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

CYBER GUIDANCE ISSUE 00231

PROXYSHELL & PROXYLOGON USED FOR "MALSPAMMING"

DATE ISSUED: 1st December 2021

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

OVERVIEW

Microsoft Exchange vulnerabilities known as ProxyLogon and ProxyShell are still being used in unpatched servers for malspamming attacks – which involve hijacking existing reply threads to deliver malware, bypassing email security filtering.

BREAKDOWN

SquirrelWaffle – a new email loader that emerged in September may be just one piece of the malware puzzle in a recent series of attacks along with Qakbot and CobaltStrike as seen by Cisco's Talos team. SquirrelWaffle campaigns steal existing email chains to insert malicious URLs into the conversation to increase the chances the victim will access the link. Trend Micro also weighed in on the conversation confirming that using replies is an easy way to circumvent email filtering security controls by using distribution through the internal domain users. Researchers and investigators disagree about the attackers motives or activities

REMEDIATION STEPS

- Apply all security patches for Microsoft Exchange released in March, May & July 2021 immediately.
- If applying patches in not possible, Trend Micro suggests:
  - Enable virtual patching modules on all Exchange servers to provide critical level protection for servers that have not yet been patched
  - Use Endpoint Detection and Response (EDR) solutions in critical servers, as it provides visibility to machine internals and detects and suspicious behaviour running on servers
  - Use Endpoint protection designed for servers
  - Apply sandbox technology on email, network and web to detect similar URLs and samples.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/attackers-hijack-email-threads-proxylogon-proxyshell/176496/
Trend Micro https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html