Ryuk Ransomware Cyber Report

Overview

During the last week of December 2018, Malwarebytes reported on highly targeted attacks that distributed Ryuk ransomware and crippled at least two companies: cloud hosting provider Data Resolution, and the umbrella company Tribune Publishing (responsible for publishing multiple newspapers).[1] The infections were reported to be secondary payloads of Emotet and Trickbot trojans.

Customer Impact

Emotet is frequently distributed via malicious email campaigns, and is capable of stealing credentials and downloading additional malware. Trickbot is a banking trojan known for targeting users of specific banks. It can exfiltrate data off of the victim's network, steal from cryptocurrency wallets, and load additional modules for other tasks.

Ryuk encrypts files and attempts to encrypt network drives. Ryuk then runs a Windows batch script to delete its encryption key, shadow copies of files, and any available backup files. Initial ransoms to decrypt files have reportedly been between 15 and 50 Bitcoin (BTC).[2] In their notes, the author(s) threatened to increase the required ransom payments by 0.5 BTC each day until the victim would pay.[3]

Campaign Analysis

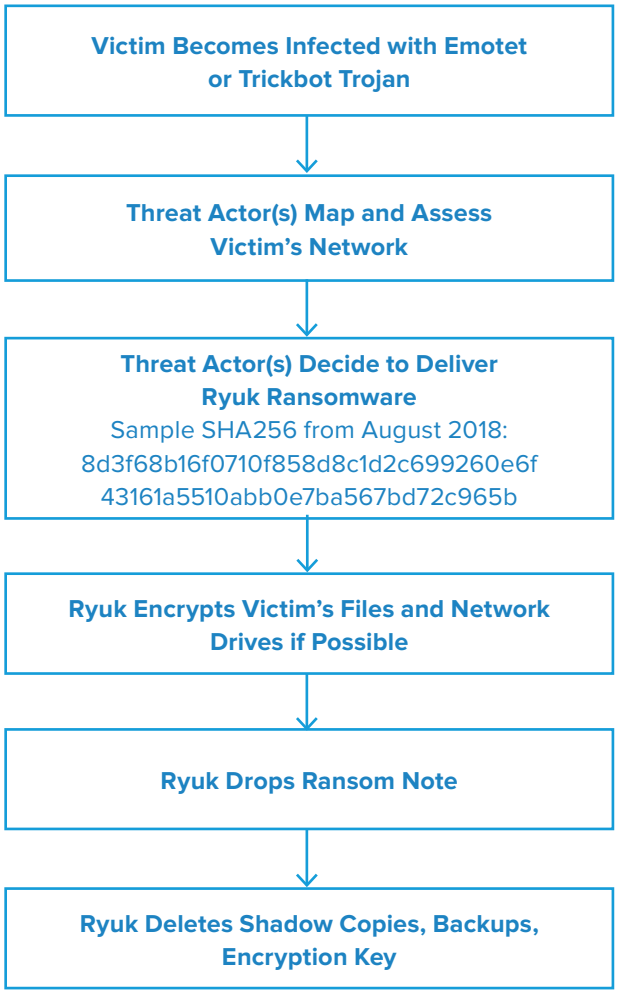
There has been a small number of recent Ryuk infections, indicating that the threat actor(s) behind the infections may be distributing the ransomware on a case-by-case basis after researching the victim's network.

Malwarebytes and Checkpoint Research report that Ryuk shares many similarities with Hermes ransomware (attributed to the Lazarus Group, a North Korean Advanced Persistent Threat group).[4] In some cases Ryuk shared exact code segments from Hermes samples. For example, both Ryuk and Hermes ignore files in the same set of directories during encryption. Infoblox published a Cyber Campaign Brief about Hermes ransomware in July, 2018.[5]

Malwarebytes observed Ryuk being distributed as a follow-on payload from Emotet and Trickbot, though the threat actor(s) may distribute it by other means as well. Malwarebytes speculated that once a host had been infected with Emotet or Trickbot, attackers would manually map out the victim's network to determine whether or not it meets some set of requirements prior to infecting it with Ryuk.

Due to the limited scale of these attacks, Infoblox cannot currently provide network indicators related to Ryuk. No source has reported the files used in the most recent attacks; however, Checkpoint Research shared some hashes in August, 2018.

Attack Chain



Vulnerabilities & Mitigation

Ryuk ransomware has been delivered as a secondary payload in targeted attacks on networks already infected with malware. As such, Infoblox recommends the following to reduce the likelihood of infection:

1. Regularly train users about potential phishes and how to handle them appropriately.
2. Require strong passwords from users.
3. Stay up-to-date on firmware updates and patches.
4. Back up data and systems regularly to minimize the potential impact of ransomware in general.
5. Ideally, store backup data off the network.

Appendix

Representative Indicators of Compromise	Description
8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567 bd72c965b3012f472969327d5f8c9dac63b8ea9c5cb0de002d16 c120a6bba4685120f58b4b8e463789a076b16a90d1aae73cea9 d3880ac0ead1fd16587b8cd79e37a1a3d89b86a50b36aea5 cc4cb60573a3660cf799a9ec1f69a3d4572d3dc277361a0ad2113af7 5f13547be184822f1268f984b79f35965a1b1f963d23b50a09741b0a ec1455091954ecf9ccd6fe60cb8e982d9cfb4b3dc8414443ccfdf c444079829d56c51024bb119211c335f95e731cfa9a744fcdb645 a57d35fb379d01b7dbdd098e	Ryuk SHA256 hashes (Reported by Checkpoint research in August, 2018)

Endnotes

1. “Ryuk ransomware attacks businesses over the holidays ….” 8 Jan. 2019, https://blog.malwarebytes.com/ cybercrime/ malware/2019/01/ryuk-ransomware-attacks-businesses-over-the-holidays/. Accessed 10 Jan. 2019.
2. As of this writing, 1 BTC is roughly $3,600 USD.
3. “Ryuk Ransomware: A Targeted Campaign … - Check Point Research.” 20 Aug. 2018, https://research. checkpoint.com/ ryuk-ransomware-targeted-campaign-break/. Accessed 10 Jan. 2019.
4. Infoblox has no evidence to confidently tie Ryuk to the Lazarus Group aside from its similarity to Hermes Ransomware.
5. “Cyber Campaign Brief: Hermes Ransomware.” 30 July. 2018, https://sites.google.com/a/infoblox.com/ cyberint-threat-labs/home/publication-repo/20180727_CCB_ Hermes_Endnotes%20%282%29.pdf?attredirects=0&d=1. Accessed 10 Jan. 2019

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com