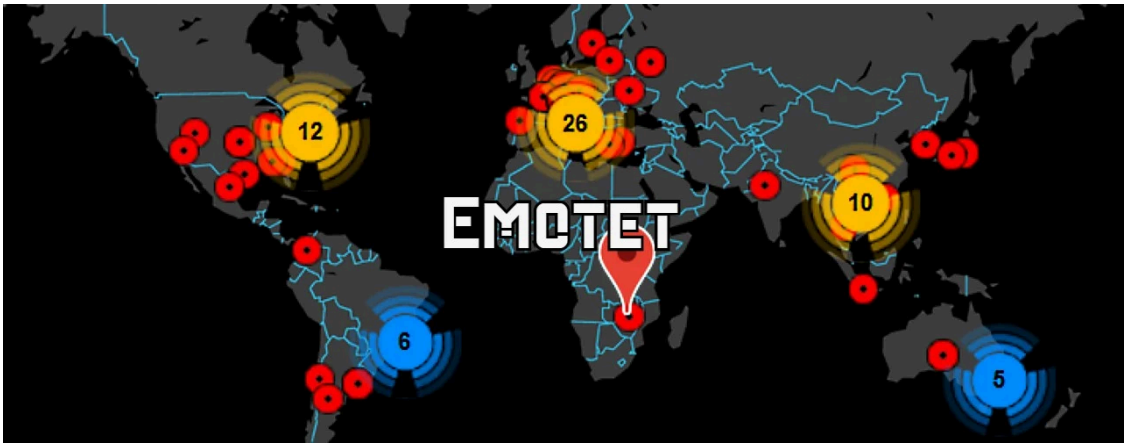
Emotet double blunder: fake ‘Windows 10 Mobile’ and outdated messages

