В сентябре 1996 года «упал» один из интернет-провайдеров в Нью—Йорке. Компьютеры со всего мира, контролируемые хакерами, посылали провайдеру по 150 запросов на подключение в секунду — гораздо больше, чем он мог обеспечить. Этот случай считается первой крупной DDoS-атакой в истории. Распределенная сеть зараженных машин довела до отказа оборудование оператора.

Прошло 20 лет, а угроза стала только серьезнее. Число атак растет экспоненциально, этому содействует, как сама архитектура всемирной сети, так и появление все большего количества подключенных устройств. Как правило, IoT-устройства имеют слабую защиту либо не имеют ее вовсе, поэтому злоумышленникам не составляет труда получить контроль над очередным десятком умных тостеров. Такие атаки теперь не только вызывают чувство раздражения из-за «подвисания» любимых сайтов, но и становятся реальной угрозой безопасности.

Согласно отчету компании Arbor Networks, занимающейся исследованиями интернета и защитой от DDoS-атак, за период с 2011 по 2014 их число увеличилось в 30 раз. При этом атаки становятся все более интенсивными. Те, что произошли в сентябре и октябре, побили все рекорды по мощности и объему трафика. Их жертвами стали Twitter и Spotify, DNS-провайдеры и множество других сайтов и сервисов.

Эксперты считают, что эти атаки были произведены с помощью вредоносной программы

Mirai, которая позволяет организовать ботнет в том числе с участием IoT-девайсов, например камер систем безопасности. На многих из них пароли либо отсутствуют, либо состоят из нескольких простых символов, одинаковых для тысяч таких устройств. Mirai отслеживает подобные устройства и умело организует их для атак.

Ботнеты — давняя история, но Mirai выводит их на новый уровень. В докладе Института критических инфраструктурных технологий объясняется, что Mirai — целая платформа с открытым кодом. Сообщество хакеров ежедневно совершенствует и усиливает свою систему. Именно Mirai была использована для недавних атаках на российские банки и для повреждения системы отопления жилых зданий в Финляндии.

Эксперты утверждают, что система уже в ближайшее время может быть модернизирована для атак на критические объекты инфраструктуры стран. Так под угрозой находятся электростанции, атомные станции. И уже совсем нетрудно представить, как системы подобные Mirai, собирают миллионы IoT-устройств для того, чтобы сделать их частью нового типа войн.

Хакерам уже приписывают влияние на ход важнейших мировых событий. Недавно мы брали интервью у владельца российского хостинг-провайдера, которого весь мир объявил в атаках на серверы Демократической партии США.