Хакеры ShinyHunters рассказали, как они получили доступ к данным сотен компаний.

В последние недели мир стал свидетелем масштабной кибератаки на компанию 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, специализирующуюся на облачном хранении данных. Хакеры ShinyHunters — это хакерская группировка, которая специализируется на похищении и продаже пользовательских данных с различных сайтов и сервисов. Группировка впервые привлекла внимание в апреле 2020 года и с тех пор взяла на себя ответственность за ряд громких утечек данных, в том числе Tokopedia, Wattpad, Pixlr, Bonobos, BigBasket, Mathway, Unacademy, MeetMindful, учетной записи Microsoft в GitHub и т.д.

 Группировка атакует сайты и репозитории разработчиков с целью похищения учетных данных или API-ключей для доступа к облачным сервисам целевых компаний. С помощью API-ключей киберпреступники получают доступ к корпоративным базам данных и похищают информацию для дальнейшей продажи или бесплатной публикации на хакерских форумах." data-html="true" data-original-title="ShinyHunters" >ShinyHunters получили доступ к учетным записям Snowflake, предварительно взломав компанию-подрядчика EPAM Systems, которая сотрудничает с клиентами Snowflake.

По предварительным данным, пострадало около 165 компаний, однако на сегодняшний день идентифицированы лишь несколько из них. Самые заметные жертвы взлома – компания по продаже билетов Ticketmaster и банк Santander, который не уточнил, откуда были украдены данные. Однако издание Wired установило, что данные банка были украдены с помощью учетной записи Snowflake, содержащей банковские реквизиты 30 миллионов клиентов, включая номера счетов, балансы, номера карт и информацию о персонале.

Snowflake пока не раскрыла детали, каким образом хакеры получили доступ к учетным записям, лишь отметив, что сеть компании не была взломана напрямую. Безопасностью инцидента занимается компания Mandiant. В своем блоге Mandiant сообщила, что в некоторых случаях злоумышленники получили доступ через подрядчиков, не уточняя, каких именно.

Тем не менее, один из хакеров, общавшийся с Wired, назвал EPAM Systems одной из таких компаний. По словам хакера, группа ShinyHunters использовала данные,

найденные в системе сотрудника EPAM, чтобы получить доступ к учетным записям Snowflake.

EPAM Systems отвергла свою причастность ко взломам, назвав заявления хакеров ложью. Однако, по словам хакера, доступ к учетным записям Snowflake был получен через заражение компьютера сотрудника EPAM в Украине с помощью вредоносного ПО. На компьютере были найдены незашифрованные логины и пароли, которые использовались для управления учетными записями клиентов Snowflake, в том числе и 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.

Кроме того, оказалось, что в учетных записях Snowflake отсутствовала многофакторная аутентификация, что позволило хакерам получить доступ через логины и пароли. Это еще раз подчеркивает важность использования многофакторной аутентификации для защиты данных.

Компании Snowflake и EPAM Systems продолжают расследование инцидента. Snowflake заявила о планах внедрить обязательное использование многофакторной аутентификации для всех своих клиентов в ближайшее время, чтобы предотвратить подобные инциденты в будущем.

Ситуация также обострила внимание к растущим рискам безопасности, связанным с использованием сторонних подрядчиков и вредоносного ПО. Mandiant указала на значительные риски, которые представляют подрядчики, имеющие доступ к системам множества клиентов.

Компрометация одного устройства подрядчика может дать злоумышленникам доступ к данным многих организаций. Стоит отметить, что помимо Ticketmaster и Santander от компрометации аккаунтов Snowflake пострадали также компании Neiman Marcus, LendingTree, Advance Auto Parts и Pure Storage.

На перекрестке науки и фантазии — наш канал