Malware-Traffic-Analysis.net - 2018-07-19 - Emotet infection traffic with Zeus Panda Banker

NOTICE:

- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- Zip archive of 4 email examples: 2018-07-19-Emotet-malspam-4-examples.zip 385 kB (384,921 bytes)

> - 2018-07-17-Emotet-malspam-1153-UTC.eml (1,153 bytes)
> - 2018-07-18-Emotet-malspam-0716-UTC.eml (247,503 bytes)
> - 2018-07-19-Emotet-malspam-1058-UTC.eml (493,762 bytes)
> - 2018-07-19-Emotet-malspam-1703-UTC.eml (1,022 bytes)

- Zip archive of the infection traffic: 2018-07-19-Emotet-infection-with-Zeus-Panda-Banker.pcap.zip 4.1 MB (4,064,731 bytes)

> - 2018-07-19-Emotet-infection-with-Zeus-Panda-Banker.pcap (4,568,407 bytes)

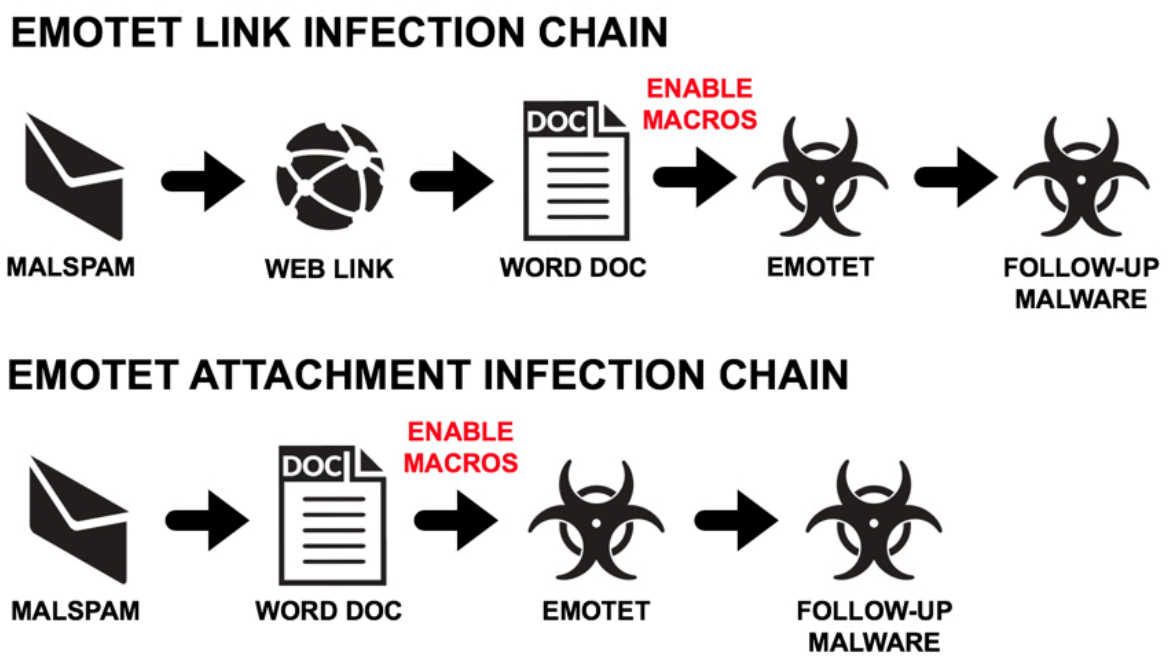
- Zip archive of the malware: 2018-07-19-malware-from-Emotet-infection.zip 690 kB (689,821 bytes)

> - 2018-07-19-downloaded-Word-doc-with-macro-for-Emotet.doc (343,296 bytes)
> - 2018-07-19-Emotet-malware-binary-1-of-2.exe (283,648 bytes)
> - 2018-07-19-Emotet-malware-binary-2-of-2.exe (280,576 bytes)
> - 2018-07-19-Zeus-Panda-Banker-caused-by-Emotet-infection.exe (265,728 bytes)

NOTES:

- I recently did a blog for Palo Alto Networks titled Malware Team Up: Malspam Pushing Emotet + Trickbot.
- It focuses on Emotet + Trickbot, but today it was Emotet + Zeus Panda Banker.

EMOTET MALSPAM I SAW FROM 2018-07-17 THRU 2018-07-19



Shown above: Flowchart for recent Emotet infection traffic.

WEB TRAFFIC BLOCK LIST

Indicators are not a block list. If you feel the need to block web traffic, I suggest the following domain and URLs:

- hxxp[:]//aulacloud[.]com[.]br/pdf/EN_en/New-Order-Upcoming/Please-pull-invoice-984495/
- hxxp[:]//zazz[.]com[.]br/Documentos/
- hxxp[:]//astraclinic[.]com/Facturas-pendientes/
- hxxp[:]//trustsoft[.]ro/NFjd6T/
- hxxp[:]//181.129.60[.]162/whoami.php
- tailbackuisback[.]xyz

EMAILS

DATA FROM 4 EMAIL EXAMPLES:

- Date: Tuesday, 2018-07-17 11:53 UTC
- Received: from 10.3.23[.]36 (UnknownHost [1.6.26[.]234])
- From: benji@overyondr[.]com <*[removed]@[removed]*>
- Subject: CUST. JFD-55-17335
- Link: hxxp[:]//aulacloud[.]com[.]br/pdf/EN_en/New-Order-Upcoming/Please-pull-invoice-984495/

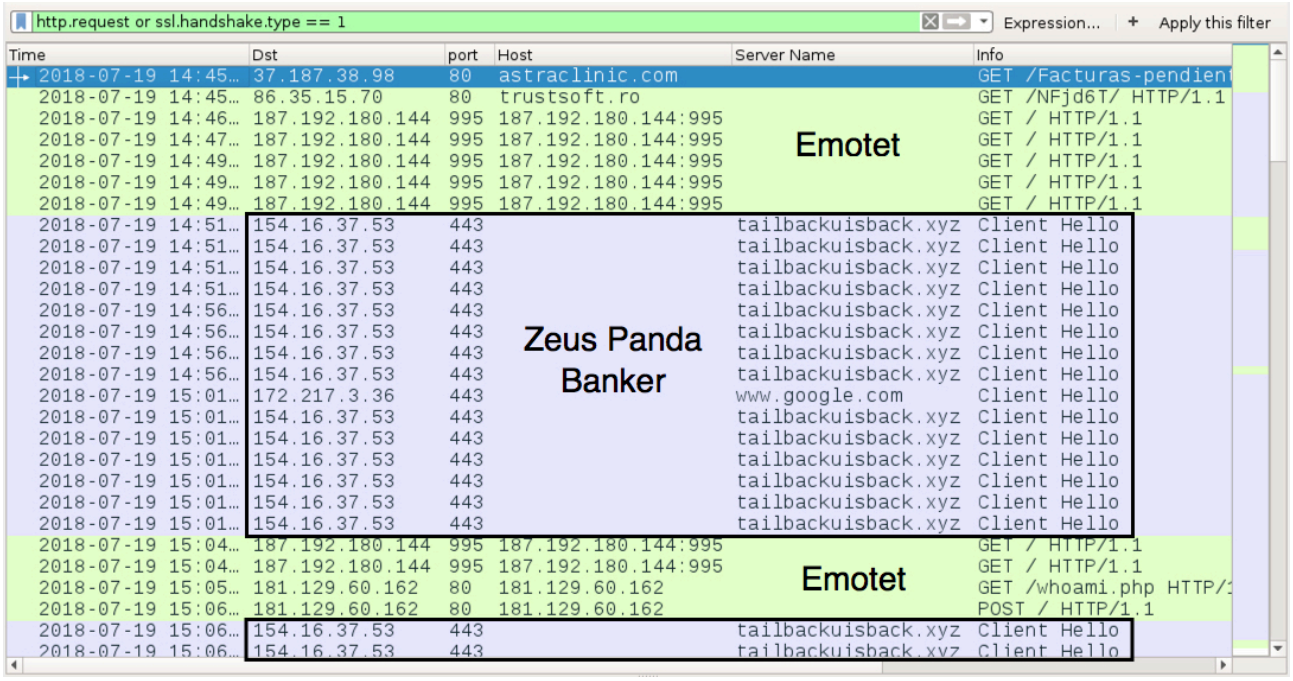
- Date: Wednesday, 2018-07-18 07:16 UTC
- Received: from [196.250.41[.]122] (port=49278 helo=10.0.0[.]52)
- From: SAV AITICA <> <almacen@francachela[.]com[.]mx>>

- Subject: Outstanding invoice
- Attachment name: INV-EB51776.doc

- Date: Thursday, 2018-07-19 10:58 UTC
- Received: from 10.0.0[.]51 (fixed-187-190-248-34.totalplay[.]net [187.190.248[.]34])
- From: Raj Jhamb <> <marcs@svtv[.]com>
- Subject: Inv. no. 1ZVO1641
- Attachment name: INV-1ZVO1641.doc

- Date: Thursday, 2018-07-19 10:58 UTC
- Received: from [189.232.17[.]251] (port=58245 helo=10.0.0[.]28)
- From: Kasaiah Amirisetty <> <edgar@dgforensiks[.]mx>
- Subject: Kasaiah Amirisetty Factura de servicio y soporte F4179871 de 19 julio
- Link: hxxp[:]//zazz[.]com[.]br/Documentos/

TRAFFIC



Shown above: Traffic from an infection filtered in Wireshark.

TRAFFIC FROM AN INFECTED WINDOWS HOST:

- 37.187.38[.]98 port 80 - **astraclinic[.]com** - GET /Facturas-pendientes/
- 86.35.15[.]70 port 80 - **trustsoft[.]ro** - GET /NFjd6T/
- 67.68.235[.]25 port 50000 - attempted TCP connections, but no response from the server
- 187.192.180[.]144 port 995 - **187.192.180[.]144:995** - GET /
- 154.16.37[.]53 port 443 - **tailbackuisback[.]xyz** - post-infection traffic caused by Zeus Panda Banker
- port 443 - **www.google[.]com** - connectivity check caused by Zeus Panda Banker
- 5.188.231[.]137 port 443 - attempted TCP connections, but no response from the server
- 91.243.80[.]2 port 443 - attempted TCP connections, but no response from the server

- 201.232.42[.]151 port 8443 - attempted TCP connections, but no response from the server
- 181.129.60[.]162 port 80 - **181.129.60[.]162** - GET /whoami.php
- 181.129.60[.]162 port 80 - **181.129.60[.]162** - POST /

FILE HASHES

MALWARE RETRIEVED FROM MY INFECTED WINDOWS HOST:

- SHA256 hash: 7bad900ea5cb2044726bd474d9b7f642c279425144e73b99463279fc83a95981
  File size: 343,296 bytes
  File name: FACTURA-QMO-39839388.doc (random file names)
  File description: Word doc downloaded from a link in Emotet malspam. Doc has macro to retreive Emotet.

- SHA256 hash: 3dd27b20b2ab85c95f8e9e1b5f4944e277ab018b3c663a8bf6262aa36183b0cf
  File size: 283,648 bytes
  File location: C:\Users*[username]*\AppData\Local\Microsoft\Windows*[random file name]*.exe
  File description: Emotet malware binary downloaded by macro in downloaded Word doc

- SHA256 hash: 5482557ca490c50f5f383c6d6d3b51efd4b215b22ee3dde51a811a4f490735cc
  File size: 280,576 bytes
  File location: C:\Users*[username]*\AppData\Local\Microsoft\Windows*[random file name]*.exe
  File description: Updated Emotet malware binary after the host was infected for a while

- SHA256 hash: 200dd176eccfe11a3456193bf1fe7d46d23408834e172991b883d59aa59ce259
  File size: 265,728 bytes
  File location: C:\Users*[username]*\AppData\Roaming*[existing directory path]**[random file name]*.exe
  File description: Zeus Panda Banker downloaded by my Emotet-infected host

Click here to return to the main page.
