Атака "умных" вещей

"Лень двигатель прогресса" - сказал когда-то русский поэт Андрей Вознесенский. Именно лень, а также стремительный темп жизни человека, год от года растущий в геометрической прогрессии, стимулирует развитие "интернета вещей". Умным вещам, которые смогут взаимодействовать между собой, в последнее время все чаще пишут хвалебные оды, обещают радужные перспективы, а IT-гиганты вкладывают баснословные суммы в IoT-проекты. По мнению аналитиков, к 2020 году на повсеместное внедрение интернета вещей потратят около 6 трлн. долларов. Непосредственно к интернету вещей в 2020 году будет подключено 24 млрд. устройств.

Утопические прогнозы рисуют нам идеальную картину мира, где умная кофеварка готовит вам бодрящий напиток в оптимальной пропорции, потому что соответствующий сигнал подала камера видеонаблюдения, определившая, что вы наконец-таки проснулись. Ну и так далее по порядку, вплоть до автоматического наполнения кормом миски вашего кота после его непродолжительного "мяуканья".

Можно представить себе и совсем иную картину, где вещи стали настолько "умны", что уже не захотели выполнять команды человека, а решили самостоятельно управлять миром. Люди больше не нужны и должны быть утилизированы, а машины могут спокойно воссоздавать самих себя и разрабатывать гораздо более совершенные механизмы. Подобное развитие событий было описано во множестве книг и кинокартин, поэтому вообразить это не так сложно.

Интернет вещей еще не нашел себя в повседневной жизни людей. На деле всё сводится к тому, что отдельные энтузиасты пытаются применить "умные вещи" в собственном быту и им приходится, например, 11 часов ждать, когда вскипит их Wi-Fi-чайник. А вот угроза, исходящая от бурно растущего мира IoT-устройств, обретает вполне конкретные черты и масштабы.

Армия IoT-устройств

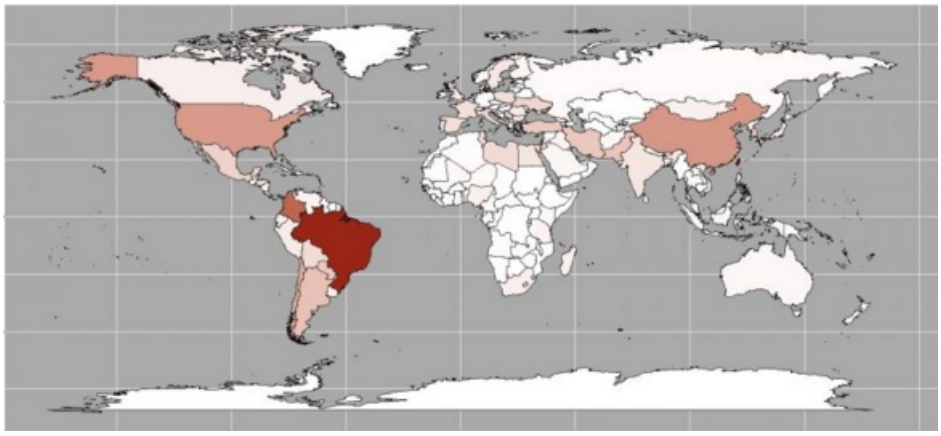
Сентябрь 2016 года, возможно, стал знаковым для всего современного интернета. Начиная с 16 сентября, неизвестными злоумышленниками было совершено несколько сильнейших в истории DDoS-атак. Суммарная мощность двух из них достигала рекордных 1Тбит/с.

Всё началось с атаки на ресурс известного в IT-среде журналиста Брайана Кребса, который в одном из своих расследований вскрыл деятельность хакерской группы V-Dos, специализирующейся на организации заказных DDoS-атак. Вскоре злоумышленники были арестованы, а на Кребса посыпались угрозы и шквал рекордных по мощности DDoS-атак.

Брайан Кребс

Проанализировав инциденты, специалисты пришли к выводу, что основной ударной силой атак были IoT-устройства: роутеры, IP-камеры, DVR и другие. Все они были объединены в различные ботнеты. Всего же с 2016 сентября было зафиксировано уже 14 DDoS-атак мощностью более 200 Mbps.

Дальше сюжет истории закручивается невероятным образом. Согласно исследованию экспертов, по всей планете около 1 млн. IoT-устройств объединены в различные ботнеты, способные проводить беспрецедентные по своим масштабам DDoS-атаки.



