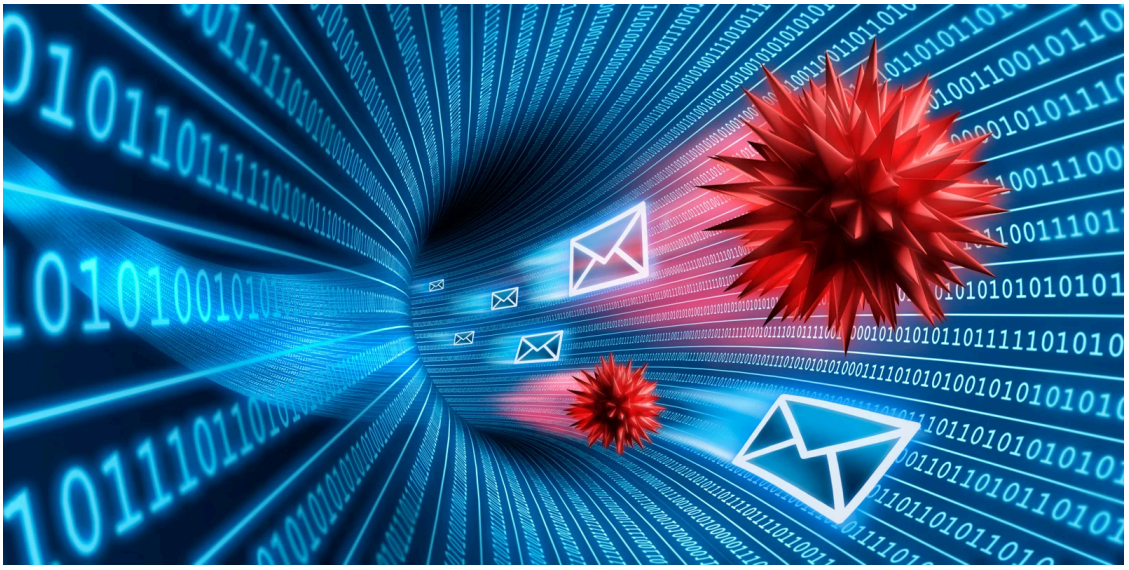
Emotet malware now distributed in Microsoft OneNote files to evade defenses

By Lawrence Abrams

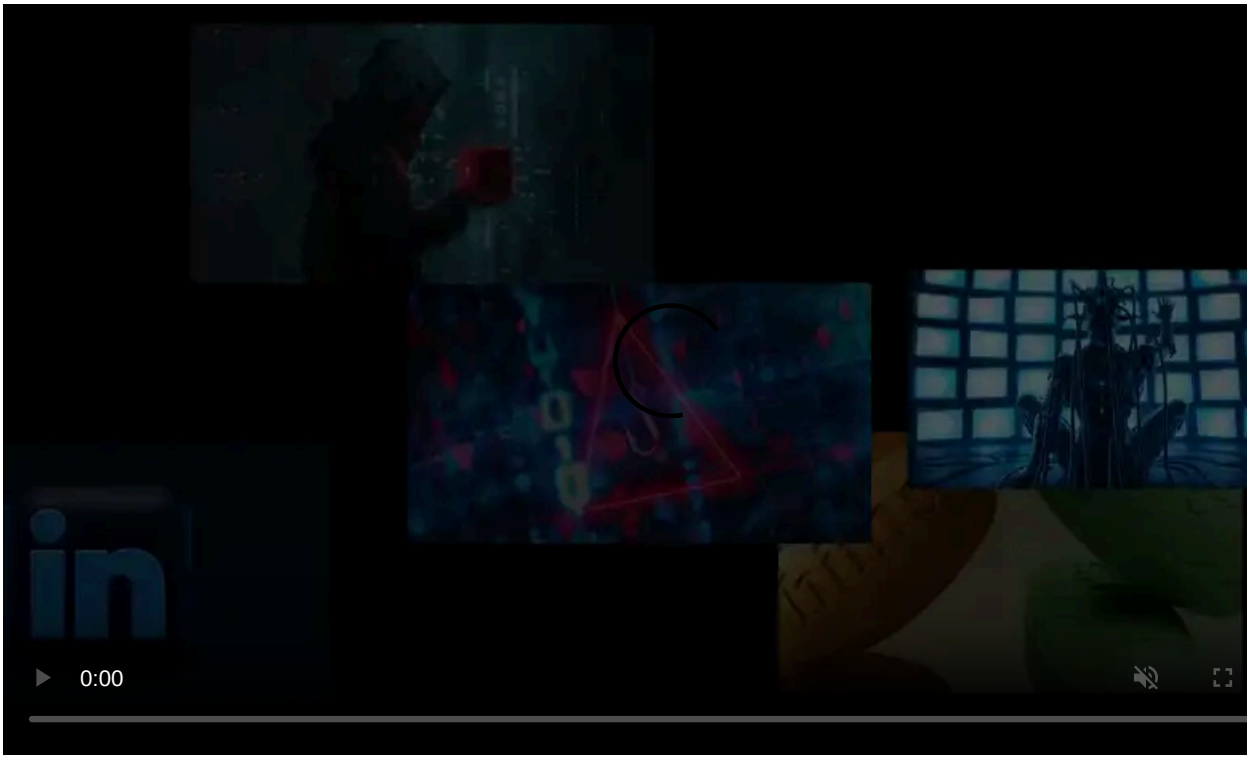
Published: 2023-03-18 · Archived: 2026-04-05 15:24:18 UTC