By Ionut Ilascu

Published: 2020-09-22 · Archived: 2026-04-06 02:03:33 UTC

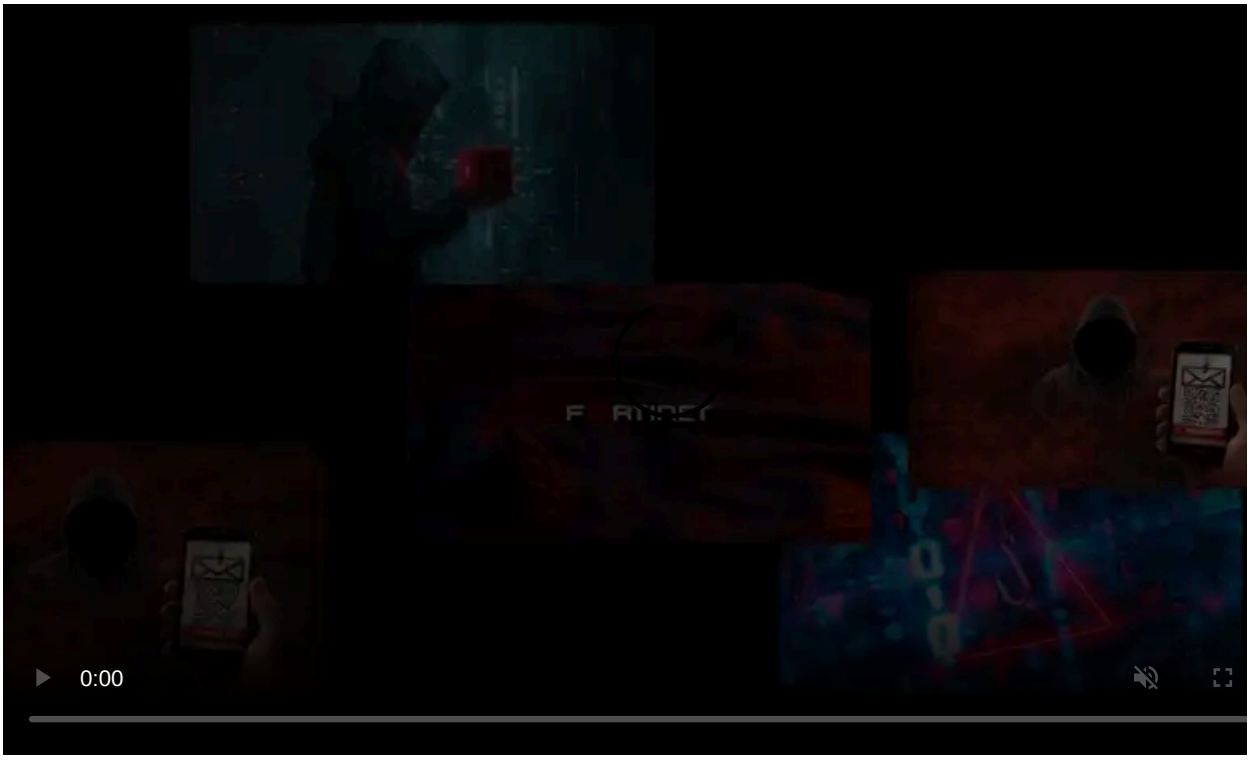


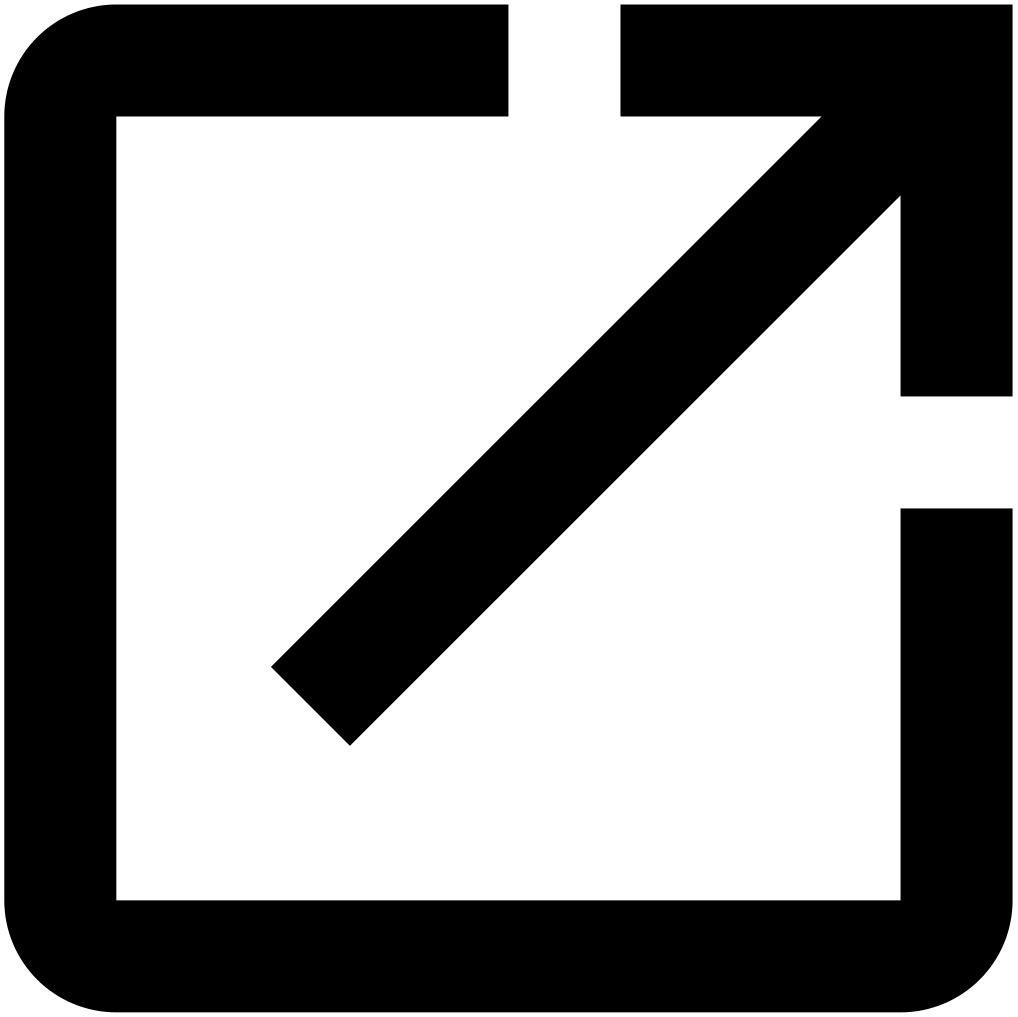
The Emotet botnet has switched up their malicious spamming campaign and is now heavily distributing password-protected archives to bypass email security gateways.

This campaign started on Friday with documents claiming to be created on the expired Windows 10 Mobile and continued with a large volume of messages pretending to be made on Android.

