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

CYBER GUIDANCE ISSUE 00146

MICROSOFT SHAREPOINT RANSOMWARE PHISHING

DATE ISSUED: 24th May 2021

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

OVERVIEW

Using the Microsoft Office SharePoint to bypass Security Email Gateways (SEGs), attackers a distributing legitimate looking document shares via email which then exploits an old bug to deploy ransomware when accessed by the user.

BREAKDOWN

While the email campaign is not particularly sophisticated and would be easily identified as suspicious by an aware user, the circumvention of technological controls still poses a significant risk that ransomware has the potential to be installed. The ransomware has been dubbed Hello by some and WickrMe based on the extension of the attached files and the use of the Wickr encrypted instant messaging service. The bug being exploited by attackers is tracked as CVE-2019-0604 that can be used for Remote Code Execution (RCE) to gain a foothold in unpatched servers. Once access is gained, Cobalt Strike is being used to move laterally to the Domain Controller and from there launch the ransomware.

REMEDIATION STEPS

- Install all available Microsoft Security Patches – this flaw was remedied in the March 2019 update.
- Use SPAM and Secure Email Gateway filtering to prevent malicious emails from reaching your users.
- Use Next Generation Endpoint Protection Software on all user devices to detect and respond to suspicious activity that uses "time-of-click" protections.
- Use URL filtering to prevent access to known malicious sites.
- Educate users to raise awareness around social engineering and phishing emails and what to do within your organisation if they suspect an email is malicious.
- This particular campaign is notorious for spelling and grammar errors and this indicator should be drawn to users attention.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/sharepoint-phish-ransomware-attacks/165671/
The Record https://therecord.media/ransomware-gang-targets-microsoft-sharepoint-servers/