KIVU THREAT INTELLIGENCE

Cyber Threat Intelligence Insights for Claims and Underwriting Professionals

Volume XIX-1 *February 1, 2019*

Purpose
To share cyber threat intelligence and aid in protecting digital assets globally

Sources
This publication incorporates publicly-available and Kivu internally-developed Cyber Threat Intelligence

Subscription/Questions
Click HERE to request being added to this product's distribution list

Contact Us

www.kivuconsulting.com

info@kivuconsulting.com

415.524.7320

New York | Denver
Washington DC | San Francisco
Amsterdam | Toronto

Kivu Myth Busters: Ryuk vs. North Korea

I. Executive Summary

Several media outlets misleadingly reported that the Ryuk ransomware variant may have been developed and operated by North Korean state-sponsored actors. Kivu conducted its own proprietary and confidential analysis of the malware variant and concludes with a high degree of confidence that the Ryuk (aka Hermes v2.1) ransomware variant was not developed by North Korean state-sponsored actors and that Ryuk usage by itself is not indicative of North Korea being behind a particular attack.

II. Background

Over the last few years, North Korea has continued to develop its Cyber Operations capabilities, and currently has an army of approximately 6,000 hackers, some of which were trained in Russia and China[1]. Unlike typical state-sponsored cyber operations programs that generally focus on intelligence gathering, influence and/or information operations and offensive capabilities, the North Korean regime also dedicates significant amount of resources toward operations for financial gain. According to research by The New York Times, North Korea's for-profit cyber operations may earn over US$1 billion a year for the regime, which would account for roughly 1/3rd of North Korea's annual exports[2].

While North Korea was able to pull off several successful cyber-heists, the primary goal of this report is to examine whether the Ryuk (aka Hermes v2.1) ransomware variant has been improperly attributed to this regime. Attribution to North Korea would have particular legal significance as knowingly paying a ransom to North Korea, a regime subject to US Office of Foreign Assets Control (OFAC) sanctions could subject an organization to severe fines (up to $20m) and its directors to prison sentences. In the insurance world, a positive attribution that North Korea was behind a specific attack could effectively prohibit an insurer from reimbursing an insured under an otherwise valid cyber insurance policy. To provide more insights into our analysis process, and to share a high-level overview of the facts that lead us to our conclusions on attribution, we've built a timeline of the events related to the development of Ryuk and known ransomware-related operations by North Korean state actors:

[1] North Korean Cyber Capabilities, In Brief https://fas.org/sgp/crs/row/R44912.pdf

[2] The World Once Laughed at North Korean Cyberpower. No More. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

a. February 2017: The Birth of the Hermes Ransomware

The first versions of Hermes ransomware, the predecessor of Ryuk, were distributed via a Russian-language hackers' forum exploit[.]in starting early February 2017.

Hermes kits was offered on the Dark Web for $300 to $400. Each kit included Hermes binaries pre-configured with 2 email addresses, used to populate ransom notes on victims' servers and/or workstations, a set of step-by-step instructions on how to execute the ransomware, and a decryption tool that would be provided to victims once they paid the ransom. The kit didn't include any exploitation tools, meaning buyers still had to either hack victims themselves or purchase credentials for compromised systems on underground markets. Significantly, Hermes advertisements mentioned that the ransomware would not work on computers in Russia, Ukraine, or Belorussia, which suggested the development team may have resided in those regions.

According to VirusTotal, the first instances for Hermes code were submitted from Russian IP addresses. It's a common practice for malware developers to check their new tools in services like VirusTotal, DynChecker or HybridAnalysis to ensure that they are not being detected by antiviruses as malicious.

On February 16, 2017, Hermes ransomware was identified by GData security researcher Karsten Hahn. On the same day Emsisoft CTO Fabian Wosar was able to reverse engineer the ransomware and build a decryption tool for it[3]. Shortly after Wosar's decryption tool was published, a new version of the Hermes ransomware was released with an updated encryption mechanism.

Key Points: Based on the combination of geo-block restrictions within the ransomware and its distribution via a Russian-language hackers' forum, it is highly unlikely it was developed by actors associated with the North Korean Regime. Oh course, it could be a fiendish North Korean plot to plant a false flag, but we need to separate healthy skepticism from paranoia. So it helps to compare Ryuk with a malware variant which is generally accepted to have come from North Korea.

b. May 2017: Global WannaCry Ransomware Attack

The WannaCry ransomware variant spread rapidly across the global networks on May 12, 2017[4]. WannaCry exploited the Server Message Block (SMB) vulnerability (aka "EternalBlue") that was leaked to the public by the Shadow Brokers hacker group in April 2017[5]. The WannaCry code was not obfuscated and was fairly easy to analyze. No overlaps in code between the WannaCry and Hermes/Ryuk ransomware variants were found by IT Security researches.

Even though the WannaCry ransomware infected over 200,000 machines it wasn't much of a money-maker for the attackers. According to CNBC, as of May 15, 2017, WannaCry attackers only made $50,000 worth of bitcoins[6], presumably from victims who didn't realize that WannaCry did not allow for successful decryption.

On September 6, 2018 the U.S. Department of Justice charged a North Korean Regime-backed programmer responsible for the WannaCry ransomware attack, as well as other malicious activities[7].

---

[3] Hermes Ransomware Decrypted in Live Video by Emsisoft's Fabian Wosar
https://www.bleepingcomputer.com/news/security/hermes-ransomware-decrypted-in-live-video-by-emsisofts-fabian-wosar/

[4] What is WannaCry ransomware, how does it infect, and who was responsible?
https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[5] SMB Exploited: WannaCry Use of "EternalBlue"
https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

[6] Hackers who infected 200,000 machines have only made $50,000 worth of bitcoins, CNBC, May 15, 2017
https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html

[7] North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, US DOJ, September 6th, 2018
https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Key Point: WannaCry is the only ransomware operation that has been attributed to North Korean groups "Lazarus" and "Dark Seoul" with a high degree of confidence. Based on both malware and indicators of compromise (IOCs) analysis, there were no overlaps found between WannaCry and Hermes/Ryuk ransomware variants.

c. October, 2017: Far Eastern International Bank (FEIB) Heist

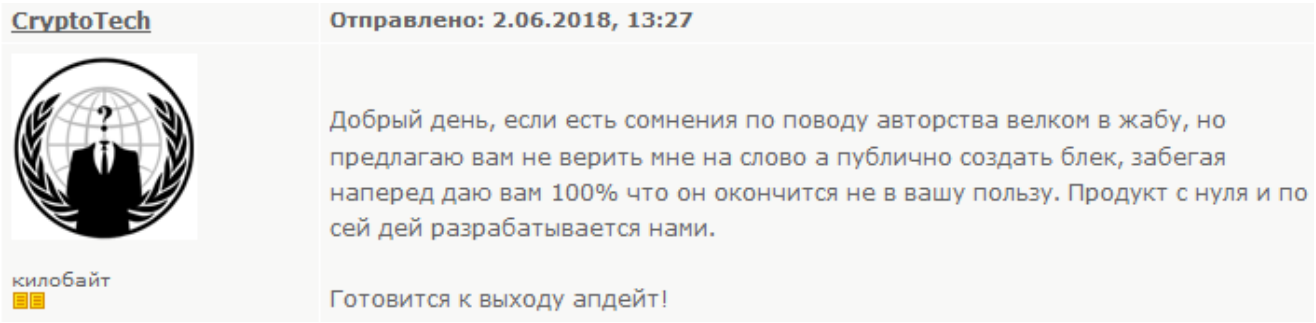
In early October 2017, Taiwanese Far Eastern International Bank (FEIB) officials discovered fraudulent attempts to wire US$60 million to foreign banks located in Sri Lanka, Cambodia and the United States[8] . Attackers believed to be members of the North Korean regime's Lazarus group used a Remote Access Trojan (RAT) malware to generate fraudulent SWIFT money moving messages[9]. In addition, the Lazarus group appears to have used a variant of the Hermes ransomware (by then freely available on the Dark Web) against the FEIB's network to create a diversion and distract the bank's security team during the heist[10].

The Hermes sample that was used in the FEIB heist was analyzed independently by several cyber security companies including Kivu, Group-IB, McAfee and CrowdStrike. All the researchers concluded that the variant of Hermes ransomware deployed by the Lazarus group was misconfigured and didn't contain the encryption keys that could enable the attackers to decrypt the files. That supports the theory that this ransomware was deployed purely to provide additional cover and buy more time for the fraudulent SWIFT transactions to stay undetected.

Key Point: Malware analysis of the Hermes "ransomware" sample used by North Korea's Lazarus group in the FEIB heist shows they had neither intent nor ability to decrypt files on the banks' systems. This misconfigured variant could have easily been purchased by the Lazarus group through underground hacker forums or downloaded and modified for free from sites like Virus Total or Hybrid Analysis.

d. June 2018: Hermes/Ryuk Authorship Questioned

In June 2018, one of Dark Web's exploit[.]in forum users expressed concerns that Hermes ransomware had not been developed by forum user "CryptoTech", who had been selling the ransomware. CryptoTech responded (in Russian) that Hermes was developed by his team from scratch and offered to provide proof via either private jabber communications, or public arbitration process. CryptoTech also shared that his team was getting ready to release a new version of Hermes. That version (i.e. Hermes v2.1) was released a month later, and it was dubbed Ryuk by IT security researchers.



Key Point: Willingness to go through exploit[.]in forum's arbitration process, along with a demonstration of inside knowledge on the upcoming release, further lends weight to CryptoTech team's sole involvement in the Hermes/Ryuk ransomware development and maintenance.

