CRYPTO SECURITY REPORT

SEPTEMBER 2018

BitIRA

Political Hacking and Consumer Theft

In the past couple of months, there have been a few prominent politically-motivated security breaches involving cryptocurrency. A July 13 indictment of 12 Russian intelligence officials purported that, in a bid to alter the outcome of the 2016 U.S. presidential election, the military personnel used Bitcoin to fund their operation. Although the indictment notes that fiat currencies were used as well, it states that Bitcoin was the primary means of laundering $95,000 of funds across the globe.

Roughly a month later, security firm Kaspersky Lab reported that North Korean hacker organization Lazarus Group managed to infect an unnamed crypto exchange with malware, with the intention to obtain a large sum of money. The report, released on August 23, alleges that the scheme involved a multi-platform virus named “AppleJeus” that was unwittingly downloaded by an employee of the exchange. Lazarus has been linked to attacks on numerous South Korean crypto exchanges in the past, including Bithumb, YouBit, and Coinlink.

This breach of an exchange followed an earlier incident involving Bancor, a token creation platform that temporarily went offline on July 9 after its security team logged a theft of ETH and NPXS tokens worth $13.5 million. Despite the heavy loss, the team managed to block 2.5 million BNT tokens from being stolen during the attack, as well as secure funds in the users’ wallets.

Finally, in August, group of independent researchers claimed to have hacked John McAfee’s supposedly-unhackable crypto wallet, Bitfi. Starting on July 24, McAfee had offered a $100,000 bounty to anyone who could hack the innovative wallet. Although an unaffiliated hacker had been reported to have also cracked the device earlier in the month, Bitfi CEO Daniel Keshin maintained that the firm wasn’t convinced he had done so.

Research and Regulation

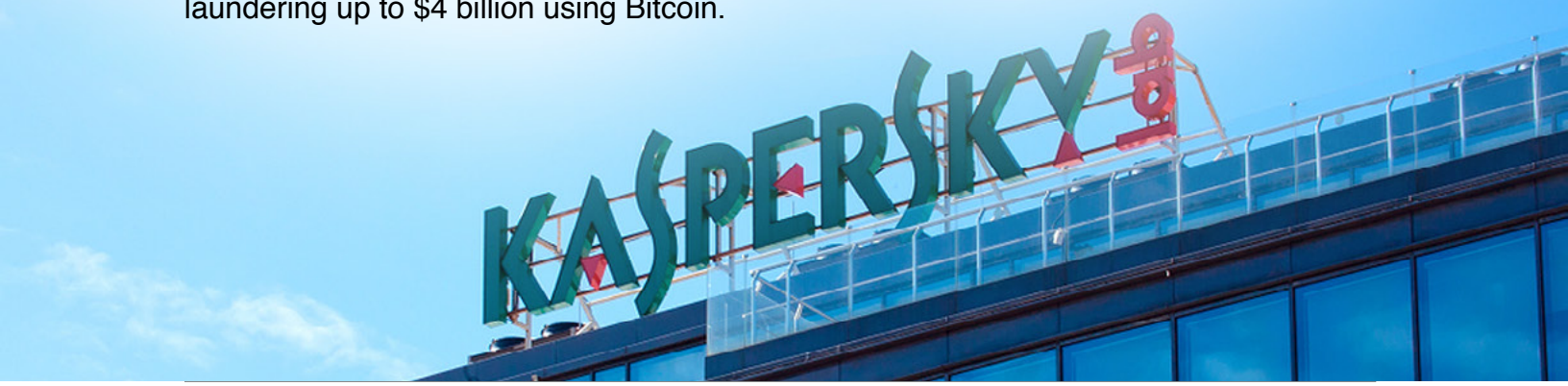
In a report titled “Spam and phishing in Q2 2018”, Kaspersky Lab revealed that their security software stopped 60,000 users from visiting fraudulent crypto websites between April and June 2018. Nonetheless, the quarter saw global cybercriminals make off with more than $2.3 million in ill-gotten cryptocurrency obtained from fake ICO sales and crypto exchange impersonation.

The bounty seems meager compared to the funds obtained by organized trading groups, which reportedly stole $825 million from the crypto market by means of price manipulation in the first six months of 2018. The Wall Street Journal’s study on this, released on August 5, listed 121 different coins that were the victims of 175 manipulation schemes by trading groups, many of which remain hidden.

To combat nefarious practices such as these, industry leaders have formed the Crypto Community Watch, which offers rewards to those who can help prevent a major scam from taking place. Groups such as ICO Alert, GZH, Step VC, ECoinmerce and NewEconomies have banded together to create a 100 BTC reward pool meant for providers of actionable tips regarding imminent frauds. The anonymous tipping form is available on the ECoinmerce website, together with a Bitcoin wallet form if the whistleblower’s testimony proves useful.

On a broader scale, the G20’s Financial Stability Board (FSB) released a framework to help monitor developments in the crypto market with the ultimate goal of subduing or eliminating scams in the space. The framework, published on July 16, will look at the size and growth of ICOs, widespread use of cryptocurrencies as payments, and price volatility compared to traditional assets to identify various risks in the market.

The efforts are taking place as Alexander Vinnik, the alleged former operator of the once-popular BTC-e exchange, awaits extradition to France after a Greek court found him guilty of fraud and money laundering on July 13. The Russian national, who is also wanted by the U.S., is accused to have defrauded over 100 French citizens between 2016 and 2018 through cryptocurrency platforms. In total, Vinnik is accused of laundering up to $4 billion using Bitcoin.



Security Threats in Perspective

Even though security breaches related to cryptocurrency happen every month, their institutional effect as a whole should be kept in perspective. In a testimony before the House Financial Services Committee on July 18, Federal Reserve Chairman Jerome Powell said that the crypto market, despite having grown to $295 billion in a short span of time, isn't large enough to be considered a threat. The central bank, Powell said, won't be looking to regulate the digital currency market.

The growth of the market has been accompanied by a seismic shift from illegitimate to legitimate uses (as a percentage of the whole), according to data from the U.S. Drug Enforcement Administration (DEA). Whereas the crypto market in 2013 attributed 90% of its transactions to dark web purchases, nowadays only 10% of all cryptocurrency transactions involve illegal dealings.

Insurance organizations are also increasingly (though cautiously) entering the crypto sphere, as investors look to hedge their assets against persistent risks. Hugh Karp, CEO of Nexus Mutual, is planning to unveil a mutual insurance product that will act as a smart contract meant to prevent financial losses. Although Karp and his company are initially focusing on Ethereum, their goal is to move not only to other cryptocurrencies but also to use blockchain for other insurance applications.

Further, a startup named Stronghold revealed its own take on crypto insurance on July 17 with the USD Anchor, a stablecoin backed by the U.S. dollar and insured by the Federal Deposit Insurance Corp (FDIC). Stronghold has partnered with IBM for this venture, and the pair seeks to offer a steady and secure digital currency that would attract investors who have previously been skittish about crypto's prospects.