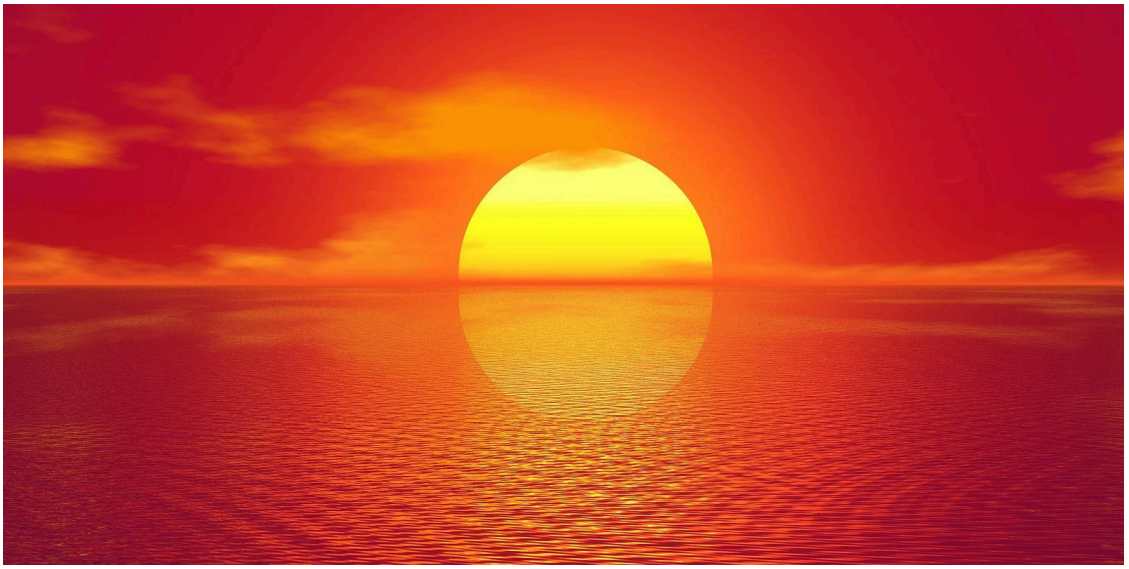
Emotet malware's new 'Red Dawn' attachment is just as dangerous

By Lawrence Abrams

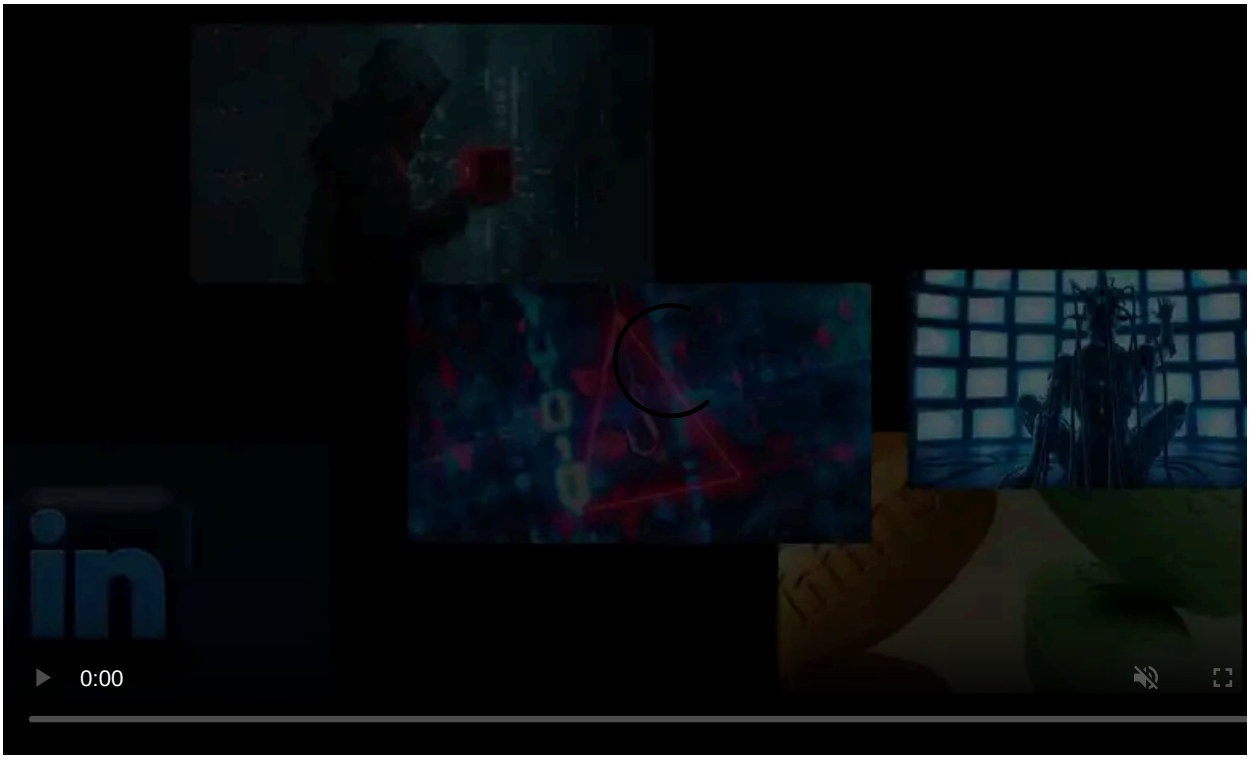
Published: 2020-08-29 · Archived: 2026-04-05 17:13:51 UTC

