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

CYBER GUIDANCE ISSUE 0268

MS ONENOTE ATTACHMENTS IN MALICIOUS EMAILS

DATE ISSUED: 23rd January 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

After Microsoft disabled macros by default in Office documents threat actors now use OneNote attachments in phishing emails which infects a machine with remote access malware.

BREAKDOWN

Threat actors have been using malicious Word and Excel attachments that launch macros to download and install malware. Since it has been disabled by default threat actors are now switching to new file format to spread malware. Microsoft OneNote is a desktop notebook application which is downloaded by default in all Microsoft 365 installations. The application is available to run the file format even if the user does not use it. These malicious spam email pretend to be an invoice, shipping notification (often impersonating DHL), or mechanical drawings. Unlike macros, OneNote allows users to insert attachments into a Notebook which are launched once double clicked. Threat actors leverage this by attaching a malicious VBS attachments that automatically launch the script when double-clicked to install malware such as Remote Access Trojan (RAT) to steal sensitive information. However, in OneNote the attachment looks like a file icon but instead attackers overlay it with a 'Double click to view file' bar to hide the VBS attachments. OneNote prompts a user with a warning before launching any attachment.

REMEDIATION STEPS

- Educate users on social engineering and the dangers of phishing attacks, how to spot them, and what to do if they receive a suspicious email in your organisation.

REFERENCES & RESOURCES

Bleeping Computers https://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/