Advanced Persistent Threat (APT)

Sinem Ozden – Ozan Emre Sayilir

This paper 3 main parts. The first aim of this paper is to give a through explanation to the Advanced Persistent Attack, its behavior and how it's different from other malware types. The second part is giving a brief explanation of Emotet and how it has the APT characteristics. Finally, statically and dynamically analyzing a selected Emotet Trojan and prove why Emotet is considered as an APT.

1. What is APT

An Advanced Persistent Attack is a malware type that allows attacker to gain access to a system or a network. Its aim is to remain undetected and access to sensitive data of the target and remain in the system for an extended period of time to complete its mission. The APT won't cause an actual damage to the computer. However, it will embed itself with the system or network and gather data. Then it will send the data that is collected from user or network and send it to the attacker in specific time periods. It also monitors the network. The of this attack is to generally data theft.

APT is generally sponsored by a government or state-sponsored group but in recent times non-state sponsored groups also start to create APT. The targets and attack type are selected before preparing the attack. APT generally targets big companies or government and governmental establishments. Thus, the creation and spreading an APT malware requires a high budget. The type of data that is collected and the motive varies. Some attacks gain competitive advantage by collecting data others infrastructure systems such as power distribution. However, the main motive is of all them is either economical or political.

2. How Does APT Spread

The APT has various spread methods. The attackers generally use social engineering methods. Social engineering is tricking users to give sensitive information or trick to download a malware that looks like an actual program. One example of social engineering is planting a malware to an E-Mail that looks from a real person. Another spread method is planting malware on a website that the victim's employees likely to visit. Attackers try to trick the target to download the APT by using different types of approaches. But of these software, E-Mail or websites look real so that the target won't get suspicious.

Another social engineering method that used by attackers is spear phishing. Unlike spam mails the spear phishing creates customized mails with malicious attachments. The context of these mails is to trick the target and motive to download the APT. These types of attack require research about the target's hierarchical organization. For example, by disguising as a person's boss or someone from IT the attacker tries to trick the target to download.

Another spread method of APT is zero-day exploit. Zero-day exploit is attacker to take advantage of a software's vulnerabilities, bugs that creates security holes, to infiltrate a system. These vulnerabilities generally not known by the developer or the users so, there is no protection regarding the bug because the developers are oblivious to threat. Some zero-day exploits occur even though the developer is aware of the vulnerability. However, attacker can achieve its goal before developers fix the bug. In some cases, to not send too much update to the users, developers can wait and send a collective update that fixes several bugs in the system. Zero-day attacks occur within a time frame, known as the vulnerability window. In this window time attackers create the malicious code to exploit the system. The window time can change from few days to several years.

3. *The A, P, T Attributes*

Advanced: The APT malware considered as advanced because it's a combination of multiple targeting methods, tools, and techniques to reach and compromise target. Also because it generally take advantage of a zero day attack that has malware payloads and uses kernel rootkits and evasion detection technologies that are more advanced compare to other malware types, makes APT more advanced.

Persistent: APT malware continuously monitoring and does interactions to achieve objectives. Unlike other malware it does not attempt constant attacks and malware updates after it infiltrated to the system. Its try to stay "low-and-slow" to stay in the system longer. The goals are to maintain long-term access to the target, in contrast to threats who only access to execute a specific task short and fast. The part of APT that makes it ft the attribute persistent if the access lost, the user notices the malware and remove it from the system the attacker reattempt access, and most often, successfully re-access the system.

Threat: APTs are a difficult to detect threat, because until detected they can stay in their host system up to years and gather data continuously. Also, the attacks are executed by coordinated human actions (sponsored by nation states or organizations that can produce similar resources) so the target is specific and toughly researched to create the best attack that can infiltrate the system and collect data. Because these projects are very well funded, creating a malware that can infiltrate the system is almost guaranteed.

4. *The Life Cycle*

- **Initial compromise** is the stage of entering the system. This is generally done by social engineering, via E-Mail, or using zero-day exploits.
- **Establish Foothold** is the stage where after entering the target machine the malware plants a remote administration software in victim's network. This software creates tunnels and net backdoors allowing access to its infrastructure.
- **Escalate privileges** is the stage malware uses exploits and password cracking to acquire administrator privileges at the targets machine.
- **Internal reconnaissance** in this stage the malware starts to collect information on infrastructure. Malware gathers information such as trust relationships, Windows domain structure.

- **Move laterally** is the stage of malware's control expands to other devices in the system, the servers and all kinds of infrastructure elements. After infiltrating these new devices the malware starts to harvest data on them.
- **Maintain presence** is crucial to APT. APT tried to stay undetected to the system and tries to ensure continued control over access channels and credentials acquired in previous stages.
- **Completing the mission** after getting the information to complete the mission APT successful filtrate stolen data from victim's network back to attacker.

5. What is Emotet

Emotet is an APT trojan that is primarily spread through phishing E-Mails that contains macro-enabled document files, or malicious links. These mails try to convince the target to click on malicious script my using key words such as "Your Invoice," "Payment Details," or an unknown upcoming shipment.

The first identified Emotet was in 2014 and through the years Emotet has gone through a few changes compare to start. Early versions were delivered as a malicious JavaScript file. Later versions use macro-enabled Office documents to retrieve a malicious payload from a C&C server. It also uses C&C service to get updates. Because it works similar to operating system updates malware can stay undetected. By using C&C it can also download other banking trojans or used as a vault for stolen information.

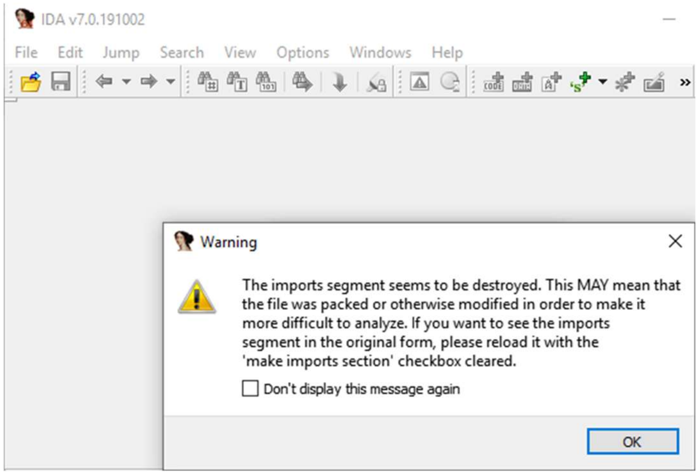
The early versions of Emotet's aim was to steal bank account details via intercepting internet traffic. In later versions includes new objectives such as money transfer systems. Emotet also have extra modules for creating and disturbing spam mails. After infiltrating to the system Emotet ransacks targets contacts list and send mail to everyone in the list. Because the mails are sent from target it looks more real and convincing to click links or download files. After Emotet infects the device it tries to infect other devices on network.

Because main aim of Emotet is everything financial it targets to everyone including individuals, companies and governments. Because it's a banking trojan it is considered one of the most destructive malwares. One of the examples of Emotet victims is city of Allentown. To remove the Emotet from the system direct help from Microsoft was required which cost more the one million dollars. The town had to shut down some of the financial and public safety operations because Trojan also spread to camera surveillance network.

6. Our Emotet

The Emotet sample we found first appeared in beginning of 2019. The trojan was hiding in a Word file which is no longer available. When the Word file open by using macros, shortcut bindings that run procedures set up before, it starts to execute itself.

The macros procedure creates a PowerShell process which tries to download the payload from five different websites, where we found the our Emotet to use. We the payload we picked was SHA256: 21145645cac74e0b590813eafd257a2c4af6c6be0bc86d873ad0e6c005c0911d. We had to download it from a separate platform because the websites used by word document were no longer available. The name of our payload was the same with its SHA256 code. We first tried to examine this executable file. However, because it was packed, the IDE we used gave us a warning it might be harder to analyze. To unpack it we decided to run the executable file.

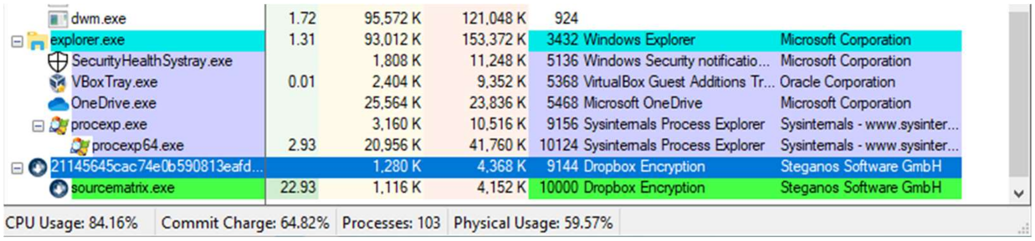


Warning

The imports segment seems to be destroyed. This MAY mean that the file was packed or otherwise modified in order to make it more difficult to analyze. If you want to see the imports segment in the original form, please reload it with the 'make imports section' checkbox cleared.

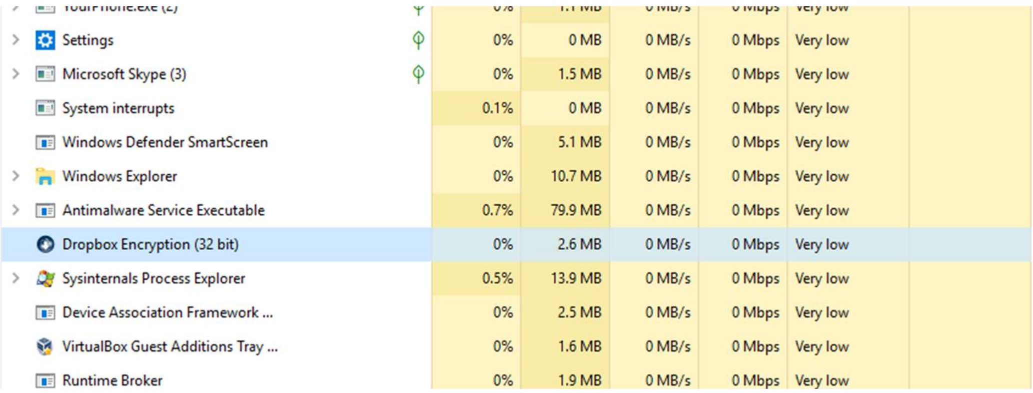
□ Don't display this message again

When we run the executable file and watch it with process manager. In process manager we could observe that the payload run another executable called sourcematrix.exe. The both of these executable's description was Dropbox Encryption. We can also see the Dropbox Encryption running at Task Manager. After the first executed executable deleted from the hard disk. We could no longer found it in the downloaded file. However, we tracked the sourcematrix.exe in another part of the computer. It created itself a directory with a same name. When double click on the sourcematrix.exe Windows won't allow user access.



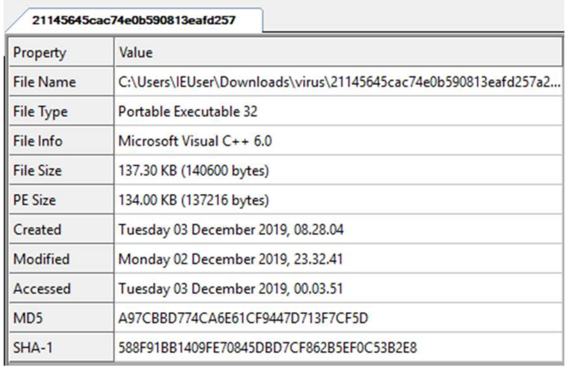
dwm.exe	1.72	95,572 K	121,048 K	924		
explorer.exe	1.31	93,012 K	153,372 K	3432	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,808 K	11,248 K	5136	Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	0.01	2,404 K	9,352 K	5368	VirtualBox Guest Additions Tr...	Oracle Corporation
OneDrive.exe		25,564 K	23,836 K	5468	Microsoft OneDrive	Microsoft Corporation
procexp.exe		3,160 K	10,516 K	9156	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	2.93	20,956 K	41,760 K	10124	Sysinternals Process Explorer	Sysinternals - www.sysinter...
21145645cac74e0b590813eafd...		1,280 K	4,368 K	9144	Dropbox Encryption	Steganos Software GmbH
sourcematrix.exe	22.93	1,116 K	4,152 K	10000	Dropbox Encryption	Steganos Software GmbH

CPU Usage: 84.16% Commit Charge: 64.82% Processes: 103 Physical Usage: 59.57%



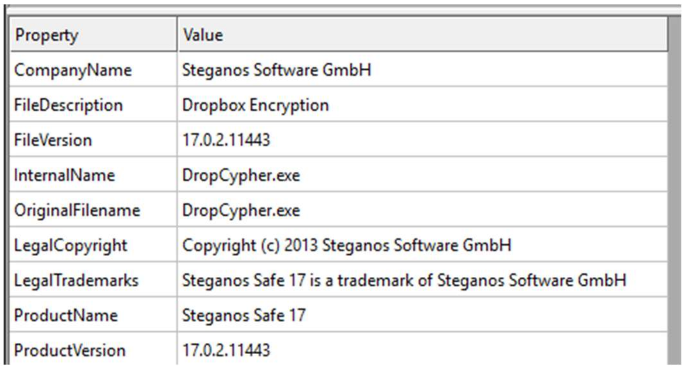
YourPhone.exe (2)	0%	1.1 MB	0 MB/s	0 Mbps	Very low
Settings	0%	0 MB	0 MB/s	0 Mbps	Very low
Microsoft Skype (3)	0%	1.5 MB	0 MB/s	0 Mbps	Very low
System interrupts	0.1%	0 MB	0 MB/s	0 Mbps	Very low
Windows Defender SmartScreen	0%	5.1 MB	0 MB/s	0 Mbps	Very low
Windows Explorer	0%	10.7 MB	0 MB/s	0 Mbps	Very low
Antimalware Service Executable	0.7%	79.9 MB	0 MB/s	0 Mbps	Very low
Dropbox Encryption (32 bit)	0%	2.6 MB	0 MB/s	0 Mbps	Very low
Sysinternals Process Explorer	0.5%	13.9 MB	0 MB/s	0 Mbps	Very low
Device Association Framework ...	0%	2.5 MB	0 MB/s	0 Mbps	Very low
VirtualBox Guest Additions Tray ...	0%	1.6 MB	0 MB/s	0 Mbps	Very low
Runtime Broker	0%	1.9 MB	0 MB/s	0 Mbps	Very low

