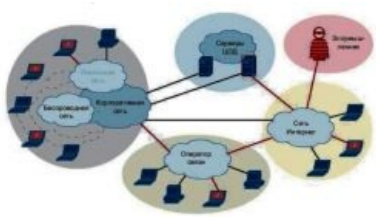
Ботнет — Lurkmore

> **Эту статью или раздел следует развикифицировать**
>
> Эта статья выглядит как или даже является копипастой из википедии. Здесь полностью отсутствуют лулзы, описание драм и прочие ништяки, зато показана значимость™ статьи, а также присутствуют нейтральная точка зрения™ и унылая спискота, или в ней много узкоспециализированной информации сомнительной ценности и энциклопедических терминов. Необходимо срочно привести статью в удобоваримый вид, пока не случилось страшное.



Ботнет обыкновенный

Зомби отакуэ

Ботнет (англ. *botnet*) — ныне распространенное в этих ваших интернетах явление, представляющее собой сеть самых обычных компьютеров, через уязвимости в ПО или по обычной ламерности юзеров заражённых специализированными, «зомбирующими» вирями (как правило, это бэкдор, позволяющий без ведома хозяина машинерии взять над ней удаленный контроль и анонимно рулить ей с любой интернетизированной точки земного шара), цель которых в первую очередь не форматнуть винчестер с 100 гигами порнухи или вызвать короткое замыкание биоса, но превратить компьютер в эдакого «зомби» (или бота), в таком состоянии которого злоумышленник сможет использовать вычислительные ресурсы оного в своих целях. Как вариант — устроить анонимную прокси, из-за которой к вам могут прийти

В крупнейшие ботнеты входит намного больше 9000 участников. Рекорд на март 2010 — сеть на 12+ млн.

Основные фичи

Список возможностей ботнетов сам по себе довольно большой, и способы применения их различаются, но в основном все они исходят из нижеприведённых:

- Downloader: присутствует в 95% вирусов. Подновляет старые версии бота, загружает через сеть практически любой контент (трояны, новые боты и т. д.). С помощью этой команды на все компьютеры одновременно могут быть установлены троянские программы, которые ищут все пароли, когда-либо введенные на данном компьютере и сохранённые в его памяти, и пересылают их на выделенный для этого сервер.
- Keylogger: перехват набиваемых на клавиатуре символов с последующей отправкой владельцу сети. В последнее время вытесняются FormGrabber'ами (читай ниже).
- FormGraber & WEB Injects: FormGraber перехватывает данные отправляемых форм с вашими паролями и прочими номерами CC и отправляет в командный центр. При этом надёжный протокол HTTPS не спасает. WEB Injects внедрение HTML или злого JS в сайты, посещаемые зараженным юзверем. Например с помощью этой технологии можно попросить ввести номер кредитки и код CVV2 при входе на легитимный сайт онлайн банка, а то и вовсе внедрить JS скрипт автозалива который будет пиздить ваши шекели в автоматическом режиме забив болт на двухфакторную аутентификацию. Самый известный представитель — Zeus и овер 9000 его вариантов. Для желающих посмотреть как оно работает вот пруф (Password : zeus).
- DDoS: атакует ресурс путём перегрузки оного множеством запросов от ботов. Создание подобного потока может вызывать серьёзные неполадки сервера, приводящие к его недоступности для обычных юзверей. Иногда это дело используют и для кибер-шантажа, требуя выкуп для остановки атаки. Разумеется, это дело могут использовать и в политических целях, атакуя правительственные сайты и прочие интересные ресурсы (нетрудно прикинуть, сколько раз за день может подвергаться подобным атакам сайт, скажем, правительства того же США). Одной из успешных в свое время была атака на сервера мелкософта с помощью вируса «MSBlast!», который в один день начал долбить запросами со всех компьютеров адрес microsoft.com, из-за чего сайт ушел в отстой. Алсо, оружие упячкоёбов.
- Spam: (более 80% мирового трафика этого дерьма — заслуга ботнетов) загрузить заранее заготовленный шаблон спам-сообщения и начать рассылку спама на указанные адреса (каждому боту выделяется своя порция натыренных у народонаселения адресов, среди которых, скорее всего, уже давно в завсегдатаях находится твой, анонимус).
- Proxy: использовать данный компьютер как прокси-сервер. Зачастую эта возможность ставится не как отдельная фишка, а сразу базовой опцией. Это

одна из прикладных функций, позволяющая использовать любой компьютер из ботнета как прокси-сервер с целью сокрытия реального адреса злоумышленника, управляющего ботнетом. Впрочем, ясен пень, такими проксиками уже давным давно пользуются не только их авторы (а вы думали, какова природа тех тормозных халявных проксиков, которые можно найти в интернетах, когда хочется потроллить на форумах любителей сразу банить по айпи поциэнтов?). Кулхацкеры и прочие мастера интернетов могут использовать зомбанутые компьютеры по самому прямому назначению — взламывать от их имени сервера, сайты, переводить денежки и т. д. Существует так-же более продвинутый вариант — backconnect proxy; при этом клиент (бот) самостоятельно подключается к серверу (владельцу ботнэта), что позволяет обойти тот-же NAT.

