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

CYBER GUIDANCE ISSUE 00152

EPSILON RED TARGET MS EXCHANGE SERVERS

DATE ISSUED: 8th June 2021

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

OVERVIEW

By hunting down unpatched Microsoft Exchange Servers threat actors are deploying ransomware attacks to with a new malware known as Epsilon Red.

BREAKDOWN

Using unpatched Microsoft Exchange Servers as an entry point and the Windows Management Instrumentation (WMI) scripting automation tool, attackers are deploying Epsilon Red, described as a "bare-bones" 64bit executable written in the Go programming language (GoLang). The malware sets up the compromised machines, and therefore network, to facilitate a full-scale ransomware attack using a series of PowerShell scripts labelled 1.ps1 and 12.ps1 and other singular numbers or letters of the alphabet. The PowerShell scripts uses basic obfuscation techniques to evade detection by anti-malware tools. The ransomware itself is labelled RED.exe, compiled by MinGW and uses the runtime unpacker UPX. It is a small, simple program that creates numerous child processes, which results in many copies of the ransomware running simultaneously to encrypt subfolders quickly. It also attempts to retrieve and crack passwords, kills active processes, deletes, and disables logs and any Volume Shadow Copies or programs labelled "Backup" or "Cloud" to prevent recovery without paying the ransom. Once the zipped file RED.7z is unpacked and implanted in %SYSTEM%\RED, there is a delay of one hour before execution of commands to modify firewalls to allow inbound connections on all TCP ports except 3389 and 5650 and download a Tor Browser or a copy of Remote Utilities. The ransom note featured in a recent attack bore similarities to those discovered in attacks carried out by the REvil Ransomware gang.

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.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/exchange-servers-epsilon-red-ransomware/166640/
Sophos	https://news.sophos.com/en-us/2021/05/28/epsilonred/
IT Brief	https://itbrief.co.nz/story/new-ransomware-epsilon-red-discovered-how-it-works
Microsoft	https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/