Атаки отказа в обслуживании (DoS)
Перехват и перенаправление трафика

БГА, РТФ
Кафедра ИБ

Зензин Александр Степанович, к.т.н.

Обзор

1. Введение, атаки отказа в обслуживании
2. Распространение вредоносных программ
3. Атака типа “TCP SYN шторм”
4. Перехват и перенаправление трафика
5. Разработка средств детектирования и защиты
6. RFC – 2827
7. Дополнительные материалы для изучения

Введение, атаки отказа в обслуживании

Целью **DoS** (Denial of Service) атаки отказа в обслуживании является блокировка каких-то ресурсов атакуемого, чаще всего это входная полоса пропускания, с целью ограничения доступа клиентов к серверу, узлу или сети жертвы. В качестве объекта атаки помимо полосы пропускания может быть вычислительная мощность процессора или информационные ресурсы операционной системы.

Атаки отказа в обслуживании направляются обычно на информационные серверы предприятия, функционирование которых является критически важным условием для работоспособности всего предприятия. Чаще всего объектами DOS-атак становятся основные веб-серверы, файловые и почтовые серверы предприятия, а также корневые серверы системы DNS.

Как правило, злоумышленник пытается организовать дело так, чтобы трафик на входе жертвы превосходил его (атакера) выходной трафик. Решить эту задачу он может разными методами. Наиболее распространенным является способ массового взлома машин и использования их для атаки. Для проведения DoS-атак злоумышленники часто координируют «работу» нескольких компьютеров (как правило, без ведома пользователей этих компьютеров). Говорят, что в таких случаях имеет место распределенная атака отказа в обслуживании (Distributed Denial of Service, **DDoS**).

Другим приемом является умножение воздействия за счет других сетевых устройств, например, NTP- или DNS-серверов (ресурсные запросы) или маршрутизаторов (использование широковещательных IP-адресов). Возможно совмещение нескольких методов DoS-атаки.

Введение, атаки отказа в обслуживании

Злоумышленник, захватив управление над группой удаленных компьютеров, «заставляет» их посылать пакеты в адрес узла-жертвы (рис. 1). Получившийся в результате мощный суммарный поток «затопляет» атакуемый компьютер, вызывая его перегрузку и, в конечном счете, делает его недоступным. Блокировка происходит в результате исчерпания ресурсов либо процессора, либо операционной системы, либо канала связи (полосы пропускания).

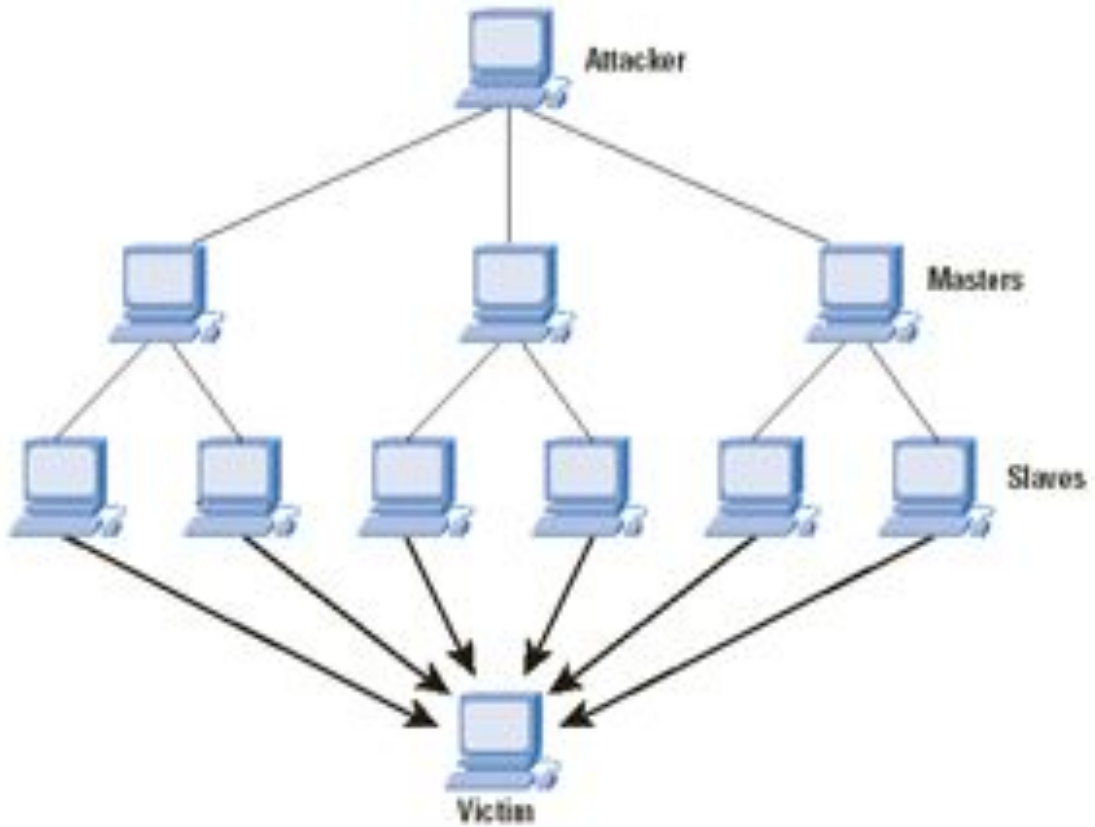

Рис. 1. Схема DDoS-атаки

Введение, атаки отказа в обслуживании

Злоумышленники (атакеры) могут применить различные способы для выявления и получения доступа к машинам-жертвам (смотри Nicholas Weaver, "Warhol Worms: The Potential for Very Fast Internet Plagues". Наиболее важными из них являются:

- *Случайное сканирование.* В этом подходе машина, зараженная вредоносным кодом (это может быть машина атакера или другая взломанная им ранее ЭВМ), сканирует определенную IP-область, выбирая адреса случайным образом, и пытается выявить уязвимую машину. Если такая обнаружена, делается попытка ее взлома и, в случае успеха, размещает там свой вредоносный код. Этот метод создает достаточно большой трафик, так как одни и те же адреса сканируются помногу раз. Преимуществом такого способа является достаточно быстрое заражение большого числа машин и создание впечатления, что сканирование происходит отовсюду. Однако высокий уровень трафика препятствует длительному продолжению атаки.
- *Сканирование по списку.* Задолго до начала сканирования атакер подготавливает достаточно обширный список потенциально уязвимых машин. Такой список может готовиться достаточно долгое время, чтобы не привлечь к этому внимания служб безопасности. Сканирование производится только для машин их этого списка. Когда обнаружена уязвимая машина, на нее устанавливается соответствующая программа, а список сканирования делится пополам. Вновь взломанной машине поручается сканирование машин одной из частей списка. Каждая из машин продолжает сканирование пока не сможет найти уязвимую ЭВМ. После этого список снова делится и процедура продолжается. Таким образом, число машин, участвующих во взломах, лавинообразно увеличивается.

Введение, атаки отказа в обслуживании

- *Топологическое сканирование.* При топологическом сканировании используется информация, содержащаяся в машине жертвы, для поиска новых потенциальных жертв. При этом на диске взломанной машины ищутся URL, которые можно попробовать атаковать. Этот метод может оказаться даже несколько более эффективным, чем сканирование по списку.
- *Сканирование локальной субсети*. Этот вид сканирования работает за firewall. Взломанная машина ищет потенциальные жертвы в своей собственной локальной сети. Эта техника может использоваться в сочетании с другими способами атак, например, взломанная машина может начать сканирование локальной сети, а когда список таких машин будет исчерпан, переключиться на сканирование других сетевых объектов.
- *Перестановочное сканирование.* При этом типе сканирования все машины совместно используют общий псевдослучайный перестановочный список IP-адресов. Такой список может быть сформирован с помощью блочного 32-битного шифра с заранее заданным ключом. Если взломанная машина была инфицирована при сканировании по списку или из локальной сети, она начинает сканирование, начиная со своей позиции в списке перестановок. Если же она оказалась скомпрометирована в процессе перестановочного сканирования, она начинает сканирование с псевдослучайной позиции списка. В случае если она встретит уже инфицированную машину, она выбирает новую псевдослучайную позицию в списке перестановок и продолжает работу с этой точки. Распознавание инфицированных машин происходит за счет того, что их отклики отличаются от откликов невзломанных ЭВМ. Сканирование прекращается, если машина встретит заданное число инфицированных машин. После этого выбирается новый ключ перекодировок и начинается новая фаза сканирования. Факт такого сканирования труднее детектировать.

Распространение вредоносных программ

Можно выделить три механизма рассылки вредоносных кодов и построения сетей для атак (смотри David Moore and Colleen Shannon, "The Spread of the Code Red Worm (crv2)," July 2001).

- *Централизованная рассылка*. В этой схеме после выявления уязвимой системы, которая должна стать зомби, выдается команда в центр рассылки для копирования вредоносного кода (toolkit) во взломанную машину. После копирования этого кода осуществляется инсталляция вредоносной программы на машине жертвы. После инсталляции запускается новый цикл атак с уже захваченной машины. Для передачи кодов программ могут использоваться протоколы HTTP, FTP и RPC.
- *Доставка от атакера (Back-chaining)*. В этой схеме все вредоносные коды доставляются в захваченную машину из ЭВМ атакера. В частности, средства атаки, установленные у атакера, включают в себя программы доставки вредоносных кодов жертве. Для этой цели на машине-жертве может использоваться протокол TFTP.
- *Автономная рассылка*. В этой схеме атакующая машина пересылает вредоносный код в машину-жертву в момент взлома.

После того как армия атакующих машин сформирована, атакер определяет вид и объект атаки и ждет удобного момента времени. После начала атаки все машины этой армии начинают слать пакеты по адресу машины-жертвы. Объем трафика при этом может быть столь велик, что может быть заблокирован даже шлюз сети, где расположена машина-жертва. Сейчас в Интернет имеется около дюжины программ автоматизации процесса на всех фазах атаки. Причем для пользования ими не требуется лицензии.

Распространение вредоносных программ

Работа машин зомби может быть автономной или синхронизироваться атакером (рис.1). Для того чтобы скрыть свой IP-адрес атакер фальсифицирует адрес отправителя. Помимо описанной выше разновидности DDoS-атаки существует разновидность **DRDoS** (Distributed Reflector DoS).

DRDoS-атаки более вредоносны и здесь еще труднее выявить первоисточник атаки, так как в процесс вовлечено больше машин (см. рис. 2).

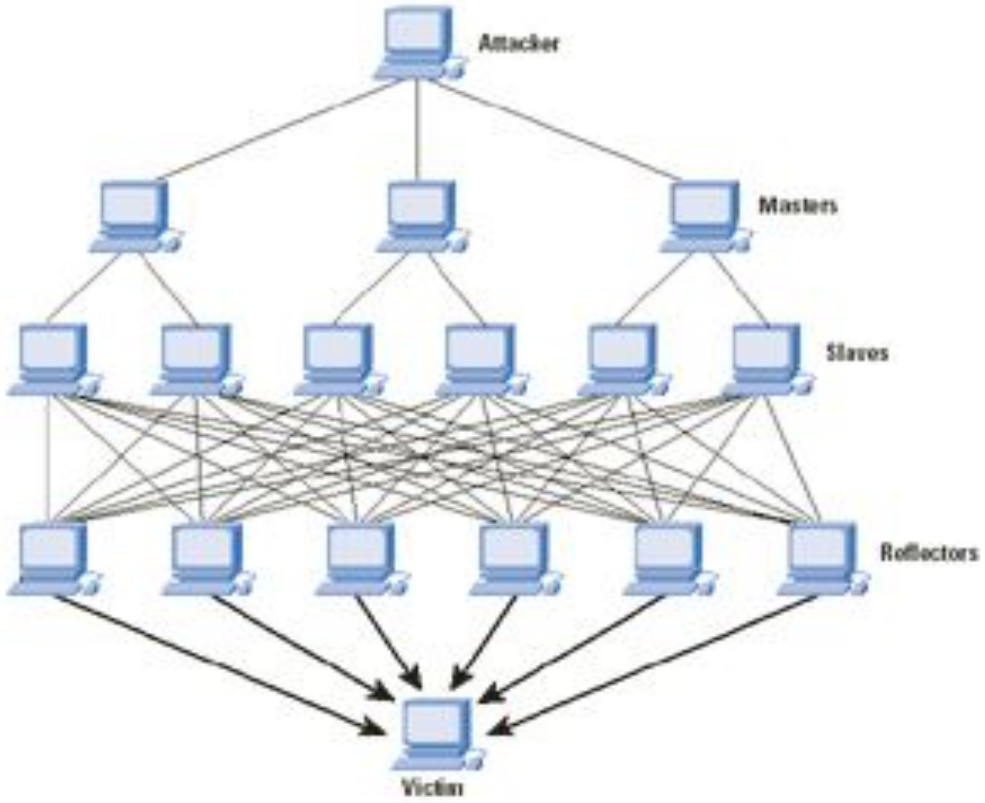

Рис. 2. Схема DRDoS-атаки

Атака типа "TCP SYN шторм"

Рассмотрим более конкретный пример проведения DoS-атаки, в которой используются особенности протокола TCP. Для установления логического соединения по протоколу TCP узлы должны обменяться тремя пакетами (рис. 3, а): сначала инициатор соединения посылает пакет с флагом SYN, на который сервер отвечает пакетом с установленными флагами ASK и SYN. Завершает процедуру пакет от узла-инициатора с флагом SYN.

Для выполнения атаки злоумышленник организует передачу на сервер массированного потока пакетов с флагом SYN, каждый из которых инициирует создание нового TCP-соединения (рис. 2, б). Получив пакет с флагом SYN, сервер выделяет для нового соединения необходимые ресурсы и в полном соответствии с протоколом отвечает клиенту пакетом с флагами ASK и SYN.

После этого, установив тайм-аут, он начинает ждать от клиента завершающий пакет с флагом ASK, который, увы, так и не приходит.

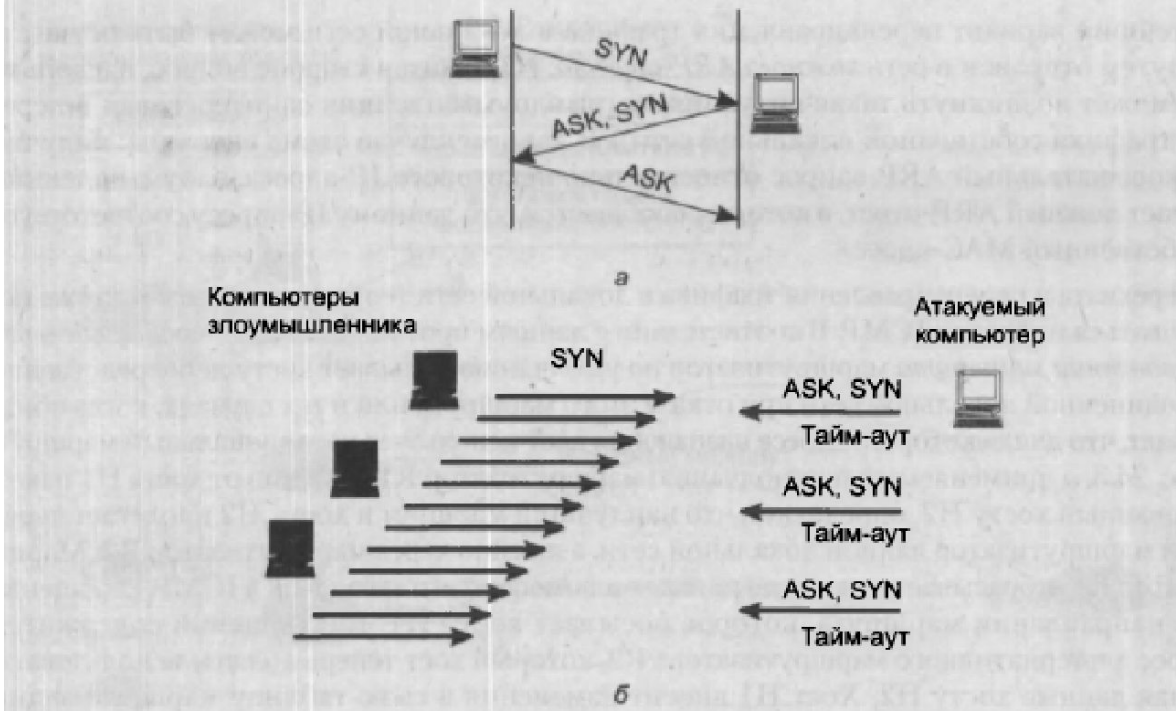

Рис. 3. Проведение DoS-атаки, в которой используются особенности протокола TCP:
а – нормальный порядок установления TCP – соединения;
б – DDoS – атака, создание множественных незакрытых TCP-соединений.

Атака типа "TCP SYN шторм"

Аналогичным образом создается множество других «недоустановленных» соединений. В результате возникает перегрузка сервера, все его ресурсы идут на поддержание множества соединений, процедуры установления которых остались незавершенными. В таком состоянии сервер уже не способен отвечать на запросы, посылаемые приложениями легальных пользователей, в результате злоумышленник достигает своей цели.

Подобный подход носит универсальный характер. Например, атака может быть осуществлена путем передачи уязвимому приложению потока запросов, синтаксически правильных, но специально сконструированных, так, чтобы вызвать перегрузку. Так, для некоторых версий веб-сервера Apache губительным оказывается поток запросов, каждый из которых содержит большое количество заголовков HTTP или символов «/». (Когда Web-сервер получает слишком много таких запросов, он может не справиться и выйти из строя).

Десятки известных примеров DDoS-атак описаны в http://www.ll.mit.edu/IST/ideval/docs/1999/attackDB.html.

Аналогичные атаки реализовывались с использованием UDP и ICMP лавин. Первая атака (UDP лавина) использует фальсифицированные пакеты, чтобы попытаться подключиться к допустимой UDP услуге и вызвать отклик, адресованный другому сайту. Системные администраторы не должны никогда допускать внешним UDP-дейтограммам попадать в диагностические порты их системы.

Перехват и перенаправление трафика

Следующий тип атак имеет целью направить трафик атакуемого компьютера по ложному адресу, в качестве которого может выступать адрес либо злоумышленника, либо третьей стороны. Потоком данных, который пользователь посылает, например, на свой корпоративный сервер или сервер банка, злоумышленник может распорядиться двумя способами. Первый состоит в том, что злоумышленник маскируется под сервера адресата, передавая клиенту ту «картинку» и те сообщения, которые тот ожидает. Так, злоумышленник может имитировать для пользователя-жертвы процедуру логического входа, получая при этом идентификатор и пароль пользователя. Эти данные в дальнейшем могут применяться для несанкционированного доступа к серверу предприятия или банка, которые и являются главной целью атаки. Второй способ заключается в организации транзита трафика. Каждый перехваченный пакет запоминается и/или анализируется на атакующем узле, а после этого переправляется на «настоящий» сервер. Таким образом весь трафик между клиентом и сервером пропускается через компьютер злоумышленника.

Простейший вариант перенаправления трафика в локальной сети может быть осуществлен путем отправки в сеть ложного ARP - ответа. (Оставим в стороне вопрос, насколько часто может возникнуть такая ситуация, когда злоумышленник заинтересован в перехвате трафика собственной локальной сети.) В данном случае схема очевидна: получив широковещательный ARP-запрос относительно некоторого IP-адреса, злоумышленник посылает ложный ARP-ответ, в котором сообщается, что данному IP-адресу соответствует его собственный MAC-адрес.

Для перехвата и перенаправления трафика в локальной сети теоретически может также использоваться протокол ICMP. В соответствии с данным протоколом ICMP-сообщение о перенаправлении маршрута маршрутизатор по умолчанию посылает хосту непосредственно присоединенной локальной сети при отказе этого маршрута.

Перехват и перенаправление трафика

Аналогичное происходит, когда протокол ICMP обнаруживает, что для некоторого адреса назначения хост использует нерациональный маршрут.

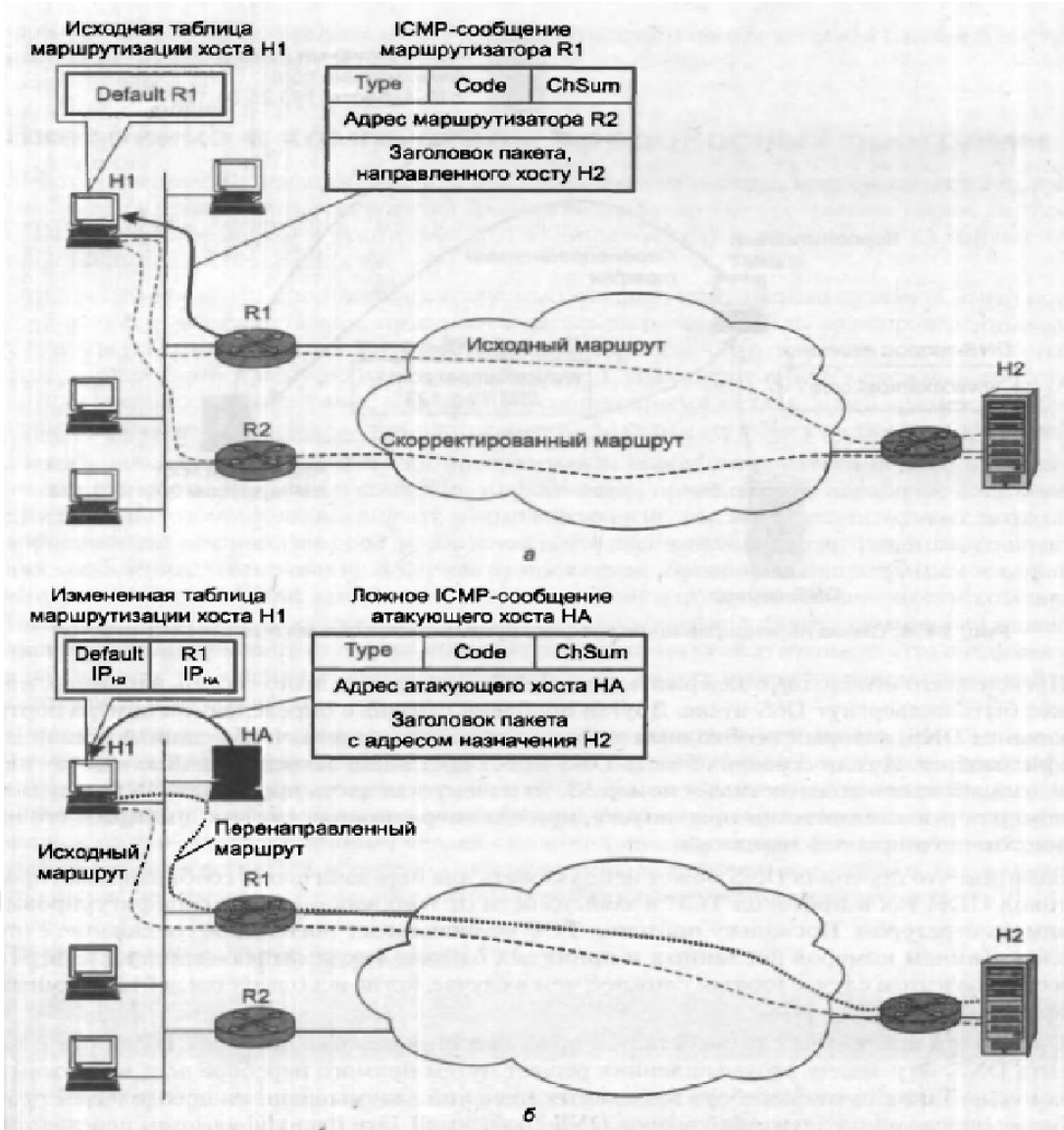

Рис. 4.Перенаправление маршрута с помощью протокола ICMP:
а – сообщение о более рациональном маршруте хосту H2 посылает маршрутизатор R1, применяемый по умолчанию;
б – сообщение о перенаправлении маршрута на себя направляет атакующий хост HA.

Перехват и перенаправление трафика

На рис. 4, а применяемый по умолчанию маршрутизатор R1, получив от хоста H1 пакет, адресованный хосту H2, определяет, что наилучший маршрут к хосту H2 пролегает через другой маршрутизатор данной локальной сети, а именно через маршрутизатор R2. Маршрутизатор R1 отбрасывает полученный пакет и помещает его заголовок в ICMP - сообщение о перенаправлении маршрута, которое посылает хосту H1. В сообщении содержится IP-адрес альтернативного маршрутизатора R2, который хост теперь должен использовать, посылая данные хосту H2. Хост H1 вносит изменения в свою таблицу маршрутизации и с этого момента отправляет пакеты хосту H2 по новому скорректированному маршруту. Для перехвата трафика, направляемого хостом H1 хосту H2, злоумышленник должен сформировать и послать хосту HI пакет, маскирующийся под ICMP - сообщение о перенаправлении маршрута (рис. 4, б). В этом сообщении содержится запрос о корректировке таблицы маршрутизации хоста H1, так чтобы во всех пакетах с адресом IP_{H2} адресом следующего маршрутизатора стал адрес IPha. являющийся адресом хоста-злоумышленника HA. Для того чтобы хост «поверил» этому сообщению, в поле IP-адреса отправителя должен быть помещен адрес маршрутизатора R1, являющегося маршрутизатором по умолчанию. Когда пакеты, передаваемые введенным в заблуждение хостом, начнут поступать на узел злоумышленника, он может либо захватывать и не передавать эти пакеты дальше, имитируя для поддержания диалога приложение, которому эти пакеты предназначались, либо организовать транзитную передачу данных по указанному адресу назначения IPн2-Читая весь трафик между узлами H1 и H2, злоумышленник получает все необходимую информацию для несанкционированного доступа к серверу H2.

Перехват и перенаправление трафика

Еще одним способом перехвата трафика является использование ложных DNS - ответов (рис. 5). Задача злоумышленника состоит в получении доступа к корпоративному серверу. Для этого ему нужно завладеть именем и паролем авторизованного пользователя корпоративной сети. Эту информацию он решает получить путем ответвления потока данных, которые корпоративный клиент посылает корпоративному серверу. Злоумышленник знает, что клиент обращается к серверу, указывая его символьное DNS-имя **www.example.com**. Известно ему также, что перед тем как отослать пакет серверу, программное обеспечение клиентской машины направляет запрос DNS-серверу, чтобы узнать, какой IP-адрес соответствует этому имени.

Цель злоумышленника — опередить ответ DNS-сервера и навязать клиенту свой вариант ответа, в котором вместо IP-адреса корпоративного сервера (в примере 193.25.34.125) злоумышленник указывает IP-адрес атакующего хоста (203.13.1.123). На пути реализации этого плана имеется несколько серьезных препятствий.

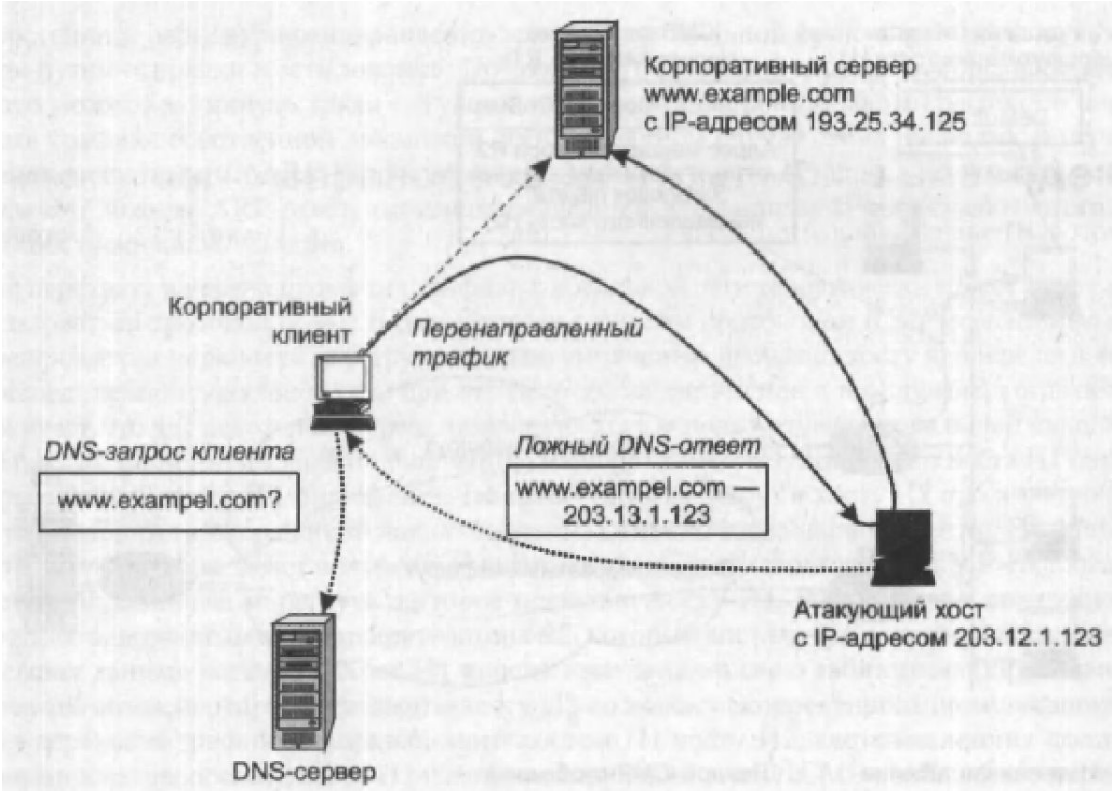

Рис. 5. Схема перенаправления трафика путем использования ложных DNS-ответов

Перехват и перенаправление трафика

Прежде всего необходимо задержать ответ DNS-сервера, для этого сервер, например, может быть подвергнут DoS-атаке. Другая проблема связана с определением номера порта клиента DNS, который необходимо указать в заголовке пакета, чтобы данные дошли до приложения. И если серверная часть DNS имеет постоянно закрепленный за ней так называемый «хорошо известный» номер 53, то клиентская часть протокола DNS получает номер порта динамически при запуске, причем операционная система выбирает его из достаточно широкого диапазона.

Заметим, что протокол DNS может использовать для передачи своих сообщений как протокол UDP, так и протокол TCP, в зависимости от того, как он будет сконфигурирован администратором. Поскольку протокол TCP устанавливает логическое соединение с отслеживанием номеров посланных и принятых байтов, «вклиниться» в диалог клиента и сервера в этом случае гораздо сложнее, чем в случае, когда используется дейтаграммный протокол UDP.

Однако и в последнем случае остается проблема определения номера UDP-порта клиента DNS. Эту задачу злоумышленник решает путем прямого перебора всех возможных номеров. Также путем перебора возможных значений злоумышленник преодолевает проблему определения идентификаторов DNS-сообщений. Эти идентификаторы передаются в DNS-сообщениях и служат для того, чтобы клиент системы DNS мог установить соответствие поступающих ответов посланным запросам. Итак, злоумышленник бомбардирует клиентскую машину ложными DNS-ответами, перебирая все возможные значения идентифицирующих полей так, чтобы клиент, в конце концов, принял один из них за истинный DNS-ответ. Как только это происходит, цель злоумышленника можно считать достигнутой — пакеты от клиента направляются на адрес атакующего хоста, злоумышленник получает в свое распоряжение имя и пароль легального пользователя, а с ними и доступ к корпоративному серверу.

Разработка средств детектирования и защиты

Разработка средств детектирования и защиты от DoS атак достаточно сложна. Разработчики должны думать заранее о каждой возможной ситуацией, так как любая слабость может быть использована во вред. Среди трудностей можно назвать:

- *DDoS-атаки перегружают машину-жертву пакетами*. Это означает, что жертвы не могут контактировать ни с кем, для того чтобы попросить помощи. Следовательно, любое ответное действие возможно только в случае, когда атака детектирована заранее. Но можно ли детектировать атаку раньше? Обычно трафик возрастает внезапно и без предупреждения (см. CERT on SMURF Attacks: http://www.cert.org/advisories/CA-1998-01.htm, CERT on TCP SYN Flooding Attacks: http://www.cert.org/advisories/CA-1996-21.html, CERT TRIN00 Report: http://www.cert.org/incident_notes/IN-99-07.html#trinoo). По этой причине механизм реакции должен быть быстрым.
- Любая попытка фильтрации входного трафика означает, что и легальный трафик может пострадать. С другой стороны, если число зомби исчисляется тысячами, трафик поглотит всю входную полосу и любая фильтрация станет бессмысленной.
- Атакующие пакеты обычно имеют фальсифицированные IP-адреса. По этой причине сложно отследить источник атаки. Более того, промежуточные маршрутизаторы или сервис- провайдеры могут отказаться сотрудничать при решении этой проблемы. При фальсификации адресов атака может происходить с очень большого числа машин и необязательно все они являются зомби.
- Механизмы защиты должны работать в разнообразной независимой от платформы программной среде. Использование ACL и репутационных списков в этом случае неэффективно (см. http://falcon.jmu.edu/~flynngn/whatnext.htm).

RFC - 2827

Появление атак DoS явилось новым вызовом для провайдеров (ISP) и для сетевого сообщества. Имеются многочисленные трудности на пути противодействия этим атакам; существуют некоторые простые средства, позволяющие ограничить эффективность этих атак и область их действенности, но они не очень широко используются (см. F. Baker and P. Savola, "Ingress Filtering for Multihomed Networks," RFC 3704, March 2004.).

В то время как **метод фильтрации**, обсуждаемый в документе RFC - 2827, не способен защитить от атак, которые осуществляются из зон с корректными префиксами IP-адресов, он позволяет заблокировать атаки, когда используются фальсифицированные адреса отправителя, не отвечающие входным правилам фильтрации. Все интернет провайдеры стремятся реализовать фильтрацию, описанную в данном документе, чтобы запретить злоумышленникам использовать фальсифицированные адреса отправителей, которые размещены вне пределов диапазона разрешенных префиксов. Другими словами, если Интернет провайдер агрегатирует маршрутные уведомления для последующих сетей, должно быть использована фильтрация, которая запрещает трафик, который исходит извне по отношению объявленному агрегатному пространству.

Дополнительным преимуществом использования этого типа фильтрации является то, что он позволяет отследить отправителя пакетов, так как злоумышленник будет вынужден использовать корректный и легально достижимый адрес отправителя.

DDoS-атаки

Если несколько лет назад атаки на сетевые объекты совершали в основном (около 90%) хулиганы, которые таким образом пытались самоутвердиться, сейчас вторжения на серверы и рабочие станции предпринимаются уже с корыстной. Речь не идет о вторжениях в банки (хотя и это бывает), все много прозаичнее, хакер взламывает большое число машин, выбирая наиболее уязвимые, и формирует базис для распределенных сетевых атак отказа обслуживания (**DDoS** - Distributed Denial of Service) на сервис-провайдеров или серверы фирм (заказы поступают от конкурентов), или для рассылки СПАМ'а, что стало в нашей стране достаточно прибыльным и относительно безопасным бизнесом. **К концу 2009 года предельные потоки DDoS-атак достигли 49 Гбит/с !** Для DDoS атаки сервера WilkiLeaks (www.wikileaks.org и cablegate.wikileaks.org опубликовавшего дипломатическую переписку и другие конфиденциальные данные) использован поток, превосходящий 10Гбит/с. ***DDoS-атаки стали одним из видов кибероружия.*** Наиболее известным программным средством для DDoS-атак является **LOIC** (Low Orbit Ion Cannon). К началу 2016 года стоимость DoS-атаки упала до 5$ за час.

Например, в ИТЭФ были вынуждены заниматься проблемами сетевой безопасности с 1995 года, когда несколько раз подверглись DoS-атакам. Маршрутизатор CISCO-4000 был достаточно тихоходен и при потоках более 2000 пакетов в секунду самоблокировался. Не имея специальных средств и навыков, на диагностику проблемы персонал в начале тратил более суток. Связано это с тем, что DoS-атаки чаще всего предпринимаются с использование фальсификации адреса отправителя. Две атаки были предприняты с ЭВМ из собственной локальной сети, взломанных ранее. Позднее такие объекты персонал научился локализовать за несколько минут. Для этого была написана специальная программа. Алгоритм этой программы доложен на конференции МаБИТ-03, МГУ октябрь 2003 год.

Дополнительные материалы для изучения

Но описанные атаки были вторичными. Оставалось не ясным, как взламывались ЭВМ-жертвы во внутренней локальной сети. Чтобы прояснить эту проблему, на входе сети ЭВМ, на которой сначала стояла программа t-meter, позднее поставили sniffer. Варьируя критерии отбора пакетов, удалось выявить IP-адреса машин, с которых производится сканирование адресов и портов ЭВМ внутренней сети Института. В настоящее время число атак из расчета на одну ЭВМ превышает 20-100/сутки.

В настоящее время по аналогичной методике анализируется поток атак на Межведомственный Суперкомпьютерный центр РАН. Для этого используется программа SNORT. При этом все данные об атаках автоматически записываются в базу данных, а по всем параметрам атаки строятся распределения (IP-адреса, порты, сигнатуры атак, время и т. д.). Для организации DDoS-атак обычно используется протокол UDP (хотя это и не является обязательным).

В последнее время (2015 г.) получили распространение DDoS атаки со стороны botnet Linux (XOR DDOS), которые способны иметь мощность, превышающую 150 Гбит/с (см. "**A Linux botnet is launching crippling DDoS attacks at more than 150Gbps**, Lucian Constantin). В первом полугодии 2016 года регистрировались до 2000 DDoS-атак ежедневно (см. "Application Security Trends For 2016", January 12, 2016, IndusFace).

Следует иметь в виду, что DDoS-атаки требуют немалых ресурсов, даже если они предпринимаются со взломанных машин (такие машины сегодня также стоят денег). По этой причине, если обычная рабочая станция может подвергнуться любой атаке, имеющей целью ее взлом, то DDoS-атаке сегодня подвергаются исключительно значимые бизнес или политические объекты (серверы новостей, финансовые учреждения, сервис-провайдеры, интернет-магазины и т.д.).

Дополнительные материалы для изучения

Рост возможности DoS-атак со временем (2002-2010гг) представлен на рис. 6.

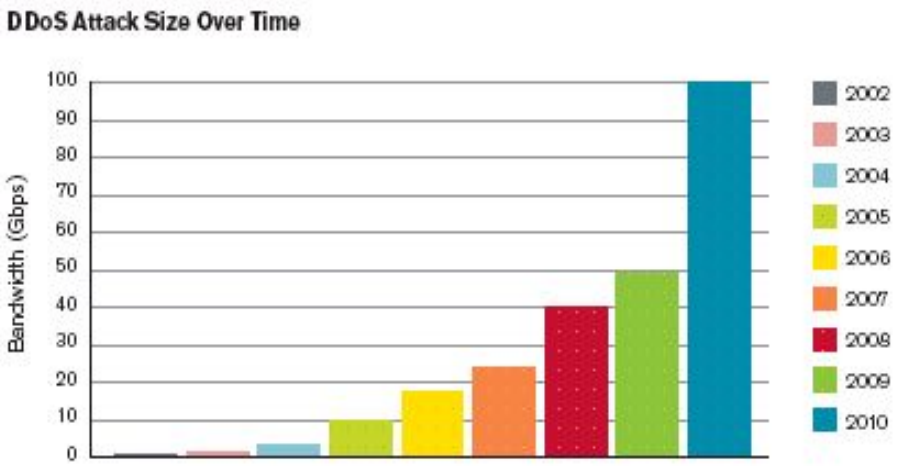

Рис. 6.

В общем потоке атак DoS-атаки занимают до 27%, см. 2014. The Danger Deepens. Neustar Annual DDoS Attacks and Impact Report.

Если в 2008 году мощность DDoS-атак достигала 40Гбит/с, то в 2014-ом превысила 400 Гбит/с. Ущерб от этих атак в 2012 году составил 1 млн. долларов в день (США).

