информации.

И в этом случае использовалось несколько источников данных для проведения расследования и экспертизы. Журналы виртуальной частной сети использовались, чтобы определить IP-адрес злоумышленника, а затем проводился анализ файловой системы и отметок времени изменения, доступа и создания, чтобы подтвердить перемещения злоумышленника в сети. Наконец, анализ реестра предоставил полную картину о действиях злоумышленника, в том числе о проведении поиска и доступе к файлам. Этот последний анализ помог определить, получал ли злоумышленник доступ к конфиденциальным данным. Посредством анализа реестра мы получили убедительные доказательства того, что злоумышленник не обращался к файлам, которые, как было установлено ранее, содержали конфиденциальные данные.

Пример 3: Судебное родео на конференции DFRWS 2008

В августе 2008 года мы с Кори Алтеидом посетили конференцию DFRWS 2008. Мы отлично провели время, а во вторник вечером Кори принимал участие в «Судебном родео» (“Forensic Rodeo”). Я не очень хотел участвовать, так как хотел понаблюдать, внимательно проследить, как другие люди подходят к решению предлагаемой задачи. Когда сидишь в офисе, выполняя обычно какой-нибудь анализ самостоятельно, не часто получаешь возможность увидеть других специалистов в действии, а не только обсудить с ними рабочие дела и связанные с этим трудности. Довольно забавно слышать от себя слова «в действии», потому что, по правде говоря, наблюдать за судебным анализом так же захватывающе, как за ростом волос на голове. Однако, в целом, это было крайне поучительное событие, предоставляющее возможность другим специалистам попробовать свои силы в решении подобных задач. Сценарий и файлы «Судебного родео» можно найти по адресу www.dfrws.org/2008/rodeo.shtml.

Задача, предлагаемая на конкурсе «Судебное родео», была связана с дампом памяти (см. главу 3) и образом, созданном с флеш-накопителя. Целью задачи было проанализировать эти два элемента данных и ответить на вопросы судей, Оуэна Кейси (Eoghan Casey) и Дэна Калила (Dan Kalil). Доктор Майкл Коэн выиграл конкурс, ответив на наибольшее количество вопросов из всех участников. Я не хочу давать никаких подсказок или раскрывать дополнительную информацию относительно конкурса, но скажу лишь, что решение задачи включало в себя анализ памяти и извлечение данных (в этот раз никакого анализа реестра!).

Пример 4: Копирование файлов

Вопрос, который мне очень часто задают, состоит в том, возможно ли определить, какие файлы были копированы на флеш-накопитель (внешнее запоминающее устройство) и с него. Я встречал этот вопрос в публичных рассылках, а когда посещал саммит SANS Forensic Summit в октябре 2008 года, мне задавали его два участника, а также члены моей собственной команды, которые отвечали на вопросы клиентов. Учитывая то, как распространены сегодня флеш-накопители, а также другие съемные носители данных, такие как цифровые камеры, устройства iPod и т. д., многие организации беспокоит проблема несанкционированного копирования информации (т. е. кражи данных,

например, интеллектуальной собственности). К сожалению, слишком часто эта проблема возникает после факта кражи, а не решается заранее.

Как мы видели в главах 4 и 5, использование съемных USB-накопителей на компьютерах можно отследить. С помощью методов анализа из обеих глав мы можем определить не только время, когда устройство было подключено к компьютеру впервые, но также и время, когда устройство было отсоединено от системы последний раз. Эта информация может быть очень полезной, когда дело касается составления схемы подключения съемных накопителей к компьютеру или нескольким компьютерам. Она также подскажет нам, с чего начинать составление временной шкалы.

Одна из проблем, связанная с исходным вопросом, состоит в том, что большинство современных операционных систем (я говорю «большинство», потому что я не видел их всех) не отслеживает и не регистрирует операции копирования или перемещения файлов в файловой системе. Однако, многие, похоже, думают, что, так как с помощью судебного анализа можно восстановить удаленные файлы, то можно совершить и другие чудеса, например, определить, кто скопировал файл из одного места в другое, и когда это было сделано. Вопреки тому, что показывают в популярных телевизионных сериалах типа «Место преступления» (*CSI*), это, в большинстве случаев, совсем не так. Если бы у эксперта были оба носителя – исходный накопитель (с которого выполнялось копирование) и целевой накопитель (на который выполнялось копирование) – то он, проведя анализ обоих носителей (и их отметок времени), смог бы определить, какой из них был исходным, а какой – целевым накопителем. Но, в большинстве случаев, у эксперта нет обоих носителей.

Наличие только одного носителя для экспертизы не позволяет эксперту точно определить, какие файлы были копированы *с* этого носителя, но эксперт может найти признаки того, какие файлы, возможно, были копированы *на* носитель, используя информацию, предоставленную в статье № 299648 (из базы знаний Microsoft), которая называется «Description of NTFS date and time stamps for files and folders» (*http://support.microsoft.com/?kbid=299648*). В этой статье дается понятное описание того, как операции копирования или перемещения файлов с одного носителя на другой влияют на отметки времени файлов. Например, если файл копируется из раздела FAT (большинство флеш-накопителей отформатировано в файловой системе FAT по умолчанию) в раздел NTFS, то дата последнего изменения файла остается такой же, а дата создания файла обновляется до текущего времени системы. То же верно в отношении случаев, когда файл копируется из каталога NTFS в подкаталог NTFS. Но если файл перемещается (а не копируется), дата создания файла остается неизмененной. Согласно этой статье, «во всех примерах дата и время изменения не меняются, если не меняется свойство файла. Дата и время создания файла меняются в зависимости от того, был ли файл копирован или перемещен».

Однако следует обратить внимание на то, что в этой статье из базы знаний не описывается способ, используемый для перемещения файлов. Например, рассмотрите следующие команды перемещения, в которых файл копируется со съемного носителя (E:\), отформатированного в FAT, в каталог в файловой системе NTFS:

```
C:\test>dir /tc E:\Dec03_0004.jpg
Volume in drive E has no label.
Volume Serial Number is 18DA-DF72
Directory of E:\
12/03/2008 09:59 PM 7,250 Dec03_0004.jpg
1 File(s) 7,250 bytes
0 Dir(s) 72,757,248 bytes free
C:\test>move E:\Dec03_0004.jpg
C:\test>dir /tc Dec03_0004.jpg
Volume in drive C has no label.
Volume Serial Number is B83C-BC0A
```

```
Directory of C:\test
12/05/2008 09:36 AM 7,250 Dec03_0004.jpg
1 File(s) 7,250 bytes
0 Dir(s) 11,019,108,352 bytes free
```

Как видно из этого примера, дата создания файла изменяется после выполнения операции перемещения, что противоречит тому, что написано в статье № 299648 из базы знаний Microsoft. Это ясно показывает необходимость тестирования и исследования инструментов и способов анализа.

Здесь нужно обратить внимание на несколько важных факторов относительно нашего анализа. Во-первых, если пользователь копирует файл, а затем изменяет файл некоторым образом, то теряется информация, которая может указать нам на то, что файл был копирован из одного места в другое; другими словами, если дата изменения файла старше, чем дата создания, это может свидетельствовать о том, что файл был копирован. Подумайте, разве файл не должен быть сначала создан, а затем, через некоторое время после этого, изменен? Программа Microsoft Word автоматически сохраняет копию файла, который вы редактируете, приблизительно каждые 10 минут. Поэтому, после первых 10 минут следует ожидать, что дата создания будет на 10 минут старше, чем дата изменения (в идеальных условиях, конечно). Во-вторых, имея только один носитель для анализа, вы не сможете точно определить, какие файлы были перемещены из одного места в другое просто из-за того, что отметки времени такого файла остаются неизмененными (при условии, что используются опции меню «Вырезать» (“Cut”) и «Вставить» (“Paste”), а не команды перемещения из командной строки).

