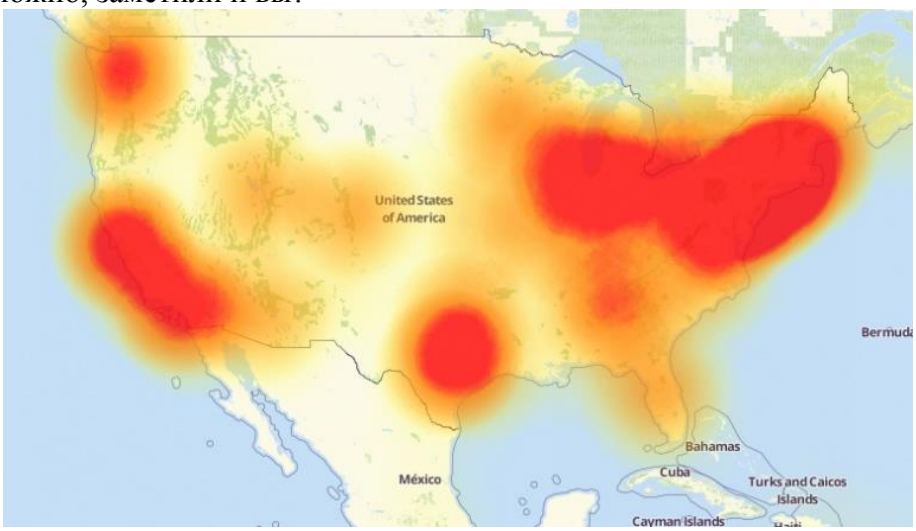
«Умная» вещь как оружие массового поражения

автор: Евгений Золотов 25 октября 2016 Источник: http://www.computerra.ru/157619/

В пятницу вечером и частью субботы (по нашему, российскому, времени) на серверы квартирующей в США компании Dyn была проведена серия атак, повлекшая затруднения доступа к нескольким десяткам самых посещаемых ресурсов Сети. Атака не была ни крупнейшей, ни особенно хитрой технически. Но было у неё свойство, которое напугало многих специалистов. Дело в том, что есть данные, позволяющие утверждать: проведена она была не с помощью компьютеров, точнее, не компьютеров в классическом смысле. За ней стояли «умные» вещи.

Dyn — компания, зарабатывающая DNS-менеджментом таких могучих доткомов, как Amazon, Twitter, PayPal, Netflix, Reddit, SoundCloud, GitHub, а также ряда крупных СМИ (The New York Times и пр.) и некоторых больших сервис-провайдеров (Visa, Verizon и др.). Попросту, она служит их распределённым DNS-сервером: когда сетянину нужен, например, IP-адрес twitter.com, это Dyn принимает запрос и выдаёт наиболее подходящий в данный момент IP-адрес. Понятно ведь, что ресурсам размера Twitter не обойтись одним сервером, у них всё многократно продублировано, да и сама Dyn устроена похожим образом (у неё дюжина дата-центров по стране, прозрачно распределяющих нагрузку). И в общем б*о*льшую часть времени всё работает нормально, пока не случается кризис вроде пятничного.

А в пятницу утром на её серверы стали миллиардами поступать вроде бы обычные запросы. Какой-нибудь узел спрашивал: а не подскажете ли вы мне адрес сайта 123.twitter.com? И тут же другой: а не подскажете 876.twitter.com? И так далее, и так далее, со случайным набором символов в начале строки. Запросы бессмысленные, однако, именно из-за случайной добавки к адресу отфильтровать их не получалось, приходилось обрабатывать. Первая атака была проведена в начале рабочего дня и продлилась два часа. Вторая — днём и устранение её заняло почти весь день. И была ещё третья, вечером. Трудности с доступом к упомянутым выше ресурсам (и десяткам, которые я не назвал) ощущались не только в Штатах: я лично ковырял тогда своё железо на предмет неизвестной ошибки — и только узнав об атаке, понял, почему не резолвились некоторые адреса. Возможно, заметили и вы?



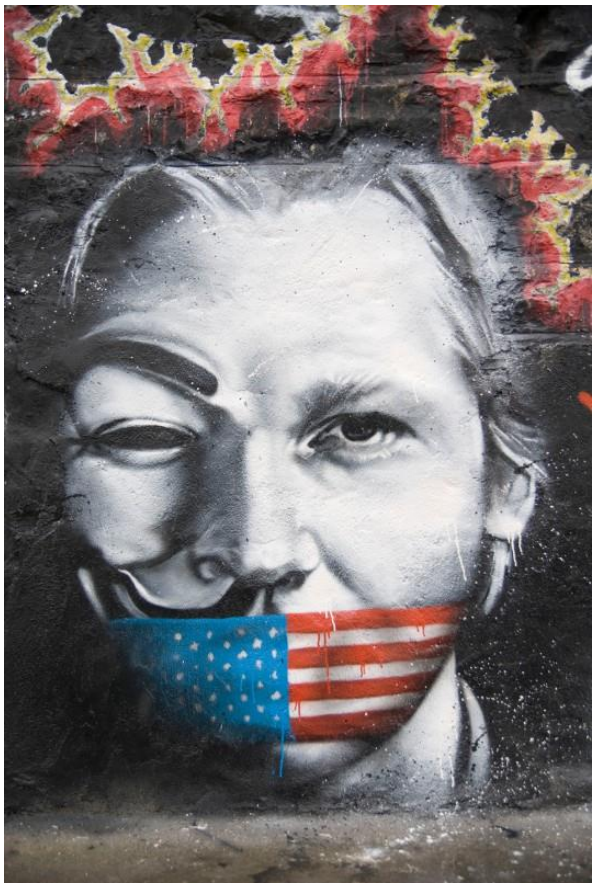
Последствия атаки ощущались максимально остро для пользователей на территории континентальных США, но «ударная волна» достигла и российской глубинки.

Непосредственных, прямых последствий у этой, в общем-то классической, DDoS не было — не считая, конечно, затруднений с доступом. А вот косвенные ещё предстоит посчитать. Потому что когда несколько часов отсутствует нормальный доступ к ресурсам вроде PayPal, это неизбежно кому-то вредит. Так что инициировано официальное расследование на самом высоком уровне и уже даже кивают в нашу сторону. Честно говоря, красная паранойя начинает уже утомлять, но в данном случае она не важна. Важны здесь два обстоятельства чисто технического свойства.

Во-первых, остались улики, подтверждающие, что значительная часть DDoS-трафика лилась с «умных» вещей, через бот-сети Mirai и Bashlight. Эти два червя заражают неполноценные цифровые системы вроде IP-камер, цифровых рекордеров, спутниковых ресиверов, точек беспроводного доступа и тому подобного — проникая через дефолтовые рутовые аккаунты, либо незакрытые уязвимости. И процесс идёт настолько успешно, что в каждый момент времени в Сети присутствуют сотни тысяч инфицированных устройств. Заражённое Mirai или Bashlight устройство достаточно перезагрузить, чтобы заразу вылечить, но уже через несколько минут оно будет заражено повторно, ибо инфицированных узлов слишком много и они сканируют интернет в поисках новых жертв.

Помогла бы перепрошивка, но перепрошивать такие вещи — сами знаете, задача непростая. Чаще всего свежих прошивок для них не существует, а если и имеются, то пользователям, на которых такое железо ориентировано, задача не по зубам. Заражённые же устройства включаются в бот-сеть и начинают, по команде из центра, к примеру, лить паразитные запросы на ту же Dyn.

Во-вторых, это не первая атака такого рода и даже вряд ли проведённая в полную силу. С месяц назад Брюс Шнайер рассказал, что неизвестные лица ведут, так сказать, крупномасштабную разведку боем: выявляют прочность критических узлов интернет-инфраструктуры, особым образом их атакуя. Организуется короткая DDoS-атака некоторой интенсивности и оценивается, как она повлияла на работоспособность жертвы. Если вывести из строя атакуемый ресурс не удалось, спустя некоторое время атаку повторяют — начиная с интенсивности большей, чем в прошлый раз. И так до тех пор, пока не будет выявлен порог сопротивляемости.



