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

CYBER GUIDANCE ISSUE 00119

RANSOMWARE DEPLOYED IN EXCHANGE ATTACKS

DATE ISSUED: 15th March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Attackers have stepped up the effects of a breach in Microsoft Exchange Servers following the discovery of the vulnerability last week (Cyber Guidance Issue 0114) and widespread attacks are being reported globally. Not only are the breaches dangerous in terms of deployment of persistent threats and data exfiltration, threat-actors are now adding the DearCry Ransomware to the mix and deploying the malware via successfully breached servers.

BREAKDOWN

Since the discovery and public disclosure of a critical vulnerability on Microsoft on-premis Exchanger servers, reports are flooding in regarding breach activity by malicious actors and is now being used to deploy the DearCry Ransomware into victims' environments. By chaining four flaws together, attackers can create a pre-authentication Remote Code Execution (RCE) allowing the full takeover of servers without the need for a set of valid credentials. When files are encrypted, they display the suffix ".CRYPT" and contain the file marker "DEARCRY!." Payment demanded is $16,000 through a reademe.txt containing contact email addresses for the attackers. While not widespread yet, researchers predict this is a serious threat and other similar attacks may follow suit and are urging all servers to be patched and updated immediately.

REMEDIATION STEPS

- Users are being urged to install all patches available immediately for on-premis Microsoft Exchange server's versions 2010, 2013, 2016 and 2019.
- See Cyber Guidance Issue 0114 for further sources.
- 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/microsoft-exchange-exploits-ransomware/164719/
CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/urgent-microsoft-exchange-security-update
Bleeping Computer	https://www.bleepingcomputer.com/news/security/ransomware-now-attacks-microsoft-exchange-servers-with-proxylogon-exploits/amp/