Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3373 24.10.2016, 16:42
21

Крупнейшая DDoS-атака в США: что надо знать

21 октября PayPal, Amazon, Netflix, Twitter и еще десяток крупнейших интернет-сервисов в США оказались недоступны из-за массированной DDoS-атаки на держателя серверов доменных имен этих сайтов, провайдера Dyn. Американцы называют эту атаку крупнейшей в истории. Рассказываем, что произошло, и какие есть версии о том, кто за этим стоит.

В 11.10 по Гринвичу, когда в Нью-Йорке было около полудня, на сайте крупнейшего в США хостинг-провайдера Dyn появилось сообщение о начале мониторинга и смягчения DDoS-атаки на серверы доменных имен (DNS). Через два часа атаку удалось отбить, но еще через два часа она возобновилась с новой силой. Всего провайдер заявил о трех волнах. Сообщение об окончательном разрешении инцидента было опубликовано спустя 11 часов после первых известий о начале атаки.

Компания Dun предоставляет услуги DNS до шести процентам американских компаний из списка Fortune 500. В общей сложности 21 октября из строя были выведены не менее 60 крупных сайтов, пользующихся DNS-службой Dyn. В том числе: Twitter, Spotify, Github, SoundCloud, Heroku, PagerDuty, CNN.com, People.com, The New York Times. Проблемы коснулись преимущественно восточного побережья США.

> Hmmmm
> RT @ncbjd: Updated #DDoS Internet outage map pic.twitter.com/yqfxtSKn5x
>
> — Left Whelk (@sun00way) 21 октября 2016 г.

Что это было?

Это была DDoS-атака (Distributed Denial of Service – распределенный отказ в обслуживании) – специальный вид хакерских атак, когда злоумышленники направляют на сервер искусственно созданный трафик, чтобы тот, не справившись с нагрузкой, перестал обслуживать обычный трафик. Обычно трафик направляется на сервер определенного сайта, но в этот раз злоумышленники атаковали серверы доменных имен (DNS).

DNS является своеобразной телефонной книгой для интернета. Это компьютер, который переводит понятные для человека буквенные доменные имена, такие как «smartbabr.com» в числовые адреса, известные как IP-адреса. Не имея доступа к этим адресам, подключенный к сети компьютер не может выполнить ваш запрос на доступ к сайту. Так что без работающего DNS, при нажатии на ссылку, содержащую адрес «twitter.com», вы ничего не получите.

> #bigdata @internap Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, Etsy, and more offline https://t.co/51jCWuGszP #IoT pic.twitter.com/wWBUEyQbxb
>
> — E Class Hosting (@EClassHosting) 21 октября 2016 г.

Кто это был?

Расследованием атаки, помимо самой компании, занимается Министерство внутренней безопасности США и ФБР. Пока виновник не назван. Известно только, что атака производилась через ботнет Mirai.

22 октября Dyn заявила:

> «На данный момент мы знаем, что это была сложная, весьма распределенная атака с участием как минимум 10 миллионов IP-адресов. Идет расследование, по результатам которого мы сможем назвать природу и источник атаки. Но уже сейчас понятно, что одним из источников трафика для атак были устройства, зараженные ботнетом Mirai. Мы наблюдали десять миллионов дискретных IP-адресов, связанных с ботнетом Mirai, которые были частью атаки».

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. Из всего этого многообразия подключенных к интернету вещей Mirai создает ботнет.

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.

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

Что такое ботнет?

Ботнет – это сеть устройств из некоторого количества хостов, с запущенными ботами – программами, которые скрытно распоряжаются чужим устройством по своему усмотрению (а точнее усмотрению тех, кто это ПО создал). Ботнеты давно используются для проведения DDoS-атак, но с развитием интернета вещей (IoT) они получили второе дыхание.

Сейчас все идет к том, что к интернету будет подключено максимум устройств – от холодильника в доме до станка на заводе. И если на заводах еще соблюдаются правила безопасности, то редкий обычный пользователь сменит пароль на роутере после его установки. Устройство с дефолтным паролем (слишком простым, или ранее уже засвеченным в сети) легко взломать, что и делают хакеры.

> @briankrebs @brianchappell #IoT #fail Too true for comfort! pic.twitter.com/4BSljTqVZv
>
> — Duncan Blues (@DuncanBlues42) 21 октября 2016 г.

В сентябре 2016 года 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. По некоторым данным, для этой атаки также использовалась Mirai. Защитить Кребса смог только Google.

Атака на Dyn последовала за выступлением директора компании по интернет-анализу Дага Мэдори на отраслевой конференции. Его доклад был посвящен как раз методам борьбы с DDoS-атаками, которые использует одна из занимающихся этим фирм под названием BackConnect, и ее методы лежат на грани допустимого. В исследовании Мэдори помогал Брайан Кребс.

Изображение: geekculture.com

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 3373 24.10.2016, 16:42
21
URL: https://babr24.com/?ADE=271032 Bytes: 7096 / 5507 Версия для печати Скачать PDF

- *Телеграм*
- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

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

На сайте опубликовано **494**
текстов этого автора.

эл.почта: babrmarket@gmail.com