Больше всего зараженных IoT-устройств обнаружено в Бразилии

Масштабы некоторых из них поражают. В своем анализе исследователи говорят о ботнетах, в которые входило порядка 150 тыс. IoT-устройств. Примечательно, что основная мишень хакеров - это IP-видеокамеры. В сети был обнаружен ботнет состоящий из 25 тыс. видеокамер. Такие устройства имеют большую полосу пропускания, поэтому вполне могут быть применены в организации атак достигающих сотни гигабит.

Новый троян

Ботнет представляет из себя сеть устройств, зараженных вредоносным ПО, которое позволяет злоумышленнику выполнять различные действия с целой армией зараженных устройств одновременно. По сути, "умные" вещи становятся подобием зомби, выполняя все, что прикажет вредоносная программа.

[Атака "умных" вещей]

Сейчас особой популярностью у киберпреступников пользуются различные модификации трояна Mirai, чей создатель недавно опубликовал исходные коды к вредоносному ПО, что в будущем может в разы увеличить количество зараженных ботнетом IoT-устройств.

Принцип работы Mirai достаточно прост - он сканирует интернет в поисках уязвимых IoT-устройств, доступных через telnet. В основном троян атакует камеры видеонаблюдения, роутеры и DVR, а после

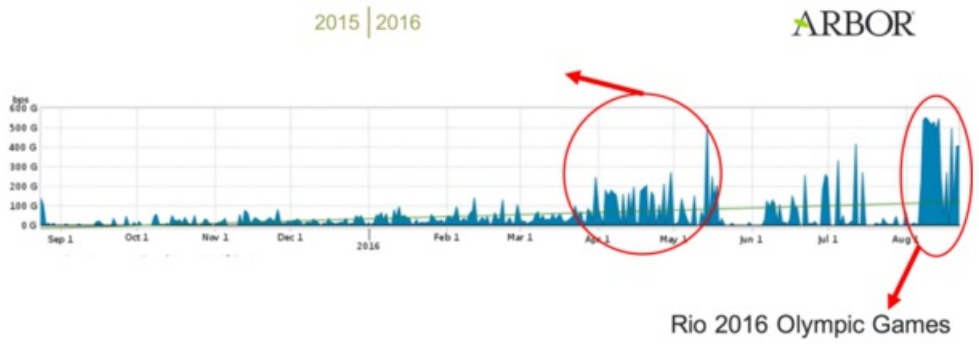
распространяется по сети. Сам же взлом устройств зачастую происходит посредством банального подбора паролей, ведь пользователи "умных" вещей зачастую оставляют заводские настройки.

Специалисты сразу же взялись за исследование новой киберугрозы и пришли к неутешительным выводам.

> "Mirai, который практически все игнорировали ранее, в силу простоты telnet-атак, на прошлой неделе стал едва ли не главным предметом обсуждения в СМИ по всему миру, а правоохранительные органы начали расследования, при поддержке множества международных компаний. Весьма вероятно, что теперь мощные DDoS-атаки станут более распространенной практикой, так как хакеры будут находить все больше уязвимых IoT-устройств или начнут заражать устройства, защищенные NAT. Производителям определенно пора прекратить выпускать устройства с глобальными паролями по умолчанию и переключиться на выпуск устройств со случайно сгенерированными паролями, указывая их на нижней части корпуса", - считают в Malwaretech.

Видео с картой заражения трояном Mirai

Рядовые пользователи интернета, уютно ползающие по любимым ресурсам, даже не подозревают о том, какая борьба происходит "под ковром" мировой паутины. В этой борьбе "темные" силы постоянно нападают, а "светлые" пытаются защитить свои стены от мощнейших атак соперников, стремящихся разрушить то, что строилось годами. К таким выводам можно прийти хотя бы ознакомившись с докладом специалистов компании Arbor Networks.



Оказывается, что атаки в несколько сотен гигабит стали обыденностью еще за несколько месяцев до начала Олимпиады в Рио. От ботнетов с завидной регулярностью страдали практически все организации, связанные с проведением игр. Во время же проведения самих игр мощность атак доходила до 540 Гбит/с. При этом основным инструментом для проведения атак выступал один единственный ботнет из IoT-устройств, при поддержке нескольких ботнетов меньшей мощности. Огромная загруженность каналов во время Олимпиады в результате чуть ли не круглосуточной трансляции на весь мир, не помешала организаторам отбить все нападки киберпреступников незаметно для наблюдавшей за играми аудиторией.

