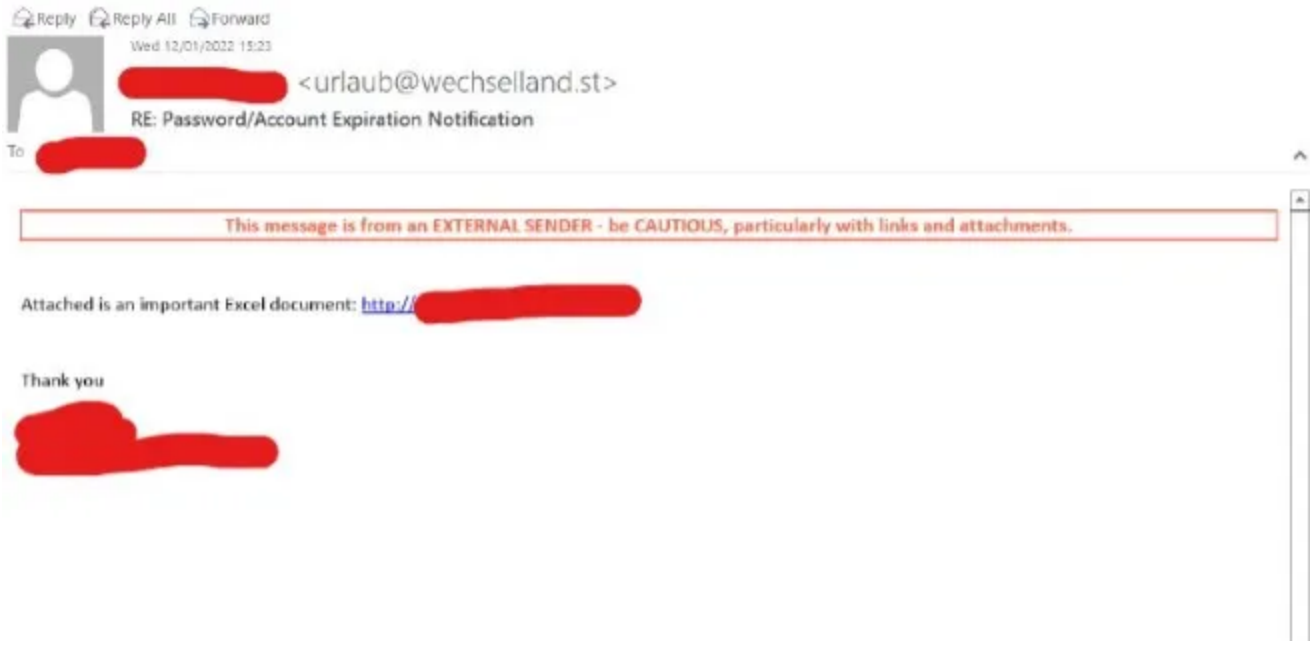
Malware Analysis Emotet Infection

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 phising. 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.

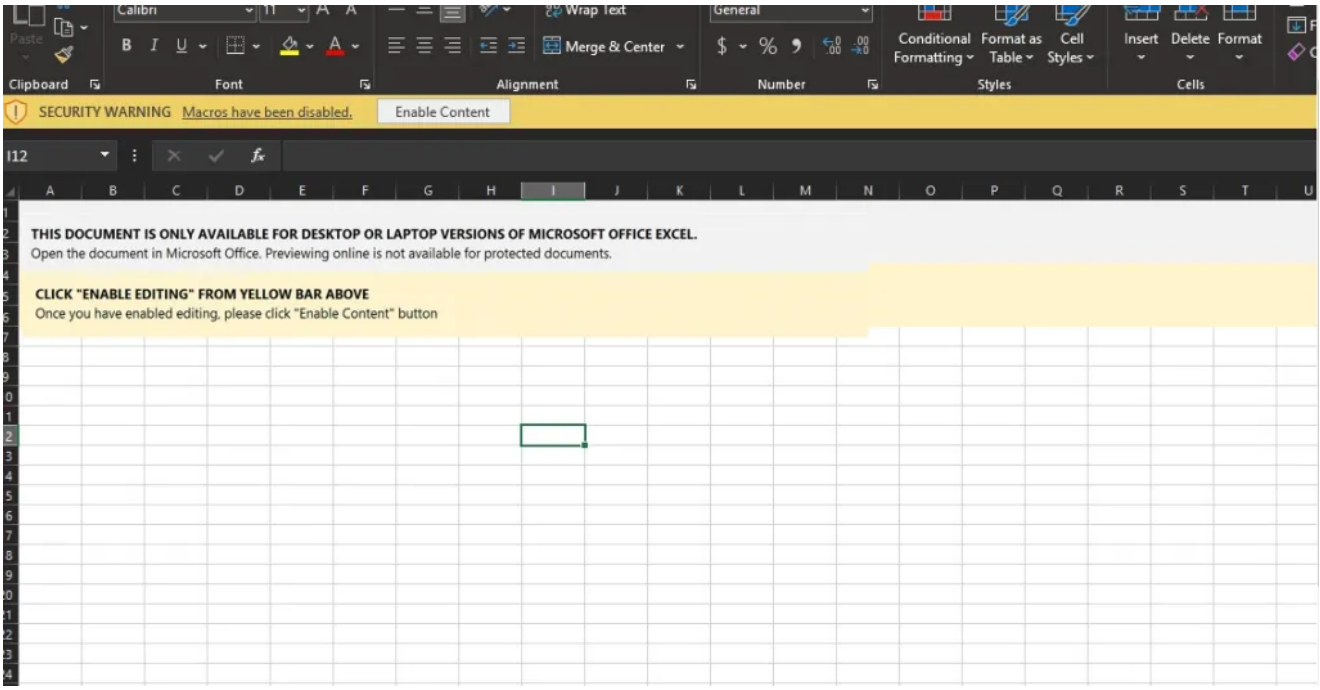
Apa Bahaya Malware Emotet?

Malware emotet menginfeksi umumya 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 lainya seperti ransomeware, mengumpulkan kontak email pada perangkat dan email gateway untuk proses spear phising dan spamming pada perangkat lain, pencurian informasi, dan lain lain.

> Baca juga: Njrat malware analysis
>
> *Baca juga: Network Analysis Command And Control*

