KIVU THREAT INTELLIGENCE

Cyber Threat Intelligence Insights for Claims and Underwriting Professionals

Volume XIX-2 *March 13, 2019*

Purpose
To share cyber threat intelligence and protect 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

Working Around Issues with Ryuk Decryptor

I. Executive Summary

A relatively new strain of ransomware, dubbed "Ryuk" by its creators, has been on the rise recently. As we move forward in 2019, the number of Ryuk infections will undoubtedly continue to grow. This is especially true now that Kivu has observed Ryuk being linked to Trickbot, a sophisticated banking trojan, with both types of malware being deployed in many attacks. This apparent partnership is one that Kivu will continue to monitor and document. Even though Ryuk ransom demands are typically in the six or even seven-figure range, the decryptor tool offered by the Ryuk attackers is far from perfect. Imperfections caused by bugs or poor coding causes additional strain on responders during an already stressful event. Significantly for victims and the cyber insurance market, problems with the Ryuk decryptor can cause major delays in bringing systems back online, leading to serious business interruption and further losses.

In response, Kivu has developed the Kivu Ryuk Response Tool (RRT) to speed up the decryption process and address some of the flaws associated with the Ryuk decryptor.

II. Issues and Work Arounds

Rearing its ugly head in late 2018, Ryuk is a Hermes ransomware derivative which is thought to be named after a fictional Japanese character in the manga series Death Note. The malware appears to be a favorite tool of criminal groups based in Russia and former Soviet satellite states. If a client makes the business decision to pay for the decryption tool, it could be very costly and will include several flaws.

```
Ryuk decryptor software
Check system for Ryuk infection...
system is clean
choose method:
  1. Decrypt per file (manually choose file)
  2. Start fully automatic decryption of all files
(write number and press enter)
2
DECRYPT START FOR 30 SECONDS, TURN OFF ALL ANTIVIRUS SOFTWARE
NOTE: don't do anything, just wait, after decrypt has been finished u see the message
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++
```

a. Special Characters and Long Paths

The most common issue seen with the Ryuk decryptor involves the way it handles (or rather does not handle) special characters and long paths in the names of infected files. If the system being decrypted has a large directory hierarchy or any special characters in the path or filename (ex. &, (,], !, or even sometimes spaces) it is possible that the decryptor will skip the file, or error out. In early Ryuk cases, we were finding that the clients often failed to recover 20 - 30% of their data. Kivu therefore has developed a proprietary protocol based around the filesystem feature known as "hard-linking," which tricks the decryptor into decrypting these special character/long path files, drastically reducing the amount of non-recoverable data.

b. Speed of Decryption

Kivu's proprietary "hard link" protocol also solves another issue with the decryption software: its speed. Not surprisingly, ransomware developers have focused their skills on speeding up the encryption process – they're not concerned with making decryption particularly efficient. Hard-linking all known encrypted files to a single directory under the root of each active disk allows the decryptor to find and decrypt files more quickly. Doing so will also relieve disk I/O fatigue that is caused by the decryptor recursively searching for encrypted files. Suddenly the decryption process takes hours rather than days, mitigating the effects of business interruption.

c. The .RYK Extension and ReadMeRyuk.txt

Another annoyance with the Ryuk decryptor lies in its developer's decision to not remove the .RYK extension from files after it finishes decrypting them. This means responders must manually remove or script the removal of the extension for all systems and files impacted. The same goes for the ransom notes, which exist in every directory touched by the Ryuk encryptor. Again, Kivu's RRT addresses this issue.

d. The Kivu Ryuk Response Tool

The Ryuk Response Tool (RRT) has been developed by Kivu to address known problems associated with the Ryuk decryptor. The RRT has the following capabilities as of version 1.5:

- Creates a directory under ALL available drive roots called HARDLINKS automatically (multi-drive support)
- Collects all files with .RYK extension and saves them to library.txt in $drive\HARDLINKS
- Creates a hard link in HARDLINKS directory to the encrypted file using a randomly generated 20-character name
- Adds target file and hard link name to a single location in $drive\HARDLINKS (for troubleshooting in case of errors)
- Removes the .RYK extension from all encrypted files
- Prompts user to delete all ransom notes
- Checks to ensure host is using PowerShell 5 or greater for best deployment of RRT

Kivu deploys the RRT in all Ryuk cases where we are retained as the incident response. We believe using the RRT helps ensure our clients get their data and systems back up and operational as fast as possible during a Ryuk infection. Kivu will continue to develop this tool to add functionality to it.

Please keep yourself protected! To help avoid an infection with Ryuk and Trickbot, we recommend the implementing the following:

- Ensure secure back-up processes and procedures are in place, followed, and tested quarterly.
- Disable any Remote Desktop services that are listening on the Internet (RDP/MSTC, Teamviewer, LogMeIN, etc).
- Disable SMBv1 throughout your entire environment.
- Develop a strong password policy and implement/enforce it.

- Ensure centrally managed anti-virus/anti-malware software are on all systems and have up-to-date definitions.
- Educate your employees on the dangers of phishing e-mails and how to spot and report suspect messages.

About the Author

Ethan Cudzilo is a Senior Analyst of Cyber Investigations at Kivu Consulting in Washington, DC. Ethan has more than 8 years of professional experience working in the Information Security domain specializing in areas such as: incident response, malware analysis, digital forensics, proactive monitoring, security control implementation, vulnerability assessments, system hardening, and policy creation, implementation & enforcement.

Prior to joining Kivu, Ethan worked as a consultant in the Entertainment, Financial and Aerospace industries. Mr. Cudzilo earned his Bachelor of Science in Information Security & Forensics from Rochester Institute of Technology (RIT).

Ethan has several certifications, including GIAC Information Security Professional (GISP), GIAC Certified Forensic Analyst (GCFA), Certified Hacking Forensic Investigator (CHFI), Certified Ethical Hacker (CEH) and is recognized as a Lethal Forensicator by the SANS Institute.

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