SANS ISC: Emotet infections and follow-up malware - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

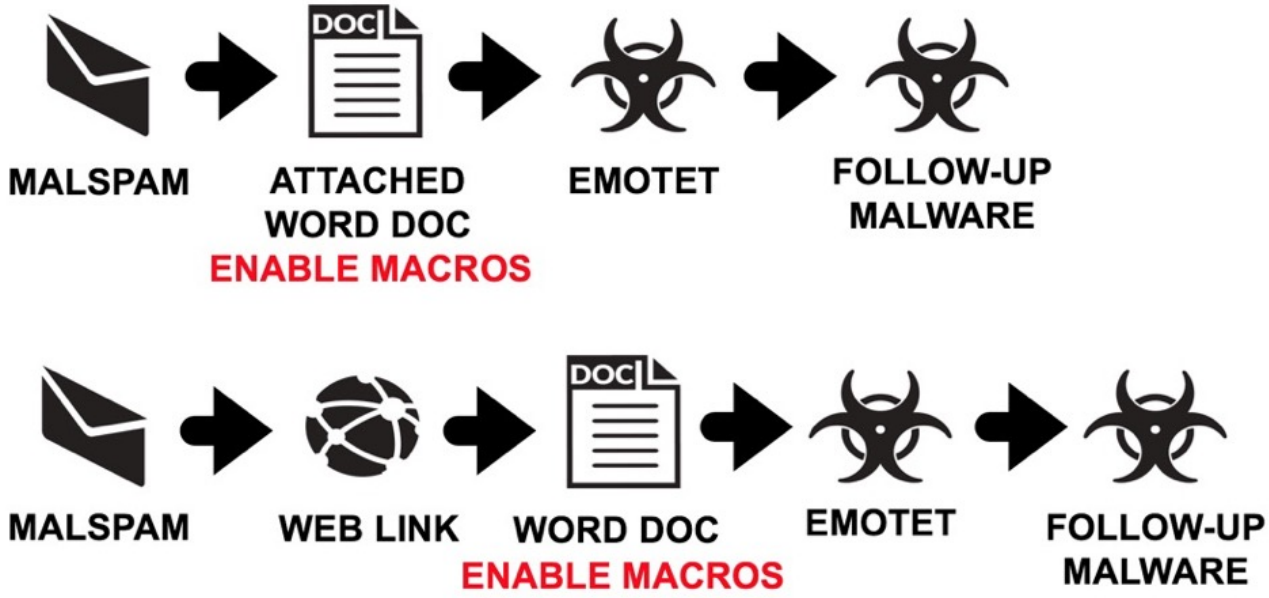
isc.sans.edu/forums/diary/Emotet+infections+and+followup+malware/24532/

Introduction

Three major campaigns using malicious spam (malspam) to distribute malware stopped sending malspam before Christmas-sometime during the week ending on Sunday 2018-12-23. These three campaigns are Emotet (also known as Feodo), Hancitor (also known as Chanitor or Tordal), and Trickbot. But this week, all three campaigns have been sending out malspam again.

Among these campaigns, Emotet is by far the most active. Dozens of indicators are discovered every day as vectors for Emotet infections. Emotet also acts a distributor for other families of malware. So far in 2019, I've seen Emotet retrieve Gootkit and the IcedID banking Trojan. As 2019 progresses, I expect to find examples of Emotet distributing other families of malware like Qakbot and Trickbot, something we saw in 2018.

