электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.491.2

Современные угрозы бот-сетей

Гончаров Н.О., *студент*
кафедра «Информационная безопасность»,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана

Научный руководитель: Троицкий И.И., к.т.н, доцент,
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Введение

Телекоммуникационная сеть - это сеть обмена и распределенной обработки информации, образуемая множеством взаимосвязанных абонентских систем и средств связи. Структура телекоммуникационной сети приведена на рис. 1.

Абонентская система - это совокупность ЭВМ, программного обеспечения, периферийного оборудования, средств связи с коммутационной подсетью.

Коммутационная подсеть - представляет собой совокупность физической среды передачи информации, аппаратных и программных средств, обеспечивающих взаимодействие абонентских систем.

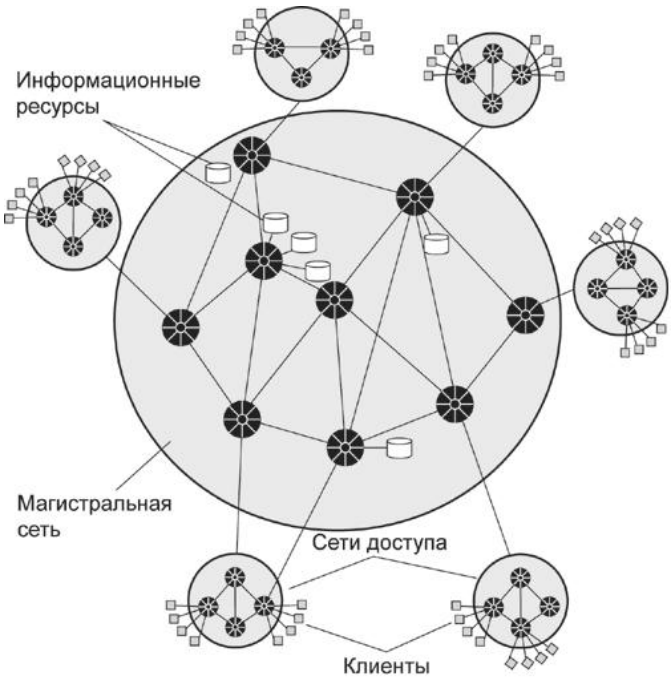


Рис. 1. Структура телекоммуникационной сети

Бот-сеть – это сеть компьютеров и других мобильных устройств, зараженных вредоносной программой, которая позволяет злоумышленникам удаленно управлять зараженными машинами без ведома пользователя.

Архитектуру бот-сетей обычно подразделяют на два основных типа – с централизованной и с децентрализованной топологией. Иногда добавляют ещё один, смешанный тип, объединяющий в себе черты двух первых, однако ничего принципиально нового в нём нет.

1. Архитектура бот-сетей с централизованной топологией управления

Централизованная топология (единый центр управления, C&C – Command & Control Centre). Все заражённые устройства подсоединяются к одному главному узлу. Центр управления следит за состоянием подключенных ботов, накапливает собираемые ими данные и выдает команды, а также постоянно ожидает подключения новых ботов, регистрируя их в своей базе. Для управления сетью злоумышленнику необходим доступ к C&C. Такой тип бот-сетей является на сегодня самым распространенным, поскольку их легче создавать и ими удобнее эффективно управлять. Структура централизованной бот-сети рассмотрена на рис. 2. Ликвидация узла C&C означает блокирование всей бот-сети, а для получения контроля достаточно перехватить управление центром.

