WIZARD SPIDER Adds New Features to Ryuk

crowdstrike.com/blog/wizard-spider-adds-new-feature-to-ryuk-ransomware/

November 1, 2019

WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN

November 1, 2019

Alexander Hanel and Brett Stone-Gross Research & Threat Intel

CrowdStrike® Intelligence analyzed variants of *Ryuk* (a ransomware family distributed by WIZARD SPIDER) with new functionality for identifying and encrypting files on hosts in a local area network (LAN). These features target systems that have recently been placed in a standby power state, as well as online systems on the LAN.

Magic Packet

The first new Ryuk feature attempts to wake LAN hosts that are in a standby power state by sending them a Wake-on-LAN (WoL) magic packet. The affected machine must support WoL, and its network card must have the setting configured in the BIOS. To identify machines on the LAN, Ryuk reads entries in the host Address Resolution Protocol (ARP) cache; in addition, for each address in the cache, it sends a WoL magic packet. The packet is sent over a User Datagram Protocol (UDP) socket with the socket option `SO_BROADCAST`

using destination port `7`. The WoL magic packet starts with `FF FF FF FF FF FF`, followed by the target's computer MAC address. An example WoL packet is highlighted in blue in Figure 1.

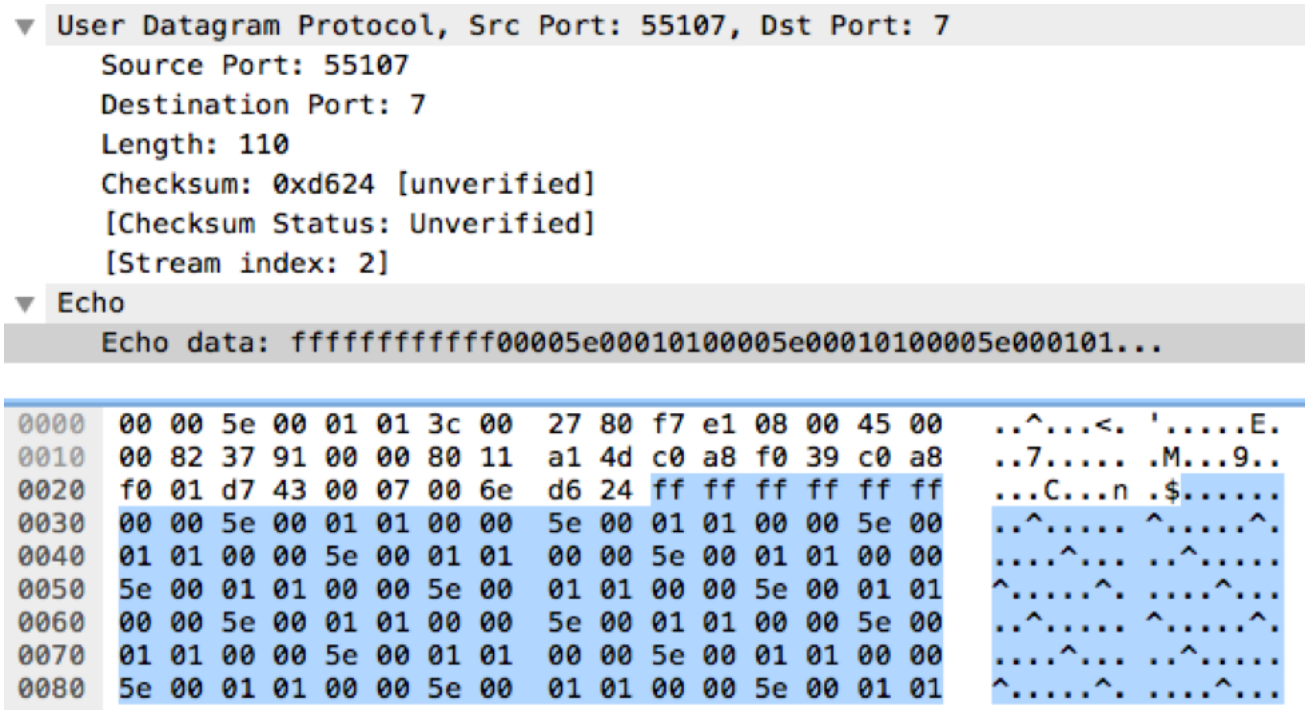

Figure 1. Ryuk Wake-on-LAN Packet Example

UDP packets observed being sent specifically to destination port `7` during a ransomware incident may be an indication that Ryuk is present.

This Wake-On-LAN implementation is somewhat naive, because the default ARP cache timeout is short-lived on modern versions of Windows. Thus, the number of systems that may be impacted by this current implementation is likely to be limited, since only systems that have recently been put to sleep would still have their MAC address present in a remote system's ARP cache.

ARP Ping Scanner

The second Ryuk feature uses ARP ping scanning to identify hosts on the LAN. To identify the proper subnet to scan, it checks each entry in the ARP cache to see whether it contains an IP address with the substrings "`10.`," "`172.16.`," or "`192.168`." in it. If an IP address contains one of these strings, it starts sending ARP and PING requests to all IP addresses in the Class C network starting with that string value. For example, if the ARP cache entry contained the IP address `192.168.240[.]57,` it would start scanning at `192.168.240[.]1` and increment the last octet by 1 until reaching the IP address `192.168.240[.]254`. If a host responds, Ryuk attempts to mount it as a network drive, using Server Message Block (SMB), and encrypt its contents.

Conclusion

By attempting to wake systems and using ARP ping scanning combined with network drive mounting, WIZARD SPIDER is seeking to maximize the number of systems that can be impacted by Ryuk's file encryption. The Wake-on-LAN feature is a novel technique that demonstrates WIZARD SPIDER's continued focus on increasing the monetization of infections via ransomware.

CrowdStrike Intelligence will continue to monitor any further development to Ryuk by WIZARD SPIDER. The CrowdStrike Falcon® endpoint protection platform detects and prevents against Ryuk. For Falcon endpoint customers, prevention settings should be set at a minimum to the following:

- Next-Gen Antivirus: Cloud/Sensor Machine Learning: Set "Prevention" slider to "Moderate"
- Malware Protection: Execution Blocking: Toggle "Prevent Suspicious Processes" to "Enabled"
- Add any hashes to your custom blacklist for added protection

SHA256 HASH	BUILD TIME
74654957ba3c9f1ce8bb513954b9deea68a5a82217806977a1247fb342db109f	2019-10-09 22:09:27
7dc3fc208c41c946ac8238405fce25e04f0c2a7a9e1d2701986217bd2445487a	2019-10-10 09:18:33

Additional Resources

- *For more information on how to incorporate intelligence on dangerous threat actors into your security strategy, please visit the Falcon X product page.*
- *Read the 2020 Global Threat Report.*
- *Read the 2019 Falcon OverWatch Report: "Observations From the Front Lines of Threat Hunting."*
- *Learn more about the CrowdStrike Falcon® Platform by visiting the product webpage.*
- *Test CrowdStrike next-gen AV for yourself. Start your free trial of Falcon Prevent™ today.*

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell