Emotet launches major new spam campaign

welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

November 9, 2018

The recent spike in Emotet activity shows that it remains an active threat

ESET Research
9 Nov 2018 - 03:11PM

The recent spike in Emotet activity shows that it remains an active threat

A week after adding a new email content harvesting module, and following a period of low activity, the malicious actors behind Emotet have launched a new, large-scale spam campaign.

What is Emotet?

Emotet is a banking Trojan family notorious for its modular architecture, persistence techniques, and worm-like self-propagation. It is distributed through spam campaigns employing a variety of seemingly legitimate guises for their malicious attachments. The Trojan is often used as a downloader or dropper for potentially more-damaging, secondary payloads. Due to its high destructive potential, Emotet was the subject of a US-CERT security notice in July 2018.

The new campaign

According to our telemetry, the latest Emotet activity was launched on November 5, 2018, following a period of low activity. Figure 1 shows a spike in the Emotet detection rate in the beginning of November 2018, as seen in our telemetry data.

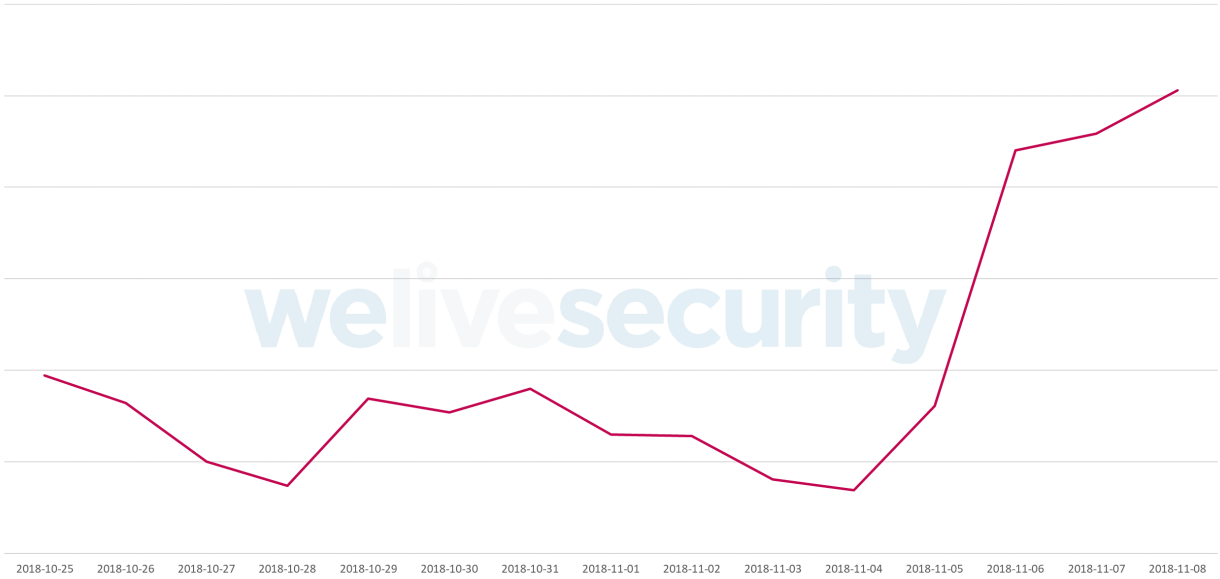

Figure 1 – Overview of ESET product detections of Emotet in the past two weeks

Breaking those detections down by country, as seen in Figure 2, this latest Emotet campaign appears to be most active the Americas, the UK, Turkey and South Africa.