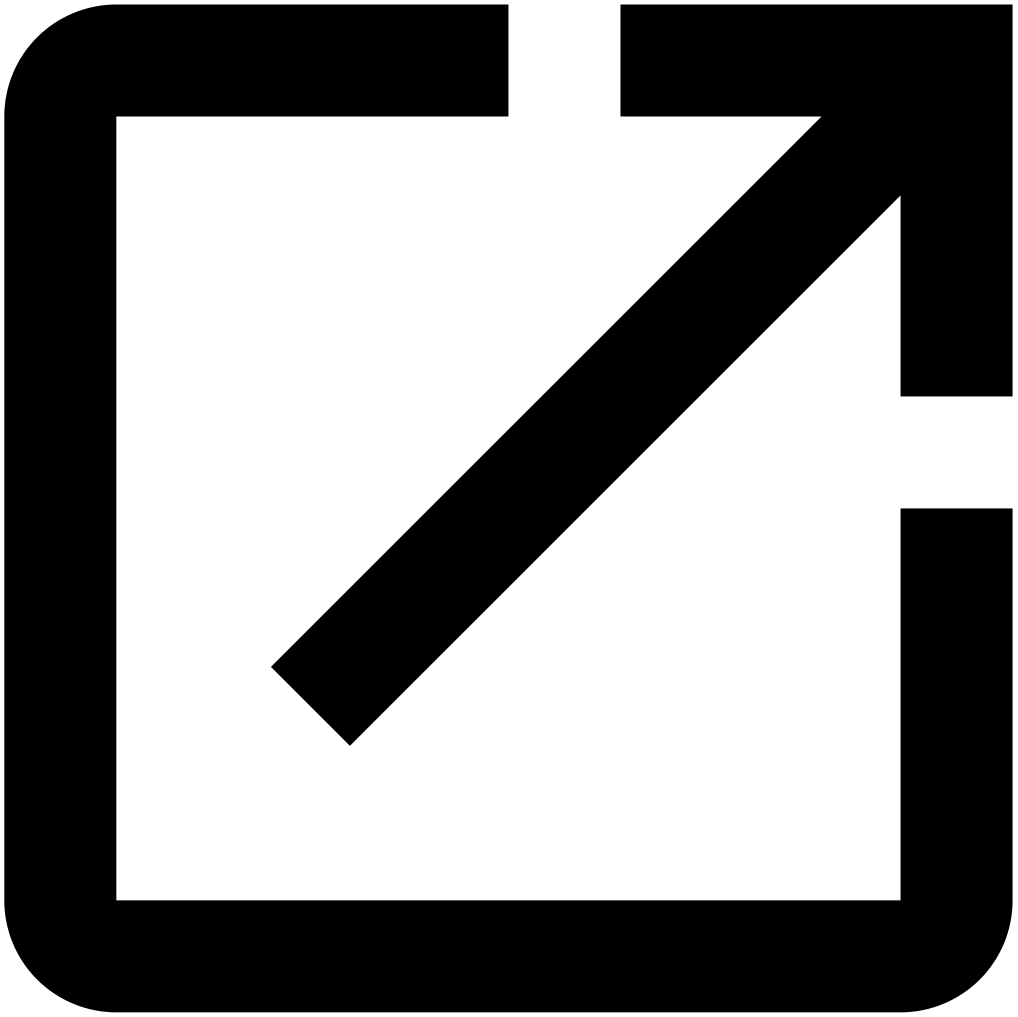


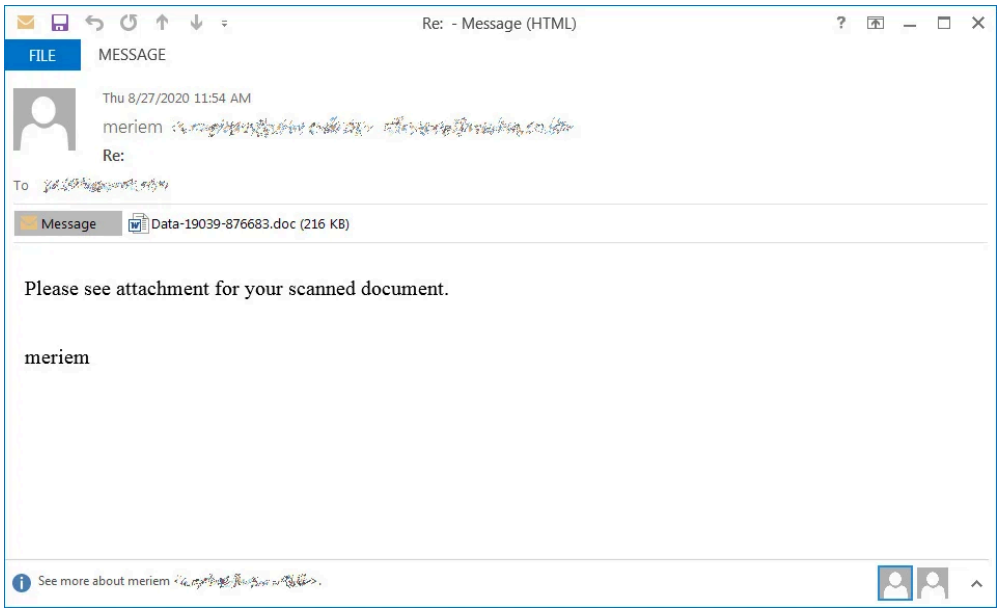
The Emotet botnet has begun to use a new template for their malicious attachments, and it is just as dangerous as ever.

After a five-month "vacation," the Emotet malware returned in July 2020 and began to spew massive amounts of malicious spam worldwide.

These spam campaigns pretend to be invoices, shipping information, COVID-19 information, resumes, financial documents, or scanned documents, as shown below.


0:00



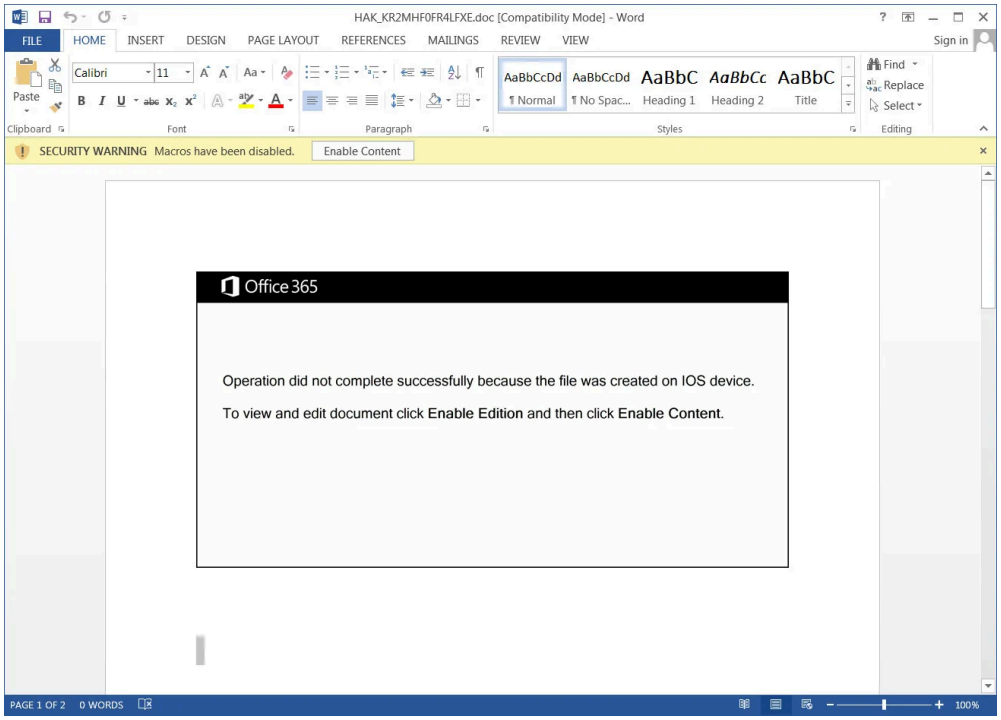


Example Emotet spam email

Attached to these spam emails are malicious Word (.doc) attachments or link 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 a user into enabling the macros, Emotet has been using a document template that tells uses that the document was created on iOS and cannot be properly viewed unless the 'Enable Content' button is clicked.

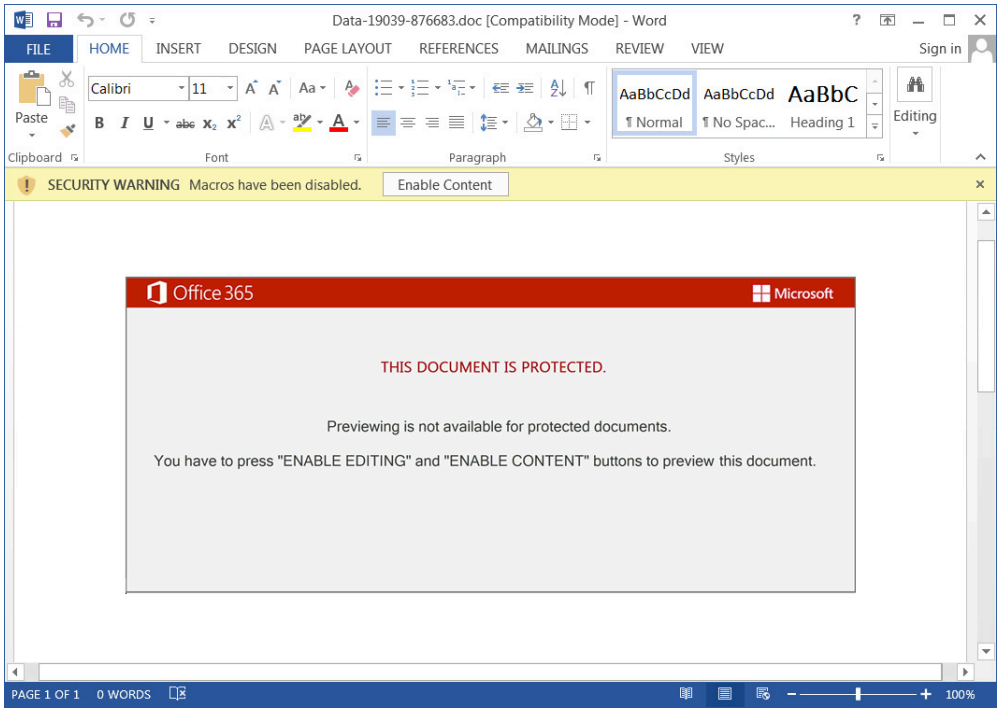


Older Emotet iOS template

On August 25th, the botnet switched to a new template that Emotet expert Joseph Roosen has named 'Red Dawn' due to its red accent colors.

The Red Dawn template also moves away from its iOS theme and now states that "This document is protected" and that previewing is not available.

It then prompts the user to click on 'Enable Editing' and 'Enable Content' to view the document.



New 'Red Dawn' Emotet attachment

Like the previous template, once enable content is clicked, malicious macros will be executed that download and install the Emotet malware on a victim's computer.

Why it's essential to recognize Emotet attachments?

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

While TrickBot and QBot can perform different malicious activities, they both will attempt to steal stored passwords, cookies, banking information, and assorted other information from a victim's computer.

To make matters worse, both trojans are known to provide access to threat actors who install ransomware such as Conti (TrickBot) or ProLock (QBot) throughout the network.

Due to this, it is vital to recognize the malicious document templates used by Emotet so that you do not accidentally become infected.
