Группа с большими связями в киберпространстве захватывает крупную долю в хакерском мире.

Symantec – это компания, специализирующаяся на кибербезопасности и предоставляющая широкий спектр решений и услуг для защиты информации и систем от киберугроз.

 Компания Symantec разрабатывает и предлагает различные продукты, включая антивирусные программы, брандмауэры, системы обнаружения и предотвращения вторжений (IDS/IPS), шифрование данных, управление идентификацией и доступом, а также другие инструменты и решения для обеспечения безопасности.

 Symantec также предоставляет услуги консультации по кибербезопасности, включая аудиты безопасности, пентестинг, обучение персонала и реагирование на инциденты безопасности. Они помогают организациям определить уязвимости, разрабатывать стратегии защиты и реагировать на кибератаки." data-html="true" data-original-title="Symantec" >Symantec провела анализ недавно выявленной программы-вымогателя RansomHub и выяснила, что программа оказалась обновлённой и переименованной версией программы Knight, которая, в свою очередь, является эволюцией другого вымогателя — Cyclops.

Knight (также известный как Cyclops 2.0) впервые появился в мае 2023 года и использовал тактику двойного вымогательства, похищая и шифруя данные жертв для получения финансовой выгоды. вирус действует на множестве платформ, включая Windows, Linux, macOS, ESXi и Android.

Knight активно рекламировался и продавался на форуме RAMP. Атаки с его участием часто использовали фишинг для распространения вредоносных вложений. Деятельность Knight в качестве RaaS-модели была прекращена в конце февраля 2024 года, когда исходный код Knight был выставлен на продажу. Это дало основание полагать, что вирус мог перейти в руки нового владельца, который решил обновить и перезапустить его под брендом RansomHub.

Вирус RansomHub, первая жертва которого была зафиксирована в том же месяце, уже связан с серией недавних атак, среди которых Change Healthcare, Christie's и Frontier Communications. Примечательно, что новая версия вируса не атакует объекты в странах СНГ, на Кубе, в Северной Корее и Китае.

Компания Symantec отметила, что обе версии вируса написаны на языке Go, а большинство их вариантов скрыты с помощью Gobfuscate. Соответствие в коде между двумя семействами значительно, что затрудняет их различие. Оба вируса имеют идентичные справочные меню, но RansomHub добавил новую опцию sleep, которая

позволяет оставаться в режиме ожидания перед выполнением команд. Подобные команды наблюдались и в других вирусах – Chaos/Yashma и Trigona.

Сходства между Knight и RansomHub также включают технику скрытия строк, записки с требованиями выкупа и способность перезагружать систему в безопасном режиме перед началом шифрования. Основное различие состоит в наборе команд, выполняемых через cmd.exe, хотя последовательность их вызова остаётся неизменной.

Записка с требованием выкупа RansomHub

Атаки RansomHub используют уязвимости ZeroLogon для получения первоначального доступа и установки инструментов удалённого управления (Atera и Splashtop) до развертывания вымогателя. По данным Malwarebytes, в апреле 2024 года это RansomHub был связан с 26 атаками.

Более того, RansomHub пытается привлечь участников других группировок, включая LockBit и BlackCat. Сообщается, что один из бывших партнёров Noberus, известный как Notchy, уже работает с RansomHub. Кроме того, инструменты, ранее связанные с другим партнёром Noberus, Scattered Spider, были использованы в недавней атаке RansomHub.

Быстрое развитие RansomHub указывает на то, что группа, возможно, состоит из опытных хакеров с большими связями в киберпространстве. Развитие группы происходит на фоне значительного роста активности программ-вымогателей. Согласно отчету Mandiant, количество публикаций на сайтах утечек данных увеличилось на 75% по сравнению с предыдущим годом.