Как хакеры смогли месяц находиться в сетях незаметно.

Дерматологическая клиника Affiliated Dermatologists (AD) стала жертвой вымогательской атаки группы BianLian, в результате которой были раскрыты персональные данные пациентов и сотрудников. Инцидент стал известен, когда злоумышленники оставили записку с требованиями выкупа в сети клиники.

10 апреля 2024 года руководство AD установило, что между 2 и 5 марта 2024 года хакеры получили доступ к системам и скопировали данные из сети клиники. Среди украденной информации оказались:

Представители клиники в письме клиентам подчеркнули, что объём утекшей информации варьируется для каждого пострадавшего, и не все категории данных присутствуют у каждого из них. По данным генпрокурора штата Мэн, инцидент затронул около 373 000 человек.

После обнаружения атаки AD предприняли срочные меры по отключению доступа к своей сети и привлекли ИБ-специалистов для восстановления системы. Кроме того, клиника предлагает пострадавшим бесплатный кредитный мониторинг и защиту от кражи личных данных.

Группировка, действующая с июня 2022 года, уже атаковала различные критически важные системы по всему миру. Так, например, в июле 2024 года хакеры украли 300 ГБ данных французской больницы CHU, а в сентябре BianLian объявила о том, что взломала ИТ-системы одной из ведущих некоммерческих организаций в мире, предположительно – международной благотворительной организации Save The Children International.

Кроме того, в марте ИБ-компания GuidePoint Security обнаружила, что группировка BianLian эксплуатирует уязвимости в программном обеспечении JetBrains TeamCity для проведения вымогательских атак.