Наконец, несмотря на то, что операция копирования или перемещения влияет на отметки времени файла, связанные с файловой системой, отметки времени, встроенные в содержимое файлов (например, OLE-содержимое в некоторых версиях документов Microsoft Office, см. главу 5) в виде метаданных не будут изменены и, следовательно, могут быть использованы в некоторых видах анализа. В зависимости от типа документа и количества метаданных, хранящихся в этом документе, вы сможете точно определить, что документ был создан в другом месте, а не на исследуемом носителе.

Исследование образа данных с целью найти файлы, которые, возможно, были скопированы на компьютер, включает в себя анализ реестра, а также анализ файловой системы и отметок времени изменения, доступа и создания. В некоторых случаях, в зависимости от типа документа, который был копирован, анализ метаданных может пролить некоторый свет на ситуацию.

Пример 5: Сетевая информация

Иногда, во время обнаружения или расследования инцидента, сотрудники, обслуживающие сеть, могут иметь доступ к журналам брандмауэра выходной фильтрации или к перехваченному сетевому трафику, который показывает сетевые пакеты (и, возможно, данные), выходящие из внутренней сети. Независимо от источника (журналы или перехваченный трафик), всегда можно найти человека, имеющего доступ к данным, которые точно показывают исходный IP-адрес трафика (так как он возникает из внутренней сети). Этот трафик можно связать с работающим компьютером во внутренней сети либо путем отслеживания статического, неизменного IP-адреса, либо посредством анализа журналов DHCP-сервера. Другой тип информации - исходный порт трафика (часть заголовка TCP или UDP), поможет вам связать исходящий трафик с процессом, выполняющимся в системе.

Прежде чем продолжать это описание, нужно отметить и понять важный факт: в компьютерной системе ничего не происходит без выполнения какого-нибудь процесса. Точнее, квант времени в системах Windows выделяется для потока, но дело в том, что для того, чтобы система создавала трафик, в ней *должен* выполняться какой-нибудь код.

Поэтому немедленное расследование подробностей сетевого трафика (т. е. исходного IP-адреса и порта) отлично соответствует термину «временн**а**я близость», который я однажды услышал от Аарона Уолтерса (Aaron Walters). Хотя этот термин звучит как фраза из какого-нибудь научно-фантастического фильма, он подразумевает, что расследование нужно начинать как можно быстрее после того, как был обнаружен инцидент, а не ждать несколько часов или дней. Соблюдая этот принцип в отношении инцидента, специалист, вероятнее всего, соберет более свежие (и, возможно, более полные) данные. Результаты команды «netstat.exe» (или сетевые подключения, отображаемые в дампе памяти) могут показать признаки выходного соединения и указать специалисту на процесс, создающий трафик. Например, ниже предоставлен фрагмент выходных данных, возвращаемых в результате команды *netstat –ano* на моем компьютере:

```
TCP 192.168.1.5:8352 98.136.112.141:80 ESTABLISHED 3536
```

Этот фрагмент выходных данных команды *netstat* показывает исходный IP-адрес и порт, используемый процессом с идентификатором 3536, которым в данном случае является «firefox.exe». Ту же информацию можно легко увидеть в перехваченном сетевом трафике (как было описано выше), а также в журналах брандмауэра или журналах, сохраняемых другими сетевыми устройствами. Знания о том, как выполнять сбор и анализ данных как в сети, так и на компьютере, помогут вам значительно сократить количество времени, необходимого для обнаружения и расследования инцидента. В такой ситуации, информацию журналов устройств можно сопоставить с перехваченным сетевым трафиком и данными, собранными с компьютера (т. е. дамп памяти), чтобы определить объем и тип данных, выходящих из сети.

Пример 6: Внедрение SQL-кода

Во второй половине 2007 года было совершено несколько атак с внедрением SQL-кода, а нескольких месяцев спустя атаки, похоже, не только стали происходить чаще, но и стали изощреннее. Внедрение SQL-кода – способ атаки, использующий уязвимости в прикладном уровне между веб-сервером и системой базы данных. Злоумышленник отправляет специально созданные запросы на веб-сервер, который передает их в базу данных без подтверждения входных данных, без проверки границ и т. д. База данных в свою очередь обрабатывает эти команды злоумышленника (см. главу 5).

Инструменты и ловушки…

Внедрение SQL-кода

Выполнив быстрый поиск в Google по словам «SQL injection» (рус. *внедрение SQL-кода*), вы найдете несколько ссылок на сайты, где этот способ атаки объясняется подробно, на презентации и советы о том, как проводить такие атаки, а также на видеоролики, демонстрирующие атаки с внедрением SQL-кода. Тот факт, что существует бесконечное количество подробнейших ресурсов для совершения этих атак, должен быть достаточным, чтобы убедить руководителей отделов информационных технологий и отделов информационной безопасности выделить средства на защиту организаций. Этого можно достичь посредством оценочного анализа сетевой инфраструктуры, который принимает во внимание хранение и обработку конфиденциальных данных, и выработки приоритетного подходка к защите данных и инфраструктуры.

В начале весны 2008 года внимание многих СМИ было обращено на определенный тип атаки с внедрением SQL-кода, во время которой предположительно автоматизированное программное обеспечение внедряло специально созданные ссылки на скрипт JavaScript в базе данных, а затем эти ссылки обрабатывались веб-браузером

пользователя, так как база данных возвращала эти ссылки на веб-сервер в виде динамического веб-содержимого. Этот тип атак привлек внимание СМИ, потому что он был достаточно заметен. Однако, были и другие атаки, о которых не говорили публично - когда злоумышленник использовал внедрение SQL-кода, чтобы проникнуть глубоко в целевую инфраструктуру и, во многих случаях, оставаться с чрезвычайно высокими привилегиями в сети значительный период времени.

Основной принцип атаки, с внедрением SQL-кода, состоит в том, что злоумышленник обходит надежную сеть из-за того, что общедоступный веб-сервер расположен в демилитаризованной зоне, а база данных находится во внутренней сети. Веб-сервер получает команды злоумышленника и передает их на сервер базы данных полностью в обход брандмауэра (потому что передача данных между веб-сервером и сервером базы данных является необходимым требованием). Во время расследования таких инцидентов команды злоумышленника были отчетливо видны в журналах веб-сервера в формате ASCII и вначале не имели специального кодирования. После извлечения журналов эксперт мог ясно увидеть первоначальное установление связи, тестирование уязвимости, разведывательные действия в сети (такие поданные злоумышленником команды, как *ipconfig /all* и *net view*) и даже подключения к другим компьютерам. В определенный момент времени злоумышленник подготавливал плацдарм для атаки в системах, к которым он получил доступ, загружая в эти системы программное обеспечение. Первоначально для загрузки файлов использовался TFTP-клиент и протокол UDP. Затем создавались и выполнялись скрипты FTP (т. е. создание скриптов с помощью команды «echo» и их запуск с помощью команды *ftp –s:filename*), чтобы загрузить архивы на платформу. Похоже, что в некоторых случаях загружаемые архивы были самораспаковывающимися исполняемыми файлами, так как в журналах веб-сервера было записано, что злоумышленник запускал файл «downloaded.exe», а затем либо проверял (посредством команды *dir*) полученные файлы, либо просто выполнял команды.

