Подписано к печати: 25.08.09г.

Свежайший номер!

От любителей — к профессионалам

КОМПЬЮТЕР

№7-8'2009

01796
Подписной индекс

Ботнеты: хакерские сети

Электронные книги

FTP-Drive: ФТП для любой программы

Фотошопинг: Apply Image Для красного платья

3G-Интернет в кармане

Tea: Чаепитие с музыкой

Создаем слайд-шоу

Википедия

Vista-2 или всё же Windows 7?

Управляй своим мобильным

Настройка установки Windows XP

Персональный мультизагрузочный диск

БОТНЕТЫ: преступные хакерские сети

В этой статье мы узнаем, что такое зомби-сети или ботнеты, как они формируются, кто и как наживается с их помощью, а также о том, каковы тенденции развития хакерских сетей будущего.

Ботнеты существуют уже около 10 лет, но, тем не менее, проблема ботнетов по-прежнему остается недооцененной. Многие пользователи (до тех пор пока им не отключат Интернет, пока они не обнаружат исчезновение денег с кредитных карточек или у них не украдут логин и пароль электронной почты) плохо ещё понимают, в чем состоит реальная угроза зомби-сетей.

Что такое ботнеты?

Ботнет – это сеть компьютеров, зараженных вредоносной программой поведения Backdoor. Backdoor'ы позволяют киберпреступникам удаленно управлять зараженными машинами (каждой в отдельности, частью компьютеров, входящих в сеть, или всей сетью целиком) без ведома пользователя. Такие программы называются ботами.

Ботнеты обладают мощными вычислительными ресурсами, являются грозным оружием и хорошим способом заработка денег для злоумышленников. При этом зараженными машинами, входящими в сеть, хозяин ботнета может управлять откуда угодно: из другого города, или даже с другой страны, а организация Интернета позволяет делать это анонимно.

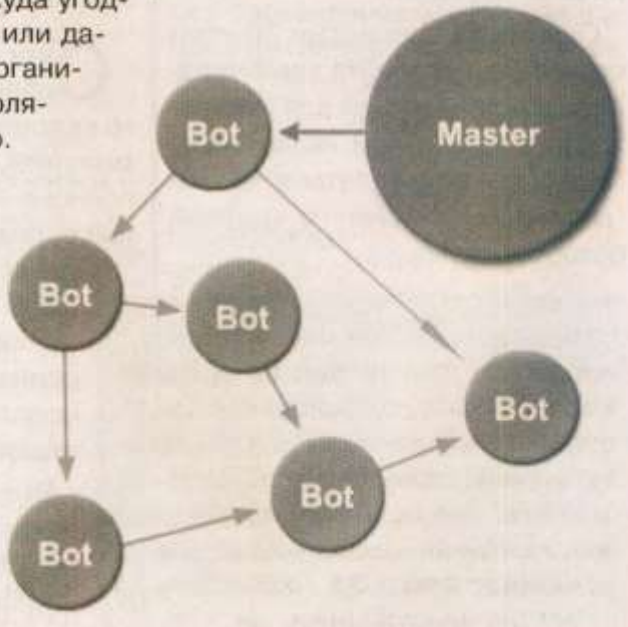
Управление компьютером, который заражен ботом, может быть прямым и опосредованным. В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело бота команды. В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду.

В любом случае хозяин зараженной машины, как правило, даже не подозревает о том, что она используется злоумышленниками. Именно поэтому зараженные вредоносной программой-ботом компьютеры, находящиеся под тайным контролем хакеров, называют еще зомби-компьютерами, а сеть, в которую они входят – зомби-сетью. Чаще всего зомби-машинами становятся персональные компьютеры обычных домашних пользователей, котоые не считают нужным платить деньги за антивирусную защиту и беспечно бороздят просторы Интернета.

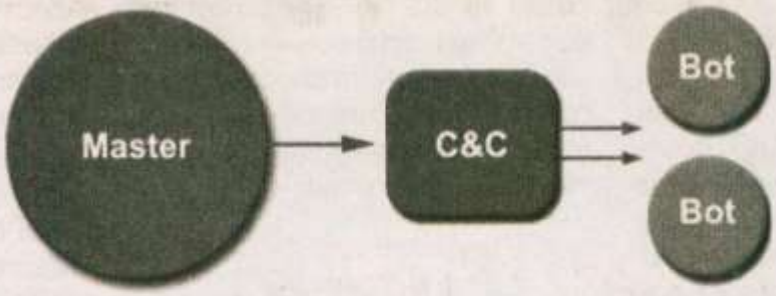
Зачем нужны ботнеты?