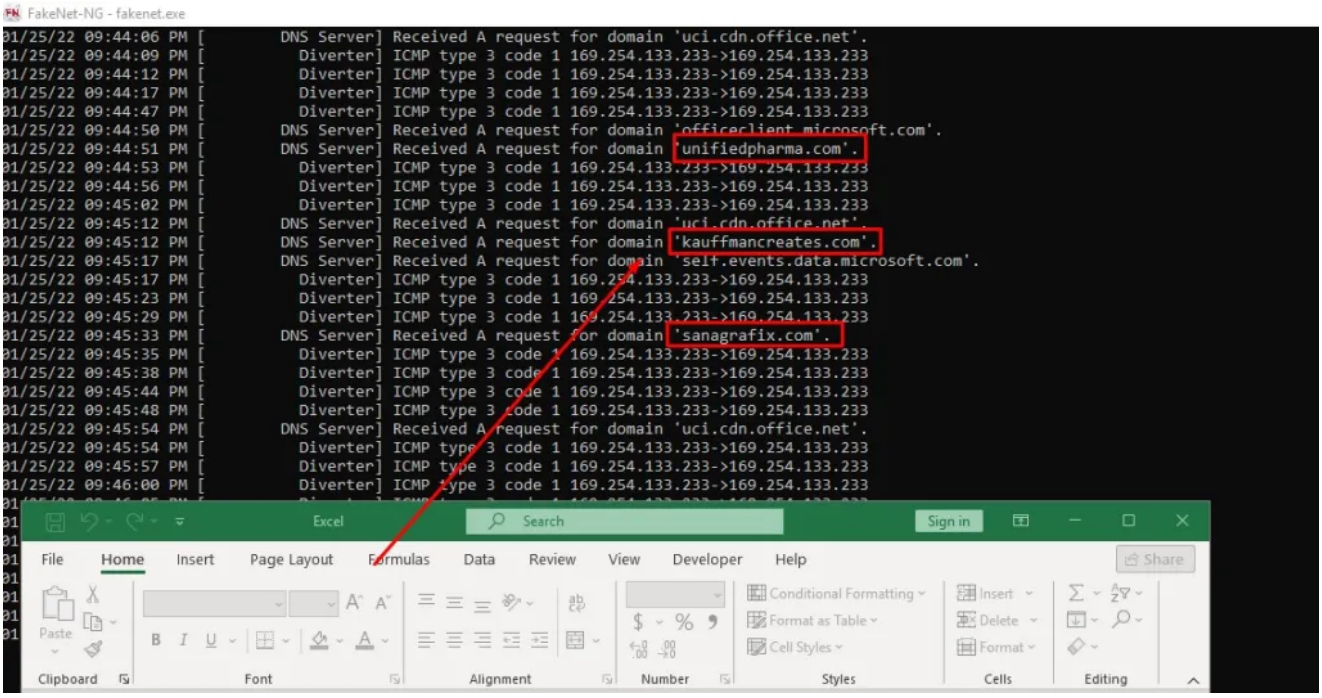
Bagaimana infeksi Malware emotet?

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 xlsm dan pdf, pada file xlsm ketika dibuka akan memberikan informasi untuk mengaktifkan enable editing atau enable content.



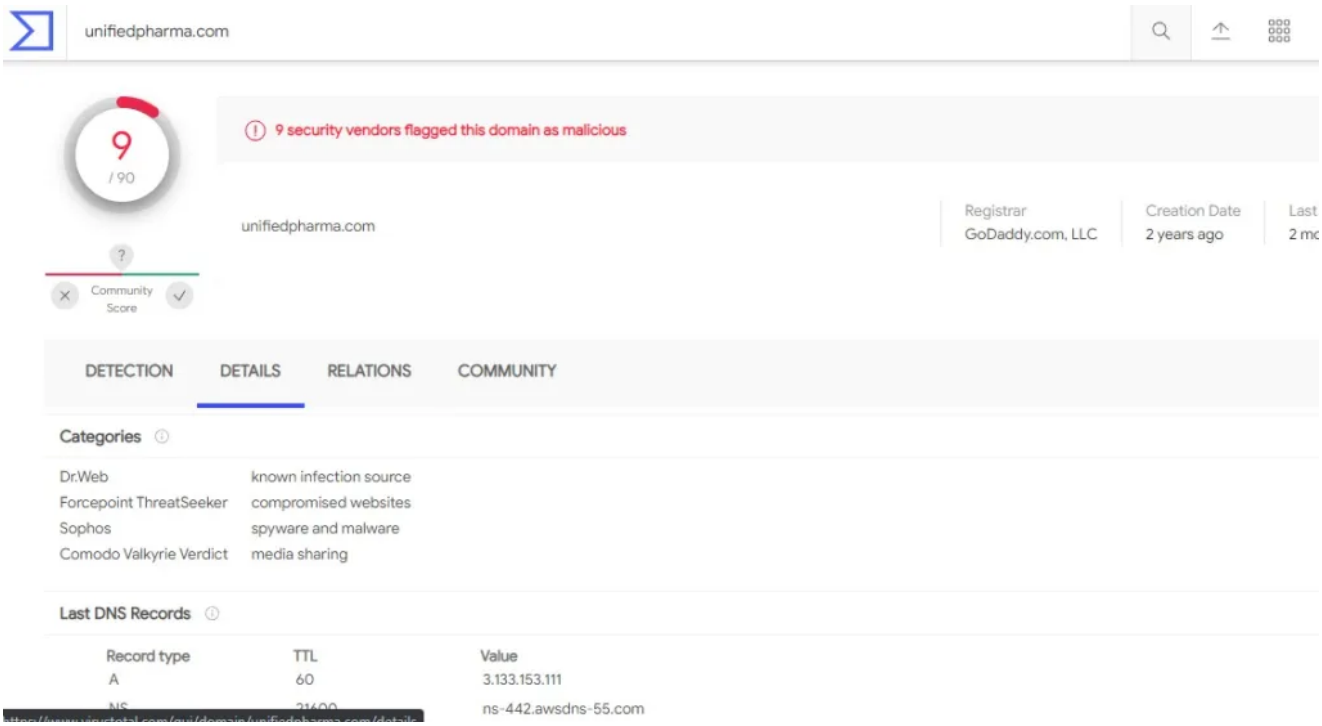
Analysis Malware emotet malware excel file

Setelah tombol enable editing atau enable content ditekan file akan loading dan proses kinerja CPU yang akan tinggi karena akan ada serivce 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.



