История о том, как две компании борются за правду.

Компания Hudson Rock – это компания, специализирующаяся на кибербезопасности и защите данных. Они известны благодаря своему продукту под названием «BreachArmor», который предлагает услуги мониторинга утечек данных и предупреждает клиентов о возможных угрозах для их конфиденциальной информации.

 Hudson Rock получила значительное внимание в СМИ в 2021 году, когда её исследователи обнаружили одну из крупнейших утечек данных в истории — базу данных с 533 миллионами аккаунтов социальной сети Facebook, которая была опубликована в открытом доступе в Интернете. Это вызвало серьезные обсуждения о проблемах конфиденциальности данных платформы и подчеркнуло важность кибербезопасности в современном Интернете." data-html="true" data-original-title="Hudson Rock" >Hudson Rock удалила свой онлайн-отчёт о взломе систем облачного хранения и аналитики В контексте сети Tor, Snowflake это тип моста, который помогает пользователям получить доступ к сети Tor в странах, где она заблокирована.
 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, ссылаясь на юридическое давление со стороны последней. В отчёте утверждалось, что злоумышленники получили доступ к системам Snowflake и украли данные сотен клиентов, включая информацию клиентов Ticketmaster — это американская компания, специализирующаяся на продаже билетов на различные мероприятия, включая концерты, спортивные соревнования, театральные постановки и другие развлекательные события. Она предоставляет услуги онлайн-бронирования и продажу билетов, а также предлагает решения для управления событиями и контроля доступа." data-html="true" data-original-title="Ticketmaster" >Ticketmaster и Santander Bank.

Hudson Rock заявила, что преступники получили доступ к учетным данным сотрудника Snowflake с помощью вредоносного ПО, что позволило им выгрузить огромное количество данных из облачных аккаунтов клиентов Snowflake. Однако, Snowflake утверждает, что такого взлома не было.

Хотя известно, что данные Ticketmaster и Santander действительно были украдены, точные детали о способе и источнике утечки пока не известны. Представитель Ticketmaster сообщил, что украденные данные были размещены в Snowflake.

Snowflake заявляет, что если данные клиентов и были украдены, то это могло произойти из-за компрометации учетных данных самих клиентов через фишинг, утечки

или вредоносное ПО, а не из-за взлома их собственных систем безопасности. Компания считает, что ограниченное число клиентов действительно могли пострадать из-за использования украденных учетных данных, особенно если у них не была включена двухфакторная аутентификация.

Компания категорически отрицает взлом своих систем и настояла на том, чтобы Hudson Rock удалила свой отчет, в котором утверждалось обратное. 3 июня Hudson Rock заявила, что удаляет весь контент, связанный с их отчетом, в соответствии с полученным от Snowflake юридическим письмом. От дальнейших комментариев компания отказалась.

Заявление Hudson Rock об удалении контента

31 мая Hudson Rock опубликовала ныне удалённый отчёт, в котором утверждалось, что злоумышленники использовали учетную запись сотрудника Snowflake в ServiceNow для доступа к базам данных до 400 корпоративных клиентов Snowflake. При этом заявлялось, что хакеры сами связались с Hudson Rock и предоставили информацию о масштабе взлома.

В Snowflake подтвердили, что учетные данные сотрудника действительно были украдены, но они использовались только для доступа к демонстрационным учетным записям, не содержащим конфиденциальных данных. Учетные записи не были защищены многофакторной аутентификацией, в отличие от производственных и корпоративных систем Snowflake.

Тем временем Snowflake признала, что ограниченное число клиентов Snowflake могли подвергнуться атаке из-за целевой кампании против пользователей без MFA. Злоумышленники могли использовать учетные данные, полученные через фишинг или вредоносное ПО, чтобы получить доступ к облачным хранилищам клиентов.

Snowflake не выявила доказательств, что взлом был вызван компрометацией учетных данных текущих или бывших сотрудников Snowflake или уязвимостью платформы компании. Вместе с CrowdStrike и Mandiant – это компания, которая занимается информационной безопасностью и аналитикой инцидентов. Она специализируется на обнаружении и решении вопросов, связанных с киберпреступностью, таких как взломы, шпионаж, вредоносное ПО и кибертерроризм. Компания предлагает широкий спектр услуг, включая аналитику инцидентов, консультационные услуги, создание и тестирование систем защиты, а также обучение и поддержку.
 Компания также

сотрудничает с правоохранительными органами по всему" data-html="true" data-original-title="Mandiant" >Mandiant, Snowflake продолжает расследование инцидента, настоятельно рекомендуя клиентам включить многофакторную аутентификацию.

Тем временем, другие крупные клиенты Snowflake, такие как Live Nation Entertainment, уже сообщили о несанкционированной активности в своих облачных базах данных. Также поступили сообщения от ИБ-специалистов, что другие клиенты Snowflake могли пострадать от кражи данных в мае.

CrowdStrike и Mandiant отказались комментировать ситуацию, ссылаясь на продолжающееся расследование. Snowflake также отказалась назвать конкретных клиентов, чьи данные были скомпрометированы.