Киберпреступность. DDos-атаки

За 30 секунд, что вы потратите на чтение этого абзаца, будет опубликовано 23 100 фотографий в Instagram, 226 000 постов в Twitter, загружена 171 000 приложений в Play market и App Store, потрачено 380 000 Долларов в онлайн режиме. В это время просматриваются 1,8 млн видео на Youtube и совершено 2 млн запросов в Google. Удивительно, не так ли?

Электронные платежи, обмен личными информационными данными в Интернете – это настоящая золотая жила для злоумышленников, желающих получить выгоду с беспечности Интернет пользователей. Структура современной киберпреступности практически сформирована. Существуют четко определённые взаимоотношения и бизнес-модели. Каждое поколение мошенников имеет свои инструменты.

Последние несколько лет актуальны DoS- и DDoS-атаки. Это разновидности атак на вычислительную систему. Их основная цель - приведение системы к отказу или затруднению получения доступа предоставляемых ресурсов. Dos- и DDoS-атаки осуществляются при помощи Троянов, или Троянских программ. Они заражают недостаточно защищенные системы и могут долгое время себя не проявлять, ожидая распоряжения владельца. После получения команды, Трояны со всех ранее заражённых компьютеров приступают одновременно высылать запросы выбранному на роль жертвы сайту.

Причины таких атак могут быть абсолютно разные: как личная неприязнь и недобросовестная конкуренция, так и шантаж, и вымогательство денег.

К примеру, 13 марта 2017 года ознаменовалось несколькими мощными DDoS-атаками на сайты российских СМИ. Первой жертвой стал сайт Первого канала, на который обрушился мусорный трафик. Днем позже,14 марта были опубликованы данные об атаках на сайты Кремля и Центробанка РФ. В копилке потерпевших DDoS-атаки добавлены так же сайты правительства Сирии, интернет-издания Lifenews, интернет-сервисы PlayStation Network и Qriocity японской корпорации Sony.

Совсем недавно, в начале марта 2018 года, на GitHub обрушилась мощнейшая DDoS-атака, чья мощность составляла 1,35 Тб/сек.

Одновременно с атакой на GitHub, 5 марта 2018 была обнаружена DDoS-атака на пока неизвестного американского сервис-провайдера. Она установила рекорд: 1,7 Тб/сек.

Маловероятно, что эти атаки станут единичным случаем. Киберпреступники научились использовать серверы Memcached для отражения и усиления мусорного трафика. Запрос, объемом всего 15 байт, может превращаться в ответ размером 134 Кб. такими серверами возможна подмена источника запроса, что позволяет направлять вредоносный поток на выбранную цель. В итоге совокупность потоков, которые могут обрушиться на жертву, способна усилить атаку в 50 000 раз.

По данным Shodan, на 5 марта 2018 года в сети можно обнаружить уже свыше 105 000 Memcached-серверов.

Атаки киберпреступников становятся все масштабнее и изощрённее. Так, «Троянский конь» является самой популярной и самой опасной из всех вредоносных программ.

Во-первых, на разработку, распространение и использование современных вредоносных программ затрачивается много ресурсов. Поэтому злоумышленников в первую очередь привлекают более простые и дешевые методы атак. Троянские программы одно из более привлекательных решений.

Во-вторых, вследствие кризиса интернет-пользователи начинают судорожно реагировать на любые события, связанные с платежными системами и онлайн-банкингом. Поэтому, когда банки разоряются, пользователи меняют владельцев, что способствует новым атакам.

Я думаю, что для борьбы с киберпреступностью нужно разработать определенный свод норм и правил предосторожности нахождения в Интернете. Подобно блокировке машины, следует разработать уникальную программу, которая будет защищать сайт от злоумышленников и оповещать о попытках нанесении вреда.

Источники:

1. https://www.golos-ameriki.ru/a/fbi-cyber-security-2010-08-07-100188734/187247.html
2. https://sibac.info/studconf/science/ix/62908
3. http://internetua.com/ustanovlen-absoluatni-rekord-po-mosxnosti-kiberataki
4. http://biz.liga.net/all/all/stati/2048983-kiberprestupnost-kak-biznes.htm