WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

CYBER INTELLIGENCE REPORT

Actor Type: Tier IV
Serial: IR-001-2018
Country: KP
Report Date: 1 Jan 2018

North Korea's Illegal Campaign to Acquire Bitcoin

EXECUTIVE SUMMARY

North Korea has been identified as conducting multiple thefts of Bitcoin cryptocurrency in 2017. In conjunction with its identification as the actor behind the Wannacry ransomware, itself an attempt to acquire Bitcoin, plus limited evidence of bitcoin mining, these actions indicate a major North Korean campaign is underway to acquire Bitcoin as a way to raise hard currency.

North Korea was likely motivated to acquire Bitcoin, by any means, because of the currency's rapidly increasing value in 2017, the possibility of hiding the thefts by converting Bitcoin into more obscure forms of cryptocurrency, and the convertibility of Bitcoin and these other cryptocurrencies to hard currency. While it is unusual for a nation-state to be involved in this type of theft, it is not much different from other North Korean criminal enterprises which have included cyber bank robbery, illegal weapons sales, and counterfeiting U.S. currency.

The White House recently announced that North Korea was behind the Wannacry ransomware campaign, although it appears to have raised little money. More successful operations to acquire Bitcoin have included:

- **Cyber attacks from February to August 2017 on several South Korean Bitcoin exchanges.** These started with spear phishing attacks designed to gain control over the systems of exchange employees and evolved into access to exchange Bitcoin wallets. These attacks have resulted in the loss of about $80 million.

- **An October 2017 spear phishing campaign in the English-language environment.** This operation sent out emails with a fake job announcement for a position in a London cryptocurrency firm. The emails contained an infected attachment that could gain control over the target system. No successful thefts in this campaign have yet been reported.

- **A December 2017 attack on Youbit, a South Korean exchange.** This theft resulted in the loss of 17% of their assets, knocking them offline, and forcing them to file for bankruptcy.

2017: NORTH KOREA AND BITCOIN

Two of the most prominent story threads in the news in 2017 have been the sudden rise of North Korea as a nuclear threat and the equally dramatic rise of Bitcoin as an investment medium. Two events in December 2017 have highlighted the intersection of these two threads into a third issue: North Korean acquisition of Bitcoin, largely through illegal means.

On 19 Dec 2017, White House homeland security adviser Tom Bossert issued a statement attributing the Wannacry ransomware attack to North Korea. The Wannacry ransomware attack took place in May 2017. The ransom demanded payment in Bitcoin. Bossert described how Wannacry had "rendered useless hundreds of thousands of computers in hospitals, schools, businesses, and homes in over 150 countries." He was unequivocal in his attribution, stating that "after careful investigation, the United States is publicly attributing the massive Wannacry cyber-attack to North Korea. We do not make this allegation lightly. We do so with evidence, and we do so with partners."[1]

The Wannacry perpetrators did not cash out until August 2017. At that time, the wallets containing ransom payments started emptying, indicating the currency was being moved in order to convert it to hard currency. In all, these wallets had contained a total of about $140,00 in Bitcoin, based on the exchange rate at the time the Bitcoin was moved. One report indicated that only 338 victims paid the $300 Bitcoin ransom out of the 300,000 systems attacked worldwide.[2] While Wannacry caused huge disruption across many countries, the bottom line suggested by this cash-out amount indicates that it was not a major resource gain for North Korea.

Also on 19 Dec 2017, it was revealed that the South Korean Bitcoin exchange had again been hit by another cyber-attack. A theft of Bitcoin from Youbit in April had reportedly resulted in a loss of about $72 million (at Bitcoin's peak value for 2017).[3] In December Youbit was hit again. This time, it had 17% of its total assets stolen and declared that it was entering bankruptcy proceedings.[4]

One researcher who had worked on analysis of the April attack stated that the company had been hit by a series of attacks that used malware previously

[1] www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917.
[2] www.zdnet.com/article/wannacry-ransomware-hackers-behind-global-cyberattack-finally-cash-out-bitcoin-windfall.
[3] www.newsweek.com/north-korea-hacking-war-bitcoin-exchanges-part-biggest-global-sting-752161.
[4] www.bloomberg.com/news/articles/2017-12-21/north-korea-said-to-be-suspect-in-hack-of-seoul-bitcoin-exchange.

associated with North Korea.[5] South Korean police and the Korea Internet and Security Agency were reportedly viewing the case as an extension of the April attack on Youbit. The Wall Street Journal also reported that there was evidence that the Youbit attack was conducted by North Korea.[6]

NORTH KOREAN INTEREST IN BITCOIN

North Korea apparently became interested in Bitcoin and its potential several years ago. Secureworks has reported that it noticed that a handful of North Korean IP addresses were involved in research on Bitcoin starting in 2013, apparently trying to figure out its functionality and how it can be converted to cash.[7] They appear to have become convinced that Bitcoin would help them with their severe shortage of hard currency.

This interest has translated in a limited way into North Korean use of legitimate methods to acquire Bitcoin as well as theft. Recorded Future reported that once the Wannacry campaign was over on 17 May, a spike in Bitcoin activity in North Korea indicated that mining activity had started on that date. Recorded Future's interpretation of this shift was that, "They may have realized by the 17th that they weren't going to get a quick return on the WannaCry attacks," and so had shifted to mining as a way to acquire Bitcoin.[8]

Once one assumes that North Korea has no qualms about being a nation-state-level thief, the interest in Bitcoin makes sense. The anonymity of transfers within the Bitcoin system means that North Korea would not be bound by banking regulations. In theory, the trail of cryptocurrency transfers can be obscured by coin tumbler services, breaking a transfer down into small-scale transactions spread across multiple routes or converting to less-well-known cryptocurrencies. These other currencies can then be cashed out for hard currency. In addition, the dramatic and ongoing rise in the value of Bitcoin in 2017 may have been the trigger for North Korea's engagement. Like many others, they likely view it as a way to get rich quick.

Targeting Bitcoin has not been the only illicit way that North Korea has tried to raise funds. It has long been involved with counterfeiting U.S. currency. It continues to be involved with weapons sales in violation of UN sanctions. In a more direct approach, as reported by the Wall Street Journal in March 2017, North Korean hackers stole US $81 million from the Bangladesh Bank in 2016 through the use of the Swift messaging network.[9]

ATTACKS ON SOUTH KOREA IN 2017

---

[5] www.reuters.com/article/us-southkorea-cyber-hackers/multi-stage-cyber-attacks-net-north-korea-millions-in-virtual-currencies-researchers-idUSKBN1ED0ZC

[6] www.bloomberg.com/news/articles/2017-12-21/north-korea-said-to-be-suspect-in-hack-of-seoul-bitcoin-exchange.

[7] www.bloomberg.com/news/articles/2017-12-14/north-korea-s-bitcoin-play.

[8] www.bloomberg.com/news/articles/2017-12-14/north-korea-s-bitcoin-play.

[9] www.scmp.com/news/china/diplomacy-defence/article/2111427/wheres-money-coming-north-koreas-nuclear-programme.

North Korea carried out a series of attacks against South Korean targets as part of its search for Bitcoin. This included attacks on Bitcoin exchanges in South Korea that resulted in the theft of about $7 million in Bitcoin when stolen, but by December this would be worth over $80 million.

Bithumb, South Korea's largest cryptocurrency exchange, was attacked in February 2017, resulting in the loss of $7 million in Bitcoin and Ethereum. Media reporting indicated that North Korea was behind the theft. The exchange was fined by the South Korean government for failure to protect its users.[10] The hackers also made away with personal information of 30,000 exchange customers, and demanded $5 million from Bithumb to erase the personal data.[11]

Attacks started against Youbit's predecessor company, Yapizon, in April.[12] A researcher at the Korean Internet and Security Agency stated that attacks on at least three Bitcoin companies during the summer of 2017 used malicious code that was identical to that previously associated with North Korea. These attacks consisted first of stealing employee personal information which was then used for spear phishing emails. These were designed to look like official messages from the Korean National Tax Service announcing an investigation into the target's taxes. The attachment with these emails contained malicious code that allowed the hackers to gain control of the target's computer. From there, the hackers were able to access the target's Bitcoin wallet or the exchange's servers themselves.[13]

FireEye identified the malware used as PEACHPIT and similar variants.[14] The U.S. Department of Homeland Security issued a warning in November 2017 that the Volgmer Trojan and the Fallchill remote access tool were also being used by North Korea.[15]

PERSONAL APPROACHES

In reports based on information from South Korea's intelligence service, North Korea has also been attempting to access digital exchange employees in South Korea through Facebook. The North Koreans reportedly pose as attractive women seeking a personal relationship with their targets. According to one South Korean cybersecurity analyst, these persons profess to be studying abroad or working at overseas think tanks. "They open Facebook accounts and maintain the online friendship for months before back-stabbing the targets

[10] www.digitaltrends.com/computing/bithumb-cryptocurrency-exchange-bitcoin-stolen.
[11] www.bbc.com/news/world-asia-42378638.
[12] arstechnica.com/tech-policy/2017/12/north-korea-suspected-in-latest-bitcoin-heist-bankrupting-youbit-exchange.
[13] www.reuters.com/article/us-southkorea-cyber-hackers/multi-stage-cyber-attacks-net-north-korea-millions-in-virtual-currencies-researchers-idUSKBN1ED0ZC.
[14] arstechnica.com/tech-policy/2017/12/north-korea-suspected-in-latest-bitcoin-heist-bankrupting-youbit-exchaange.
[15] www.scmp.com/news/asia/east-asia/article/2120056/us-says-north-korean-malware-lurking-computer-networks-allowing.

in the end," using their access to send files with embedded malware to the targets.[16]

NORTH KOREAN ATTACKS ELSEWHERE

South Korean exchanges have not been the only targets in 2017. In mid-December, Secureworks reported that North Korea was conducting a spear phishing campaign in the English-language environment, targeted on cryptocurrency executives. The lure was a fake job opening for chief financial officer at a London cryptocurrency company. The email campaign reportedly started on 25 Oct 2017, although Secureworks reported that some related activity starting in 2016. The probable intent was for the email to circulate among executives in other cryptocurrency companies. The Reuters report on the campaign stated that "those who clicked on the hiring link were infected by malicious code from an attached document in the email that installed software to take remote control of a victim's device." Secureworks reported that the campaign was ongoing.[17]

CRYPTOCURRENCY THEFT BY OTHERS

The North Korean government is not the only actor targeting Bitcoin. There have been many thefts of cryptocurrencies over the past two years that have not been linked to North Korea. In December 2017 NiceHash, a Slovenia-based cryptocurrency company, reported that its digital wallet had been pilfered. NiceHash is primarily a mining service, and miners sometimes leave their gains in the NiceHash wallet. The value of the loss was not revealed by NiceHash, but others estimated it at over $60 million.[18]

In addition to the NiceHash theft, there have been several other major cryptocurrency hacks, including the following:

- In June 2016 the Distributed Autonomous Organization, an Ethereum investment entity, lost about $60 million of its currency to hackers. A codebase change subsequently allowed restoration of the funds.
- In August 2016 the cryptocurrency exchange Bitfinex lost 120,000 Bitcoin to hackers, then worth $72 million. The exchange was able to return the funds to users by April 2017.
- In July 2017 CoinDash's website was hacked during its initial coin offering, and about $7 million in Ethereum was rerouted to the hackers.
- In November 2017 Tether, which markets cryptocurrencies tied to dollar value, lost $31 million in its currency to hackers. It disseminated a

[16] www.scmp.com/news/asia/east-asia/article/2125055/beautiful-woman-who-wants-be-your-new-facebook-friend-may-really.
[17] securityaffairs.co/wordpress/66780/apt/lazarus-apt-cryptocurrency.html.
[18] www.scmp.com/tech/article/2123253/thieves-stole-potentially-millions-dollars-bitcoin-hacking-attack.

software update in an attempt to keep the lost currency from being further distributed.[19]

In a different sign of turbulence in the cryptocurrency world, media reports indicate that Pavel Lerner, the CEO of the UK-based Bitcoin exchange EXMO, was kidnapped in Ukraine on 26 Dec 2017. He was reportedly bundled into a black Mercedes by men in balaclavas as he left his office in Kiev. On 28 December, EXMO's website was also hit by a distributed-denial-of-service attack that suspended trading.[20]

CONCLUSIONS

North Korea was likely motivated to acquire Bitcoin, by any means, because of its rapidly increasing value, the possibility of hiding the money trail after the theft, and its convertibility to hard currency. Cryptocurrency theft may seem like a desperate measure for a nation-state, but it is in line with other illegal activities conducted by the North Koreans.

Despite North Korea being named as the Wannacry perpetrator and the theft from Bitcoin exchanges, there are other signs that the North Korean interest in Bitcoin will continue. In November 2017, the elite Pyongyang University of Science and Technology reportedly hosted a foreign lecturer to teach its students about Bitcoin technology. The university reported that the discussion covered "the inner working of Bitcoin, its risks, and the measures taken to ensure security."[21] It is doubtful that North Korea can be embarrassed into stopping its assault on Bitcoin entities, and they appear to be testing the target base beyond South Korea.

Prepared: Silkworm
Reviewed: J. Petrequin, B. Schenkelberg
Approved: J. Stutzman
Info. Cut-Off: 29 Dec 2017

For questions or comments regarding this report, please contact the lab directly by at 603-606-1246, or feedback@wapacklabs.com.

[19] www.fastcompany.com/40505199/bitcoin-heist-adds-77-million-to-hacked-hauls-of-15-billion.
[20] www.telegraph.co.uk/technology/2017/12/28/bitcoin-exchange-chief-executive-kidnapped-leaves-work.
[21] money.cnn.com/2017/12/12/technology/north-korea-bitcoin-hoard/index.html.