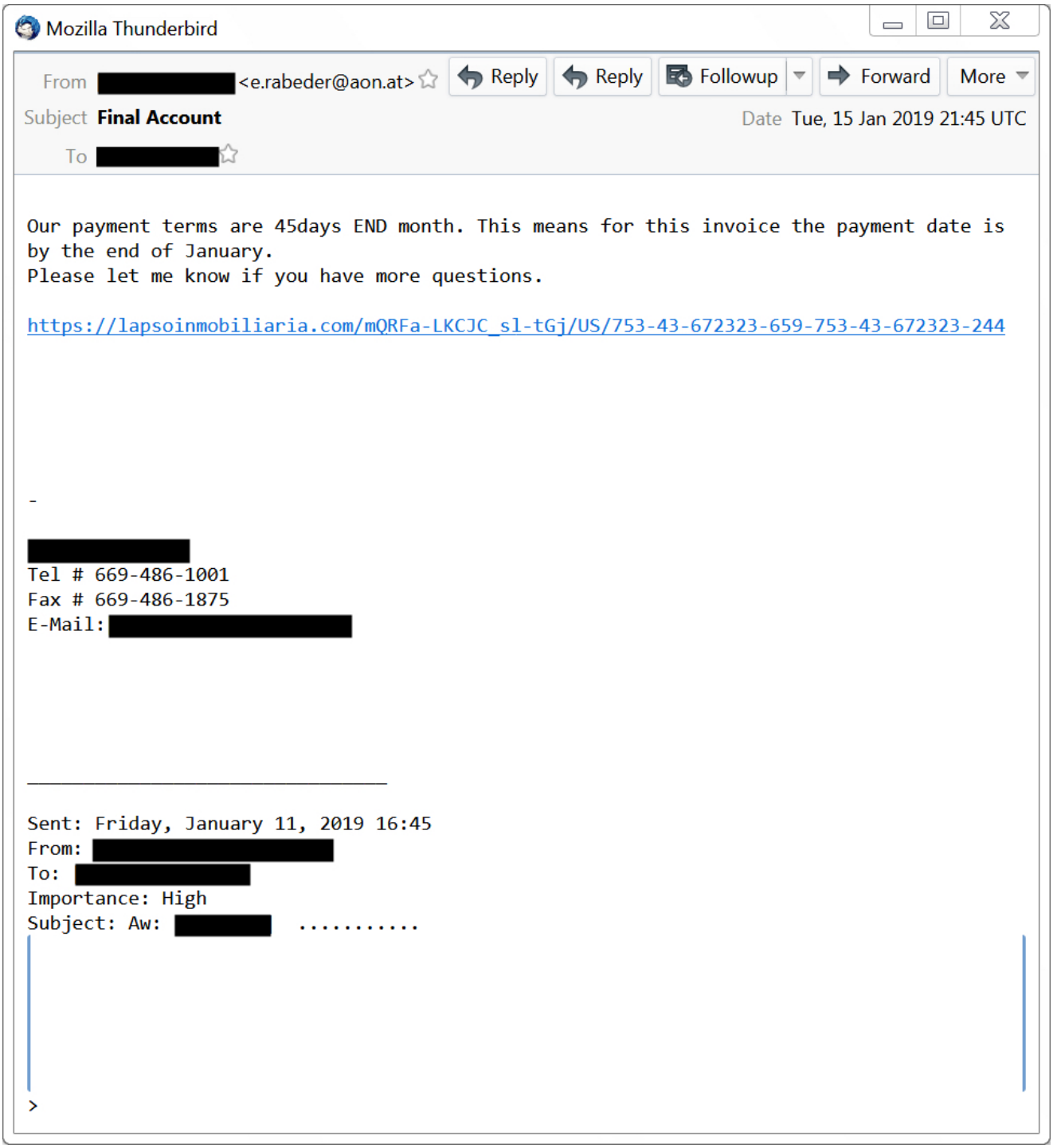
Today's diary examines recent Emotet malspam and two examples of infection traffic from Tuesday 2019-01-15.