В атаке на Dyn подозревали даже пресловутых Анонимусов и сторонников Wikileaks (мол, мстят за то, что Штаты обрубили Ассанжу интернет в эквадорском посольстве), но это скорее желаемое, выдаваемое за действительное…

Стоят за этой активностью скорее всего государственные структуры — и Шнайер тоже считает вероятными виновниками нас и Китай. В его понимании, такие «проверочные атаки» подобны провокациям времён

Холодной войны, когда «случайным» заходом самолёта на чужую территорию вскрывались узлы обороны противника. И даже удар по Dyn — это ещё не война, а всего лишь очередная провокация. Настоящее нападение будет мощным и масштабным, затронет сразу множество ключевых объектов.

Какие цели оно может преследовать? Возможно (тут Шнайера продолжают уже другие эксперты), дестабилизацию обстановки в день президентских выборов в США. Беспрецедентная по размаху кибердиверсия, в результате которой окажутся разом недоступны крупнейшие социальные сети, платёжные системы (и, возможно, банки), средства массовой информации, способна деморализовать общественность и если не повлиять направленно на результат, то по крайней мере помешать нормальному течению выборов. Достойная цель.

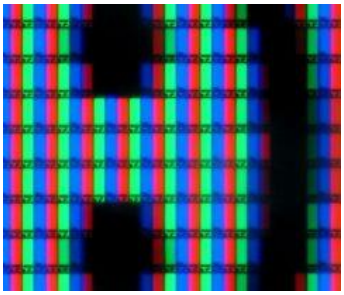
Соединяя всё это, получаем мрачную картину. Есть силы, которым выгодны удары по ключевым объектам инфраструктуры Сети. Есть ресурсы, с помощью которых такие удары могут быть настолько сильными, что противостоять им невозможно физически. Наконец, есть печальный парадокс «умных» вещей: не патчить нельзя, но патчить невозможно! И ситуация с «дырявыми» «умными» вещами становится только тяжелей: их уже миллионы, а будет намного больше.

Поэтому рассматривайте нападение на Dyn как предвестника бури. Когда-то мы боялись загрузочных вирусов, прятавшихся на дискете. Потом больше всего — заразных макросов в офисных документах. Теперь вступаем в новую эпоху, когда глупые «умные» вещи, направляемые умелой рукой, будут раз за разом ставить на колени весь интернет в угоду политическим силам.

P.S. В статье использованы графические работы Thierry Ehrmann, Downdetector.

Bashlight, DDoS, DNS, Dyn, Mirai, бот-сети, красная жара, политика, умная вещь, эволюция Сети

ЧИТАЙТЕ ТАКЖЕ



Вирус для монитора

Ах, этот глупый «умный» дом!

«Интернет (плохих) вещей»: почему холодильник, рассылающий спам, — это действительно страшно

Хакеры устроили восстание машин

Екатерина Бельц Источник: http://therunet.com/analytics/18359

Атаки через IoT-устройства происходят все чаще и становятся мощнее, на прошлой неделе благодаря интернету вещей удалось вызвать перебои в работе крупнейших сервисов

В пятницу, 21 октября, была зафиксирована крупная DDoS-атака на провайдера Dyn. Она привела к сбоям в работе таких ресурсов, как Twitter, Amazon, Reddit, Airbnb, Tumblr, GitHub, PayPal, Spotify, SoundCloud, Medium, The New York Times и Vox Media. В общей сложности Dyn работает с 6% компаний из списка Fortune 500. В атаке были задействованы «десятки миллионов отдельных IP адресов». По некоторым данным мощность атаки достигала 1,2 Тб/с. Ответственность за взлом на себя взяли New World Hackers, но эксперты говорят, что нападение было организовано через IoT-устройства.

Атака была замечена экспертами из службы X-Force IBM примерно в 12:30 PM EDT (8:30 МСК), говорится в отчете, присланном в редакцию theRunet. Аналитики выделили три этапа кибернападения. Первый начался в 7:00 AM EDT (15:00 МСК) 21 октября, второй — через 5 часов, в 12:00 PM EDT (8:00 МСК). «Третий был зафиксирован несколько позже, но во время него никакого ощутимого воздействия на систему не было», — указано в отчете. Нормальная работа сервисов была восстановлена в 1:00 PM EDT (21:00 МСК).

