Finding the Bitcoin wallet from 10 years ago, the guy made 500 times more profit

He said he felt lucky because he lost his wallet password. Because if not, he will sell all the Bitcoin he has, missing the opportunity to earn a fortune 500 times higher than when he bought it.

2 years ago, a cryptocurrency player named 'Michael' contacted hacker Joe Grand to help restore access to more than $2.7 million worth of Bitcoin, stored in encrypted format on his computer. But Grand refused.

Specifically, Michael stored his 43.6 BTC (worth about 4,000 euros, equivalent to 5,300 USD in 2013) in a digital wallet with a password. He created the password using the RoboForm password manager and saved it in an encrypted file using the TrueCrypt tool. After some time, this file became corrupted and Michael lost the previously created 20-character password.

The journey to find the lost Bitcoin wallet password from 10 years ago

The person Michael sought help from was Joe Grand - a famous hardware hacker, nicknamed 'Kingpin'. In 2022, this person helped another person regain access to 2 million USD in money just because he forgot the PIN code to his Trezor wallet. Since then, dozens of people have contacted Grand to help them get their property back. But most were rejected by Grand for many reasons.

In Michael's case, he stored his assets in an electronic wallet software, which means Grand's hardware hacking skills cannot help. Grand considered brute-force - writing a script to automatically guess millions of possible passwords to find Michael's exact password. But he realized this approach was not feasible.

Then, the hacker also thought about the probability that the RoboForm program could make mistakes when creating the password, helping him guess the password more easily. However, Grand doubted whether such a vulnerability really existed, so he refused to hack it.

Michael contacted many other cryptography experts. They all said they couldn't get his money back. In June 2023, he contacted Grand again in the hope of convincing the hacker to help. This time, Grand agreed. He cooperated with a friend named Bruno in Germany, who also specializes in hacking digital wallets.

Grand and Bruno spent months reverse engineering the version of the RoboForm software Michael used in 2013. They discovered that the random password generator did indeed have a major flaw. This makes the random number generator 'not so random'.

RoboForm confused the random passwords with the date and time on the user's computer. In other words, it determines the computer's date and time, then generates predictable passwords. If you know the date and time as well as other parameters, you can guess any password that was created on that date and time.

Similarly, if Michael knows when he created his password and the parameters (number of characters in the password, including lowercase and uppercase letters, numbers and special characters), the number of password guesses will decrease. .

Hackers can then attack RoboForm's date and time checking function and make it go back in time. Ultimately, the software will come up with the same password it generated for Michael in 2013.

'Losing your password turns out to be a blessing'

But the problem is that Michael can't remember when he created the password.

According to the wallet log, Michael transferred Bitcoin for the first time on April 14, 2013. But he couldn't remember whether he created the password on the same day or at some other time. So, Grand and Bruno customized RoboForm to create 20-character passwords with upper and lower case letters, numbers and 8 special characters from March 1 to April 20, 2013.

But the software still cannot create the correct password. So Grand and Bruno extended the time frame from April 20 to June 1, 2013, using the same parameters. Still no miracle happened.

The two hackers repeatedly asked Michael if he was sure about the parameters he used.

'They really annoyed me, because who knows what I was doing 10 years ago,' he recalls. He found other passwords created with RoboForm in 2013 and two of them did not use special characters. So Grand and Bruno adjusted the script one more time.

In November 2023, they contacted Michael to make an appointment to meet in person. 'I thought, 'Oh my God, they're going to ask me again to install software," he said.

However, when they met, the two hackers revealed that they had finally found the correct password. It was created on May 15, 2013, at 4:10:40 pm GMT. 'In the end we got lucky because the parameters and time ranges were correct,' Grand wrote in an email to *Wired* .

Released by US-based company Siber Systems, RoboForm was one of the first password managers on the market and currently has more than 6 million users worldwide. Siber Systems confirmed to *Wired* that the above vulnerability has been fixed in version 7.9.14 dated June 10, 2015.

'I'm still not sure I can trust this password generator, without knowing how they've patched it in the latest versions. I'm not sure if RoboForm knows how dangerous this vulnerability is,' Grand said.

As for Michael, after completing the task, Grand and Bruno took 1% of the Bitcoins in his account and returned the password to the owner. At that time, Bitcoin was worth 38,000 USD/coin. Michael waited until it increased to $62,000 (500 times more than when he bought it) and sold some of it. He currently has 30 BTC, worth $3 million and is waiting for the price to rise to $100,000.

Michael exclaimed how lucky he was because he lost his password many years ago. Because if not, he will sell all his Bitcoin when it is worth 40,000 USD and miss the opportunity to earn a huge fortune like now. 'Losing my password turned out to be a blessing,' Michael told *Wired* .