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

CYBER GUIDANCE ISSUE 00177

LEMONDUCK MALWARE TARGETS MICROSOFT & LINUX

DATE ISSUED: 3rd August 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

This new cryptomining malware removes competing malware on infected systems and prevents new infections by patching the vulnerabilities it used to gain entry as well as disabling Microsoft Defender and other vendor-supplied anti-malware tools and capabilities.

BREAKDOWN

Distribution methods for LemonDuck attacks includes phishing emails, exploits, USB devices and brute force attacks, existing vulnerabilities in on-premises Microsoft Exchange Servers and the Eternal Blue SMB exploit - targeting both Windows and Linux systems. The malware uses automated tools to carry out server discovery activities before loading CobaltStrike, web shells and additional malware modules and a host of other tools. The group behind the attacks are known for their hands-on hacking post-breach. Gaining its name from the PowerShell script "Lemon_Duck" that launches Notepad and JavaScript code within while also acting as a tracking agent, the attack comprises of running scripts against Outlook to utilise present credentials and further disperse phishing emails to all contacts. Attempts to "own" a victim's network makes this attack more than just a cryptomining operation as the attackers also have full access to infected devices, can establish persistence and ensures it is difficult to remove by using file-less malware that executes in-memory and process injection techniques. Scripts are hosted on multiple sites making it difficult for enforcement agencies to track and take down.

REMEDIATION STEPS

- Apply the latest patches available to avoid exploitation of older and known (high-profile) vulnerabilities.
- Check vulnerabilities known to be exploited be LemonDuck and remediate in your environment:
  CVE-2017-0144 (EternalBlue), CVE-2017-8464 (LNK RCE), CVE-2019-0708 (BlueKeep), CVE-2020-0796 (SMBGhost), CVE-2021-26855 (ProxyLogon), CVE-2021-26857 (ProxyLogon), CVE-2021-26858 (ProxyLogon), and CVE-2021-27065 (ProxyLogon).

REFERENCES & RESOURCES

ZDNet https://www.zdnet.com/article/microsoft-warns-over-this-unusual-malware-that-targets-windows-and-linux
https://www.zdnet.com/article/microsoft-this-unusual-windows-and-linux-malware-does-everything-it-can-to-stay-on-your-network