Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 11229 31.10.2016, 16:42
14

Как понять, что твой компьютер стал частью ботнета?

21 октября 2016 года на крупнейшего держателя серверов доменных имен в США, провайдера Dyn, обрушилась массированная DDoS-атака. Несколько часов жители Восточного побережья США не могли зайти на десятки сайтов, в том числе PayPal, Amazon, Netflix и Twitter. Провайдер обвинил в атаке ботнет Mirai, заявив, что он задействовал около 100 тысяч «зомбированных» устройств интернета вещей – IP-камер, маршрутизаторов, и других IoT-приборов.

Но как ботнет получил доступ к такому количеству устройств? И были ли в курсе владельцы этих несчастных гаджетов, посылавших запросы на Dyn? А может быть, мое устройство тоже под угрозой?

Как понять, что компьютер стал частью ботнета, и прекратить это безобразие – в обзоре Smartbabr.

Что такое ботнет?

Ботнет – это сеть устройств из некоторого количества хостов, с запущенными ботами – программами, которые скрытно распоряжаются чужими устройствами по своему усмотрению (а точнее усмотрению тех, кто это ПО создал). Ботнет в основном славен тем, что может:

- доставлять неудобство только владельцу устройства, то есть использовать дополнительные средства каждого очередного зараженного устройства для решения задач, требующих больших вычислительных мощностей;
- доставлять неудобство владельцу устройства и недругам создателя ботнета, то есть устраивать прокси-активность (от англ. proxy — право пользоваться от чужого имени).

Например, ботнет может запускать атаки типа DDoS, или организовывать доступ для своих «создателей» в хорошо защищенные корпоративные сети через зараженный компьютер с правами в корпоративной среде, что позволяет украсть важные данные или использовать ресурсы среды для мощных DDoS-атак.

«Ещё одна идея, – добавляет эксперт-исследователь компании «Перспективный мониторинг» Юрий

Черемкин, – разная географическая распределённость заражённых объектов для сокрытия местонахождения атакующих».

Какие устройства могут пострадать?

Все, которые обладают IP-адресом.

> *«Вредоносный код, превращающий устройство в бота, может быть разработан хакерами для заражения любого подключенного к интернету девайса, будь то компьютер, смартфон, домашний роутер, IP-камера или видеорегистратор. Особо уязвимы IoT-устройства и гаджеты на хрупкой ко взломам ОС Android»*, – отметил инженер компании DDoS-GUARD.

В сентябре 2016 группировка vDOS задействовала ботнет из почти 150 тысяч зараженных видеорегистраторов для атак на сайт известного журналиста Брайана Кребса, который ранее раскрыл имена основателей этой группировки. Защитить его смог только Google.

Но вернемся к компьютерам и смартфонам.

> *«Так как ботнеты являются разновидностью ПО, то не существует принципиальных различий между загрузкой на десктоп или смартфон. Однако разные операционные системы и платформы могут быть заражены по-разному»* – поясняет Юрий Черемкин.

В среднем количество уязвимостей для настольных решений выше, чем для мобильных. Из-за встроенных механизмов безопасности инфицировать мобильные устройства сложнее, но злоумышленники обходят их, пользуясь доверчивостью и невнимательностью юзеров.

Часто пользователей вынуждают установить якобы легитимное ПО, которое впоследствии загружает необходимый для превращения смартфона в бот функционал в обход магазинов приложений. Кроме того, ранее легитимное приложение может быть модифицировано. В апреле 2016 года специалисты из FireEye подтвердили, что это возможно. Вредоносы маскировались по WhatsApp, Twitter, Facebook, Skype, Telegram и ВК.

Как это работает?

Посмотрим на примере прославившегося в США ботнета Mirai.

Mirai – это созданная хакерами программа, которая взламывает онлайн-устройства и использует их для проведения DDoS-атак. По одной версии, программа использует почтовые вирусы, чтобы заразить сначала домашний компьютер, а потом и все, что к нему подключено – видеорегистратор, телеприставку, роутер и так далее. Если речь идет о корпоративной сети, то Mirai может захватить даже IP-камеры, используемые для видеонаблюдения.

По другой версии, Mirai непрерывно сканирует устройства IoT и заражает их, используя таблицу устанавливаемых производителем имен пользователей и паролей. Устройство остается зараженным до первой перезагрузки, если после пароль не был сменен, то устройство заражается снова.

Получив тем или иным способом доступ к устройствам интернета вещей, Mirai создает из них ботнет.

