

DOW JONES, A NEWS CORP COMPANY

Nikkei ▼ **22883.23** -0.04%Hang Seng ▲ **29375.06** 0.48%U.S. 10 Yr ▲ **5/32** Yield 2.483%Crude Oil ▼ **58.02** -0.12%Yen ▲ **113.40** 0.01%

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<https://www.wsj.com/articles/north-korea-is-suspected-in-bitcoin-robbery-1513790899>

ASIA

# North Korea Is Suspected in Bitcoin Heist

Pyongyang's hackers turn to cryptocurrency and banks as Kim regime hunts for funds



The Youbit digital-currency exchange in Seoul collapsed on Tuesday after an attack by hackers. PHOTO: YONHAP NEWS/NEWSCOM/ZUMA PRESS

By Timothy W. Martin, Eun-Young Jeong and Steven Russolillo

Updated Dec. 20, 2017 6:59 p.m. ET

SEOUL—Investigators in South Korea are looking into North Korea's possible involvement in a heist from a bitcoin exchange that collapsed here on Tuesday, according to people familiar with the situation, as the sanctions-choked regime develops new ways to raise money.

The investigation into the hack of Seoul-based exchange Youbit, led by South Korean law enforcement and a state cybersecurity agency, is still in its infancy and a review of the malware code could take weeks, the people said.

But the people said there were telltale signs and historical evidence that North Korea was behind the Youbit attack. North Korean hackers in April targeted the same cryptocurrency exchange, operating under a different name, several of the people said. Yopian, the company that operates Youbit, suspended trading and filed for bankruptcy after Tuesday's hack.

The bitcoin heist follows similar suspected Pyongyang-directed offensives against other South Korean cryptocurrency exchanges—and an increasing number of attempts to steal from individual investors.



A North Korean missile launch, shown in an undated photo released in September by the country's Korean Central News Agency. As sanctions squeeze North Korea, the regime has developed new ways to raise money for its weapons programs. PHOTO: KCNA/REUTERS

On Tuesday, the White House said North Korea directed this year's WannaCry ransomware attack, which locked digital files and demanded bitcoin payment for their release.

South Korean police and the Korea Internet & Security Agency said they had begun an investigation into the Yobit hack but were still determining the scope of the situation.

A North Korean cyber army of 7,000 hackers around the world has shifted tactics over the past two years to become more motivated by financial gain, pilfering from banks and, more recently, focusing on cryptocurrencies, according to cybersecurity researchers. North Korea has denied involvement in the hacking incidents.

North Korean leader Kim Jong Un has a critical need for funds as his regime advances its nuclear-weapons program in the face of tightened economic sanctions.

"North Korea is an ideal country to use hacking and financial tools like bitcoin," said Troy Stangarone, a senior director at the Korea Economic Institute in Washington. "They're experimenting with ways to earn back lost money from sanctions."

The bitcoin craze has created a unique opportunity, as a rush of new investors bet on a market they had barely heard of until recently, said Ryan Kalember, a senior vice president at Proofpoint Inc., a cybersecurity firm that published a recent report detailing Pyongyang's bitcoin campaigns.

"Much of the cryptocurrency system is highly vulnerable," Mr. Kalember said. "Because this world is moving so fast and now it's so lucrative, it's really exactly what a cybercriminal" is looking for.

---

#### RELATED READING

---

- What North Korea Might Do With Bitcoin
- Cryptocurrency Exchange Collapses, Files for Bankruptcy After Second Hack
- Hackers Just Stole \$66,000 in Bitcoin. Now What?
- Good News! You Are a Bitcoin Millionaire. Bad News! You Forgot Your Password
- Hackers' Latest Weapon: Cyber Extortion
- Digital Clue Links North Korea to Theft at New York Fed, Security Firm Says

The bitcoin itself is supposed to be secure and safeguarded by a unique encryption code. But cyberthieves have breached cryptocurrency exchanges or so-called digital wallets, stealing encrypted passwords as well as bitcoins.

For North Korea, stealing bitcoin could be an attractive endeavor because of the cryptocurrency's ability to rise sharply in value over a relatively short period. The price of one bitcoin started this year at just under \$1,000 and has experienced a frenetic rally, with choppy price swings, to as high as nearly \$20,000 this past weekend.

The moves in bitcoin and other digital currencies starkly contrast most traditional financial markets in 2017, like stocks and bonds, where volatility has been historically low.

For average consumers, online marketplaces can convert bitcoin into regular cash that can be sent to bank accounts. But North Korea is allegedly swiping vast sums of bitcoin—significantly more than individuals typically own— and must also cover its tracks.

To do that, North Korea, in theory, could divvy up the bitcoin bounty into different accounts, then move the smaller sums in and out of different cryptocurrency exchanges. Each transfer would further erode the links to the original owners. Eventually, North Korea could create enough anonymity to cash out the bitcoin like anyone else.

South Korea is among the most active bitcoin markets, ranking No. 3 after the U.S. and Japan in terms of national currency trade volume, according to data firm Coinhills, which tracks digital currencies. South Korea has no legal protections for consumers who become victims of exchange hackings, unlike with its banks and securities firms, said Ahn Chan-sik, an attorney at Seoul law firm HMP Law.

But lax security protocols haven't repelled investors, a concern even for virtual currencies' biggest advocates. "Investors need to be more alert," said Kim Hwa-joon, the co-head of a cryptocurrency exchange industry group. "Consumers need to be more sensitive about where they put their money."

Exchanges are aware that security breaches present serious risks. One of South Korea's top exchanges by trading volume, Coinone, is headed by a former hacker. Since 2017, the company has worked with hackers who conduct mock attacks to try to breach its system.

Pyongyang's cyberwarfare capabilities first drew global attention for the hack of Sony Pictures Entertainment in 2014, when the regime's cyber goals were more focused on obtaining military information, destabilizing networks or intimidating opponents.

North Korea has turned in recent years to increasingly sophisticated financial warfare.

North Korea was blamed for last year's cybertheft of \$81 million from Bangladesh's central bank, followed by a \$60 million theft this year from a Taiwanese bank. Cybersecurity researchers say North Korea was involved in other attacks in Mexico, Poland, India and the U.K.

The hackers have executed scams such as planting viruses into South Korean ATMs or point-of-sale devices to steal personal information, according to researchers. South Korean government groups and agencies withstand 1.5 million daily North Korean hacking attempts, law-enforcement and intelligence officials said.

Pyongyang's bitcoin interest has taken root more recently. North Korea targeted three cryptocurrency exchanges in South Korea between April and October, people familiar with that investigation said. That includes an April attack on a predecessor to Yobit, then known as Yapizon.

Steve Lim, chief strategy officer at the Coinone exchange, doesn't think the Yobit incident alone will dramatically curb bitcoin interest. "People will shrug it off in a few months' time, as long as there aren't any more of these kinds of incidents," he said.

Yapian said the security breach caused it to lose 17% of its total assets, but didn't specify the financial value of the losses. The value of the heist is difficult to determine as exchanges aren't required to provide information about their operations beyond registering their business when they first open.

On Dec. 1, Yobit purchased a one-year cyberinsurance policy from DB Insurance Co., a South Korean firm, with damage coverage up to about \$2.8 billion.

A spokesman at DB Insurance said Yobit hasn't filed a claim. Yobit has up to three years to do so.

**Write to** Timothy W. Martin at [timothy.martin@wsj.com](mailto:timothy.martin@wsj.com), Eun-Young Jeong at [Eun-Young.Jeong@wsj.com](mailto:Eun-Young.Jeong@wsj.com) and Steven Russolillo at [steven.russolillo@wsj.com](mailto:steven.russolillo@wsj.com)

Copyright ©2017 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.