UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0292

EMOTET NOW SPREAD VIA ONENOTE ATTACHMENTS

DATE ISSUED:20 20th March 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

Threat actors are now leveraging Microsoft OneNote attachments to deliver malware via phishing emails after Microsoft disabled macros by default in Word and Excel Office documents. They create intricate templates that appear to be a protected document with a message to 'double-click' a design element to view the file.

BREAKDOWN

Emotet is one of the most distributed malware in the past previously deployed through Microsoft Word and Excel attachments with malicious macros. Last summer Microsoft released an advisory in which the files containing macros downloaded from the internet will be automatically blocked. However, security researcher Abel discovered that Emotet malware is now being distributed via Microsoft OneNote attachments. Social engineering method such as malicious emails crafted as guides, how-to's, invoices, and job references are being employed to trick users. The emails contain a Microsoft OneNote document that prompts the user to double-click the 'View' button to display the document properly. A malicious VBScript file called 'click.wsf' is hidden underneath the "View" button. Once a user clicks on the button, a warning is displayed before launching the embedded file in OneNote, but historic behaviour suggests users will ignore this and are most likely to press the OK button. If the user clicks on the OK button, the embedded click.wsf VBScript file will be executed and download the Emotet malware as a DLL. It will run silently on the compromised device serving as a base for other cyberattacks.

REMEDIATION STEPS

- Create Microsoft Office group policies to either block or restrict the launch of embedded file attachments in Microsoft OneNote files.
- Educate users on how to spot phishing and social engineering emails and what to do with them in your
- organisation.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evade-defenses/
Malware Bytes	https://www.malwarebytes.com/blog/threat-intelligence/2023/03/emotet-onenote