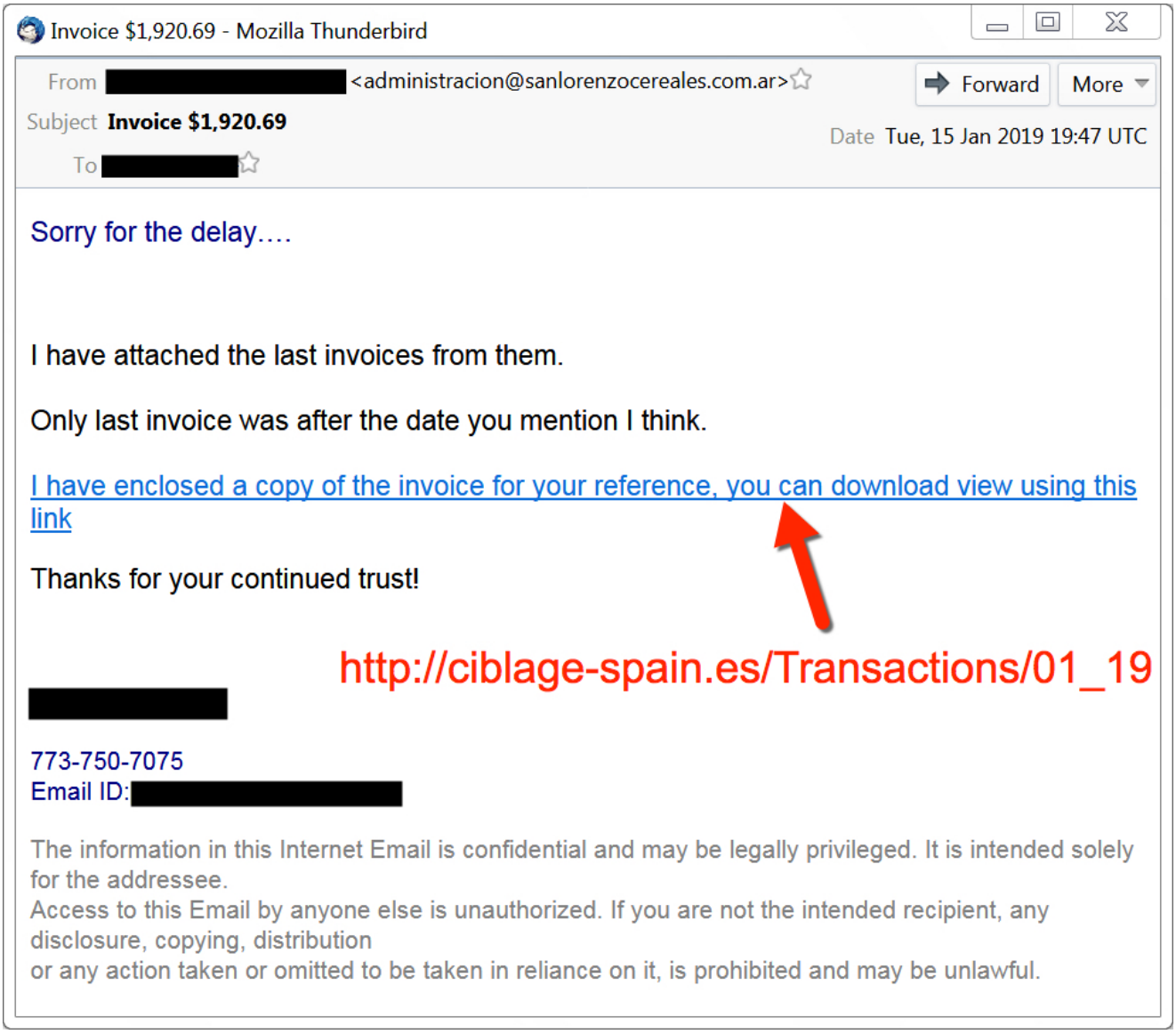
Shown above: Chain of events for Emotet malware distribution seen so far this year.

The malspam

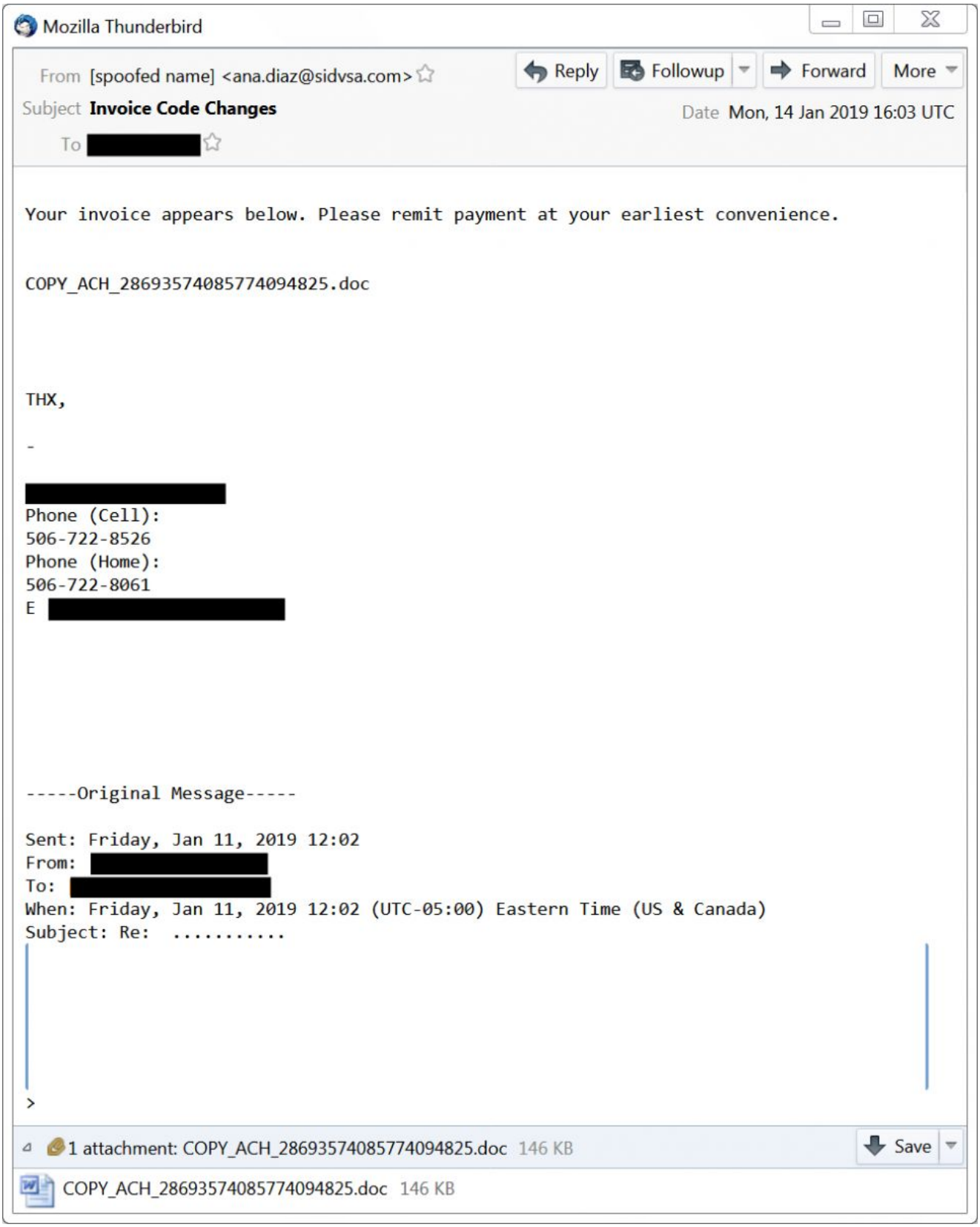
As usual, emails pushing Emotet use Microsoft Word documents with malicious macros. On vulnerable Windows hosts, opening these documents in Microsoft Word and enabling macros will attempt an Emotet infection. So far this week, Emotet malspam had a link to download the Word document, or it's had a Word document directly attached to the email. See the images below for examples.