- VNC/TeamViewer.
- Cryptomining криптовалют — новое дыхание ботнетов, теперь железки лохов греются ради прямой прибыли этих ваших красноглазиков, и ведь хер докажешь. пруф№ 1пруф№ 2

Благодаря им ты каждый день материшь спам-фильтр провайдера и подметаешь свой почтовый ящик. А может, и сам торчишь там на заднем плане

Бывают еще и другие, не входящие в этот список фичи, но они не являются такими популярными и реализуются опционально в отдельных версиях ботов. Бывают опции, позволяющие делать скриншот экрана юзера заражённого компьютера, мониторить вводимые с клавиатуры пароли, выводить из строя центрифуги и т. д.

Коммерческое применение

Использование botnet далеко не всегда осуществляется владельцем сети: за нее вполне может вбашлять энное количество денег какая нибудь рекламная конторка и взять сеть в аренду (причём целенаправленное создание ботнетов на продажу является вполне прибыльным криминальным бизнесом). Кроме того, с успешно зомбированных машин зачастую невозбранно тырятся находящиеся там почтовые адреса, которые затем продаются спамерам и пополняют их рассылочный список. Также, при загрузке на зомбированную машину трояна, с неё можно сграббить все возможные пароли к аськам, сайтам, ФТП и т. д., которые тоже перепродаются либо используются для массового заражения веб-ресурсов (если, например, удастся сграббить пароли от фтп-аккаунтов) в целях пополнения бот-сети.

На самом деле

На самом деле, дела обстоят более готично. Ботнеты — это вам не коллекция ботов для детских шалостей типа флуда, спама, прокси. Хотя несомненно, должны существовать и быдло-ботнеты, предназначенные именно для спама, флуда и т. д. Настоящий ботнет — это сложная распределённая система, которая, кроме выполнения вышеописанных действий, используется для порабощения всё большего числа компьютеров. То есть, она не сидит себе пассивно, не ждёт, пока очередной ламер скачает себе где-то протрояненый кейген или откроет атач письма (этот путь появления новых ботов тоже даёт чуть более половины всех ботов). Она эти самые кейгены и генерит, и распихивает по сети.

Откуда появляются новые боты. Злоумышленник ломает сайт. Ну как ломает. Запускает сканер уязвимости по всяким там блогам, форумам, CMS. Находит дырявый сайт и модифицирует его. Контент сайта не меняется, выглядит взломанный сайт так же, просто к нему дописывают код эксплоита. Код эксплоита в зашифрованной форме хранит ссылку на загрузчик вируса. Пользователь заходит не на порнуху, не на кряки, а на самый обычный форум, и через дырку браузера автоматически (без всяких там предложений скачать) запускает загрузчик вируса. В загрузчике вируса прописана ссылка, откуда он должен скачать «боевую часть», что он, собственно, и делает: скачивает и запускает. После этого новый компьютер присоединяется к ботнету.

Иногда для того чтобы пополнить ботнет новой тушкой совсем необязательно заражать компьютер жертвы трояны. Авторы ботнетов вполне отдают себе отчет в том, что антивирусы палят любые изменения операционной системы у жертвы. Эволюцию ботнетов можно разделить на несколько этапов: первоначально, во времена зарождения ботнетов, когда весь софт был пиратским, а обновления системы были отключены так как после определенных обновлений слетала активация ворованной венды, компьютер не мудрствуя лукаво заражали трояны. Благо антивирусник если и был, то был точно таким же ворованным. Потом по мере появления кошерных бесплатных антивирей, система перестала быть целью для экспериментов, а группа риска переместилась на программы, требующие для своей работы постоянный коннект с сетью — всевозможные браузеры, асечки (привет QIP!) и прочие подобные софтины. Началась повальная эпоха клонов асечки, клонов браузеров, которая по привычке продолжается до сих пор. В некоторых случаях, когда потенциальная программа-жертва умела работать с плагинами или аддонами, вставляли именно их — вспомним всевозможные говнотулбары и прочую вредоносную хуйню подобного плана. Но прогресс на месте не стоит, и многие могли заметить повальный бум говноигр на флэше, и всевозможных говноретрансляторов радио, расплодившихся в интернете. Все становится понятным, если вспомнить что флэш есть ни что иное как закрытый программный код, исполняемый на компьютере клиента. Представьте себе картину — ничего не подозревающий юзер сидит играет в браузерную игру или слушает радио он-лайн, а хитрый флеш в это время скрытно от нашего ушастого,

занимается своими темными делами.