Представители группировки сказали, что поводом к проведению атаки послужило отключение интернета основателю WikiLeaks Джулиану Ассанжу, который находится в посольстве Эквадора в Лондоне. В отчете IBM также упоминается пост New World Hacking в Twitter, опубликованный 22 октября, где говорится о том, что группа уходит в отставку. «Мы взломали сеть не ради славы, а по определенной причине. Мы не хотим провести остаток жизни в тюрьме», — сообщили хакеры.

We want everyone to read this, goodbye. pic.twitter.com/YCiewVC1Kt

— New World Hackers (@NewWorldHacking) 23 октября 2016 г.

Сходства с атакой на OVH

Это нападение было одним из самых мощных за все время, в прошлый раз с такой же силой был атакован французский хостинг-провайдер OVH. Скорость трафика достигала 1 ТБ/с.

Ранее от тех же хакеров пострадал сайт KrebsOnSecurity, принадлежащий исследователю в области кибербезопасности Брайну Кребсу. Атака на Кребса была намного слабее, но и она тогда впечатлила экспертов.

Алексей Качалин

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО РАЗВИТИЮ БИЗНЕСА КОМПАНИИ POSITIVE TECHNOLOGIES В РОССИИ

В сентябре 2016 года аналогичная атака на сайт krebsonsecurity.com — 620 Гб/с, около 1 млн. взломанных IoT-устройств считалась пределом возможностей. Последние события показали, что это далеко не максимальный показатель

В случае с OVH атака осуществлялась с помощью ботнета, состоящего более, чем из 150 тысяч IoT-устройств. При этом бот-сеть, использованная для атаки, была способна генерировать до 1,5 Тб/с, используя tcp/ack, tcp/ack+psh и tcp/syn, заметил Дмитрий Волков, руководитель департамента киберразведки, сооснователь Group-IB. Эксперт также подчеркнул, что Атаки на компании Dyn и OVH действительно стали самыми мощными в истории.

Дмитрий Волков

РУКОВОДИТЕЛЬ ДЕПАРТАМЕНТА КИБЕРРАЗВЕДКИ, СООСНОВАТЕЛЬ GROUP-IB

Достигнуть таких мощностей помогли как раз IoT-устройства. Первой целью была компания OVH. Для атаки использовалась бот-сеть под названием Mirai, состоящая по большей части из IoT-устройств, в том числе камер наблюдения и DVR (видеорегистраторов)

Сеть насчитывала 145 607 камер наблюдения, написал тогда в своем Twitter глава крупнейшего европейского хостинга.

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

— Octave Klaba / Oles (@olesovhcom) 23 сентября 2016 г.
Впоследствии исходный код составляющих ботнета Mirai, предположительно использованного при проведении этих атак, был опубликован пользователем «Anna-senpai» на андеграундном форуме, отметил Волков.

В сообщении содержались инструкции для настройки ботнета. Исходный код также появился на Github. Хакеры часто публикуют коды в открытом доступе, чтобы защитить себя, таким образом, доступ к вирусу появляется у многих разработчиков и автор кода больше не является его единственным владельцем. После этого доказать вину подозреваемого становится невозможно.

Дмитрий Волков
РУКОВОДИТЕЛЬ ДЕПАРТАМЕНТА КИБЕРРАЗВЕДКИ, СООСНОВАТЕЛЬ GROUP-IB

Публикация исходных кодов привела к тому, что эту вредоносную программу станут использовать все большее количество атакующих. И атаки будут также мощными.

В случае с Mirai так и произошло. Как указано в отчете IBM, этот вирус использовался и при атаке Dyn. При этом оба нападения вполне могли быть организованы разными людьми, отмечает Денис Легезо, антивирусный эксперт «Лаборатории Касперского».

Денис Легезо
АНТИВИРУСНЫЙ ЭКСПЕРТ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

После инцидента с сайтом Кребса код Mirai был выложен в открытый доступ и им мог воспользоваться кто угодно

Публикация кодов имеет и позитивный эффект, они могут использоваться в образовательных целях, а также для выпуска патчей.

Андрей Арефьев
ДИРЕКТОР ПО РАЗВИТИЮ ПРОДУКТОВ ГК INFOWATCH

Я за открытую безопасность и считаю, что если проблема доступна широкой общественности, то ее быстрее исправят производители

Как работают ботнет-сети?

Принцип работы подобных вирусов заключается в сканировании всего диапазона IP-адресов для поиска устройств со стандартными (дефолтными) учетными данными для заражения и распространения ботнета, рассказывает Волков. Задачу хакерам облегчает то, что сейчас нет никаких стандартов безопасности интернета вещей.

Мошенники получают доступ к устройствам интернета вещей с помощью подбора паролей, подыскать ключ к IoT-гаджетам проще, чем к ПК. Как правило, для доступа к «умной» технике используются стандартные комбинации.

Денис Легезо
АНТИВИРУСНЫЙ ЭКСПЕРТ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

К устройствам интернета вещей довольно легко получить доступ, ведь многие пользователи не меняют стандартные настройки от производителя, включая пароли, обновления прошивок выходят нерегулярно и они редко устанавливаются владельцами на конечные устройства

Зачастую хакеры подключаются к устройствам благодаря тому, что разработчики используют один и тот же пароль для различных гаджетов. Как показывают исследования Positive Technologies, в ряде атак на IoT, помимо вышеперечисленных уязвимостей, использовались также бэкдоры, оставленные разработчиками (как правило в виде служебных учетных записей с одинаковым паролем на всех устройствах).

Мария Воронова
ВЕДУЩИЙ ЭКСПЕРТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ КОНСАЛТИНГА ГК INFOWATCH

Создается впечатление, что при проектировании технологий для IoT вопросы информационной безопасности (ИБ) если и

рассматриваются, то зачастую не в самую первую очередь, а дальнейшие доработки с точки зрения информационной безопасности происходят с учетом выявленных уязвимостей, к сожалению, уже в процессе жизненного цикла продукта

Через интернет вещей хакеры могут получить доступ к конфиденциальным данным пользователя. Например, через умные часы по Bluetooth можно подключиться к смартфону. «При этом устройство может «забирать» с подключенного смартфона учетные данные WiFi-точек и самостоятельно выходить в сеть Интернет без дополнительных действий владельца», — рассказывает Качалин.

В России стандарты безопасности в сфере IoT достаточно сложно выработать, поскольку «умные» гаджеты не так распространены, как в развитых странах.

Алексей Качалин
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО РАЗВИТИЮ БИЗНЕСА КОМПАНИИ POSITIVE TECHNOLOGIES В РОССИИ

По оценкам аналитиков доля IoT в РФ составляла 1,5% от мировой в 2015 г и несмотря на многократный рост в абсолютном количестве устройств к 2020 году сократится до 0,3%. Таким образом отставание будет только увеличиваться. В таких условиях сложно говорить о возможности диктовать мировому рынку требования к продуктам, в том числе и по безопасности

Дальше — больше

По мнению экспертов, в будущем стоит ждать более серьезных и мощных атак. «Сейчас к интернету вещей подключено гораздо больше устройств, чем в предыдущие годы. Каждый день их становится все больше, и они защищены меньше, чем когда-либо. Из-за этого хакерам проще их скомпрометировать и использовать в собственных целях», — отметили эксперты из исследовательского подразделения Cisco Talos, занимающимся мониторингом и анализом киберугроз.

Аналитики Cisco также подчеркнули, что атаки становятся более продуманными. Хакеры концентрируются на конкретной цели, из-за чего атаку сложнее предотвратить.

«Атака, для которой раньше требовалось 100 скомпрометированных систем, сейчас может быть произведена из дома при помощи всего одного домашнего сетевого соединения» — Cisco Talos

Кроме того, стоит иметь резервное соединение, чтобы в при DDoS-атаке сайт компании оставался доступным для пользователей.

Фактически, сейчас нет никаких серьезных способов защиты IoT от хакеров и ответственность за безопасность лежит, скорее, на вендорах, «которым необходимо уделять больше внимания безопасности умных устройств на этапе производства», — говорит Легезо. Также за безопасностью интернета вещей должны следить представители госструктур и разрабатывать законодательную базу и новые стандарты использования подобных устройств. Если же никакие меры не будут предприняты, то новые атаки могут стать угрозой нормального функционирования всего интернета.