Сайт вымогателей Qilin пропал после атаки на лондонские больницы.

Специалисты Recorded Future сообщают, что 5 июня сайт вымогателей Qilin внезапно перестал работать. Утром он был доступен, но позже начал отображаться код ошибки 0xF2, что обычно указывает на перенос сайта на новый сервер. Причина недоступности сайта пока неясна. Специалисты предполагают, что это может быть результатом действий правоохранительных органов или намеренным отключением сайта самой группой.

Сайт Qilin отображает ошибку 0xF2

Если сайт Qilin был отключен в ответ на атаку на медучреждения Лондона, которая привела к введению режима ЧС, это было бы удивительно быстрой реакцией правоохранительных органов.

Стоит отметить, что в последние месяцы правоохранительные органы проводят множество операций по срыву деятельности различных групп вымогателей. Возможно, хотя и не доказано, что международная коалиция уже имела доступ к системам Qilin и выбрала этот момент для того, чтобы сорвать деятельность группировки.

С другой стороны, отключение сайта не обязательно указывает на действия правоохранительных органов, так как .Onion – псевдо-домен верхнего уровня, созданный для обеспечения доступа к анонимным или псевдо-анонимным адресам сети Tor. Подобные адреса не являются полноценными записями DNS, и информация о них не хранится в корневых серверах DNS. Но при установке дополнительного программного обеспечения, необходимого для выхода в сеть Tor, программы, работающие с Интернетом, получают доступ к сайтам в доменной зоне .onion, посылая запрос через сеть Tor-серверов." data-html="true" data-original-title="Onion" >onion сайты, используемые киберпреступными группами, известны своей ненадежностью. Возможно, что сама группа решила отключить сайт, чтобы избежать дополнительного внимания после крупного инцидента.

Аффилированные участники группы Qilin (Agenda), предоставляющей вымогательское ПО как услугу (Ransomware-as-a-Service, 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), зарабатывают большие деньги на своих кибератаках. Группа Qilin действует по крайней мере с августа 2022 года и предоставляет своим партнерам 80% – 85% от суммы выкупа.

На перекрестке науки и фантазии — наш канал