UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00136

UNPATCHED EXCHANGE SERVER CRYPTOJACKING

DATE ISSUED: 19th April 2021

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Cryptojacking is the latest attack seen against vulnerable on-premis Microsoft Exchange Servers using the ProxyLogon exploit and are being used to host Monero cryptocurrency mining malware.

BREAKDOWN

Sophos Labs released a report stating that they had seen activity from an unknown attacker attempting to install cryptojacking malware on to vulnerable Exchange servers, hosting the payload on another compromised Exchange server. Executables noted were Mal/Inject-GV and XMR-Stak Miner (PUA). PowerShell was used to retrieve a win_r.zip file from the compromised server's Outlook Web Access logon path which contained batch scripts that utilised certutil.exe to download additional uncompressed files. The base54 payload in written out to the file system and decoded by the certutil program. Then a second command adds the outputs to the same directory and once decoded runs an executable to extract the miner and its configuration data and once running, deletes any evidence it existed. It appears that the attacker has modified code for tools freely available on GitHub.

REMEDIATION STEPS

- Install patches and security updates released for Microsoft Exchange Server versions 2013, 2016, 2019 – although 2010 is considered out of support, there is still a patch available for this version.
- See Sophos resources for a full list of Indicators of Compromise (IoCs) and further CVE info.
- Report any incidents of breach to CERT NZ by calling 0800 CERTNZ or via their website https://www.cert.govt.nz/it-specialists/report-an-incident/

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/attackers-target-proxylogon-cryptojacker/165418/
Sophos	https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/ https://github.com/sophoslabs/IoCs/blob/master/PUA-QuickCPU_xmr-stak.csv