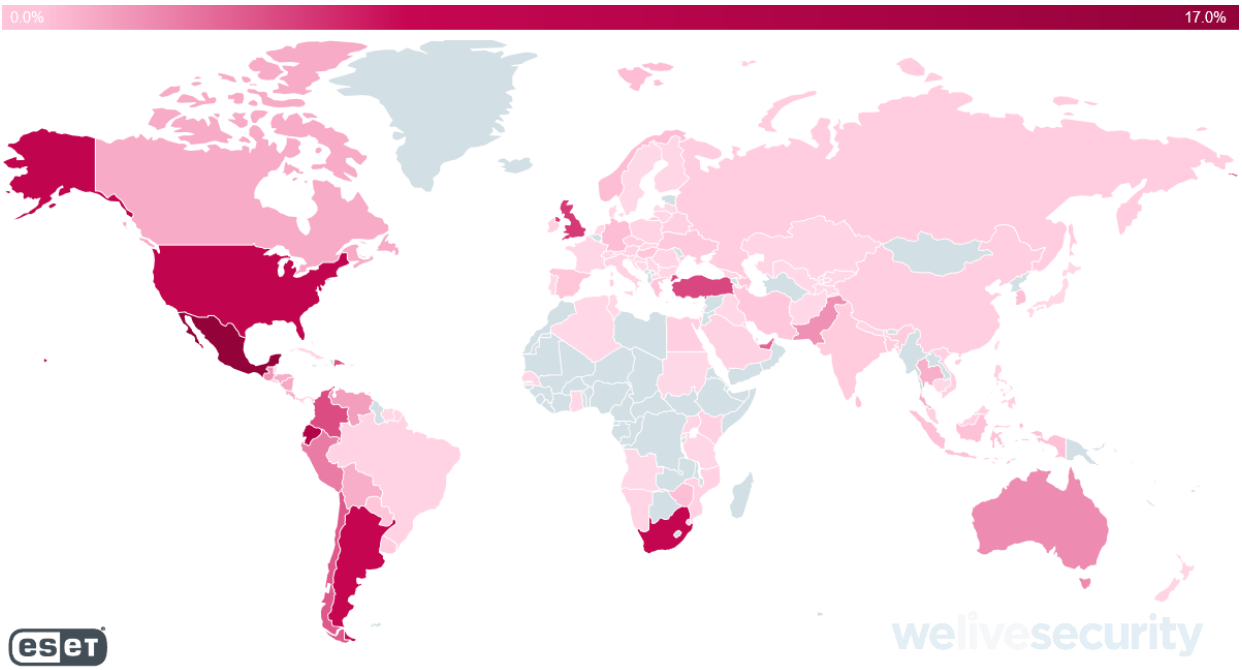

Figure 2 – Distribution of ESET detections of Emotet in November 2018 (including both file and network detections)

In the November 2018 campaign, Emotet makes use of malicious Word and PDF attachments posing as invoices, payment notifications, bank account alerts, etc., seemingly coming from legitimate organizations. Alternately, the emails contain malicious links instead of attachments. The email subjects used in the campaign suggest a targeting of English and German-speaking users. Figure 3 shows Emotet activity in November 2018 from the perspective of document detections. Figures 4, 5 and 6 are example emails and attachments from this campaign.

```
$ diff -W200 -y <(xxd -s 0x13ab08 SCANPASS_QXWEGRFGCVT_323803488900X_jpeg.exe) <(xxd -s 0x13ab08 decrypted)
0013ab08: a571 ffd9 6c69 7665 7219 31ee 7559 7269  .q..liver.1.uYri     |    0013ab08: a571 ffd9 6c69 7665 724d 5a90 0003 0000  .q..liverMZ.....
0013ab18: 2826 2b2f 2ebb a67a 62d1 7e75 4456 6e75  (&+/...zb.~uDVnu     |    0013ab18: 0004 0000 00ff ff00 00b8 0000 0000 0000  ................
0013ab28: 7833 7e75 546b 7e75 5a72 6928 222b 2f2e  x3~uTk~uZri("+/.     |    0013ab28: 0040 0000 0000 0000 0000 0000 0000 0000  .@..............
0013ab38: 4459 7a62 697e 7544 566e 7578 737e 7554  DYzbi~uDVnuxs~uT     |    0013ab38: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0013ab48: 6b7e 755a 72e9 2822 2b21 31fe 577a d660  k~uZr.("+!1.Wz.`     |    0013ab48: 0000 0000 0080 0000 000e 1fba 0e00 b409  ................
0013ab58: b354 fc57 22b8 5927 161c 274b 0e07 3515  .T.W".Y'..'K..5.     |    0013ab58: cd21 b801 4ccd 2154 6869 7320 7072 6f67  .!..L.!This prog
0013ab68: 1b49 4f0b 4c4f 2a37 1516 491c 1064 241b  .IO.LO*7..I..d$.     |    0013ab68: 7261 6d20 6361 6e6e 6f74 2062 6520 7275  ram cannot be ru
0013ab78: 1b58 1a10 5510 242d 5537 1d0d 4d0c 2622  .X..U.$-U7..M.&"     |    0013ab78: 6e20 696e 2044 4f53 206d 6f64 652e 0d0d  n in DOS mode...
```

Figure 3 – Distribution of ESET detections of Emotet-related documents in November 2018

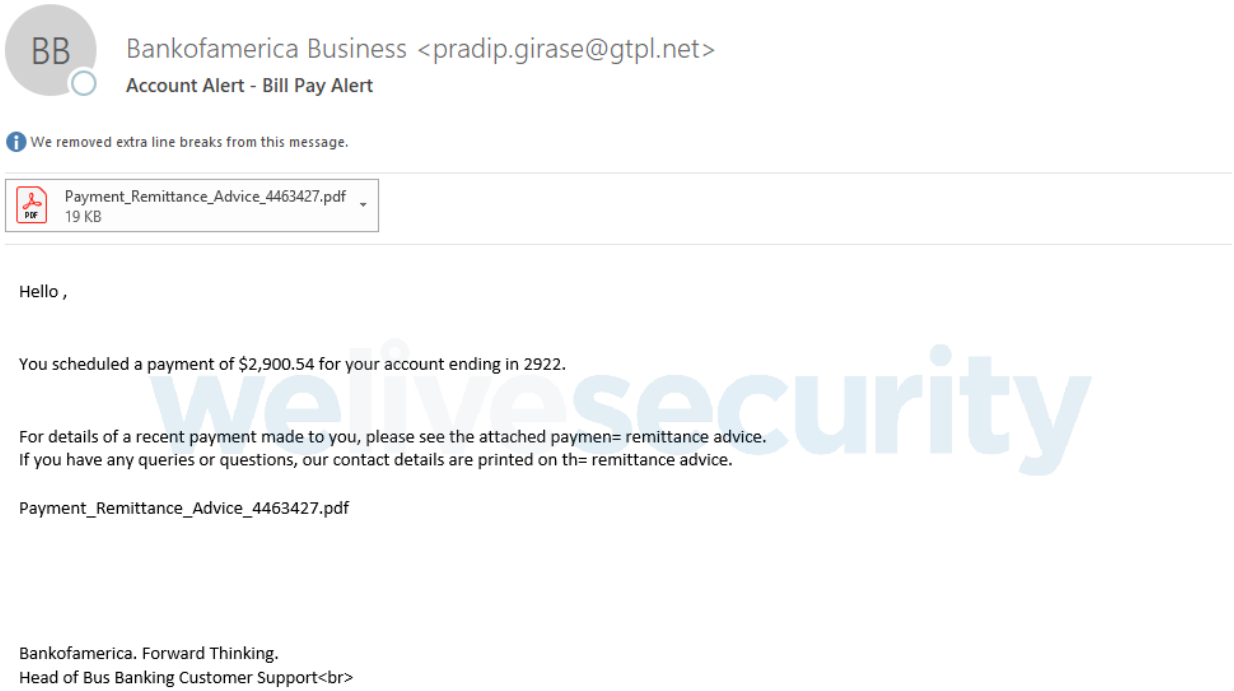

Figure 4 – Example of a spam email used in the latest Emotet campaign

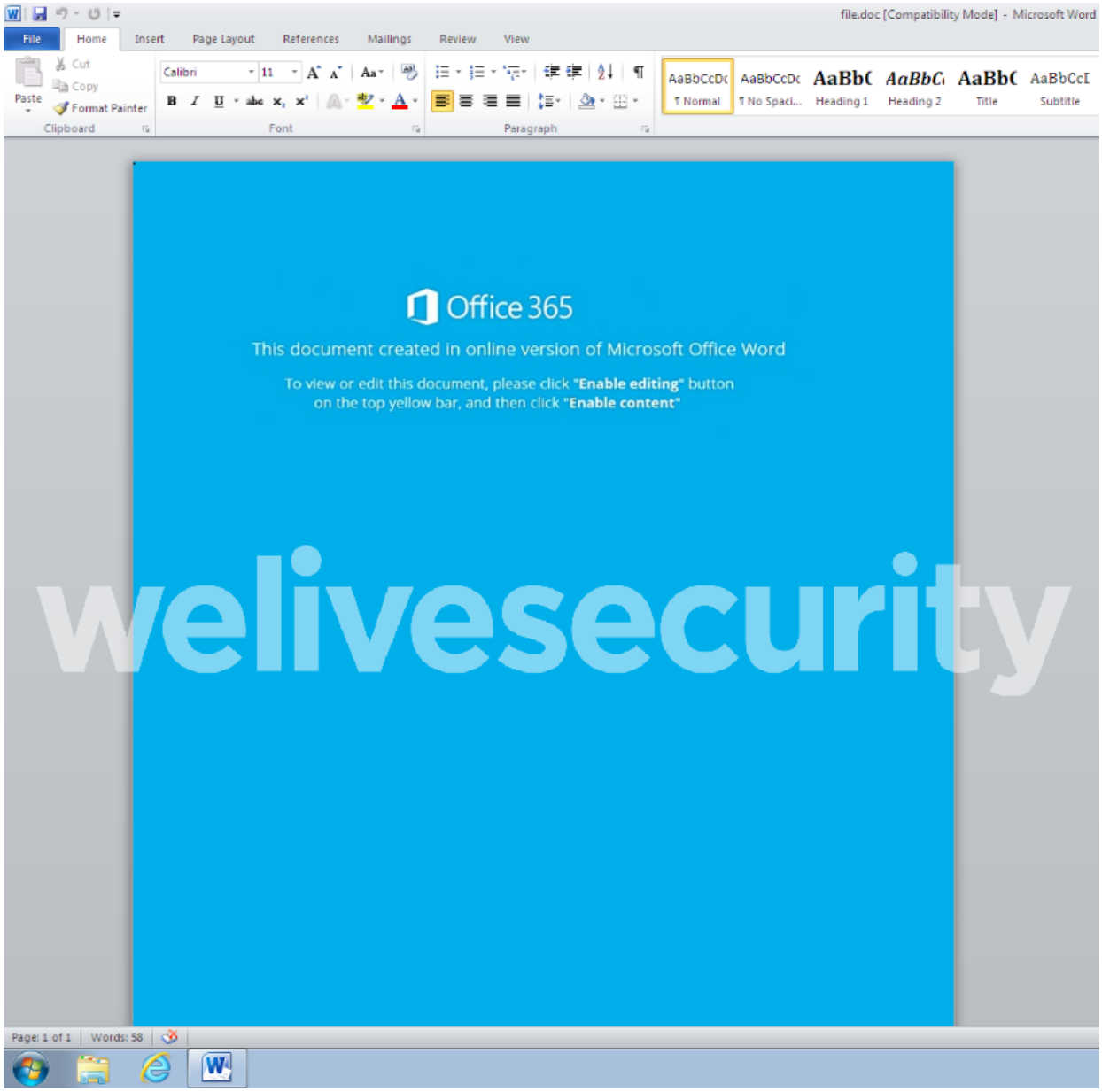

Figure 5 – Example of a malicious Word document used in the latest Emotet campaign

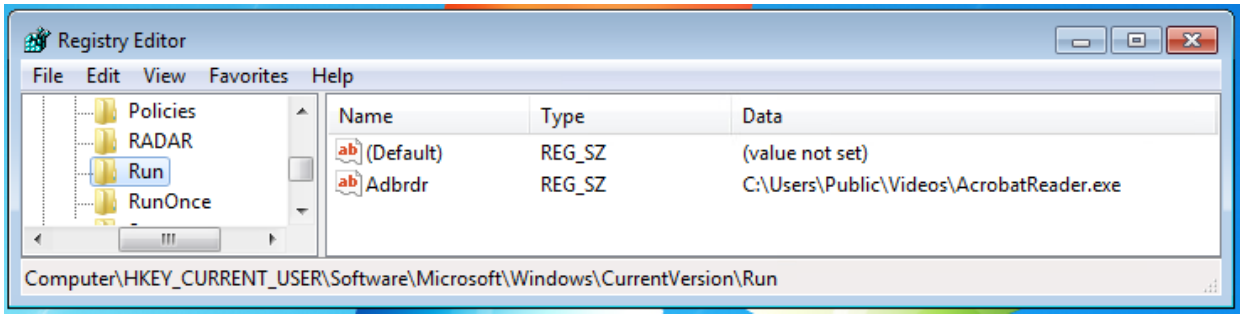

Figure 6 – Example of a malicious PDF used in the latest Emotet campaign

The compromise scenario in this November 2018 campaign starts with the victim opening a malicious Word or PDF file attached to a spam email seemingly coming from a legitimate and familiar organization.

Following the instructions in the document, the victim enables macros in Word or clicks on the link in the PDF. The Emotet payload is subsequently installed and launched, establishes persistence on the computer and reports the successful compromise to its C&C server. In turn, it receives instructions on which attack modules and secondary payloads to download.

The modules extend the initial payload's functionality with one or more of credential-stealing, network propagation, sensitive information harvesting, port forwarding, and other capabilities. As for the secondary payloads, this campaign has seen Emotet dropping TrickBot and IcedId on compromised machines.

Conclusion

This recent spike in Emotet activity just goes to show that Emotet continues to be an active threat – and an increasingly worrying one due to the recent module updates. ESET systems detect and block all Emotet components under detection names listed in the IoCs section.

Indicators of Compromise (IoCs)

Example hashes

Note that new builds of Emotet binaries are released approximately every two hours, so hashes may not be the latest available.

Emotet

SHA-1	ESET detection name
51AAA2F3D967E80F4C0D8A86D39BF16FED626AEF	Win32/Kryptik.GMLY trojan
EA51627AF1F08D231D7939DC4BA0963ED4C6025F	Win32/Kryptik.GMLY trojan
3438C75C989E83F23AFE6B19EF7BEF0F46A007CF	Win32/Kryptik.GJXG trojan
00D5682C1A67DA31929E80F57CA26660FDEEF0AF	Win32/Kryptik.GMLC trojan

Modules

SHA-1	ESET detection name
0E853B468E6CE173839C76796F140FB42555F46B	Win32/Kryptik.GMFS trojan
191DD70BBFF84D600142BA32C511D5B76BF7E351	Win32/Emotet.AW trojan
BACF1A0AD9EA9843105052A87BFA03E0548D2CDD	Win32/Kryptik.GMFS trojan

SHA-1	ESET detection name
A560E7FF75DC25C853BB6BB286D8353FE575E8ED	Win32/Kryptik.GMFS trojan
12150DEE07E7401E0707ABC13DB0E74914699AB4	Win32/Kryptik.GMFS trojan
E711010E087885001B6755FF5E4DF1E4B9B46508	Win32/Agent.TFO trojan

Secondary payloads

TrickBot

SHA-1	ESET detection name
B84BDB8F039B0AD9AE07E1632F72A6A5E86F37A1	Win32/Kryptik.GMKM trojan
9E111A643BACA9E2D654EEF9868D1F5A3F9AF767	Win32/Kryptik.GMKM trojan

IcedId

SHA-1	ESET detection name
0618F522A7F4FE9E7FADCD4FBBECF36E045E22E3	Win32/Kryptik.GMLM trojan

C&C servers (active as of November 9, 2018)

187.163.174[.]149:8080
70.60.50[.]60:8080
207.255.59[.]231:443
50.21.147[.]8:8090
118.69.186[.]155:8080
216.176.21[.]143:80
5.32.65[.]50:8080
96.246.206[.]16:80
187.163.49[.]123:8090
187.207.72[.]201:443
210.2.86[.]72:8080

37.120.175[.]15:80
77.44.98[.]67:8080
49.212.135[.]76:443
216.251.1[.]1:80
189.130.50[.]85:80
159.65.76[.]245:443
192.155.90[.]90:7080
210.2.86[.]94:8080
198.199.185[.]25:443
23.254.203[.]51:8080
67.237.41[.]34:8443
148.69.94[.]166:50000
107.10.139[.]119:443
186.15.60[.]167:443
133.242.208[.]183:8080
181.229.155[.]11:80
69.198.17[.]20:8080
5.9.128[.]163:8080
104.5.49[.]54:8443
139.59.242[.]76:8080
181.27.126[.]228:990
165.227.213[.]173:8080

9 Nov 2018 - 03:11PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion