Case Study: Emotet Thread Hijacking, an Email Attack Technique

unit42.paloaltonetworks.com/emotet-thread-hijacking/
Brad Duncan

September 23, 2020

By Brad Duncan

September 23, 2020 at 6:00 AM

Category: Malware, Unit 42

Tags: botnet, cyber crime, Emotet, MealyBug, TA542



This post is also available in: <u>日本語 (Japanese)</u>

Executive Summary

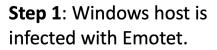
Malicious spam (malspam) pushing Emotet malware is the most common email-based threat, far surpassing other malware families, <u>with only a few other threats coming close</u>.

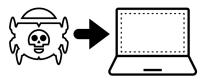
In recent weeks, we have seen significantly more Emotet malspam using a technique called "thread hijacking" that utilizes legitimate messages stolen from infected computers' email clients. This malspam spoofs a legitimate user and impersonates a reply to the stolen email. Thread hijacked malspam is sent to addresses from the original message.

This technique is much more effective than less sophisticated methods, which many people have now learned to spot. The approach is more successful at convincing potential victims to click on an attached file, or to click on a link to download a malicious Word document with macros designed to infect a user with Emotet.

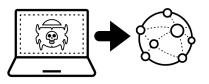
Here, we review a case study of Emotet's thread hijacking process so we can better recognize and understand this technique.

Palo Alto Networks customers are protected from this threat because our <u>Threat Prevention</u> security subscription detects and prevents these types of Emotet infections. <u>AutoFocus</u> users can track Emotet activity using the <u>Emotet</u> tag.





Step 2: Emotet-infected host sends data collected from its email client through C2 traffic.



Step 3: Hosts from Emotet botnet spoof email chains from the stolen data.

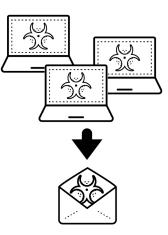


Figure 1. Visual representation of Emotet's thread hijacking process.

Case Study Timeline

To illustrate Emotet's thread hijacking process, our case study focuses on an infection from Sept. 3, 2020. In this example, Emotet hijacks the most recent email in an Outlook inbox from an infected host.

The timeline is:

- 15:35 UTC Legitimate message received by email client on host.
- 16:31 UTC Host infected with Emotet.
- 16:34 UTC Legitimate message collected from infected host is sent through Emotet command and control (C2) traffic.
- 18:22 UTC Emotet botnet sends spoofed email using legitimate message from the infected host.

This process took one hour and 51 minutes to progress from the infection to the arrival of a thread-hijacked email.

Legitimate Email From the Infected Host

In our example, a vulnerable Windows 10 host used Microsoft Outlook as its email client. Outlook was synchronized to a Microsoft account at k********.r***@outlook.com (we have redacted information from the email addresses for this case study). The most recent message in the infected host's email client is shown in Figure 2, and we have loaded a redacted copy of the legitimate email to GitHub.

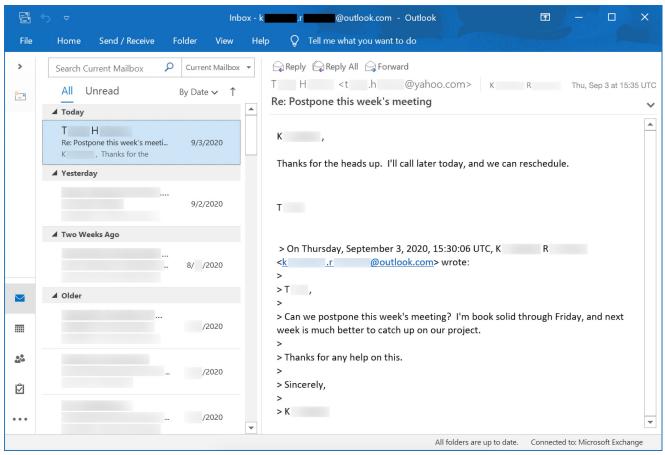


Figure 2. Most recent email from an infected host's Outlook client. As we see in Figure 2, the most recent email was received at 15:35 UTC, approximately one hour before the host was infected with Emotet. This email is a response from t****.h*****@yahoo.com to a previous message from k*********.r*****@outlook.com.

Data Exfiltration Through C2 Traffic

Emotet uses HTTP POST requests over C2 traffic to send data collected from the infected host. This data is encoded or otherwise encrypted before it is sent over HTTP.

Most of these POST requests contain only a small amount of encoded data from the infected host, often much less than 1,000 bytes. These requests contain an extra 4 kB of data for padding and form header data. Figure 3 shows a typical example of Emotet C2 traffic from our case study.

POST AV02AHIZ24G3:15h1W4C/GBPU/UCWHDDRDUG//JWB YPAG5/FWT8V25/H/KS2V1408VC1[L4K2/952W27TEB6/4LUD4ZS1E/.HTTF/1.1 Concent-Type: ULipat/Tomatia. User Agent: M021IA/A (compatible; NSIE 7.0; Windows NT 6.2; W0464; Trident/T.0; NET4.0C;	 Wireshark · Follow TCP Stream (tcp.stream eq 2) · 2020-09-03-Emotet-epoch-1-ii 	nfection-wtih-Trickbot-gtag-mo	or119.pcap	- + ×
Content-Disposition: form-dit:::nama="features" Content-Disposition: form-dit:::nama="features" T/0:k.b:rz./. a.5b.!s.JN.P!	Content-Type: multipart/form-data; boundary=DNKCVU User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; T Host: 50.121.220.50 Content-Length: 4772 Connection: Keep-Alive	HEURÌWİRXrRgNV5fA ident/7.0; .NET4.0C;	NET4.0E)	ITTP/1.1
at. 3 00 [SW.P.	Content-Disposition: form-data; name="kcmkfpazgfkvyxjzph"; filename="eu		neader info	_
at. 3 00 [SW.P.		675 bytes of er	coded data	
.HTTP/1.1 200 0K Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 Sofert plks, 1forer plks, 1form Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 :	duf#>t.z.eq4z.0ZC.R>d.x.!.{. .fW*(W.U. +.p`i9/+jk.<.;f.au}CZ	Gi~.X.kC#92 R.)h\[y)n}F_KGy> /7.4.0W.u. Cs52/	V.	bytes of
.HTTP/1.1 200 0K Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 Sofer plk; flower plk; flow Entire conversation (149 kB) * Show and save data as ASCI * Stream 2 :				
.HTTP/1.1 200 0K Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 Sofer plk; flower plk; flow Entire conversation (149 kB) * Show and save data as ASCI * Stream 2 :	DNKCVHEuRlwiRxrRqNv5fA			
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 1 fum. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •				
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 1 fum. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •		•••••		
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 1 fum. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •		•••••	•••••••••••••••••••••••••••••••••••••••	•••••
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 1 fum. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •				
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 1 fum. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •				
HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: Lext/html; charset=UFF-8 Sdentp4ks, 116 server p4ks, 11 um. Entire conversation (149 kB) • Show and save data as ASCII • Stream 2 •				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$			••••••	•••••
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 \$				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡		• • • • • • • • • • • • • • • • • • • •		
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡		••••••••••••••••••••••••••••	• • • • • • • • • • • • • • • • • • • •	
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡		••••••		•••••
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡		••••••	••••••	•••••
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Server: nginX Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream 2 ‡				
Date: Thu, 03 Sep 2020 16:32:08 GMT Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII				
Content-Type: text/html; charset=UTF-8 5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII	5			
5 client pkts, 116 server pkts, 1 turn. Entire conversation (149 kB) * Show and save data as ASCII * Stream				*
Entire conversation (149 kB) Show and save data as ASCII Stream 2				
Find:				Stream 2
	Find:			Find <u>N</u> ext
Image: Second	@Help	Filter Out This Stream Prin	it Save as E	Back × <u>C</u> lose

Figure 3. Example of HTTP POST data from Emotet C2 traffic in our case study.

Since the amount of encoded data is so small, it does not contain any email chain data collected from the infected user's email client. However, at 16:34 UTC, we find 13.9 kB of encoded data sent over Emotet HTTP C2 traffic as shown in Figure 4.

