30 миллионов клиентов навсегда попрощались с данными своих карт.

Группа хакеров 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 заявила о взломе Santander Bank, одного из мировых лидеров в финансовой сфере. В результате атаки были похищены личные данные более 30 миллионов клиентов, которые сейчас выставлены на продажу за $2 миллиона.

Santander Bank, со штаб-квартирой в Испании и огромной сетью из 8518 филиалов по всему миру, подтвердил утечку данных. В первую очередь она затронула клиентов в Испании, Чили и Уругвае, а также некоторых сотрудников банка. В заявлении компании говорится, что утечка произошла через стороннего подрядчика.

ShinyHunters, известная своими масштабными кибератаками, недавно также взяла на себя ответственность за взлом американской компании Ticketmaster, где были украдены 560 миллионов пользовательских записей, включая частичные данные платёжных карт.

Группировка ShinyHunters в настоящий момент является владельцем и администратором BreachForums – онлайн-сообщество, которое специализируется на обсуждении информационной безопасности и кибербезопасности. Участники могут обмениваться информацией о свежих уязвимостях, обнаруженных уязвимостях, техниках и способах защиты, а также обмениваться инструментами и скриптами. На форумах также можно найти информацию о продаже и покупке учетных данных, информационных баз и другой конфиденциальной информации. Некоторые форумы также предоставляют сервисы для проверки на уязвимости и тестирования защиты. Однако, некоторая информация может быть незаконной и неэтичной, и может использоваться для неправомерных действий." data-html="true" data-original-title="BreachForums" >BreachForums, известной платформы для киберпреступлений.

Несмотря на недавние усилия ФБР по закрытию форума, группа быстро восстановила его инфраструктуру. Кроме того, у киберпреступников уже появилась альтернатива в лице Breach Nation, запущенной хакером под псевдонимом USDoD.

Касательно взлома Santander Bank, представители ShinyHunters предлагают на продажу массив данных, включающий:

Доступность столь большого объёма чувствительной финансовой информации вызывает серьёзные опасения по поводу возможности кражи личных данных, мошенничества и других незаконных действий. Этот инцидент подчёркивает постоянные угрозы, с которыми сталкиваются финансовые учреждения и их клиенты.

Santander Bank уже предпринял меры по устранению последствий утечки, однако клиентам рекомендуется внимательно следить за своими счетами на предмет подозрительной активности. Также рекомендуется использовать двухфакторную аутентификацию и регулярно обновлять пароли, чтобы снизить риск дальнейшего использования данных киберпреступниками.