Comnews.ru, Москва, 13 мая 2019

КРИПТОМАЙНЕРЫ И ПРОЧИЕ НЕПРИЯТНОСТИ

Автор: Сюткина Влада

Начни утро с ComNews!

Самым активным вредоносным программным обеспечением (ПО) в I квартале 2019 года были криптомайнеры. В первой тройке - криптомайнеры Cryptoloot, Coinhive и XMRig. При этом в марте этого года Coinhive, прекративший работу восьмого марта, впервые с декабря 2017 года уступил верхнюю позицию. Такие данные приводят специалисты Check Point Research.

По словам технического директора Check Point Software Technologies в России Никиты Дурова, несмотря на то, что восьмого марта сервис Coinhive прекратил работу, одноименный зловред остался в топ-10 самых активных угроз марта. "В моменты своей самой активной работы Coinhive атаковал 23% организаций по всему миру", - отметил Никита Дуров, добавив, что, Coinhive может вновь возобновить свою деятельность. "Тем более что многие сайты все еще содержат JavaScript-код Coinhive и сегодня, хотя майнинг ими уже не осуществляется", - пояснил Никита Дуров.

Представитель компании Dr.Web Максим Якушев отметил, что согласно данным серверов статистики Dr.Web, в январе-апреле 2019 года наиболее активным оказалось рекламное ПО и другие нежелательные программы. В то время как в почтовом трафике преобладали вредоносные сценарии, написанные на JavaScript, а также угрозы, использующие уязвимость документов Microsoft Office. "К примеру, только в январе количество таких угроз выросло на 50% по сравнению с прошлым месяцем. Однако уже в феврале был зарегистрирован спад активности вредоносного ПО: статистика серверов Dr.Web зарегистрировала снижение количества уникальных угроз на 9,73% по сравнению с январем", - указал Максим Якушев.

Повышенная активность распространения рекламного ПО и других нежелательных программ, как заявил Максим Якушев, связана с условиями, созданными рекламными компаниями и меньшей потенциальной ответственностью за распространение такого ПО. "Что касается других вредоносных программ, то их активность в большей степени обусловлена активностью их авторов, нежели другими факторами", - добавил Максим Якушев.

В пресс-службе "Лаборатории Касперского" корреспонденту ComNews сообщили, что в I квартале 2019 года ландшафт киберугроз был примерно такой же как и годом ранее. "Однако наметилась интересная тенденция. В феврале количество срабатываний веб-антивируса на майнящие скрипты было на 29,09% меньше, чем в январе, в марте - на 14,08% меньше, чем в феврале, а в апреле уже на 37,06% меньше, чем, соответственно, в марте. Это удивительным образом совпадает с решением, пожалуй, самого известного веб-майнера Coinhive прекратить работу", - указали в "Лаборатории Касперского".

По словам технического директора Eset Russia Виталия Земских, широкий резонанс сейчас получают крупные атаки и взломы. "Но, если говорить о количественных измерениях, картина иная. В прошлом квартале среди киберугроз наиболее активна так называемая адварь (adware) - ПО, предназначенное для показа рекламы в браузере. Распространены вредоносные скрипты, перенаправляющие пользователей на потенциально опасные URL-адреса. Картина характерна как для мирового, так и для российского рейтингов киберугроз. Статистика учитывает число срабатываний антивирусных продуктов Eset на компьютерах пользователей", - проинформировал Виталий Земских.

Руководитель отдела аналитики информационной безопасности Positive Technologies Евгений Гнедин указал корреспонденту ComNews на то, что ряд тенденций, сформировавшихся в течение 2018 года, сохраняют свою актуальность и сейчас. "В частности, мотивацией киберпреступников в значительной доле атак является получение данных различной степени критичности", - рассказал Евгений Гнедин. Он также отметил, что общий тренд использования вредоносного ПО как одного из самых популярных методов атаки также в целом сохраняется и по сей день. "При этом доставляются зловреды

с помощью фишинговых рассылок - этот метод не теряет своей эффективности", - заметил Евгений Гнедин.

В пресс-службе "Лаборатории Касперского" корреспонденту ComNews указали, что тенденции I квартала 2019 года во многом повторяют тенденции IV квартала 2018 года. "Например, как в IV квартале 2018, так и в I квартале 2019 активно атаковали пользователей банковские троянцы Buhtrap и RTM, целью которых была кража денег со счетов малого и среднего бизнеса. Злоумышленников прежде всего интересуют бухгалтеры, а среди профессиональных сфер - информационные технологии, преимущественно региональные компании, юриспруденция и малое производство. Также пользователей продолжают атаковать майнеры и мобильные банковские троянцы", - рассказали в "Лаборатории Касперского".

Что касается наиболее ярких инцидентов в области информационной безопасности в I квартале 2019 года в компании сказали следующее: "В I квартале 2019 года эксперты "Лаборатории Касперского" выявили относительно новую схему распространения рекламного и вредоносного ПО через популярный торрент-трекер The Pirate Bay. Схема получила название PirateMatryoshka, поскольку включает в себя ряд компонентов, каждый из которых запускает действие последующего. Безусловно, многоуровневое вредоносное ПО - не редкость, однако PirateMatryoshka - очень изощренная угроза. Это пример массовой нецелевой атаки с применением фишинга. Проникая на компьютер жертвы, зловред открывает путь как нежелательным программам, так и вредоносному контенту, в том числе майнерам, стилерам и бэкдорам. В начале 2019 года мы продолжали наблюдать таргетированные атаки с использованием шифровальщиков. Один из ярких примеров, хоть и зафиксированный в апреле, - атака на Одинцовский водоканал. Также компанией были обнаружены сложнейшие целевые атаки - ShadowHammer и TajMhal".

По словам Никиты Дурова, одним из наиболее ярких событий в начале 2019 года стала обнаруженная специалистами Check Point Research уязвимость в защитном приложении Guard Provider, устанавливаемом на смартфоны компании Xiaomi. "Проблема потенциально могла затронуть более 150 млн мобильных устройств. С помощью этой уязвимости злоумышленники могли бы удаленно скомпрометировать смартфоны", - отметил Никита Дуров.

Представитель компании Dr.Web Максим Якушев указал корреспонденту ComNews на следующее: "Наиболее значимым инцидентом в январе-апреле 2019 года по мнению специалистов компании Dr.Web было обнаружение в популярном мобильном браузере UC Browser скрытой возможности загрузки и запуска непроверенного кода. Приложение способно скачивать вспомогательные программные модули в обход серверов Google Play. Это нарушает правила корпорации Google и представляет серьезную угрозу, поскольку таким образом на Android-устройства может быть загружен любой код, в том числе вредоносный. На момент обнаружения число загрузок UC Browser из Google Play превысило 500 млн. Всем установившим эту программу угрожает потенциальная опасность".

Виталий Земских сообщил корреспонденту ComNews о том, что в первом квартале компания Eset продолжила наблюдать атаки на цепочки поставок. "Это один из трендов кибербезопасности, которые мы анонсировали в 2018 году. В 2019 тенденция получила новое развитие. Пожалуй, наиболее резонансная история - компрометация Asus. Атакующие закрепились в сети компании и раздавали бэкдоры с помощью легитимного сервиса обновлений Asus Live Update. Число потенциальных жертв - сотни тысяч. Похожая схема использовалась в атаках на азиатских производителей компьютерных игр, о которых мы писали в марте. Для внедрения бэкдора скомпрометированы две игры и одна игровая платформа. Опасность атак на цепочки поставок в том, что их сложно обнаружить на стороне пользователя. Клиент по умолчанию доверяет разработчику своего софта и ставит рекомендуемые обновления без дополнительного анализа", - отметил он.

В компании Group-IB внимание корреспондента ComNews обратили на следующее: "В начале года Group-IB сообщила о масштабной волне вредоносных рассылок группы Silence в России. С начала года это самая крупная атака, насчитывающая более 80 000

получателей - сотрудников российских кредитно-финансовых организаций, среди которых основную долю занимают банки и крупные платежные системы. Массовая атака началась с фишинговых рассылок Silence 16 января. Впервые в практике Silence вредоносное вложение было замаскировано под приглашение на iFin-2019. В рамках январской кампании специалисты Group-IB обнаружили еще две фишинговые рассылки, нацеленные на российские банки, якобы от имени начальников отделов межбанковских операций несуществующих банков - ЗАО "Банк ICA" и ЗАО "Банкуралпром". Отправители обращались в банки с просьбой оперативно рассмотреть вопрос по открытию и обслуживанию корреспондентских счетов их организаций. Во вложении содержался архив с договором, при распаковке которого на компьютер пользователя загружалась все та же вредоносная программа Silence.Downloader".

По словам аналитика InfoWatch Андрея Арсентьева, говоря об утечках конфиденциальной информации, можно выделить несколько крупных инцидентов, зарегистрированных в I квартале. "Самая крупная утечка квартала, одна из самых масштабных в истории, - это компрометация данных из облачных баз компании verifications.io. В общей сложности исследователи обнаружили на незащищенных серверах Mongo DB более 2 млрд записей персональных данных, которыми оперировала эта маркетинговая компания. "Чемпионом" среди хакеров стал злоумышленник под сетевым ником Ghosticplayers. В феврале-марте он выложил в даркнет для продажи порядка 870 млн записей персональных данных, похищенных из нескольких десятков компаний. Вновь "отличилась" крупнейшая социальная сеть Facebook. Выяснилось, что компания не один год хранила сотни миллионов пользовательских паролей в незашифрованном виде, причем доступ к этим данным имели тысячи сотрудников. Из случаев похищения коммерческих секретов и производственных ноу-хау можно выделить инцидент в компании Coca-Cola. Ее бывший инженер обвиняется в краже технологий для производства упаковки. Компания оценивает ущерб в $120 млн", - рассказал Андрей Арсентьев.

Андрей Арсентьев отметил, что аналитический центр InfoWatch в январе-марте зарегистрировал почти на 19% больше утечек, чем в I квартале 2018 года. В общей сложности было скомпрометировано около 6,5 млрд записей пользовательских данных, что примерно в 4 раза больше, чем за аналогичный период прошлого года. "Если в результате хакерских атак утекло в 19 раз больше записей, то в ходе внутренних нарушений различного характера - в 2,5 раза больше. По сравнению с январем-мартом 2018 г. доля утечек, спровоцированных внешними злоумышленниками, выросла с 36,2% до 48%. Доля умышленных нарушений в общей совокупности утечек выросла с 55,8% до 71,1%. В I квартале утечек внутреннего характера не стало больше, но существенно изменилась их структура. Такие инциденты стали значительно опаснее для бизнеса и государственных структур. Во-первых, в январе-марте 2019 г. по сравнению с аналогичным периодом прошлого года выросла доля умышленных нарушений внутреннего характера - с 30,9% до 43,8%. Во-вторых, в результате действий внутренних нарушителей в несколько раз чаще стала утекать такая чувствительная информация, как коммерческие секреты и производственные ноу-хау", - отметил он.

Более половины всех утечек первого квартала, по словам Андрея Арсентьева, пришлось на три отрасли - высокотехнологичные компании (сфера связи и ИТ), медицина и госсектор (отрасли указаны в порядке убывания - прим. ComNews). Заметно выросло число утечек в ритейле, промышленности и муниципальных организациях.

