



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF COMPUTER SCIENCE (COMPUTER SECURITY) WITH HONOURS

SEMESTER 2 SESSION 18/19

**BITS 3443
DIGITAL FORENSICS**

PROJECT FORENSIC SKILL: FORENSIC ANALYSIS

GROUP MEMBERS:

No.	Student's Name	Matric No
1.	Wan Mohammad Faisal Bin Sammio	B031720043
2.	Nurul Qurratu Ain Nabilah Binti Ros Madi	B031710379
3.	Muhammad Ziqrie Bin Mustaffa	B031710264
4.	Sujaha Aniqaaah Binti Halim	B031720031
5.	Muhammad Haziq Bin Mehat	B031710190

LECTURER'S NAME: Ts.Dr.Siti Rahayu Binti Selamat

Table of Content

Objective of the analysis	1
Scope of the analysis	1
Forensics tools that used for analysis	1
Method of any analysis done in detail	2
Detail of anomalies found	3
Analysing anomalies	6
Findings/results of the analysis	17
Scenario of case	17
Conclusion of the analysis	23
Recommendation	23
Reference	24

Objective of the analysis

- To analyse network packets in order to determine the nature of the case of the attacks or source of an attack.
- To compare the evidence. We tries to do analysing on network traffic data that is collected from different tools to make our tasks easier.
- To identify and detect potentially evidence and establish detailed analytical documents.

Scope of the analysis

- The scope of this project will be focusing on analysing the EternalBlue exploitation. We are focussing on SMB protocol on port 445. In addition, we also analyse some potential malware in the packet to identify the activity or malware behaviour. Besides, anomalies are expected to be inspect by getting access to the source packet in the Wireshark.

Forensics tools that used for analysis

- **Wireshark** - Wireshark is a network packet analyser. A network packet analyser will try to capture network packets and tries to display that packet data as detailed as possible. It is used for network troubleshooting, analysis, software and communications protocol development, and education. This tool is used to inspect recorded traffic. They can be either packet-centric or session-centric.
- **NetworkMiner 2.4** - NetworkMiner is a Network Forensic Analysis Tool for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network. NetworkMiner can also parse pcap files for off-line analysis and to regenerate/reassemble transmitted files and certificates from pcap files. This tool is data-centric which analyse the traffic content.

Method of any analysis done in detail

Types of network forensic collection methods we are conducting is "Stop, look and listen." This method investigates each data packet on the network, but only grabs those that appear to be suspicious and in need of additional analysis. First things first, we must find anomalies or abnormal activity to help our analysis easier. So, we find the anomalies in the NetworkMiner and then access each of the anomalies to figure out their behaviour.

```
[2019-05-14 09:42:41 UTC] Error : Error: Exception when loading image "troll1.jpg". Parameter is not valid.
[2019-02-23 19:38:31 UTC] Error : Frame 10714 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10718 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10722 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10726 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10730 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10734 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10738 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10742 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10746 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10750 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10754 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10758 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10762 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10776 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10780 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10784 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10788 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC] Error : Frame 10792 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-05-14 09:42:44 UTC] Error : Error: Exception when loading image "win.png". Parameter is not valid.
[2019-05-14 09:42:44 UTC] Error : Error: Exception when loading image "tin.png". Parameter is not valid.
[2019-05-14 09:42:47 UTC] Error : Error: Exception when loading image "sin.png". Parameter is not valid.
[2019-05-14 09:42:48 UTC] Error : Error: Exception when loading image "favicon[1].ico". Argument 'picture'
as a Icon.
```

Figure 1 show anomalies found in NetworkMiner2.4

Detail of anomalies found

Based on these two website Hybrid-analysis.com and urlhaus.abuse.ch, we have figure out what type of malware they are based on anomalies in NetworkMiner. Based on Gary Kessler File Signature, the MZ byte is the Windows/DOS executable file. Anomalies that has JPG or PNG format is actually exe/dll file after we follow TCP stream in Wireshark.

Table 1 shows the result of the file we export from Wireshark.

Anomalies	File type	Labelled as	Activity	Packet no	URL	Date [time-UTC]	Origin
troll1.jpg	exe/dll - first 2 bytes of MZ	Malicious site	Bombarding victims with multiple malware exploits. (IcedID-Bokbot)	3119	http://209.141.55.226/troll1.jpg	23/02/19 [19:27:08]	United States
Tinx86_14.exe	exe/dll - first 2 bytes of MZ	Trojan. generic // Trickbot downloader	Reads terminal service related keys	6249	http://46.249.62.199/Tinx86_14.exe	23/02/19 [19:33:30]	Netherlands
Sw9JKmXqaSj.exe	exe/dll - first 2 bytes of MZ	Trojan. Yakes // Trickbot downloader	Reads terminal service related keys	6262	http://46.249.62.199/Sw9JKmXqaSj.exe	[19:33:31]	Netherlands
EternalBlue MS17-010 attempt	N/A	N/A	Exploit SMB	10714, 10718, 10722, 10726, 10730, 10734, 10738, 10742, 10746, 10750, 10754, 10758, 10762, 10776, 10780, 10784, 10788, 10792		23/02/19 [19:38:31]	
win.png	exe/dll - first 2	Malware download	Used to serve malware	10966	http://85.143.218.7/win.png	24/02/19 [19:38:31]	194017 St.Petersburg Russia

	bytes of MZ		(TrickBot EXE)				
tin.png	exe/dll - first 2 bytes of MZ	Malware download	Used to serve malware (TrickBot EXE)	11986	http://85.143.218.7/ti n.png	24/02/19 [19:39:04]	194017 St.Petersburg Russia
sin.png	exe/dll - first 2 bytes of MZ	Malware download	Used to serve malware (TrickBot EXE)	20146	http://85.143.218.7/si n.png	24/02/19 [19:42:20]	194017 St.Petersburg Russia

How do we conduct this analysis in summary.

1. First, find common malware format for example exe/dll to find which host is infected by malware. At first we found 2 exe file. We use filter in Wireshark to find exe file in pcap using [ip contains "This program"]. All the exe file is in 10.2.23.231 which mean it is infected host.
2. When we found the infected host, we try to specify the infected host with http request to know whether the exe has made request to port 80 or make outgoing session. The command is [ip.addr eq 10.2.23.231 and http.request].
3. Next, we find for URL that is related to exe/dll file based on anomalies in NetworkMiner tool...commonly exe/dll file that has been programmed by a hacker will communicate to the CnC server for next action. The CnC server is related to attacker or botmaster.
4. The alternative is by finding anomalies in NetworkMiner and find the name of anomalies in the Wireshark and follow TCP stream and found MZ in the first 2 bytes. MZ is a format for Windows EXE/DLL. Although the file is in png or jpeg format, it is actually an EXE/DLL format if the first 2 bytes is MZ, it has been alter or modified by the attacker to deceived victims. Then, we analyse the malware activity to further investigation and understanding.
5. Besides, to determine whether the DC server is infected or not, we try to filter out port that is commonly used by Trojan at port 4444 or 4321. The command is [tcp.port == 4444] or [tcp.port == 4321]. Anyway, we do not find any suspicious activity in the DC server.

Analysing anomalies

To check the file, the step we use is Binwalk in Linux (Parrot OS). This step is to examine the binary image for embedded files and executable code.

For troll.jpg, win.jpg, sin.png, tin.png files, the real files extension are Windows executable file.

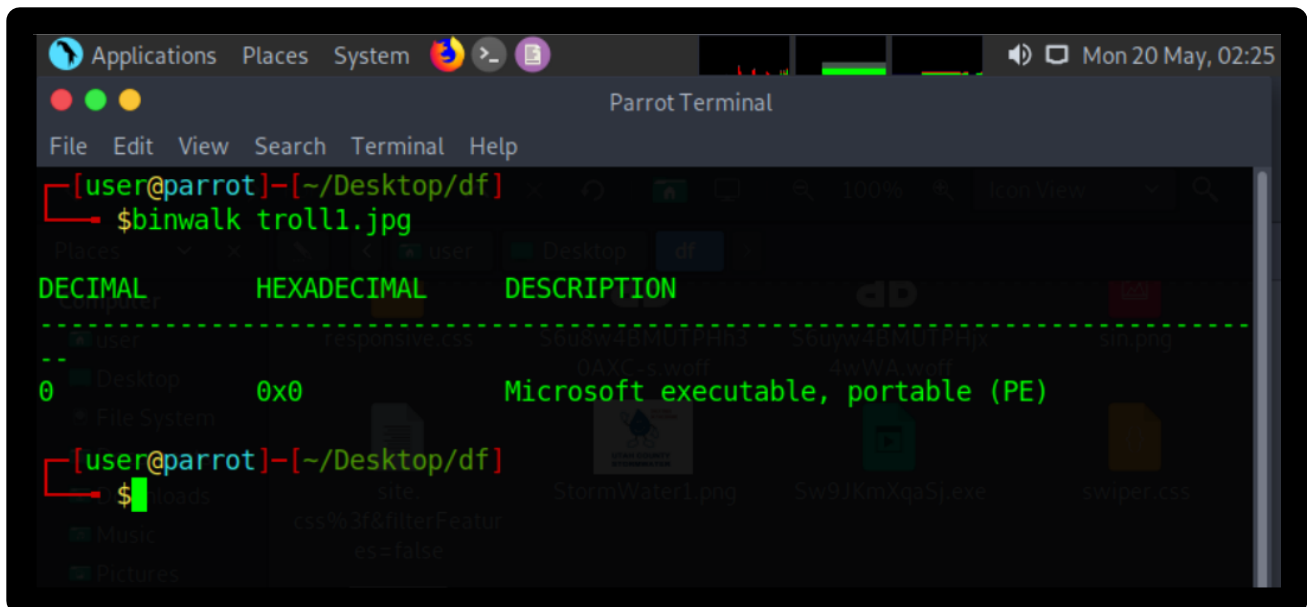


Figure 2 shows troll.jpg after Binwalk using Linux(Parrot OS)

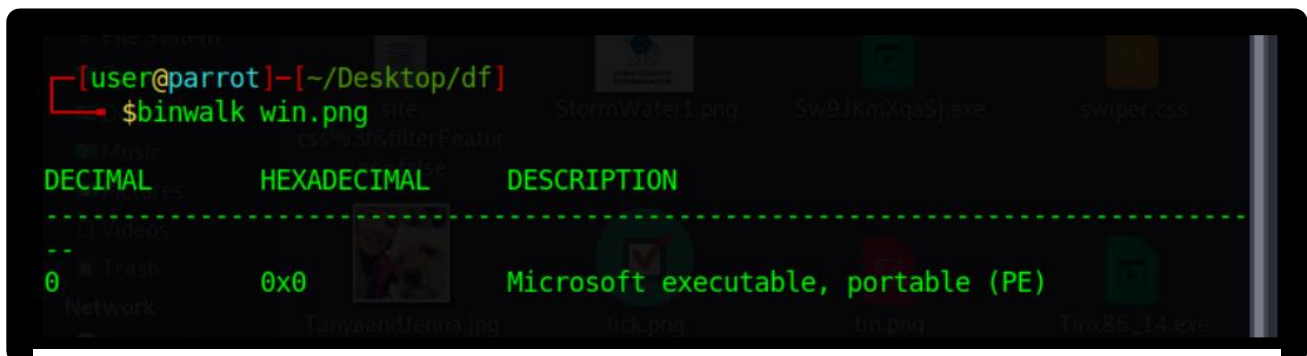


Figure 3 show win.png result after Binwalk.


```
[user@parrot]--[~/Desktop/df]
$binwalk tin.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Microsoft executable, portable (PE)

Figure 4 show tin.png result after Binwalk.

```
[user@parrot]--[~/Desktop/df]
$binwalk win.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Microsoft executable, portable (PE)

Figure 5 show sin.png result after Binwalk.