Dumb and dumber

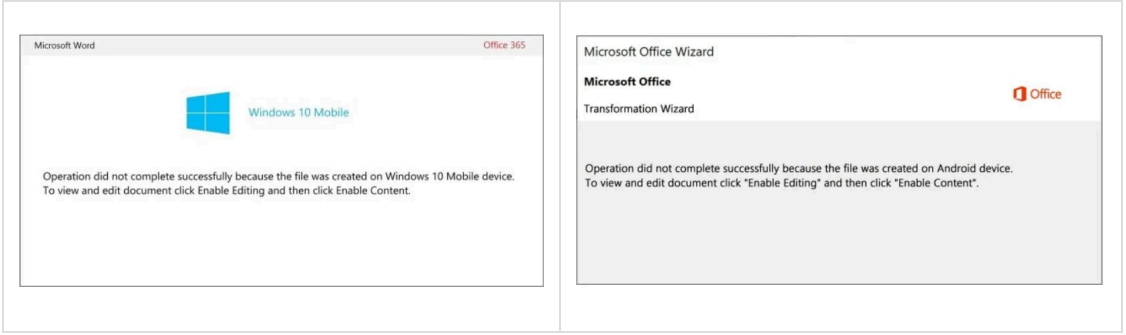
Trying to trick users into enabling macros to see documents created on a different operating system may be a convincing stratagem but using Windows 10 Mobile (since the beginning of the month) is a blunder since the OS reached end of life in January 2020.


0:00



Microsoft says that Emotet switched the ruse on Monday and started to deliver documents claiming to be made on Android and that “Enable Content” (thus activating embedded macro code) needs to be clicked to view the document.

source: Microsoft



Emotet operators blundered again by using outdated text in the email subject and body. This should be a clear tell for recipients, making it easy for them to spot the compromise attempt.

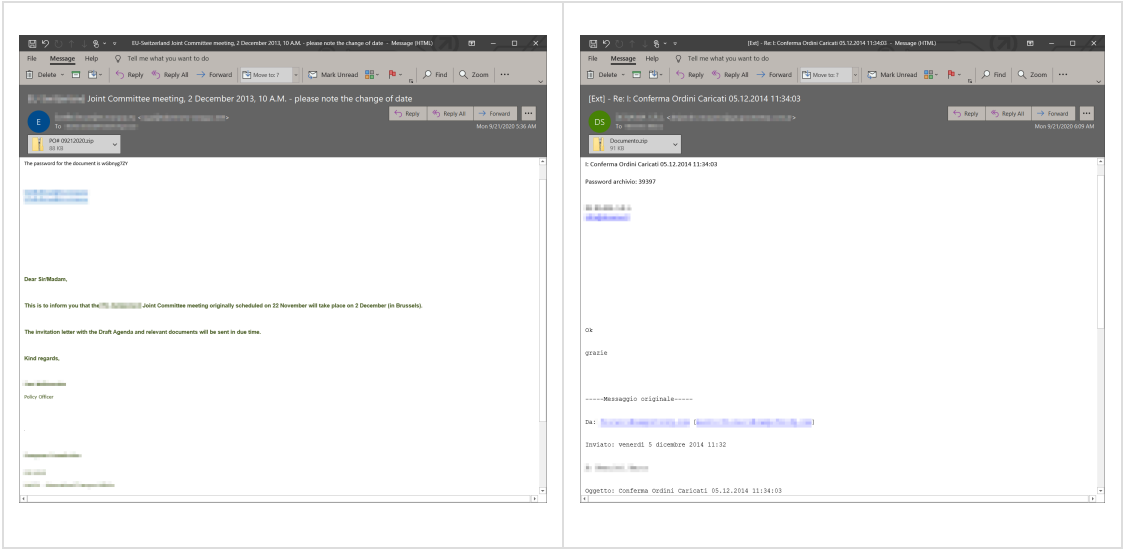
Microsoft announced early today that Emotet targeted various regions of the world with localized emails. Some of the languages used are English, French, and Italian.

The theme varies from invitations to meetings and order confirmations to reports, all of them being compressed into a password-protected archive.

After recipients extracted the attached document using the password provided in the email body and open it, they launch the embedded malicious macro that downloads the Emotet payload (some sources indicate it is QakBot in most cases).

However convincing the messages may be, as seen in the screenshots from Microsoft, they are obsolete, mentioning dates from 2013 and 2014.

source: Microsoft



Operation Zip Lock has been ongoing for weeks

While Microsoft noticed this campaign on Friday, the Cryptolaemus group of researchers fighting Emotet say that this has been happening for so many weeks that they named it Operation Zip Lock.

Emotet has used password-protected in the first half of 2019 (confirmed by Trend Micro) but Cryptolaemus says that this time the distribution is through Epoch 3 - a subgroup of the botnet with separate infrastructure.

The group says that organizations in Japan were targeted this way since at least September 1 and that the method then slowly propagated to Epoch 1 and 2 this month, being used by all three Emotet Epochs starting September 14.

Last week, TrickBot pulled a similar stunt by sending out documents with protected access. They were not archived, though. The lures varied from orders, invoices, documents, and the less and less common "new coronavirus case" theme.

Source: https://www.bleepingcomputer.com/news/security/emotet-double-blunder-fake-windows-10-mobile-and-outdated-messages/