CRYPTO SECURITY REPORT

MAY 2019

BitIRA

Crypto Criminals Shift Targets and Methods

When one method of cybercrime declines, another form sometimes takes its place. The good news is that cryptojacking of consumers' computers and devices is "essentially extinct", according to a recent report by the cybersecurity firm, MalwareBytes. The bad news it that the target has shifted to businesses, which have seen a rise of 235% in malware detections since last year. Another form of cybercrime on the rise is crypto ransomware, the average payout of which has risen by 89% since January, based on new research.

In the past 15 months, hackers have managed to steal more than $50 million from consumers' digital wallets using a new technique called SIM-swapping (a type of identity theft). Crypto marketplaces are being targeted as well, especially by arbitrage bots that manipulate decentralized exchanges for profit (a controversial topic since a WSJ article last year claimed that 95% of the volume on such platforms was fake).

On a positive note, a long-standing talking point by crypto skeptics – that crypto is used extensively for funding terrorism – may soon be laid to rest. The RAND Corporation, a think tank, published a report in March that found that cryptocurrencies are not currently a viable form of financing for terrorists. On the level of governments, though, North Korea continues to extensively make use of cryptocurrency for skirting economic sanctions, including directly financing its nuclear program.

Fighting Back Against Cybercrime

One way to combat crypto hacking is by evolving the software code of existing cryptocurrencies. The newest release of Bitcoin Core, the 18th such version, features significant security updates. The major change is to enable a connection between Bitcoin full nodes and hardware wallets, bridging a gap that will allow users to have more control over their digital assets.

On the prosecution side, New York has made its first conviction of money launders that were using cryptocurrency. Such outcomes suggest that even a decentralized financial system, like Bitcoin, can be regulated to prevent crime.

Greater efforts are being made to raise consciousness among organizations about how to mitigate against cybercrime. A new report by Moody's Investor Service has warned corporations about some hidden security risks of using private blockchains, which are becoming more popular and prevalent. A study by the World Economic Forum (WEF) has also detailed that most security breaches do not happen because of the skill of the hackers but rather because no (or inadequate) preventative measures were taken that could have staved off a cyberattack.

Consumers also have more resources available to educate themselves about crypto security. The SEC has recently published a warning detailing the six "red flags" of a crypto scam for which investors should be watchful. Bitcoinist has also outlined the five main types of crypto phishing scams that commonly target consumers. When it comes to avoiding crypto security breaches, knowledge definitely is power.