[8] North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist
https://www.bleepingcomputer.com/news/security/north-korean-hackers-used-hermes-ransomware-to-hide-recent-bank-heist/
[9] Malware-Wielding Hackers Hit Taiwanese Bank
https://www.bankinfosecurity.com/report-malware-wielding-hackers-hit-taiwanese-bank-a-10368
[10] Taiwan Heist: Lazarus Tools and Ransomware, October 16th, 2017, BAE Systems,
https://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html

e. August-2018: First infections by "Ryuk" ransomware spotted in the field

On August 13, 2018 the first instances of 2.1 Hermes ransomware (AKA "Ryuk" after its ransom note "RyukReadMe.txt".) infections were observed and reported by @MalwareHunterTeam[11]. Further analysis showed significant overlaps in code base with previous versions of Hermes.

Key Point: First victims of Ryuk/Hermes v2.1 were spotted at least 9 days prior to this version being advertised for sale on the exploit[.]in forum, indicating that the core development team also runs their own ransomware operations.

f. August-2018: Hermes v2.1 Released

On August 22, 2018 Hermes v2.1 was released on Exploit[.]in. According to CrowdStrike[12], at about the same time the Ryuk ransomware operators started to closely collaborate with the known Russia-based Trickbot operator Wizard Spider (note: prior to that Wizard Spider primarily focused on wire fraud). CrowdStrike's findings are consistent with the cyber threat intelligence that Kivu gleaned through its extensive work in the ransomware response field. For the majority of Ryuk ransomware cases since August 2018, the initial intrusion vectors were Trickbot trojan infections. Kivu also observed that in some instances Ryuk's victims were infected with Trickbot as early as June and July of 2018, but the trojan stayed dormant for several weeks and didn't implement Ryuk ransomware encryption until August and September. This may indicate that the collaboration agreement between both groups was made as early as June 2018, and Trickbot operators started to accumulate a backlog of compromised victims in anticipation of the upcoming release of the newer Hermes variant. It's also possible that the Trickbot group had an exclusive head start to use the new Hermes v2.1 for 2 to 3 weeks prior to it being offered for sale on August 22, 2018.

Key Point: The strong link between Ryuk and Trickbot (operated by a known Russia-based group) is yet more evidence linking Ryuk to Russia.

III. Conclusion

Based on Kivu's findings, there's very strong evidence that the Hermes/Ryuk ransomware is most likely being developed and operated by Russian-based groups of cybercriminals. There is no evidence currently available that any Russian hacking groups are connected to or sponsored by North Korea.

It is of course possible that North Korean attackers (in the same way as attackers anywhere in the world) could purchase and use Ryuk. And Kivu together with other cyber security researchers) concluded that North Korean attackers used a misconfigured variant of the Hermes ransomware in the heist on Taiwanese Far Eastern International Bank's (FEIB). However, Kivu believes that based on the currently available evidence, there is nothing specifically linking Ryuk to North Korean attackers and the identification of the Ryuk variant is not per se indicative that North Korea lurks in the shadows.

As we have seen for most other ransomware attacks, reasonable attribution must be based on multiple factors including an analysis of the attack vector, use of specific tools, linguistics, and targets. The specific malware variant deployed (including Ryuk) is just one of these factors.

---

[11] https://malwarehunterteam.com/

[12] Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware, Crowd Strike, January 10, 2019 https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

About the Author

Evgueni Erchov is an Associate Director of Cyber Investigations at Kivu Consulting in Washington, DC. Evgueni has more than 20 years of professional experience in cybercrime investigations, computer forensics, app development, cryptocurrency blockchain technology and cyber threat intelligence in the federal and private sectors.

Prior to joining Kivu, Evgueni worked at the Federal Deposit Insurance Corporation (FDIC) where he provided incident response, malware reverse engineering and post-breach investigative services to FDIC-insured banks.

Mr. Erchov earned his Bachelor of Science in Information Systems and Technologies from Moscow Engineering Physics Institute (MEPhI) and MBA with IT Management concentration from George Washington University (GWU).

Evgueni is a Certified Information Systems Security Professional (CISSP), DCITA Digital Media Collector (DMC), DCITA Digital Forensics Examiner (DFE), Information Technology Infrastructure Library (ITIL) v3, US Army Cyber Operations Planner (ACOP) and Project Management Professional (PMP).

About Kivu

Kivu's data security experts and forensic investigators are experienced in protecting organizations against compromise of data, theft of trade secrets and unauthorized access to personally identifiable information. You can count on our real world investigative experience to provide cutting edge data security advice on issues we are seeing in the field right now. Our qualifications include IT certifications; Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and various forensic certifications including; Encase Certified (EnCE), SANS/GIAC Certified Incident Handler (GCIH), Certified Ethical Hackers, and reverse malware experts. Our experts have prior backgrounds as network security professionals, IT administrators and legal counsel.

Kivu's investigators have testified as computer forensic experts in US state and Federal courts, and presented their findings to US and EU regulators.

More information about Kivu can be found at www.kivuconsulting.com.

San Francisco - New York - Washington, DC – Denver – Toronto - Amsterdam