Внедрение в компьютеры вредоносных программ

БГА, РТФ
Кафедра ИБ

Зензин Александр Степанович, к.т.н.

Обзор

1. Внедрение в компьютеры вредоносных программ
2. Троянские программы
3. Сетевые черви
4. Вирусы.
5. Шпионские программы
6. Спам
7. Дополнительные материалы для изучения

Внедрение в компьютеры вредоносных программ

Многочисленная группа атак связана с внедрением в компьютеры вредоносных программ (malware), к числу которых относятся троянские и шпионские программы, черви, вирусы, спам, логические бомбы и некоторые другие типы программ, нацеленные на нарушение информационной безопасности.

Эти программы могут проникать на атакуемые компьютеры разными путями. Самый простой из них — «самодоставка», когда пользователь загружает файлы из непроверенных источников (съемных носителей или веб-сайтов) либо беспечно открывает подозрительный файл, пришедший к нему по электронной почте. Существуют и более сложные представители вредоносных программ, обладающие собственными механизмами «размножения», копии таких программ распространяются по компьютерам сети без участия пользователей.

Ущерб, наносимый вредоносными программами, может выражаться не только в уничтожении, искажении или похищении информации, приведении в нерабочее состояние программного обеспечения, а значит, и компьютера в целом, но и в значительных затратах времени и сил администраторов на обнаружение и распознавание атак, фильтрацию внешних сообщений, тестирование и перезагрузку систем. Вредоносные программы в начале этого десятилетия были одной из основных причин нарушения безопасности компьютерных сетей. В последние годы суммарный ущерб, нанесенный вредоносными программами предприятиям, резко снизился. Это связывают, в том числе, с улучшением качества антивирусных средств и ужесточением наказаний за такого рода преступления.

На практике злоумышленники часто сочетают в одной и той же программе различные типы угроз. Например, некоторые черви способны маскироваться под троянские программы или подобно вирусам заражать исполняемые файлы на локальном диске, а некоторые вирусы наделены способностями червей самокопироваться на другие компьютеры. Кроме того, можно встретить и другую классификацию вредоносных программ, где, скажем, троянские программы и черви рассматриваются как разновидности вирусов.

Троянские программы

Троянские программы, или трояны (trojan), — это разновидность вредоносных программ, которые наносят ущерб системе, маскируясь под какие-либо полезные приложения.

Троянские программы могут применять в качестве прикрытия знакомые пользователю приложения, с которыми он работал и раньше, до появления в компьютере «троянского коня». При другом подходе в полном соответствии с древней легендой троянская программа принимает вид нового приложения, которое пытается заинтересовать пользователя-жертву какими-то своими якобы полезными функциями.

Однако суть троянской программы и в том и в другом случаях остается вредительской: она может уничтожать или искажать информацию на диске, передавать данные (например, пароли) с «зараженного» компьютера на удаленный компьютер хакера, приводить в неработоспособное состояние установленное на атакованном компьютере программное обеспечение, участвовать в проведении DoS-атак на другие удаленные компьютеры. Так, одна из известных троянских программ AIDS TROJAN DISK7, разосланная нескольким тысячам исследовательских организаций на дискете, при запуске перемешивала символы в именах всех файлов и заполняла все свободное пространство жесткого диска. После этого программа от имени злоумышленника предлагала помощь в восстановлении диска, требуя взамен вознаграждение для автора этой программы. (Злоумышленники могут также шантажировать пользователя, зашифровывая его данные.) Кстати, описанное компьютерное преступление завершилось поимкой хакера-шантажиста.

Троянские программы могут быть отнесены к самому простому по реализации виду вредоносных программ.

Сетевые черви

Сетевые черви (worm) — это программы, способные к самостоятельному распространению своих копий среди узлов в пределах локальной сети, а также по глобальным связям, перемещаясь от одного компьютера к другому без всякого участия в этом процессе пользователей сети.

Поскольку большинство сетевых червей передаются в виде файлов, основным механизмом их распространения являются сетевые службы, основанные на файловом обмене. Так, червь может рассылать свои копии по сети в виде вложений в сообщения электронной почты или путем размещения ссылок на зараженный файл на каком-либо веб-сайте. Однако существуют и другие разновидности червей, которые для своей экспансии используют более сложные приемы, например, связанные с ошибками («дырами») в программном обеспечении.

Главная цель и результат деятельности червя состоит в том, чтобы передать свою копию на максимально возможное число компьютеров. При этом для поиска компьютеров — новых потенциальных жертв — черви задействуют встроенные в них средства. Типичная программа-червь не удаляет и не искажает пользовательские и системные файлы, не перехватывает электронную почту пользователей, не портит содержимое баз данных, а наносит вред атакованным компьютерам путем потребления их ресурсов. Если червь обладает возможностью повторного заражения, то число его копий растет лавинообразно, и вредоносные программы все более и более загружают процессор, захватывая новые области памяти, отбирая пропускную способность сетевых соединений, пока, наконец, программы легальных пользователей не потеряют возможность выполняться.

Сетевые черви

При создании типичного сетевого червя хакер, прежде всего, определяет перечень сетевых уязвимостей, которые он собирается использовать для проведения атак средствами создаваемого червя. Такими уязвимостями могут быть как известные, но не исправленные на некоторых компьютерах ошибки в программном обеспечении, так и пока неизвестные никому ошибки, которые обнаружил сам хакер. Чем шире перечень уязвимостей и чем более они распространены, тем больше узлов может быть поражено данным червем.

Червь состоит из двух основных функциональных компонентов: атакующего блока и блока поиска целей.

- Атакующий блок состоит из нескольких модулей (векторов атаки), каждый из которых рассчитан на поражение конкретного типа уязвимости. Этот блок открывает «входную дверь» атакуемого хоста и передает через нее свою копию.
- Блок поиска целей (локатор) собирает информацию об узлах сети, а затем на основании этой информации определяет, какие из исследованных узлов обладают теми уязвимостями, для которых хакер имеет средства атаки.

Эти два функциональных блока являются обязательными и присутствуют в реализации любой программы-червя. Некоторые черви нагружены их создателями и другими вспомогательными функциями, которые обсуждаются позже.

Упрощенно жизненный цикл червя может быть описан рекурсивной процедурой, состоящей из циклического запуска локатора и атакующего блока на каждом из последующих заражаемых компьютеров (рис. 1).

Сетевые черви

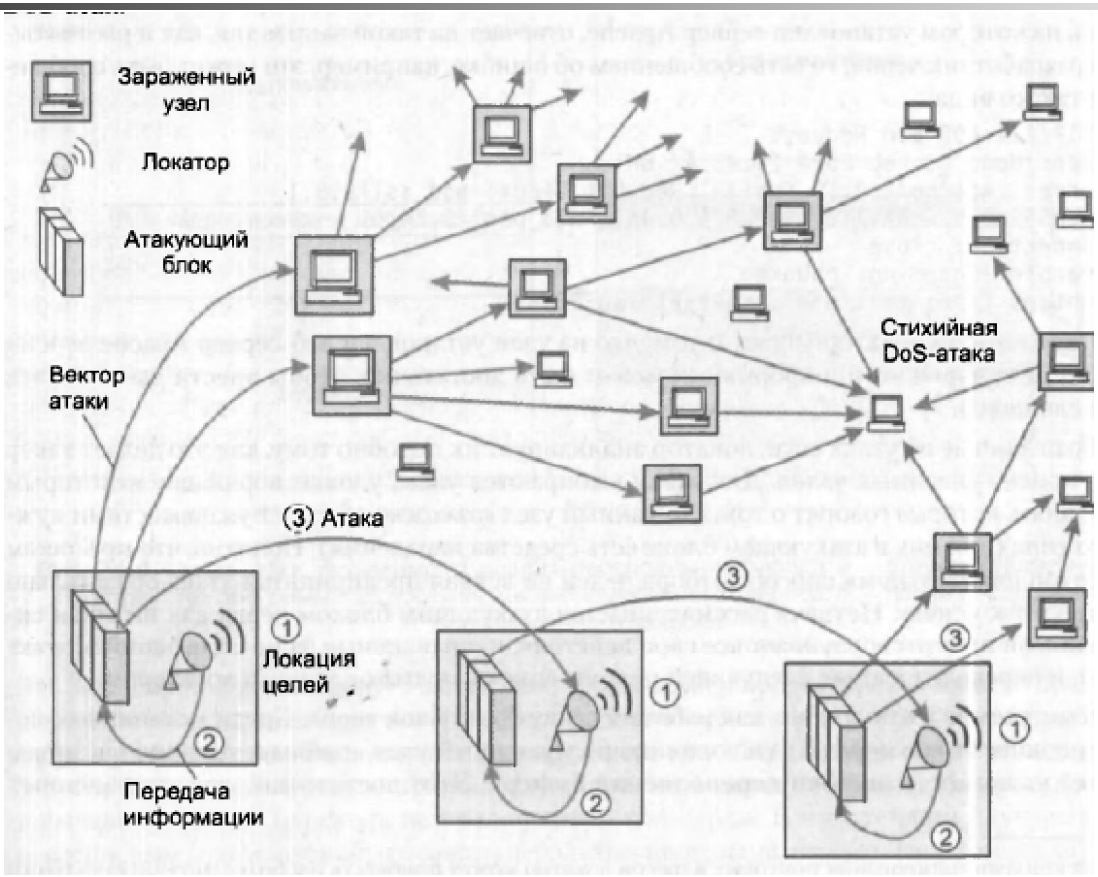


Рис. 1 Экспансия червя в сети

В начале каждого нового цикла червь, базирующийся на захваченном в результате предыдущей атаки компьютере, запускает локатор для поиска и формирования списка узлов-целей, пригодных для проведения каждой из специфических атак, а затем, используя средства атакующего блока, пытается эксплуатировать уязвимости узлов из этого списка. В результате успешной атаки червь копирует все свои программы на «новую территорию» и активирует локатор. После этого начинается новый цикл.

