Новая версия ботнета меняет парадигму с DDoS-атак к майнингу.

Специалисты Aqua Security обнаружили новую вариацию Ботнет — это совокупность подключенных к Интернету устройств, которые могут включать персональные компьютеры (ПК), серверы, мобильные устройства и устройства Интернета вещей (IoT), которые заражены и контролируются вредоносным ПО без ведома их владельца." data-html="true" data-original-title="Ботнет" >ботнета Gafgyt, которая активно атакует серверы со слабыми SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений. Протокол похож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования.

 SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

 SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удаленно работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео." data-html="true" data-original-title="SSH" >SSH-паролями, работающие в облачных средах. Вредоносное ПО использует вычислительную мощность графических процессоров взломанных устройств для майнинга криптовалюты.

Ботнет Gafgyt (BASHLITE, Lizkebab, Torlus) активно действует с 2014 года и прославился своей способностью эксплуатировать слабые или дефолтные пароли для получения контроля над маршрутизаторами, камерами и DVR-видеорегистраторами. В арсенале Gafgyt также имеются инструменты для использования известных уязвимостей в устройствах Dasan, Huawei, Realtek, SonicWall и Zyxel. Захваченные устройства превращаются в часть ботнета, способного организовывать DDoS-атака – распределенная атака типа отказ в обслуживании, которая являет собой одну из самых распространенных и опасных сетевых атак. В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов.

 DDoS-атака заключается в непрерывном обращении к сайту со многих компьютеров, которые расположены в разных частях мира. В большинстве случаев эти компьютеры заражены вирусами, которые управляются мошенниками централизовано и объедены в одну ботсеть (ботнет). Компьютеры, которые входят в ботсеть, рассылают спам, участвуя, таким образом, в DDoS-атаках." data-html="true" data-original-title="DDoS" >DDoS-атаки.

Новая версия ботнета Gafgyt использует брутфорс для взлома SSH-серверов со слабыми паролями, после чего запускает майнеры криптовалюты с помощью модуля «systemd-net». Перед этим ботнет завершает работу конкурирующих вредоносных

программ, уже запущенных на взломанной машине, чтобы монополизировать ресурсы системы.

Кроме того, Gafgyt использует червя, написанного на языке Go, который сканирует интернет на предмет плохо защищенных серверов и заражает их, тем самым расширяя масштабы ботнета. Червь сканирует SSH, Telnet, а также учетные данные, связанные с игровыми серверами и облачными средами AWS, Azure и Hadoop.

Основной целью атакующих является запуск майнера XMRig — это программное обеспечение для майнинга криптовалюты Monero.
 Зачастую используется злоумышленниками в качестве инструмента для криптомайнинга без согласия владельца компьютера." data-html="true" data-original-title="XMRig" >XMRig, который добывает криптовалюту Monero. В данном случае злоумышленники используют флаги —opencl и —cuda, чтобы задействовать вычислительные мощности GPU.

Новая версия ботнета отличается от предыдущих и нацелена на облачные среды с мощными CPU и GPU, вместо того чтобы сосредоточиться на DDoS-атаках. По данным Shodan, в интернете доступно более 30 миллионов SSH-серверов, что подчеркивает необходимость принимать меры по защите от брутфорс-атак и возможного взлома.

Примечательно, что после начала пандемии, в период с 14 по 31 декабря 2020 года, специалисты выявили в общей сложности 18 000 уникальных хостов и около 900 уникальных полезных нагрузок. Чаще всего встречались заражения семействами вредоносов Gafgyt и Mirai — на них приходилось 97% из 900 полезных нагрузок.