Ботнеты могут использоваться злоумышленниками для решения криминальных задач разного масштаба: от рассылки спама до атак на государственные сети. Но в основном они могут быть поделены на такие категории:

Рассылка спама. Это наиболее распространенный и один из самых простых вариантов эксплуатации ботнетов. В настоящее время более 80% спа-



ма рассылается с зомби-машин. Спам с ботнетов не обязательно рассылается владельцами сети. За определенную плату спамеры могут взять ботнет в аренду.



Именно спамеры могут по достоинству оценить эффективность ботнета: по статистическим данным, среднестатистический спамер зарабатывает 50-100 тысяч долларов в год. Многотысячные ботнеты позволяют спамерам осуществлять с зараженных машин миллионные рассылки в течение короткого времени.

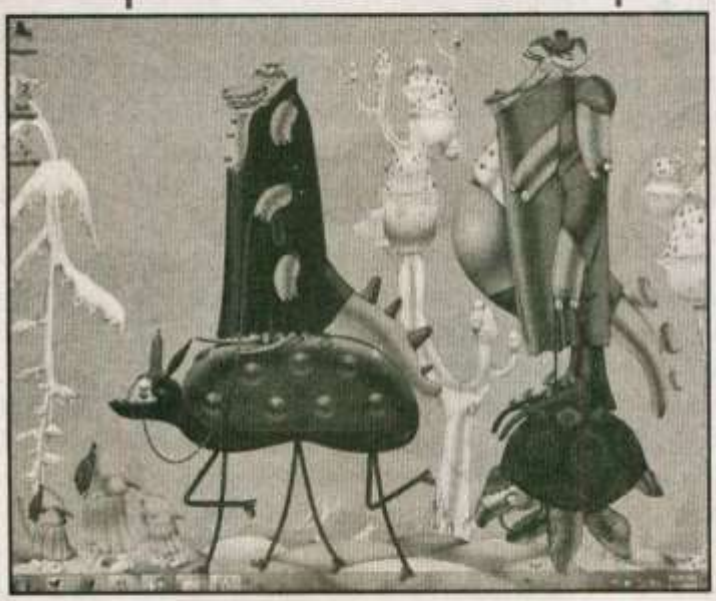
Кроме обеспечения скорости и масштабности рассылок, ботнеты решают еще одну проблему спамеров. Адреса, с которых активно рассылается спам, зачастую попадают в черные списки почтовых серверов, и письма, приходящие с них, блокируются или автоматически помечаются как спам.

Рассылка спама с сотен тысяч зомби-машин позволяет не использовать для рассылки одни и те же адреса. Еще одна изюминка ботнетов – возможность сбора адресов электронной почты на зараженных машинах. Украденные адреса продаются спамерам либо используются при рассылке спама самими хозяевами ботнета. При этом растущий ботнет позволяет получать новые и новые адреса.

Кибершантаж. Ботнеты широко используются и для проведения DDoS атак (Distributed Denial of Service – распределенная атака типа "отказ в обслуживании"). В ходе такой атаки с зараженных ботом машин создается поток ложных запросов на атакуемый сервер в Сети. В результате сервер из-за перегрузки становится недоступным для пользователей. За остановку атаки злоумышленники, как правило, требуют выкуп.

Сегодня многие компании работают только через Интернет, и для них недоступность серверов означает полную остановку бизнеса, что, естественно, приводит к финансовым потерям. Чтобы поскорее вернуть стабильность своим серверам, такие компании скорее выполнят требования шантажистов, чем обратятся в полицию за помощью. Именно на это и рассчитывают хакеры, поэтому DDoS-атак становится все больше.

Анонимный доступ в Сеть. Злоумышленники могут обращаться к серверам в Сети, используя зомби-машины, и от имени зараженных машин совершать киберпреступления, например, взламывать веб-сайты или переводить украденные денежные средства.



Продажа и аренда ботнетов. Один из вариантов незаконного заработка при помощи ботнетов основывается на сдаче ботнета в аренду или продаже готовой сети. Создание ботнетов для продажи является отдельным направлением киберпреступного бизнеса.

Фишинг. Адреса фишинговых страниц могут довольно быстро попасть в черные списки. Ботнет дает возможность фишерам быстро менять адрес фишинговой страницы, используя зараженные компьютеры в роли прокси-серверов. Это позволяет скрыть реальный адрес веб-сервера фишера.