Сетевые черви

На рисунке показано, как червь лавинообразно распространяется по сети. Заражение тысяч компьютеров может занять всего несколько минут. Некоторые виды червей не нападают на уже зараженные и/или подвергающиеся атаке в данный момент узлы. Если же такая проверка не предусмотрена в алгоритме работы червя, то в сети случайным образом могут возникать очаги стихийных DoS-атак.

Локатор идентифицирует цели по адресам электронной почты, IP-адресам, характеристикам установленных на хостах операционных систем, номерам портов, типам и версиям приложений.

Для сбора информации локатор может предпринимать действия, связанные как с поисками интересующих данных на захваченном им в данный момент хосте, так и путем зондирования сетевого окружения. Простейший способ получить данные локально — прочитать файл, содержащий адресную книгу клиента электронной почты. Помимо почтовых адресов, локатор может найти на узле базирования другие источники информации, такие как таблицы конфигурационных параметров сетевых интерфейсов, ARP-таблицы и таблицы маршрутизации. Зная IP-адреса хоста базирования и шлюзов, локатор достаточно просто может определить IP-адреса других узлов этой сети. Для идентификации узлов локатор может также использовать ICMP-сообщения или запросы ping, указывая в качестве адресов назначения все возможные IP-адреса. Для определения того, какие приложения работают на том или ином хосте, локатор сканирует различные *хорошо известные* номера TCP- и UDP-портов. Определив тип приложения, локатор пытается получить более детальные характеристики этого приложения.

Сетевые черви

Например, пусть некоторая программа-червь имеет в своем арсенале средства для атаки на некоторые версии веб-сервера Apache. Для поиска потенциальных жертв локатор этого червя зондирует узлы сети, посылая умышленно ошибочные запросы к веб-серверу:

GET / HTTP/1.1\r\n\r\n

Узел, на котором установлен сервер Apache, отвечает на такой запрос так, как и рассчитывал разработчик червя, то есть сообщением об ошибке, например, это может быть сообщение такого вида:

HTTP/1.1 400 Bad Request
Date: Mon, 23 Feb 2004 23:43:42 GMT
Server: Apache/1.3.19 (UNIX) (Red-Hat/Linux) mod_ssl/2.8.1
OpenSSL/0.9.6 DAV/1.0.2 PHP/4.0.4pll mod_perl/1.24_01
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

Из этого ответа локатор узнает о том, что на узле установлен веб-сервер Apache версии 1.3.19. Для червя этой информации может быть достаточно, чтобы внести данный узел в число целей.

Собрав данные об узлах сети, локатор анализирует их подобно тому, как это делает хакер при поиске уязвимых узлов. Для атаки выбираются узлы, удовлетворяющие некоторым условиям, которые говорят о том, что данный узел возможно обладает уязвимостями нужного типа (для них в атакующем блоке есть средства нападения). Понятно, что при таком «предположительном» способе отбора целей не всякая предпринятая атака обязательно приводит к успеху. Неудача рассматривается атакующим блоком червя как штатная ситуация, он просто сворачивает все свои действия и переходит к атаке следующей цели из списка, подготовленного локатором.

Сетевые черви

Рассмотрим более подробно, как работает атакующий блок червя. Среди механизмов, позволяющих червю передать свою копию на удаленный узел, наиболее длинную историю имеет уязвимость ошибки переполнения буфера. Этот достаточно распространенный вид уязвимости связан с неправильной работой некоторых программ, когда у них переполняется буфер.

При трансляции программ, написанных на многих языках программирования, в исполняемом (объектном) модуле в сегменте локальных переменных отводится место для буферов, в которые будут загружаться данные при выполнении процедур ввода. Например, в программе веб-сервера должен быть предусмотрен буфер для размещения запросов, поступающих от клиентов. Причем размер буфера должен быть равен максимально допустимой для данного протокола длине запроса. В том же сегменте локальных переменных транслятор размещает команду возврата из процедуры, которой будет передано управление при завершении процедуры (рис. 2, а).

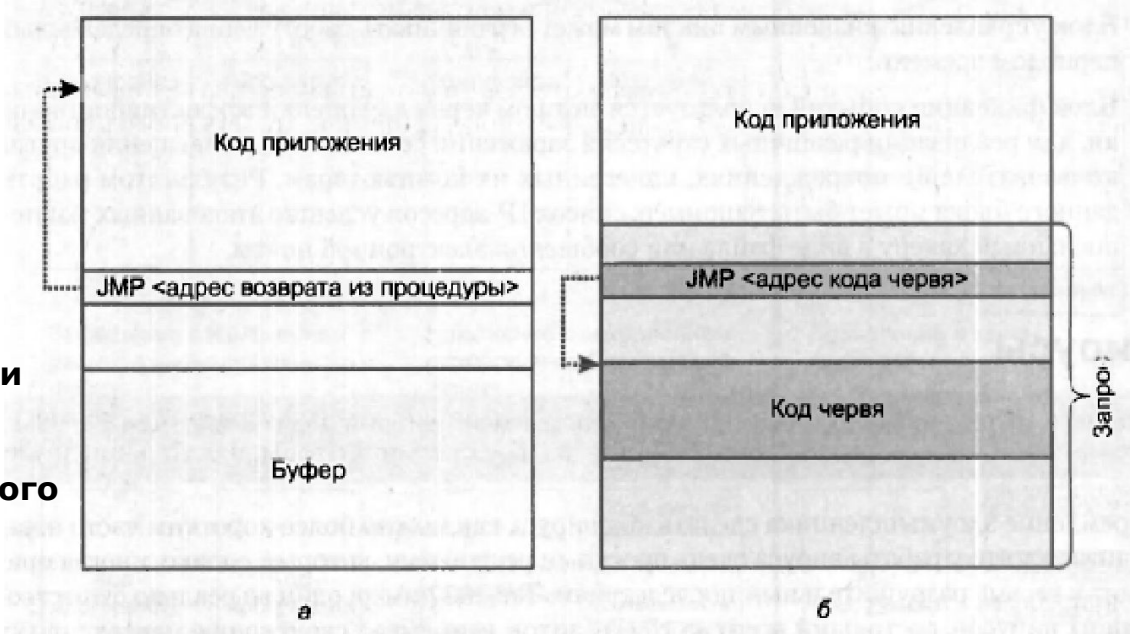


Рис. 2. Схема атаки на уязвимость ошибки переполнения буфера:
а — структура адресного пространства программы до поступления злонамеренного запроса;
б — после поступления злонамеренного запроса

Сетевые черви

Для правильной работы программы очень важно, чтобы вводимые данные (в нашем примере — запрос клиента) всегда укладывались в границы отведенного для них буфера. В противном случае эти данные записываются поверх команды возврата из процедуры. А это, в свою очередь, означает, что процедура не сможет завершиться корректно: при передаче управления на адрес команды возврата процессор будет интерпретировать в качестве команды то значение из запроса, которое записано поверх команды возврата. Если такого рода переполнение возникло в результате случайной ошибки, то маловероятно, что значение, записанное поверх команды возврата, окажется каким-либо осмысленным кодом. Иное дело, если это переполнение было специально инициировано злоумышленником.

Злоумышленник конструирует запрос так, чтобы сервер прореагировал на него предсказуемым и желательным для хакера образом. Для этого хакер посылает нестандартный запрос, размер которого превышает размер буфера (рис. 2, б). При этом среди данных запроса в том месте, которое приходится как раз на команду возврата, злоумышленник помещает команду перехода на вредоносный код червя. В простейшем случае таким вредоносным кодом может быть совсем небольшая программа, переданная в том же запросе.

Итак, атакующий блок червя посылает некорректный запрос уязвимому серверу, его буфер переполняется, код команды возврата из процедуры замещается кодом команды передачи управления вредоносной программе, которая выполняет копирование всех оставшихся программных модулей червя на вновь освоенную территорию.

Сетевые черви

Хотя рассмотренный подход применим к самым различным приложениям, для каждого типа приложений хакер должен сформировать специальный атакующий запрос, в котором смещение кода команды передачи управления вредоносной программе точно соответствовало бы местоположению команды возврата в процедуру атакуемого приложения. Именно поэтому для червя при проведении такого вида атак так важно получить информацию о типе и версиях программного обеспечения, установленного на узлах сети.

