High-profile Twitter accounts hacked to promote Bitcoin scam

welivesecurity.com/2020/07/16/high-profile-twitter-accounts-hacked-bitcoin-scam/

July 16, 2020

Tech titans and prominent politicians among victims of a sprawling hack that Twitter says leveraged its internal tools

Amer Owaida

16 Jul 2020 - 04:40PM

Tech titans and prominent politicians among victims of a sprawling hack that Twitter says leveraged its internal tools

Twitter is reeling from what is arguably the biggest security breach in its history after the accounts of a long list of high-profile figures – including Barack Obama, Joe Biden, Elon Musk, Bill Gates and Jeff Bezos – were hijacked and used to promote a Bitcoin scam.

The spate of attacks started late on Wednesday, with one of the first suspicious tweets then fired off from the account of the Tesla and SpaceX CEO. The now-deleted tweet followed a familiar pattern, bringing echoes of cryptocurrency scams that used Musk's name and promised to return double the amount of bitcoin sent:

"I'm feeling generous because of Covid-19. I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!" read the message that appeared on Musk's account.

RELATED READING: What to do if your Twitter account has been hacked
A flurry of similar tweets were also sent out from the other hijacked handles; apparently, some people fell for the ploy, since one of the cryptocurrency addresses has, as of the time of writing, received 12.86 BTC (some US$117,000).

> We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly.
>
> — Twitter Support (@TwitterSupport) July 15, 2020

The social media giant took a number of steps to swiftly remedy the situation. This included temporarily locking all compromised accounts, with Twitter stating that it would restore access only when it could do so securely. In short order, the company went on to take the unprecedented step of temporarily locking down *all* verified accounts, i.e. accounts marked by a blue tick.

> We also limited functionality for a much larger group of accounts, like all verified accounts (even those with no evidence of being compromised), while we continue to fully investigate this.
>
> — Twitter Support (@TwitterSupport) July 16, 2020

All the while, Twitter sought to keep everyone appraised by maintaining a steady stream of tweets informing about the developing situation. Eventually, the company started restoring functionality to the accounts, allowing them to tweet again.

So, how did it all happen?

Obviously the key question that screams for an answer is: “How was the massive hack executed?” According to the microblogging site, the incidents were caused by a social engineering attack on its employees:

> We detected what we believe to be a coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools.
>
> — Twitter Support (@TwitterSupport) July 16, 2020

Meanwhile, a Motherboard article seems to suggest that there may be more to the story, as several confidential sources from the black-hat community told the site that they had actually paid a Twitter insider to do the job.

In response, a Twitter spokesperson told Motherboard that the company was looking into whether the employee had possibly hijacked the account, or provided the cybercriminals with access to the tool.

RELATED READING: Insider threats: A persistent and widespread problem
ESET Security Specialist Jake Moore put the issue into a broader context: “Acting like a help desk, these employee accounts were enabled to use a specific admin tool and do whatever they wanted, which is likely to be a problem for many businesses. Some organizations lend an incredible amount of trust to certain employees. However, although they may be trusted not to compromise an account themselves, it must be taken into consideration that the employees will be targeted by criminal hackers.”

He also had some advice to share urging Twitter users to watch out for online scams: “When a message seems too good to be true it probably is, regardless of who has posted it. Bitcoin doubling schemes are synonymous with the criminal fraternity and must be avoided and reported where possible.”

16 Jul 2020 - 04:40PM

Newsletter

Discussion