Кража конфиденциальных данных. Этот вид криминальной деятельности, пожалуй, никогда не перестанет привлекать киберпреступников, а с помощью ботнетов улов в виде различных паролей и прочих конфиденциальных данных пользователей увеличивается в тысячи раз! Бот, которым заражены компьютеры в зомби-сети, может скачать другую вредоносную программу, например, троянца, ворующего пароли.

В таком случае инфицированными троянской программой окажутся все компьютеры, входящие в эту зомби-сеть, и злоумышленники смогут заполучить пароли со всех зараженных машин. Украденные пароли перепродаются или используются, в частности, для массового заражения веб-страниц (например, пароли для всех найденных FTP-аккаунтов) с целью дальнейшего распространения вредоносной программы-бота и расширения зомби-сети.

Типы ботнетов

Классификация ботнетов сегодня достаточна проста. Она основывается на архитектуре ботнетов и протоколах, используемых для управления ботами. До сих пор были известны лишь два типа архитектуры ботнетов:

Ботнеты с единым центром. В ботнетах с такой архитектурой

все зомби-компьютеры соединяются с одним центром управления, или C&C (Command&Control Centre). C&C ожидает подключения новых ботов, регистрирует их в своей базе, следит за их состоянием и выдает им команды, выбранные владельцем ботнета из списка всех возможных команд для бота. Соответственно, в C&C видны все подключенные зомби-компьютеры, а для управления централизованной зомби-сетью хозяину сети необходим доступ к командному центру.

Ботнеты с централизованным управлением являются самым распространенным типом зомби-сетей. Такие ботнеты легче создавать, ими легче управлять, и они быстрее реагируют на команды. Впрочем, бороться с ботнетами с централизованным управлением тоже легче: для нейтрализации всего ботнета достаточно закрыть C&C.

Децентрализованные ботнеты, или P2P-ботнеты (от англ. "peer-to-peer", что означает "соединение типа "точка-точка""). В случае децентрализованного ботнета боты соединяются не с центром управления, а с несколькими зараженными машинами из зомби-сети. Команды передаются от бота к боту: у каждого бота есть список адресов нескольких "соседей", и при получении команды от кого-либо из них он передает ее остальным, тем самым распространяя команду дальше. В этом случае злоумышленнику, чтобы управлять всем ботнетом, достаточно иметь доступ хотя бы к одному компьютеру, входящему в зомби-сеть.

На практике построение децентрализованного ботнета не очень удобно, поскольку каждому новому зараженному компьютеру необходимо предоставить список тех ботов, с которыми он будет связываться в зомби-сети. Гораздо проще сначала направить бот на централизованный сервер, где он получит список ботов-"соседей", а затем уже переключить бот на взаимодействие через P2P-подключения.

Команды для ботов в ботнетах

Команды, которые выполняют боты, бывают самые разные, но, как правило, они входят в нижеприведенный список. Названия команд могут отличаться в разных реализациях ботов, но суть остается той же. Итак, команды:

Update: загрузить и выполнить указанный исполняемый файл или модуль с указанного сервера. Эта команда является базовой, поскольку именно она реализуется в первую очередь. Она позволяет обновлять исполняемый файл бота по приказу хозяина зомби-сети, в случае если хозяин хочет установить модернизированную версию бота. Эта же команда позволяет заражать компьютер другими вредоносными программами (вирусами, червями), а также устанавливать другие боты на компьютер.

Flood: начать процесс создания потока ложных запросов на указанный сервер в Сети с целью вывода из строя сервера или перегрузки интернет-канала указанного сегмента глобальной Сети. Создание подобного потока может вызывать серьезные неполадки сервера, приводящие к его недоступности для обычных пользователей. Такой тип атаки с использованием ботнетов носит название DDoS-атаки.

Spam: загрузить шаблон спам-сообщения и начать рассылку спама на указанные адреса (для каждого бота выделяется своя порция адресов).

Proxy: использовать данный компьютер как прокси-сервер. Зачастую эта функция не выделяется в отдельную команду, а сразу включается в общий функционал бота. Это одна из прикладных функций, позволяющая использовать любой компьютер из ботнета как прокси-сервер с целью сокрытия реального адреса злоумышленника, управляющего ботнетом.

Существуют и другие команды, однако они не входят в число наиболее популярных и поэтому реализованы лишь в отдельных ботах.