Помимо локатора и атакующего блока червь может включать некоторые дополнительные функциональные компоненты.

- **Блок удаленного управления и коммуникаций** служит для передачи сетевым червям команд от их создателя, а также для взаимодействия червей между собой. Такая возможность позволяет хакеру координировать работу червей для организации распределенных атак отказа в обслуживании. Сетевые черви могут быть также использованы для организации параллельных вычислений при решении таких требующих большого объема вычислений задач, как, например, подбор секретного ключа шифрования или пароля.
- **Блок управления жизненным циклом** может ограничивать работу червя определенным периодом времени.
- **Блок фиксации событий** используется автором червя для оценки эффективности атаки, для реализации различных стратегий заражения сети или для оповещения других пользователей о повреждениях, нанесенных их компьютерам. Результатом работы данного блока может быть, например, список IP-адресов успешно атакованных машин, посланный хакеру в виде файла или сообщения электронной почты.

Вирусы

Вирус (virus) — это вредоносный программный фрагмент, который может внедряться в другие файлы.

Стремление злоумышленника сделать код вируса как можно более коротким часто ограничивает логику работы вируса очень простыми решениями, которые, однако, иногда приводят к весьма разрушительным последствиям. Так, например, один из реально существовавших вирусов, состоящий всего из 15 (!) байтов, записывал свою копию поверх других файлов в начало каждого сектора диска, в результате система очень быстро терпела крах. Некоторым утешением в таком и подобных ему случаях является то, что одновременно с крахом компьютера прекращает свое существование и вирус.

Вирус может внедрять свои фрагменты в разные типы файлов, в том числе в файлы исполняемых программ (рис. 1). При этом возможны самые разные варианты: замещение кода, когда размер инфицированного файла не меняется, вставка вирусного кода целиком в начало или конец исходной программы, замена фрагментов программного кода фрагментами вируса с перестановкой замещенных фрагментов и без перестановки и т. д., и т. п. Более того, код вируса может быть зашифрован, чтобы затруднить его обнаружение антивирусными программами.

В отличие от червей вирусы (так же как и троянские программы) не содержат в себе встроенного механизма активного распространения по сети, они способны размножаться своими силами только в пределах одного компьютера. Как правило, передача копии вируса на другой компьютер происходит с участием пользователя.

Вирусы

Рис. 3 Различные варианты расположения кода вируса в зараженных файлах

Вирусы

Например, пользователь может записать свой файл, зараженный вирусом, на сетевой файловый сервер, откуда тот может быть скопирован всеми пользователями, имеющими доступ к данному серверу. Пользователь может также передать другому пользователю съемный носитель с зараженным файлом или послать такой файл по электронной почте. То есть именно пользователь является главным звеном в цепочке распространения вируса за пределы своего компьютера. Тяжесть последствий вирусного заражения зависит от того, какие вредоносные действия были запрограммированы в вирусе злоумышленником. Это могут быть мелкие, но раздражающие неудобства (замедление работы компьютера, уменьшение размеров доступной памяти, трата рабочего времени на переустановку приложений) или серьезные нарушения безопасности, такие как утечка конфиденциальных данных, разрушение системного программного обеспечения, частичная или полная потеря работоспособности компьютерной сети.

Шпионские программы

Шпионские программы (spyware) — это такой тип вредоносных программ, которые тайно (как правило, удаленно) устанавливаются злоумышленниками на компьютеры ничего не подозревающих пользователей, чтобы отслеживать и фиксировать все их действия.

В число таких действий может входить введение имени и пароля во время логического входа в систему, посещение тех или иных веб-сайтов, обмен информацией с внешними и внутренними пользователями сети и пр., и пр. Собранная информация пересылается злоумышленнику, который применяет ее в преступных целях.

Заметим, что в качестве шпионских программ могут использоваться не только созданные специально для этих целей вредоносные программы, но и программы легального назначения. Так, опасным средством шпионажа могут стать легальные системы мониторинга сети, такие, например, как популярные сетевые мониторы Wireshark или Microsoft Network Monitor. Исходное назначение этих программ состоит в том, чтобы дать администратору сети возможность следить за сетевым трафиком, в частности захватывать пакеты, используя механизм фильтрации, просматривать их содержимое, собирать статистику по загрузке устройств. В руках же злоумышленника такая программа превращается в мощный инструмент «взлома» сети, который позволяет перехватывать пакеты с паролями и другой секретной информацией. Они также позволяют путем сканирования TCP- и UDP-портов определять типы приложений, работающих в сети, что является очень важной информацией для подготовки атаки.

ПРИМЕЧАНИЕ

Практически все сетевые мониторы построены в архитектуре клиент-сервер. Клиенты, обычно называемые агентами, захватывают и, если необходимо, фильтруют трафик, а затем передают его серверной части монитора для дальнейшей обработки. Серверная часть монитора может работать как в локальной сети, так и на удаленном компьютере, однако клиентские части всегда устанавливаются на компьютерах в тех сегментах сети, в которых протекает интересующий администратора (или злоумышленника) трафик. Необходимым условием для работы агентов монитора является установка сетевого адаптера компьютера, на котором запущен этот агент, в неразборчивый режим приема (см. раздел «MAC-адреса»). Поэтому одним из способов, пресекающих несанкционированный захват и анализ сетевого трафика, является отслеживание всех интерфейсов сети, работающих в неразборчивом режиме приема.

Спам

Спам — это атака, выполненная путем злоупотребления возможностями электронной почты.

Учитывая ту важную роль, которую играет электронная почта в работе современных предприятий и организаций, можно понять, почему спам, дезорганизирующий работу этой службы, стал рассматриваться в последние годы как одна из существенных угроз безопасности.

Спам отнимает время и ресурсы на просмотр и удаление бесполезных сообщений, при этом ошибочно могут быть удалены письма с критически важной информацией, особенно велика вероятность этого при автоматической фильтрации писем. Посторонняя почта, которая нередко составляет 70 % получаемых сообщений, не только снижает эффективность работы предприятия, но и зачастую служит средством внедрения вредоносных программ. Кроме того, спам часто является элементом различных мошеннических схем, жертвами которых могут стать как отдельные сотрудники, так и предприятие в целом.

Спамеры, то есть лица, рассылающие спам, используют для своих целей разнообразные и иногда весьма сложные методы и средства. Так, например, для пополнения баз данных адресов ими может выполняться автоматическое сканирование страниц Интернета, а для организации массовой рассылки они могут прибегать к распределенным атакам, когда зомбированные с помощью червей компьютеры бомбардируют спамом огромное число пользователей сети.

Некоторые наиболее опасные виды сетевых атак

Некоторые классы атак, например, использующие ***переполнение буфера*** или ***переполнение стека*** (а также ***heap overflow***), являются составной частью многих видов вредоносных атак. Атаки переполнения имеют в свою очередь много разновидностей. Одна из наиболее опасных предполагает ввод в диалоговое окно помимо текста присоединенного к нему исполняемого кода. Такой ввод может привести к записи этого кода поверх исполняемой программы, что рано или поздно вызовет его исполнение.

Вирусы - вредоносные программы, способные к самокопированию. Передача от зараженной машины к незараженной может осуществляться с помощью приложения к почтовому сообщению. Способностью к саморассылке обладают ***сетевые черви***, первым сетевым червем был Morris Worm, ориентированный на UNIX BSD. Первые вирусы (например, макровирус Melissa (1999г), распространялись через e-mail с привлечение адресной базы данных почтового сервиса, они получили распространение задолго до широкого внедрения Интернет. В начале они распространялись через дискеты, куда попадали вместе с копируемыми играми и программами. Позднее они стали распространяться с помощью макросов, присоединенных к документам WORD. Большинство вирусов содержат в себе:

- **Репликатор**: Когда основная программа активируется, вирус пытается скопировать себя в один из каталогов машины-жертвы.
- **Маскератор**: Вирус всегда имеет какое-то средство, способное скрыть его от антивирусной программы.
- **Тело вируса** (Payload). Программа, которая может выполнять различные функции от блокировки определенных функций машины-жертвы, до полного разрушения данных.

Дополнительные материалы для изучения

Многие вредоносные коды, например, троянский конь с удаленным доступом (remote access Trojan) используют маскировку под программы, работающие с внешними устройствами. Так они могут оставаться неактивными, например, пока не используется мышка (см. статью Anthony M. Freed "Remote access Trojan evades detection using mouse functions"). Для решения своих задач хакеры могут использовать специальные трюки "ожидания", заимствованные из документации "Microsoft's MSDN" . Так для активации кода могут использоваться, например:

- WH_CALLWNDPROC - ожидать определенного сообщения, передаваемого из одного окна в другое.
- WH_CBT - средство для обучения, использующее компьютер, запоминающее и воспроизводящее нажатие определенных клавиш.
- WH_GETMESSAGE - возврат ввода от мышки, клавиатуры или другой системы.
- WH_KEYBOARD - трюк с клавиатурой, используемый в атаках перехвата ввода с клавиатуры.
- WH_MOUSE - трюк с мышкой, который описывает Symantec.
- WH_MSGFILTER - детектирует прикосновение к клавише, меню или другому средству Windows.
- WH_DEBUG - любое переполнение, запускающее отладчик.