(http.request or tls.handshake	.type eq 1) and !(ssdp)			🛛 🖃 👻 🏓 basic basic+ basic+dns
me	Dst	port	Host	Info
2020-09-03 16:31:19		80	ie-koubou.co.jp	GET /wp backup/http://DOC/Fb4PEwdRyYnv
2020-09-03 16:31:43		80	morinchoiniere.com	GET /wp-admin/8/ HTTP/1.1
2020-09-03 16:32:02	50.121.220.50	80	50.121.220.50	POST /WOSAHIZAFgF3IhShv0C/GaP9uvICWMbl
2020-09-03 16:33:22	50.121.220.50	80	50.121.220.50	POST /IGLft2vXEpG0gspy/ HTTP/1.1
2020-09-03 16:33:25		443	62.210.90.75:443	POST /LHJbA/vhQue/1nYsC4q/X03eKZHOI/ H
2020-09-03 16:34:04	54.37.42.48	8080	54.37.42.48:8080	POST /AJX6Q8G2M7/ HTTP/1.1
2020-09-03 16:34:06	54.37.42.48	8080	54.37.42.48:8080	POST /sZmoLA/zwqLLDLX2HWBrpX3c/kL5q9zh
2020-09-03 16:34:06	62.210.90.75	443	62.210.90.75:443	POST /FiTv6l6JG3MnsiszD/xxITJuh7zBjpvv
2020-09-03 16:34:06	54.37.42.48	8080	54.37.42.48:8080	POST /VgxBsJNqpEqSgfgoEd/ HTTP/1.1
2020-09-03 16:34:07	54.37.42.48	8080	54.37.42.48:8080	POST /lNZuyLwljg/ZYmWW8LP96L/KJmUIZLp
2020-09-03 16:34:07	62.210.90.75	443	62.210.90.75:443	POST /qq3EpipG/5PsUvoWnOto866Fir/J1xoF
2020-09-03 16:34:08			54.37.42.48:8080	POST /sX33TOOVbYiJ/NLfa4nB/dLPA4/GKEB
2020-09-03 16:34:09		8080	54.37.42.48:8080	POST /oDDeCrA82pCAfHd3bFa/E0K3hdPp4p/
2020-09-03 16:34:10	62.210.90.75	443	62.210.90.75:443	POST /c3rDuRWfhhbKaQ69/3aTz6d09S7yKP4,
2020-09-03 16:37:16	- Wireshark · Follow T	CP Stre	eam (tcp.stream eq 7) · 2020-	09-03-Emplet-epoch-1-infection-wtih-Trickbot-gtag-mor119.
2020-09-03 16:37:17	[\$h X4	R /	Y 7 H "	POST /c3rDuRWfhhbKaQ69/3aTz6d09S7yKP4/
2020-09-03 16:41:09	KBwRmwegR/ HTTP			
2020-09-03 16:41:33			art/form-data: bounda	ary=pEXUlR9ybsMzTuBJrU13
2020-09-03 16:41:48				E 7.0; Windows NT 6.2; WOW64; Trident/7.0;
2020-09-03 16:42:27	.NET4.0C; .NET4			,
2020-09-03 16:42:42			40	
2020 00 02 16.42.50	Host: 62.210.90	. / 3:44	43	
2020-09-03 16:42:59	Host: 62.210.90 Content-Length:		A	ST conding approximately 12.0 kB
2020-09-03 16:43:58	Content-Length:	1387		ST sending approximately 13.9 kB
2020-09-03 16:43:58 2020-09-03 16:44:30		13870 p-Ali	🕵 🛨 HTTP POS	
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41	Content-Length: Connection: Kee	13870 p-Ali	💒 🛨 HTTP POS	
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43	Content-Length: Connection: Kee	13870 p-Ali	🕵 🛨 HTTP POS	
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46	Content-Length: Connection: Kee Cache-Control:	13870 p-Aliv no-cao	🕵 🛨 HTTP POS	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43	Content-Length: Connection: Keep Cache-Control:	13870 p-Aliv no-cao	HTTP POS che of encode pEXU1R9ybsMZTuBJrU1	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control:	13870 p-Aliv no-cao tion:	HTTP POS che of encode pEXU1R9ybsMZTuBJrU1	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control:	13870 p-Aliv no-cao tion:	HTTP POS che of encode pEXULR9ybsMzTuBJrU1 form-data; name="zpf	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 .	1387(p-Aliv no-cao tion: pplica	HTTP POS of encodepEXULR9ybsMZTuBJrU1 form-data; name="zpf ation/octet-stream	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposi Content-Type: a =.dI+.m03 . %=.AJ'.J	1387(p-Aliv no-cao tion: pplica	HTTP POS of encodepEXUIR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-streamtTJ.i@	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'J .d	13870 p-Aliv no-cao tion: pplica	HTTP POS of encode of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ tTJ.i@ tTJ.i@	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5	1387(p-Aliv no-cao tion: pplica	6 ← HTTP POS ve of encode of encode pEXUIR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ jp.?rS>vU .v/z/	d data ¹³ faxfpuldygveji"; filename="wqgxovedol" Z@y.S.C .
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .d	1387(p-Aliv no-cao tion: pplica	6 ← HTTP POS ve of encode of encode pEXUIR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ jp.?rS>vU .v/z/	d data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposi Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (YD	13870 p-Aliy no-cao tion: pplica	6 ← HTTP POS ve of encode of encode pEXUIR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ jp.?rS>vU .v/z/	d data ¹³ faxfpuldygveji"; filename="wqgxovedol" Z@y.S.C .
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposi Content-Type: a =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (13870 p-Aliv no-cao tion: pplica	6 ← HTTP POS of encode pEXUIR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS>vU v}.".N@*.r	d data ¹³ faxfpuldygveji"; filename="wqgxovedol" Z@y.S.C .
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: 1 Content-Disposit Content-Type: ap =.dI+.m03 %=.AJ'.J .dX.+. %bMUt5 (NcUr.Cq0 }D 	13870 p-Aliv no-cao tion: pplica g\$.N. s 	6 ← HTTP POS che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS>vU .v}.".N@*.r	d data ¹³ faxfpuldygveji"; filename="wqgxovedol" .z@y.s.c . .r@qcc.oUW,.5.`.q@ZD"Szi!.Y.3(
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: 1 Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (NcUrCq(}D C}; &]9.V.K\$p.	13870 p-Aliv no-cao tion: pplica q\$.N. s aw	6 ← HTTP POS che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS>VU .V}.".N@*.r 	<pre>ed data J3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.Cr.r@qCC.oUW,.5.`.q@ZD"Szi!.Y.3(QC.gBH@4km .a;.</pre>
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (KcUrCq0 }D NKFs.:]9.V.K\$p. A	13870 p-Aliv no-cao tion: pplica d\$.N. s .\aw bxEb.	6 ← HTTP POS ve che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ p.?rS>VU .v}.".N@*.r .{.%&. T7.=YUB.{.q.U.n. 08,.>c8dF.u.iW.	d data I3 faxfpuldygveji"; filename="wqgxovedol" Z@y.S.C r@qcc.oUW, .5.`.q@ZD"Szi!.Y.3(QC.gBH@4km .a;. #H>.1}tHU=eQ.kVLL.wO
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposi Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMU5 (.NC.UT.Cq0 }D NKFs.]9 . 	13870 p-Aliv no-cao tion: pplica d\$.N. s .\aw bxEb.	6 ← HTTP POS ve che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ p.?rS>VU .v}.".N@*.r .{.%&. T7.=YUB.{.q.U.n. 08,.>c8dF.u.iW.	<pre>ed data J3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.Cr.r@qCC.oUW,.5.`.q@ZD"Szi!.Y.3(QC.gBH@4km .a;.</pre>
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (13870 p-Alix no-cao tion: pplica q\$.N. s aw bxEb.	6 ← HTTP POS ve che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS>vU .v}.".N@*.r .{.%&. T7.=YUB.{qUn. .08,.>.c8dF.u.iW	ad data
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dx.+ %DMUt5 (Nc.UT.Cq0 }D .NKFs.3 fs.3 	13870 p-Alix no-cao tion: pplica q\$.N. s aw bxEb.	6 ← HTTP POS of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS.>VU .V}.".N@*.r .{.%& T7.=.YUB.{.q.U.n. .08,.>c8dF.u.iW W.\$q.Gc.< "{.dD.,tg5z.j x.r'.+	d data I3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.C .reqcc.oUW, .5.`.q@ZD"Szi!.Y.3(.qc.gBH@4km .a;. #H.>.1}tHU=eQ.kVLL.wO A[8m.&<
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (NcUrCq0 }D NKFs.: 	13870 p-Alix no-cao tion: pplica q\$.N. s aw bxEb. 	6 ← HTTP POS ve che of encode pEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-stream tTJ.i@ .Jp.?rS>vU .v}.".N@*.r .{.%&. T7.=YUB.{qUn. .08,.>.c8dF.u.iW	d data I3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.C .reqcc.oUW, .5.`.q@ZD"Szi!.Y.3(.qc.gBH@4km .a;. #H.>.1}tHU=eQ.kVLL.wO A[8m.&<
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dx.+ %DMUt5 (Nc.UT.Cq0 }D .NKFs.3 fs.3 	13870 p-Alix no-cao tion: pplica q\$.N. s w bxEb. w	6 ★ HTTP POS of encode of encodepEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-streamtTJ.i@ .Jp.?rS.>VUV/z/}	d data I3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.C .reqcc.oUW, .5.`.q@ZD"Szi!.Y.3(.qc.gBH@4km .a;. #H.>.1}tHU=eQ.kVLL.wO A[8m.&<
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: I Content-Disposi Content-Type: al =.dI+.m03 . %=.AJ'.J .dX.+. %bMUt5 (.NC.UT.Cq0 }D NKFS. 	13870 p-Alix no-cao tion: pplica q\$.N. s w bxEb. w	6 ★ HTTP POS of encode of encodepEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-streamtTJ.i@ .Jp.?rS.>VUV/z/}	ad data I3 faxfpuldygveji"; filename="wqgxovedol" Z@y.S.C r@qCC.oUW, .5.`.q@ZD"Szi!.Y.3(QC.gBH@4km .a;. #H>.1}tHU=eQ.kVLL.wO A[8m.& <euq3q;?< td=""> rg9N.8 W OLCO ow and save data as ASCII</euq3q;?<>
2020-09-03 16:43:58 2020-09-03 16:44:30 2020-09-03 16:47:41 2020-09-03 16:47:43 2020-09-03 16:47:46 2020-09-03 16:47:46	Content-Length: Connection: Keep Cache-Control: n Content-Disposit Content-Type: ap =.dI+.m03 . %=.AJ'.J .dX.+ %bMUt5 (NcUrCq0 }D NKFs. fs. fs. 	13870 p-Alix no-cao tion: pplica q\$.N. s w bxEb. w	6 ★ HTTP POS of encode of encodepEXUlR9ybsMzTuBJrU1 form-data; name="zpf ation/octet-streamtTJ.i@ .Jp.?rS.>VUV/z/}	d data I3 faxfpuldygveji"; filename="wqgxovedol" .Z@y.S.C .reqcc.oUW, .5.`.q@ZD"Szi!.Y.3(QC.gBH@4km .a;. #H.>.1}tHU=eQ.kVLL.wO A[8m& <euq3q.;?< td=""> tg9N.8 W 01c0</euq3q.;?<>

Figure 4. Approximately 13.9 kB of encoded data in Emotet C2 traffic at 16:34 UTC.

This amount is large enough to contain email chain data collected from the infected Windows host. It is the only significant amount of data sent in HTTP POST requests from the Emotet-infected host before we find the thread-hijacked email at 18:22 UTC.

Spoofed Message From Hijacked Email

At 18:22 UTC, a spoofed email was received by t****.h*****@yahoo.com, the Yahoo account that had sent the most recent message in correspondence to the infected host. It contains an attached Word document with macros for Emotet. This message is shown in Figure 5, and we have loaded <u>a copy of the spoofed email</u> to GitHub.

Re: Postpone this week's meeting K R k @outlook.com K Regards, T T
k @outlook.com K , Thanks for the heads up. I'll call later today, and we can reschedule
Thanks for the heads up. I'll call later today, and we can reschedule
Regards, T
T
> On Thursday, September 3, 2020, 15:30:06 UTC, K
<pre>> On Thursday, September 3, 2020, 15:30:06 UTC, K </pre> <pre> R </pre> <pre></pre>
> T ,
> Can we postpone this week's meeting? I'm book solid through Friday, and next week is much better to catch up on our project.
>
> Thanks for any help on this.
> > Sincerely,
>
> K
Mes_G697doc 259.4kB Figure 5. Hijacked email sent from the Emotet botnet.

The message is a reply to t****.h*****@yahoo.com that spoofs k*******.r***@outlook.com from the infected host.

These thread-hijacked messages either have an attached file, or they have a link to download a malicious Word document with macros designed to infect a vulnerable host with Emotet.

Emotet's thread-hijacked message from this case study spoofed the name in the sending address line from the infected host. Headers from the spoofed message indicate the actual sender may have been from a botnet host in Brazil, or a Brazil-based host may have been used to relay the message. Botnet hosts from all over the world are used to send these thread-hijacked messages from Emotet infections.

```
Return-Path: <vinicius.sc@somahospitalar.com.br>
Received: from 191.252.199.165 (EHLO mail199165.hm1831.locaweb.com.br)
 by 10.197.33.12 with SMTPs; Thu, 3 Sep 2020 18:22:33 +0000
X-Originating-Ip: [191.252.199.165]
Received-SPF: pass (domain of somahospitalar.com.br designates 191.252.199.165 as permitted
sender)
Authentication-Results: atlas321.free.mail.bf1.yahoo.com;
 dkim=unknown;
 spf=pass smtp.mailfrom=somahospitalar.com.br;
 dmarc=unknown
X-Apparently-To: t****.h*****@yahoo.com; Thu, 3 Sep 2020 18:22:33 +0000
Received: from mcbain0004.email.locaweb.com.br (189.126.112.85) by
mail199145.hm1831.locaweb.com.br id ha4q682n8lgj for <t****.h*****@yahoo.com>; Thu, 3 Sep 2020
15:22:11 -0300 (envelope-from <vinicius.sc@somahospitalar.com.br>)
X-Original-To: <t****.h****@yahoo.com>
Received: from LEONARD0039.mail.collab.local (martin0001.email.locaweb.com.br [189.126.112.73])
        by mcbain0004.email.locaweb.com.br (Postfix) with ESMTP id 7D02D180FD3
        for <t****.h*****@yahoo.com>; Thu, 3 Sep 2020 15:22:11 -0300 (-03)
Received: from [200.87.242.147] (200.87.242.147) by
LEONARD0039.mail.collab.local (10.30.188.44) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256) id
 15.1.2044.4; Thu, 3 Sep 2020 15:22:35 -0300
Date: Thu, 3 Sep 2020 14:22:10 -0400
Locaweb_Exchange: Yes
From: K******** R******* <vinicius.sc@somahospitalar.com.br>
To: T**** H***** <t***.h****@yahoo.com>
Subject: Re: Re: Postpone this week's meeting
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="--2721644617813540782547331541442470"
Message-ID:
        <8cadda8f-2f82-407d-9688-a3a2533458b4@LEONARD0039.mail.collab.local>
X-Originating-IP: [200.87.242.147]
X-ClientProxiedBy: PENNY0001.mail.collab.local (10.30.190.2) To
LEONARD0039.mail.collab.local (10.30.188.44)
X-AuthUser: vinicius.sc@somahospitalar.com.br
Content-Length: 360155
```

Figure 6. Header lines from hijacked message sent to t****.h*****@yahoo.com.

These spoofed messages tend to be the most recent emails from a victim's email client because those are the most likely to fool someone.

Of note, we cannot always assume the spoofed sending address is from an infected victim. If the original message from an infected victim has multiple recipients, a hijacked email could spoof one of the other recipients.

Conclusion

We've stored an example of the legitimate email that was hijacked in this case study.

We've also stored an example of the spoofed messages sent from the Emotet botnet.

The pcap of infection traffic from this case study is also available.

This case study shows an example of Emotet thread hijacking so we can better understand how Emotet malware utilizes this technique. Emotet is a very active threat that constantly updates its malware in an attempt to evade detection. This vector of infection can reach a great deal of potential victims.

However, organizations with effective spam filtering that follow best security practices have a much lower risk from this infection vector. Palo Alto Networks customers are further protected from this threat, because our <u>Threat Prevention</u> security subscription detects and prevents these types of Emotet infections. <u>AutoFocus</u> users can track Emotet activity using the <u>Emotet</u> tag.

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our <u>Terms of Use</u> and acknowledge our <u>Privacy</u> <u>Statement</u>.