

В сети уже оказались 3,7 ГБ конфиденциальных сведений. Что будет дальше?

В начале июня хакерская группировка Qilin совершила масштабную кибератаку на частную компанию Synnovis, которая предоставляет лабораторные услуги нескольким крупным больницам Лондона. Это привело к серьезным сбоям в работе медучреждений.

На днях хакеры неожиданно заявили, что их действия были политически мотивированным протестом. В анонимной переписке с BBC они принесли извинения за причиненные неудобства, но свою вину открыто не признали. По словам киберпреступников, атака была совершена в отместку британскому правительству за его действия в неназванном военном конфликте.

В результате инцидента пострадали семь больниц, управляемых двумя трастами NHS. Медучреждениям пришлось отменить или перенести почти 1600 операций и амбулаторных приемов, включая онкологические операции и даже трансплантацию органов.

Долгое время пострадавшая компания и следователи не разглашали подробностей расследования. Как стало известно сейчас, хакеры проникли в IT-систему Synnovis, зашифровали файлы и потребовали выкуп за восстановление доступа. Стоит отметить, что общая сумма контрактов трастов с Synnovis составляет внушительную цифру – почти 1,1 миллиарда фунтов стерлингов, что подчеркивает важность компании для системы здравоохранения.

На одной из платформ для обмена сообщениями группировка Qilin опубликовала 104 файла, каждый объемом 3,7 ГБ. Публикация сопровождается логотипом Synnovis, описанием компании и ссылкой на ее официальный сайт. По информации BBC, опубликованные данные могут включать в себя имена пациентов, даты рождения, номера NHS. На данный момент неизвестно, есть ли среди утекших файлов результаты анализов.

NHS England заверила общественность, что совместно с Национальным центром кибербезопасности и другими партнерами проводится тщательный анализ данных для подтверждения их происхождения и содержания. Представители службы подчеркнули серьезность ситуации: "Мы понимаем, насколько тревожным может быть это развитие событий для многих людей. Относимся к нему крайне серьезно".

Исследователи отмечают, что публикация украденных данных обычно указывает на

Группа Qilin, погрузившая больницы Лондона в хаос, требует деньги за спокойствие пациентов

отказ компании-жертвы выплатить требуемый выкуп. Как правило, злоумышленники требуют оплату в биткойнах за расшифровку систем или удаление похищенных сведений.

Произошедший инцидент в очередной раз демонстрирует необходимость повышения уровня кибербезопасности в медицинском секторе, который становится все более привлекательной мишенью для киберпреступников из-за ценности информации, хранящейся в системах больниц и поликлиник.