Для передачи боту команд хозяина ботнета необходимо, как минимум, установить сетевое соединение между зомби-компьютером и компьютером, передающим команду. Все сетевые взаимодействия основаны на сетевых протоколах, определяющих правила общения компьютеров в сети. Поэтому существует классификация ботнетов, основанная на используемом протоколе общения.

По типу используемых сетевых протоколов ботнеты делятся на следующие группы:

IRC-ориентированные. Это один из самых первых видов ботнетов, где управление ботами осуществлялось на основе IRC (Internet Relay Chat). Каждый зараженный компьютер соединялся с указанным в теле программы-бота IRC-сервером, заходил на определенный канал и ждал команды от своего хозяина.

IM-ориентированные. Не очень популярный вид ботнетов. Отличается от своих IRC-ориентированных собратьев только тем, что для передачи данных используются каналы IM-служб (Instant Messaging), например AOL, MSN, ICQ и др. Невысокая популярность таких ботнетов обусловлена сложностями, возникающими при создании отдельного аккаунта IM-службы для каждого бота

Веб-ориентированные. Относительно новая и быстро развивающаяся ветвь ботнетов, ориентированная на управление через www. Бот соединяется с определенным веб-сервером, получает с него команды и передает в ответ данные. Такие ботнеты популярны в силу относительной легкости их разработки, большого числа веб-серверов в Интернете и простоты управления через веб-интерфейс.

Другие. Кроме перечисленных выше существуют и другие виды ботнетов, которые соединяются на основе своего собственного протокола, базируясь лишь на стеке протоколов TCP/IP: используют лишь общие протоколы TCP, ICMP, UDP.

Эволюция ботнетов

История ботнетов началась в 1998-1999 годах, когда появились первые программы поведения **Backdoor** – небезызвестные **NetBus** и **BackOrifice 2000**. Это были концепты, т.е. программы, в которых реализованы принципиально новые технологические решения. **NetBus** и **BackOrifice2000** впервые несли полный набор функций удаленного управления зараженным компьютером, что позволяло злоумышленникам работать с файлами на удаленном компьютере, запускать новые программы, получать снимки экрана, открывать/закрывать CD-привод и т.д.

Изначально созданные как троянские программы, бэкдоры работали без разрешения или уведомления пользователя. Для управления зараженным компьютером злоумышленник должен был сам установить соединение с каждой инфицированной машиной. Первые бэкдоры работали в локальных сетях на основе стека протоколов TCP/IP и, по сути, являлись демонстрацией вариантов использования Windows API для удаленного управления компьютером.

Клиентские программы для удаленного управления компьютерами уже в начале 2000-х могли одновременно управлять сразу несколькими машинами. Однако, в отличие от современных бэкдоров, программы NetBus и BackOrifice2000 выступали в роли сетевого сервера: они открывали определенный порт и пассивно ждали подключений хозяина (Backdoor'ы, используемые для построения ботнетов сегодня, устанавливают соединения сами).

Затем кто-то из злоумышленников придумал сделать так, чтобы зараженные бэкдорами компьютеры сами выходили на связь и их всегда можно было видеть онлайн (при условии, что они включены и работают). Скорее всего, этот "кто-то" был хакером, потому что боты нового поколения использовали традиционный для хакеров канал связи – IRC (Internet Relay Chat).

Вероятно, разработку новых ботов сильно упростило то, что в самой системе IRC изначально функционировали боты с открытым исходным кодом, но не направленные на удаленное управление системой, а с другим функционалом (эти программы отвечали на запросы пользователей, например, выдавали информацию о погоде или о времени последнего появления определенного пользователя в чате).

Компьютеры, зараженные новыми ботами, стали соединяться с IRC-серверами, в качестве посетителей выходить на связь через определенный IRC-канал и ждать указаний от хозяина ботнета. Хозяин мог в любое время появиться онлайн, увидеть список ботов, отослать команды сразу всем зараженным компьютерам или отправить отдельное сообщение одной машине. Это был первый механизм реализации ботнета с централизованным управлением, позже названный C&C (Command & Control Centre).