Существует три класса вирусов: **заражающие файлы, систему или загрузочную зону системного диска** и **макро вирусы**. Как вирусы так и черви могут распространяться посредством электронной почты (в этом варианте они синонемичны). *В последнее время хакеры научились встраивать червей в графические файлы*.

Дополнительные материалы для изучения

Примером вирусной атаки может быть сайт форума "Высокие технологии 21-го века». Те кто посетил сайт и не имел адекватной защиты, получил копию этой заразы на свой компьютер.

Этот пример лишний раз свидетельствует, что наличие антивирусной защиты необходимо на каждом компьютере

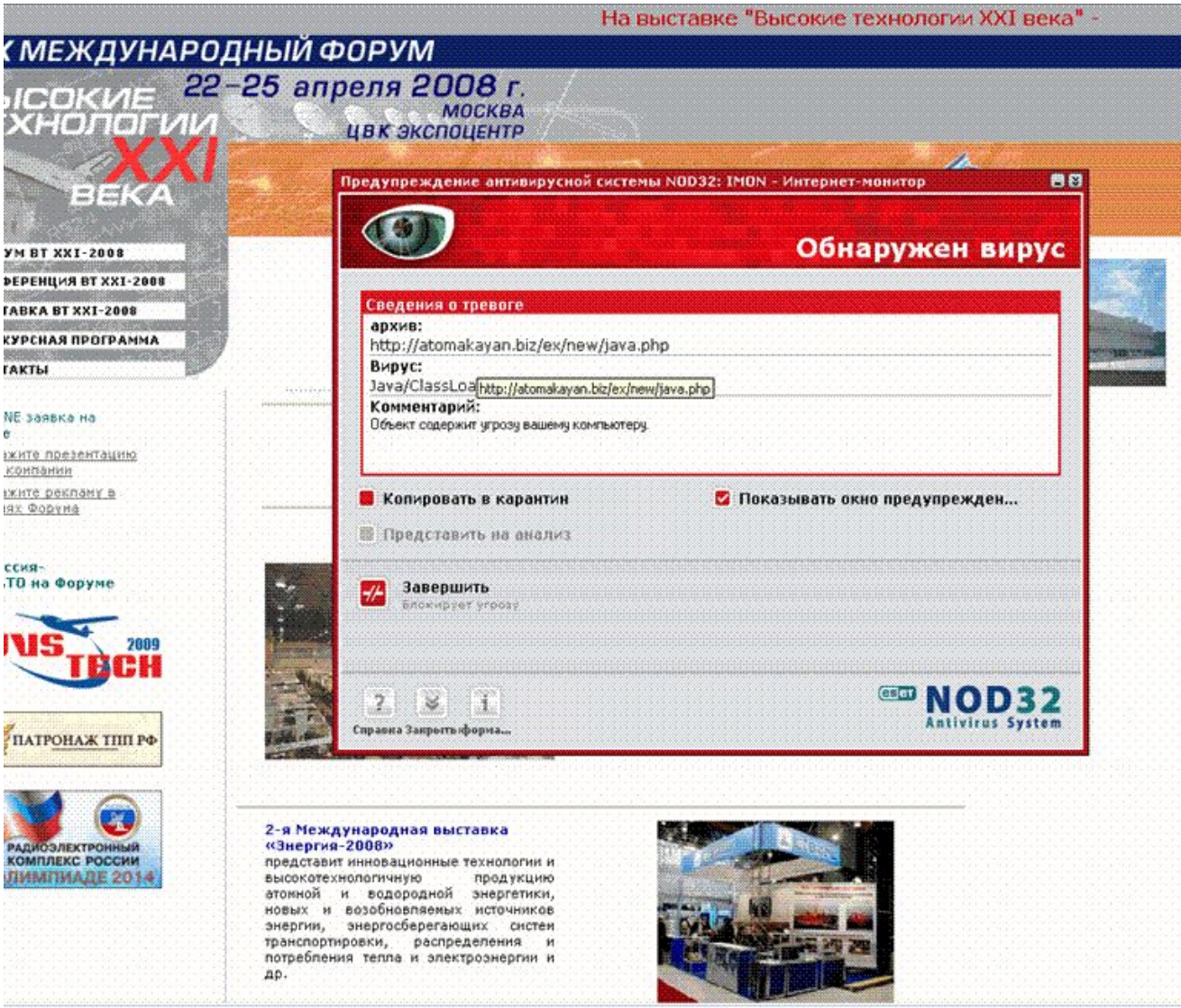


Рис. 4. Уведомление о вирусном заражении сайта www.vt21.ru

Дополнительные материалы для изучения

Известно, что многие вирусы и черви содержат в себе секции виртуально неизменных кодов. При заражении сети обычно появляется большое число идентичных пакетов. Кроме того, при этом в сети можно обнаружить большие пакеты, направленные внутрь или за пределы сети. Эти особенности могут быть использованы при детектировании вирусов или червей с неизвестной сигнатурой. Именно эти признаки были использованы системой **ASE** (Automatic Signature Extraction), разработанной компанией CISCO для своих маршрутизаторов, для детектирования вирусов и червей "нулевого дня". Соответствующие фрагменты кода были включены в IOS маршрутизаторов (версии IOS 12.4(15)T или выше).

С первого квартала 2005 года число WEB-базирующихся вредоносных кодов выросло на 540% (Gartner Inc). из обследованных 450 000 сайтов по крайней мере 10% используются для загрузки вредоносных кодов посетителям, В последнее время резко возрос интерес к программам обеспечения WEB-безопасности.

С момента создания до момента обнаружения вируса проходят часы, дни, недели, а иногда и месяцы (в среднем около года). Это зависит от того, насколько быстро проявляются последствия заражения. Чем это время больше, тем большее число ЭВМ оказывается заражено. После выявления факта заражения и распространения новой разновидности вируса требуется от пары часов до трех недель на выявление сигнатуры, создания противоядия и включения его сигнатуры в базу данных противовирусной программы. Временная диаграмма жизненного цикла вируса представлена на рис. 5 (" Network Security", v.2005, Issue 6, June 2005, p 16-18). Только за 2004 год зарегистрировано 10000 новых сигнатур вирусов. Червь Blaster заразил 90% машин за 10 минут. За это время антивирусная группа должна обнаружить объект, квалифицировать и разработать средство противодействия. Понятно, что это нереально. Так что антивирусная программа является не столько средством противодействия, сколько *успокоительным*.

Дополнительные материалы для изучения

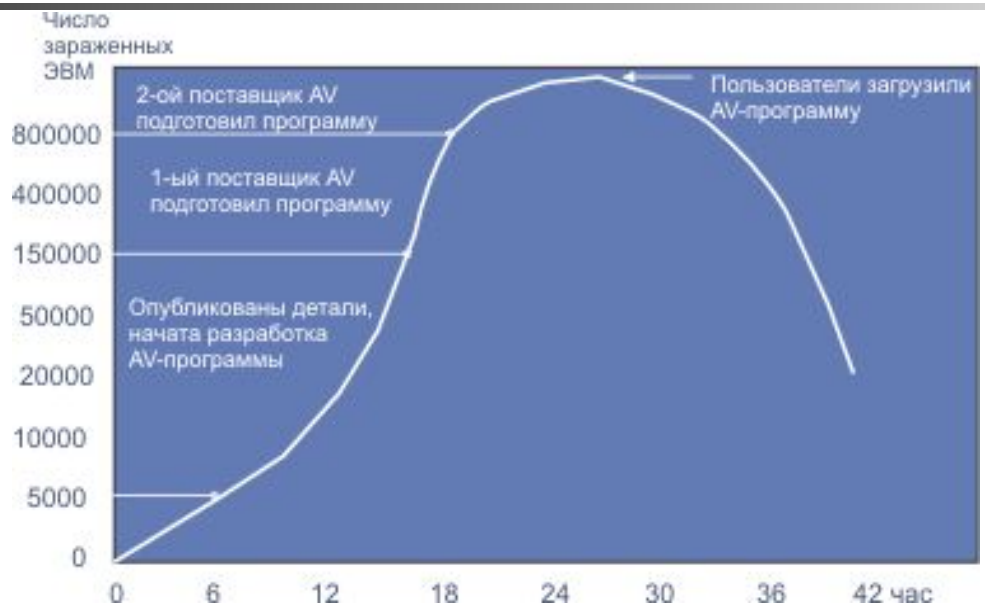


Рис.5. Диаграмма жизни вируса при благоприятном сценарии

Эти же соображения справедливы и для всех других видов атак. Когда сигнатура атаки становится известной, сама атака обычно не опасна, так как уже выработаны средства противодействия и уязвимость перекрыта. Под сигнатурой здесь подразумевается некоторый *характерный двоичный образ фрагмента кода*. Именно по этой причине такое внимание уделяется системе управления программными обновлениями (пэтчами).