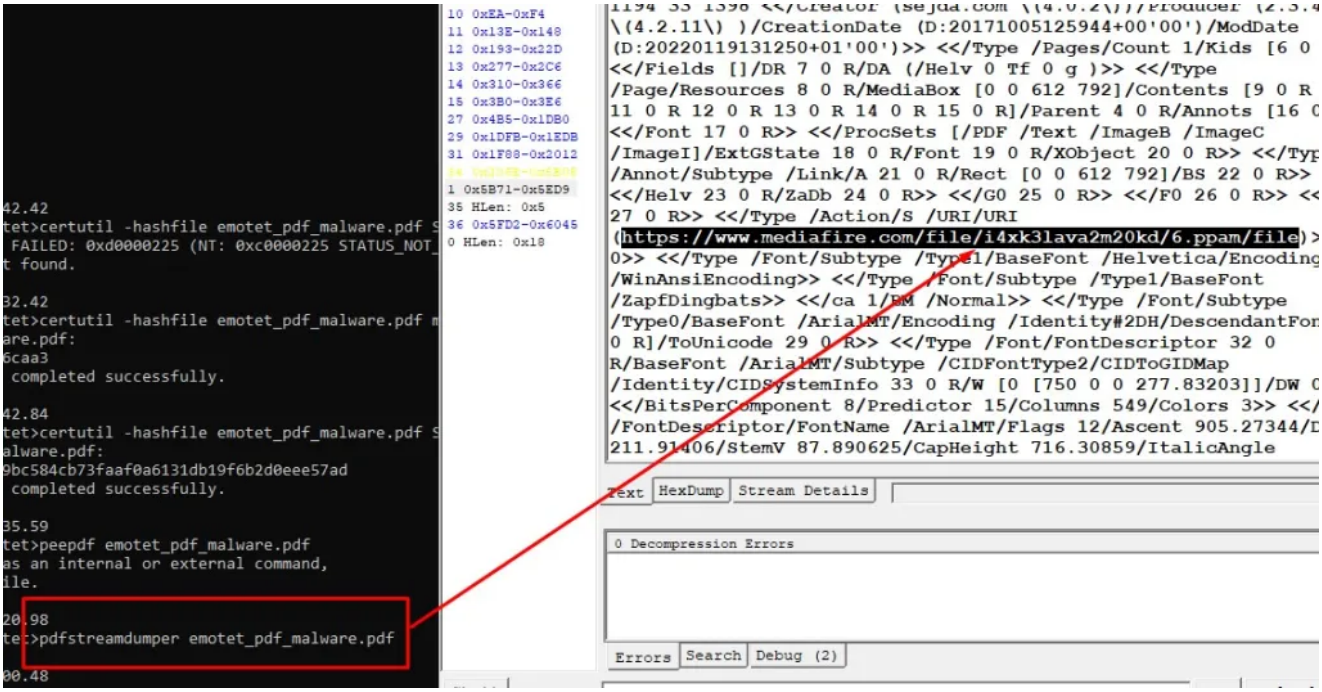
Analysis Malware emotet DNS Request

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.



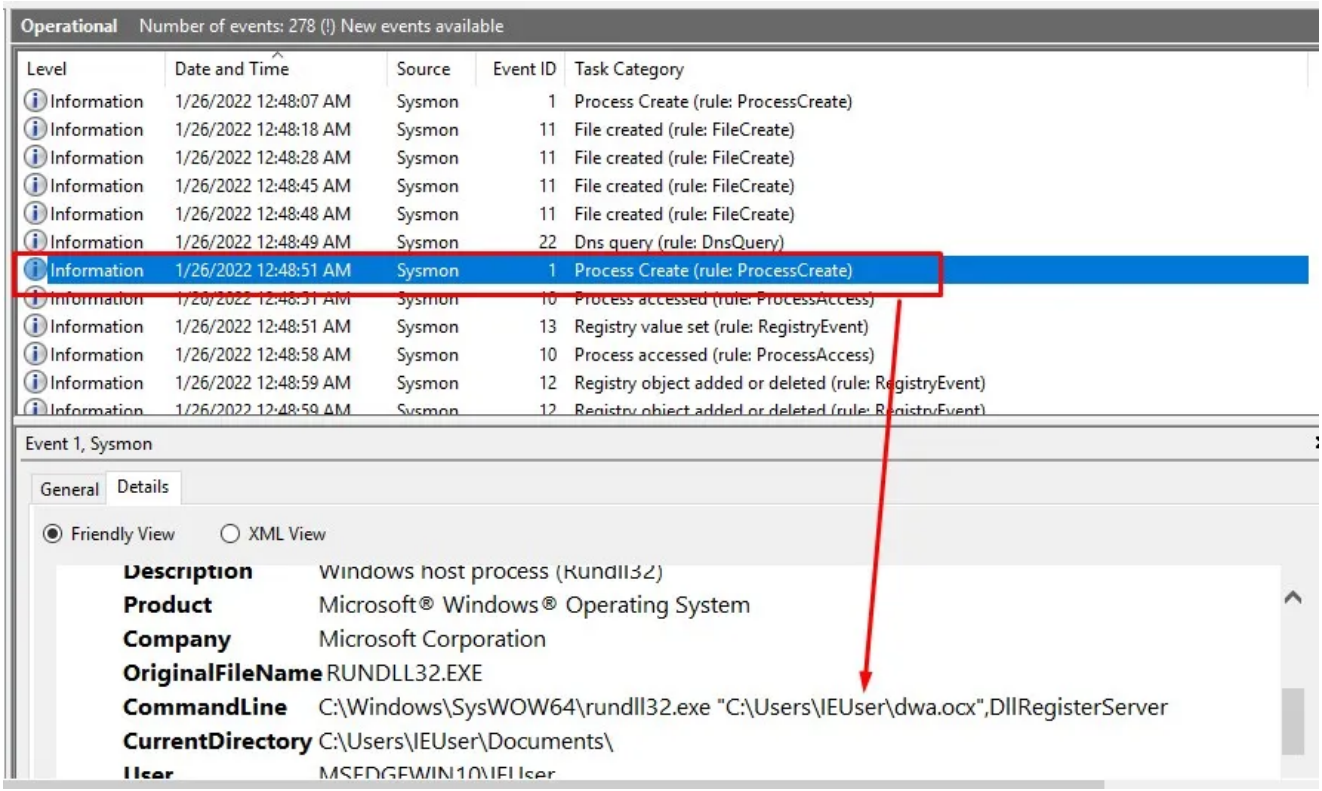
Analysis Malware emotet Domain IOC

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



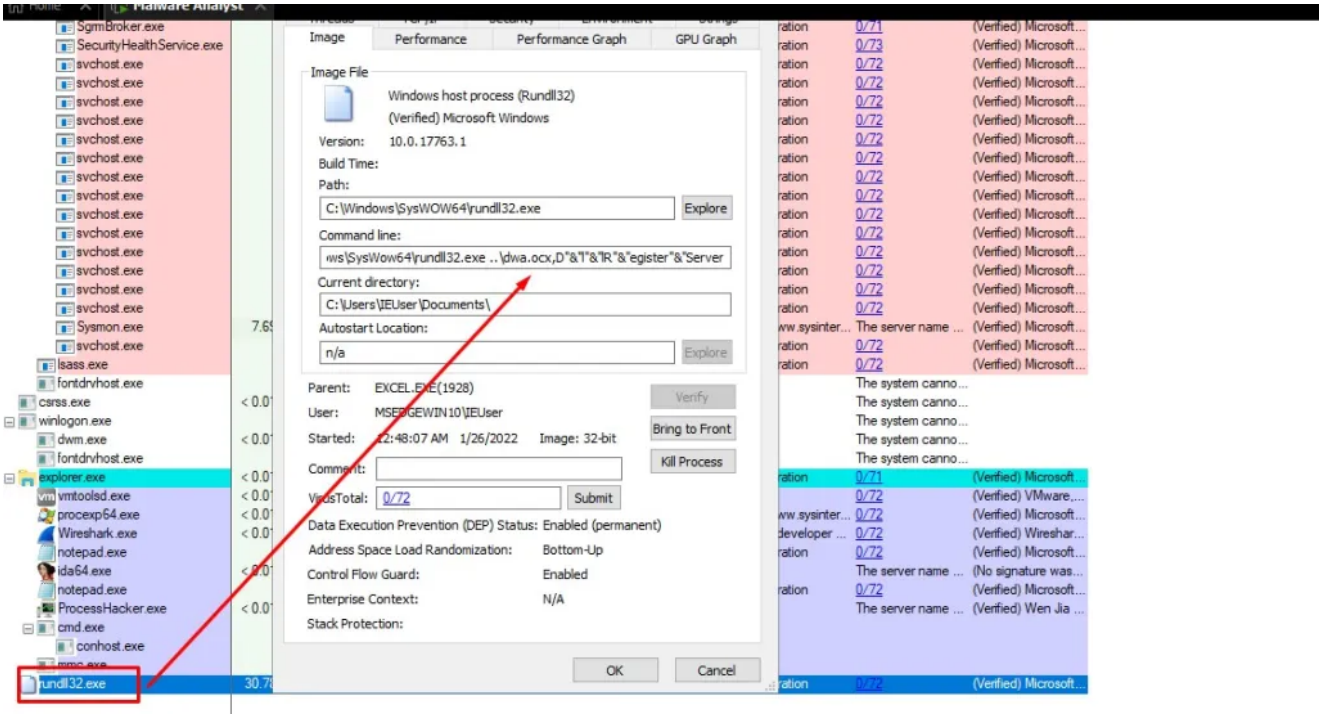
Analysis Malware emotet url donwload

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.



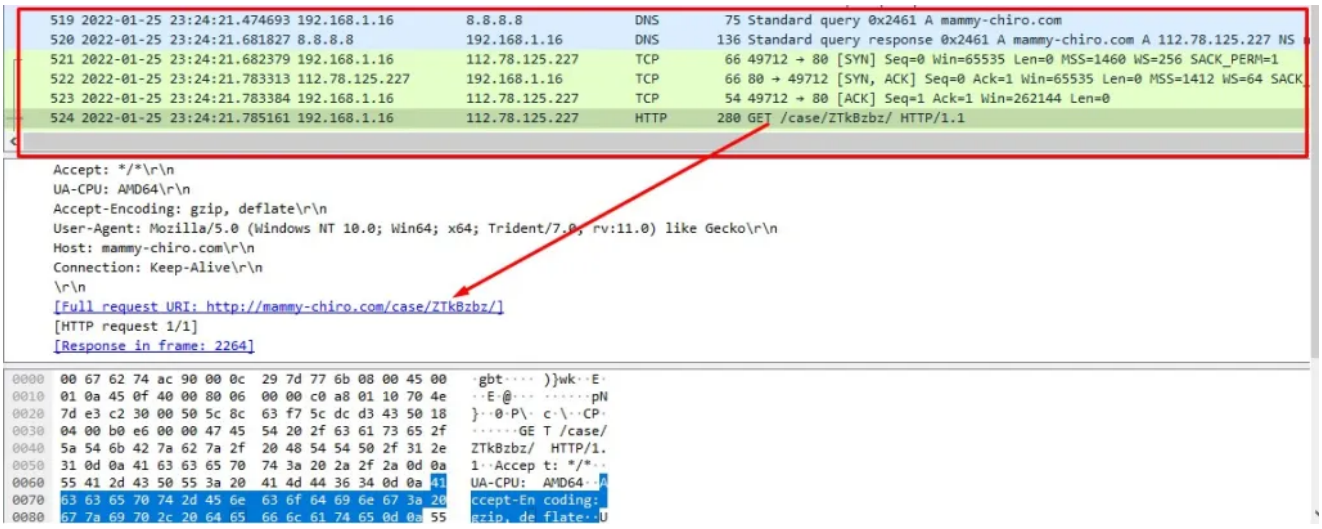
Analysis Malware emotet dorp ActiveX

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

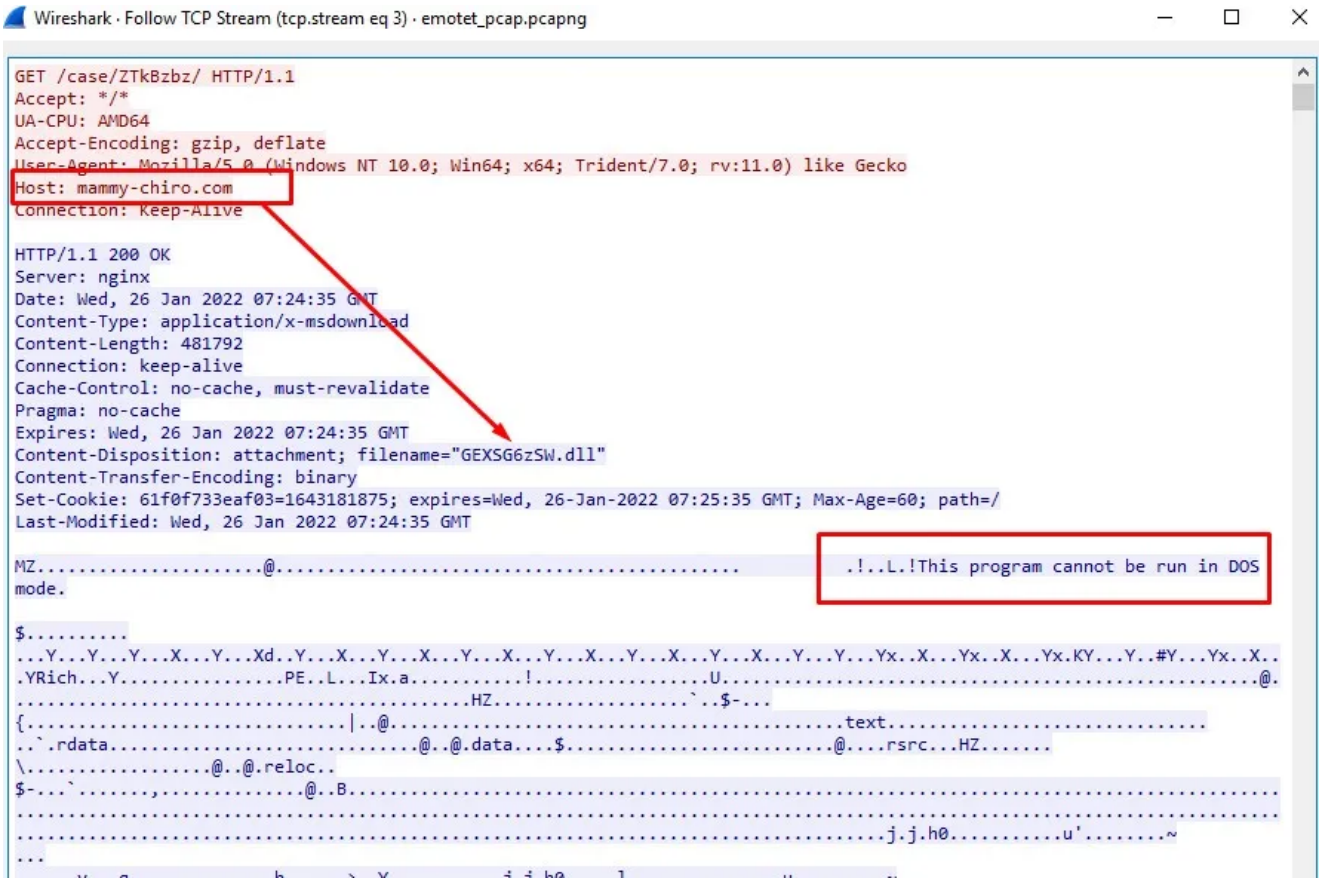


Analysis Malware emotet running activeX

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



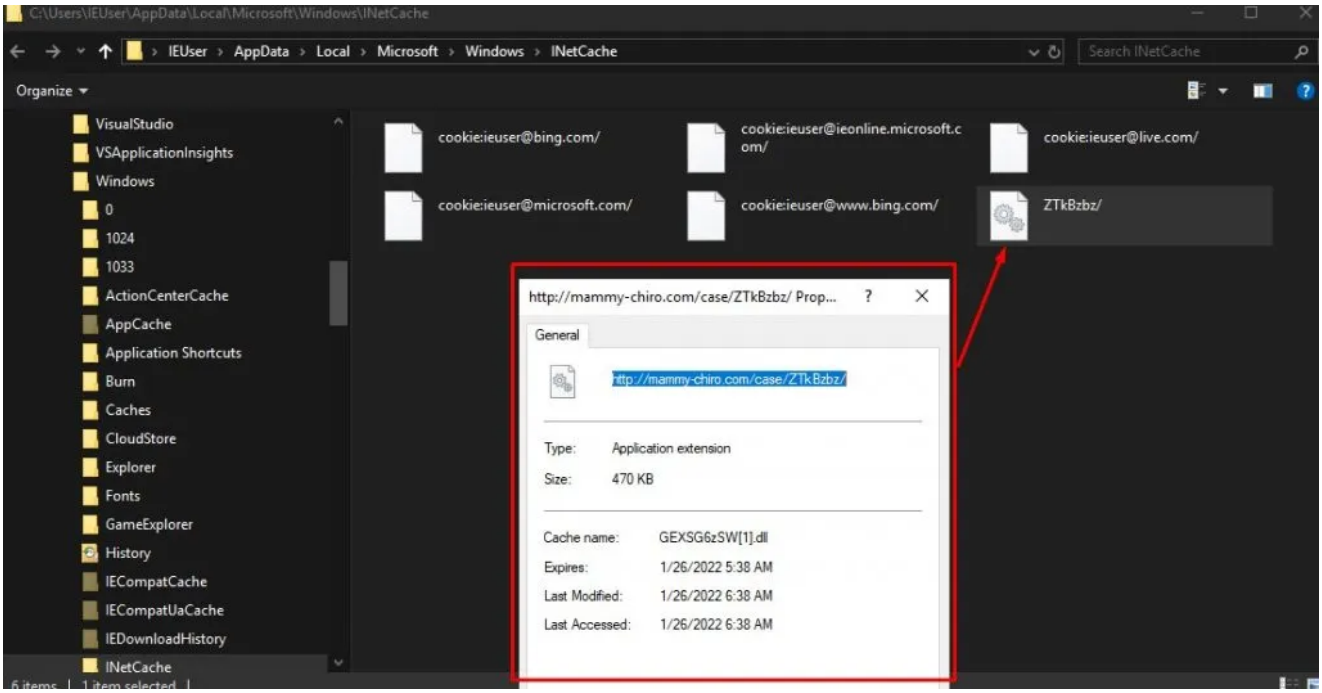
Drop dll Analysis Malware emotet



Download file malware emotet