Then we decided to look at the file properties of this payload. The payload is a C++ file that has Win32 API functions. We could also confirm the process manager and task manager that to a user this trojan looks like a Dropbox executable. We could also see the information such as when we created and download this file. The trademark of the creator can also be seen in the description. We also found the DLL’s which used in the code.

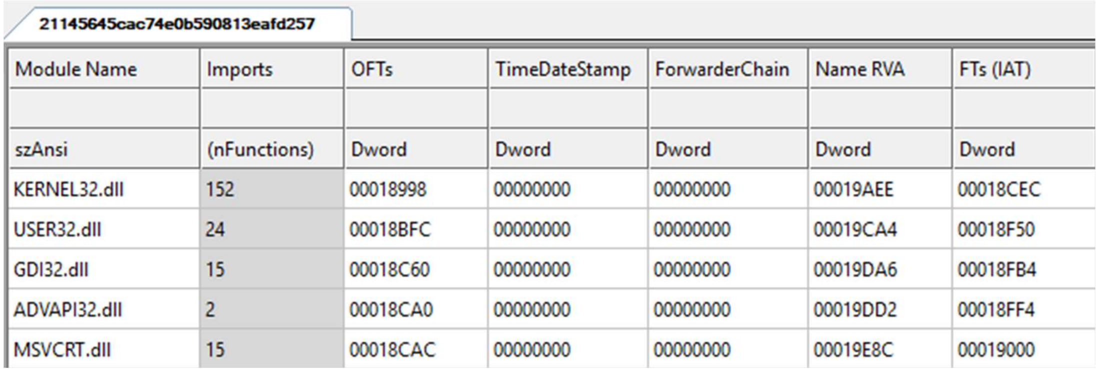


21145645cac74e0b590813eafd257

Property	Value
File Name	C:\Users\IEUser\Downloads\virus\21145645cac74e0b590813eafd257a2...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	137.30 KB (140600 bytes)
PE Size	134.00 KB (137216 bytes)
Created	Tuesday 03 December 2019, 08.28.04
Modified	Monday 02 December 2019, 23.32.41
Accessed	Tuesday 03 December 2019, 00.03.51
MD5	A97CBBD774CA6E61CF9447D713F7CF5D
SHA-1	588F91BB1409FE70845DBD7CF862B5EF0C53B2E8



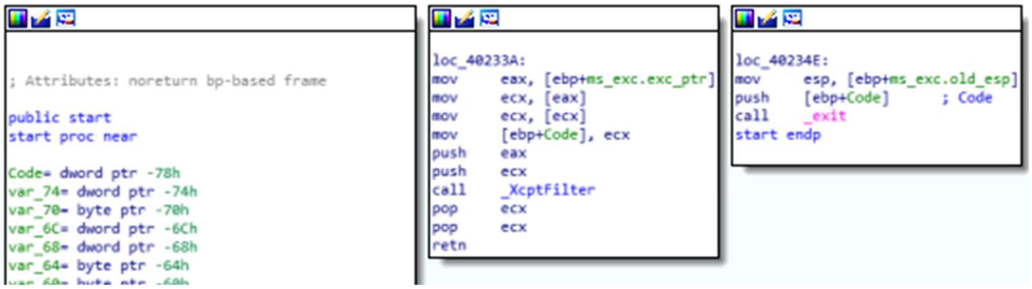
Property	Value
CompanyName	Steganos Software GmbH
FileDescription	Dropbox Encryption
FileVersion	17.0.2.11443
InternalName	DropCypher.exe
OriginalFilename	DropCypher.exe
LegalCopyright	Copyright (c) 2013 Steganos Software GmbH
LegalTrademarks	Steganos Safe 17 is a trademark of Steganos Software GmbH
ProductName	Steganos Safe 17
ProductVersion	17.0.2.11443



21145645cac74e0b590813eafd257

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	152	00018998	00000000	00000000	00019AEE	00018CEC
USER32.dll	24	00018BFC	00000000	00000000	00019CA4	00018F50
GDI32.dll	15	00018C60	00000000	00000000	00019DA6	00018FB4
ADVAPI32.dll	2	00018CA0	00000000	00000000	00019DD2	00018FF4
MSVCRT.dll	15	00018CAC	00000000	00000000	00019E8C	00019000

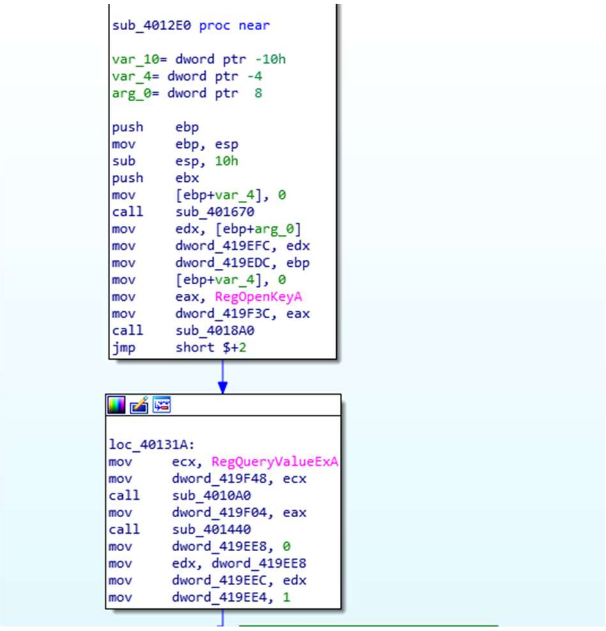
When we tried to analyze the sourcematrix.exe with IDE it was still packed. We suspect that the right two subroutines that aren’t connecting to any other maybe packer that payload has. Thus, we unpacked it with another program.



```
; Attributes: noreturn bp-based frame

public start
start proc near

Code= dword ptr -78h
var_74= dword ptr -74h
var_70= byte ptr -70h
var_6C= dword ptr -6Ch
var_68= dword ptr -68h
var_64= byte ptr -64h
```

```
loc_40233A:
mov     eax, [ebp+ms_exc.exc_ptr]
mov     ecx, [eax]
mov     ecx, [ecx]
mov     [ebp+Code], ecx
push    eax
push    ecx
call    _XcptFilter
pop     ecx
pop     ecx
retn
```

```
loc_40234E:
mov     esp, [ebp+ms_exc.old_esp]
push    [ebp+Code]      ; Code
call    _exit
start endp
```

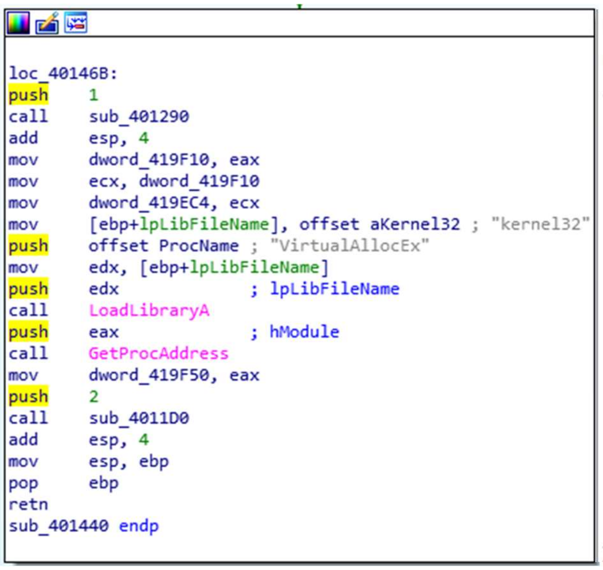


```
sub_4012E0 proc near

var_10= dword ptr -10h
var_4= dword ptr -4
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
sub     esp, 10h
push    ebx
mov     [ebp+var_4], 0
call    sub_401670
mov     edx, [ebp+arg_0]
mov     dword_419EFC, edx
mov     dword_419EDC, ebp
mov     [ebp+var_4], 0
mov     eax, RegOpenKeyA
mov     dword_419F3C, eax
call    sub_4018A0
jmp     short $+2
```

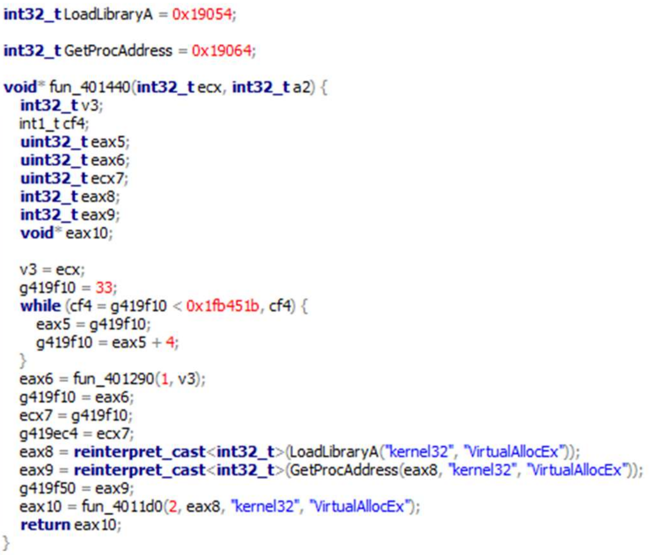
```
loc_40131A:
mov     ecx, RegQueryValueExA
mov     dword_419F48, ecx
call    sub_4010A0
mov     dword_419F04, eax
call    sub_401440
mov     dword_419EE8, 0
mov     edx, dword_419EE8
mov     dword_419EEC, edx
mov     dword_419EE4, 1
```

We found a few suspicious looking subroutines. The subroutine 4012d0 is called towards the end of the big process. This subroutine then calls 4012e0 subroutine. In this subroutine the suspicious and possible malicious intended code starts. The suspicions subroutines contained win32 functions such as RegOpenKeyA and RegQueryValueExA. The RegOpenKeyA and RegQueryValueExA are win32 registry functions. These functions extract the content of the registry keys. In the registry keys the information such as user preferences and settings kept. These functions in the image probably used for getting user information. This subroutine the calls 401440 subroutine to allocate a memory.

In subroutine 401440 the VirtualAllocEx function allocates a space in memory for the program. In this memory that allocated information which was copied from a specific address is kept. The information that kept in this space is probably the information extracted from the registers in previous subroutine. After the allocation the program jumps subroutine 4011D0

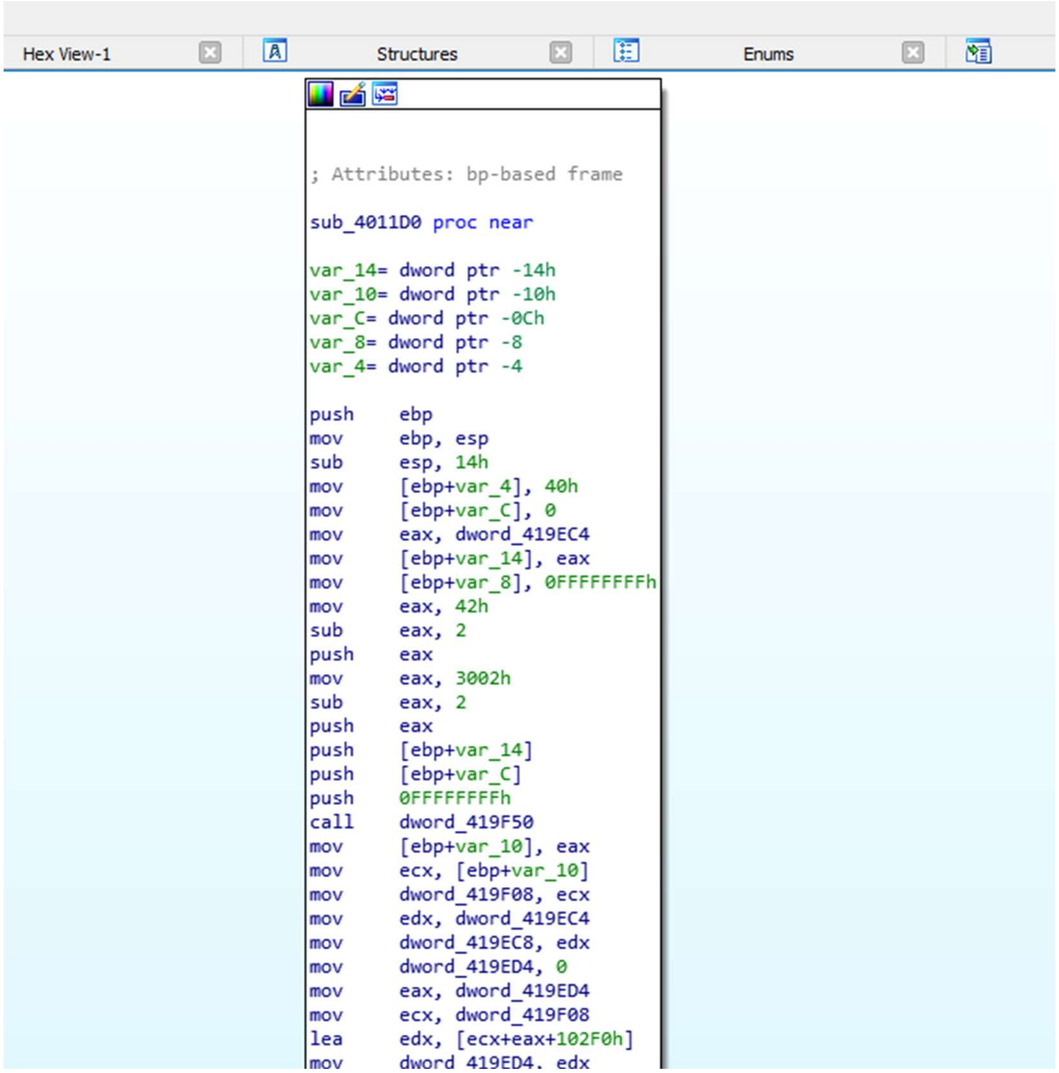


```
loc_40146B:
push    1
call    sub_401290
add     esp, 4
mov     dword_419F10, eax
mov     ecx, dword_419F10
mov     dword_419EC4, ecx
mov     [ebp+lpLibFileName], offset aKernel32 ; "kernel32"
push    offset ProcName ; "VirtualAllocEx"
mov     edx, [ebp+lpLibFileName]
push    edx             ; lpLibFileName
call    LoadLibraryA
push    eax             ; hModule
call    GetProcAddress
mov     dword_419F50, eax
push    2
call    sub_4011D0
add     esp, 4
mov     esp, ebp
pop     ebp
retn
sub_401440 endp
```



```
int32_t LoadLibraryA = 0x19054;

int32_t GetProcAddress = 0x19064;

void* fun_401440(int32_t ecx, int32_t a2) {
  int32_t v3;
  int1_t cf4;
  uint32_t eax5;
  uint32_t eax6;
  uint32_t ecx7;
  int32_t eax8;
  int32_t eax9;
  void* eax10;

  v3 = ecx;
  g419f10 = 33;
  while (cf4 = g419f10 < 0x1fb451b, cf4) {
    eax5 = g419f10;
    g419f10 = eax5 + 4;
  }
  eax6 = fun_401290(1, v3);
  g419f10 = eax6;
  ecx7 = g419f10;
  g419ec4 = ecx7;
  eax8 = reinterpret_cast<int32_t>(LoadLibraryA("kernel32", "VirtualAllocEx"));
  eax9 = reinterpret_cast<int32_t>(GetProcAddress(eax8, "kernel32", "VirtualAllocEx"));
  g419f50 = eax9;
  eax10 = fun_4011d0(2, eax8, "kernel32", "VirtualAllocEx");
  return eax10;
}
```

The subroutine 4011D0 encrypts the allocated space.



```
; Attributes: bp-based frame

sub_4011D0 proc near

var_14= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 14h
mov     [ebp+var_4], 40h
mov     [ebp+var_C], 0
mov     eax, dword_419EC4
mov     [ebp+var_14], eax
mov     [ebp+var_8], 0FFFFFFFFh
mov     eax, 42h
sub     eax, 2
push    eax
mov     eax, 3002h
sub     eax, 2
push    eax
push    [ebp+var_14]
push    [ebp+var_C]
push    0FFFFFFFFh
call    dword_419F50
mov     [ebp+var_10], eax
mov     ecx, [ebp+var_10]
mov     dword_419F08, ecx
mov     edx, dword_419EC4
mov     dword_419EC8, edx
mov     dword_419ED4, 0
mov     eax, dword_419ED4
mov     ecx, dword_419F08
lea     edx, [ecx+eax+102F0h]
mov     dword_419ED4, edx
```

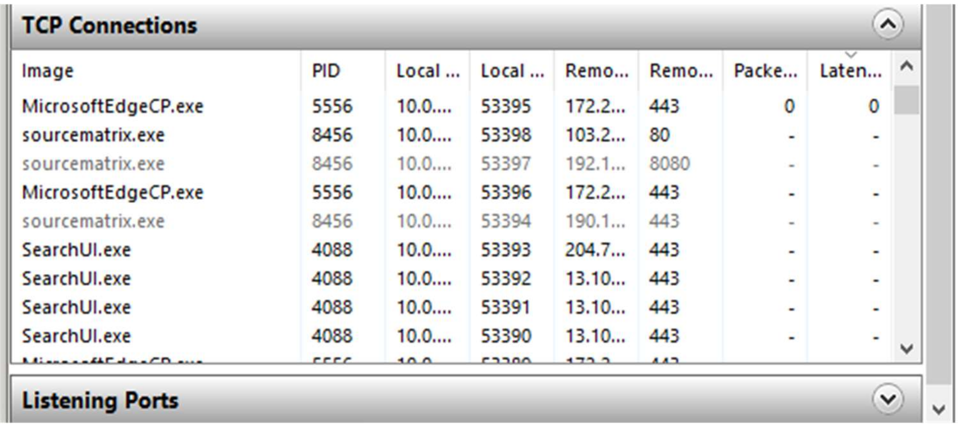
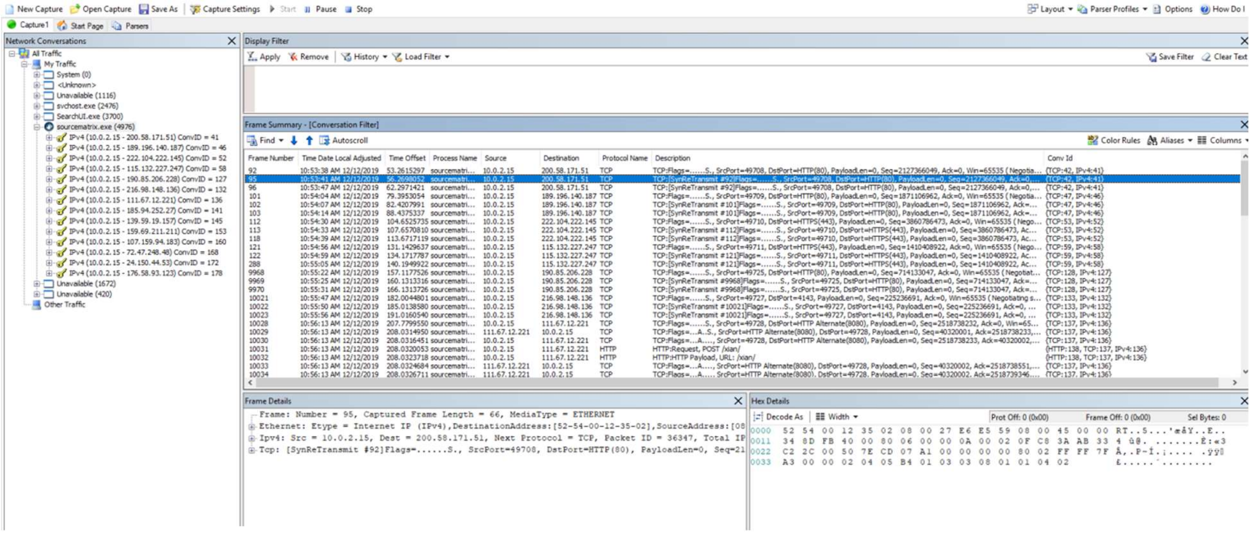


Image	PID	Local ...	Local ...	Remo...	Remo...	Packe...	Laten...
MicrosoftEdgeCP.exe	5556	10.0....	53395	172.2...	443	0	0
sourcematrix.exe	8456	10.0....	53398	103.2...	80	-	-
sourcematrix.exe	8456	10.0....	53397	192.1...	8080	-	-
MicrosoftEdgeCP.exe	5556	10.0....	53396	172.2...	443	-	-
sourcematrix.exe	8456	10.0....	53394	190.1...	443	-	-
SearchUI.exe	4088	10.0....	53393	204.7...	443	-	-
SearchUI.exe	4088	10.0....	53392	13.10...	443	-	-
SearchUI.exe	4088	10.0....	53391	13.10...	443	-	-
SearchUI.exe	4088	10.0....	53390	13.10...	443	-	-

Then we checked if the program was connected to internet. In resource monitor we could see that the sourcematrix.exe was connected to the internet and used it actively.



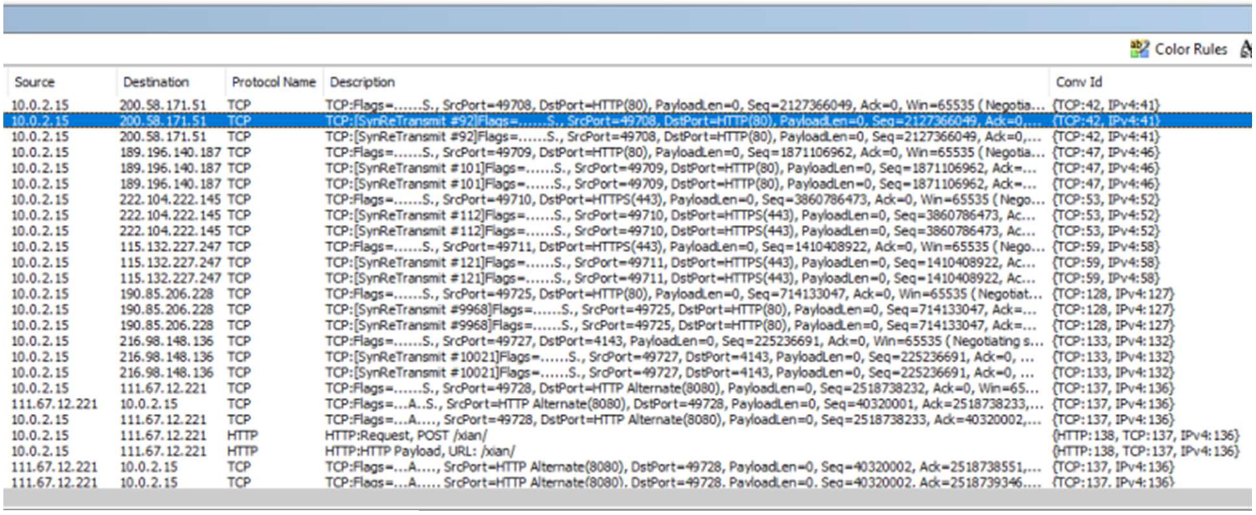
```
All Traffic
  My Traffic
    System (0)
    <Unknown>
    Unavailable (1116)
    svchost.exe (2476)
    SearchUI.exe (3700)
    sourcematrix.exe (4976)
      IPv4 (10.0.2.15 - 200.58.171.51) ConvID = 41
      IPv4 (10.0.2.15 - 189.196.140.187) ConvID = 46
      IPv4 (10.0.2.15 - 222.104.222.145) ConvID = 52
      IPv4 (10.0.2.15 - 115.132.227.247) ConvID = 58
      IPv4 (10.0.2.15 - 190.85.206.228) ConvID = 127
      IPv4 (10.0.2.15 - 216.98.148.136) ConvID = 132
      IPv4 (10.0.2.15 - 111.67.12.221) ConvID = 136
      IPv4 (10.0.2.15 - 185.94.252.27) ConvID = 141
      IPv4 (10.0.2.15 - 139.59.19.157) ConvID = 145
      IPv4 (10.0.2.15 - 159.69.211.211) ConvID = 153
      IPv4 (10.0.2.15 - 107.159.94.183) ConvID = 160
      IPv4 (10.0.2.15 - 72.47.248.48) ConvID = 168
      IPv4 (10.0.2.15 - 24.150.44.53) ConvID = 172
      IPv4 (10.0.2.15 - 176.58.93.123) ConvID = 178
    Unavailable (1672)
    Unavailable (420)
  Other Traffic
```

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description	Conv Id
92	10:53:38 AM 12/12/2019	53.2615297	sourcematri...	10.0.2.15	200.58.171.51	TCP	TCP:Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0, Win=65535 (Negotia...	{TCP:42, IPv4:41}
95	10:53:41 AM 12/12/2019	56.2698052	sourcematri...	10.0.2.15	200.58.171.51	TCP	TCP:[SynReTransmit #92]Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0,...	{TCP:42, IPv4:41}
96	10:53:47 AM 12/12/2019	62.2971421	sourcematri...	10.0.2.15	200.58.171.51	TCP	TCP:[SynReTransmit #92]Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0,...	{TCP:42, IPv4:41}
101	10:54:04 AM 12/12/2019	79.3953054	sourcematri...	10.0.2.15	189.196.140.187	TCP	TCP:Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=0, Win=65535 (Negotia...	{TCP:47, IPv4:46}
102	10:54:07 AM 12/12/2019	82.4207991	sourcematri...	10.0.2.15	189.196.140.187	TCP	TCP:[SynReTransmit #101]Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=...	{TCP:47, IPv4:46}
103	10:54:14 AM 12/12/2019	88.4375337	sourcematri...	10.0.2.15	189.196.140.187	TCP	TCP:[SynReTransmit #101]Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=...	{TCP:47, IPv4:46}
112	10:54:30 AM 12/12/2019	104.6525735	sourcematri...	10.0.2.15	222.104.222.145	TCP	TCP:Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ack=0, Win=65535 (Nego...	{TCP:53, IPv4:52}
113	10:54:33 AM 12/12/2019	107.6570810	sourcematri...	10.0.2.15	222.104.222.145	TCP	TCP:[SynReTransmit #112]Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ac...	{TCP:53, IPv4:52}
118	10:54:39 AM 12/12/2019	113.6717119	sourcematri...	10.0.2.15	222.104.222.145	TCP	TCP:[SynReTransmit #112]Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ac...	{TCP:53, IPv4:52}
121	10:54:56 AM 12/12/2019	131.1429637	sourcematri...	10.0.2.15	115.132.227.247	TCP	TCP:Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ack=0, Win=65535 (Nego...	{TCP:59, IPv4:58}
122	10:54:59 AM 12/12/2019	134.1717787	sourcematri...	10.0.2.15	115.132.227.247	TCP	TCP:[SynReTransmit #121]Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ac...	{TCP:59, IPv4:58}
288	10:55:05 AM 12/12/2019	140.1949922	sourcematri...	10.0.2.15	115.132.227.247	TCP	TCP:[SynReTransmit #121]Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ac...	{TCP:59, IPv4:58}
9968	10:55:22 AM 12/12/2019	157.1177526	sourcematri...	10.0.2.15	190.85.206.228	TCP	TCP:Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=0, Win=65535 (Negotiat...	{TCP:128, IPv4:127}
9969	10:55:25 AM 12/12/2019	160.1313316	sourcematri...	10.0.2.15	190.85.206.228	TCP	TCP:[SynReTransmit #9968]Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=...	{TCP:128, IPv4:127}
9970	10:55:31 AM 12/12/2019	166.1313726	sourcematri...	10.0.2.15	190.85.206.228	TCP	TCP:[SynReTransmit #9968]Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=...	{TCP:128, IPv4:127}
10021	10:55:47 AM 12/12/2019	182.0044801	sourcematri...	10.0.2.15	216.98.148.136	TCP	TCP:Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, Win=65535 (Negotiating s...	{TCP:133, IPv4:132}
10022	10:55:50 AM 12/12/2019	185.0138580	sourcematri...	10.0.2.15	216.98.148.136	TCP	TCP:[SynReTransmit #10021]Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, ...	{TCP:133, IPv4:132}
10023	10:55:56 AM 12/12/2019	191.0160540	sourcematri...	10.0.2.15	216.98.148.136	TCP	TCP:[SynReTransmit #10021]Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, ...	{TCP:133, IPv4:132}
10028	10:56:13 AM 12/12/2019	207.7799550	sourcematri...	10.0.2.15	111.67.12.221	TCP	TCP:Flags=......S., SrcPort=49728, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2518738232, Ack=0, Win=65...	{TCP:137, IPv4:136}
10029	10:56:13 AM 12/12/2019	208.0314950	sourcematri...	111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A..S., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320001, Ack=2518738233,...	{TCP:137, IPv4:136}
10030	10:56:13 AM 12/12/2019	208.0316451	sourcematri...	10.0.2.15	111.67.12.221	TCP	TCP:Flags=...A...., SrcPort=49728, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2518738233, Ack=40320002,...	{TCP:137, IPv4:136}
10031	10:56:13 AM 12/12/2019	208.0320053	sourcematri...	10.0.2.15	111.67.12.221	HTTP	HTTP:Request, POST /xian/	{HTTP:138, TCP:137, IPv4:136}
10032	10:56:13 AM 12/12/2019	208.0323718	sourcematri...	10.0.2.15	111.67.12.221	HTTP	HTTP:HTTP Payload, URL: /xian/	{HTTP:138, TCP:137, IPv4:136}
10033	10:56:13 AM 12/12/2019	208.0324684	sourcematri...	111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320002, Ack=2518738551,...	{TCP:137, IPv4:136}
10034	10:56:13 AM 12/12/2019	208.0326711	sourcematri...	111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320002, Ack=2518739346,...	{TCP:137, IPv4:136}

```
Frame: Number = 95, Captured Frame Length = 66, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[52-54-00-12-35-02],SourceAddress:[08
Ipv4: Src = 10.0.2.15, Dest = 200.58.171.51, Next Protocol = TCP, Packet ID = 36347, Total IP
Tcp: [SynReTransmit #92]Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=21
```

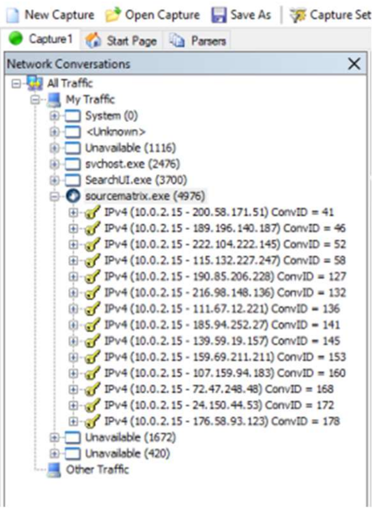
```
0000  52 54 00 12 35 02 08 00 27 E6 E5 59 08 00 45 00 00  RT..5...'æåY..E..
0011  34 8D FB 40 00 80 06 00 00 0A 00 02 0F C8 3A AB 33  4 û@. .......È:«3
0022  C2 2C 00 50 7E CD 07 A1 00 00 00 00 80 02 FF FF 7F  Â,.P~Í.¡..... .ÿÿ
0033  A3 00 00 02 04 05 B4 01 03 03 08 01 01 04 02        £.....´........
```

Image 0. Complete Screenshot



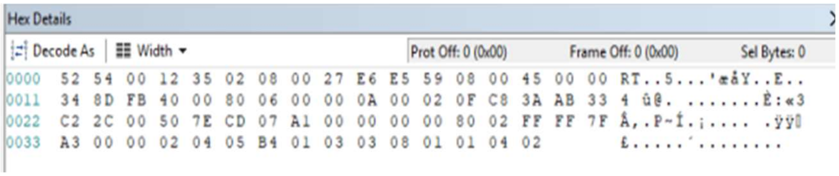
Source	Destination	Protocol Name	Description	Conv Id
10.0.2.15	200.58.171.51	TCP	TCP:Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0, Win=65535 (Negotia...	{TCP:42, IPv4:41}
10.0.2.15	200.58.171.51	TCP	TCP:[SynReTransmit #92]Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0,...	{TCP:42, IPv4:41}
10.0.2.15	200.58.171.51	TCP	TCP:[SynReTransmit #92]Flags=......S., SrcPort=49708, DstPort=HTTP(80), PayloadLen=0, Seq=2127366049, Ack=0,...	{TCP:42, IPv4:41}
10.0.2.15	189.196.140.187	TCP	TCP:Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=0, Win=65535 (Negotia...	{TCP:47, IPv4:46}
10.0.2.15	189.196.140.187	TCP	TCP:[SynReTransmit #101]Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=...	{TCP:47, IPv4:46}
10.0.2.15	189.196.140.187	TCP	TCP:[SynReTransmit #101]Flags=......S., SrcPort=49709, DstPort=HTTP(80), PayloadLen=0, Seq=1871106962, Ack=...	{TCP:47, IPv4:46}
10.0.2.15	222.104.222.145	TCP	TCP:Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ack=0, Win=65535 (Nego...	{TCP:53, IPv4:52}
10.0.2.15	222.104.222.145	TCP	TCP:[SynReTransmit #112]Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ac...	{TCP:53, IPv4:52}
10.0.2.15	222.104.222.145	TCP	TCP:[SynReTransmit #112]Flags=......S., SrcPort=49710, DstPort=HTTPS(443), PayloadLen=0, Seq=3860786473, Ac...	{TCP:53, IPv4:52}
10.0.2.15	115.132.227.247	TCP	TCP:Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ack=0, Win=65535 (Nego...	{TCP:59, IPv4:58}
10.0.2.15	115.132.227.247	TCP	TCP:[SynReTransmit #121]Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ac...	{TCP:59, IPv4:58}
10.0.2.15	115.132.227.247	TCP	TCP:[SynReTransmit #121]Flags=......S., SrcPort=49711, DstPort=HTTPS(443), PayloadLen=0, Seq=1410408922, Ac...	{TCP:59, IPv4:58}
10.0.2.15	190.85.206.228	TCP	TCP:Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=0, Win=65535 (Negotiat...	{TCP:128, IPv4:127}
10.0.2.15	190.85.206.228	TCP	TCP:[SynReTransmit #9968]Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=...	{TCP:128, IPv4:127}
10.0.2.15	190.85.206.228	TCP	TCP:[SynReTransmit #9968]Flags=......S., SrcPort=49725, DstPort=HTTP(80), PayloadLen=0, Seq=714133047, Ack=...	{TCP:128, IPv4:127}
10.0.2.15	216.98.148.136	TCP	TCP:Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, Win=65535 (Negotiating s...	{TCP:133, IPv4:132}
10.0.2.15	216.98.148.136	TCP	TCP:[SynReTransmit #10021]Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, ...	{TCP:133, IPv4:132}
10.0.2.15	216.98.148.136	TCP	TCP:[SynReTransmit #10021]Flags=......S., SrcPort=49727, DstPort=4143, PayloadLen=0, Seq=225236691, Ack=0, ...	{TCP:133, IPv4:132}
10.0.2.15	111.67.12.221	TCP	TCP:Flags=......S., SrcPort=49728, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2518738232, Ack=0, Win=65...	{TCP:137, IPv4:136}
111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A..S., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320001, Ack=2518738233,...	{TCP:137, IPv4:136}
10.0.2.15	111.67.12.221	TCP	TCP:Flags=...A...., SrcPort=49728, DstPort=HTTP Alternate(8080), PayloadLen=0, Seq=2518738233, Ack=40320002,...	{TCP:137, IPv4:136}
10.0.2.15	111.67.12.221	HTTP	HTTP:Request, POST /xian/	{HTTP:138, TCP:137, IPv4:136}
10.0.2.15	111.67.12.221	HTTP	HTTP:HTTP Payload, URL: /xian/	{HTTP:138, TCP:137, IPv4:136}
111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320002, Ack=2518738551,...	{TCP:137, IPv4:136}
111.67.12.221	10.0.2.15	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=49728, PayloadLen=0, Seq=40320002, Ack=2518739346,...	{TCP:137, IPv4:136}

Image 1. Complete Screenshot



```
All Traffic
  My Traffic
    System (0)
    <Unknown>
    Unavailable (1116)
    svchost.exe (2476)
    SearchUI.exe (3700)
    sourcematrix.exe (4976)
      IPv4 (10.0.2.15 - 200.58.171.51) ConvID = 41
      IPv4 (10.0.2.15 - 189.196.140.187) ConvID = 46
      IPv4 (10.0.2.15 - 222.104.222.145) ConvID = 52
      IPv4 (10.0.2.15 - 115.132.227.247) ConvID = 58
      IPv4 (10.0.2.15 - 190.85.206.228) ConvID = 127
      IPv4 (10.0.2.15 - 216.98.148.136) ConvID = 132
      IPv4 (10.0.2.15 - 111.67.12.221) ConvID = 136
      IPv4 (10.0.2.15 - 185.94.252.27) ConvID = 141
      IPv4 (10.0.2.15 - 139.59.19.157) ConvID = 145
      IPv4 (10.0.2.15 - 159.69.211.211) ConvID = 153
      IPv4 (10.0.2.15 - 107.159.94.183) ConvID = 160
      IPv4 (10.0.2.15 - 72.47.248.48) ConvID = 168
      IPv4 (10.0.2.15 - 24.150.44.53) ConvID = 172
      IPv4 (10.0.2.15 - 176.58.93.123) ConvID = 178
    Unavailable (1672)
    Unavailable (420)
  Other Traffic
```

Image 2. IP Addresses that Program Connects



```
0000  52 54 00 12 35 02 08 00 27 E6 E5 59 08 00 45 00 00  RT..5...'æåY..E..
0011  34 8D FB 40 00 80 06 00 00 0A 00 02 0F C8 3A AB 33  4 û@. .......È:«3
0022  C2 2C 00 50 7E CD 07 A1 00 00 00 00 80 02 FF FF 7F  Â,.P~Í.¡..... .ÿÿ
0033  A3 00 00 02 04 05 B4 01 03 03 08 01 01 04 02        £.....´........
```

Image 1. The Content of the

In the program Microsoft Network Monitor we can see that the payload connects to IP address. (image 2) The payload send them packages (image 1) which, probably contains information about process in the system. But they are encrypted. (image 3) This IP address also can send packages which can contain commands. These commands may ask payload to download updates or other malicious malware.

7. *The Programs Used*

The programs we used for analysis are:

- Microsoft Network Monitor
- IDA freeware
- Snowman
- CFF_Explorer
- ProcessExplorer
- Wireshark

8. *Conclusion*

To conclude, Emotet trojan we analyzed downloads itself to host machine via Microsoft Words macros to download itself. Then the downloaded payload creates another payload and delete itself from the disk. The new payload that created tries to learn the current running processes, host names, encode them and sends the encoded information back to the attacker. The malware register itself as a protected resource to the host system. It is hard to detect; it hides itself by taking small amount of CPU and Memory. The attacker could send payloads through the malware.