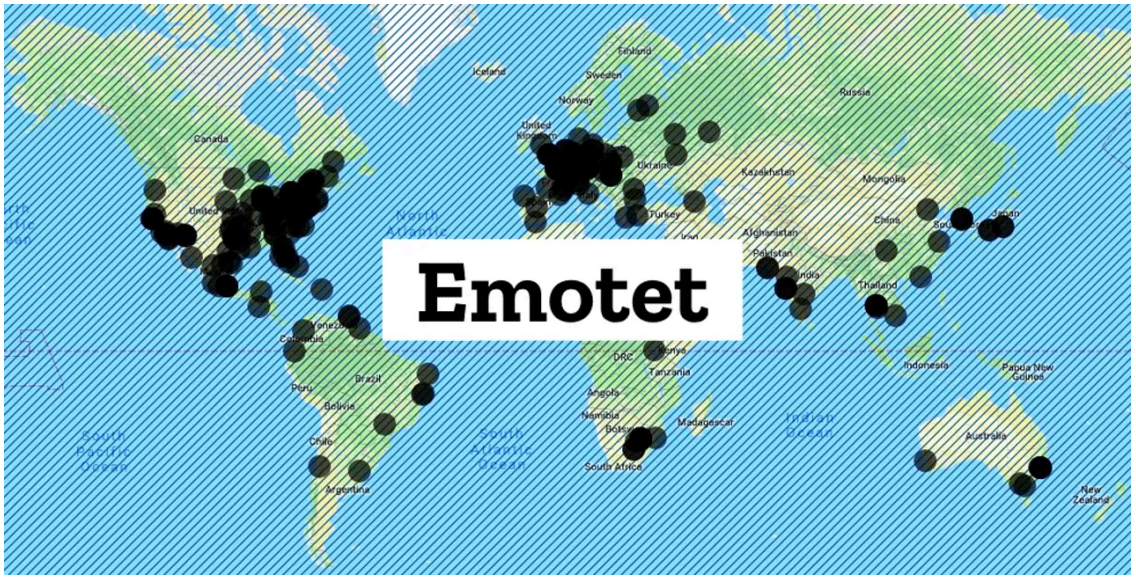
New Emotet attacks use fake Windows Update lures

By Catalin Cimpanu

Published: 2020-10-15 · Archived: 2026-04-05 22:56:31 UTC



In today's cyber-security landscape, the Emotet botnet is one of the largest sources of malspam — a term used to describe emails that deliver malware-laced file attachments.

These malspam campaigns are **absolutely crucial** to Emotet operators.

They are the base that props up the botnet, feeding new victims to the Emotet machine — a Malware-as-a-Service (MaaS) cybercrime operation that's rented to other criminal groups.

To prevent security firms from catching up and marking their emails as "malicious" or "spam," the Emotet group regularly changes how these emails are delivered and how the file attachments look.

Emotet operators change email subject lines, the text in the email body, the file attachment type, but also the content of the file attachment, which is as important as the rest of the email.

That's because users who receive Emotet malspam, besides reading the email and opening the file, they still need to allow the file to execute automated scripts called "macros." Office macros only execute after the user has pressed the "Enable Editing" button that's shown inside an Office file.


enable-editing.png
Image: Microsoft

Tricking users to enable editing is just as important to malware operators as the design of their email templates, their malware, or the botnet's backend infrastructure.

Across the years, Emotet has developed a collection of boobytrapped Office documents that use a wide variety of "lures" to convince users to click the "Enable Editing" button.

This includes:

- Documents claiming they've been compiled on a different platform (i.e., Windows 10 Mobile, Android, or iOS) and the user needs to enable editing for the content to appear.
- Documents claiming they've been compiled in older versions of Office and the user needs to enable editing for the content to appear.
- Documents claiming to be in Protected View and asking the user to enable editing. (Ironically, the Protected View mechanism is the one blocking macros and showing the Enable Editing button/restriction.)
- Documents claiming to contain sensitive or limited-distribution material that's only visible after the user enables editing.
- Documents showing fake activation wizards and claiming that Office activation has been completed and the user only needs to click enable editing to use Office; and many more.

But this week, Emotet arrived from a recent vacation with a new document lure.

File attachments sent in recent Emotet campaigns show a message claiming to be from the Windows Update service, telling users that the Office app needs to be updated. Naturally, this must be done by clicking the Enable Editing button (don't press it).


emotet-windows-update.jpg
Image: @catnap707/Twitter

According to an update from the Cryptolaemus group, since yesterday, these Emotet lures have been spammed in massive numbers to users located all over the world.

Per this report, on some infected hosts, Emotet installed the TrickBot trojan, confirming a ZDNet report from earlier this week that the TrickBot botnet survived a recent takedown attempt from Microsoft and its partners.

These boobytrapped documents are being sent from emails with spoofed identities, appearing to come from acquaintances and business partners.

Furthermore, Emotet often uses a technique called conversation hijacking, through which it steals email threads from infected hosts, inserts itself in the thread with a reply spoofing one of the participants, and adding the boobytrapped Office documents as attachments.

The technique is hard to pick up, especially among users who work with business emails on a daily basis, and that is why Emotet very often manages to infect corporate or government networks on a regular basis.

In these cases, training and awareness is the best way to prevent Emotet attacks. Users who work with emails on a regular basis should be made aware of the danger of enabling macros inside documents, a feature that is very rarely used for legitimate purposes.

Knowing how the typical Emotet lure documents look like is also a good start, as users will be able to dodge the most common Emotet tricks when one of these emails lands in their inboxes, even from a known correspondent.

Below is a list of the most popular Emotet document lures, according to a list shared with ZDNet by security researcher @ps66uk.

emotet-windows-10.png
Image: Cryptolaemus

emotet-ios.png
Image: Sophos

emotet-android.jpg
Image: @pollo290987/Twitter

emotet-openoffice.png
Image: @ps66uk/Twitter

emotet-office.png
Image: Cryptolaemus

emotet-office-rus.jpg
Image: Cryptolaemus

emotet-word.jpg
Image: @JAMESWT_MHT/Twitter

emotet-word-2.png
Image: @ps66uk/Twitter

emotet-word.png
Image: @ps66uk/Twitter

emotet-word-eror.png
Image: @ps66uk/Twitter

emotet-activation-wizard.png
Image: @Myrtus0x0/Twitter

emotet-red-dawn.jpg
Image: Cryptolaemus

emotet-protected.jpg
Image: @catnap707/Twitter

emotet-protected.png
Image: @ps66uk/Twitter

emotet-interruption.png
Image: @ps66uk/Twitter
