Хакеры нанесли сильный удар по билетной империи, опубликовав 1,3 ТБ данных компании.

IT-системы 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 предположительно были взломаны киберпреступниками, которые утверждают, что украли 1,3 ТБ данных о 560 миллионах клиентов корпорации – и теперь продают всю информацию за $500 000.

Злоумышленники заявили, что получили доступ к личной информации, включая имена, адреса электронной почты, номера телефонов, физические адреса, данные о заказах и частично данные кредитных карт.

Министерство внутренних дел Австралии подтвердило, что правительство осведомлено об инциденте и Национальное управление кибербезопасности уже взаимодействует с Ticketmaster для выяснения всех обстоятельств. Однако сама Ticketmaster пока не дала никаких комментариев по поводу произошедшего и не сообщила, когда именно данные были украдены.

Группировка 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 выставила предположительно украденные файлы Ticketmaster на продажу на даркнет-форуме и заявила, что данные включают «детали мошенничества с клиентами» и «многое другое».

Сомнения по поводу подлинности данных высказали специалисты из VX-Underground – это сообщество и архив, посвященные кибербезопасности и хакерству. Оно было основано в 2000 году и стало одним из ведущих источников информации о

компьютерных вирусах, вредоносных программ и других аспектах кибератак. В сообществе участвуют как профессионалы в области информационной безопасности, так и люди с большим интересом к хакерской культуре." data-html="true" data-original-title="VX-Underground" >VX-Underground. По их информации, кражу могли совершить другие преступники, а ShinyHunters лишь продают похищенное от их имени. База данных, предположительно, содержит записи с 2011 года и даже ранее.

Аналитик угроз из Emsisoft Бретт Кэллоу отметил, что пока неясно, является ли база данных подлинной и когда именно она была получена. Однако, судя по опубликованным скриншотам, продажа данных началась 28 мая на вновь возрожденном форуме 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, администратором которого является ShinyHunters.

Объявление о продаже данных Ticketmaster

ShinyHunters также утверждают, что пытались связаться с Ticketmaster перед тем, как выставить данные на продажу, но не получили ответа. Группа уже известна по другим громким кибератакам, включая кражу данных 70 миллионов клиентов AT&T, которые они пытались продать за $1 миллион.

Утечка данных произошла в неудачное время для Ticketmaster, принадлежащей корпорации Live Nation — это американская компания, занимающаяся организацией и продвижением живых музыкальных и развлекательных мероприятий. Она занимается концертами, фестивалями и турами артистов, а также управляет рядом концертных площадок и оказывает услуги по продаже билетов." data-html="true" data-original-title="Live Nation" >Live Nation Entertainment. Недавно Министерство юстиции США подало в суд на компанию за её антиконкурентные действия и монопольный контроль над индустрией живых концертов.

В ИБ-компании Dasera отреагировали на атаку, заявив The Register, что утечка данных может серьёзно повлиять на репутацию и доверие клиентов Ticketmaster. По мнению Dasera, для восстановления доверия компания должна быть максимально прозрачной о случившемся инциденте, его последствиях и мерах, предпринимаемых для предотвращения подобных ситуаций в будущем. Dasera предлагает провести полный аудит и пересмотр всей системы безопасности Ticketmaster.

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.

BreachForums долгое время был головной болью для правоохранительных органов. Его бывший администратор Конор Брайан Фицпатрик, известный под псевдонимом «Pompompurin», был приговорён к 20 годам условного наказания в январе, но Shiny Hunters возродила BreachForums, в который привлекла новых участников, а чуть позже новый сайт подвергся взлому, и данные более 4700 пользователей оказалась в сети.

Затем ФБР снова захватило сайт, а после захвата инфраструктуры BreachForums популярный хакер USDoD объявил о запуске Breach Nation всего через 24 часа после того, как на главной странице BreachForums появилось уведомление о захвате сайта ФБР.