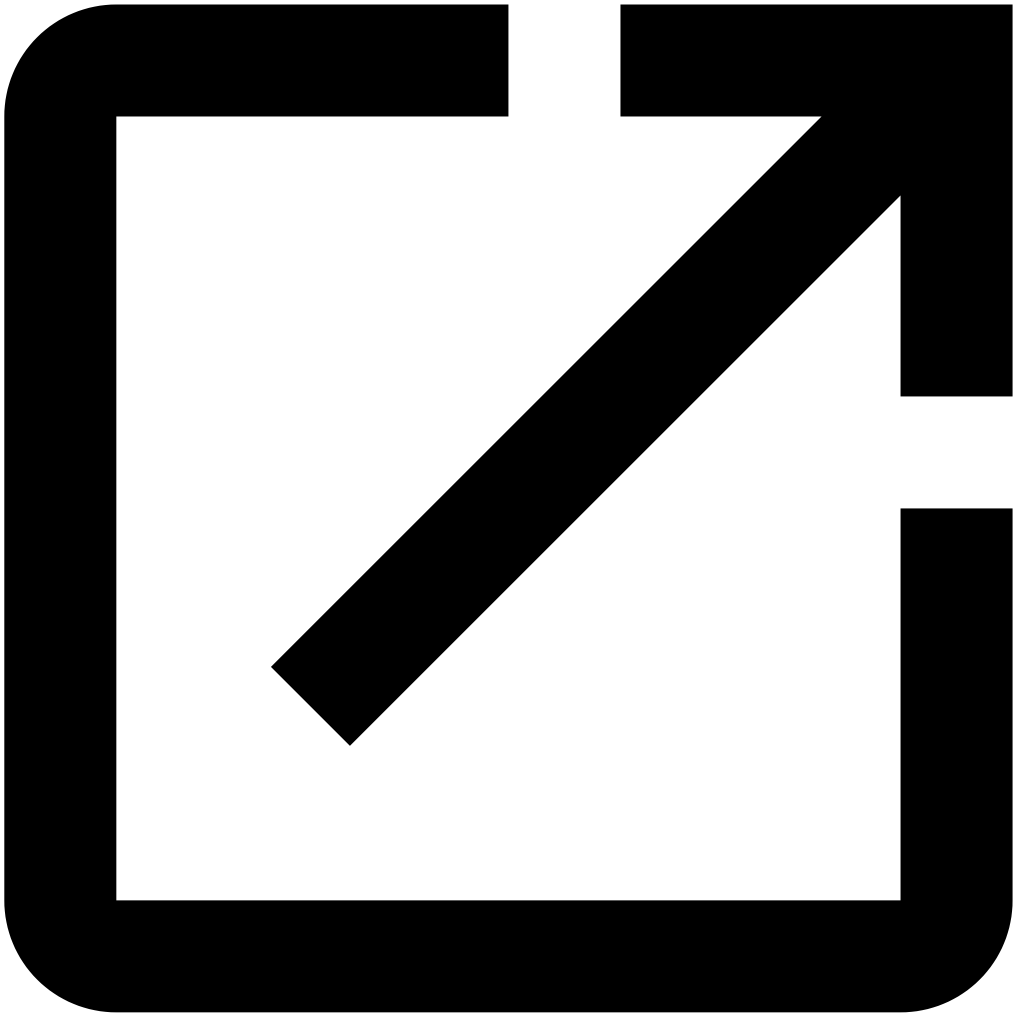


The Emotet malware is now distributed using Microsoft OneNote email attachments, aiming to bypass Microsoft security restrictions and infect more targets.

Emotet is a notorious malware botnet historically distributed through Microsoft Word and Excel attachments that contain malicious macros. If a user opens the attachment and enables macros, a DLL will be downloaded and executed that installs the Emotet malware on the device.

Once loaded, the malware will steal email contacts and email content for use in future spam campaigns. It will also download other payloads that provide initial access to the corporate network.


0:00

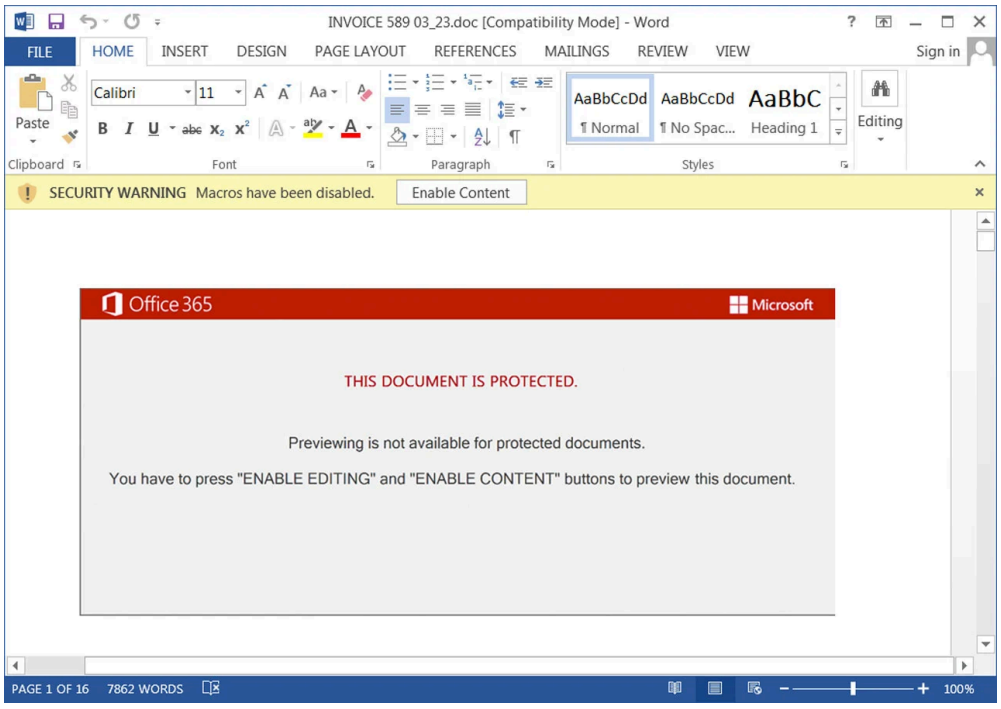


This access is used to conduct cyberattacks against the company, which could include ransomware attacks, data theft, cyber espionage, and extortion.

While Emotet was one of the most distributed malware in the past, over the past year, it would stop and start in spurts, ultimately taking a break towards the end of 2022.

After three months of inactivity, the Emotet botnet suddenly turned back on, spewing malicious emails worldwide earlier this month.

However, this initial campaign was flawed as it continued to use Word and Excel documents with macros. As Microsoft now automatically blocks macros in downloaded Word and Excel documents, including those attached to emails, this campaign would only infect a few people.



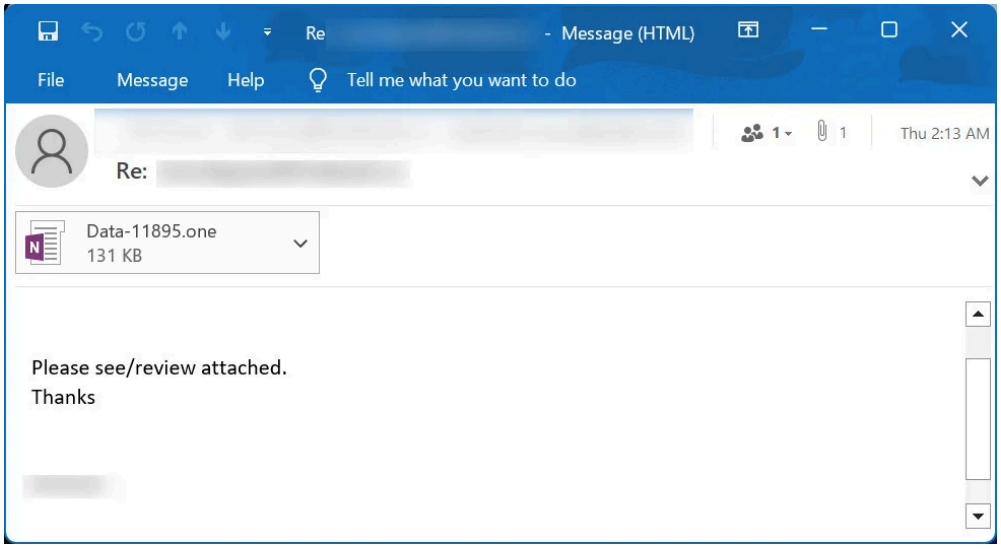
Malicious Emotet Word document used earlier this month
Source: BleepingComputer

Due to this, BleepingComputer predicted that Emotet would switch to Microsoft OneNote files, which have become a popular method for distributing malware after Microsoft began blocking macros.

Emotet switches to Microsoft OneNote

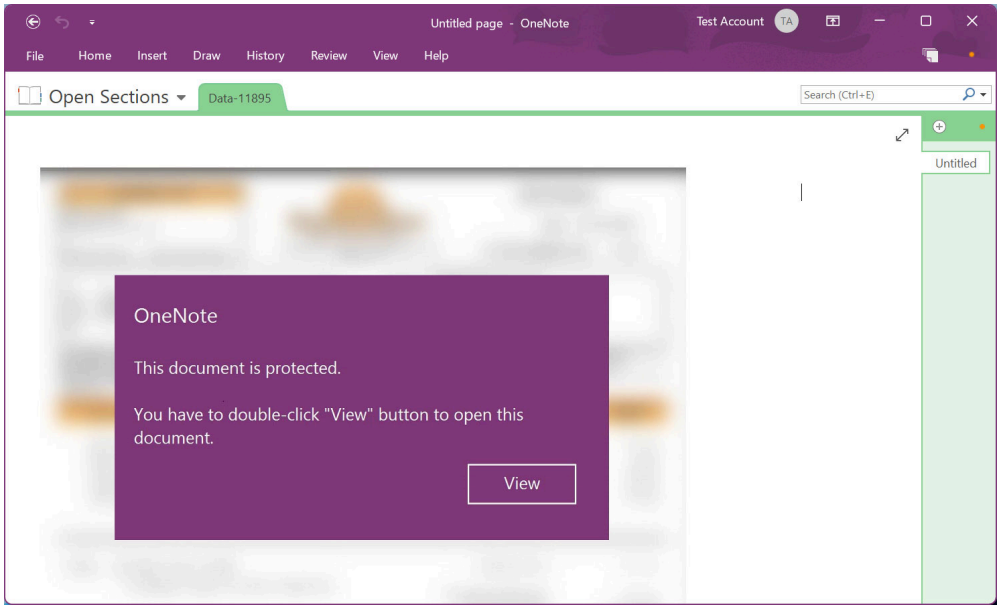
As predicted, in an Emotet spam campaign first spotted by security researcher abel, the threat actors have now begun distributing the Emotet malware using malicious Microsoft OneNote attachments.

These attachments are distributed in reply-chain emails that impersonate guides, how-tos, invoices, job references, and more.



Emotet spam email
Source: BleepingComputer

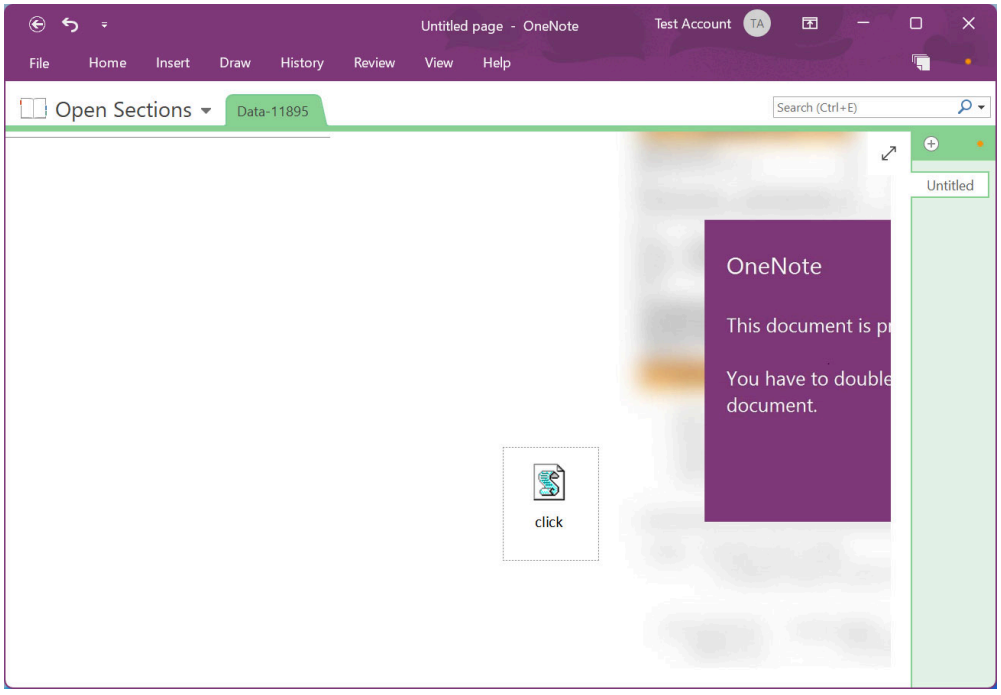
Attached to the email are Microsoft OneNote documents that display a message stating that the document is protected. It then prompts you to double-click the 'View' button to display the document properly.



Malicious Microsoft OneNote attachment
Source: BleepingComputer

Microsoft OneNote allows you to create documents that contain design elements that overlay an embedded document. However, when you double-click on the location where the embedded file is located, even if there is a design element over it, the file will be launched.

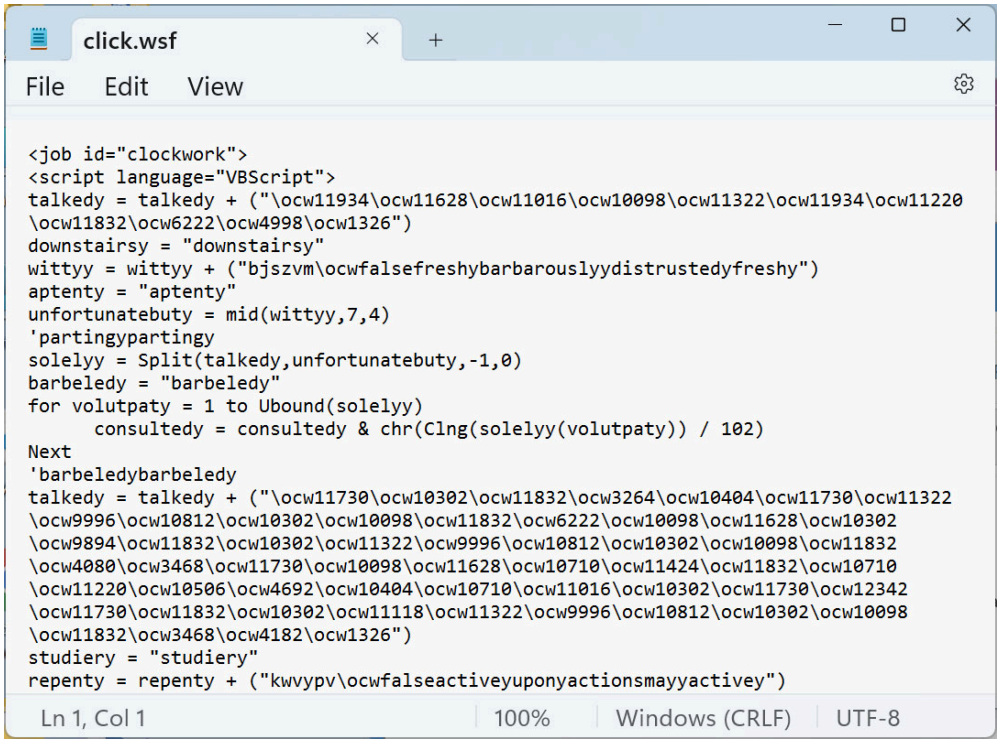
In this Emotet malware campaign, the threat actors have hidden a malicious VBScript file called 'click.wsf' underneath the "View" button, as shown below.



Hidden click.wsf file in the Microsoft OneNote document

Source: BleepingComputer

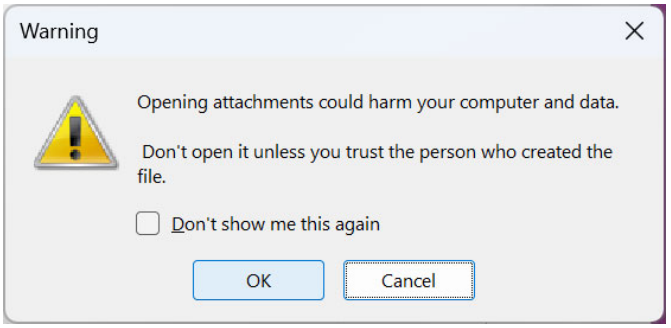
This VBScript contains a heavily obfuscated script that downloads a DLL from a remote, likely compromised, website and then executes it.



Malicious click.wsf VBScript file

Source: BleepingComputer

While Microsoft OneNote will display a warning when a user attempts to launch an embedded file in OneNote, history has shown us that many users commonly click 'OK' buttons to get rid of the alert.



Warning when opening a file embedded in Microsoft OneNote

Source: BleepingComputer

If the user clicks on the OK button, the embedded click.wsf VBScript file will be executed using WScript.exe from OneNote's Temp folder, which will likely be different for each user:

```
"%Temp%\OneNote\16.0\Exported\{E2124F1B-FFEA-4F6E-AD1C-F70780DF3667}\NT\0\click.wsf"
```

The script will then download the Emotet malware as a DLL [VirusTotal] and store it in the same Temp folder. It will then launch the random named DLL using regsvr32.exe.

Emotet will now quietly run on the device, stealing email, contacts, and awaiting further commands from the command and control server.

While it is not known what payloads this campaign ultimately drops, it commonly leads to Cobalt Strike or other malware being installed.

These payloads allow threat actors working with Emotet to gain access to the device and use it as a springboard to spread further in the network.

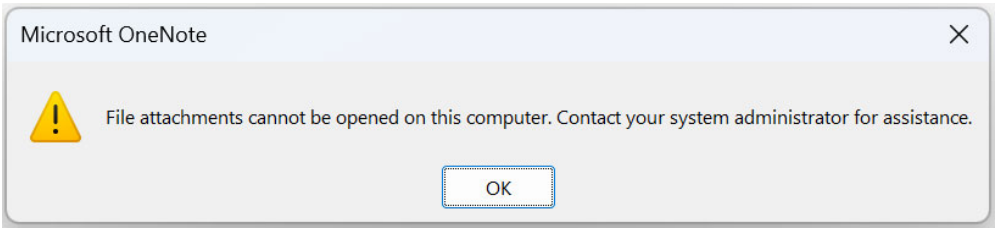
Blocking malicious Microsoft OneNote documents

Microsoft OneNote has become a massive malware distribution problem, with multiple malware campaigns using these attachments.

Due to this, Microsoft will be adding improved protections in OneNote against phishing documents, but there is no specific timeline for when this will be available to everyone.

However, Windows admins can configure group policies to protect against malicious Microsoft OneNote files.

Admins can use these group policies to either block embedded files in Microsoft OneNote altogether or allow you to specify specific file extensions that should be blocked from running.

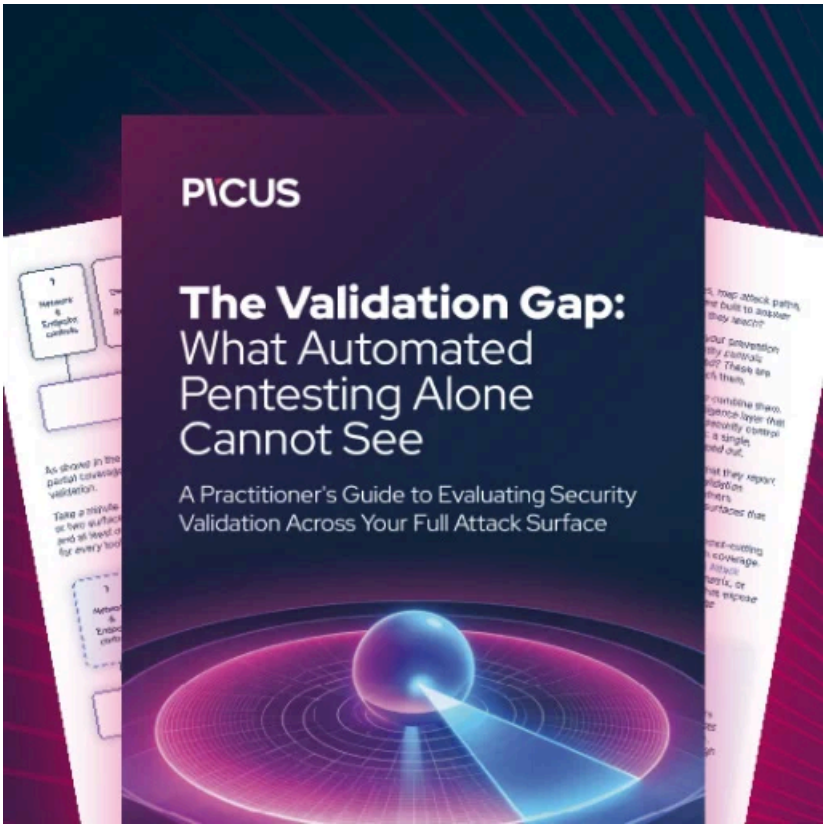


All file attachments are blocked in Microsoft OneNote

Source: BleepingComputer

You can read more about the available group policies in a dedicated article BleepingComputer wrote earlier this month.

It is strongly suggested that Windows admins utilize one of these options until Microsoft adds further protections to OneNote.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/emotet-malware-now-distributed-in-microsoft-onenote-files-to-evade-defenses/