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

CYBER GUIDANCE ISSUE 00250

'CUBA' RANSOMWARE GANG EXPLOITS PROXYSHELL

DATE ISSUED: 1st March 2022

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

OVERVIEW

ProxyShell/ProxyLogon is remaining one of the most exploited vulnerabilities in the wild off the back if their discovery in 2021. With vast numbers of servers remaining unpatched, cyber-criminal ransomware gangs such as "Cuba" continue to take advantage of these "chinks in their victim's armour."

BREAKDOWN

The group scans for vulnerable internet facing services in their initial reconnaissance using WEDGECUT and once found deploys webshells to set up a backdoor and establish a foothold. Alternatively, they have also been known to distribute malware via social engineering emails and phishing campaigns. A standard pattern of behaviour is to use legitimate credentials for valid accounts to escalate privileges acquired by using Mimikatz and Wicker. The Hancitor malware downloader is used in the initial stages of compromise to add NetSupport RAT as well as BEACON and BUGHATCH deployed using the TERMITE memory-dropper. BURNTCIGAR is also used to disable endpoint security software. Additionally, another unique feature of this group is they seem to be the only ones to use the COOLDRAW ransomware suggesting it may be proprietary, Not only does the group encrypt files, they also commonly exfiltrate data and steal valuable files. One of the most targeted nations by the group are our neighbours in Australia so it may be only a matter of time before their attention shifts across the ditch to NZ.

REMEDIATION STEPS

- Learn more about how to protect against Ransomware by checking out all the tips in our "Hot Topic: Ransomware" blog article and download your free copy of our Ransomware Defence Checklist.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/microsoft-exchange-exploited-cuba-ransomware/178665/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/
Security Affairs	https://securityaffairs.co/wordpress/125274/cyber-crime/cuba-ransomware-fbi-flash-alert.html