FINE PRINT

Protecting Cryptocurrency Assets

by Joshua Gold and Stephen D. Palley

With cryptocurrency assets now topping $1.5 trillion globally, there is escalating potential for theft of assets held in bitcoin and other forms of digital currency. The recent surge in bitcoin prices and large institutions' heightened interest in dealing in these new currencies have raised the stakes. As more businesses consider investing in cryptocurrency and incorporating cryptocurrency transactions into their operations, they will need to take security and insurance coverage issues into account.

FBI, CISA AND TREASURY DEPARTMENT ISSUE WARNING

In a joint advisory issued on February 17, 2021, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Treasury highlighted the threat to cryptocurrency posed by the AppleJeus code exploit, which has been attributed to North Korean threat actors. According to the advisory, these actors "are targeting cryptocurrency exchanges and accounts to steal and launder hundreds of millions of dollars in cryptocurrency." There are variations on the scam, but a common tactic uses a copy of a legitimate-sounding cryptocurrency trading platform or virtual wallet to steal credentials and other vital information from victims in the United States and elsewhere.

During the past year alone, organizations in over 30 countries have reportedly been targeted in these cryptocurrency thefts. According to the advisory, "It is likely that these actors view modified cryptocurrency trading applications as a means to circumvent international sanctions on North Korea—the applications enable them to gain entry into companies that conduct cryptocurrency transactions and steal cryptocurrency from victim accounts."

The attacks have frequently targeted enterprises in sectors like finance and energy. A previous CISA alert warned that "North Korea's widespread international bank robbery scheme" exploits critical systems and presents risks to financial institutions around the world.

One malware trap involving cryptocurrencies is a program known as Union Crypto. According to CISA's analysis, the program loads a legitimate-looking cryptocurrency trading application, which engages in "the simultaneous buying and selling of securities, currency or commodities in different markets or in derivative forms to take advantage of differing prices for the same asset." The application exhibits no signs of malicious activity, but when launched, it collects and exfiltrates the victim's information.

MITIGATION TECHNIQUES

According to the advisory, companies the exploit impacts should immediately contact law enforcement, and take a number of technical risk mitigation steps. These include generating new keys for cryptocurrency wallets, and/or moving funds to new wallets; using hardware wallets to keep the private keys in a separate, secured storage area; introducing two-factor authentication as an extra layer of verification; removing impacted hosts from the network and changing all passwords to any accounts associated with impacted hosts; and updating and installing patches for all software and hardware, including any antivirus software, host-based intrusion

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

May 2021

detection software and firewall firmware. Companies should also assume the threat actors have moved laterally within the network and downloaded additional malware, and should scan systems thoroughly as a result.

CISA also recommended the following proactive mitigation steps to defend against AppleJeus malware and related activity:

- Verify the source of cryptocurrency-related applications.
- Use multiple wallets for key storage,
- striking the appropriate risk balance between hot (online) and cold
- (offline) storage.
- Use custodial accounts with multi-factor authentication mechanisms to verify both users and devices.
- Patronize cryptocurrency service businesses that offer indemnity protections for lost or stolen cryptocurrency.
- Consider having a dedicated device for cryptocurrency management.
- Train users to identify common social engineering, phishing and spearphishing techniques and report any suspicious activity.
- Insurance Considerations
- Insurance markets have begun to roll out dedicated products specifically designed to cover cryptocurrencies. Substantial limits may be available for both assets in cold storage (under a specie policy) or assets in hot wallets.

Cold storage refers to cryptocurrency that is kept secure using offline storage not connected to the internet. This typically involves hardware devices, but could also include private keys written on paper and kept in a safe. Specie policies were originally created to cover material assets like precious metals, diamonds or currency kept in bank vaults. The coverage has been updated in recent years to provide similar protection for cryptocurrency assets in cold storage. Large cryptocurrency exchanges and custodians may secure this coverage on their own behalf for client assets. Cryptocurrency custody and trading platform BitGo, for example, has reported that it maintains $100 million in specie coverage.

Crime policies are typically used to cover assets in hot wallets, which are connected to the internet. Cryptocurrency exchange Coinbase reported in 2019 that it had secured $255 million in coverage for hot wallet assets, placed through Lloyd's syndicates.

Individual corporate policyholders that have custody of their own cryptocurrency may also have coverage under their dedicated cyber insurance and commercial crime coverage policies, and may have coverage under personal lines insurance policies as well. However, this is not an absolute certainty, and any company that has a position in cryptocurrency assets and intends to practice "self-custody" should carefully review their own policies. They need to determine if, given their risk appetite, using a third-party custodian with well-developed security protocols and coverage in place would be a safer approach, even though it may provide less control over the assets themselves.

While some insurance companies have taken the position that cryptocurrency is not "personal property" subject to coverage, this argument is contrary to established principles of insurance policy interpretation. Questions may also arise regarding valuation of a loss and the amount to be reimbursed—that is, whether the value should reflect the price of the currency at the time of the loss, the price at the time of acquisition, or the price at the time the claims payment is made. Here, the correct position may turn on facts, circumstances and policy language, but given the volatility in cryptocurrency markets, reaching the right answer is vitally important for any policyholder who has suffered a significant loss. R

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com