Как криптографам удалось восстановить 20-символьный код RoboForm спустя 11 лет?

В современном мире, где криптовалюты становятся все более популярными, историй о потерянных и вновь обретенных цифровых сокровищах становится все больше. Одна из таких историй произошла с европейским криптоинвестором, которого мы будем называть «Майкл».

Два года назад Майкл обратился за помощью к известному специалисту по взлому аппаратных систем Джо Гранду. Дело в том, что в 2013 году, когда стоимость биткойнов была относительно невысокой, Майкл решил обезопасить свои 43,6 BTC (на тот момент около $5300) от возможных кибератак.

Для этого он использовал программный кошелек — специальное приложение для хранения криптовалюты на компьютере в зашифрованном виде. В отличие от аппаратных кошельков, представляющих собой физические устройства, программные решения более уязвимы для взлома, но при правильной настройке также могут обеспечить высокий уровень защиты.

Майкл сгенерировал 20-символьный пароль с помощью менеджера паролей RoboForm, а затем зашифровал его при помощи утилиты TrueCrypt. Впоследствии этот зашифрованный файл был поврежден, и единственная копия пароля оказалась недоступной.

На протяжении нескольких лет Майкл безуспешно пытался вернуть свои сбережения. Он обращался к различным экспертам по криптографии, но все они лишь разводили руками — шансов практически не оставалось. В 2022 году Гранд смог помочь другому человеку, разблокировав кошелек Trezor с помощью сложных аппаратных методов взлома. Однако случай Майкла отличался тем, что он использовал программный, а не аппаратный кошелек, что существенно затрудняло задачу.

Первоначально Гранд отказался браться за это дело, но спустя время Майкл снова обратился к нему, и на этот раз хакер согласился. Для совместной работы он привлек своего давнего друга Бруно из Германии, также имеющего опыт во взломе цифровых кошельков.

На протяжении многих месяцев Гранд и Бруно изучали старую версию RoboForm , которую, предположительно, использовал Майкл. И вот, после долгих усилий они обнаружили критическую уязвимость в генераторе псевдослучайных чисел, отвечающем за создание паролей. Оказалось, что пароли привязывались к дате и

времени на компьютере пользователя, из-за чего их можно было предсказать с довольно высокой точностью.

Оставалась одна важная проблема: Майкл не помнил, когда именно сгенерировал злополучный пароль. По записям в кошельке было видно, что первая транзакция прошла 14 апреля 2013 года. Но четкой даты все же не было. Команде пришлось перебирать различные временные периоды и параметры генерации, что заняло еще больше времени.

Гранду и Бруно приходилось регулярно обращаться к Майклу за уточнениями, досаждая ему расспросами о событиях десятилетней давности. Криптоинвестор приводил примеры старых паролей RoboForm, но их параметры порой различались. Однако в ноябре 2022 года специалисты наконец добились прорыва и смогли встретиться с Майклом лично, чтобы поделиться потрясающей новостью. Им все же удалось воссоздать оригинальный 20-символьный пароль, сгенерированный 15 мая 2013 года в 16:10 по Гринвичу.

По последним данным, команда разработчиков RoboForm, по всей видимости, осознала критичность уязвимости и исправила ее в версии 7.9.14 от 10 июня 2015 года, увеличив энтропию генератора. Однако компания не проинформировала своих 6 миллионов пользователей о необходимости сгенерировать новые пароли для важных учетных записей.

По мнению Гранда, это могло оставить уязвимыми тех, кто продолжал использовать скомпрометированные пароли. Он также не уверен, что последующие версии RoboForm полностью защищены от подобных проблем, так как неизвестно, какие именно действия предприняли разработчики.

Что касается Майкла, то для него вся эта история оказалась весьма выгодной. момент восстановления доступа к кошельку стоимость его 43,6 BTC составляла $2,6 млн. Он выждал еще несколько месяцев, а когда курс Биткойн — это криптовалюта, использующая технологию блокчейн для совершения платежей и обеспечения целостности транзакций. Биткойн является децентрализованной валютой, то есть его не контролирует никакой государственный орган или банк. Биткойн поддерживается сетью компьютеров, расположенных по всему миру, которые обрабатывают и подтверждают транзакции в блокчейне. Он может использоваться для оплаты товаров и услуг или для обмена на другую валюту." data-html="true" data-original-title="Биткойн" >биткойна вырос до $62 000 за монету, продал часть активов. Сейчас на его счету осталось 30 BTC общей стоимостью около $3 млн.

И мужчина не спешит расставаться с ними, рассчитывая на дальнейший рост курса до $100 000. Как он сам с улыбкой признался, то, что он потерял доступ к своему кошельку несколько лет назад, в итоге сослужило ему хорошую службу. В противном случае он мог распродать все биткойны еще при курсе $40 000 и лишиться будущих миллионов.

На перекрестке науки и фантазии — наш канал