Автор: Administrator
18.09.2016 18:28 -

В своем блоге известный журналист, специализирующийся на информационной безопасности, Брайан Кербс (Brian Krebs), нередко разоблачает различных хакеров и раскрывает схемы работы киберпреступников. Хакерский андеграунд уже неоднократно пытался отомстить Кребсу, но это не останавливает исследователя. На этот раз Брайан Кребс разоблачил деятельность хакерской группы vDos, предоставляющей услуги DDoS-атак на заказ, после чего операторы сервиса были арестованы в Израиле.

В минувший четверг, 8 сентября 2016 года, Кребс опубликовал в своем блоге результаты очередного расследования. Журналист рассказал о том, что операторы сервиса vDos, предоставляющие услуги DDoS на заказ, за два года заработали более $600 000, произведя более 150 000 атак.

Кребс пишет, что все началось с расследования деятельности аналогичного сервиса PoodleStresser, изучением которого занимался некий анонимный следователь, поддерживавший связь с Кребсом. Тот же следователь впоследствии сумел обнаружить уязвимость в сервисе vDos, которая позволила ему скачать с сервера злоумышленников БД и файлы конфигурации.

База данных, среди прочего, содержала информацию о платежах, полученных злоумышленниками от «клиентов». Самые ранние финансовые записи датированы 2014 годом, но сервис vDos начал работу в 2012 году. Опираясь на цифры из БД, Кребсу удалось подсчитать, что за последние два года злоумышленники заработали на DDoS-атаках $618 000. Также исследователь предположил, что суммарный доход операторов vDos за эти годы составил более миллиона долларов.

Анонимный источник также сообщил Кребсу, что серверы группы находятся с Болгарии, но потом совместное расследование показало, что операторы vDos – это двое граждан Израиля. Такой вывод помогли сделать обнаруженные заявки в службу поддержки, а также тот факт, что сервис имел встроенное ограничение и не мог атаковать израильские IP-адреса.

В своем блоге Кребс рассказал, что операторы сервиса известны под псевдонимами AppleJ4ck и P1st (или же M30W). Хотя они скрывали свои личности, Брайан Кребс все же сумел отследить злоумышленников. На основании некоторых имен, email-адресов и

телефонных номеров исследователь пришел к выводу, что за этими псевдонимами скрываются граждане Израиля Ярден Бидани (Yarden Bidani) и Итай Хури (Itay Huri).

Вскоре после публикации данной статьи, как только материал начал набирать популярность на Reddit, Slashdot и так далее, на сайт Кребса обрушилась DDoS-атака. Согласно данным исследователя, все началось с незначительных 20 Гбит/с, но постепенно атака набрала мощность и достигла 128 Гбит/с, что привело к перебоям в работе ресурса.

Вскоре стало понятно, что именно получило поводом для атак. В субботу, 10 сентября 2016 года, израильские СМИ сообщили, что местные правоохранительные органы арестовали операторов vDos еще на прошлой неделе, по наводке, полученной от коллег из ФБР. Однако в пятницу, 9 сентября, Бидани и Хури были отпущены под залог: их поместили под домашний арест, запретили пользоваться телефонами и компьютерами, а также покидать страну. Именно в это время начались DDoS-атаки на сайт Брайана Кребса. Исследователь пишет, что пакеты содержат встроенное сообщение «GoDieFaggot», а атаки продолжаются до сих пор.

Почти одновременно с этим исследователю стало известно, что серверы vDos ушли в оффлайн 9 сентября 2016 года и на данный момент по-прежнему недоступны. Кребс заявляет, что недоступность vDos – это следствие так называемой BGP-атаки. Как известно, протокол динамической маршрутизации в интернете BGP (Border Gateway Protocol) уязвим перед атаками с изменением маршрутизации когда некий узел начинает выдавать себя за другой. Из-за этого многие маршрутизаторы могут изменить свои таблицы маршрутизации, перенаправляя трафик совсем не туда, куда нужно.

В устроении такой атаки на vDos признались специалисты компании BackConnect Security. Они сообщили Кребсу, что им пришлось пойти эти на крайние меры, после того как 8 сентября 2016 года vDos обрушил на их фирму DDoS-атаку мощностью выше 200 Гбит/с. Затем операторы DDoS-сервиса прислали сотрудникам BackConnect Security письмо, в котором взяли на себя ответственность за инцидент. Специалисты решили узнать о противнике как можно больше и обнаружили ту самую публикацию в блоге Брайана Кребса, в которой журналист, в числе прочего, перечислял IP-адреса серверов злоумышленников.

Хотя эта история явно еще не окончена, подводя промежуточный итог, Брайан Кребс

сообщил, что он и специалисты компании CloudFlare решили опубликовать логи vDos. Объемный файл (ZIP), покрывающий период времени с апреля до июня 2016 года уже доступен для скачивания. Теперь все жертвы DDoS-атак могут поискать в логах сервиса свои IP-адреса и домены, проверив, не стоят ли vDos за тем или иным инцидентом.