Подмена субдомена DNS

В последнее время широкое распространение получили хакерские операции перехвата субдоменных имен (**DNS subdomain hijacking**). Это особенно легко сделать, если DNS-сервис является внешним по отношению к организации или фирме. Например, если имеется домен www.example.com, хакером создается субдомен cheap-drugs.example.com, который переадресует запросы на IP-адрес хакера. Перехват имен субдоменов может производиться самыми разными способами. Целью хакера является размещение своего вредоносного сайта в благонадежной на вид доменной области. Для хакера такой тип атак привлекателен тем, что он может поставить под удар большое число машин, даже защищенных Firewall или IPS. Среди жертв хакеров оказались домены apptech.com, cfi.gov.ar, eap.edu, fabius-ny.gov, haskell.edu (данные с сайта RechRepublic).

Особое внимание хакеров привлекают кэширующие серверы имен (**CNS** - Caching NameServer). См. DNS security best practices to prevent DNS poisoning attacks. При реализации рекурсивных запросов всегда есть возможность модификации запроса или отклика. Для решения этой проблемы был разработан протокол DNSSEC.

Отмечается, что поддержка протокола multicast DNS открывает широкие возможности для DDoS атак (см. "**Over 100,000 devices can be used to amplify DDoS attacks via multicast DNS**", Lucian Constantin, IDG News Service, April 1, 2015). Domain Name System (mDNS; RFC-6762 и RFC-6804) является протоколом, который позволяет устройствам в локальной сети распознавать друг друга и выявлять доступные виды сервиса. Поддержка протокола возможна также системами **NAS** (Network Attached Storage). К сожалению, практические реализации протокола не следуют строго его регламентациям, допускают выход запросов за пределы локальной судсети, что создает условия для DDoS-атак.

В зависимости от типа запроса mDNS может выдать данные об устройстве (модель, серийный номер, MAC-адрес и предоставляемых сервисах. Эти данные могут помочь хакеру спланировать будущую атаку. Этот протокол помогает организовать DoS-атаку, так как отклик всегда по размеру в несколько раз больше запроса.

Сокращение имени субдомена DNS

Некоторые сервис-провайдеры по ряду причин используют сокращенные имена субдоменов DNS для обозначения названия своих сервисов (например, в Twitter или e-mail). В последнее время сокращенное имя URL сервиса is.gd использовалось достаточно активно для переадресации клиентов на phishing-сайты. За время активности (см. рис. 7B) на сайт поступило 50 млрд. запросов. Ниже приведен пример ссылки-переадресации на вредоносный сайт:

http://is.gd/Tb###U?2.taobao.com/item.htm?spm=2007.1000337

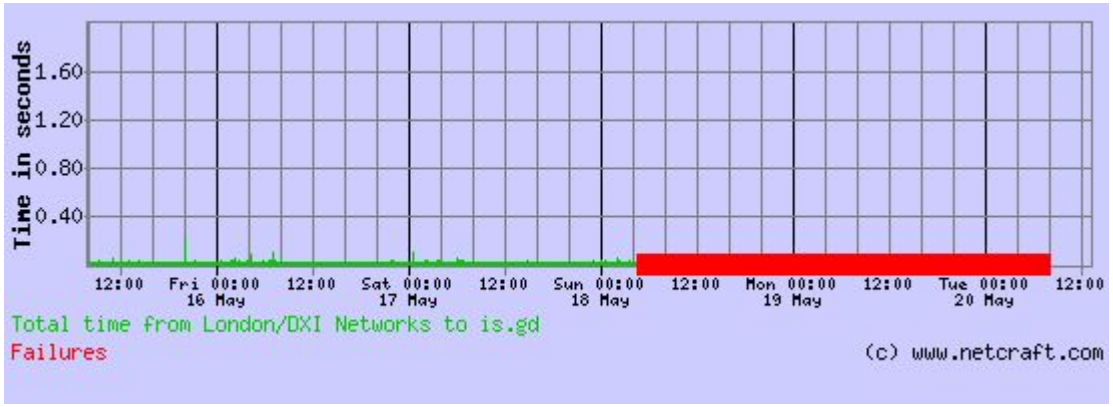

Рис. 7B. Активность субдомена is.gd (данные Netcraft)

На рис. 7С приведены доли 5 ведущих URL, использованных для переадресации на phishing-сайты.

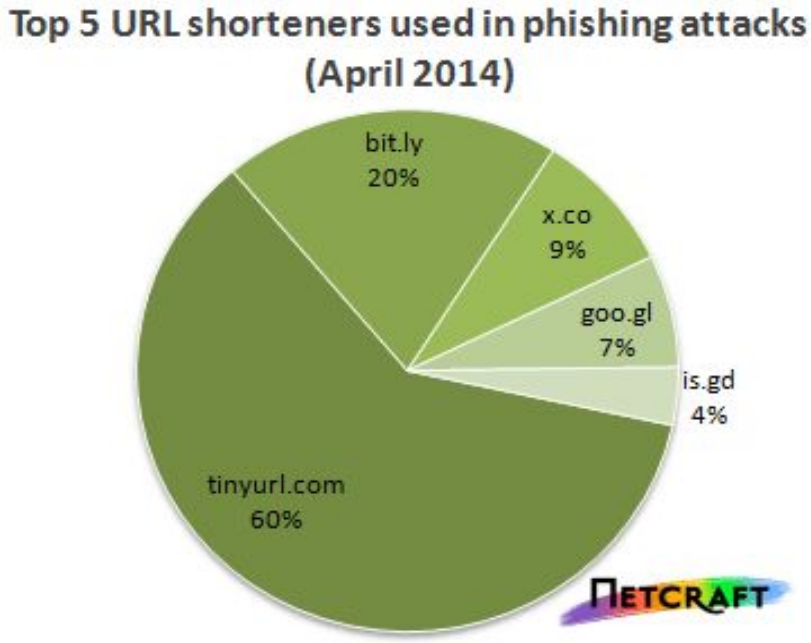

Рис. 7С. Доли сокращенных имен доменов, используемых для phishing-атак

Вывод прост сокращение имен доменов, используемых для названий сервисов, удобно, но почти всегда опасно для пользователей.

Чтобы быть в курсе того, что делается в вашем домене (здесь предполагается, что ваш домен имеет имя example.com), полезно время от времени использовать утилиту **dig**:
dig @a.iana-servers.net example.com axfr

Большую угрозу могут представлять фальсификации серверов обновления (WINDOWS, антивирусных библиотек и т.д.), так как при таком "обновлении" в ЭВМ жертвы может быть записана любая вредоносная программа.

MAC-flooding

Атака MAC-flooding относится к классу разведовательных атак. Этот вид атаки может использоваться также в качестве DoS-атаки. Атакующая машина забивает коммутатор (switch) огромным числом кадров с неверными MAC-адресами отправителя. Коммутаторы имеют ограниченную память для таблицы переадресации (MAC-порт) и при такой атаке таблица будет заполнена некорректными MAC-адресами, пришедшими от машины-атакера. При поступлении легального трафика из-за отсутствия соответствующих записей в таблице переадресации пакеты будут направляться на все выходы коммутатора. В результате атакер, взломавший машину, которая реализует данную атаку, получит большое количество ценной для него информации. Кроме того, это может вызвать перегрузку каналов и самого switch.