Под сигнатурой здесь подразумевается последовательность бит (в памяти или на жестком диске), которая характеризует вредоносный код. Распознаванию сигнатуры может препятствовать ***полиморфизм*** такого кода, т.е. вариабильность кода, сохраняющая его функциональность. Известно, что некоторые современные разновидности Malware (malicious software) перекомпилируют себя каждые 5 минут, внося в текст неисполняемые команды (NOP) и, таким образом, варьируя свою сигнатуру.

Дополнительные материалы для изучения

Большинство антивирусных средств используют эвристические подходы, помогающие распознать вредоносный код, несмотря на его вариации. Одним из таких подходов является анализ действий (операций, поведения программы), выполняемых программой (например, модификация содержимого какого-то критического файла), а не ее сигнатуры.

Черви имеют обычно более сложную структуру и включают в себя следующие секции:

- **Средство проникновения**. Этот вредоносный код ищет уязвимости машины-жертвы. (*Уязвимость - это деликатное название опасной ошибки в программе*).
- **Инсталлятор**. Программа установки вредоносного кода на машине жертвы.
- **Средство поиска**. Программа поиска других машин - потенциальных жертв. Для этого может использоваться e-mail, локальные связи зараженной машины и средства DNS.
- **Сканнер**. Программа, которая просматривает выявленные машины на предмет наличия у них уязвимостей, которые может использовать данная версия червя.
- **Тело червя** (Payload). Исполняемая программа червя, которая может создавать условия для удаленного доступа в зараженную машину или перехватывать любой ввод с клавиатуры, включая имена и пароли.

Некоторые вирусы и черви имеют встроенные SMTP-программы, предназначенные для их рассылки и люки для беспрепятственного проникновения в зараженную машину. Новейшие версии снабжены средствами подавления активности других вирусов или червей. Таким образом могут создаваться целые сети зараженных машин (BotNet = ro**bot Net**work), готовых по команде начать, например DDoS-атаку.

Дополнительные материалы для изучения

Существует две схемы управления botnet: *централизованная* и *децентрализованная (peer-to-peer)*. Разумеется, возможно и комбинирование этих двух технологий. Для управления botnet используются протоколы IRC и HTTP. В botnet обычно имеется один или несколько серверов, которые ретранслируют машинам-зомби инструкции от хакера. *Боты взаимодействуют с центром в среднем раз в два часа*.

Сеть botnet, созданная с помощью кода Conficker в 2009 году, содержала около 6 миллионов машин. Всего зарегистрировано 5 версий этого сетевого червя. В начале декабря 2009 году было детектировано около 400 000 IP-адресов, зараженных этим вредоносным кодом.

Для управления машинами-зомби может использоваться протокол **IRC** (Internet Relay Chart), эта схема относится к централизованному типу. Система рассылки сообщений IRC поддерживается большим числом серверов и по этой причине этот канал обычно трудно отследить и запротоколировать. Этому способствует также то, что большинство систем более тщательно контролируют входной трафик, а не выходной. IRC-управление к началу 2010 года стало неэффективным (время жизни не более суток). Но и принципы управление типа peer-to-peer нейтрализуются достаточно быстро.

Для управления botnet в последнее время стали применяться **социальные сети**. Следует иметь в виду, что зараженная машина может служить помимо DoS-атак, для сканирования других ЭВМ и рассылки SPAM, для хранения нелегальных программных продуктов, для управления самой машиной и кражи документов, хранящихся там, для выявления паролей и ключей, используемых хозяином.

Дополнительные материалы для изучения

Для реализации централизованной схемы контроля может быть использован также протокол HTTP. Если выявить и заблокировать работу центрального сервера botnet, она прекратит свою работу, хотя все машины участницы останутся взломаны. Botnet с децентрализованной схемой управления (P2P) более устойчивы и по этой причине более опасны. Смотри также 10 answers to your questions about botnets. Чтобы представить себе структуру современных сетей botnet, посмотрите на рис. 6.

Не следует пытаться уничтожить botnet, достаточно сделать создание такой сети слишком дорогим и опасным, т.е. сделать отношение цена/выгода неприемлемым.

К сожалению пока не придумано надежных средств обнаружения новых вирусов (сигнатура которых не известна).

Следует постоянно помнить, что дополнительные WEB-сервисы (FTP, DNS, доступ к DB и т.д.) создают новые угрозы безопасности. Уязвимости обнаруживаются время от времени в широко используемых программах, например, Internet Explorer, Outlook и Outlook Express. Эти атаки для проникновения в систему используют переполнение буферов.

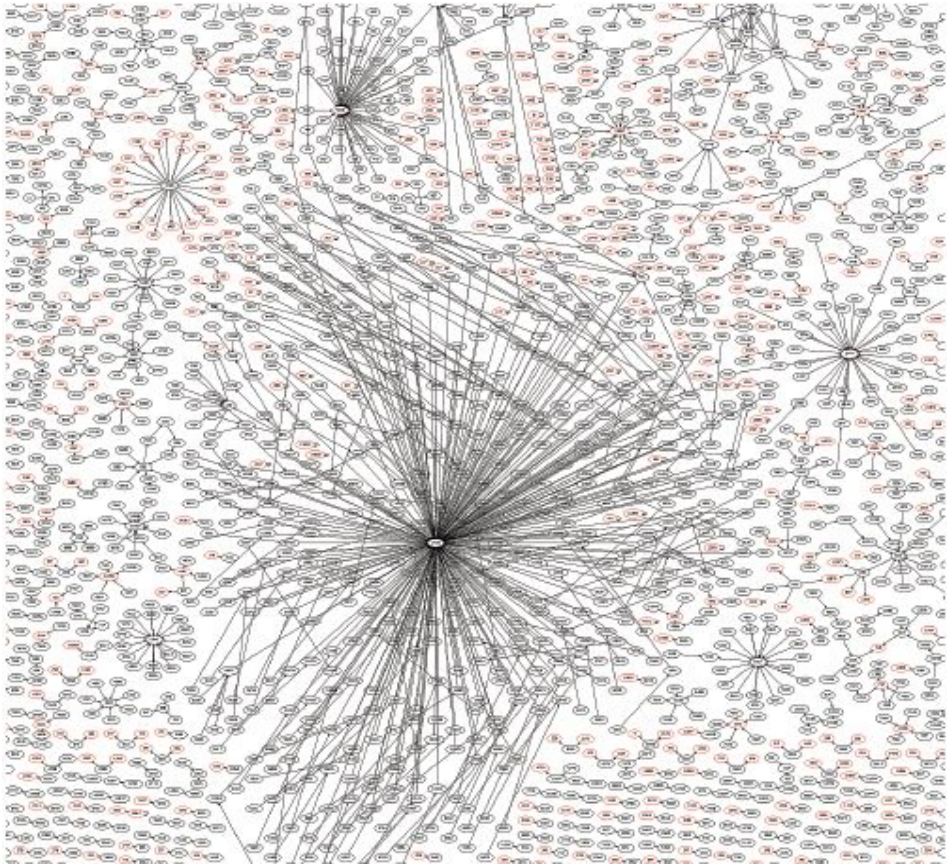
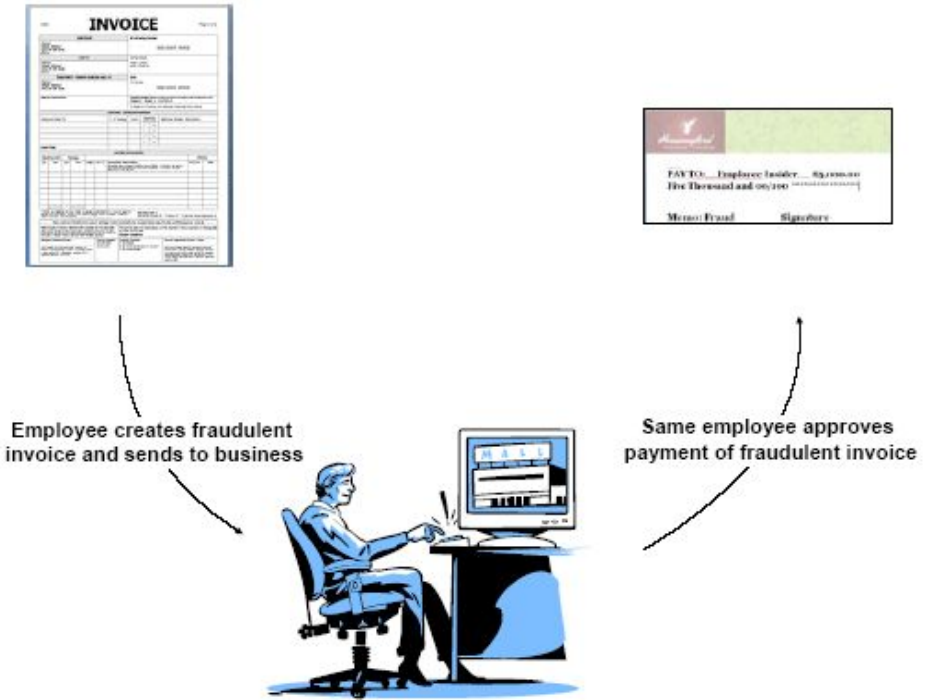


Рис.6. Пример структуры связей современных сетей botnet (Blue Coat Security Labs)

Дополнительные материалы для изучения

Khobe (Kernel Hook Bypassing Engine). В 2010 году появилась программа, позволяющая сегодня обойти практически все известные антивирусные защиты для Windows XP и Windows 7. Первое упоминание о такой возможности появилось в 2007 году. Эта программа использует уязвимости в службе таблиц дескрипторов ядра операционной системы (SSDT). Данная техника может быть скомбинирована с атакой на Acrobat Reader или Sun Java Virtual Machine. Принцип ее функционирования заключается в следующем. Сначала посылается абсолютно безвредный код, после того, как его безвредность антивирусной программой установлена, и до начала его исполнения этот код подменяется другим. В условиях, когда в системе параллельно исполняется много процессов, и один процесс, как правило не знает, что творит другой, такую операцию достаточно просто реализовать. Очевидно, что злоумышленник должен иметь возможность исполнять двоичный код на машине-жертве.

На рис. 7 показан пример схемы, при которой инсайдер похищает средства компании. Инсайдер формирует фальшивый счет и направляет ее в систему обработки. Позднее он одобряет оплату этого счета. Может показаться, что такая схема может пройти только один раз. Но это не так. Во-первых, контроль всех электронных документов осуществляется не так часто, во-вторых, в эту схему обычно включается несколько человек (в том числе и внешних) или просто эту работу реализует частично или полностью вредоносная программа, установленная на сервере платежей. Факт кражи будет установлен лишь когда сумма станет значительной.



Дополнительные материалы для изучения

WEB-страницы иногда имеют скрытые ссылки на конфиденциальные данные. Именно на это рассчитывают хакеры.

Практика показывает, что 80% усилий тратится на противодействие внешним атакам, а 70% реальных атак, наносящих ущерб, производится из локальной сети.

Phishing - получение паролей, PIN-кодов и пр. (последующая кража информации). Впервые этот вид атак зарегистрирован в 1996 году. Этот вид атаки начинается с рассылки почтовых сообщений, содержащих ссылку на известный ресурс (или имитирующий такую ссылку). Практика показывает, что примерно четверть получателей открывают phishing-сообщения. Дизайн WEB-страницы обычно копируется с воспроизводимого ресурса. На фальсифицируемой странице может быть, например, написано, что банк, где вы имеете счет, проводит акцию по проверке безопасности доступа. Вам предлагается ввести номер вашей кредитной карты и PIN-код. Если вы это сделаете, злоумышленники сообщат, что все в порядке, а с вашего счета через некоторое время пропадут деньги.

Но если это не сопряжено с банком, опасность такой атаки нисколько не уменьшается. Получив доступ к вашему акаунту, злоумышленники получат доступ к конфиденциальной информации и т.д. Служба администратора часто присылает новый пароль, не проверяя личность человека, приславшего запрос. Так терминалы иногда стоят в общедоступных помещениях, а сотрудник может ненадолго отойти от дисплея, не прерывая сессию, посторонний может сесть на его место, поменять пароль или загрузить троянского коня, получив доступ в систему. Злоумышленник может подсмотреть пароль и через плечо работающего легального пользователя. Хорошей практикой является отсутствие документов и тем более паролей на вашем рабочем столе. Длительная пауза в работе должна автоматически запирать дисплей.

Дополнительные материалы для изучения

Критическая информация в laptop или notebook должна быть зашифрована. Одним из возможных средств атак является использование **IDN** (International Domain Name). Дело в том, что в системах, поддерживающих IDN, допускается использование букв национальных алфавитов, а, например, некоторые буквы латинского и русского алфавитов пишутся идентично. Этим могут воспользоваться злоумышленники, они могут зарегистрировать имена, которые выглядит как имена известной фирмы, например microsoft.com, где некоторые буквы заменены на русские, так что это внешне не заметно, например, буквы с или о. Тогда при ошибочной замене одной или нескольких букв на русские клиент попадет не на сайт компании Microsoft, а на внешне неотличимый от него сайт злоумышленника. В среднем электронные мошенничества наносит ущерб порядка 895$, частота же таких преступлений достаточно быстро растет.

Пример подобного сообщения представлен ниже.

Дополнительные материалы для изучения

Анализ инцидента показал, что произведена полная подмена страниц. Утилита Traceroute указывала на вроде бы легальный адрес в США...

При получении почтового сообщения, содержащего URL, возможна фальсификация адресов. Например написана ссылка www.microsoft.com, а на самом деле уход может происходить на адрес barmaley.com. Для этого можно записать URL в виде: <A href=http://barmaley.com>www.microsoft.com. Хакер при этом может справедливо полагать, что читатель почтового сообщения не станет рассматривать HTML-код сообщения, а будет руководствоваться тем, что видит на экране.

SMITH BARNEY citigroup

Dear **Valued Customer,**

SmithBarney Citigroup, is committed to maintaining a safe environment for our customers. To protect the security of your account, SmithBarney Citigroup, employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Citibank system for unusual activity.

We are contacting you to remind you that on Nov. 28, 2004 our Account Review Team identified some unusual activity in your account. In accordance with SmithBarney's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account closure.Visit now log on page and sign to account verification process:

https://www.smithbarney.com/login/login.cgi?redir=s

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.

Sincerely,

SmithBarney Citigroup, Account Review Department.

Разновидностью такого рода атак является атака через DNS (или каким-то иным способом), когда страница известного URL подменяется страницей злоумышленника (spoofing).

При получении почты следует иметь в виду, что поле сообщения **From:** можно легко фальсифицировать. Хакер это может сделать для того, чтобы вы отнеслись с большим доверием к присланному сообщению. Протокол же SMTP и почтовые приложения не осуществляют проверку соответствия IP-адреса отправителя и поля From. Фильтрация сообщений по полю From предусмотрена лишь в программах AntiSPAM.

Традиционные программы antiSPAM не могут идентифицировать phishing-атаки. Такие сообщения не содержат ключевых слов, по которым детектируется SPAM (например, Viagra, pharmaceuticals или discount), они отправлены с адресов, еще не попавших в репутационные списки. Часто это адреса ваших хороших знакомых или коллег.

Троянский конь (Spyware)

Эта программа, которая на вид имеет безобидное назначения, на самом деле содержит определенные вредоносные функции. Она может фиксировать все нажатия клавиш на терминале или мышке, способна записывать screenshot'ы и передавать эти данные удаленному хозяину. Если на ЭВМ оказался установленным общеизвестный троянский конь, машина становится уязвимой. Именно с этим связано сканирование хакерами номеров портов известных троянских коней. Многие современные вирусы и черви могут загружать в зараженную ЭВМ троянского коня (или программу spyware), целью которого может быть не только получение паролей, но также номера кредитной карты и PIN-кода. В некоторых случаях зараженная машина может стать источником DoS-атаки.

Дополнительные материалы для изучения

Исследования, проведенные в 2004 году, показали, что 90% PC имеют какой-то вид spyware (это не обязательно троянские кони). В среднем каждая ЭВМ содержит в себе до 26 разновидностей таких программ (возможно, это и преувеличение, но если вы не предпринимали специальных мер, как минимум одна такая программа в вашей ЭВМ имеется). Следует учитывать, что Spyware, имеют примерно те же возможности, что и троянский конь, встраиваются в другие программы и распространяется несколько другими методами. Программа *троянский конь* может рассылать себя другим машинам (как и сетевой червь). Кроме того, в отличие от троянских коней эти программы часто не обнаруживаются антивирусными программами. Смотри www.earthlink.net/about/press/pr_spyAudit, www.ssppyy.com и securityresponse.symantec.com.

Программа "Троянский конь" обычно содержит в себе следующие секции:

- **Переименование**. Файлу, содержащему вредоносный код присваивается имя, которое напоминает одну из штатных программ системы.
- **Разрушение**. Секция мешает выявлять вредоносный код с помощью антивирусной программы.
- **Полиморфный код**. Программа, которая регулярно модифицирует сигнатуру вредоносного кода.

Функцией Spyware является сбор данных об активности вашей машины, о криптоключах, паролях и другой критической и конфиденциальной информации. Spyware.Ssppyy может попасть к вам вместе с поздравительной открыткой. Если хотя бы один пользователь откроет такую открытку, вся система окажется скомпрометированной. 80% данных Spyware отсылает своему хозяину по почте (порт=25), некоторые разновидности этих программ содержат в себе почтовый сервер. Расходы на противодействие spyware увеличи - ваются ежегодно примерно в пять раз (создание программ, обновление БД сигнатур и т.п.).

Дополнительные материалы для изучения

Симптомами присутствия spyware в вашем компьютере могут служить следующие признаки: (см. Recognizing and Avoiding Spyware).

- Неспровацировано открываются окна
- Вас переадресуют на сайт, отличный от того, имя которого вы ввели
- В окне вашего браузера появляется иконка нового программного средства
- Появилась новая иконка в списке заданий в нижней части вашего экрана
- Изменилась базовая страница вашего браузера
- Изменилась страничка поисковой программы вашего браузера
- Перестали работать некоторые клавиши в вашем браузере (напр., клавиша табулятора)
- Появляются необъяснимые сообщения об ошибках
- Ваш компьютер неожиданно замедляет свою работу (например, при спасении файлов и т.д.)

Проверка моей машины с помощью программы **BPS Spyware** показала, что там содержится около 2000 таких программ (машина не сканировалась на предмет spyware); всего по результатам сканирования удалено 17825 объектов), но с момента инсталляции ОС на машине работала антивирусная программа. Последние полгода там работал ZoneAlarm. Полная очистка ЭВМ от spyware, размещенных в файлах, в cookies, в реестре и т.д. заняла достаточно много времени.

В последнее время троянские кони стали использоваться для отслеживания места пребывания хозяина машины (laptop). В перспективе, когда машины получат датчики GPS, эта задача существенно упростится.

Дополнительные материалы для изучения

Cookie содержит информацию о вашем имени, установках и предпочтениях при просмотре конкретного сайта. Эта информация заносится на ваш компьютер при просмотре этого сайта. На рис. 8 показана схема вторжения для троянского коня adwind-java. Для вторжения необходимо наличие активного модуля языка Java.

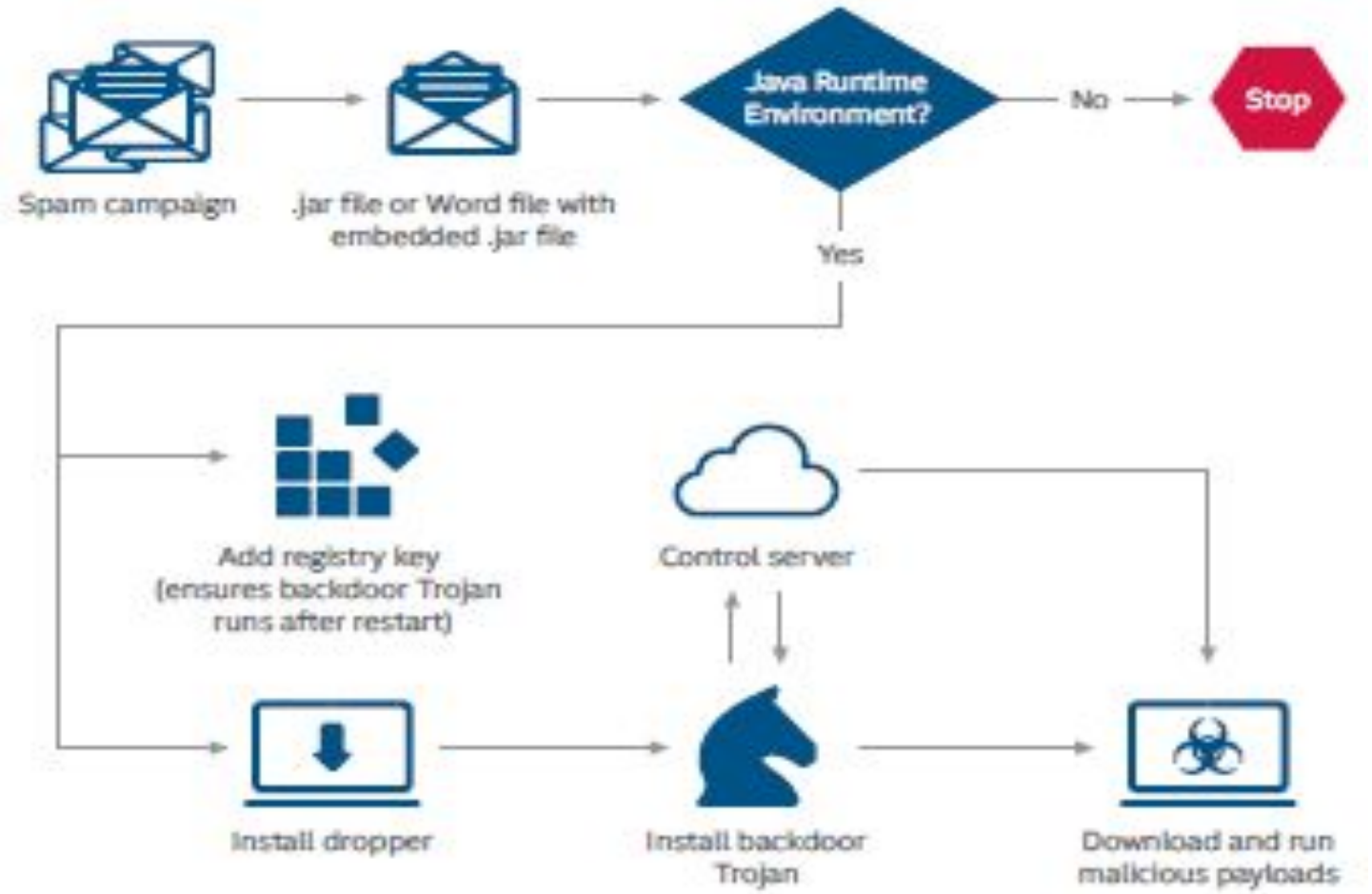


Рис.8. Схема вторжения для троянского коня Adwind

Дополнительные материалы для изучения

SPAM составляет до 90% полного объема почтовых сообщений. Сопряжено это с тем, что рассылка SPAM стала достаточно доходной частью полукриминального бизнеса. Это связано с потерями сетевых ресурсов, о времени получателей я уже не говорю. Часть таких сообщений часто заражена вирусами, червями или троянскими конями. Эффективность современных фильтров SPAM достигает 90%. При этом следует учитывать, что такие фильтры сильно загружают серверы DNS. Для минимизации SPAM обычно рекомендуется иметь несколько почтовых адресов, например, один для частной переписки, один для деловой и один для информационных обменов, подписки и пр. Это облегчает распознавание SPAM. Полезно самому создавать уникальные адреса для каждого вида обменов и время от времени их менять (см. email.about.com/library/weekly). Это легко делать в случае подписных листов.

Рекомендуется удалить свой почтовый адрес из своего WEB-сервера. Не рекомендуется покупать что-либо по рекомендациям SPAM-рассылок, тем более что в 95% случаях это могут оказаться недобросовестные поставщики. В последнее время для исключения распознавания SPAM по содержанию, отправители стали использовать графическую форму представления текста. По данным Sophos 60% SPAM рассылается через взломанные ЭВМ. SPAM не только раздражает, съедая сетевые ресурсы, он делает бизнес менее эффективным. Представьте сколько времени сотрудники тратят на просмотр таких сообщений, сколько средств и ресурсов тратится на приобретение и обслуживание программ, фильтрующих почту, и вы поймете, что SPAM не безобиден и уже сегодня наносит ущерб более значительный, чем сетевые вирусы. Следует также учесть, что SPAM стал одним из основных средств рассылки троянских коней spyware, phishing и прочих разновидностей malware. ***В мае 2008 года ботнет Srizbi рассылала до 60 миллиардов SPAM-сообщений в сутки***.

Дополнительные материалы для изучения

SPAM используется и для заражения машин вредоносными кодами. Для этой цели обычно применяются приложения со встроенными скриптами и другими опасными программами.

Разновидность SPAM, рассылаемая через **IM** (от instant message мгновенное сообщение (в системах, используемых для сетевого общения, например, ICQ)), иногда называют **SPIM**. “Пассивные” атаки с помощью, например, sniffer особенно опасны, так как, во-первых, практически недетектируемы, во-вторых, предпринимаются из локальной сети (внешний Firewall бессилен).

Scam - мошеннический трюк, заключающийся в том, чтобы, ссылаясь на авторитетных лиц, втереться в доверие и извлечь коммерческую выгоду. Первооткрывателями этого вида мошенничества были адресаты из Нигерии. Смотри en.wikipedia.org/wiki/Scam. Начиная с 2008 года стал активно использоваться мошеннический трюк, когда предлагается антивирусное (или любое программное защитное средство), при попытке загрузки которого машина оказывается заражена вредоносным кодом. Причем доступ к этой программе часто оказывается платным, что внушает дополнительное доверие потенциальной жертвы.

В организациях с 10000 сотрудников сплошь и рядом имеется до 16000 акоунтов за счет уже давно не используемых (люди уволились). Такие неиспользуемые акоунты могут стать объектом атаки, тем более что их создание может относиться ко времени, когда безопасности паролей не уделялось должного внимания. По этой причине администратор должен требовать регулярного обновления паролей и удалять устаревшие, неиспользуемые акоунты.

