Как новая группа привлекает элиту киберпреступности с 90% комиссией.

В феврале 2024 года на арену киберпреступности вышла новая платформа RansomHub, предоставляющая услуги вымогательского ПО по модели Программа-вымогатель как услуга (Ransomware-as-a-Service, RaaS) – это бизнес-модель, при которой программа-вымогатель сдается в аренду киберпреступникам.

 Разработчик вымогательского ПО предоставляет готовый код шифровальщика другим хакерам. Клиент арендует код шифровальщика у его автора, настраивает его под себя, а затем использует в атаках по своему усмотрению.

 В Raas-модели разработчик программы-вымогателя забирает себе небольшой процент от выкупа жертвы, а большая часть средств достается атакующему.
" data-html="true" data-original-title="RaaS" >RaaS. Платформа заражает системы Windows, Linux и ESXi, используя вредоносное ПО на основе Go и C++. Новый отчет Insikt Group описывает ключевые аспекты деятельности RansomHub, ее связи с ранее известным ПО Knight и меры по защите от угрозы

Группировка быстро набрала обороты и стала четвертой по числу публично заявленных атак за последние 3 месяца. А привлекательная комиссия в 90% привлекает опытных аффилиатов, что приводит к резкому скачку числа заражений.

С момента своего появления RansomHub нанес вред 45 жертвам в 18 странах, преимущественно в ИТ-секторе. Такой факт указывает на стратегию «охоты на крупную дичь», когда злоумышленники выбирают такие компании, которые с большей вероятностью выплатят значительные суммы выкупа из-за серьезных финансовых последствий простоя.

Особо примечательна тактика использования RansomHub неправильно настроенных экземпляров Amazon S3 для доступа к резервным копиям не только основного объекта атаки, но и других клиентов того же поставщика резервных копий. В таких атаках киберпреступники шантажируют поставщиков решений по резервному копированию, угрожая утечкой данных клиентов.

Insikt Group выявила пересечения в коде между RansomHub и другими группами вымогателей, такими как ALPHV (BlackCat) и Knight Ransomware. Сходства могут свидетельствовать о возможных связях или общих ресурсах среди групп.

Напомним, что 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.

Версии шифровальщика RansomHub для Linux и Windows написаны на Go, а новая версия ESXi — на C+. Отметим, что создание шифратора ESXi позволяет злоумышленникам увеличить базу потенциальных целей – группа может ориентироваться на растущее число предприятий, использующих виртуализированные среды.

Insikt Group – это подразделение компании Recorded Future, специализирующееся на исследовании угроз в области кибербезопасности. Группа занимается анализом и мониторингом киберактивностей, выявлением и изучением киберугроз, а также разработкой стратегий для защиты от них. В своих расследованиях группа использует разнообразные источники данных, предоставляя доклады и аналитические материалы, которые помогают организациям и государственным учреждениям защититься от сложных и развивающихся киберугроз." data-html="true" data-original-title="Insikt Group" >Insikt Group обнаружила, что версия RansomHub для ESXi создает файл /tmp/app.pid, чтобы предотвратить запуск одновременно нескольких экземпляров. Специалисты также нашли уязвимость в коде: если файл содержит «-1», вредоносное ПО попытается завершить несуществующий процесс, что приведет к бесконечному циклу и остановит шифрование данных.

Для защиты от RansomHub Insikt Group разработала правила YARA и Sigma, которые могут использоваться для обнаружения присутствия или выполнения файлов вымогательского ПО в затронутой среде. Правила охватывают версии для ESXi, Linux и Windows. Аналитики могут искать в логах командной строки команды, используемые RansomHub для остановки виртуальных машин, удаления теневых копий и остановки службы Internet Information Service (IIS).

На перекрестке науки и фантазии — наш канал