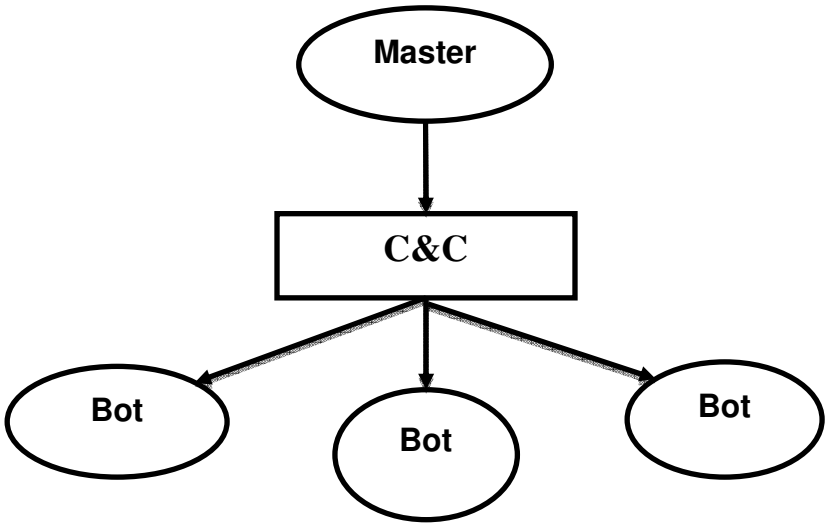


Рис. 2. Архитектура бот-сетей с централизованной топологией управления

2. Архитектура бот-сетей с децентрализованной топологией управления

Децентрализованная топология. Здесь боты соединяются не с единым центром управления, а с несколькими соседними, также зараженными машинами по известному принципу peer-to-peer. Структура децентрализованной бот-сети рассмотрена на рис. 3.

Ликвидировать или заполучить такую сеть гораздо труднее, поскольку владельцу для управления всей бот-сетью достаточно иметь доступ хотя бы к одной из заражённых машин. С другой стороны, управлять P2P бот-сетью не так удобно, как сетью с C&C.

На практике построение децентрализованной бот-сети не очень удобно, поскольку каждому новому зараженному компьютеру или устройству необходимо предоставить список тех ботов, с которыми он будет связываться в бот-сети. Чаще всего бота сначала направляют на централизованный сервер, где он получит список соседних ботов, а затем переключают его на взаимодействие через P2P-подключения. Такая смешанная топология также относится к типу P2P, хотя на отдельном этапе боты используют C&C. Бороться с децентрализованными бот-сетями гораздо сложнее, поскольку отсутствует единый центр управления.

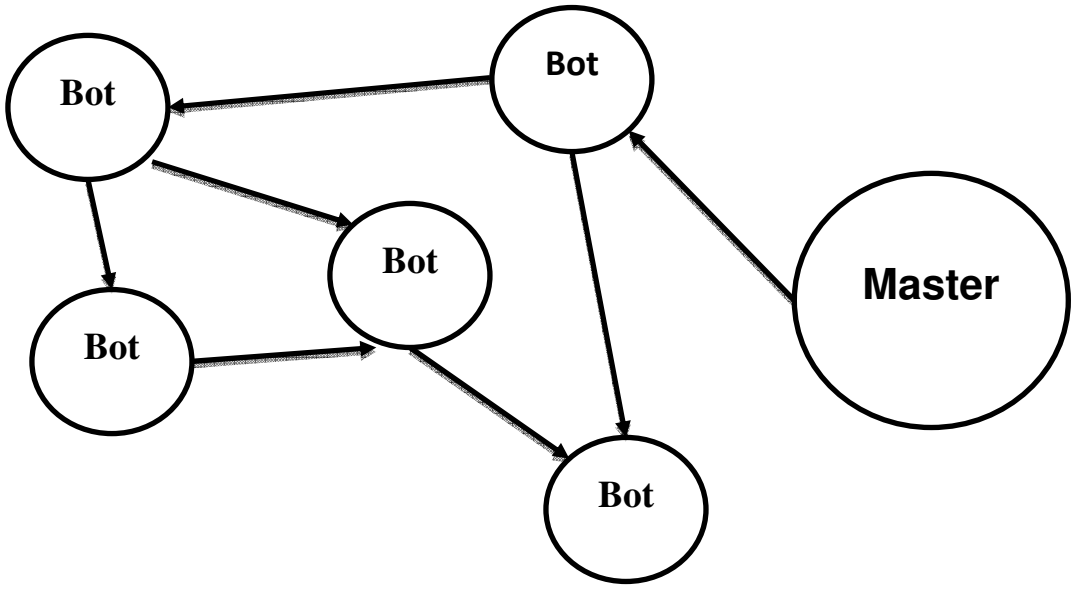


Рис. 3. Архитектура бот-сетей с децентрализованной топологией управления

3. Классификация бот-сетей по используемым сетевым протоколам

Для передачи команд боту, владельцу бот-сети необходимо установить сетевое соединение между заражённым компьютером или устройством и компьютером, передающим команду. Все сетевые взаимодействия основаны на сетевых протоколах, определяющих правила общения компьютеров в сети. Поэтому существует классификация бот-сетей, основанная на используемом протоколе общения.