Дополнительные материалы для изучения

Следует также учитывать, что средний сотрудник имеет в среднем как минимум 20 паролей (рабочей станции, сервера, базы данных, почты, социальной сети и пр.), это дополнительно усложняет ситуацию. Чрезмерные требования к сложности пароля могут иметь обратное действие - человек его забывает или записывает на видном месте. При большом числе паролей человек выбирает их похожими или даже одинаковыми, что упрощает их подбор злоумышленником. Опросы показывают, что средний человек способен помнить 4 пароля, а должен знать до 40! Именно этот факт делает привлекательным применение многофакторных систем аутентификации (специальные карты-ключи, биометрические данные, например, отпечатки пальцев, голос или радужка глаз).

При разработке новых устройств и программ надо уже на стадии проектирования встраивать в них средства безопасности. Должны быть разработаны специальные курсы обучения тому, как писать безопасные программы, например, CGI (Common Gateway Interface).

Еще одной, достаточно новой угрозой является **IM** (Instant Messaging - по существу это Internet Relay Chart (IRC - протокол, разработанный для коммуникации пользователей интернета в режиме реального времени). Хотя большинство систем IM (MSN, Yahoo IM, AIM и др.) имеют стандартные номера портов, блокировать доступ для этого сервиса, закрыв эти порты, нельзя, так как системы могут воспользоваться другими номерами портов, например, 80, 23, 20 и т.д.. К этому классу уязвимостей следует отнести и сервис ICQ. Возможно, некоторые читатели сталкивались с появлением на экране их дисплея окна, приглашающего сыграть в "бесплатном" казино, это одно из проявлений подобных атак. Некоторые пользователи могут полагать, что они в безопасности, так как не используют e-mail. Для защиты от этого вида атак нужно специализированное программное обеспечение. Следует также помнить, что однажды запретив IM, нельзя быть уверенным, что вы полностью защищены с этой стороны. Например, автоматическое обновление Windows XP SP2 включает в себя загрузку Windows Messenger, что сведет на нет ваши усилия.

Дополнительные материалы для изучения

IM является частью набора технологий **UC** (Unified Communication), который становится все более популярным. Уязвимость таких систем увеличивается за счет того, что сервисы e-mail, IM, SMS, VoIP и пр. реализуются независимо. Помимо этого, сегодня для IM характерно отсутствие четкой политики безопасности, а средства IM инсталируются клиантами сети предприятия без информирования администратора. Потери из расчета на один инцидент в 2008 году достигли 288 000$.

Вообще в отношении IM любой пользователь и сетевой администратор должен ответить на ряд вопросов:

1. Следует ли использовать IM в его сети вообще?
2. Могут ли пользователи использовать IM на системах, принадлежащих вашей организации?
3. Нуждается ли организация в специфическом программном обеспечении IM?
4. Следует ли использовать криптографию для обеспечения безопасности IM?
5. Допустимо ли использование IM для частного обмена внутри и вне локальной сети?
6. Следует ли вводить ограничения на передачу данных служебного характера, передаваемых посредством IM?
7. Следует ли вводить определенные требования на запись (журналирование) обменов посредством IM?

Следует внедрять средства записи всех IM-обменов. Это позволит иметь архив всех обменов. Служащие же, зная, что все обмены на предприятии записываются, будут вести себя более осмотрительно. Параллельно можно внедрить фильтрацию IM по ключевым словам, чтобы исключить утечку критической информации. Такие фильтры могут блокировать также передачу вредоносных кодов внутри IM-сообщений.

Дополнительные материалы для изучения

Так как **беспроводные сети** находят все более широкое применение, а безопасность таких каналов оставляет желать лучшего, возможен перехват трафика с помощью средств типа sniffer. Высокой безопасности можно не получить даже в случае применения VPN и двухфакторной аутентификации (SecurID). Для хакера такие объекты атаки привлекательны тем, что им не нужно устанавливать соединение с каким-либо объектом в локальной сети, не оставляя следов в FireWall или IDS. Обычный просмотр WEB-страниц может помочь украсть индивидуальные параметры. Пользователи корпоративной сети при работе с WEB-страницами (просмотр требует аутентификации) могут получить уведомление: "Your connection to the network has been lost - please reenter your username and password". Инициатором такого сообщения может быть злоумышленник, который рассчитывает получить ваши аутентификационные параметры.

Беспроводные средства облегчают атаки и стационарных объектов. Клиент, купивший карту доступа, получает динамический адрес и его локализация и идентичность достаточно трудно установить. Существуют специальные средства для выявления приборов 802.11, например, Kismet или Air Defense (разновидность IDS). Но такие средства могут использоваться как во благо, так и во вред, они могут помочь обнаружить плохо сконфигурированные точки доступа. Для таких сетей особенно актуальна проблема однозначной идентификации пользователя, где бы он ни находился. Обычно портативные ЭВМ после включения пытаются установить соединение с известными им беспроводными точками подключения (их число может превышать сотню), атакер может сформировать точку доступа, имитирующую один из таких узлов, для установления соединения с данной ЭВМ и получения параметров доступа.

Дополнительные материалы для изучения

В последнее время появились экраны, работающие по технологии стелз, способные экранировать радиоволны определенных частот. Это позволяет обезопасить беспроводные локальные сети, сохраняя работоспособность мобильных телефонов. Эта технология может помочь исключить интерференцию систем, работающих на идентичных частотах.

Если нет насущной потребности, следует дезактивировать вход USB на уровни BIOS. Заметной уязвимостью обладают все переносные ЭВМ. Человек, получивший к такой ЭВМ доступ, за несколько минут может установить новый пароль (с помощью загрузочного диска) и скопировать оттуда любую информацию или установить там троянского коня. Особую категорию составляют домашние ЭВМ. Многие компании одобряют работу своих сотрудников дома (экономится электричество, рабочее место и пр.), удобно это и работникам (экономится время в пути и бензин). При подключении к офисной сети предпринимаются достаточно серьезные меры безопасности, но эта же машина может использоваться детьми, подключающимися к самым разным сайтам, среди которых могут быть ЭВМ злоумышленников. При этом нет никакой гарантии, что в такую машину не попадет троянский конь или другая вредоносная программа. После же подключения в сети компании такая машина может стать источником угрозы для других ЭВМ локальной сети. Покидая рабочее место, целесообразно выйти из ОС (произвести процедуру Logoff), но все ли это делают? По этой причине после 30-60 сек пассивности, ЭВМ должна сама выполнить эту процедуру. Многие компании в случае успешной сетевой атаки скрывают этот факт, чтобы сохранить доверие клиентов. Это приводит к тому, что число жертв увеличивается (такой же атаке подвергаются другие, не предупрежденные об угрозе).

Дополнительные материалы для изучения

Сигнатуры современных атак могут быть достаточно изощренными. Это может быть не просто попытка установить соединение с определенным портом, а вполне определенная последовательность попыток соединений, приводящая к соединению. Это характерно для доступа к некоторым люкам, специально оставленным хакером в какой-то программе. Такая схема исключает детектирование окон уязвимости простым поиском открытых портов (так работают некоторые программы поиска вторжений). Подробности этой техники смотри по адресу www.portknocking.org.

Появились сообщения о разработки вредоносных кодов, написанных на JavaScript. В это трудно поверить, но если это так, масштаб сетевых угроз увеличивается весьма существенным образом. Ведь в этом случае не нужно ничего копировать с вредоносного сайта, достаточно туда заглянуть. Но по-прежнему главной уязвимостью остается неопытный и малообразованный пользователь.

Наибольшую угрозу представляют атаки с помощью программ, специально написанных для вторжения в конкретную ЭВМ или сеть. К сожалению, большинство разработчиков приложений не учитывает требования безопасности. Сертификация программ, как правило, не включает в себя аспект безопасности (попыток вторжения). Следует разделять уязвимости "врожденные" и специально созданные хакером. Эти два вида бывает трудно разделить, если вы покупаете нелегальное программное обеспечение. Хороший хакер готовит вторжение с тщательной разведки объекта атаки. Это не обязательно сканирование или попытки подбора пароля. Такую информацию хакер может получить из описаний разработанных на сервере-мишени программных продуктов (требования к ОС, версии и т.д.) Он может послать запросы на серверы Whois, посылая команды finger или почтовому серверу и пр.

Дополнительные материалы для изучения

В отдельности такие запросы не говорят ни о чем. Но, если собирать статистику о клиентах сети (используемые запросы, ping, traceroute, сканирования определенных портов и т.д.), то по совокупности этих данных можно с приемлемой вероятностью прогнозировать угрозу.

При стратегическом планировании в сфере сетевой безопасности следует учитывать тенденцию в направлении распределенных систем и более широкого внедрения беспроводных систем. Оба эти фактора делают решение проблем значительно труднее.

По мнению экспертов в последнее время важной мишенью атак становятся приложения, особенно те, которые взаимодействуют или доступны через Интернет. На долю таких приложений приходится до 70% успешных сетевых атак (данные Gartner Group).

В последнее время атаки серверов становятся двухэтапными. Так как сервер обычно защищен лучше рабочей станции, сначала атакуется именно она (например, через e-mail или Explorer). А далее с рабочей станции предпринимается уже атака сервера. Собственно атака даже может быть не нужна, если на рабочую станцию в результате атаки был загружен троянский конь или spyware. Ведь эти коды позволяют перехватить пароль, когда он еще не зашифрован.