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

CYBER GUIDANCE ISSUE 00140

EXCHANGE PROXYLOGON USED TO ESTABLISH APT

DATE ISSUED: 27th April 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

The Prometei botnet is the latest in a string of criminal activity targeting two of the ProxyLogon vulnerabilities affecting on-premis Microsoft Exchange Servers and is installing Monero miners and establishing a complete foothold making it an Advanced Persistent Threat.

BREAKDOWN

While cryptojacking has already been seen in a series of attacks targeting vulnerable Microsoft Exchange Servers, the Prometei malware – named for the Greek Titan Prometheus, god of fire – gives the attacker complete control over any infected devices, increasing the potential scope of damage. It is speculated that from this foothold, the attackers will be able to infect connected endpoint devices, exfiltrate information and open the door to collaboration with ransomware gangs. Various industries and geographies have already been targeted by the threat in a random pattern. The malware copies itself onto the C: Drive and creates a firewall rule allowing connections over HTTP, and sets a registry key for added persistence before downloading the payload from the C2 (Command and Control) Server. The XMRig cryptominer (discussed in Cyber Guidance 136) is used to mine Monero cryptocurrency. The attackers are able to add additional modules to increase their attack capability at any time and uses a range of tools (including Mimikatz, EternalBlue and BlueKeep) to propagate across a network and gain access to as much information and as many systems and possible.

REMEDIATION STEPS

- Install patches and security updates released for Microsoft Exchange Server versions2013, 2016, 2019– although 2010 is considered out of support, there is still a patch available for this version.
- See Microsoft resources below 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

Microsoft https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
Threatpost https://threatpost.com/prometei-botnet-apt-attacks/165574/