IRC-ориентированные - это вид бот-сетей, где управление ботами осуществляется на основе IRC (Internet Relay Chat). Каждый зараженный компьютер соединялся с указанным в теле программы-бота IRC-сервером, заходит на определенный канал и ждёт команды от своего владельца.

IM-ориентированные - отличается от IRC-ориентированных тем, что для передачи данных используются каналы IM-служб (Instant Messaging), например AOL, MSN, ICQ и др. Невысокая популярность таких бот-сетей обусловлена сложностями, возникающими при создании отдельного аккаунта IM-службы для каждого бота. Дело в том, что боты должны выходить в Сеть и постоянно присутствовать онлайн. Поскольку большинство IM-служб не позволяют входить в систему с разных компьютеров, используя один и тот же аккаунт, у каждого бота должен быть свой номер IM-службы. При этом владельцы IM-служб всячески препятствуют любой автоматической регистрации аккаунтов. В результате владельцы IM-ориентированных бот-сетей сильно ограничены в числе имеющихся зарегистрированных аккаунтов, а значит и в числе ботов, одновременно присутствующих в сети. Такая сеть реагирует на команды очень медленно.

Веб-ориентированные - самый распространённый на сегодняшний день тип бот-сетей, ориентирован на управление через веб-сервисы и сервера. Бот соединяется с определенным веб-сервером, получает с него команды и передает в ответ данные. Такие бот-сети популярны в силу относительной легкости их разработки, большого числа веб-серверов в Интернете и простоты управления через веб-интерфейс.

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

4. Проблемы и угрозы Бот-сетей

Бот-сети несут в себе следующие угрозы:

- Похищение персональных данных и конфиденциальных данных.
- Фишинг.
- Рассылка спама.
- Осуществление спам-рассылок.
- Анонимный доступ в Сеть.
- Кибершантаж и осуществление DDoS-атаки.
- Похищение денег.

По подсчетам экспертов приблизительно 80% спама рассылается как раз при помощи бот-сетей. Среднестатистический злоумышленник зарабатывает приблизительно 50-100 тысяч долларов в год на таких сетях. Бот-сети, предназначенные для рассылки спама, так же могут собирать адреса электронной почты на зараженных машинах.

Кибершантаж один из самых широко применяемых способов использования бот-сетей. Злоумышленники проводяи широкомасштабные DDoS-атак (Distributed Denial of Service, распределённая атака типа отказ в обслуживании). В ходе такой атаки с заражённых компьютеров и мобильных устройств на сервер посылается большой поток ложных запросов до тех пор, пока сервер не будет перегружен и станет не доступен пользователям, после чего владельцы бот-сети требуют выкуп за остановку атаки на сервер.

Бот-сети позволяют злоумышленникам получать анонимный доступ в Сеть. Это позволяет им от имени зараженных компьютеров осуществлять взлом сайтов, кражу денег с банковских счетов и т.д.

Фишинг **-** в переводе с английского фишинг означает – рыбная ловля, выуживание – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Бот-сеть позволяет злоумышленникам быстро менять адрес фишинговой страницы, используя зараженные машины в качестве прокси-серверов, и при этом скрывать реальный адрес страницы.

Кража конфиденциальных данных **–** один из видов использования бот-сети, который позволяет красть всевозможные данные пользователей, которые потом перепродаются или используются для массового заражения веб-страниц с целью расширения бот-сети.

5. Перспективы развития и использования бот-сетей

Самой распространённой угрозой за последний год является кража средств со счетов абонента и прикреплённых через системы мобильного банкинга кредитных карт.

В конце лета 2013 года был обнаружена бот-сеть, использующий функции технологии мобильной коммерции «мобильный платеж». Общая схема по работе такой бот-сети такова:

1. Злоумышленник распространял своего трояна с помощью SMS-рассылок на мобильные телефоны по базам сотовых операторов.
2. Установленные трояны перехватывали все SMS и отправляли их на сервер злоумышленника.
3. На своем сервер злоумышленник смотрит сообщения, показывающие, что у клиента есть карта или счет в банке привязанный к этому номеру телефона.

4. Как только злоумышленник находит такой номер телефона, то он, отправляя специальные SMS-команды, переводил деньги со счета жертвы на телефон жертвы, при этом все уведомления от банка просто скрывались трояном на телефоне.

5. Далее с помощью тех же СМС, злоумышленник переводит деньги с баланса пополненного телефона жертвы на другие номера или электронные кошельки.

Схема является простой и не требует ничего сложного. Всем этим функционалом обладают трояны, которые ранее использовались для отправки SMS на премиум номера.

Опасность бот-сетей усугубляется тем, что их создание и использование становится все более простой задачей, с которой в ближайшем будущем будет в состоянии справиться любой желающий.

Перспективы использования мобильных бот-сетей будут привлекать все большее количество злоумышленников. В последние полгода каждые два месяца фиксируется появление новой преступной группы с собственной мобильной бот-сетью. Таких групп будет все больше, троянские программы будут все совершеннее, а методы и объемы их распространения будут стремится к результатам распространения обычных вредоносных программ.

6. Заключение

Современное развитие телекоммуникационных сетей связи и мобильного ПО намного упрощает задачу быстрого развёртывания бот-сетей. Уязвимости в мобильных ОС(в частности самой распростанённой - Android) позволяют беспрепятственно распространять вредоносное ПО.

Современные бот-сети умело маскируются, постоянно меняют доменные имена центров управления. Многие бот-сети используют случайно сгенерированные доменные имена центров управления, однако владелец регистрируемых имен в системе остается одним. За час может быть сгенерировано огромное количество доменных имён, каждое из которых может являться центром управления. Многие алгоритмы и методы защиты от бот-сетй основываются на сигнатурной базе в данном случае будут неэффективными.

Также основываясь на том, что у нас нет возможности контролировать всё программное обеспечение, устанавливаемое на устройства, которые работают в сети, оптимальным решением будет на первом этапе анализировать DNS-трафик. Это позволит обнаружить даже неизвестные ранее бот-сети, отслеживая лишь малую часть сетевого трафика. Для того, чтобы своевременно применять меры защиты, необходимо эффективно выявлять заражённых бот-программой устройства и предполагаемые центры управления. Только так мы сможем снизить причинённый ущерб к минимуму.

Список литературы

1. Narasimha Reddy A.L. Detecting networks employing algorithmically generated domain names. Available at: http://repository.tamu.edu/bitstream/handle/1969.1/ETD-TAMU-2010-08-8417/ASHWATH-KUMAR-KRISHNA-REDDY-THESIS.pdf?sequence=2, accessed 04.11.2014.
2. Barabosch Th., Wichmann A., Leder F., Gerhards-Padilla E. Automatic extraction of domain name generation algorithms from current malware. NATO Symposium IST-111 on Information Assurance and Cyber Defence. Available at: http://net.cs.uni-bonn.de/fileadmin/user_upload/wichmann/Extraction_DNGA_Malware.pdf, accessed 04.11.2014.
3. Massi J., Panda S., Rajappa G., Selvaraj S., Revankar S. Botnet Detection and Mitigation. Proceedings of Student-Faculty Research Day. Available at: http://csis.pace.edu/ctappert/srd2010/c4.pdf, accessed 04.11.2014.
4. Ивасюк Б.Д., Долуев И.А. Вирусная сеть ботнет // European researcher. 2011. № 5-1 (7), С. 607-608.
5. Котенко И.В., Коновалов А.М., Шоров А.В. Исследование бот-сетей и механизмов защиты от них на основе методов имитационного моделирования // Известия вузов. Приборостроение. 2010. Т. 53. № 11. С. 42-45.
6. Котенко И.В., Коновалов А.М., Шоров А.В. Исследовательское моделирование бот-сетей и механизмов защиты от них // Новые технологии. 2012. № 1. Приложение к журналу Информационные технологии. 32 с.