ВОЗРАСТАЮТ ЦЕЛЕВЫЕ АТАКИ на IoT и сетевые уязвимости

В.Дягилев, глава представительства Check Point Software Technologies в России и СНГ

DOI: 10.22184/2070-8963.2018.75.6.72.73

Развитие технологии Интернета вещей не лишено рисков. Устройства и приложения, которые используют цифровые данные, полностью зависят от уровня безопасности и сохранности этих данных. Киберпреступники знают об уязвимых местах и используют все лазейки, чтобы заразить сеть зловредом и получить контроль над устройствами пользователя.

Согласно исследованию Check Point, к современным крупномасштабным киберугрозам "Пятого поколения" готовы лишь 3% компаний. Текущий уровень защиты организаций не только не соответствует, а сильно отстает от экспоненциально прогрессирующих угроз. Этот факт вызывает серьезные опасения, поскольку о новом поколении угроз стало широко известно еще в 2017 году, когда мы столкнулись с атаками WannaCry.

В своем отчете Global Threat Index за июль 2018 года компания Check Point Software Technologies Ltd. отмечает значительное увеличение эксплойтов, направленных на три основные уязвимости Интернета вещей.

Топ-3 IoT-уязвимостей

По оценкам экспертов, к 2020 году к интернету будет подключено 20 млрд IoT-устройств. С мая 2018 года количество атак, связанных с распространением в IoT вредоносных программ, таких как Mirai, IoTroop/Reaper и VPNFilter, увеличилось более чем в два раза. В течение июля 2018 года три IoT-уязвимости вошли в рейтинг 10 наиболее часто эксплуатируемых:

- удаленное выполнение кодов MVPower DVR-маршрутизатора (на 5-м месте);
- удаленное выполнение команд маршрутизатора D'Link DSL-2750B (на 7-м месте);
- обход аутентификации маршрутизатора DANAN GPON A (на 10-м месте).

В общей сложности в июле 2018 года 45% организаций во всем мире подверглись атакам на эти уязвимости, в июне атаки на них ощутили 35% компаний, в мае – 21%. Все эти уязвимости позволяют злоумышленникам выполнить вредоносный код и получить удаленный контроль над требуемыми устройствами.

Самые активные зловреды

В июле 2018 года Coinhive сохранил статус самого распространенного вредоносного ПО, он атаковал 19% организаций во всем мире; Cryptoloot и Dorkbot оказались на втором и третьем местах рейтинга соответственно, каждый из вредоносов атаковал 7% организаций в мире.

- Coinhive – криптомайнер, предназначенный для онлайн-майнинга криптовалюты Monero без ведома пользователя, когда он посещает веб-страницу. Встроенный JavaScript использует большое количество вычислительных ресурсов компьютеров конечных пользователей для майнинга и может привести к сбою системы.
- Cryptoloot – криптомайнер, который использует мощность ЦПУ жертвы, а также имеющиеся ресурсы для криптомайнинга – добавление транзакций в блочную цепь и выпуск новой валюты. Он конкурирует с Coinhive, пытается заполучить преимущество, запрашивая меньший процент дохода от веб-сайтов.
- Dorkbot – IRC-червь, предназначенный для удаленного выполнения кода оператором, а также для загрузки дополнительного вредоносного ПО в зараженную систему. Это банковский троян, основной целью

которого является кража конфиденциальной информации и запуск атак типа "отказ в обслуживании". Из мобильных зловредов самыми активными отмечаются:

- Lokibot – банковский троян для Android, который также может превратиться во вредоносную программу-вымогателя, блокирующую телефон в случае удаления прав администратора;
- Triada – модульный бэкдор для Android, предоставляющий права суперпользователя загруженному вредоносному ПО, так как способствует его встраиванию в системные процессы. За Triada также замечен спуфинг URL-адресов, загруженных в браузер;
- Guerilla – программа-кликер рекламы для Android, способная связываться с удаленным сервером команд и контроля (C&C), загружать дополнительные вредоносные плагины и выполнять непрекращающийся переход к рекламе без согласия или ведома пользователя.

Топ-3 самых эксплуатируемых уязвимостей в июле 2018 года

- Переполнение буфера IIS WebDAV ScStoragePathFromUrl (CVE-2017-7269) Microsoft. Отправляя созданный запрос по сети на сервер Microsoft Windows Server 2003 R2 через службы Microsoft Internet Information Services 6.0, удаленный злоумышленник может выполнить произвольный код или вызвать отказ условий обслуживания на целевом сервере. Главным образом это связано с уязвимостью переполнения буфера, вызванной ненадлежащей проверкой длинного заголовка в HTTP-запросе.
- Контентное удаленное выполнение кода в Apache Struts2 (CVE-2017-5638). В Apache Struts2 существует уязвимость удаленного выполнения кода с использованием многокомпонентного парсера Jakarta. Злоумышленник может воспользоваться этой уязвимостью, отправив недействительный тип содержимого в качестве части запроса на загрузку файла. Успешное использование может привести к выполнению произвольного кода в зараженной системе.
- Программа для утечки информации OpenSSL TLS DTLS Heartbeat (CVE-2014-0160; CVE-2014-0346). В пакете OpenSSL есть уязвимость, связанная с утечкой информации. Она возникает из-за ошибки при обработке heartbeat-пакетов TLS/DTLS. Злоумышленник может использовать эту уязвимость для раскрытия содержимого памяти подключенного клиента или сервера.

Делаем выводы

Известные уязвимости предоставляют киберпреступникам простую и относительно беспрепятственную точку входа в корпоративные сети, что позволяет им выполнять широкий спектр атак. Уязвимости устройств Интернета вещей часто являются "путем наименьшего сопротивления", поскольку как только одно устройство скомпрометировано, через него можно проникнуть в другие подключенные к нему устройства. Таким образом, для обеспечения безопасности сетей организациям крайне важно устанавливать патчи к известным уязвимостям, как только они становятся доступны. Для защиты от известных и неизвестных уязвимостей организациям необходимо разворачивать многоуровневую стратегию кибербезопасности, которая защищает как от кибератак известных семейств вредоносного ПО, так и от новых угроз.

Global Threat Impact Index и ThreatCloud Map разработаны ThreatCloud intelligence, самой большой совместной сетью по борьбе с киберпреступностью, которая предоставляет данные об угрозах и тенденциях атак из глобальной сети датчиков угроз. База данных ThreatCloud, содержащая более 250 млн адресов, проанализированных для обнаружения ботов, более 11 млн сигнатур вредоносных программ и более 5,5 млн зараженных сайтов, продолжает ежедневно идентифицировать миллионы вредоносных программ. ■