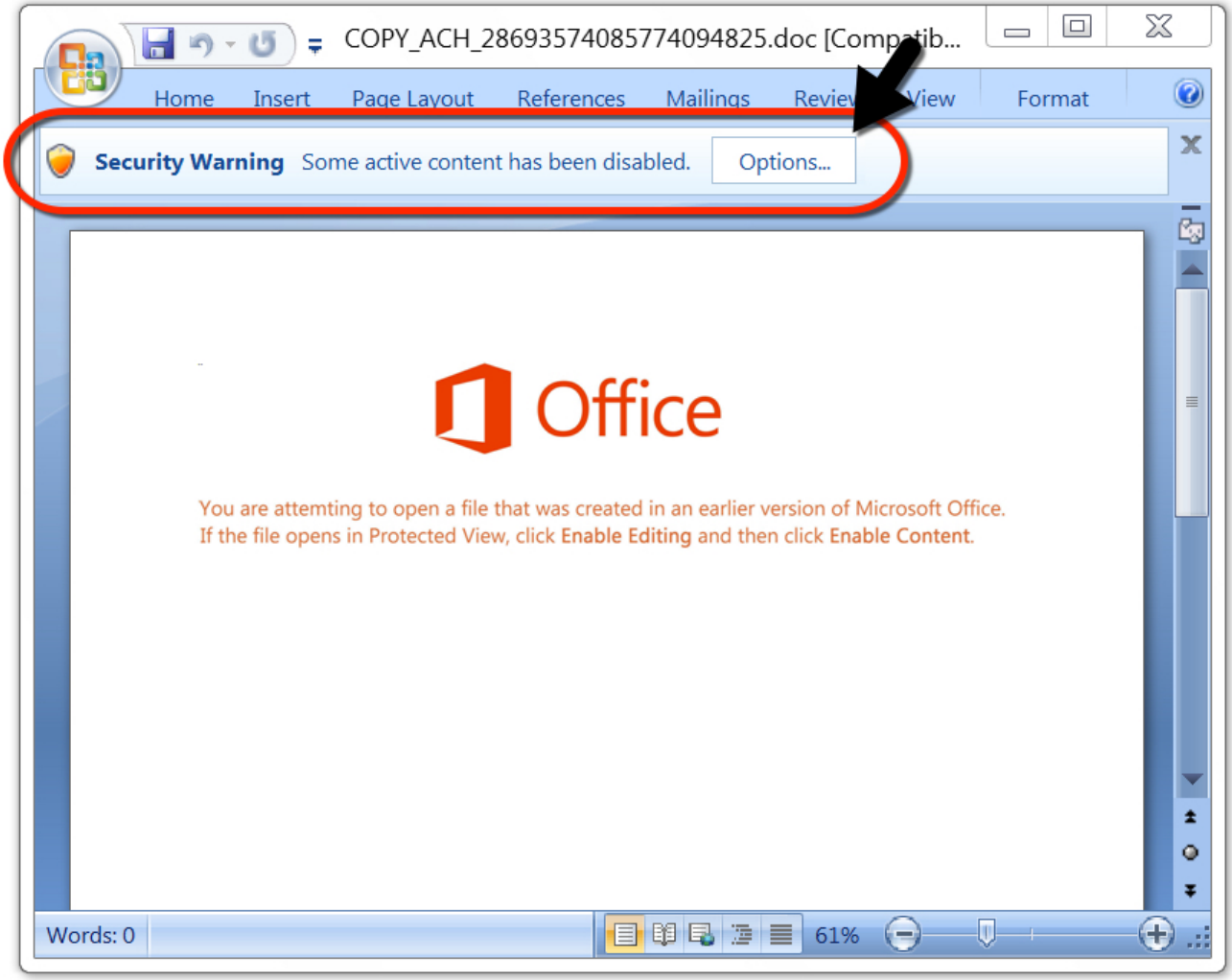
Shown above: Screenshot 1 of 3 - Emotet malspam with link for Word doc from Tuesday 2019-01-15.



Shown above: Screenshot 2 of 3 - Emotet malspam with link for Word doc from Tuesday 2019-01-15.



Shown above: Screenshot 3 of 3 - Emotet malspam with attached Word doc from Monday 2019-01-14.



Shown above: Example of Word document with macro to infect a vulnerable Windows host with Emotet.

The traffic

Network traffic is typical for what we've seen with recent Emotet infections from December 2018. Emotet frequently uses HTTP traffic over non-standard TCP ports (not TCP port 80). This may cause issues when reviewing the infection traffic in Wireshark. Traffic on ports like TCP port 53 (associated with DNS activity like zone transfers) and TCP port 22 (normally associated with SSH) may not be decoded as HTTP in Wireshark. That was the case with two examples of infection traffic I generated on Monday.

Post-infection activity from the first run included Gootkit, which had similar in traffic patterns that I've previously documented. Post-infection activity from the second run included IcedID (also known as Bokbot), something I've also documented.

Indicators of Compromise (IoCs)

The following are indicators from two infections on Tuesday 2019-01-15. Any malicious URLs, IP addresses, and domain names have been “de-fanged” to avoid issues when viewing today’s diary.

Malware from the first run:

SHA256 hash: 2b8c45af81889ce22ffaf3a78d79a307ce3ab4ebeabbd00bc5982d60a89a2c87

- File size: 158,208 bytes
- File location: hxxp://mdmshipping[.]org/wp-content/uploads/Clients_transactions/012019/
- File name: 190115_invoice.doc
- File description: Downloaded Word doc with macro for Emotet

SHA256 hash: 4cb1c0ce3de256e671b096729ae35b65b5f4ac67fe0ca9bbdc27e84aaf25a4d3

- File size: 151,552 bytes
- File location: hxxp://www.al-bay[.]com/JbDEG76/
- File location: C:\Users*[username]*\AppData\Local\tablesvcs\tablesvcs.exe
- File description: Emotet executable retrieved by Word macro

SHA256 hash: e1f60b891005dfd0f6738444406c8e57d644cc3ce0154f8d17454c886637dfbd

- File size: 151,552 bytes
- File location: C:\Users*[username]*\AppData\Local\tablesvcs\tablesvcs.exe
- File description: Emotet executable updated after initial infection

SHA256 hash: 9fd057d99bad388e08f3d71c1d78e90b308e0eb656ecaec88cd70d31f723118e

- File size: 315,392 bytes
- File location: C:\ProgramData\7gYMH.exe
- File description: Gootkit executable retrieved by my Emotet-infected host

Malware from the second run:

SHA256 hash: abd3942b115eef97d1dca7bbc05022689ee78090b02fb930d202148b9218323c

- File size: 153,088 bytes
- File location: hxxp://ciblage-spain[.]es/Transactions/01_19/
- File name: 012019_INV_0049.doc
- File description: Downloaded Word doc with macro for Emotet

SHA256 hash: a2d4ccd13954f43ab541b10f879f0d8b5fcf4fa24fffa1b08444bd2313242a78

- File size: 155,648 bytes
- File location: hxxp://starbilisim[.]net/umEgLOOKUD/
- File location: C:\Users*[username]*\AppData\Local\pesicy\pesicy.exe
- File description: Emotet executable retrieved by Word macro

SHA256 hash: e1f60b891005dfd0f6738444406c8e57d644cc3ce0154f8d17454c886637dfbd

- File size: 151,552 bytes
- File location: C:\Users*[username]*\AppData\Local\pesicy\pesicy.exe
- File description: Emotet executable updated after initial infection

SHA256 hash: 4f519a9e1df4558336263f398c44796cb412e7ef56d3290f0f12b422eb325730

- File size: 275,456 bytes
- File location: C:\ProgramData\35YXoiR.exe
- File description: IcedID executable retrieved by my Emotet-infected host

