UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 0280

CRYPTOMINERS TARGET MS EXCHANGE PROXYSHELL

DATE ISSUED: 20th February 2023

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

OVERVIEW

Threat actors are exploiting 'ProxyShell' vulnerabilities in Microsoft Exchange servers to deploy cryptocurrency miners on Windows machines. The new malware dubbed as "ProxyShellMiner" leverages a security flaw to co-opt the target's computing resources to mine crypto currencies like Bitcoin.

BREAKDOWN

'ProxyShell' is a combination of three Exchnage vulnerabilties that were previously addressed by Microsoft in May 2021. When chained together they allow adversaries to bypass Access Control List (ACL) controls and elevate privileges on the Exchange PowerShell backend, effectively permitting the attacker to perform unauthenticated, Remote Code Execution (RCE). An attacker gains initial access to the target's network and drops a .NET 'dropper' script into the NETLOGON folder of the domain controller. This loads the crypto-mining malware on all the devices in the network. The malware then downloads additional files to establish persistence on the machine and activate the mining activities. It deploys XMRig – one of the most popular cryptocurrency mining malware variants, generating the Monero (XMR) cryptocurrency for attackers by using the system's CPU and sometimes GPU. It also creates a firewall rule that blocks outgoing traffic to evade detection from security tools.

REMEDIATION STEPS

- Apply all updates and security patches for ProxyShell vulnerability in Microsoft Exchange Servers.
- Monitor systems and network for typical signs of crypto-mining operation such as increased CPU usage, degraded performance, and slow application response.
- Ensure that information about cryptomining is included in company comms, cybersecurity awareness training, and company policy to drive recognition that such activities are not an acceptable use of company resources.
- Block websites hosting JavaScript miners both at the gateway and the endpoints.
- Ensure that you are utilising a Next Generation Antivirus (NGAV) and anti-malware solution that does not solely rely on software signatures to detect malicious activity. Ensure agents are set to auto-update.
- Implement security-in-depth/defense-in-depth multilayered protections.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/microsoft-exchange-proxyshell-flaws-exploited-in-new-crypto-mining-attack/