EXAMINING NORTH KOREA’S PURSUIT OF CRYPTOCURRENCIES

Luke McNamara
Principal Analyst
FireEye
Overview

- Background on TEMP.Hermit Threat Activity
- Pivoting to Cyber Crime
- South Korea Cryptocurrency Exchange Targeting
- Further activity
- Impact
- Takeaways & Outlook
History of TEMP.Hermit

- Closely aligns with Lazarus Group
- Since 2013: targets of interest to the North Korean state
- Government victims in the United States, South Korea; energy sector
- TTPs: Spearphishing, SWCs, usage of wiper malware
- Separate from APT37 (Reaper)
Hermit pivots to cyber crime

- Since at least 2016 has also targeted financial organizations for monetary gain (MACKTRUCK, NESTEGG)
- Initially traditional finance targets, SWIFT fraud
- Late 2016: injects on financial regulatory orgs’ webpages
Office 39

- Public reporting on Office 39 details involvement in multiple avenues of illicit financial activity
  - Counterfeiting
  - Smuggling
  - Running hostels and restaurants abroad.
Early indications of cryptocurrency interest

- February 2017: strategic watering hole compromise of cryptocurrency news website
- WannaCry (May 2017)
- BTC ransoms exchanged for more anonymous cryptocurrency Monero
South Korean exchanges experienced some of the highest volume in Asia after China closed exchanges in 2017.

- Hundreds of billions of won traded daily
- One in five South Koreans invest in cryptocurrencies
- Until recently, little to no KYC
Cryptocurrency Exchanges: Prime Targets

- Centralized pools of liquidity, “hot wallets” an attractive target.
- Great for trading cryptocurrencies, not recommended for securely storing coins.
- Can’t reverse transactions on an immutable ledger
- Puts increased onus of security on the user
April 22\textsuperscript{nd} – Wallets on South Korean cryptocurrency exchange Yapizon are compromised

April 26 – The United States announces a strategy of increased economic sanctions against North Korea.

Early May – Spearphishing against South Korean Exchange #1 begins.

Late May – South Korean Exchange #2 (Bithumb) targeted and later compromised via spearphish.

Early June – More suspected North Korean activity believed to be targeting cryptocurrency service providers in South Korea.

Early July – South Korean Exchange #3 targeted via spear phishing to personal account.
Tactic, Techniques, and Procedures (TTPs)

- Spearphishing personal email accounts of employees
- Used lures related to tax information, job postings, and employee resumes
- PEACHPIT, MANUSCRYPNT, and other malware used
Cashing Out

- TEMP. Hermit actors likely had multiple avenues to cash out
  - Cash out for won on another SK exchange
  - OTC trades
  - Exchange for other currencies
Other reporting

- South Korean government confirms hacks of multiple exchanges
- Reports of mining and cryptojacking
- North Korean university sponsors blockchain course
- UK-based cryptocurrency firm reports being spearphished
Targeting identification

- TEMP.Hermit cryptocurrency lure used to spearphish electronics manufacturer in South Korea
- Coinspace spearphishing
  - Suggestive of opportunistic targeting
Assessing the Impact

- If this activity is to evade international sanctions, how successful has it been?
- North Korea's 2016 GDP in real terms stood at 32.0 trillion won ($28.50 billion)
- Timeline matters when it comes to cashing out
Assessing the Impact, cont.

- **Yapizon exchange** (aka Youbit, Yapian) (2017): 4000 bitcoins stolen according to KISA

- **Bithumb exchange** (2017): ~$7 million USD stolen at the time according to South Korean government officials.

- **WannaCry ransomware** (2017): ~52.2 bitcoins acquired, later converted to Monero
Takeaways

- Traditional financial sector targeting has continued
- Continued price decline in cryptocurrency market may reduce some of this activity
- Indications of some interest in cryptomining malware (Monero especially)
Takeaways, cont.

- TTPs that TEMP.Hermit adopts in targeting the cryptocurrency sector will give insight into how their capabilities and skills are evolving.
- Targeting personal email accounts highlights how an organization’s attack surface extends beyond its networks.
Outlook: What next?

- What will be the impact of thawing diplomatic relations on North Korean cyber operations?
  - Cyber espionage?
  - Destructive activity?
  - Cyber crime?
QUESTIONS?