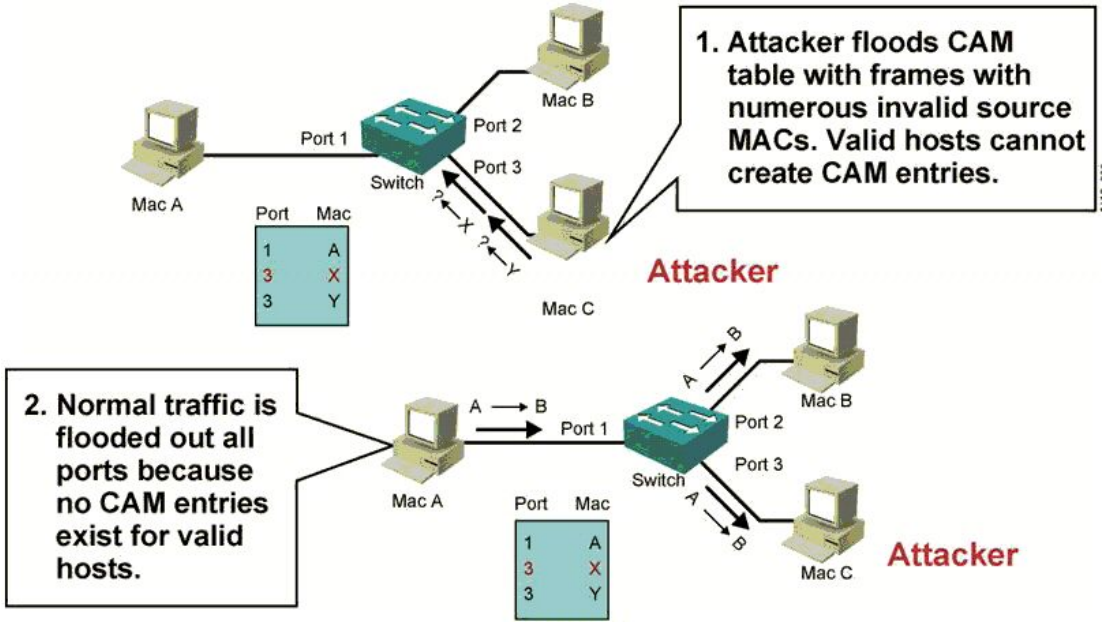

Рис. 7. Схема атаки MAC-flooding

Дополнительные материалы для изучения

Следует учитывать, что характер атак становится все более изощренным. Хакеры объединяются в клубы, издают журналы и продают хакерские CD. Сегодня крайне актуальным становится кооперирование их потенциальных жертв. Для профессиональных DDoS атак могут использоваться машины, взломанные ранее (зомби). Большие группы таких машин иногда называются армиями.

Обычно наибольшее внимание привлекают атаки из области вне локальной сети (SQL- или XSS-injection). Реально несравненно большую угрозу представляют визиты сотрудников в социальные сети (Facebook, Twitter и т.д.), e-mail phishing или drive-by download (так называетмые приглашенные атаки), а также атаки инсайдеров (сетевые объекты, работающие в области, защищенной сетевым экраном). *В случае посещения вредоносного сайта киберпреступники могут просканировать машину жертвы на предмет наличия известных уязвимостей*. Под инсайдером подразумеваются не только сотрудники, работающие в локальной сети, но также скомпрометированные машины LAN (например, посредством USB-флэшей или любых других переносимых носителей или laptop'ов). Классическим примером инсайдерской атаки является утечка данных госдепартаметна США, опубликованных на сервере WikiLeaks.

USB-флэш атака

По данным департамента обороны США возможны достаточно забавные атаки. Атакер изготовляет специальные USB-флэши, загружает в них специальное программное обеспечение и разбрасывает такие устройства в местах, где их могут найти сотрудники интересующих его организаций. Найденное устройство будет рано или поздно вставлено в компьютер дома или на службе и станет источником заражения сети, поставляя атакеру ценные сведения. Главная особенность атаки - практически полная безопасность атакера. Ведь даже если жертва отследит адрес, куда отсылаются данные, можно всегда утверждать, что организатора подставили, а доказать обратное будет проблематично.

На рис. 8 представлена диаграмма классификации угроз по степени их опасности. Смотри Unveiling the Security Illusion: the need for active network forensics. 95% посылаемых на WEB-сайты постов являются спамом или содержат вредоносные коды. 71% зараженных сайтов являются совершенно легальными (их создали не для заражения посетителей вредоносными кодами, данные конца 2009 года). *58% всех краж данных осуществляется через WEB-серверы*.

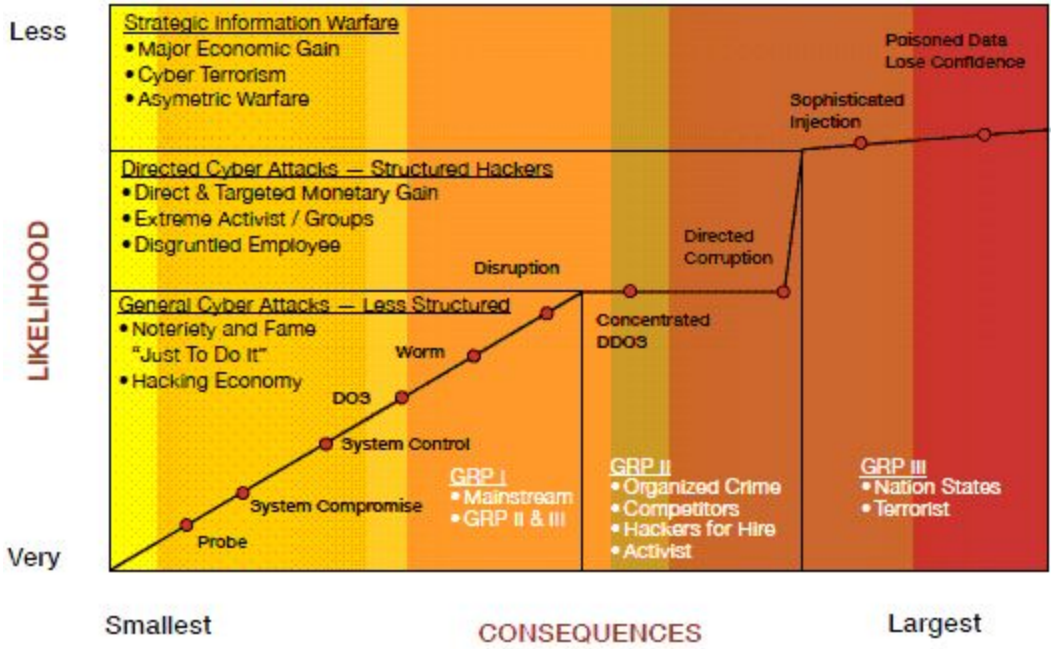

Рис. 8. Классификация различных угроз по их степени опасности

Дополнительные материалы для изучения

Впрочем, самыми опасными остаются неизвестные атаки неизвестного типа - *атаки нулевого дня*.

На рис. 9 видно, что все началось с сетевого хулиганства, стимулом которого было самоутверждение, (до 2004г это в основном вирусы и сетевые черви), а к 2010 году все вышло на высокий профессиональный уровень, где двигателем является алчность или политика, (APT, динамические, многофункциональные троянские кони и botnet с элементами стэлз).

Самое ужасное, потенциально опасные программные продукты стали разрабатывать вполне добропорядочные компании. Они это делают для реализации виртуальной рекламы своих продуктов, для получения данных о своих клиентах (их предпочтениях). Становится все труднее обнаружить отличие между чисто хакерскими творениями и такими встроенными объектами в совершенно нормальные программные приложения. Существует и российская фирма, специализирующаяся на разработке хакерских программ. РФ наверное единственная страна, где бизнесмены могут легально вести такой бизнес.

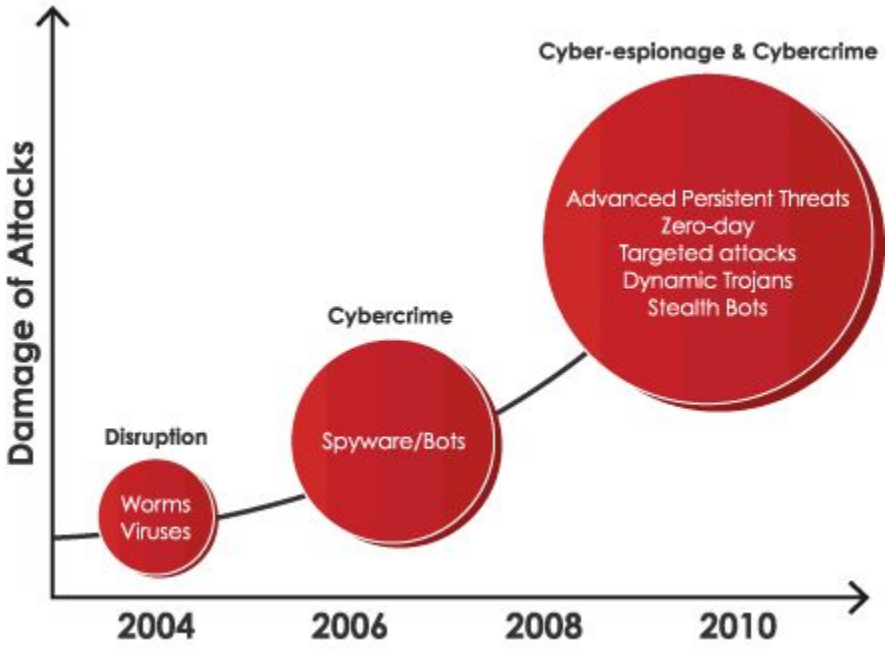

Рис. 9. Эволюция вредоносности атак со временем

Дополнительные материалы для изучения

Некоторые компании стали разрабатывать вредоносные программы на продажу, например, Mpack. Компания **DTC** (Dream Coders Team) продает этот продукт по цене до 1000$. При этом предлагается даже послепродажное обслуживание и обновление арсенала атак. Они утверждают, что это исследовательская программа, что-то вроде Nessus. В крайнем случае они оправдываются тем, что торгуют же люди оружием...

Согласно данным на начало 2007 года, если машина, подключенная к Интернет, остается незащищенной в течение 30 минут, с 50% вероятностью она окажется взломанной (станет зомби). В настоящее время по данным института SANS в мире существует около 3-3,5 миллионов таких зомби (и их число стремительно растет). Спрос на такие машины достаточно велик (для рассылки SPAM), цена 20000 машин зомби колеблется от 2 до 3 тысяч долларов США (и имеет тенденцию к падению из-за массовости производства). Машины делятся на группы примерно 20 ЭВМ в каждой и эти группы активируются поочередно. Каждая машина посылает по 630 сообщений в час. Именно это обстоятельство может свидетельствовать о том, что машина является зомби, ведь вряд ли кто-то способен подготовить и послать столько сообщения за час. По данным ФБР (США) ежегодний ущерб от киберпреступлений превышает 67 миллиардов долларов.

Дополнительные материалы для изучения

Почтовый протокол SMTP содержит в себе достаточно богатые возможности для хакеров. Прежде всего это касается приложений, написанных на WinWord или Exel. Дело в том, что просматривая такой документ вы видите лишь малую часть кодов в нем содержащихся. Сравните число символов текстового файла с образом того же файла в WinWord. Но это еще не все. В WinWord имеется возможность использования скриптов, написанных на Visual Basic (**VB**), которые могут использоваться для форматирования текста и для других самых разных целей. Но язык VB достаточно мощное средство, способное общаться через сеть с другими объектами. Но, просматривая приложение, написанное на WinWord, вы не будете даже предупреждены, что при этом на вашей машине исполняется какая-то программа. Про последствия этого можно только догадываться....

В мае 2006 года 21-летний Джинсон Джеймс Анчета (Ancheta) из пригорода Лос Анжелеса был приговорен к 57 месяцам тюрьмы и штрафу в 15000$ за создание сети машин-зомби с суммарным числом машин 400 000. Некоторые взломанные им машины принадлежали центру вооружений морской авиации США в Калифорнии. Анчета занимался продажей взломанных машин, рекламируя свой "товар" через Internet Relay Channel.

Мало зарегистрировать атаку, надо определить и корректно интерпретировать IP-адрес, откуда эта атака исходит. Чаще всего, имея IP-адрес, достаточно легко отследить путь атаки, например посредством *Trace Route*. Полезным может оказаться утилита NSLookup, а также служба Whois, которая позволяет определить сервис-провайдера атакера и его географическое положение. Существуют и специальные утилиты (базы данных), позволяющие с достаточной точностью определить географическое положение машины по ее IP-адресу (например, GeoIP). Но хакеры знают о таких возможностях и часто используют анонимные прокси-серверы, чтобы скрыть свой IP-адрес. Такие серверы могут создаваться на взломанных ранее машинах-зомби.

Дополнительные материалы для изучения

Новые возможности может дать абсолютное географическое позиционирование всех машин (GPS). Уже в 2008 году в США дорогостоящие покупки стало возможно сделать только с машин с географической привязкой. Это стимулируется также случаями потери или кражи портативных машин, где хранилась ценная конфиденциальная информация. Если IP- или MAC-адрес можно фальсифицировать, то систему GPS не обманешь. Впрочем здесь предстоит еще решить проблемы связи IP-адреса и географического положения.

Но существует класс атак с фальсификацией адреса отправителя, когда задачу определения IP-атакера решить затруднительно. Эта техника используется большинством атак отказа обслуживания (DoS), а также некоторыми другими (смотри RFC-2827 или http://book.itep.ru/6/rfc2827.htm).

Многие атакеры используют социальную инженерию и психологию, чтобы спровоцировать потенциальную жертву к действиям, которые нанесут ущерб. Например, год назад в ИТЭФ пришли письма, которые, если верить заголовку были посланы сетевым администратором. Приложение к письму было заархивировано, но для деархивации требовался ключ, который содержался в тексте письма. В самом письме говорилось, что приложение, содержит инструкцию по улучшению безопасности. Почтовый сервер ИТЭФ имеет антивирусную защиту. Но зашифрованность приложения препятствовала распознаванию сигнатуры вируса. Хотя здравый смысл подсказывает, что сетевому администратору не нужно шифровать сообщение, адресованное клиентам сети, среди пользователей нашлось около десятка простаков, которые попались на эту удочку.

Дополнительные материалы для изучения

Потенциальную угрозу безопасности могут представлять специальные вставки во встроенное программное обеспечение процессора, BIOS, аппаратную память микросхем-драйверов внешних устройств, операционной системы и приложений. Аналогичные угрозы представляют любые программы с неизвестными исходными кодами, включая обеспечение маршрутизаторов. Считывать данные можно путем регистрации электромагнитного излучения дисплея и других устройств ЭВМ, и даже анализируя звук при нажатии терминальных клавиш. Этим список способов несанкционированного доступа не исчерпывается. Но эти угрозы рассматриваются в специальных дисциплинах.

Если имеется несколько ЭВМ, объединенных в систему, и к этой системе имеет доступ определенное число удаленных клиентов, то наиболее уязвимыми являются соединения клиентов с этой системой. Хакеры стараются атаковать самое слабое звено в системе. Особенно уязвимы пользовательские, домашние ЭВМ. Зная это, некоторые банки предлагают своим клиентам удешевленные или даже бесплатные средства защиты (например, антивирусные программы). Некоторые корпорации и сервис-провайдеры предоставляют своим клиентам антивирусные программы и firewall.

Следует, впрочем, иметь в виду, что только 40% вредоносных кодов может быть детектировано современными антивирусными программами (данные на начало 2010 года; Yankee Group).

Принципы сигнатурного анализа сформировались в середине 90-х годов прошлого века. Число сигнатур атак превысило 3000 к 2005 году и их многообразие продолжало лавинообразно увеличиваться, достигнув в 2009 году двадцати миллионного масштаба. Каждый месяц фиксируется порядка 5000 новых сигнатур (2009). Имеет место динамический прогресс системы щит-меч.

Дополнительные материалы для изучения

С учетом полиморфизма проблемы перед разработчиками антивирусных и других аналогичных программ становятся все более сложными. Многие администраторы и хозяева сетей полагают, что до сих пор все обходилось. Главный аргумент - у них на серверах нет соблазнительной информации, а фирма является небольшой, чтобы стать мишенью атаки. Такая позиция рано или поздно приведет к серьезным потерям. Это касается не только компаний, имеющим конкурентов (о них позаботятся непременно), или структур, имеющих на серверах конфиденциальную информацию (например, государственные учреждения), но и сетей, которые на первый взгляд не должны быть привлекательными для хакеров. Анализ показывает, что *все общедоступные серверы* атакуются иногда по несколько тысяч раз в час (это уже на грани DoS-атаки), хотя ничего привлекательного на этих серверах нет и вся информация является общедоступной.

Рост числа сигнатур атак является фактором, работающим на стороне атакеров. Ведь все больше машинных ресурсов нужно на проверку. Этому способствует и усложнение новых сигнатур. Пока быстродействие машин росло достаточно быстро, это было не заметно. Но при выходе на скорости работы каналов передачи данных 10-100Гбит/с проблема стала весьма острой.

Прерывать работы по совершенствованию систем сетевой защиты нельзя. Рассчитывать на получение бесплатных разработок из Интернет наивно. Каждая вторая такая программа сама содержит в себе spyware! Поставщик антивирусной программы (особенно бесплатной версии) может быть сам разработчиком вируса или spyware.