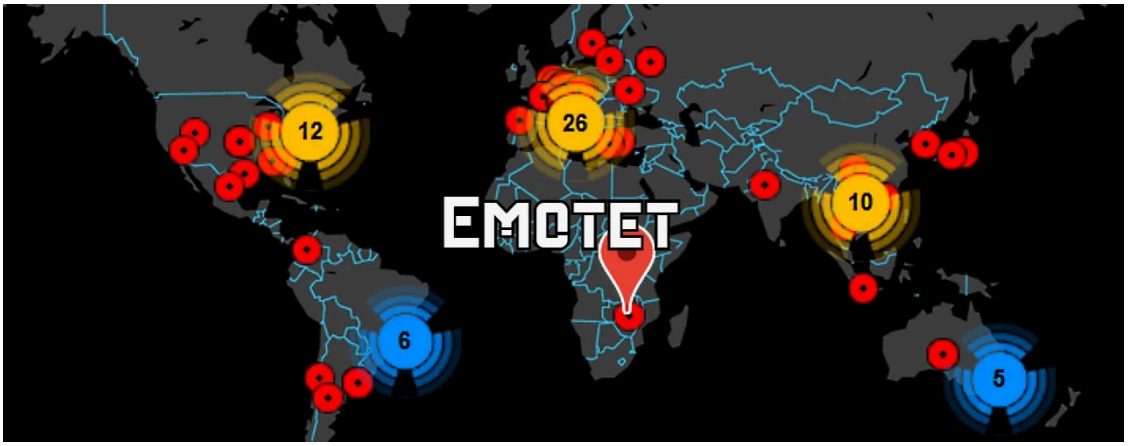
Emotet malware now wants you to upgrade Microsoft Word

By Lawrence Abrams

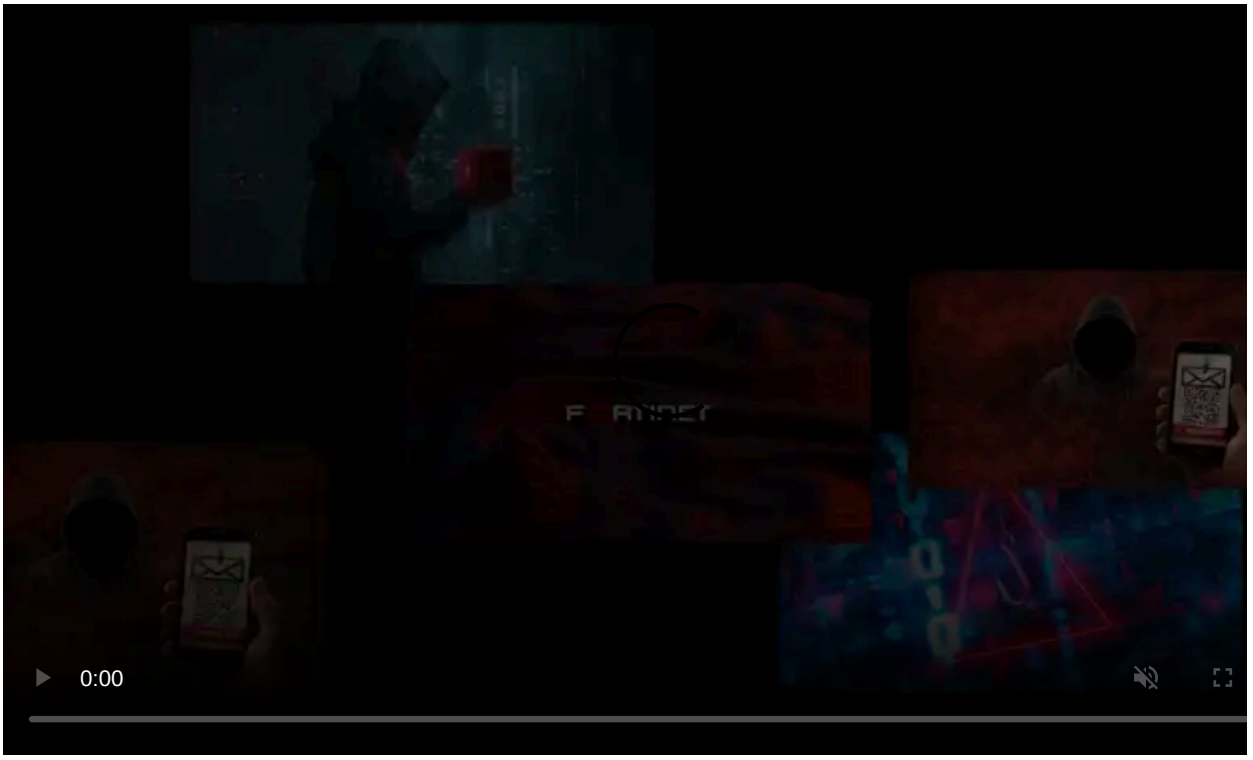
Published: 2020-10-24 · Archived: 2026-04-06 00:14:21 UTC

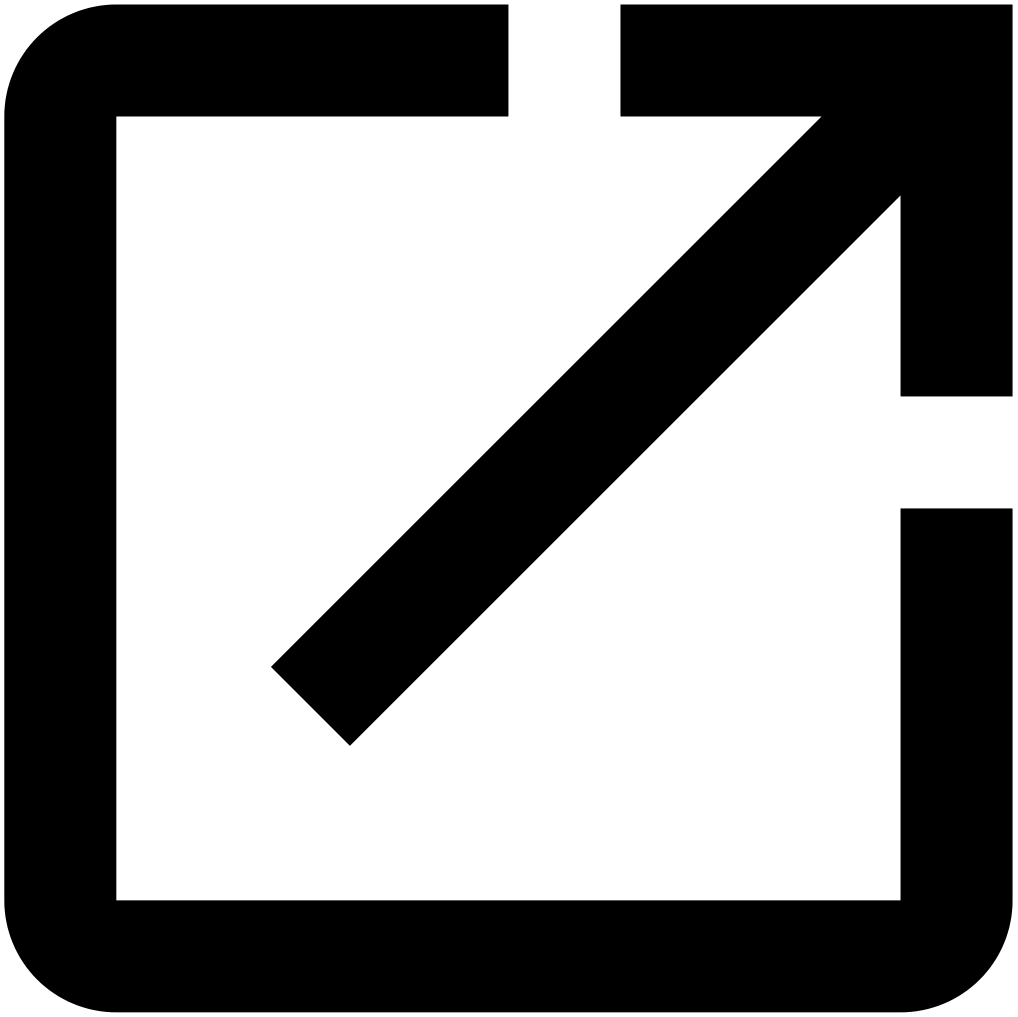


Emotet switched to a new template this week that pretends to be a Microsoft Office message stating that Microsoft Word needs to be updated to add a new feature.

Emotet is a malware infection that spreads through emails containing Word documents with malicious macros. When opening these documents, their contents will try to trick the user into enabling macros so that the Emotet malware will be downloaded and installed on the computer.

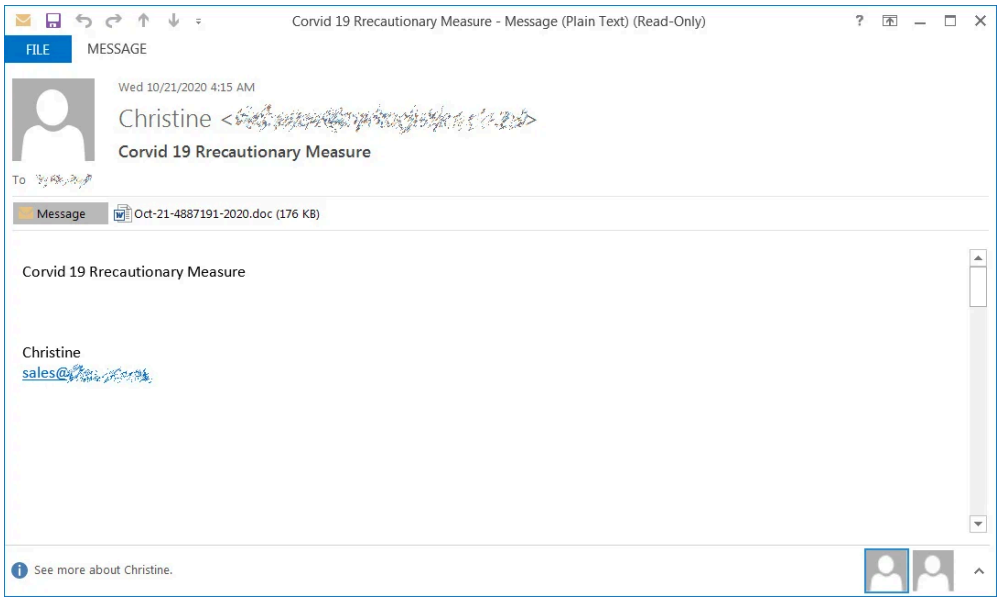
Once the malware is installed, Emotet will use the computer to send spam emails and ultimately install other malware that could lead to a ransomware attack on the victim's network.


0:00



New malicious document template

Emotet spam campaigns use a variety of lures to trick recipients into open an attachment, such as pretending to be invoices, shipping notices, resumes, or purchase orders, or even COVID-19 information, as shown below.



Example Emotet spam email

Attached to these spam emails are malicious Word (.doc) attachments or links to download one.

When opened, these attachments will prompt a user to 'Enable Content' so that malicious macros will run to install the Emotet malware on a victim's computer.

To trick users into enabling the macros, Emotet uses various designs, or document templates, that displays a warning to the user.

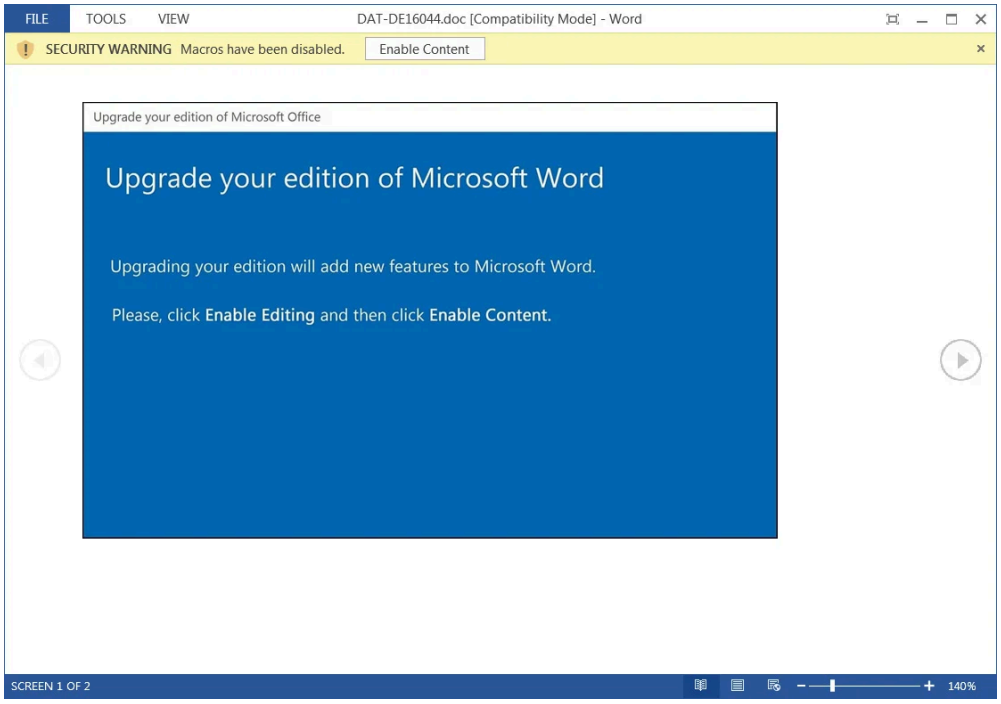
Emotet switched to a new template this week that pretends to be a Microsoft Office message stating that Microsoft Word needs to be updated to add a new feature.

Upgrade your edition of Microsoft Word

Upgrading your edition will add new feature to Microsoft Word.

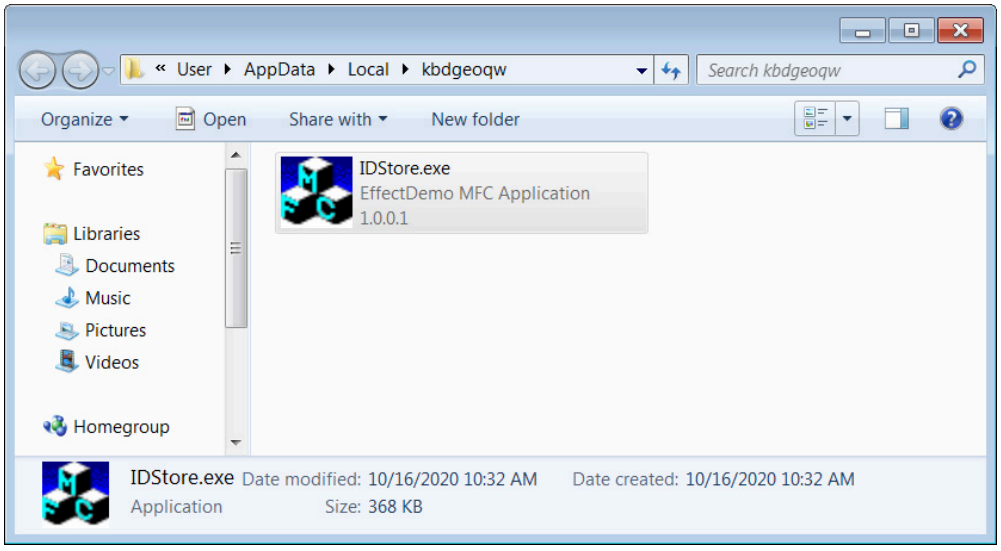
Please click **Enable Editing** and then click **Enable Content**.

To upgrade Microsoft Word, the document tells the user to click on the Enable Editing and then the Enable Content button, which will cause cause the malicious macros to execute.



New Upgrade Microsoft Word Emotet attachment

These malicious macros will download and install the Emotet malware into the victim's %LocalAppData% folder, as shown below.



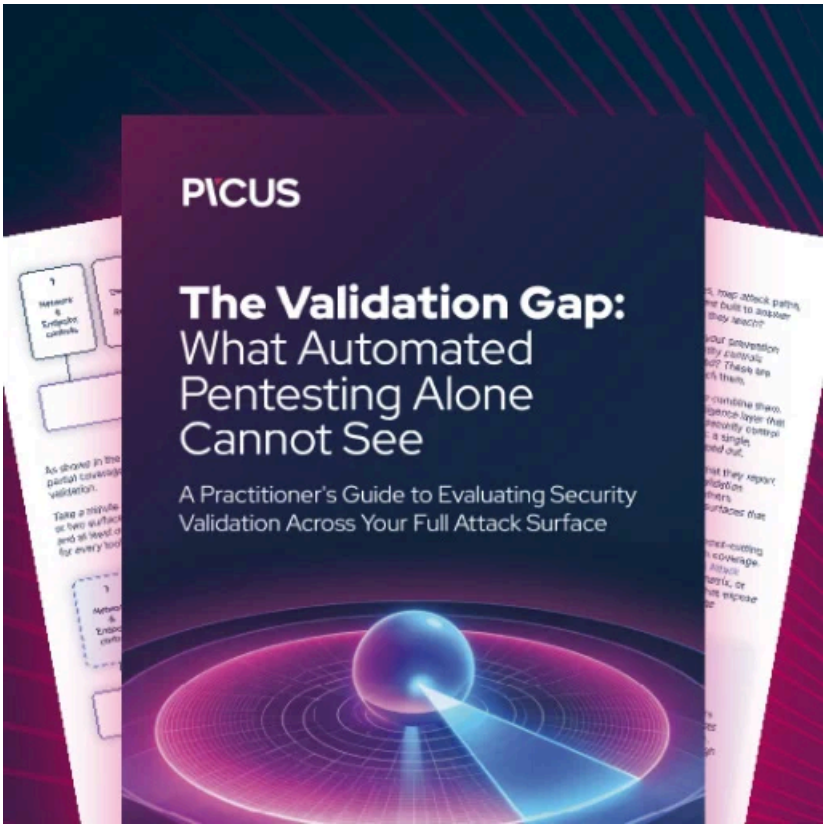
Emotet malware installed in Windows

Why it's necessary to recognize Emotet attachments?

Emotet is considered the most widely spread malware targeting users today. It is particularly dangerous as it installs other infections such as the Trickbot and QBot malware onto a victim's computer.

When installed, TrickBot and QBot will attempt to steal stored passwords, bank information, and assorted other information, but also commonly lead to Conti (TrickBot) or ProLock (QBot) ransomware attacks.

Due to this, it is important that all email users recognize malicious document templates used by Emotet so that you do not accidentally become infected.



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-wants-you-to-upgrade-microsoft-word/