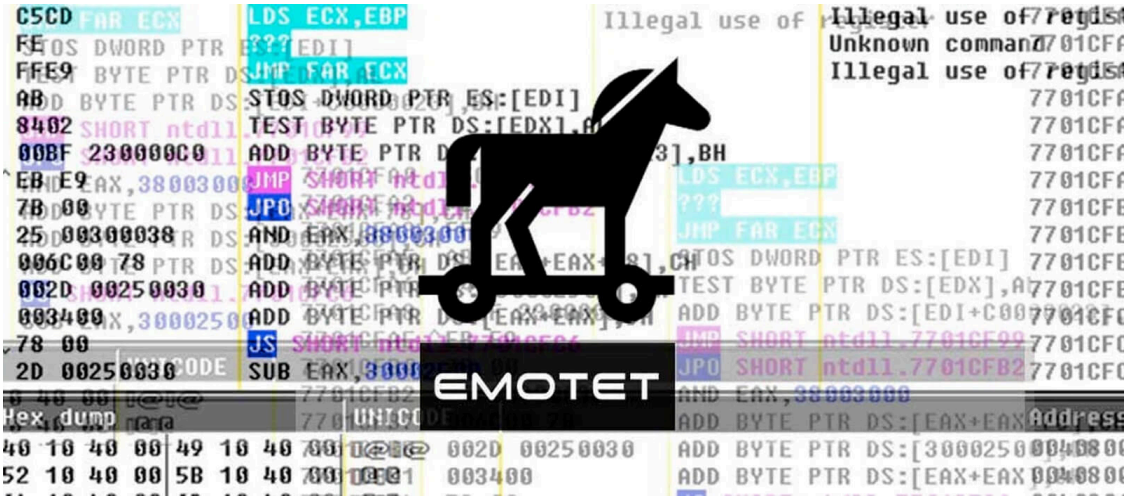
Epic Fail: Emotet malware uses fake ‘Windows 10 Mobile’ attachments

By Lawrence Abrams

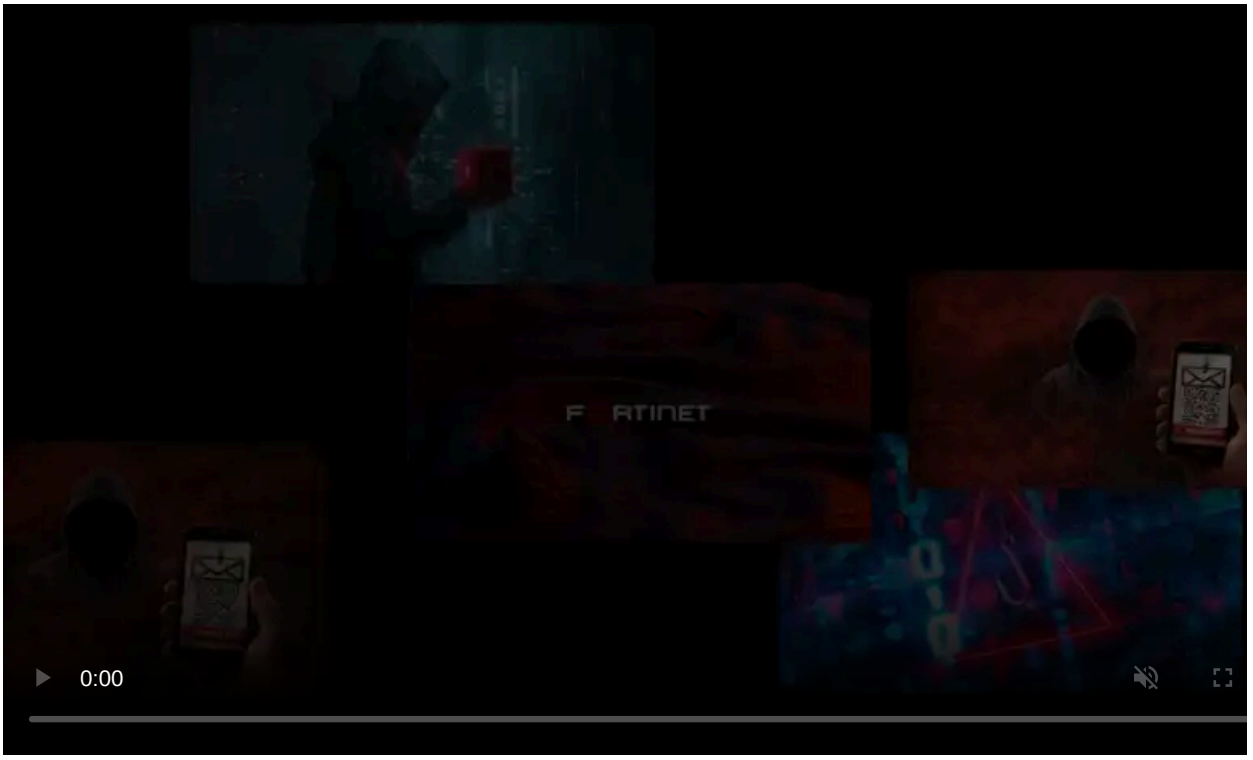
Published: 2020-09-02 · Archived: 2026-04-05 20:28:27 UTC