SHA256 hash:
92352a5a9e473c8939e3a609253f65d3afaa392f872134ba73c3972d2c5e4830

- File size: 275,456 bytes
- File location: C:\ProgramData\{A2EE4104-C104-4A1F-9FCE-D86635165D72}\floflbjnc.exe
- File description: IcedID executable made persistent on my Emotet-infected host

Emotet Infection traffic from the first run:

- 92.222.210[.]16 port 80 - ***mdmshipping[.]org*** - GET /wp-content/uploads/Clients_transactions/012019/
- 149.255.58[.]108 port 80 - ***www.al-bay[.]com*** - GET /JbDEG76
- 149.255.58[.]108 port 80 - ***www.al-bay[.]com*** - GET /JbDEG76/
- 189.146.157[.]111 port 20 - Attempted TCP connections (no response from the server)
- 216.244.228[.]62 port 53 - ***216.244.228[.]62:53*** - GET /
- 187.163.177[.]194 port 22 - Attempted TCP connections (no response from the server)
- 181.164.8[.]8 port 22 - ***181.164.8[.]8:22*** - GET /
- 189.129.134[.]124 port 20 - Attempted TCP connections (no response from the server)
- 189.225.146[.]180 port 8443 - ***189.225.146[.]180:8443*** - GET /

Gootkit infection traffic from the first run:

- 66.23.200[.]58 port 443 - ***mid.centralcoastbagels[.]com*** - HTTPS/SSL/TLS traffic
- DNS query for ***loredanusos[.]com*** - response: No such name
- DNS query for ***bigiterra[.]com*** - response: No such name
- DNS query for ***getlowfast[.]com*** - response: No such name

Emotet infection traffic from the second run:

- 87.98.154[.]146 port 80 - ***ciblage-spain[.]es*** - GET /Transactions/01_19
- 87.98.154[.]146 port 80 - ***ciblage-spain[.]es*** - GET /Transactions/01_19/
- 149.255.58[.]108 port 80 - ***www.al-bay[.]com*** - GET /JbDEG76
- 149.255.58[.]108 port 80 - ***www.al-bay[.]com*** - GET /cgi-sys/suspendedpage.cgi
- 159.253.42[.]200 port 80 - ***starbilisim[.]net*** - GET /umEgLOOKUD
- 159.253.42[.]200 port 80 - ***starbilisim[.]net*** - GET /umEgLOOKUD/
- 187.163.177[.]194 port 22 - Attempted TCP connections (no response from the server)
- 181.164.8[.]8 port 22 - ***181.164.8[.]8:22*** - GET /
- 189.129.134[.]124 port 20 - Attempted TCP connections (no response from the server)
- 189.225.146[.]180 port 8443 - Attempted TCP connections (no response from the server)
- 66.50.57[.]73 port 8080 - ***66.50.57[.]73:8080*** - GET /
- 186.15.66[.]98 port 443 - ***186.15.66[.]98:443*** - GET /
- 181.211.11[.]171 port 443 - ***181.211.11[.]171:443*** - GET /

IcedID infection traffic from the second run:

- 185.223.163[.]26 port 443 - ***kepleted[.]pw*** - HTTPS/SSL/TLS traffic
- 194.165.3[.]3 port 80 - ***bestcontrol[.]at*** - GET /data2.php?45DD8E695E0FFFAB
- 185.223.163[.]26 port 443 - ***stronour[.]host*** - HTTPS/SSL/TLS traffic
- 194.165.3[.]3 port 443 - ***bestcontrol[.]at*** - HTTPS/SSL/TLS traffic
- 194.165.3[.]3 port 443 - ***exeterol[.]host*** - HTTPS/SSL/TLS traffic
- 194.165.3[.]3 port 443 - ***decretery[.]host*** - HTTPS/SSL/TLS traffic

Final words

Pcaps of the infection traffic and malware associated with today's diary can be found here.

Brad Duncan
brad [at] malware-traffic-analysis.net