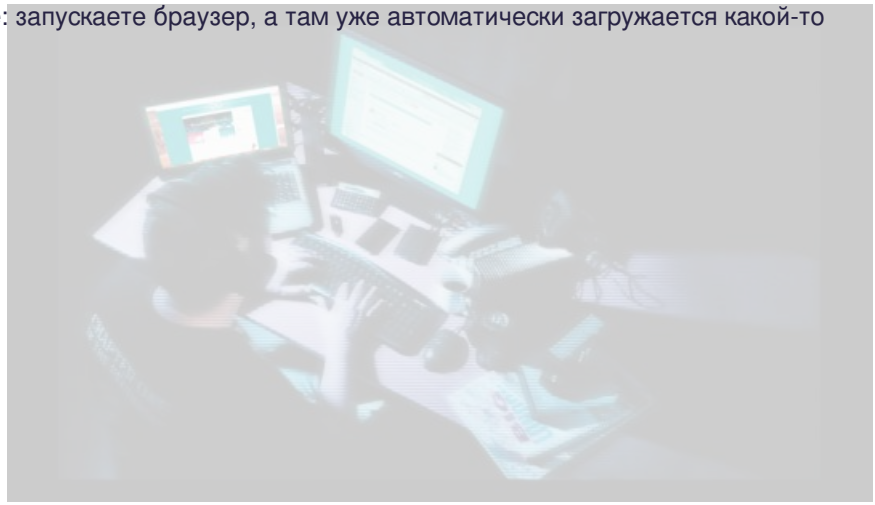
Исходный код расположен в открытом доступе в Dark Net, поэтому его могут использовать разные хакерские группировки.

Как понять, что компьютер стал ботом?

Можно подойти к нему, и спросить: «Бот ты, или не бот?» Но вряд ли это сработает. Хотя...

Есть несколько верных признаков, которые могут свидетельствовать о заражении:

- Наиболее заметное проявление: запускаете браузер, а там уже автоматически загружается какой-то неизвестный вам сайт, то есть на него посылается запрос без каких-либо действий с вашей стороны.



- Если браузер и клиенты систем обмена сообщениями (Skype, WhatsApp) не запущены, но при этом вы видите много исходящих сетевых подключений непонятно куда: это верный признак, что гаджет заражен.
- Если возникает разница в типовом поведении устройства, например, отсутствуют периоды бездействия, либо появляется высокая активность каких-то приложений, то это может служить признаком в общем случае.
- Если система слушает какие-то левые порты (TCP или UDP), вполне возможно, что это командная линия внедрившегося в нее бота.

Но все это не определяющие признаки: они могут быть связаны с другими проблемами в устройстве, а ботнеты для сокрытия активности могут выполнять свои действия только в моменты бездействия устройства или его подключения к электропитанию.

«Основным признаком заражения является эксплуатация сетевых или локальных ресурсов устройства, поэтому одним из критериев является увеличенная загрузка ресурсов устройства. – подытожил Юрий Черемкин. – Обнаружить такую активность можно различными дополнительными средствами, например, мониторами активности и загрузки ресурсов».

«Для проверки в Windows существует полезная команда netstat, – рассказал инженер компании DDoS-GUARD. – На Linux есть ее аналоги (утилита ss из пакета iproute2). Netstat (network statistics) – утилита командной строки, выводящая на дисплей устройства состояние TCP-соединений (как входящих, так и исходящих), таблицы маршрутизации, число сетевых интерфейсов и сетевую статистику по протоколам».

Как вы поняли, если есть малейшее подозрение на заражение, то лучше обратиться к специалисту.

Как вернуть компьютер к нормальной жизни?

Если вы нашли корень зла, то проблем нет - удаляйте обычными способами: вручную или при помощи антивируса. Но, скорее всего, вручную ничего не получится: вредоносы могут (в случае настольных ОС) маскироваться под системные процессы или дублировать себя многократно в местах автозапуска; при наличии нескольких процессов, они могут сами себя клонировать, чтобы их невозможно было завершить.

Но даже если ботов получится удалить, проблему могут сохраниться.

> «После удаления зловредов бывает так, что ОС утрачивает работоспособность, ибо сами тела гадостей удалены, а настройки, которые эта гадость переделала под себя, остаются. Тогда приходится править руками реестр, и если вы в этом мало разбираетесь, лучше доверить это профессионалу», – советует инженер компании DDoS-GUARD.

По словам Юрия Черемкина, устройства с разблокированным загрузчиком — первые в категории риска. Если загрузчик разблокирован, то злоумышленники смогут получить системные права, встроить зловред и вернуть оригинальное состояние устройства. Такие действия могут быть выполнены менее чем за 10 минут (говоря об Android, это операции root и de-root).

Наиболее надёжным способом является откат к заводским настройкам либо принудительный даунгрейд устройства, однако здесь также могут быть проблемы, так как не всегда даунгрейды возможны из ограничений доступности прошивок под устройства, а возврат к заводским настройкам не всегда гарантирует удаление

зловредов.

В случае с компьютером тоже есть радикальный способ, к которому всегда можно прибегнуть в крайнем случае – скинуть систему до заводских настроек/переустановить ОС.

Как подстраховаться?

Менять пароли на всех устройствах. Чем чаще будете менять, и чем пароли будут сложнее, тем лучше;

Проверять количество установленных сетевых подключений и удалять подозрительные;

Не качать файлы с сомнительных ресурсов;

Регулярно обновлять операционную систему и основное программное обеспечение;

Закрыть все возможные бреши в программном обеспечении устройств: отключить разрешения на стороннее внедрение в ОС.

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 11229 31.10.2016, 16:42
14
URL: https://babr24.com/?ADE=271068 Bytes: 9266 / 8543 Версия для печати Скачать PDF

Автор текста: **Полина Чехова**,
журналист.

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта