New Ryuk Ransomware Variant Poses Threat to HPH Sector

Executive Summary

The French National Agency for the Security of Information Systems (ANSSI) has identified a new variant of the Ryuk ransomware that is capable of self-replicating using existing Windows processes. The malware, which previously targeted the U.S. Healthcare and Public Health (HPH) Sector in October 2020, uses a privileged domain account as an initial infection point. After this foothold is established, the new variant spreads through the network, copying a unique version of the ransomware executable to new devices. Unlike previous versions of Ryuk, this new variant lacks any exclusion mechanisms to prevent multiple simultaneous infections or reinfections from occurring. Mitigations for this new variant, while limited, are included in the report below.

Report

Ryuk ransomware, first identified in August 2018, is a prolific ransomware that directly targeted the U.S. HPH Sector in October 2020. According to the Federal Bureau of Investigation (FBI), Ryuk has more completed ransomware payments than any other ransomware worldwide. ANSSI recently released a thorough report on a new variant of Ryuk that has developed self-replicating and worm-like abilities. A computer worm can spread copies of itself from device to device without human interaction or the need to attach itself to a specific software program.

In the case of a Ryuk infection, files will be encrypted and appended with .RYK and the files RyukReadMe.txt and RyukReadMe.html will appear in affected directories. These ransom notes direct victims to contact the ransomware operators at two specific email addresses and provide a Bitcoin wallet for ransom payment. Unlike other ransomware operators, Ryuk is not associated with a "name and shame" site where operators post ransom notes or identify victims and data exfiltration as part of a double extortion strategy is not part of its functionality. There is no evidence that this pattern of behavior has changed in the new Ryuk variant.

The agency's analysis identified the initial infection point as a privileged domain account. As the new variant moves through the network, it scans for network shares and copies a unique version of the ransomware executable to each of them as they are found. The new versions of the ransomware executable use the filename lan.exe or rep.exe. According to ANSSI's analysis, the worm also encrypts files with the AES256 algorithm of Microsoft's CryptoAPI and a unique AES key wrapped with an RSA public key stored in the binary code for each file. Currently, this self-spreading ability is limited to Windows machines.

Due to the tenacity of the new Ryuk variant, prevention is a more effective tool than mitigation or remediation once Ryuk takes hold in a system. The new variant also lacks any exclusion mechanisms such as a Mutual Exclusion Objection (MUTEX) to prevent multiple Ryuk processes from running on a single machine, so reinfection of the same device is possible once the initial infection is cleared. Ryuk infections most commonly begin with the deployment of a form of "dropper" malware as a foothold in the victim's machine. Cybercriminals often use TrickBot, Emotet, BazarLoader, and Zloader to introduce Ryuk. A list of mitigations for this attack chain can be found in the Cybersecurity and Infrastructure Security Agency's October 28, 2020 alert (AA20-302A), linked in the References section below.

Analyst Comment

ANSSI recommends changing the password or disabling the account for the privileged user that served as Ryuk's initial entry point to the network and then forcing a domain password change. This can be done using KRBTGT, a local default account found in Active Directory that acts as a service account for the Key Distribution Center service for Kerberos authentication. However, the agency cautions that this technique is not painless: "this would induce many disturbances on the domain – and most likely require many reboots – but would also immediately contain the propagation."

References

Artnz, Peter. "Ryuk ransomware develops worm-like capability," MalwareBytes. March 2, 2021. https://blog.malwarebytes.com/malwarebytes-news/2021/03/ryuk-ransomware-develops-worm-like-capability/

Davis, Jessica. "Update to Ryuk Ransomware Variant Adds Network Worming Capability," HealthITSecurity. March 2, 2021. https://healthitsecurity.com/news/update-to-ryuk-ransomware-variant-adds-network-worming-capability

Umawing, Joel. "Threat spotlight: the curious case of Ryuk ransomware," MalwareBytes. December 12, 2019. https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

Seals, Tara. "Ryuk Ransomware: Now with Worming Self-Propagation," ThreatPost. March 2, 2021. https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/

"Alert (AA20-302A)," Cybersecurity and Infrastructure Security Agency. October 28, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

"A Tsunami of Ryuk Ransomware Attacks Hits U.S. Hospitals," CISOMAG. October 29, 2020. https://cisomag.eccouncil.org/ryuk-ransomware-targeting-us-hospitals/

"The Ryuk Ransomware," French National Agency for the Security of Information Systems. March 1, 2021. https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-006/

"What is a computer worm, and how does it work?," Norton LifeLock. August 28, 2019. https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html