Packet no 6249 = tinx86_14.exe- remote access related. TROJAN

Tinx86_14.exe

This report is generated from a file or URL submitted to this webservice on February 14th 2019 22:51:19 (CEST) and action script *Heavy Anti-Evasion*
 Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
 Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - [learn more](#)

Threat Score: 100/100
 AV Detection: 71%
 Labeled as: Trojan.Generic

[Overview](#) [Login to Download Sample \(2.6MiB\)](#) [Downloads](#) [External Reports](#) [Re-analyze](#) [Hash Not Seen Before](#)

[No similar samples](#) [Report Abuse](#)

[Link](#) [Twitter](#) [E-Mail](#)

Incident Response

Risk Assessment

- Remote Access** Reads terminal service related keys (often RDP related)
- Persistence** Writes data to a remote process
- Fingerprint**
 - Queries kernel debugger information
 - Reads the active computer name
 - Reads the cryptographic machine GUID
- Spreading** Detected a large number of ARP broadcast requests (network device lookup)
- Network Behavior** Contacts 1 host [View all details](#)

Figure 6 show explanation about Tinx86_14.exe

MITRE ATT&CK™ Techniques Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
		Hooking 1	Hooking 1	Process Injection 2 1	Hooking 1	Network Service Scanning 1	Remote Desktop Protocol 1
		Kernel Modules and Extensions 1	Process Injection 2 1			Query Registry 3	
						System Network Configuration Discovery 1	

Figure 7 show explanation about Tinx86_14.exe.

```

  ▾ Hypertext Transfer Protocol
    > GET /Tinx86_14.exe HTTP/1.1\r\n
      Connection: Keep-Alive\r\n
      Host: 46.249.62.199\r\n
      \r\n
      [Full request URI: http://46.249.62.199/Tinx86_14.exe]
      [HTTP request 1/1]
      [Response in frame: 11971]
  
```

Figure 8 shows the request URL of tinx86_14.exe from Wireshark

```

> Flags: 0x4000, Don't fragment
  Time to live: 128
  Protocol: TCP (6)
  Header checksum: 0x68d0 [valid]
  [Header checksum status: Unverified]
  Source: 10.2.23.231
  Destination: 46.249.62.199
  
```

Figure 9 show the infected victim is 10.2.23.231 as it has all the anomalies found in NetworkMiner

```

  ▾ Ethernet II, Src: HewlettP_9f:c0:2d (00:11:0a:9f:c0:2d),
    > Destination: Cisco_83:b4:1a (00:04:c0:83:b4:1a)
    > Source: HewlettP_9f:c0:2d (00:11:0a:9f:c0:2d)
    Type: IPv4 (0x0800)
  
```

Figure 10 show MAC address of infected victim

Hosts (50)	Files (118)	Images (16)	Messages	Credentials (10)	Sessions (244)	DNS (154)	Parameters (2958)	Keywords (29)	Anomalies
<input checked="" type="checkbox"/> Show Cookies <input checked="" type="checkbox"/> Show NTLM challenge-response <input type="checkbox"/> Mask Passwords									
	Protocol	Username	Password	Valid login	Login timestamp				
dc.stormtheory.info	NTLMSSP	STORMTHEORY\ruby.ferguson	NTLM Challenge: D2AF112B9D76003C - LAN Manager R...	Unknown	2019-02-23 19:24:37 UTC				

Figure 11 based on NetworkMiner, the infected user account is Ruby Ferguson and the domain is stormtheory.info

Packet no 6262 = Sw9JKmXqaSj.exe - Remote Access Related /Reads terminal service related keys (often RDP related)



Sw9JKmXqaSj.exe 

This report is generated from a file or URL submitted to this webservice on March 16th 2019 14:23:58 (CEST)
 Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
 Report generated by Falcon Sandbox v8.30 © Hybrid Analysis - [learn more](#)

malicious
 Threat Score: 100/100
 AV Detection: 40%
 Labeled as: Trojan.Yakes

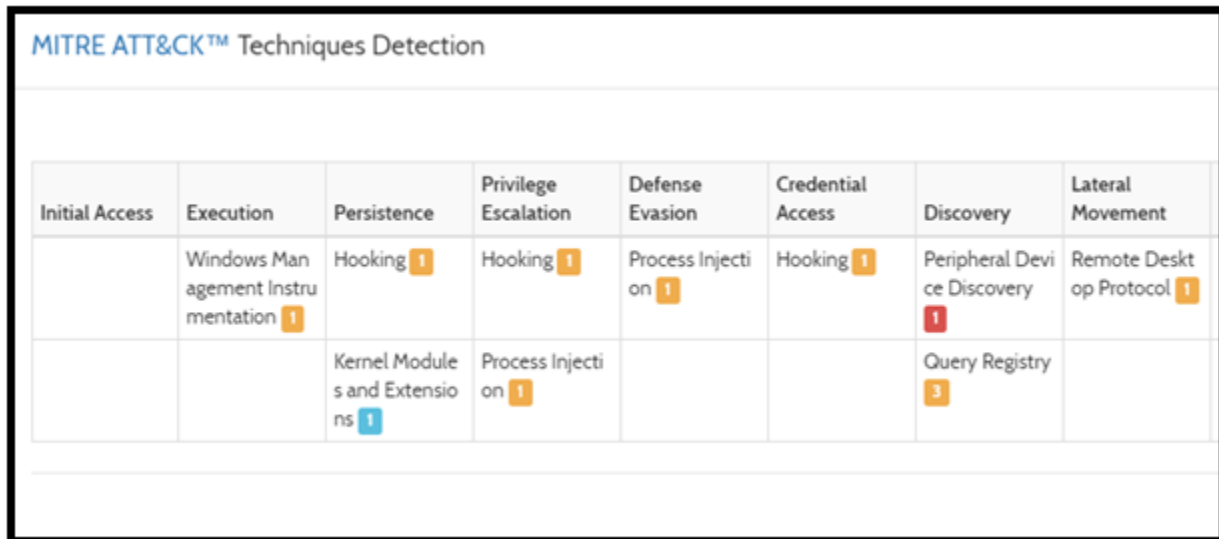
Overview | Login to Download Sample (79KB) | Downloads | External Reports | Re-analyze | Hash Not Seen Before
 Show Similar Samples | Report Abuse

Incident Response

Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Fingerprint	Queries kernel debugger information Reads the active computer name Reads the cryptographic machine GUID
Network Behavior	Contacts 1 host. View all details

Figure 12 show Sw9JKmXqaSj.exe detail



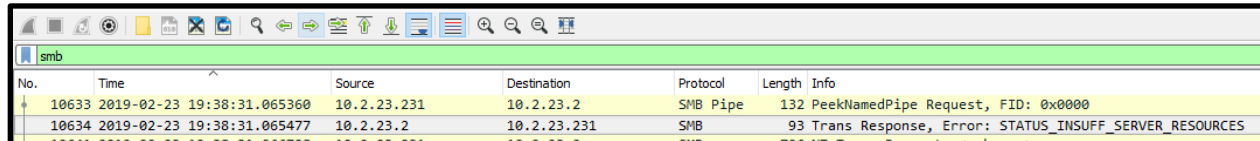
MITRE ATT&CK™ Techniques Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
	Windows Management Instrumentation 1	Hooking 1	Hooking 1	Process Injection 1	Hooking 1	Peripheral Device Discovery 1	Remote Desktop Protocol 1
		Kernel Modules and Extensions 1	Process Injection 1			Query Registry 3	

Figure 13 show Sw9JKmXqaSj.exe behaviour

Packet no 10633 - Protocol SMB Pipe = A hidden feature of Metasploit, is the ability to add SMB Named Pipe listeners in a meterpreter session to pivot on an internal network. Attacker might use command of “set payload windows/x64/meterpreter/reverse_named_pipe” to conduct pivoting.

Packet no 10634 - SMB error message = STATUS_INSUFF_SERVER_RESOURCES (Insufficient server memory to perform the requested operation) based on https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/8f11e0f3-d545-46cc-97e6-f00569e3e1bc



No.	Time	Source	Destination	Protocol	Length	Info
10633	2019-02-23 19:38:31.065360	10.2.23.231	10.2.23.2	SMB Pipe	132	PeekNamedPipe Request, FID: 0x0000
10634	2019-02-23 19:38:31.065477	10.2.23.2	10.2.23.231	SMB	93	Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES

Figure 14 show SMB pipe and error message

Packet no 16539 -NTLMSSP Challenge Error STATUS_MORE_PROCESSING_REQUIRED (There is more data available to read on the designated named pipe.)

```

SMB Header
Server Component: SMB
[Response to: 16538]
[Time from request: 0.000140000 seconds]
SMB Command: Session Setup AndX (0x73)
NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
> Flags: 0x98, Request/Response, Canonicalized Pathnames,
> Flags2: 0x4805, Error Code Type, Extended Security Nego
  
```

Figure 15 show NTLMSSP error message

Dest	Protocol	Length	Info
209.141.55.226	HTTP	365	GET /troll1.jpg HTTP/1.1
198.185.159.135	HTTP	936	POST /api/census/RecordHit?crumb=BetopJHi
8.253.129.66	HTTP	271	GET /msdownload/update/v3/static/trustedr
46.249.62.199	HTTP	130	GET /Tinx86_14.exe HTTP/1.1
46.249.62.199	HTTP	132	GET /Sw9JKmXqaSj.exe HTTP/1.1
87.236.22.142	HTTP	159	GET /data2.php?C68FF38437D96CED HTTP/1.1
85.143.218.7	HTTP	123	GET /win.png HTTP/1.1
85.143.218.7	HTTP	198	GET /tin.png HTTP/1.1
23.218.156.17	HTTP	197	GET /pki/crl/products/CSPCA.crl HTTP/1.1
72.21.81.240	HTTP	356	GET /msdownload/update/v3/static/trustedr
216.239.32.21	HTTP	245	GET /plain HTTP/1.1
85.143.218.7	HTTP	198	GET /sin.png HTTP/1.1
190.146.112.216	HTTP	340	POST /win14/FERGUSON-WIN-PC_W617601.A224C
190.146.112.216	HTTP	316	POST /win14/FERGUSON-WIN-PC_W617601.A224C
190.146.112.216	HTTP	699	POST /win14/FERGUSON-WIN-PC_W617601.A224C
161.119.42.22	HTTP	314	GET / HTTP/1.1

Figure 16 show http.request filter in Wireshark

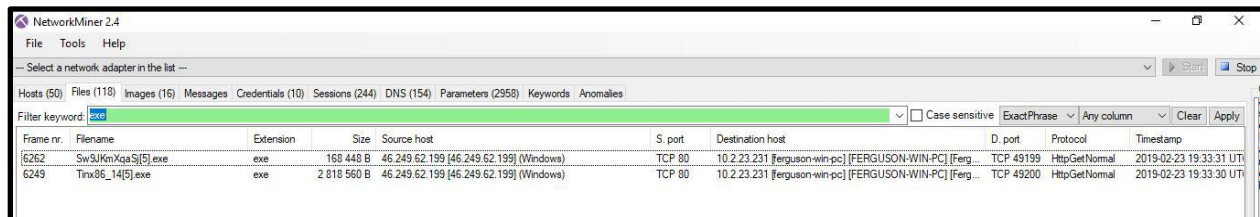
Based on the figure above, it based on filter of “http.request” in wireshark. We found all the anomalies that has been stated in networkMiner that has request to http.

Table 2 below show malware signature based on VirusTotal result.

Malware	Signature
Troll1.jpg - Mostly 50/71 detection as trojan	SHA-256 8cf2cddda8522975a22da3da429339be471234eacc0e11c099d6dcb732cf3cbb MD5 c9d7cca380a983bae2170e159b0eef5d SHA-1 559a05242fd61714da79c5d95c67b8e9edfec616
Tinx86_14.exe - Mostly 50/71 detection as trojan	SHA-256 f1b789be1126b557240dd0dfe98fc5f3ad6341bb1a5d8be0a954f65b486ad32a MD5 2a5ae5050a02bf3477c21a609a0f7b80 SHA-1 a0bcf06358319c190dfe6a8d979e185020e5af04
Sw9JKmXqaSj.exe - Mostly 46/70 detection as trojan	SHA-256 D43159c8bf2e1bd866abdbb1687911e2282b1f98a7c063f85ffd53a7f51efed4 MD5 901a99ca72a48f3a067886b158db217e SHA-1 cce0b8b2580ba4c49e5744ce96c324dcfbca9de6
Win.png Mostly 50/69	SHA-256 38c6c5b8d6fa71d9856758a5c0c2ac9d0a0a1450f75bb1004dd988e23d73a312

detection as trojan	MD5 26a97b078e5c6bfaf5170a6520c786bf SHA-1 5240075708299993915fe76197d33b0976755435
Tin.png Mostly 54/72 detection as trojan	SHA-256 4c957072ab097d3474039f432466cd251d1dc7d91559b76d4e5ead4a8bd499d5 MD5 0f7e98a8980410bfd81158598dff11b6 SHA-1 e3591fc815429040edfc1627101aa6f65dbf97e3
Sin.png Mostly 57/71 detection trojan	SHA-256 3abae6dd2ddae23b2de2ccbcc160a4a5773bef8934d0e6896d50197c3d3c417f MD5 2684f88431df44a9e096890a8a552a67 SHA-1 fb513aa01475b6a4847dad0fa0011502b43335ce

Throughout the analysis, the Wireshark and NetworkMiner 2.4 were used to analyse the evidence. In Wireshark, our group try to find if there are any suspicious file in the evidence provided and after a long search, there are two executable files named **Tinx86_14.exe** and **Sw9JKmXqaSj.exe** send by someone with IP address 46.249.62.199 to the **target IP address 10.2.23.231** at **19:33:33** and **19:33:37** respectively. From NetworkMiner 2.4, the information gathered as the figure below.

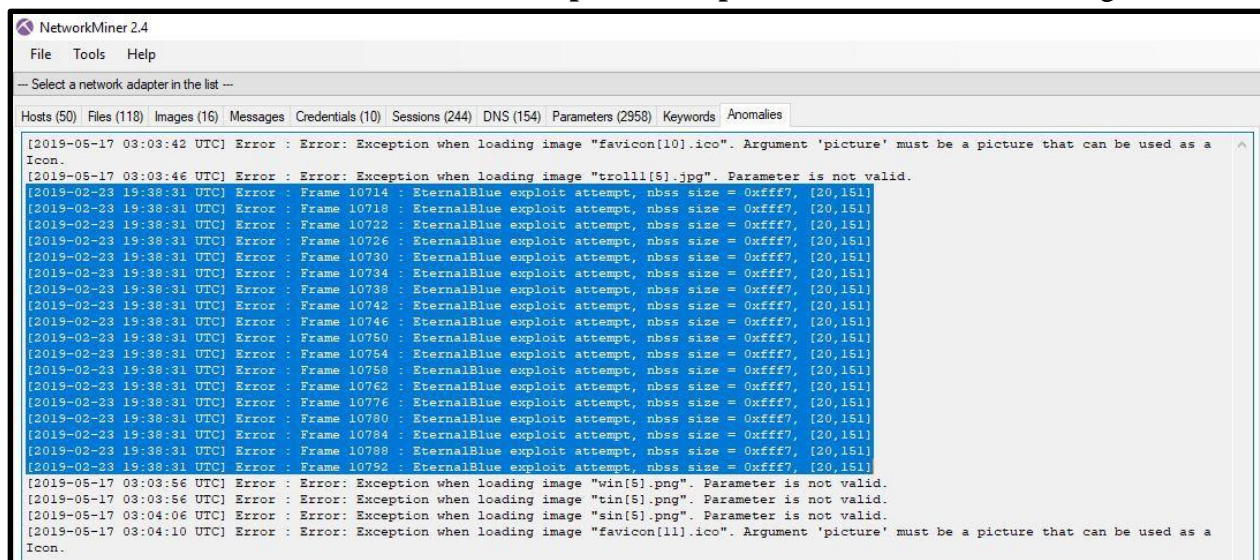


Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
6262	Sw9JKmXqaSj[5].exe	exe	168 448 B	46.249.62.199 [46.249.62.199] (Windows)	TCP 80	10.2.23.231 [ferguson-win-pc] [FERGUSON-WIN-PC] [Ferg...	TCP 49199	HttpGetNormal	2019-02-23 19:33:31 UT
6249	Tinx86_14[5].exe	exe	2 818 560 B	46.249.62.199 [46.249.62.199] (Windows)	TCP 80	10.2.23.231 [ferguson-win-pc] [FERGUSON-WIN-PC] [Ferg...	TCP 49200	HttpGetNormal	2019-02-23 19:33:30 UT

Figure 17 show exe file from infected client at 10.2.23.231

Through further investigation, both files were suspected related to banking trojan caused by **IcedID infection**. These infection lead to stolen of victim credential information. The trojan were spread through SMB vulnerability where we can see the attempt of exploiting EternalBlue in port 445.

In NetworkMiner 2.4, through Anomalies menu there are some error results that can be seen in **23/2/2019** at **19:38:31**. The **EternalBlue exploit attempt** occurred as shown in the figure below.



Timestamp	Error Message
[2019-05-17 03:03:42 UTC]	Error : Error: Exception when loading image "favicon[10].ico". Argument 'picture' must be a picture that can be used as a Icon.
[2019-05-17 03:03:46 UTC]	Error : Error: Exception when loading image "troll[5].jpg". Parameter is not valid.
[2019-02-23 19:38:31 UTC]	Error : Frame 10714 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10718 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10722 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10726 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10730 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10734 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10738 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10742 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10746 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10750 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10754 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10758 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10762 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10776 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10780 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10784 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10788 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-02-23 19:38:31 UTC]	Error : Frame 10792 : EternalBlue exploit attempt, nbss size = 0xffff7, [20,151]
[2019-05-17 03:03:56 UTC]	Error : Error: Exception when loading image "win[5].png". Parameter is not valid.
[2019-05-17 03:03:56 UTC]	Error : Error: Exception when loading image "tin[5].png". Parameter is not valid.
[2019-05-17 03:04:06 UTC]	Error : Error: Exception when loading image "sin[5].png". Parameter is not valid.
[2019-05-17 03:04:10 UTC]	Error : Error: Exception when loading image "favicon[11].ico". Argument 'picture' must be a picture that can be used as a Icon.

Figure 18 show EternalBlue exploit attempt in NetworkMiner

The screenshot displays the Wireshark network protocol analyzer interface. At the top, the menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #10714, an Ethernet II frame of 186 bytes on wire (1488 bits) captured on Ethernet II. The frame contains an Internet Protocol Version 4 packet (10.2.23.231 to 10.2.23.2) and a Transmission Control Protocol segment (Seq: 49221, Ack: 445, Len: 132).
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header (Type: IPv4), the Internet Protocol Version 4 header (Src: 10.2.23.231, Dst: 10.2.23.2), and the Transmission Control Protocol segment (Seq: 49221, Ack: 445, Len: 132).
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII. The data starts with 'a4 1f 72 c2 09 6a 00 11' and continues with a series of zeros, indicating a large segment of data.

The IcedID used Emotet's trojan's botnet to deliver the **DRIDEX CnC** for critical attack. This can be seen in PacketTotal as shown in the figure below where the **target IP address is 10.2.23.231 at 19:41:55, 23/2/2019**.

Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol
2019-02-23 19:41:55 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49550	TCP
2019-02-23 19:42:15 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	195.123.246.99	447	10.2.23.231	49556	TCP
2019-02-23 19:44:59 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49560	TCP
2019-02-23 19:48:19 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49562	TCP
2019-02-23 19:48:21 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49563	TCP
2019-02-23 19:49:39 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	195.123.246.99	447	10.2.23.231	49567	TCP
2019-02-23 19:55:34 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49580	TCP
2019-02-23 19:58:56 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49582	TCP
2019-02-23 20:02:19 Z	A Network Trojan was detected	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex CnC)	1	213.226.68.112	443	10.2.23.231	49583	TCP

Figure 20 show DRIDEX CnC was used to steal victim credential information.

Findings/results of the analysis

Scenario of case

The attackers and victim may be in the same network or has been infected with trojan/botnet (pivot). Then the attackers are trying to take control of victim's server. It might be botnet infected client pc (pivot) trying to access Active Directory server by exploiting the SMB protocol vulnerability using EternalBlue Microsoft Security Bulletin MS17-010 according to securitybulletins/2017/ms17-010.

WHO -

Possible attacker(s): 209.141.55.226, 46.249.62.199, 85.143.218.7

Infected victim (client):

No	IP	MAC	NIC Vendor	User account
1	10.2.23.231	00110A9FC02D	Hewlett Packard	FERGUSON-WIN-PC-ruby.ferguson

Main target (Windows Server 2008 R2):

On Microsoft Servers, a domain controller (DC) is a server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain.

No	IP	MAC	NIC Vendor	Domain Controller	Domain
1	10.2.23.2	A41F72C2096A	Dell Inc	STORMTHEORY-DC	stormtheory.info

WHAT CASE: EternalBlue exploitation attempt against Active Directory attack over port TCP 445

WHEN: 23/2/19 around 19:38:31 UTC hours

WHERE: Utah County, USA

HOW: The attackers (209.141.55.226) send IcedID(troll1.jpg) directly as spam and the malware acts as a downloader that installs TrickBot (a prolific piece of banking malware), which in turn installs other modules on victims' machines. Windows client (10.2.23.231) initially infected with IcedID. Then, Trickbot downloaders (Sw9JKmXqaSj.exe and Tinx86_14.exe) retrieved by the IcedID-infected client (10.2.23.231). There infected client is going to be botnet aimed as a pivot to exploit the SMB vulnerability over port 445 on the DC server. However, the infected client could not success to exploit the SMB Eternalblue on DC server as there are no infection anomalies on the DC server.

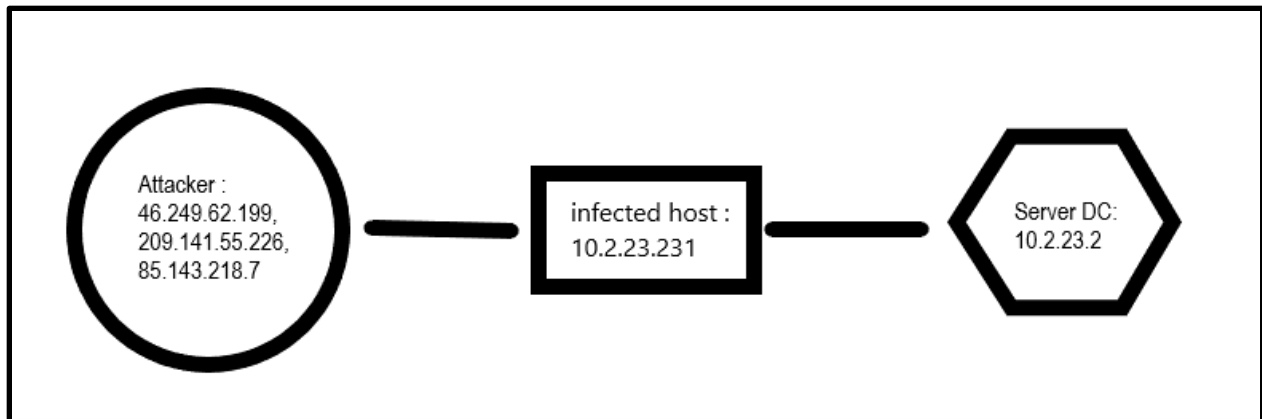


Figure 21 show crime chain of network topology.

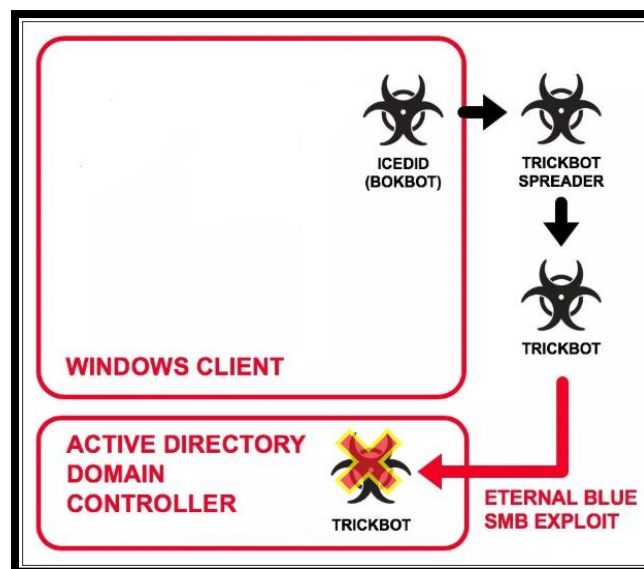


Figure 22 show how IcedID and Trickbot operation to exploit the SMB using EternalBlue style.

Sequence of malware activity

Troll1.jpg - First troll1.jpg is infected client with IcedID. It bombarding victims with multiple malware exploits. (IcedID-Bokbot). IcedID will bombarding client with Trickbot downloader.

3119	2019-02-23 19:27:08.171418	10.2.23.231	49195	209.141.55.226	80	HTTP	365	GET /troll1.jpg HTTP/1.1
3120	2019-02-23 19:27:08.171493	209.141.55.226	80	10.2.23.231	49195	TCP	54	80 → 49195 [ACK] Seq=1 Ack=312 Win=64240 Len=0
3199	2019-02-23 19:27:10.455483	209.141.55.226	80	10.2.23.231	49195	TCP	1330	80 → 49195 [PSH, ACK] Seq=1277 Ack=312 Win=64240 Len=
3200	2019-02-23 19:27:10.455808	10.2.23.231	49195	209.141.55.226	80	TCP	54	49195 → 80 [ACK] Seq=312 Ack=2553 Win=64240 Len=0
3201	2019-02-23 19:27:10.456945	209.141.55.226	80	10.2.23.231	49195	TCP	1330	80 → 49195 [PSH, ACK] Seq=2553 Ack=312 Win=64240 Len=
3202	2019-02-23 19:27:10.457183	10.2.23.231	49195	209.141.55.226	80	TCP	54	49195 → 80 [ACK] Seq=312 Ack=3829 Win=62964 Len=0
3203	2019-02-23 19:27:10.458158	209.141.55.226	80	10.2.23.231	49195	TCP	1330	80 → 49195 [PSH, ACK] Seq=3829 Ack=312 Win=64240 Len=
3204	2019-02-23 19:27:10.458372	10.2.23.231	49195	209.141.55.226	80	TCP	54	49195 → 80 [ACK] Seq=312 Ack=5105 Win=64240 Len=0

Tinx86_14.exe and Sw9JKmXqaSj.exe - Both exe file is a Trojan generic or Trickbot downloader. Trickbot downloader is retrieved by IcedID-infected client. It will download the Trickbot EXE such as win.png, sin.png, and tin.png for later attack. The infected client is going to be botnet aimed as a pivot to exploit the smb vulnerability over port 445 on the DC server.

6249	2019-02-23 19:33:30.137505	10.2.23.231	49200	46.249.62.199	80	HTTP	130	GET /Tinx86_14.exe HTTP/1.1
6250	2019-02-23 19:33:30.137601	46.249.62.199	80	10.2.23.231	49200	TCP	54	80 → 49200 [ACK] Seq=1 Ack=77 Win=64240 Len=0
6262	2019-02-23 19:33:31.127146	10.2.23.231	49199	46.249.62.199	80	HTTP	132	GET /Sw9JKmXqaSj.exe HTTP/1.1
6263	2019-02-23 19:33:31.127243	46.249.62.199	80	10.2.23.231	49199	TCP	54	80 → 49199 [ACK] Seq=1 Ack=79 Win=64240 Len=0
6360	2019-02-23 19:33:33.378341	46.249.62.199	80	10.2.23.231	49200	TCP	1330	80 → 49200 [PSH, ACK] Seq=57421 Ack=77 Win=64240 Len=
6361	2019-02-23 19:33:33.378594	10.2.23.231	49200	46.249.62.199	80	TCP	54	49200 → 80 [ACK] Seq=77 Ack=58697 Win=64240 Len=
6362	2019-02-23 19:33:33.466500	10.2.23.231	49199	46.249.62.199	80	TCP	54	49199 → 80 [ACK] Seq=79 Ack=11485 Win=62964 Len=
6363	2019-02-23 19:33:33.535975	46.249.62.199	80	10.2.23.231	49199	TCP	1514	80 → 49199 [ACK] Seq=11485 Ack=79 Win=64240 Len=
6364	2019-02-23 19:33:33.536036	46.249.62.199	80	10.2.23.231	49199	TCP	1514	80 → 49199 [ACK] Seq=12945 Ack=79 Win=64240 Len=
6365	2019-02-23 19:33:33.536053	46.249.62.199	80	10.2.23.231	49199	TCP	1514	80 → 49199 [ACK] Seq=14405 Ack=79 Win=64240 Len=
6366	2019-02-23 19:33:33.536069	46.249.62.199	80	10.2.23.231	49199	TCP	1514	80 → 49199 [ACK] Seq=15865 Ack=79 Win=64240 Len=

How SMB exploitation attempt occur

10623	2019-02-23 19:38:31.063292	10.2.23.231	49218 10.2.23.2	445 TCP	66 49218 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
10624	2019-02-23 19:38:31.063558	10.2.23.2	445 10.2.23.231	49218 TCP	66 445 → 49218 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 ..
10625	2019-02-23 19:38:31.063704	10.2.23.231	49218 10.2.23.2	445 TCP	54 49218 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10626	2019-02-23 19:38:31.063882	10.2.23.231	49218 10.2.23.2	445 SMB	105 Negotiate Protocol Request
10627	2019-02-23 19:38:31.064238	10.2.23.2	445 10.2.23.231	49218 SMB	263 Negotiate Protocol Response
10628	2019-02-23 19:38:31.064389	10.2.23.231	49218 10.2.23.2	445 SMB	130 Session Setup AndX Request, User: anonymous
10629	2019-02-23 19:38:31.064489	46.249.62.199	80 10.2.23.231	49200 TCP	1330 80 → 49200 [PSH, ACK] Seq=2589005 Ack=77 Win=64240 Len=1276 [TCP s...
10630	2019-02-23 19:38:31.064633	10.2.23.2	445 10.2.23.231	49218 SMB	199 Session Setup AndX Response
10631	2019-02-23 19:38:31.065015	10.2.23.231	49218 10.2.23.2	445 SMB	125 Tree Connect AndX Request, Path: \\10.2.23.2\IPC\$
10632	2019-02-23 19:38:31.065160	10.2.23.2	445 10.2.23.231	49218 SMB	104 Tree Connect AndX Response
10633	2019-02-23 19:38:31.065360	10.2.23.231	49218 10.2.23.2	445 SMB Pipe	132 PeekNamedPipe Request, FID: 0x0000
10634	2019-02-23 19:38:31.065477	10.2.23.2	445 10.2.23.231	49218 SMB	93 Trans Response, Error: STATUS_INSUFF_SERVER_RESOURCES
10799	2019-02-23 19:38:31.088668	10.2.23.2	445 10.2.23.231	49234 TCP	54 445 → 49234 [RST, ACK] Seq=355 Ack=138 Win=0 Len=0

#Frame 10623 = client SYN stand for synchronize and request to start session in TCP connection.