Mirai оказался не так прост, чтобы осваивать лишь видеокамеры. Последние данные говорят о том, что вирус атакует оборудование для сетей сотовой связи канадского производителя Sierra Wireless, аппаратурой которого пользуются мобильные операторы по всему миру. Под угрозой оказались роутеры и шлюзы AirLink, используемые в сетях 3G и 4G LTE по всему миру. Наиболее уязвимы к заражению модели LS300, GX400, GX/ES440, GX/ES450 и RV50.

Sierra Wireless GX400

Проблема в том, что Mirai захватывает оборудование путем подбора логина и пароля, а клиенты Sierra Wireless часто оставляют дефолтные логин и пароль в ACEmanager.

> "Так как вредоносное ПО базируется только в памяти, перезагрузка устройства поможет избавиться от заражения. Однако если устройство после этого продолжит использовать пароль, назначенный ACEmanager по умолчанию, скорее всего, вскоре произойдет повторное заражение", — пишут представители Sierra Wireless.

Заражение сотовых сетей подобным трояном чревато катастрофой для работы сотового оператора. Как отмечают в Sierra Wireless, устройства AirLink - это настоящий хребет сети. Они имеют огромную полосу пропускания, а с помощью них злоумышленники могут проникнуть в другие компоненты сети. Для организаторов DDoS-атак такая аппаратура может стать настоящей находкой.

Примечательно, что неприятный инцидент, связанный с DDoS-атакой на сотового оператора, случился на прошлой неделе в Екатеринбурге. Тогда пострадала сеть сотового оператора "Мотив". В результате связь отсутствовала у 30 тыс. абонентов. Судя по всему, атака была достаточно мощной, поскольку чтобы справиться с ней специалистам компании понадобилось более семи часов. Не исключено, что и эта атака была осуществлена посредством ботнета, объединяющего в себе "умные" вещи или воздействием на устройства сети.

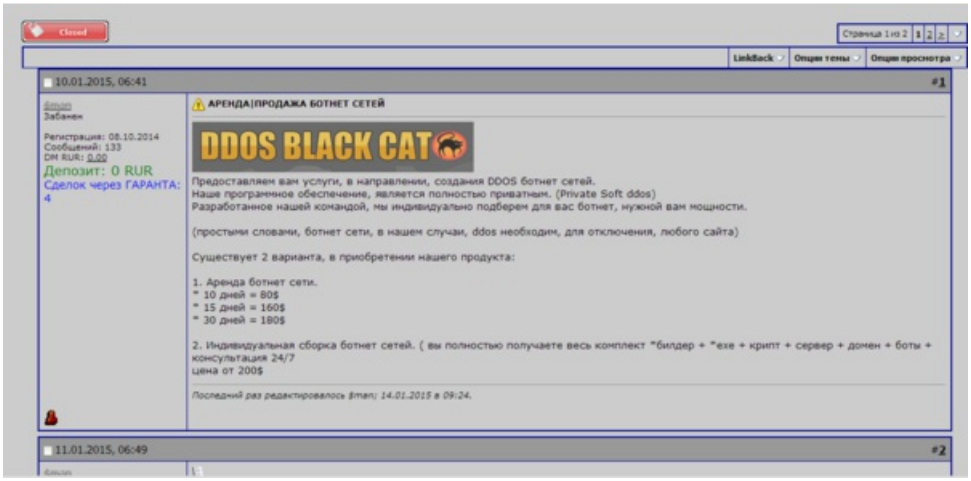
Ботнет в аренду

Троян изначально не примечательный для специалистов по защите информации вдруг стал серьезной угрозой для всего интернета. По мнению экспертов, дальнейшее объединение устройств в более масштабные бонеты способно серьезно тормозить сеть. Киберпреступность же получила в свои руки мощный инструмент для шантажа и зарабатывания денег.