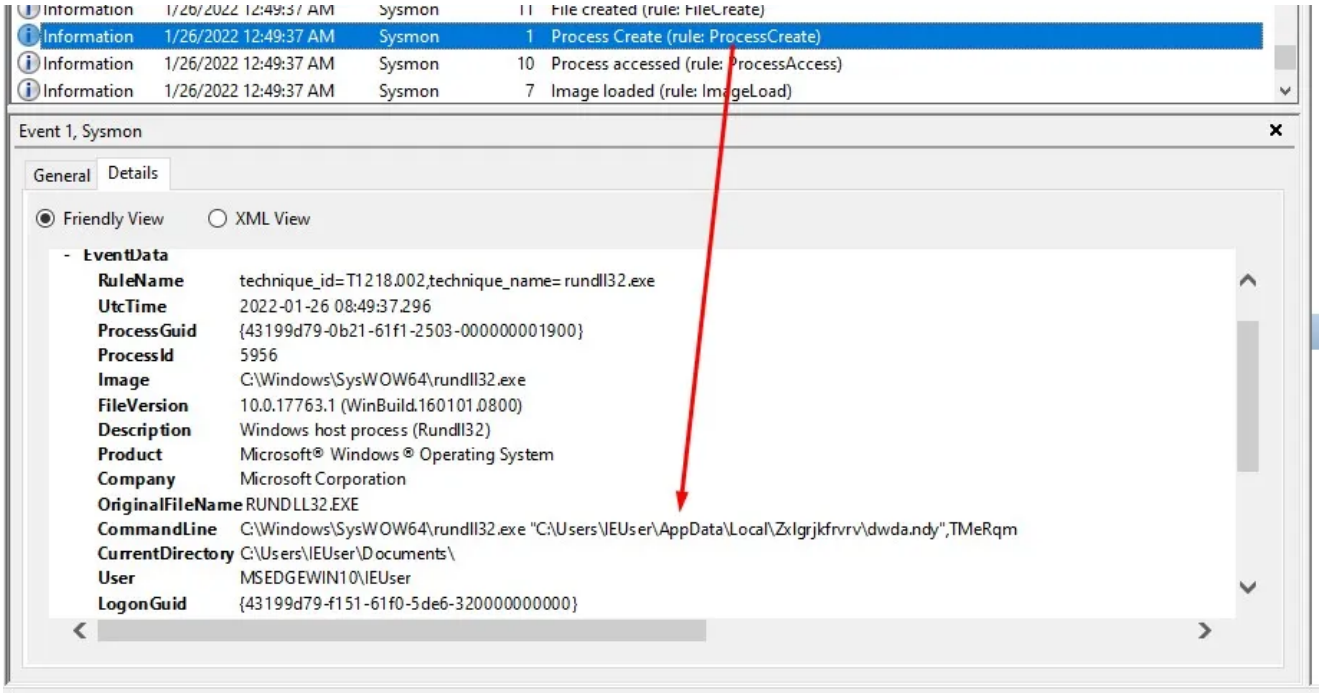
Komunikasi diatas diawali dengan **DNS Request** untuk melihat apakah domain memiliki response **200**, ketika respons didapatkan malware emotet akan melanjutkan dengan melakukan **Three–way handshake** dan mendrop dll malware menggunakan fungsi **activeX** yang sebelumnya pada file **dwa.ocx**. File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

