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

CYBER GUIDANCE ISSUE 0299

ONENOTE TO BLOCK DANGEROUS FILE EXTENSIONS

DATE ISSUED: 3rd April 2023

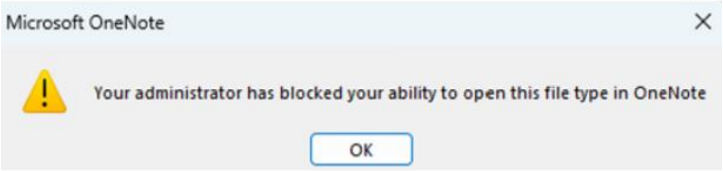
IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Threat actors continue to leverage OneNote documents by embedding malicious ISO and ZIP files to drop malware and disguising them with design elements in numerous ongoing phishing campaigns. Microsoft has responded with steps announced to harden the OneNote application.

BREAKDOWN

Since mid-December 2022, threat actors have been spreading malware using OneNote attachments in phishing emails, infecting victims using remote access malware that can be used to install additional malware, steal passwords, and cryptocurrency wallet information. Previously, OneNote cautioned users that opening attachments could harm their data but still allowed them to open embedded files labelled as dangerous. However, with the new changes, OneNote will block users from directly opening an embedded file with a dangerous extension and show them the following dialog box.



Microsoft will be blocking 120 high-risk file extensions from OneNote. This change is planned to begin rolling out with Version 2304 in April 2023. However, it will not be available in OneNote on the web, OneNote for Windows 10, OneNote on a Mac, or OneNote on Android or iOS devices.

REMEDIATION STEPS

- Block unnecessary file extensions by activating the 'Block additional file extensions for OLE embedding' policy under User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Security Settings and select the extensions you want to be blocked.
- Restrict the launch of OneNote-embedded file attachments through Microsoft Office group policies.
- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/microsoft-onenote-will-block-120-dangerous-file-extensions/

Microsoft https://learn.microsoft.com/en-us/deployoffice/security/onenote-extension-block