"Одной из самых ярких тенденций I квартала стал заметный рост числа утечек конфиденциальной информации, хранящейся в незащищенных облачных базах. По итогам 2018 г. аналитики InfoWatch отметили рост числа таких утечек почти в 1,5 раза. Если тенденции I квартала сохранятся, то по итогам 2019 года, скорее всего, придется констатировать рост числа "облачных" утечек в разы. Стоит отметить, что более уязвимым становится сегмент АСУ ТП. Это связано как с общим ростом числа уязвимостей оборудования, так и с увеличением числа подключенных к Сети компонентов промышленных систем. Если проблема уязвимостей продолжит нарастать, а компании не будут уделять должного внимания защите систем, то, скорее всего, не за горами случаи

разрушительных атак на АСУ ТП, вплоть до полного вывода из строя критической инфраструктуры", - заявил Андрей Арсентьев.

Что касается прогноза ситуации в области информационной безопасности во II квартале 2019 года, Виталий Земских сказал следующее: "Думаю, что новые атаки на цепочки поставок не заставят себя ждать. Малые и средние компании, в отличие от корпораций, зачастую игнорируют вопросы безопасности. Что делает их идеальным инструментом целевых атак на крупные организации, выступающие их заказчиками. В этом плане для атакующих крайне интересны небольшие разработчики ПО. Как вы помните, в 2017 году эпидемия Petya/NotPetya началась с компрометации сервера обновлений бухгалтерского софта. Вероятно, увидим также компрометацию облачных сервисов".

В компании Group-IB относительно прогноза ситуации в области информационной безопасности во II квартале 2019 года корреспонденту ComNews заявили следующее: "Получив необходимый опыт для проведения целенаправленных атак на банки в России, группа Silence начала успешно применять свои навыки для атак на международные компании, активно готовя инфраструктуру и тестируя новые инструменты. Атака на банк в Индии - это лишь начало глобальной экспансии Silence. Помимо того, несмотря на арест весной 2018 года в испанском городе Аликанте одного из лидеров Cobalt, продолжаются атаки на финансовые организации. А несерьезное отношение антивирусных аналитиков, банков и e-commerce ресурсов к угрозе JS-снифферов, простота их использования и низкий уровень входа в преступную деятельность, может привести к росту количества зараженных сайтов, жертв и их скомпрометированных данных. В дополнение к этому, банковский Android-троян Anubis будет наиболее серьезной угрозой среди мобильных вредоносных программ. Также будут атаки со стороны Android-банкеров Red Alert и нового CometBot, а криптолокер Troldesh, один из самых популярных шифровальщиков, будет распространяться не только от имени банков, но их подрядчиков и компаний разных отраслей - ретейл, оптовая торговля, нефтегаз, строительство. Вместе с тем, в Европе, США, Канаде наиболее опасными банковскими троянами под Windows будут Backswap, Trickbot, Gootkit и IcedID. В Японии наиболее опасными банковскими троянами останутся Gozi и Ramnit. Новый банкер Danabot будет расширять географию и возможно начнет атаковать другие европейские страны, а не только Польшу".

По словам Андрея Арсентьева, скорее всего, во II квартале сохранится высокая хакерская активность. Заметную роль будут играть политически мотивированные атаки, то есть те, которые совершаются по заказу тех или иных государств. "Компания InfoWatch ожидает, что в ближайшие месяцы продолжит фиксироваться большое число утечек с незащищенных облачных серверов. Компании все шире используют облачные среды для более удобного хранения массивов данных, но не всегда учитывают все аспекты безопасности. Отсюда рост числа незащищенных хранилищ. Надо учитывать, что интерес к теме растет не только у исследователей, но и у злоумышленников - с помощью специальных поисковиков они активно изучают сетевое пространство на предмет наличия незащищенных серверов. Найдя такое хранилище, злоумышленники могут скопировать данные к себе, удалить их из базы и потребовать выкуп у компании. По мере роста конкуренции в различных отраслях повышается ценность коммерческой информации и ноу-хау. Поэтому, вполне вероятно, что во II квартале продолжится рост числа утечек данной информации. Прежде всего, он провоцируется умышленными действиями сотрудников и линейных руководителей", - указал Андрей Арсентьев.

http://www.comnews.ru/content/119486/2019-05-13/kriptomaynery-i-prochie-nepriyatnosti