Во время расследования инцидентов было собрано несколько образцов исполняемых файлов, которые загружались в систему. Сначала результаты проверки этих файлов антивирусными программами или такими сайтами, как VirusTotal.com, были отрицательными. В следующем году специалисты по расследованию инцидентов продолжали сталкиваться с атаками с внедрением SQL-кода, которые становились все сложнее. За короткое время поисковые термины, используемые для обнаружения атак с внедрением SQL-кода в журналах веб-серверов, стали бесполезными, потому что злоумышленники начали использовать новые способы для кодирования (шестнадцатеричное кодирование или, в некоторых случаях, кодирование набора символов) своих команд. Следовательно, критерии поиска нужно было обновить, чтобы обнаружить эти атаки. Один из способов сделать это – определить страницу, к которой выполняется запрос, а затем выполнить поиск необычно длинных запросов, отправляемых к этой странице. Добавление новых найденных ключевых слов к критериям поиска позволило уменьшить количество ошибочных результатов, а специально созданные Perl-скрипты помогли быстро декодировать запросы в понятный для человека формат. Еще один способ для передачи исполняемого кода в систему заключался в следующем: злоумышленник разбивал исполняемый файл на 512-байтные части и отправлял каждую часть по порядку в поля базы данных (не забывайте, что посредством внедрения SQL-кода злоумышленник выполняет команды в базе данных с теми же привилегиями, что и у базы данных, которые для Microsoft SQL Server обычно являются системными), а затем вновь собирал и выполнял исполняемый файл в файловой системе сервера базы данных. В случаях, в которых использовался этот способ, нам удалось извлечь и повторно собрать исполняемый код из журналов веб-сервера, а затем подтвердить, что мы правильно отформатировали исполняемый файл, проанализировав заголовок PE-файла (см. главу 6).

Когда у нас были исполняемые файлы с похожими именами, в архиве от предыдущих атак с внедрением SQL-кода, мы использовали инструмент «ssdeep.exe»

(http://ssdeep.sourceforge.net/) Джесси Корнблюма (Jesse Kornblum) для сравнения нечетких хэш-значений (fuzzy hash) и в большинстве случаев определяли, что файлы были похожи на 98 или 99 процентов. Анализируя PE-заголовок, чтобы разбить исполняемый файл на разделы, мы смогли определить разделы, которые изменились (путем сопоставления хэша MD5) по сравнению с предыдущими версиями файлов.

Способы отслеживания злоумышленника в сети во время расследования атак с внедрением SQL-кода включали в себя анализ реестра, так как злоумышленнику удавалось в определенный момент времени взаимодействовать с проводником Windows взломанной системы. В некоторых случаях были взломаны коллективные (или совместные) учетные записи администраторов (т. е. они имели легко угадываемые пароли), но в большинстве случаев злоумышленник создавал учетные записи уровня администратора домена (иногда существование этих учетных записей подтверждалось записями об их создании в журнале регистрации событий), а затем использовал их, чтобы получить доступ к другим компьютерам в сети. Анализ файловой системы показал создание профилей пользователей в системах и предоставил начальную временную шкалу использования этих учетных записей, тогда как анализ реестра предоставил данные о действиях злоумышленника в этих системах, а также об использовании механизмов сохраняемости, применяемых злоумышленником для вредоносных программ, которые были добавлены во взломанные системы. Так как веб-сервер не взламывается во время атаки с внедрением SQL-кода, журналы веб-сервера показали полную картину первоначальных действий злоумышленника при получении доступа к сетевой инфраструктуре (иногда разведывательные действия совершались за несколько недель или месяцев до атаки). Анализ вредоносных файлов показал, что с течением времени использовались похожие инструменты более высокого уровня.

Пример 7: Все дело в приложении

Не так давно я проводил расследования инцидента, который, предположительно, был связан с незаконными действиями. Как это часто происходит, когда я работаю консультантом компании, первое сообщение об инциденте я получил от клиента, а для большинства моих клиентов характерно то, что они не являются опытными специалистами по расследованию инцидентов. В данном случае инцидент был связан с повторяющимися запросами «подозрительных» доменных имен – подозрительных в том смысле, что как минимум один из доменов, похоже, находился в Китае. Клиент выполнил поиск имени домена в Google и обнаружил, что оно связано с уязвимостью приложения, выявленной весной 2008 года. Узнав об этом, клиент вызвал мою команду.

Прибыв на место, я обнаружил, что с отдельного компьютера отправлялась по меньшей мере часть подозрительного DNS-трафика. Этому компьютеру, вероятно, был назначен статический IP-адрес (без использования DHCP), поэтому клиенту было относительно легко отследить компьютер и изъять его у сотрудника. К сожалению, единственными принятыми мерами было выключение компьютера и извлечение его из сети; сбор содержимого физической памяти или других энергозависимых данных не был выполнен перед завершением работы системы. Еще один недостаток состоял в том, что, когда сотруднику сообщили, что его компьютер был источником подозрительного трафика, и что компьютер нужно будет исследовать, он, по некоторым сведениям, заявил, что собирается «надежно удалить данные» из системы. На этом этапе цель моего исследования состояла из двух частей: (1) определить, действительно ли этот сотрудник устанавливал и использовал программу для надежного удаления данных, и (2) определить источник подозрительных запросов к DNS.

Сначала я должен был создать образ НЖМД компьютера сотрудника. В то же время я попытался собрать информацию о любых журналах, которые могут быть доступны в сети. Мне сказали, что в отчете для руководства показаны записи о наиболее часто встречающихся запросах к DNS, и что есть несколько журналов из устройства

обнаружения ботнетов, где показаны записи о запросах к DNS; однако ничего не упоминалось о китайском доменном имени, которое было главной причиной беспокойства клиента, когда он обращался ко мне за помощью. Я обратил внимания, что в сетевых журналах запросы к DNS были показаны в алфавитном порядке вместе с отметками времени.

После того как я создал образ НЖМД, проверил его достоверность и убедился, что вся моя документация в порядке, я открыл примечания к делу, монтировал в своем рабочем ноутбуке созданный образ как файловую систему в режиме только для чтения и начал проверку с использованием антивирусных приложений. Пытаясь сократить объем данных и найти то, что клиент неопределенно описал как «что-то подозрительное», я проверил монтированный образ при помощи нескольких антивирусных приложений, в том числе специальных приложений для поиска отдельных вредоносных файлов. Мне удалось обнаружить несколько файлов, которые могли быть вредоносными программами или артефактами вредоносных программ, но, судя по метаданным и содержимому файлов, это, вероятно, были ошибочные результаты. Затем я исследовал журналы из системы, в том числе журналы установленного антивирусного приложения и журналы средства удаления вредоносных программ (файлы «mrt.log», см. главу 5). Ни один из них не свидетельствовал о действиях, которые могли бы относиться к рассматриваемому делу.