О появлении IRC-ботнетов стало известно довольно быстро. Как только о них появились публикации в хакерских журналах,

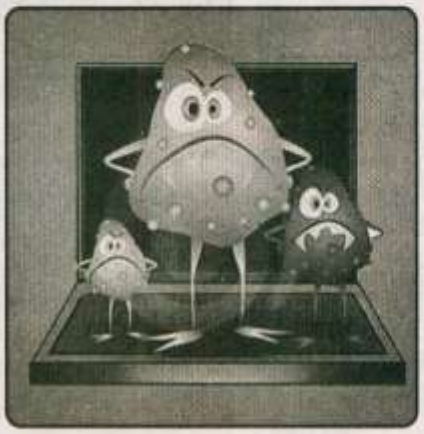
появились "угонщики" ботнетов, люди, которые обладали, возможно, теми же знаниями, что и владельцы ботнетов, но охотились за более легкой наживой. Они искали такие IRC-каналы, где было подозрительно много посетителей, заходили на них, изучали и "угоняли" ботнет: перехватывали управление сетью, перенаправляли боты на другие, защищенные паролем, IRC-каналы и в результате получали полный единоличный контроль над "чужой" сетью зараженных машин.

Следующим этапом развития ботнетов стало перемещение центров управления во всемирную паутину. Сначала хакеры разработали средства удаленного управления сервером, которые были основаны на таких популярных скрипт-движках, как Perl и PHP. Затем кто-то создал такое соединение компьютера в локальной сети с сервером в Интернете, которое позволяло откуда угодно управлять компьютером.

Схема удаленного управления компьютером в локальной сети в обход таких средств защиты, как прокси и NAT, была опубликована в Интернете и быстро стала популярной в определенных кругах. Удаленное управление было основано на установлении HTTP-соединения с управляющим сервером с использованием локальных настроек компьютера.

Полулегальные разработки средств удаленного управления, направленные на получение в обход защиты удаленного доступа к машинам в локальных сетях, дали толчок к созданию веб-ориентированных ботнетов. Чуть позже был разработан простой скрипт управления небольшой сетью компьютеров, а злоумышленники нашли способ использовать такие управляемые сети в корыстных целях.

На этом эволюция ботнетов не закончилась. Перебрав варианты использования протоколов, разработчики ботнетов переключились на архитектуру сети. Оказалось, что ботнет классической архитектуры (много ботов и один центр управления) чрезвычайно уязвим, так как зависит от критического узла – центра управления, при отключении которого сеть можно считать потерянной. Решения в виде одновременного заражения компьютеров разными ботами, ориентированными на разные центры управления, иногда срабатывают, но такие ботнеты гораздо сложнее поддерживать, поскольку нужно следить сразу за двумя-тремя центрами управления.



☺ ☺ ☺

– Как будет по-английски «без окон, без дверей»?

– «Ноу Виндоус, ноу Гейтс»!

Весьма эффективными и опасными с точки зрения экспертов могут стать ботнеты с архитектурой P2P, в которых центра управления нет. Владельцу сети достаточно дать команду одной из машин, дальше боты передают команду сами. В принципе каждый компьютер в ботнете может соединиться с любым другим компьютером, входящим в ту же сеть. Эксперименты по созданию таких ботнетов проводились довольно давно, однако первый крупномасштабный ботнет на основе P2P-архитектуры появился только в 2007 году. И именно P2P-ботнеты сейчас занимают внимание исследователей информационной безопасности.

Заключение

На сегодняшний день ботнеты являются одним из основных источников нелегального заработка в Интернете и грозным оружием в руках злоумышленников. Ожидать, что киберпреступники откажутся от столь эффективного инструмента, не приходится. Эксперты по безопасности с тревогой смотрят в будущее, ожидая дальнейшего развития ботнет-технологий.

Опасность ботнетов усугубляется тем, что их создание и использование становится все более простой задачей, с которой в ближайшем будущем будут в состоянии справиться даже школьники. А цены на развитом и структурированном ботнет-рынке весьма умеренные.

В построении интернациональных ботнетов могут быть заинтересованы не только киберпреступники, но и государства, готовые использовать зомби-сети как инструмент политического давления. Кроме того, возможность анонимно управлять зараженными машинами вне зависимости от их географического нахождения позволяет провоцировать конфликты между государствами: достаточно организовать кибератаку на серверы одной страны с компьютеров другой.

Сети, объединяющие ресурсы десятков, сотен тысяч, а порой и миллионов зараженных машин, обладают очень опасным потенциалом, который (к счастью!) пока не использовался в полном объеме. Между тем, вся эта грозная кибермощь опирается на инфицированные компьютеры домашних пользователей. Именно они составляют подавляющее большинство зомби-машин, и именно их злоумышленники используют в своих целях.

Андрей Оселедько