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



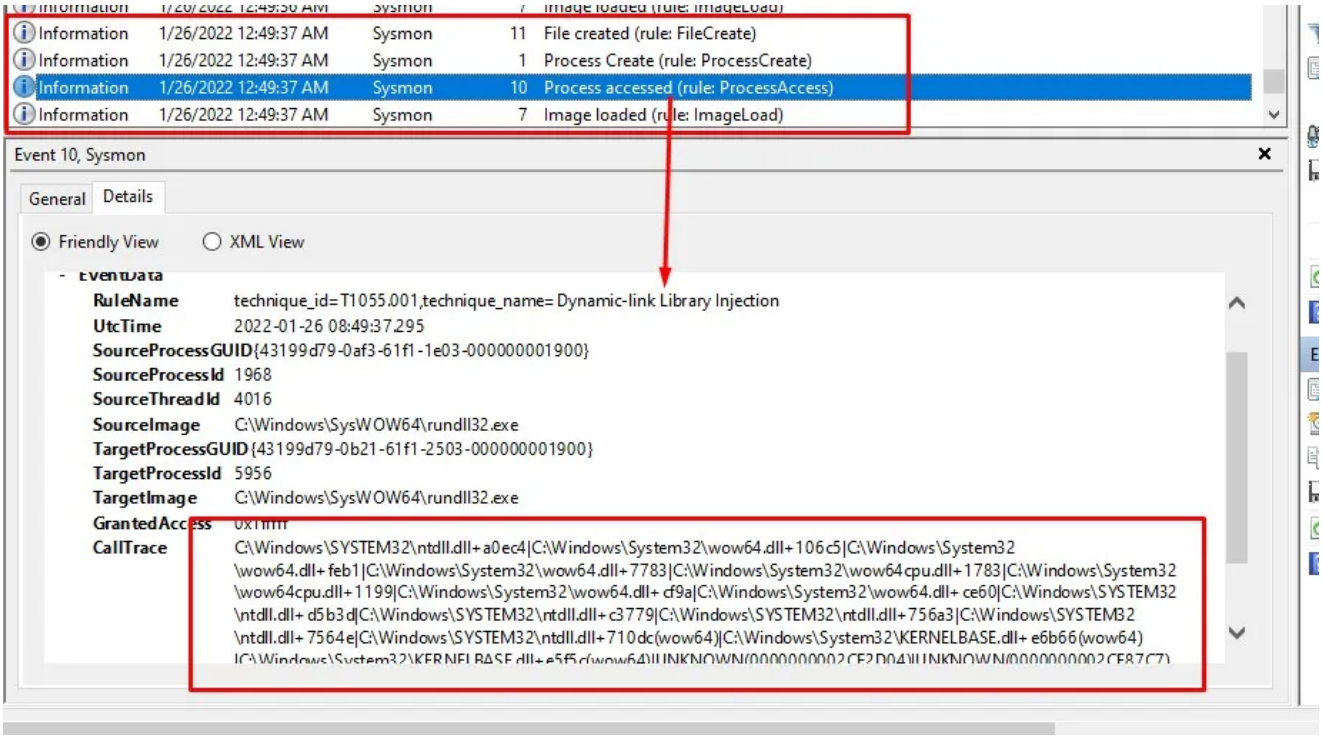
Analysis Malware emotet drop dll file

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



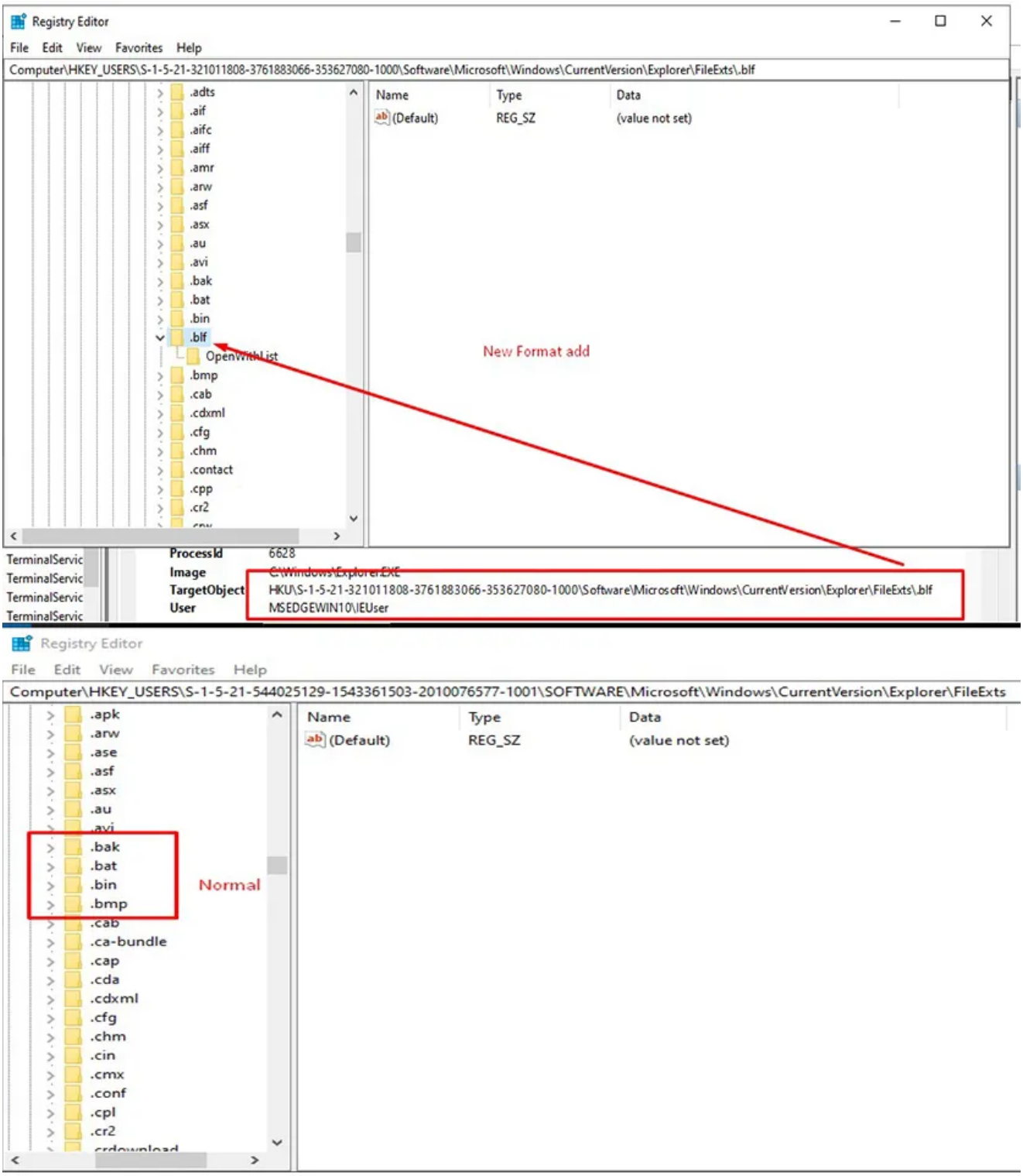
Analysis Malware emotet running uniqe file

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

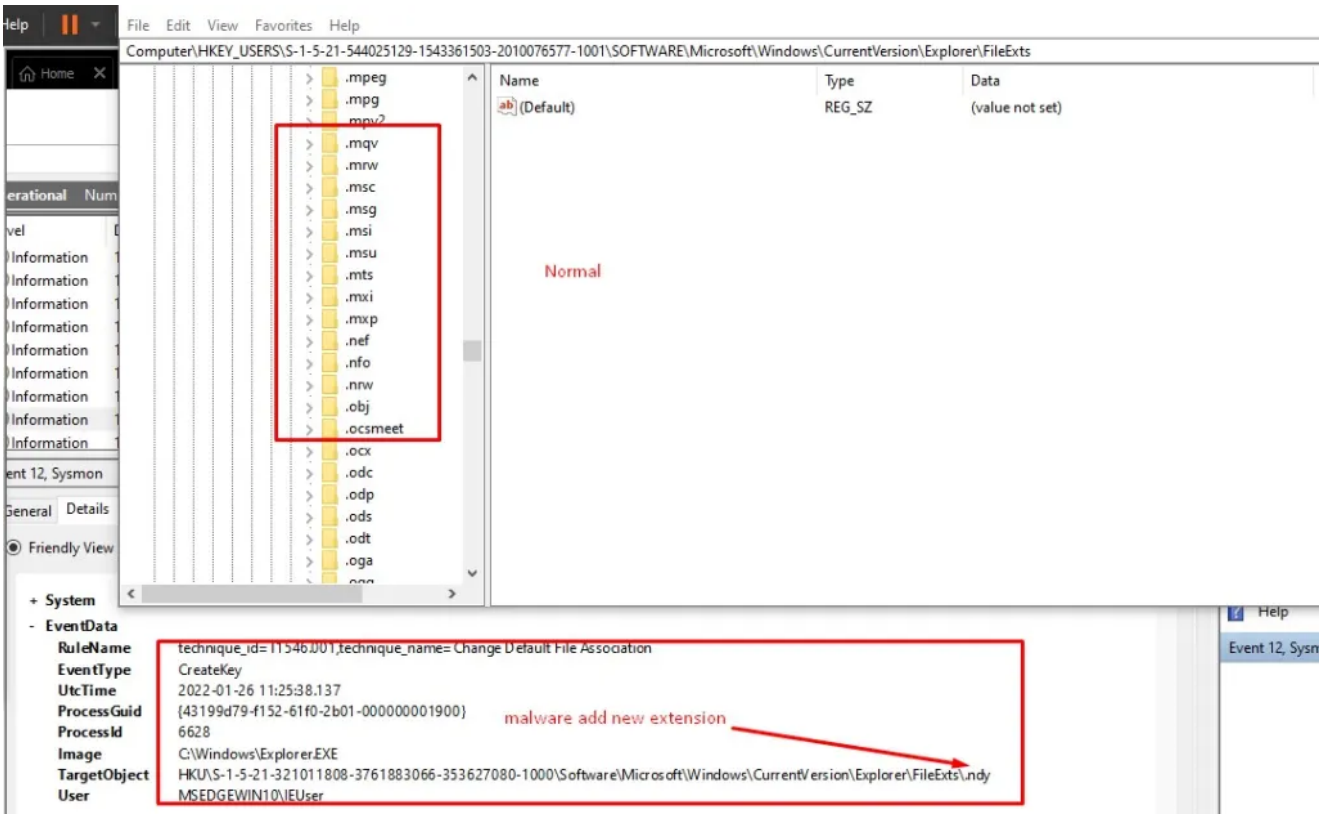


Analysis Malware Emotet Dynamic-link Library injection

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.

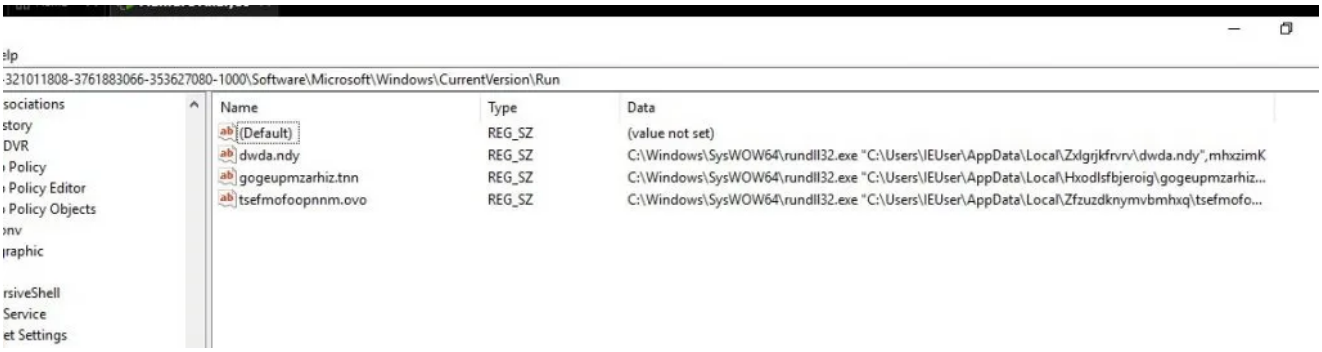


Analysis Malware Emotet Add new extension



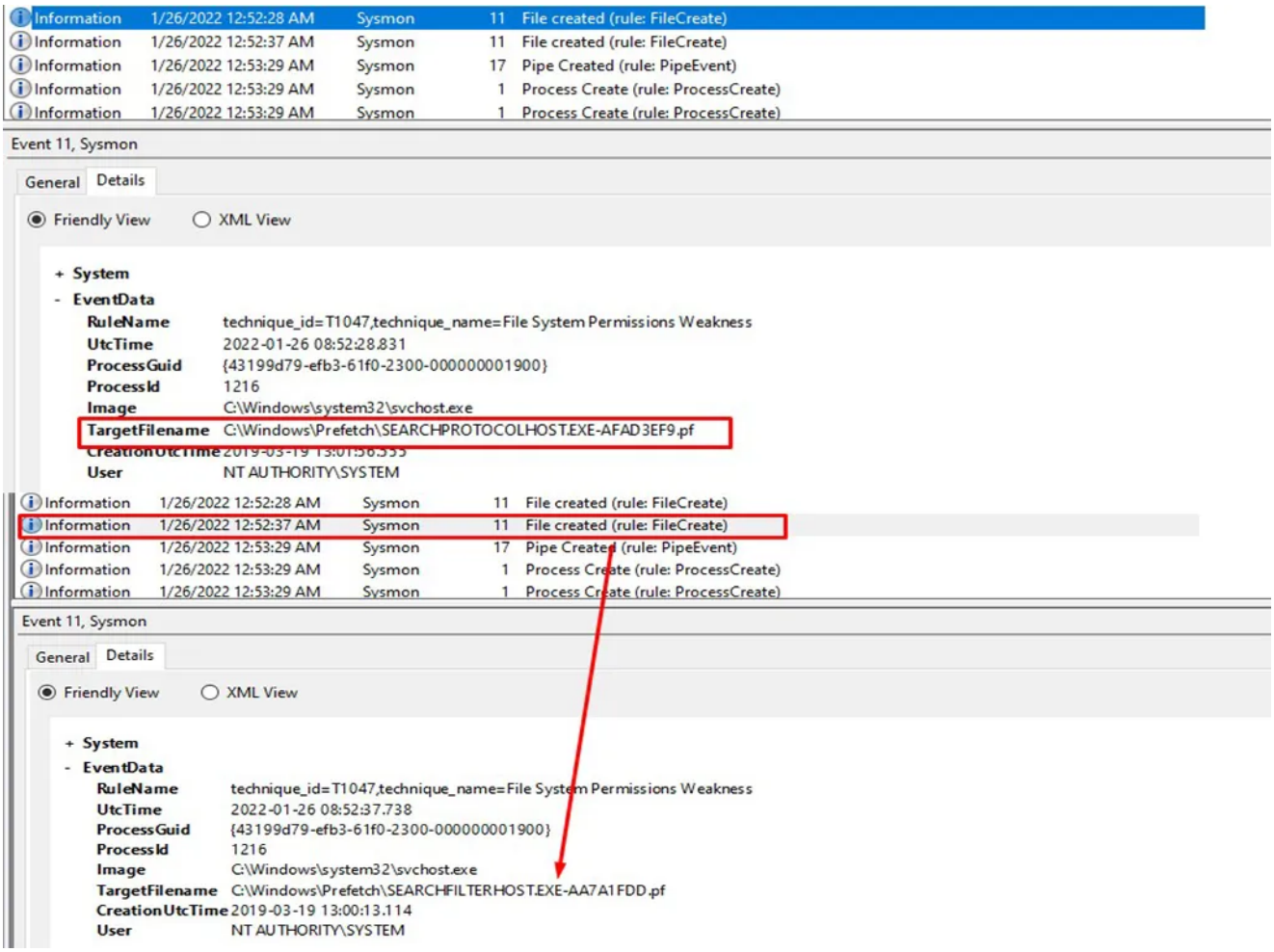
Add another new extension Analysis Malware emotet

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



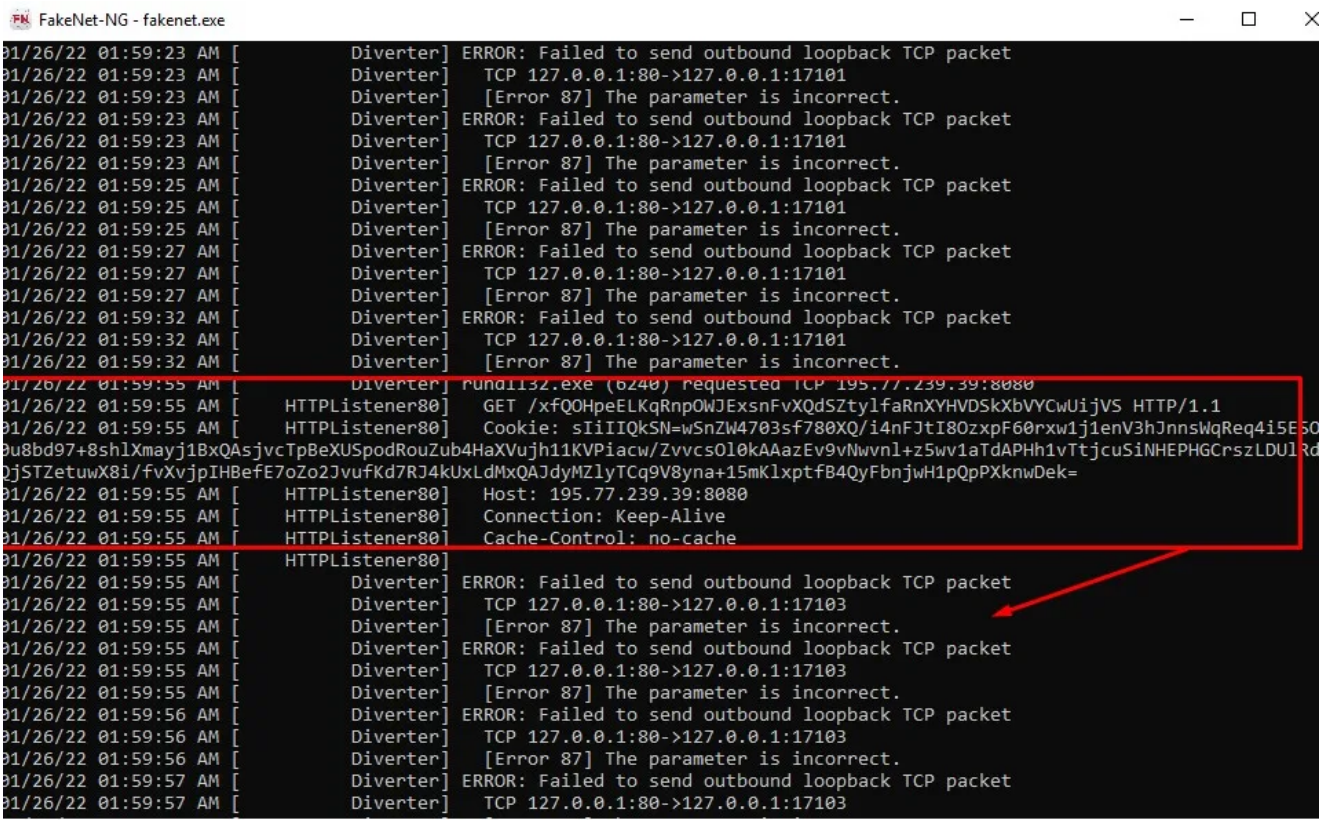
Registry Analysis Malware Emotet autorun

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



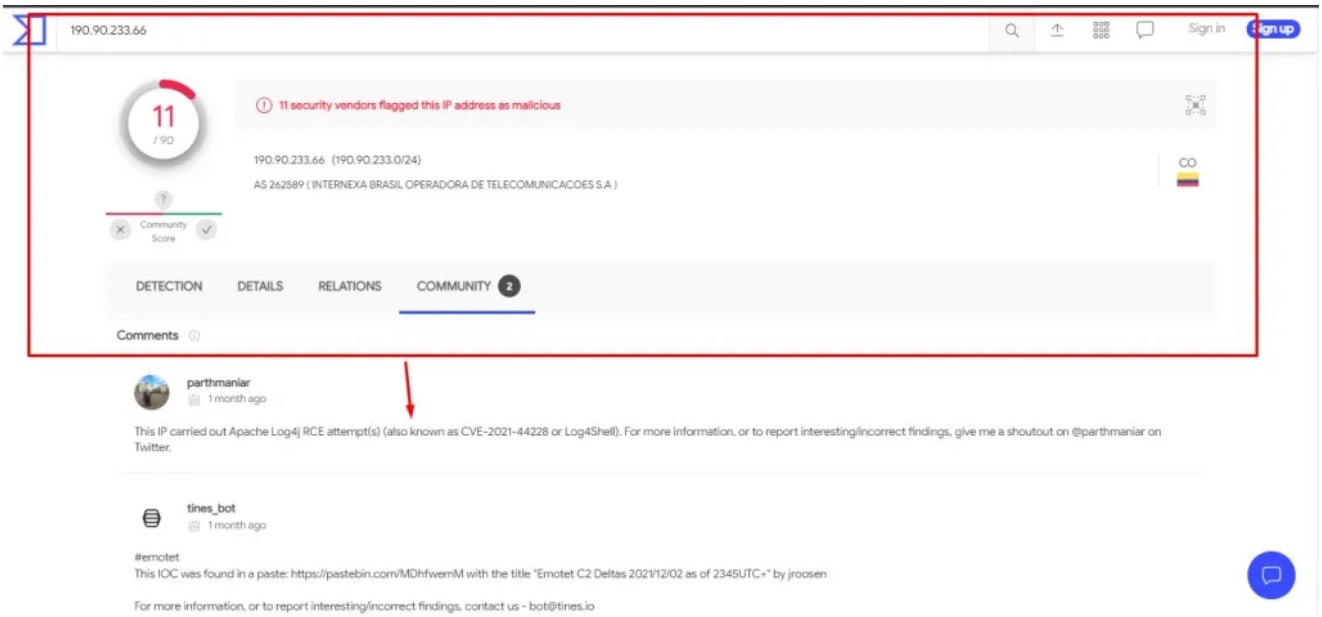
Analysis Malware Emotet Search host and protocol

Ketika proses infeksinya 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.



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 lainya)`
  `C:\Users\IEUser\AppData\Local\{uniqe folder}\{uniqe 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 {.ndy, .tnn, .ovo, .blf}` **`note: format emotet masih banyak ini hanya sebagaian 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