Satoshi nakamoto’s email compromised

Bitcoin Founder Satoshi Nakamoti’s Account Compromised

When Theymos received an unlikely e-mail from the founder of Bitcoin, he knew immediately that something was wrong. After further investigation into the matter it was found that Satoshi’s e-mail address was hacked.

Recently Theymos, a Bitcoin expert, posted a thread on Bitcointalk soon after he received a message from an e-mail Id that belonged to Satoshi Nakamoti. The Id used to send the e-mail was [email protected] , which is Satoshi’s old e-mail.

The message was what raised more suspicion. The sender wrote, “ Michael, send me some coins before I hitman you.”

Theymos was certain that Satoshi Nakamoto did not send such a strange e-mail and so assumed that Satoshi Nakamoto’s accounts had been compromised.

This e-mail ID was used by Satoshi to register on the P2P Foundation. After P2P foundation created a post about this on their website, credibility was added to Theymos’ statement.

It was found that Satoshi used the P2P account during his first few years of Bitcoin.

The account was used once this year by the owner to state something. He wrote, “ I am not Dorian Nakamoto” when some journalists by Newsweek supposedly linked his identity with a man named Dorian Satoshi Nakamoto.

Later, another post was made from the owner’s account. The post informed Satoshi sharply that his dox, passwords and IP addresses were being sold on the darknet.

The sender mentioned matter-of-factly that Satoshi’s IP leaked when he used his email account back in 2010.

The message also threatened Satoshi and told him that he was not safe. He was asked to run and hide before anyone could harm him.

Whether the accounts were compromised recently or before the Dorian Nakamoto scandal is not known.

The hackers have also managed to enter the Project Bitcoin on SourceForge. This was an old page that was restored after a brief period when Bitcoin developers requested SourceForge to do it.

The hackers replaced all the words “ Bitcoin” with “ Buttcoin.” This suggests that an individual or a group related to Buttcoin are responsible for the account’s hacking. Buttcoin is a small group of trolls who hate Bitcoin.

They could not however access Bitcoin’s coding repository called GitHub. This is because when it was thought long ago that Santoshi’s account might be hacked, he was removed.

What motives these hackers have is not known yet. They had scopes to enhance their financial status by pretending to be Satoshi.

But since they did not take advantage and easily declared that the account was hacked, it is perceived that their motive is something else.

Like Andreas Antonopoulos stated in his tweet, the messages can be thought as subtle warnings. They could also be an attempt to pressurize Satoshi into panic action. The matter could be simpler than people think it is though.

Some suggestions state that Satoshi’s GMX email account had expired which made it easy for someone else to claim it.

Peter Todd argued this suggestion by stating that he had forwarded emails from Satoshi’s account in 2011. This means that hacking seems like a more probable scenario.

GMX was asked to provide a detailed clarification for the happening, which might explain some of the issues when posted.

Previous Attacks

As the issue of Satoshi Nakamoto’s email being hacked alarmed the world, a much older story surfaced. There was a similarity that observers noticed between the recent hacking and the previous story where an attempt was made to hijack Bitcoin evangelist Roger Ver’s online accounts back in May.

After then hacking, no details could be found about Satoshi Nakamoto’s real identity. Bitcoin informed that even the ransom that Santoshi’s alleged hacker demanded online have stalled at only 1. 55 BTC instead of its 25 BTC target.

Once again, Satoshi’s identity is safe but now the attention has shifted from him to the perpetrator.

@LulzClerk is the Twitter account that the hacker provided in his interview with a blog. The account’s homepage has alternate online handles like ‘ Savaged’ and ‘ Nitrous’ listed, which seemed very familiar.

These were used by the person involved in the Roger Ver hacking/blackmailing incident too. It is very likely that the identities were intentionally placed by the hacker to mislead the investigation.

However Ver told in a statement that even though there is no sure proof, the same names and images are being used as this case. The hacker is claiming himself as the same person and his attitude supports the claim too.

Roger Ver also added that the 37. 6 BTC reward that he offered to the public to discourage the hacker during the time remained unclaimed. The bounty was unclaimed as the alleged criminal had still not been confidently identified.

Numerous posts on popular forums like Bitcoin Talk and Reddit had identified and doxxed individuals to be the hacker over the past few months but Ver could not find any real evidence to back the claims.

Ver is working with his associates to build an official website with appropriate details. He also announced the reward and included conditions of the reward.

Any informant will have to provide documentary evidence to claim the 37. 6 BTC reward. The evidence should be submitted to block chain certification site Proof of Existence, and also to the proper law enforcement agencies.

If the submission leads to an arrest and then to a conviction, the informant is expected to contact Ver through the website. Then, the timestamp given by Proof of Existence will be used to check if the information was responsible.

This process will help Ver avoid random claims from people who have no idea who the hacker really is. According to him, the system also allows the informant help anonymously if that is what he wants. He can provide Bitcoin address only to receive the reward.

After the conviction, if no informant identifies themselves, or if the law enforcement arrests the perpetrator without any informant's help, Ver promised that he will donate the 37. 6 BTC to charity.

Ver also added that if the website idea becomes popular, he would add more bounties for different cases.

The site could be used to solve many other notorious Bitcoin mysteries. Examples of such events include Satoshi Nakamoto's account hacking, Mt Gox and Bitcoinica.

He ended saying that he was sure the public will have lots more ideas.