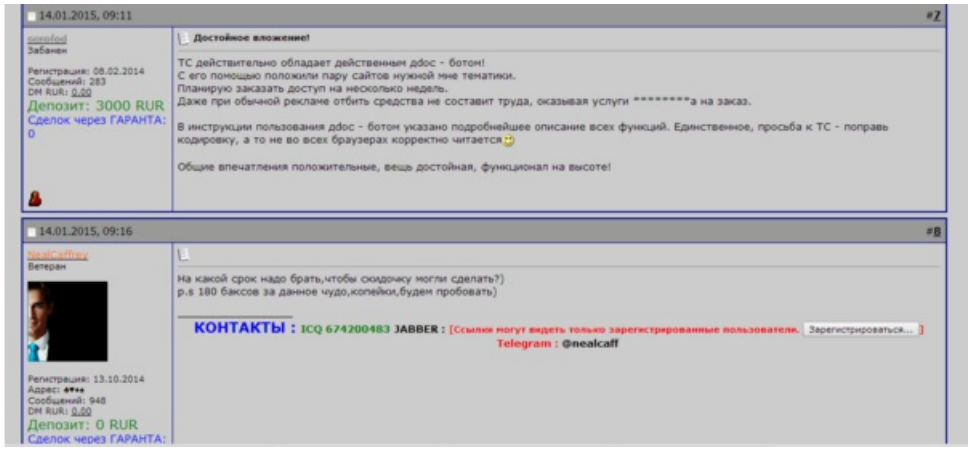
Это доказывает разоблачительная статья Брайана Кребса, о которой упоминалось выше. Журналист опубликовал информацию о деятельности группировки vDos, которая за два года сумела организовать более 150 тыс. атак, заработав на этом более 600 тыс. долларов. Хакеры за вознаграждение проводили атаки на сайты, а также сдавали ботнеты в аренду.

Бизнес по созданию и аренде ботнетов сейчас процветает, а с постоянной разработкой новых вредоносных программ его популярность среди киберпреступников только растет.

Честно, я думал, что оформить заказ на такую услугу можно лишь заглянув в "темную" часть мировой паутины. Однако по запросу "Яндекс" сразу же выдал мне ссылку на форум, где по правилам запрещено распространение ботнетов, но эти услуги там предлагают.



Ну а дальше все, как в интернет-магазине с кучей отзывов довольных клиентов и вопросов заинтересовавшихся.



Подобных ресурсов в сети бесчисленное количество. Не все они созданы для нанесения серьезного урона. Некоторые специализируются лишь на распространении спама. Какие же тогда услуги предоставляют обитателя "даркнета"?

Рекомендации специалистов

Для защиты от заражения специалисты по информбезопасности в первую очередь предлагают менять все заводские настройки. В частности, это относится к паролям и логинам. Для большого количества устройств можно использовать специальные программы генераторы-паролей.

В случае же с системами видеонаблюдения, стоит изолировать их доступность из интернета (настройками роутера или firewall). Внутренним устройствам также лучше ограничить доступ к DVR и дать только тем адресам, которым он необходим. Доступ самого DVR к сети также стоит ограничить, оставив доступ лишь к необходимым адресам.

Как подчеркивают эксперты, развитие "интернета вещей" открывает широкие возможности для создания все более мощных ботнетов. В первую очередь дело здесь в том, что многие "умные гаджеты" выпускаются без какой либо защиты от заражения, а в некоторых случаях схемы подключения устройства к сети упрощается максимально.

Для полноты картины список самых крупных DDoS-атак за последнее время:

- Атака на китайскую компанию Imperva в середине июля. Ее мощность достигала 470 Гб/с.
- 19 сентября были атакованы серверы Blizzard, в результате чего многим геймерам был ограничен доступ к популярным игровым серверам. Сделано это было для рекламы. Хакеры ждали пока запись об атаке в их твиттере наберет 2 тыс. репостов. После достижения этой отметки они прекратили атаку на серверы Blizzard.
- В сентябре после разоблачения группировки хакеров журналистом Брайаном Кребсом, на его ресурс была совершена атака мощностью 620 Гбит/с.
- Более 150 тыс. IoT-устройств атаковали сеть провайдера OVH. Мощность атаки достигла 1 Тб/с.
- 21 октября рекорд был обновлен. DDoS "весом" более 1 Тбит/с обрушился на DNS-провайдера Dyn. В итоге, в течение некоторого времени недоступными оказались многие популярные сервисы: Twitter, Reddit, Yelp, Imgur, PayPal, Airbnb, Pinterest, Shopify, Soundcloud, Spotify, GitHub, Heroku, Etsy, Box, Weebly, Wix, Squarespace, CPAN, NPM, Basecamp, Twilio, Zoho, HBO, CNN, Starbucks, Yammer и так далее.

Уже сейчас становится ясно, что угроза миру "интернета вещей" и миру от "интернета вещей" вполне осязаема, и вполне может уже на данном этапе доставить массу неудобств и проблем всей экосистеме мирового интернета. Таким образом, дальнейшее становление мира IoT-устройств, и постройки целых платформ и производств на его основе невозможно без выработки эффективной стратегии защиты, которая смогла бы обезопасить "умные" устройства от взлома.