Единственный реальный способ что-то сделать с ботнетом — это взять контроль над ним. Этим и занимаются «люди в черном». Причем делают это очень оригинально: специально заражают свои компы; вводят их в существующий ботнет, отслеживают, как происходит управление. И в конце концов, собрав полную информацию о протоколах, берут ботнет в свои руки. Будем наивно надеяться, что они всё-таки уничтожают ботнеты, а не конфискуют для своих нужд...

Use the Force, Luke

Однако, не все то зло, каким кажется. Частным случаем ботнета является научная компьютерная сеть. Проще говоря — ботанам какого-либо задротского универа стает мало своего несчастного, забитого проном, мейнфрейма для расчетов, скажем, вероятности нежелательной беременности самки тихоокеанского сухогруза при встрече с дельфином, и они на своем/универском сайте слезно просят о помощи в вычислениях при помощи небольшой программули. Рассочувствовашийся юзер бегом качает прогу и запускает ее на своем ведре, тем самым добровольно вступив в ряды «ученых». Радостные гики потирают потные лапки, а комп нашего подопытного шкварчит процессором, выясняя ту самую вероятность (точнее выполняя мизерный процент необходимых вычислений). Обычно за такие эксперименты комьюнити задротов награждает «оператора» юнита ботнета какой-нибудь плюшкой (грамотой/сертификатом/еще одним ботом).

Алсо

Бытует мнение, что вся глобальная сеть Интернет является одним большим ботнетом, спроектированным на основе старого пиндосского ARPAnet'а и доведённая до ума по приказу ZOG'а, и в данный момент с помощью этой сети они наблюдают за тобой, юный Анон. Так может быть, лучше таки поменьше сидеть в этих ваших интернетах? Впрочем, ZOG вездесущ, и в реале от него тоже не скроешься.

Галерея

Ареал обитания ботнета Waledac, уничтоженного 25го февраля 10 года

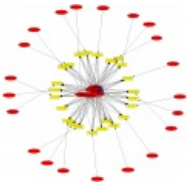


Схема управления ботнетом (трастринг)

См. также

- Tor

Ссылки

- Описание RAT от группы HellKnights

Software

12309 1C 3DS MAX 8-bit Ache666 Alt+F4 Android BonziBuddy BrainFuck BSOD C++ Chaos Constructions Cookies Copyright Ctrl+Alt+Del Denuvo DOS DRM Embrace, extend and extinguish FL Studio Flash FreeBSD GIMP GNU Emacs Google Google Earth I2P Internet Explorer Java Lolifox LovinGOD Low Orbit Ion Cannon Me MediaGet MenuetOS Microsoft Miranda Movie Maker MS Paint Open source Opera PowerPoint PunkBuster QIP Quit ReactOS Rm -rf SAP SecuROM Sheep.exe Skype StarForce Steam T9 Tor Vi Windows Windows 7 Windows Phone 7 Windows Phone 8 Windows Vista Wine Winlogon.exe Wishmaster Word ^H ^W Автоответчик Антивирус

Windows Vista Wiki Winlogon.exe Wishmaster Word Ж Автоответчик Антивирус
Ассемблер Баг Билл Гейтс и Стив Джобс Блокнот Бот Ботнет Браузер Варез Винлок
Вирусная сцена Генерал Фейлор Глюк Гуй Даунгрейд Демосцена Джоэл Спольски
Донат Защита от дурака Звонилка Интернеты Кевин Митник Китайские пингвины
Костыль Красноглазики Леннарт Поттеринг Линуксоид Линус Торвальдс Лог Ман
Машинный перевод Мегапиксель

Интернет

Интернеты 127.0.0.1 ADSL Bitcoin CMS DDoS Frequently asked questions GPON I2P
Internet White Knight IPv6 IRC MediaGet Miranda NO CARRIER QIP Ru@razlogoff.org
SEO Skype Tor TOS Via WAP Ёбаное ВТ Админ Акадо Американские интернеты
Анонимус Аська Бан Бесплатный хостинг картинок Блог Блогосфера Бот Ботнет
Браузерка Бугагашечки Бурление говн Вап-чаты Веб 1.0 Веб 2.0 Вики Виртуал
Вордфильтр Голосование ногами Гостевуха Диалап Дом.ру Домашняя страница Дорвей
Единый реестр запрещённых сайтов Жаббер Заповеди интернета Заработок в интернете
Идентификация пользователей в интернете Известные интернет-флешмобы Имиджборд
Инвайт Интернет-магазин Интернет-сервисы Искра Кик Кириллические домены
Кликбейт Коммент Комьюнити Лесенка Лог Локалка Макхост Мем Микроблог
Мобильный интернет Модератор Некропост Ник Оптимизатор Ответы Офлайн
Оффтопик Письма счастья Подкаст Поисковая бомба Покровитель интернетов Пост
Правила интернетов Предыдущий оратор Премодерация Пруфлинк Рерайтинг Ростелеком
Сабж Сетевые онанисты Симпафка Синдром вахтёра Ситилайн Скайнет Скриншот
Смайл Социальная сеть

ae:Botnet urban:Botnet en.w:Botnet w:Ботнет