«Лаборатория Касперского»: BlueNoroff опустошает счета криптовалютных стартапов

Эксперты «Лаборатории Касперского» раскрыли серию атак кибергруппы BlueNoroff на малый и средний бизнес по всему миру. Кампания, получившая название SnatchCrypto, нацелена на организации, которые работают с криптовалютами, смарт-контрактами, сервисами DeFi (децентрализованные финансы), блокчейном и финтех-индустрией. Злоумышленники делают ставку на человеческий фактор, отправляя сотрудникам организаций-жертв полнофункциональный бэкдор Windows под видом договора или другого документа. Чтобы красть криптовалюту, злоумышленники разработали сложную инфраструктуру, эксплойты, вредоносные импланты.

BlueNoroff входит в состав более крупной группы, Lazarus, и использует её диверсифицированную структуру и продвинутые технологии. Сейчас BlueNoroff сконцентрировалась на атаках на криптовалютные стартапы. Большинство таких компаний не могут позволить себе крупные инвестиции в систему безопасности. Злоумышленники знают об этом и применяют в атаках на стартапы сложные схемы социальной инженерии. Так, BlueNoroff рассылает письма якобы от существующих венчурных компаний в качестве приманки, чтобы заставить жертву открыть приложение к письму — документ с поддержкой макросов. Исследователи «Лаборатории Касперского» обнаружили, что в ходе кампании SnatchCrypto неправомерно использовались торговые марки и имена сотрудников более 15 венчурных организаций. Эксперты уверены, что реальные компании не имеют никакого отношения ни к атакам, ни к электронным письмам.

Открывая документ MS Word, внимательный пользователь может заметить, что происходит что-то подозрительное

Если документ с поддержкой макросов открывается на устройстве, не подключённом к интернету, он не представляет опасности. Скорее всего, он будет выглядеть как договор или другой безобидный документ. Но если в момент запуска файла компьютер подключён к интернету, то на устройство жертвы загружается другой документ с поддержкой макросов, развёртывающий вредоносное ПО.

В арсенале BlueNoroff есть различные методы заражения, которыми злоумышленники пользуются в зависимости от ситуации. Кроме заражённых документов Word группа также распространяет вредоносное ПО в архивных файлах с ярлыками Windows. Оно позволяет в дальнейшем создать полнофункциональный бэкдор. После этого BlueNoroff развёртывает другие вредоносные инструменты для наблюдения: клавиатурный шпион и программу для снятия скриншотов. Затем злоумышленники неделями или месяцами отслеживают нажатия клавиш и ежедневные действия пользователя, планируя стратегию кражи денег. Обнаружив подходящую потенциальную жертву, которая использует популярное браузерное расширение для управления криптокошельками (например, Metamask), они подменяют основной компонент расширения фейковой версией.

По данным исследователей, злоумышленники получают уведомление о крупных переводах. Когда скомпрометированный пользователь пытается перевести деньги на другой счёт, они перехватывают процесс транзакции и изменяют его. Чтобы завершить начатую транзакцию, пользователь нажимает «Подтвердить». В этот момент атакующие меняют адрес получателя и увеличивают сумму перевода до максимума, фактически опустошая счёт одним движением.

В настоящее время группа BlueNoroff активна и атакует пользователей в разных странах

«Поскольку злоумышленники постоянно придумывают новые способы обмана, даже малому бизнесу нужно обучать своих сотрудников основам кибербезопасности. Это особенно важно, если компания работает с криптокошельками: стоит помнить, что криптовалютные сервисы и расширения являются привлекательной целью как для кибергрупп, так и для рядовых мошенников, поэтому нуждаются в хорошей защите», — комментирует Сонсу Пак (Seonsgu Park), старший исследователь Глобального центра исследований и анализа угроз (GReAT) «Лаборатории Касперского».

Чтобы защитить организации, «Лаборатория Касперского» рекомендует соблюдать несколько важных мер безопасности:

- обучайте сотрудников азам кибербезопасности, поскольку многие целевые атаки начинаются с фишинга или других методов социальной инженерии;
- регулярно проводите аудит кибербезопасности сетей и устраняйте все уязвимости, обнаруживаемые в периметре или внутри сети;
- заражённое расширение трудно обнаружить вручную, если плохо знать Metamask. Однако модификация расширения Chrome оставляет след: браузер необходимо перевести в режим разработчика и установить расширение Metamask из локального каталога, а не из онлайн-репозитория. Если плагин устанавливается из онлайн-репозитория, Chrome активирует проверку цифровой подписи кода и гарантирует его целостность. Поэтому, если сомневаетесь, проверьте расширение Metamask и настройки Chrome прямо сейчас;
- установите EDR-решение и решение для защиты от сложных атак, которые позволяют выявлять угрозы, расследовать и своевременно устранять инциденты; предоставьте сотрудникам SOC доступ к актуальной информации об угрозах и регулярно развивайте их навыки с помощью специализированных тренингов;
- наряду с защитой конечных точек используйте сервисы для защиты от сложных атак. Сервис Kaspersky Endpoint Detection and Response поможет обнаружить и остановить атаку на ранних этапах, до того как злоумышленники достигнут своих целей.

***

За дополнительной информацией и комментариями, пожалуйста, обращайтесь в пресс-службу «Лаборатории Касперского» по адресу empr@kaspersky.com или по телефону +7 495 797 8700. Подписывайтесь на официальный канал пресс-службы в Telegram @Kaspersky4media и следите за нашими новостями в социальных сетях и на официальных ресурсах: