Данные клиентов люксового магазина выставлены на продажу в даркнете.

Американский ритейлер Neiman Marcus – это американская люксовая сеть универмагов, основанная в 1907 году. Компания предлагает широкий ассортимент высококачественных товаров, включая одежду, обувь, аксессуары, косметику и предметы интерьера. Neiman Marcus славится своим исключительным уровнем обслуживания клиентов и эксклюзивными продуктами, делая акцент на элитный и премиальный сегмент рынка. Основные магазины сети расположены в крупных городах США, а также работает интернет-магазин, позволяющий совершать покупки онлайн." data-html="true" data-original-title="Neiman Marcus" >Neiman Marcus подтвердил утечку данных после кибератаки, в результате которой злоумышленники попытались продать украденную базу данных компании. Инцидент произошёл в рамках недавней массовой компрометации аккаунтов на платформе В контексте сети Tor, Snowflake это тип моста, который помогает пользователям получить доступ к сети Tor в странах, где она заблокирована.<br /> Snowflake это комбинация JavaScript-базированного прокси и моста, которая позволяет пользователям получить доступ к сети Tor через веб-браузер, без необходимости загружать и настраивать программное обеспечение Tor." data-html="true" data-original-title="Snowflake" >Snowflake.

Согласно уведомлению о нарушении данных, поданному в офис Генерального прокурора штата Мэн, утечка затронула 64 472 человека. В компании сообщили, что несанкционированный доступ к базе данных был получен в период с апреля по май 2024 года.

В ходе расследования установлено, что злоумышленники также получили доступ к персональной информации клиентов. В числе украденных данных оказались имена, контактная информация, даты рождения и номера подарочных карт Neiman Marcus и Bergdorf Goodman. Коды активации подарочных карт не были скомпрометированы, в связи с чем они остаются действительными.

Neiman Marcus отключил доступ к платформе базы данных сразу после обнаружения утечки, инициировал расследование с участием экспертов по кибербезопасности и уведомил правоохранительные органы. Компания также подтвердила, что данные были украдены из её аккаунта в Snowflake.

Информация о нарушении безопасности появилась после того, как хакер под псевдонимом «Sp1d3r» выставил данные Neiman Marcus на продажу на хакерском форуме за $150 000. Этот же злоумышленник связан с продажей данных множества компаний, пострадавших в ходе недавних атак на платформу Snowflake.

По данным «Sp1d3r», украденная информация включала последние четыре цифры номеров социального страхования, данные о транзакциях клиентов, их электронные адреса, истории покупок, данные сотрудников и миллионы номеров подарочных карт (без кодов активации). Также сообщается, что хакер пытался шантажировать Neiman Marcus перед публикацией данных, но не получил ответа.

Исследование, проведённое компанией Snowflake совместно с Mandiant и CrowdStrike, выявило, что злоумышленник, известный как UNC5537, использовал украденные учётные данные для атаки на 165 организаций, не настроивших многофакторную аутентификацию. Группировка UNC5537 широко известна в исследовательском сообществе своими финансово мотивированными киберпреступлениями.

Для атаки злоумышленники использовали украденные учётные данные, которые не были обновлены или изменены в течение нескольких лет. Помимо Neiman Marcus от компрометации аккаунтов Snowflake пострадали также компании Santander, Ticketmaster, LendingTree, Advance Auto Parts, Los Angeles Unified и Pure Storage.

Конечно, по факту жертв гораздо больше, но пока только вышеперечисленные организации публично заявили об утечке. В будущем мы ещё услышим о множестве компаний, пострадавших в рамках данной атаки.