CRYPTO SECURITY REPORT

JULY 2019

BitIRA

Malware Across Platforms and Devices

“Pernicious and malicious cryptomining drops are continually evolving new ways to exploit their victims”, notes a CoinDesk article that describes the recent detection of a new type of mining malware. This malware specifically targets Android devices by hacking the common process of SSH connections between mobile products.

Another unusual new security threat was reported in late June. Called “LoudMiner”, the malware makes use of virtualization software on Windows and macOS for cryptocurrency mining by running a Tiny Core Linux virtual machine. This methodology allows the malware to target computers running different operating systems, all to mine monero (XMR).

Trend Micro also reported that month that the Oracle WebLogic server had a vulnerability that was being exploited by cryptojacking malware. The report described “an interesting twist” in the technology of the malware – “the malware hides its malicious codes in certificate files as an obfuscation tactic”. A new version of WebLogic Server has been released to patch up the cryptojacking vulnerability.

Security Measures, Public and Private

The fight against crypto crime happens on multiple fronts, sometimes using controversial measures. The Financial Action Task Force (FATF), an influential intergovernmental organization, issued guidance on regulating cryptocurrencies that included a requirement for crypto exchanges to exchange information about their customers when transferring funds between firms. Intended to fight back against money laundering, cryptocurrency advocates argue that such a rule would be impractical to enforce and have an overall negative impact on the market.

The publication of Facebook's white paper about its cryptocurrency, Libra, made waves across the highest levels of government, finance and industry. Even Jerome Powell, the head of the U.S. Federal Reserve, commented that he believed a Facebook coin would not significantly undermine the current monetary system. He did foresee "quite high expectations from a safety and soundness regulatory standpoint" for Libra, signaling that such a high-profile cryptocurrency would be watched hawkishly by government regulators.

Private industry is also investing in cryptocurrency security. Fidelity's proprietary investment arm, Eight Roads, contributed to a $16 million investment in Fireblocks, a platform for securing digital assets in transit. The founders of Fireblocks seek to eliminate the fundamental causes of digital asset loss – theft of private keys, spoofing, and others. Utilizing chip-level security and MPC technology, Fireblocks allows for safe transition of digital currencies from multiple states of storage to be transferred on the blockchain using multiple layers of security.

Keeping Your Crypto Safe

While great strides are being made in the field of cryptocurrency security, investors still need to be vigilant with their digital assets. Even in 2019, CoinDesk has reported that there have been seven crypto exchanges that have experienced large-scale hacking attacks in the first half of the year.

The benefits of blockchain, such as anonymity and a decentralized monetary system, also create security challenges, as an MIT professor recently described. If an investor's private keys are lost or compromised, for instance, there is no central authority that can restore the funds.

Cryptocurrency custodianship, a growing industry, can help mitigate against security breaches by offering safe crypto storage solutions. But even then, investors need to stay abreast of the latest crypto security developments and know the best ways to keep their coins safe, as Bitcoinist described in a recent article.

For more detailed information, see the BitIRA Cryptocurrency Security Guide.