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

CYBER GUIDANCE ISSUE 00058

RYUK RANSOMWARE EXPLOITS 'ZEROLOGON'

DATE ISSUED: 27th October 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The Zerologon exploit recently identified by Microsoft CVE-2020-1472 has been exploited by a group using Ryuk Ransomware with devastating effect.

BREAKDOWN

In this particular attack, phishing emails were sent containing the Bazar loader and from there, the attackers were able to escalate their privileges using the Zerologon flaw and completely encrypt the system, moving across the victim's network in under five hours. By compromising the Active Directory services and using a variety of tools including Cobalt Strike, AdFind, WMI and PowerShell as well as built in tools such as Nltest, compromising the Domain Controller and resetting the password was the first step before spreading to the secondary controller using Remote Desktop Protocol (RDP) using a built in administrator account. Further lateral movement was facilitated using Server Message Block (SMB and Windows Management Instrumentation (WMI) executions of Cobalt Strike. The attackers then set their sights on the back up servers and deployed ransomware executable files. Thereafter the same malware was deployed to workstations and other servers within the environment, finalising their attack by executing Ryuk on the Primary Domain Controller. This is just one example of the serious nature of attacks that may take place if servers remain unpatched and vulnerable to the Zerologon flaw.

REMEDIATION STEPS

- Apply the appropriate patches on all Domain Controllers from Microsoft to remove the Zerologon flaw
- Educate users on spotting phishing emails and correct procedure if phishing is suspected.
- Ensure all data and systems are backed up external to the main network, including offsite and remote backups
- Ensure the team has the means and ability to detect, respond to and isolate any attack in a timely manner

REFERENCES & RESOURCES

Threatpost https://threatpost.com/ryuk-ransomware-gang-zerologon-lightning-attack/160286/
Financial Cert https://www.financialcert.tn/2020/10/20/ryuk-ransomware-group-using-zerologon-vulnerability-to-accomplish-their-objective-faster/
Born City https://borncity.com/win/2020/10/23/franzsische-it-firma-sopra-steria-von-ryuk-ransomware-befallen-zerologon-ausgenutzt/