Затем я приступил к анализу журнала регистрации событий Windows. Все три журнала событий имели размер 512 килобайт, а журнал событий безопасности не содержал записей (посредством анализа файла куста реестра «Security» я узнал, что аудит не был включен). Журнал событий приложений содержал ряд записей, созданных антивирусным приложением, но гораздо важнее то, что в журнале событий системы было записано, что в течение последних нескольких недель система перезагружалась несколько раз. В каждом случае после записи о событии, в которой говорилось, что была запущена служба журнала событий, была еще одна запись о том, что было запущено отдельное антишпионское приложение. Я записал это и составил таблицу, показывающую приблизительное время запуска системы, на основании этих записей о событиях. Мне удалось сопоставить значения времени запуска системы и значения времени из нескольких журналов устройства обнаружения ботнета, предоставленных клиентом. Три самых полных журнала (на самом деле это были фрагменты журналов устройства, содержащие данные о действиях, связанных с исследуемым компьютером) показывали записи об операциях поиска в DNS, которые начинались почти в то же время, когда запускалась система. Фактически, первая запись в каждом журнале была тесно взаимосвязана с временем запуска антивирусного приложения. Однако журналы устройства, для обнаружения ботнетов, также не содержали упоминаний о китайском домене.

Затем я выполнил поиск имени подозрительного китайского домена по всему накопителю, предполагая, что увижу совпадения поиска только в файле подкачки. Тем не менее, к моему великому удивлению, я обнаружил ссылки не только на это доменное имя, но и на другие имена, в нескольких файлах кустов реестра (что в основном касается файла «NTUSER.DAT» для всех пользователей и файлов, найденных в точках восстановления Windows XP), а также в файле «hosts» (значение файла «hosts» в отношении сопоставления имен объясняется в статье по адресу http://support.microsoft.com/kb/172218). Исследование файла «hosts» показало, что отдельное антишпионское приложение, установленное в системе, добавило несколько записей в этот файл (в комментариях файла указывалось, что записи были добавлены этим приложением), перенаправляя все из них на адрес localhost (т. е. 127.0.0.1), эффективно отклоняя запросы на подключение к этим доменам. В результате исследования файлов кустов реестра было обнаружено, что в то же время (исходя из отметок времени *LastWrite*) те же доменные имена, в том же порядке, были добавлены в разделы реестра, принудительно помещая эти домены в «Зону ограниченных узлов» (“Restricted Zone”) в настройках браузера Internet Explorer. Таким

образом эффективно устанавливались ограничения на то, что пользователи могли сделать в Internet Explorer, если им удавалось подключиться к хостам в этих доменах.

На данном этапе я был почти уверен, судя по всей информации, которую я получил, а также нашел в Интернете, что подозрительная активность была не результатом работы вредоносной программы (вируса, червя или шпионского ПО), а результатом взаимодействия двух антишпионских приложений; то есть одно из них изменило реестр и файл «hosts», а второе выполнило DNS-запросы для каждого доменного имени, перечисленного в файле «hosts». Я нашел одно сообщение на интернет-форуме, свидетельствующее о том, что дело, возможно, в этом, и договорился с клиентом провести исследование компьютера в сети в реальных условиях эксплуатации, чтобы подтвердить эту информацию. Мы выполнили начальную загрузку системы, отключили службы антишпионского приложения и перезапустили систему, снова включили службы и еще раз выполнили перезагрузку, и даже изменили файл «hosts», чтобы он содержал определенные записи, и опять перезагрузили систему. Каждый раз, как и ожидалось, мы видели DNS-трафик в сети (с помощью анализатора сетевых пакетов на отдельном компьютере в той же подсети); в случае, когда система перезагружалась с отключенным антишпионским приложением, мы совсем не увидели запросов доменных имен к DNS.

Наконец, в результате анализа реестра и содержимого папки «Prefetch» не было найдено никаких признаков того, что сотрудник устанавливал в системе программу для надежного стирания данных или запускал такую программу со съемного носителя.

Использование комплексных способов исследования и сопоставление нескольких подкрепляющих источников данных позволило нам определить источник подозрительной и потенциально вредоносной активности. Во время первоначального расследования клиент собрал лишь небольшое количество данных, а затем сделал предположение о вредоносной активности, основываясь только на поиске в Google информации об отдельном доменном имени. Отсутствие нужных данных (т. е. всех перехваченных сетевых пакетов, более подробных сетевых журналов, дампа физической памяти или частей энергозависимых данных из исследуемой системы и т. д.) привело к тому, что анализ занял больше времени и, как следствие, стоил клиенту дороже. В конце концов исследование компьютера в реальных условиях (в загруженном состоянии в сети) позволило нам подтвердить, что активность была результатом работы надежного приложения (в действительности двух взаимодействующих приложений), и что после запросов доменных имен к DNS не следовали попытки подключиться к хостам в этих доменах посредством протокола UDP или TCP.

Начало работы

На форумах я довольно часто вижу следующий вопрос: «С чего начинать экспертизу?». С чего начинать анализ при наличии множества данных – образов, созданных из нескольких систем, перехваченных сетевых пакетов, файлов журналов и т. д.? Что делать в первую очередь?

Универсальный ответ на все вопросы, который я узнал во время шестимесячного обучения в подготовительной школе в Квантико в штате Вирджиния (где проходят подготовку все офицеры морской пехоты США) звучит так: «Все зависит от обстоятельств». Он был уместен тогда и с таким же успехом приемлем сейчас, потому что он правильный. Допустим, у вас есть образ данных, полученный из отдельного компьютера. Какая операционная система выполнялась или была доступна в то время, когда создавался образ? Какая была платформа? Документировалось ли создание образа? Вероятно, вы думаете, какое это имеет значение – но посмотрите на свои инструментальные средства и вы увидите, что они используются для работы с разными файловыми системами. У вас образ данных из ОС Linux? Если да, то какая файловая система в образе: ext2, ext3 или ReiserFS?

Ну ладно, ладно! Я знаю, что это книга о судебной экспертизе ОС Windows. Но я надеюсь, вы понимаете, что я хочу сказать. Начиная исследование, эксперт должен принимать во внимание несколько факторов. Один из таких факторов – это файловая система. Есть ли у вас инструменты, необходимые для открытия и просмотра созданного образа? Однако еще важнее то, что эксперт должен обдумать свои цели. Что он надеется получить в результате экспертизы? Чего нужно достичь посредством исследования имеющихся данных? Видите, как легко мне было объяснить вам, что «все зависит от обстоятельств»?

Самое важное в начале экспертизы – понять ее цели. Независимо от того, в какой среде вы работаете, любая экспертиза должна иметь причину или цель. Если вы сотрудник правоохранительных органов, что вы ищите? Вы пытаетесь найти информацию о пропавшем ребенке или определить, продавал ли владелец компьютера незаконные изображения? Если вы консультант, то перед началом экспертизы вы уже должны встретиться с клиентом и тщательно обсудить, что он хочет получить или чего он хочет достичь в результате. Даже если вы специалист, в срочном порядке расследующий инцидент, вы должны понимать, что вам нужно получить в результате своих действий, *до* того, как вы фактически выполните их. Если вы расследуете заражение системы вредоносной программой, пытаетесь ли вы определить артефакты этой программы или получить копию ее кода, чтобы предоставить его производителю вашего антивирусного приложения? Или вы исследуете причину, по которой необычный трафик поступает на один из компьютеров во внутренней сети? Цели экспертизы или расследования должны определять ваши действия.

Инструменты и ловушки…

Цели расследования инцидентов

Работая специалистом по расследованию инцидентов, я часто (на самом деле все чаще и чаще) замечаю, что начальное расследование инцидента, проводимое сотрудниками клиента, может подвергнуть организацию большей опасности, чем сам инцидент.

Я понимаю, что сейчас вы, вероятно, перечитываете последнее предложение и пытаетесь понять его смысл. Ведь оно не до конца понятно, не так ли? Суть в том, что во многих случаях начальное расследование инцидента проводится сотрудниками ИТ-отдела, и их действия и процедуры ориентированы в первую очередь на информационные технологии. Очень часто первостепенной задачей (поставленной руководством) сотрудников ИТ-отдела является поддержание систем (почтовых серверов, сетей и т. д.) в рабочем состоянии. Поэтому, если в системе обнаружен вредоносный файл, цель этих сотрудников – удалить его и как можно быстрее восстановить работоспособность зараженной системы. Это может означать «очистку» системы посредством удаления вредоносных файлов или стирания всех данных и восстановления операционной системы, данных и т. д. с незараженного носителя или из резервной копии. Кроме того, это также может означать замену компьютера целиком.

Самый важный фактор, влияющий на все это, связан с регулятивными органами. Штат Калифорния начал с закона SB-1386, требующего уведомлять любого жителя Калифорнии, если его личная информация (которая исчерпывающе определена и описана в тексте закона) была раскрыта в результате нарушения системы безопасности или вторжения в систему. На момент написания этой книги несколько других штатов приняли похожие законы, и, возможно, скоро будет принят федеральный закон США. Добавьте к этому стандарты Visa PCI, а также требования закона HIPAA, агентства SEC других регулятивных органов, и вы получите несколько дополнительных стимулов для того, чтобы составить надежный план расследования инцидентов. Во многих случаях регулятивные органы требуют, чтобы план расследования был задокументирован и прошел оценку на соответствие их стандартам. С другой стороны, цена за отсутствие

подробного плана расследования может включать в себя штрафы, а также различные расходы на уведомление пользователей и обнародование информации о нарушении системы безопасности и раскрытии конфиденциальных данных.

Лучший способ объяснить, как эти два фактора связаны между собой, – использовать пример. Инфраструктура компании была заражена вредоносной программой через браузер, в результате чего пришлось выполнить очистку приблизительно двух десятков систем. Во время начального расследования было обнаружено несколько признаков того, что в состав вредоносной программы, возможно, входит регистратор работы клавиатуры или какой-то сетевой компонент, однако точно ничего не определено (системы были очищены без проведения или документирования анализа первопричины). Когда, после того как все системы были очищены и снова введены в эксплуатацию, об этом узнал юрисконсульт компании, он задал вопрос: «Были ли раскрыты какие-либо конфиденциальные данные, находившиеся на зараженных системах?». Как могут ответить на него сотрудники ИТ-отдела? Ведь их задачей было очистить системы и вернуть их в эксплуатацию, чтобы поддержать работоспособность компании. Не было собрано никаких сведений, чтобы определить, находились ли конфиденциальные данные (личная информация, например, имена, адреса и номера социального страхования, или другие данные, например, номера кредитных карточек) в этих системах или были ли они раскрыты в результате заражения вредоносной программой.

Когда дело касается риска, регулятивные органы устанавливают, что если вы не можете точно определить, что данные не были каким-либо образом раскрыты, то должны сообщить обо всех данных, которые находились в этой системе или были ей доступны. Проще говоря, если вы не можете доказать, что конфиденциальные данные не были раскрыты, то должны уведомить всех, что их данные, возможно, были раскрыты. Этот пример совершенно ясно показывает, что расследование инцидента – это теперь не просто информационно-технологический процесс, а единый бизнес-процесс, в котором учувствуют юрисконсульты, сотрудники компании, отдел по связям с общественностью и даже высшее руководство.

Документация

Ключом к любым экспертизам или анализам, которые вы проводите, будет ваша документация. Документацию нужно вести таким образом, который позволил бы вам, или кому-то еще, вернуться к материалам позже (например, через 6 месяцев, один год или еще позднее) и понять или даже проверить результаты экспертизы. Это значит, что документация должна быть понятной, точной и достаточно подробной, чтобы показать полную картину того, что вы делали, что нашли, и как интерпретировали полученные данные.

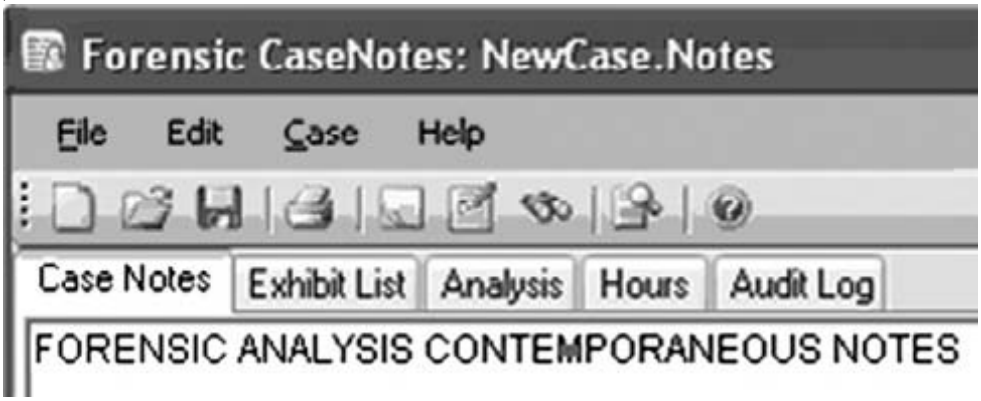
Документацию нужно вести любыми доступными средствами. Не нужно искать или приобретать специальное приложение, которое сохраняет документацию в собственном формате. Дело в том, что, возможно, через год вы не будете пользоваться этим приложением, или у человека, которому нужно просмотреть вашу документацию, возможно, нет этого приложения. Простого текстового редактора будет достаточно, но желательно иметь возможности форматирования текстового процессора, например, Microsoft Word. Используя текстовый процессор, можно вставить в документ ссылки и изображения, например, схемы расположения выводов накопителей, снимки экрана и даже ссылки на руководства по разборке ноутбуков (очень полезно, когда вам предоставляют ноутбук, который нужно разобрать, чтобы получить доступ к его НЖМД). Кроме того, многие форматы документов (такие как MS Word и Adobe PDF) текстового процессора можно просматривать и открывать на разных платформах. Бесплатный пакет OpenOffice (www.openoffice.org) предоставляет возможность работать с документами формата Microsoft Word даже в ОС Linux (и Windows). Говоря о форматах документов, нужно также не забывать о формате ваших отчетов. Используя тот же текстовый

процессор, можно записывать примечания к делу, а затем, когда вы будете готовы, можно вырезать и вставить их непосредственно в отчет. При составлении отчета, вам, возможно, не понадобится тот же уровень детализации, что присутствует в примечаниях к делу, но эту информацию можно легко перенести в отчет и изменить ее соответствующим образом.

Итак, что нужно документировать? Один из элементов, который мне нужно отслеживать как консультанту, – это часы, включаемые в счет клиенту за работу, выполненную во время экспертизы. Иногда я могу быть старшим экспертом в деле и отслеживать не только рабочие часы других специалистов, но и задачи, которые им ставят, а также результаты их расследований и сделанные ими затраты. Эту информацию можно очень легко, и в то же время понятно, записать, используя формат таблицы. Записывая эти данные в примечаниях к делу, вместе с результатами экспертизы, я смогу показать время, которое я потратил, если мне придется обосновывать эту информацию позднее. Кроме того, та же информация вводится в приложение для выставления счета непосредственно из примечаний к делу – между этими двумя документами не должно быть никаких расхождений. Это позволяет мне свести ошибки к минимуму, особенно в этой чрезвычайно важной области экспертизы.

В своей документации я также регистрирую, к каким данным я получал доступ с целью исследования, и какие носители содержат эти данные, т. е. внешние USB-накопители, встроенные НЖМД, CD- или DVD-диски и т. д. Я отслеживаю эту информацию по серийному номеру элемента, чтобы я мог ссылаться на этот элемент в течении всей экспертизы.

Полезный инструмент для отслеживания примечаний к делу – приложение Forensic CaseNotes от компании QCC Information Security (www.qccis.com/?section=casenotes). На илл. 8.1 показаны вкладки, которые я создал для регистрации всей упомянутой выше информации.



Илл. 8.1. Вкладки в приложении Forensic CaseNotes.

Независимо от того, какое приложение вы выбрали для создания примечаний к делу, примечания должны быть доступны, точны и наглядно показывать ваши действия во время экспертизы и результаты экспертизы, чтобы эти действия можно было проверить и подтвердить при необходимости.

Инструменты и ловушки…

Подтверждение анализа

В примечания к делу я люблю включать любую документацию, подтверждающую мою цепь рассуждений. Иногда я добавляю примечания, опираясь на проверку теории, но я также получил университетское образование, а один из принципов, которому я научился во время написания диссертации, состоит в том, что необходимо подтверждать то, что пишешь. Не сложно делать утверждение, когда знаешь о чем-то, но добавляя похожие утверждения, высказанные другими, вы делаете свой анализ более достоверным. Отличный источник для такой подтверждающей документации при анализе

операционных систем Windows – это база знаний Microsoft. Часто поиск по самой базе знаний Microsoft, или даже в Google, предоставит вам ссылки на ценную информацию, которая может ответить на ваши вопросы и подтвердить результаты анализа. Кроме того, к статьям из базы знаний Microsoft можно перейти через другие сайты, например, через Eventid.net.

Одна из статей базы знаний, которую я использую довольно часто, называется «Description of Ntfs date and time stamps for files and folders» (http://support.microsoft.com/?kbid=299648). В ней описывается, как на отметки времени MAC (изменения, доступа и создания) влияют операции копирования и перемещения между файловыми системами и в файловых системах (а именно FAT и NTFS). В других статьях базы знаний описываются коды состояний веб-сервера IIS, которые отображаются в журналах веб-сервера, объясняется, как хранятся файлы в корзине ОС Windows XP и 2003, и т. д. В базе знаний существует множество статей, которые могут подтвердить достоверность результатов анализа, а ссылки на эти статьи можно легко добавить в примечания к делу или в отчеты.

Цели

Много лет тому назад я обсуждал экспертизу, проведенную другим специалистом из другой организации, с одним из сотрудников службы безопасности нашей компании. Специалист-консультант обнаружила троян SubSeven в созданном образе данных, что было одной из задач, которые она должна была выполнить по контракту (т. е. определить, были ли установлены вредоносные программы в системе); однако мой коллега заметил, что она не определила скрытый DOS-раздел. Почему? Потому что это не было целью ее экспертизы. Когда я разговаривал с консультантом, она сказала, что на самом деле заметила скрытый раздел при подготовке к исследованию образа, и даже написала об этом в своих примечаниях к экспертизе. Однако это был не тот вопрос, на который ей надо было ответить согласно контракту, он не имел отношения к экспертизе, и, следовательно, об этом не было указано в итоговом отчете.

Важно, чтобы все эксперты помнили об этом, независимо от того, работают ли они консультантом или в правоохранительных органах. Можно погрязнуть в бесконечных поисках «подозрительных действий» и никогда их не закончить, если у вас нет (или вы не придерживаетесь) четко определенных целей экспертизы.

Когда вы знаете, что вы должны или что вам нужно искать, вы также получаете отправную точку для вашей экспертизы. Инцидент связан с заражением вредоносной программой или с вторжением? Является ли целью экспертизы определить мошенничество или нарушение пользователем правил использования сети? Если вы понимаете, что вы должны искать, вы сможете легче определить, с чего начинать поиск.

Мой друг рассказывал мне, как однажды просматривал отчет, касающийся случая заражения вредоносной программой. Собрав данные и завершив анализ, эксперт написал отчет, включающий в себя исчерпывающий трактат, объемом около двадцати страниц, о возможностях вредоносной программы. Мой друг сказал, что, дочитав отчет до конца, он вынужден был спросить у эксперта, была ли вредоносная программа на самом деле обнаружена в образе данных системы. Ведь клиент платит именно за ответ на этот вопрос, а в отчете, охватывающем почти три десятка страниц, не было ясно сформулировано, найдена ли вредоносная программа в образе данных.

Компьютерно-техническая экспертиза может быть дорогостоящей задачей, поэтому ее цели нужно четко определять с самого начала. Эксперт может потратить много времени на исследование образа данных, а команда специалистов может потратить еще больше на прочесывание множества систем в сетевой инфраструктуре, если единственная задача, которую им поставили, – найти все, что связано с вредоносными действиями. Четко определенные цели помогут сфокусировать подход к анализу, разработать план

расследования или анализа, а также обозначить конечный этап экспертизы. Цели анализа необходимо сформулировать, понять и подробно задокументировать.

Контрольные списки

Отличный способ начать анализ – использовать контрольные списки. Контрольный список в общих чертах обозначает задачи, которые требуется выполнить. Правильно составленный контрольный список содержит больше пунктов, чем нужно (так как он предназначен для того, чтобы быть исчерпывающим), и экспертам необходимо обосновывать и подтверждать причины, по которым пропускаются определенные пункты списка или не выполняются определенные действия.

Контрольные списки не должны быть сложными. Контрольный список может содержать задачи, которые выполняются во время каждой экспертизы, например, монтирование образа как накопителя в режиме только для чтения на испытательном компьютере и проверка образа при помощи антивирусных (см. главу 5) и антишпионских приложений. Можно также включить в список загрузку образа и проверку «работающей» системы при помощи средств обнаружения руткитов (см. главу 7). Можно добавить в список поиск номеров кредитных карт, номеров социального страхования и других конфиденциальных данных или поиск электронной почты (веб-почты и т. д.) и журналов чатов в зависимости от типа проводимой экспертизы.

Один из примеров контрольного списка – перечень задач, связанных с документированием информации о каждом анализируемом образе. Например, возможно, вы захотите задокументировать такие сведения, как имя компьютера, время последнего завершения работы системы и другую извлеченную из образа исходную информацию, которая может иметь отношение к экспертизе. Некоторые параметры, такие как отключение обновления времени последнего доступа, настройки для удаления файлов в системе в обход корзины или для очистки файла подкачки при завершении работы в системе, могут иметь значительное влияние на остальную часть анализа.

Еще один пример контрольного списка – перечень действий, которые нужно выполнить, если предполагается, что в системе присутствует вредоносная программа. Этот список может быть простым и состоять из таких задач, как монтирование образа при помощи SmartMount и проверка образа одним антивирусным приложением, или же он может быть более основательным и включать в себя проверку образа с использованием нескольких антивирусных и антишпионских приложений (с документированием сведений об их версиях), а также ряд других действий. К таким действиям может относиться загрузка образа при помощи LiveView и выполнение проверок на наличие руткитов. Когда я выполняю антивирусную проверку образа данных, я в первую очередь, как правило, просматриваю образ, чтобы определить, было ли установлено на накопителе какое-нибудь антивирусное приложение, и, если было, выясняю его название и версию. Затем я могу просмотреть журналы этого приложения, чтобы узнать, была ли обнаружена вредоносная программа, и, если была, то когда это произошло, и какие действия были предприняты приложением (перемещение в карантин, попытка перемещения в карантин, закончившаяся неудачно, и т. д.). Кроме того, я обычно просматриваю журналы регистрации событий, чтобы определить, были ли отправлены уведомления, например, о том, что обнаружена вредоносная программа или что работа антивирусного приложения была аварийно завершена (известная тактика некоторых вредоносных программ). Также есть файл «mrt.log» (см. главу 5), который позволяет мне узнать о том, какие механизмы защиты были задействованы в системе во время обновлений Windows.

Каким бы точным и обширным не был контрольный список, он должен содержать достаточное количество этапов документирования, чтобы другой эксперт мог при необходимости повторить и подтвердить ваши действия.

Контрольные списки не должны быть пошаговым руководством по проведению экспертизы. Контрольный список следует рассматривать как начальный этап экспертизы,

как способ, позволяющий удостовериться в том, что отдельные задачи выполнены (или по меньшей мере задокументированы причины, по которым они не выполнены). Контрольный список позволяет вам убедиться, что вы предусмотрели все основные действия или большинство из них, и повторить те действия, которые нужно повторять во время каждой экспертизы, не беспокоясь о том, что вы забудете о какой-либо операции. Как и ваши приложения и утилиты для анализа, контрольные списки – это инструменты, которые можно использовать с пользой для себя. Контрольные списки – это процесс, а когда у вас есть процесс, у вас есть что-то, что вы можете улучшить (и наоборот, если вы не помните, что делали в течение последней экспертизы, как вы можете усовершенствовать свои действия?).

Примерный контрольный список с именем «Incident Analysis Checklist.doc» находится на носителе, который идет в комплекте с этой книгой. Этот список представляет собой простой документ Word, содержащий некоторые из тех же полей, которое обозначены вкладками, показанными на илл. 8.1. Он включает в себя несколько основных полей, в которых указываются сведения об инциденте и эксперте, а также даты начала и окончания экспертизы. Кроме того, он содержит таблицы для элементов, которые будут проанализированы (образы данных, перехваченный сетевой трафик, файлы журналов и т. д.), и кнопки-флажки для выбора основных целей экспертизы и действий, которые можно использовать во время анализа. Этот раздел может включать в себя задачи, которые являются частью стандартных процедур в вашей организации, например, определение операционной системы в образе данных, определение учетных записей пользователей в этой системе, извлечение данных из реестра, проверка на наличие вредоносных программ и т. д. Несмотря на то, что этот контрольный список состоит только из одной страницы, эксперт может добавлять дополнительные страницы в процессе проведения анализа и записывать результаты непосредственно в список. Не забывайте, что данный контрольный список является только примером, и его можно расширить или изменить в соответствии с вашими конкретными требованиями.

Инструменты и ловушки…

Какая версия Windows?

Часто при исследовании работающего компьютера или анализе образа данных мне нужно знать, с какой версией Windows я работаю. Судя по тому, что я вижу на общедоступных форумах, это не проблема для специалистов или экспертов, но я провел множество исследований работающих компьютеров и судебных экспертиз и знаю, что те различия между версиями Windows, которые многие считают незначительными, могут в действительности быть довольно существенными. Из главы 3 вы узнали, что основные структуры ядра (т. е. структуры EProcess и EThread) могут отличаться друг от друга не только в зависимости от версий Windows, но и в зависимости от пакетов обновлений в одной и той же версии! С точки зрения судебного анализа, в некоторых версиях Windows имеются артефакты, которых нет в других версиях; известный пример – точки восстановления системы, которые есть в Windows XP, но отсутствуют в Windows 2000 или Windows 2003.

Возможно, самый распространенный способ для определения версии операционной системы Windows, с которой вы работаете, – проверка содержимого нескольких разделов реестра. В разделе Microsoft\Windows NT\CurrentVersion куста Software вы найдете такие параметры, как CSDVersion, BuildLab и ProductID, которые можно использовать для определения версии ОС Windows. Статья № 189249 (http://support.microsoft.com/kb/189249) из базы знаний Microsoft предоставляет информацию для определения версии работающей системы программными средствами, а также дает представление о том, как сделать то же самое во время экспертизы.

Еще один способ определить версию – найти файл «ntoskrnl.exe» в каталоге «system32» и проанализировать информацию о версии из этого исполняемого файла. Этот

способ также работает с такими файлами, как «cmd.exe» и «winver.exe» (обратите внимание, что при выполнении «winver.exe» из командной строки откроется диалоговое окно «О программе Windows» (“About Windows”), в котором показана основная информация об операционной системе, в том числе версия системы и объем физической памяти).

Наконец, если вы работаете с ОС Windows XP и хотите определить ее версию (Home или Professional Edition), найдите файл «prodspec.ini» в каталоге «system32» и перейдите к разделу «[Product Specification]». В своей системе я увидел строку «Product=Windows XP Professional».

Если вы знаете, какую версию ОС Windows вы исследуете, это поможет вам определить, какие артефакты искать, где их искать, и какие артефакты отсутствуют там, где они должны быть. Все это может существенно повлиять на результаты экспертизы.

Что дальше?

Теперь, когда вы начали документирование, понимаете цели и составили контрольный список действий – что дальше? Что происходит дальше? На этом этапе начинается фактический анализ. Предположим, что вы анализируете образ данных, созданный из ОС Windows, и, задокументировав сведения о клонировании, операционной системе и учетных записях пользователей в системе, вам нужно выполнить несколько других задач анализа как часть стандартного этапа обработки данных дела, например, поиск по ключевым словам и проверку на наличие вредоносных программ. Если список ключевых слов относительно короткий, добавьте его непосредственно в документацию по анализу и выполните поиск. Или, если вы решили не выполнять поиск, укажите причину этого. Также укажите, какие приложения использовались для проверки на наличие вредоносных программ, или объясните, почему проверка не была проведена.

Поиск в Google по словам «digital forensic analysis checklists» (рус. *контрольные списки для компьютерно-технической экспертизы*) предоставит вам разнообразные подходы, используемые для создания этих списков. Некоторые списки включают в себя такие задачи, как сигнатурный анализ, выявление графических изображений (в том числе фильмов и фотографий), анализ истории просмотра веб-страниц, анализ корзины и файлов ярлыков (.lnk) Windows и т. д. Все эти операции могут быть необходимы для вашей экспертизы или быть частью стандартных процедур по обработке данных дела в вашей организации. В любом случае ваши действия во время анализа должны быть тщательно и точно задокументированы, особенно если вы начнете действовать не по плану и проводить анализ нестандартно (некоторые могут назвать это вдохновением). Документирование действий, совершенных по вдохновению, расширит ваши знания, а также позволит вам вернуться к материалам дела позднее и при необходимости повторить эти действия.

Расширенный анализ временной шкалы

Как обсуждалось в главе 5, информация временной шкалы, которую эксперт получает в результате использования инструмента ***fls*** и скрипта «mactime.pl», ограничена только файлами и каталогами из образа данных и не учитывает другие события или артефакты в образе, также содержащие информацию с отметками времени. Частично чтобы решить эту проблему, Майкл Клопперт (Michael Cloppert) разработал инструмент Ex-Tip, доступный на сайте Sourceforge (http://sourceforge.net/projects/ex-tip/). Кроме того, на сайте SANS есть статья Майка о разработке и применении инструмента Ex-Tip (https://www2.sans.org/reading_room/whitepapers/forensics/32767.php). Ex-Tip учитывает дополнительные источники данных с отметками времени, такие как разделы реестра и журналы антивирусных приложений, анализирует эти данные, приводит их к одному

общему формату времени (время Unix) и предоставляет их в несколько ином, но тем не менее текстовом формате.

Такие инструменты и служебные программы, как например RegRipper (подробно рассмотренная в главе 4), могут предоставить дополнительные функциональные возможности для извлечения значений с отметками времени из файлов кустов реестра. Тогда как модуль, используемый с Ex-Tip, извлекает все разделы и их отметки времени *LastWrite* из файла куста, RegRipper работает более тонко и извлекает только интересующие вас разделы, сокращая объем обрабатываемых данных (чтобы не заваливать эксперта результатами) и предоставляя контекст к найденным данным. Например, как упоминалось в главе 4, в разделе RecentDocs и его подразделах содержатся списки недавно использованных файлов, и последний открывавшийся файл относительно легко определяется в параметре MRUList (или MRUListEx). Поэтому подключаемые модули программы RegRipper могут предоставить не только отметку времени *LastWrite* раздела, но и имя последнего открывавшегося файла. Более того, такие параметры реестра, как те, что находятся в разделах UserAssist, содержат данные с отметками времени, и их можно извлечь с помощью соответствующего подключаемого модуля и вставить в промежуточный файл в соответствующем формате.

Другие файлы можно также проанализировать на наличие данных с отметками времени. Например, как обсуждалось в главе 5, журналы регистрации событий Windows содержат отметки времени создания и сохранения для каждой записи о событии. Файлы «rp.log» в точках восстановления системы в Windows XP содержат информацию не только о времени создания точки восстановления, но и о причине (контрольная точка системы, установка драйвера и т. д.) создания такой точки. Эта информация добавляет контекст к имеющимся данным, и ее можно сопоставить с информацией, полученной из выходных данных инструмента «fls.exe». Есть также файлы журналов антивирусных приложений и некоторые другие файлы, содержащие информацию, которую можно (и, возможно, нужно) включить в анализ временной шкалы. К дополнительным источникам информации могут относиться события, введенные вручную, например, создание файлов аварийного дампа памяти и т. д.

Как упоминается в статье Майкла, существует несколько средств для анализа доступных данных с отметками времени (после того как данные приведены к общему формату времени и предварительно обработаны) и представления этих данных в понятном и наглядном формате. Например, два таких средства – это Zeitline (http://projects.cerias.purdue.edu/forensics/timeline.php) и EasyTimeline (http://en.wikipedia.org/wiki/Wikipedia:EasyTimeline). Инструмент Zeitline основан на компонентах Swing языка Java, и, по всей видимости, он не обновлялся с 2006 г. Инструмент EasyTimeline предлагает графический подход к представлению данных с отметками времени. Другой инструмент с богатыми функциональными возможностями – это Simile Timeline, который первоначально был доступен на сайте Массачусетского технологического института, а теперь предлагается как виджет Google (http://www.simile-widgets.org/timeline/). Simile Timeline имеет возможность не только отображать события, происходившие в определенный момент времени (например, время последнего доступа к файлу) и период времени (например, антивирусная проверка), но и показывать данные с отметками времени на отдельных, расположенных рядом полосах, чтобы информация была разделена, но при просмотре сопоставлялась с другими данными.

Одним из аспектов использования текстового выходного формата или одного из вышеупомянутых графических выходных форматов может быть изменение способа, с помощью которого эксперты определяют события, например, посредством выходных данных утилиты «fls.exe».

Краткое изложение

Многие эксперты считают, что недостаточно исследовать только часть образа данных, например, файловую систему, чтобы сделать вывод по экспертизе или делу. Они используют данные из реестра, файлы, найденные в файловой системе, и даже дампы памяти и перехваченные сетевые пакеты, чтобы составить полную картину инцидента. В конце концов зачем основывать выводы на одном виде данных, когда можно связать между собой несколько разных элементов данных, чтобы подтвердить результаты экспертизы? Однако, независимо от того, какое количество данных вы используете, ключом к этим данным будет ваша документация.

Быстрое повторение

Изучение конкретных примеров

- Изучение конкретных примеров – отличный способ показать, как можно объединить на первый взгляд несопоставимые элементы информации и способы анализа в единую структуру, чтобы получить более качественное представление об анализе. Многим людям нравится видеть то, что сделали другие, и во многих случаях это заставит читателей обдумать то, что они увидели, проверить свои собственные способы анализа или даже усовершенствовать существующие методики.

Начало работы

- Имейте в виду, что во время анализа самое главное – придерживаться поставленных целей (вполне вероятно, что отклонение от плана или целей может замедлить анализ), а также кратко документировать все свои действия.

Расширенный анализ временной шкалы

- Представление имеющихся данных в формате временной шкалы может быть чрезвычайно мощным инструментом для эксперта.
- Разнообразные источники данных в исследуемом образе могут содержать ценную информацию с отметками времени, в том числе содержимое файлов журналов, разделы и параметры реестра и содержимое Корзины.

Часто задаваемые вопросы

Вопрос: Я провожу экспертизу, в которой мне нужно определить, когда пользователь входил в систему, однако первоначальный анализ показал, что аудит событий входа в систему не включен, и я не вижу признаков этих событий в журналах событий безопасности. Как мне определить, когда пользователь входил в систему?

Ответ: В операционной системе Windows есть несколько источников информации, которые позволяют определить, когда учетная запись пользователя использовалась для входа в систему. Анализ файла куста «SAM» позволит вам получить время последнего входа в систему для пользователя, а время последнего изменения файла «NTUSER.DAT» в профиле пользователя будет свидетельствовать о том, когда пользователь последний раз выходил из системы. Анализ пользовательского файла «NTUSER.DAT», в частности разделов UserAssist и RecentDocs, предоставит вам большое количество информации о действиях пользователя. Отметки времени *LastWrite* в разделах, используемых для хранения списков недавно использованных файлов, могут также быть очень полезны. Так как файл «NTUSER.DAT» содержит множество данных о взаимодействии пользователя с оболочкой Windows, в нем можно найти большое количество информации с отметками

времени. Кроме того, анализ той же информации из соответствующих файлов кустов в точках восстановления системы в Windows XP покажет вам хронологическую последовательность данных. Данный способ анализа, в котором применяется сочетание анализа файловой системы и реестра, позволит вам получить более полную картину о действиях пользователя в системе.

Вопрос: Во время расследования инцидента я собрал сетевой трафик, а также энергозависимые данные из системы, которая, как я предполагаю, заражена. Как мне сопоставить эти два вида данных и связать их вместе?
Ответ: Сетевой трафик содержит два важных элемента информации, которые можно использовать для связывания этих данных с отдельной системой, – исходный или целевой IP-адрес и порт. IP-адрес позволит вам связать трафик с отдельной системой (можно также использовать MAC-адрес в Ethernet-кадрах).

Содержание

http://computer-forensics-lab.org

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