UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00115

RYUK RANSOMWARE'S TERRIFYING EVOLUTION

DATE ISSUED: 8th March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Researchers have discovered a new and alarming version of the notorious Ryuk Ransomware which possess worm-like capabilities of self-replication propagation.

BREAKDOWN

First seen in 2021 in a campaign targeting Windows the French National Agency for the Security of Information Systems (ANSSI) has disclosed that this variant scans private IP ranges (10.0.0.0/8, 172.16.0.0/16 and 192.168.0.0/16) seeking network shares and copying a unique version of the ransomware executable to each one as they are discovered. The file extension are rep.exe or lan.exe and upon launch, the ransomware is pushed to every machine that has Remote Procedure Call enabled. The ransomware may also infect Address Resolution Protocol (ARP) tables, sending a "Wake-on-LAN" packet to each host in the cache with the intention to mount network shares using Server Message Block (SMB) on each identified host. Once installed, the ransomware will execute using a scheduled task to carry out the encryption of all files and in an effort to prevent file recovery it will delete any Volume Shadow Copies. Microsoft CryptoAPI is used to carry out the encryption using AES256 and secured with an RSA public key stored in the binary code. This ransomware is often deployed paired with another malware through a phishing campaign such as Emotet or TrickBot which act as an installer or 'dropper' that the attacker will use initially to escalate privileges and move laterally across a network.

REMEDIATION STEPS

- Educate users on the dangers of phishing, social engineering, and email attachments, how to identify these kinds of attacks and what to do if they suspect and email, hyperlink, or attachment to be malicious.
- Use endpoint malware detection and remediation software to scan and halt suspicious behaviour.
- Use network monitoring tools to discover, alert on, and block anomalous behaviour – particularly relating to network shares in this instance.
- Develop, carry out, and test a regular backup schedule in line with your organisation's IT Security policies.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/ryuk-ransomware-worming-self-propagation/164412/
KnowBe4 https://blog.knowbe4.com/heads-up-new-ryuk-ransomware-strain-now-worms-itself-to-all-your-windows-lan-devices