The Emotet malware is now using malicious email attachment that pretends to be made by Windows 10 Mobile, an operating system that reached the end of life in January 2020.

The Emotet botnet spreads through spam emails that contain malicious Word documents. These Word documents contain malicious macros that will download and install Emotet on a victim's computer when enabled.

Once installed, Emotet will steal a victim's email to use in additional spam campaigns and download and install other malware such as TrickBot and QBot, which commonly lead to network-wide ransomware attacks.

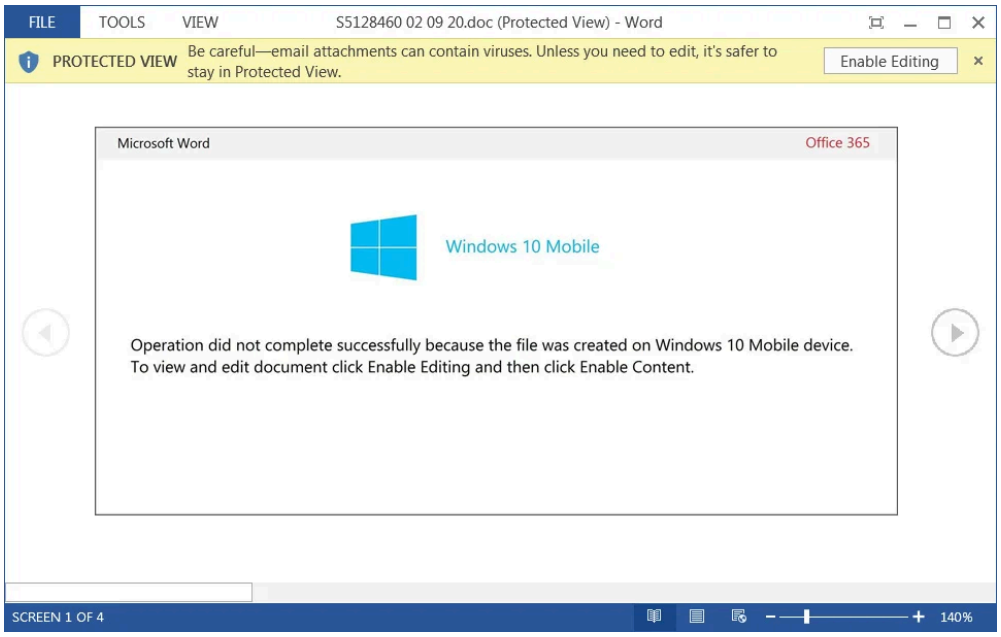

F RTINET
0:00

Tricking a user into enabling Word macros

When a Word document with macros is opened, Microsoft Word will open it in a 'Protected View' that does not allow the macros to execute.

Due to this, the Emotet malware operators create stylized Word documents that are designed to trick the user into clicking on the 'Enable Editing' and 'Enable Content' buttons so that macros will be enabled.

In a recent update to the malicious Word documents, Emotet tracking group Cryptolaemus have discovered that a new document template is being used that pretends to be created on 'Windows 10 Mobile.'



Malicious 'Windows 10 Mobile' Word document

Windows 10 Mobile

Operation did not complete successfully because the file was created on Windows 10 Mobile device.
To view and edit document click Enable Editing and then click Enable Content.

The Windows 10 Mobile operating system was first released in 2015. and due to lack of market share, it reached the end of life in January 2020.

While there are people who continue to use Windows 10 Mobile today, it is not a large user base, and the chances that anyone is sending you documents from a Windows 10 Mobile device is relatively low.

If you receive an email with a Word document stating it was made in Windows 10 Mobile, do not enable editing or content, and immediately trash it.