#10624 = SYN/ACK mean it is available.

#10625 = ACK stands for acknowledgement, when the receiver gets the packets, the receiver sends ACK to the sender for the confirmation that packets are received by the receiver.

#10629 = PSH/ACK mean transmitting data (Includes Payload).

#10631 = After the initial SMB handshake, related aspect of this attack is that the malware is configured to connect to a hardcoded local IP (10.2.23.2)

#10633 = look at SMB Pipe. It is Pipe listeners in a meterpreter session to pivot on an internal network.

#10634 = error STATUS_INSUFF_SERVER_RESOURCES (fail to exploit).

#10799 = RST/ACK is used to end a TCP session.

Win.png - TrickBot EXE is sending data to infected client.

10966	2019-02-23	19:38:31.324212	10.2.23.231	49262	85.143.218.7	80	HTTP	123	GET /win.png HTTP/1.1
10967	2019-02-23	19:38:31.324291	85.143.218.7	80	10.2.23.231	49262	TCP	54	80 → 49262 [ACK] Seq=1 Ack=70 Win=64240 Len=0
10968	2019-02-23	19:38:31.337121	46.249.62.199	80	10.2.23.231	49200	TCP	1330	80 → 49200 [PSH, ACK] Seq=2592833 Ack=77 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10969	2019-02-23	19:38:31.442053	10.2.23.231	49200	46.249.62.199	80	TCP	54	49200 → 80 [ACK] Seq=77 Ack=2594109 Win=62964 Len=0
10970	2019-02-23	19:38:31.539681	85.143.218.7	80	10.2.23.231	49262	TCP	1330	80 → 49262 [PSH, ACK] Seq=1 Ack=70 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10971	2019-02-23	19:38:31.540078	85.143.218.7	80	10.2.23.231	49262	TCP	1330	80 → 49262 [PSH, ACK] Seq=1277 Ack=70 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10972	2019-02-23	19:38:31.540145	85.143.218.7	80	10.2.23.231	49262	TCP	1330	80 → 49262 [PSH, ACK] Seq=2553 Ack=70 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10973	2019-02-23	19:38:31.540219	10.2.23.231	49262	85.143.218.7	80	TCP	54	49262 → 80 [ACK] Seq=70 Ack=3829 Win=64240 Len=0
10974	2019-02-23	19:38:31.542471	85.143.218.7	80	10.2.23.231	49262	TCP	1330	80 → 49262 [PSH, ACK] Seq=3829 Ack=70 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10975	2019-02-23	19:38:31.545620	85.143.218.7	80	10.2.23.231	49262	TCP	1330	80 → 49262 [PSH, ACK] Seq=5105 Ack=70 Win=64240 Len=1276 [TCP segment of a stream already in the socket]
10976	2019-02-23	19:38:31.545773	10.2.23.231	49262	85.143.218.7	80	TCP	54	49262 → 80 [ACK] Seq=70 Ack=6381 Win=64240 Len=0

```

9B.....1....-N..q.b...:0.3.f.....`.....E...g.....frmMain.
.&Never get caught by another GPF again!...B.".#....$.Form1.&.'.50...P.....F...2.....cmdStop....S&top GPF
Handler.....7.g.....4.....cmdStart....&Start GPF Handler.X...7.g.....,.....cmdError...
.&Raise GPF...
..7.g.....Label1....
With this module, you can safeguard yourself and your programs from every VB programmers worst nightmare, the General
Protection Fault. Simply call the "StartGPFHandler" method when your program starts, and call "StopGPFHandler" when
your program stops. Place any recovery or shutdown code within the "ExceptionHandler" function in the module, and
relax =).....x...G.....D....      .lblStatus...      .UN-SAFE!!.....
G.w.....%.w.....Arial....., @.....# @.....h# @...` @.....5.....@.P...].----D..
7.....@.....L..P.....t...A..
9B.....@.....VB5!6&*.....~.....
.      4.@...
0.....@...@...@.x.....SafeGuard.ExceptionHandler..ExceptionHandler.....
..#@.....

```

Some information in win.png

Tin.png and sin.png - TrickBot EXE is requesting http at port 80. It is trying to communicate to 85.143.218.7. While sin.png is also TrickBot EXE is requesting http at port 80. It is also trying to communicate to 85.143.218.7 and is sending data to target at 10.2.23.231.

11986	2019-02-23 19:39:04.487874	10.2.23.231	49273 85.143.218.7	80 HTTP	198 GET /tin.png HTTP/1.1
11987	2019-02-23 19:39:04.487950	85.143.218.7	80 10.2.23.231	49273 TCP	54 80 → 49273 [ACK] Seq=1 Ack=145 Win=64240 Len=0

20146	2019-02-23 19:42:20.188912	10.2.23.231	49558 85.143.218.7	80 HTTP	198 GET /sin.png HTTP/1.1
20147	2019-02-23 19:42:20.188989	85.143.218.7	80 10.2.23.231	49558 TCP	54 80 → 49558 [ACK] Seq=1 Ack=145 Win=64240 Len=0
20148	2019-02-23 19:42:21.569362	85.143.218.7	80 10.2.23.231	49558 TCP	1330 80 → 49558 [PSH, ACK] Seq=1 Ack=145 Win=64240 Len=1276
20149	2019-02-23 19:42:21.670580	10.2.23.231	49558 85.143.218.7	80 TCP	54 49558 → 80 [ACK] Seq=145 Ack=1277 Win=62964 Len=0

TCP Keep Alive - One part send a packet with 1 byte to the other part. When two hosts are connected over a network via TCP/IP, TCP Keepalive Packets can be used to determine if the connection is still valid, and terminate it if needed. Persistent connection. Referring based on research paper on Data Stolen Trojan Detection Based on Network Behaviors by Yiguo Pu et al (2013), some Trojans use long TCP connection to transmit small packets.

28871	2019-02-23 20:09:31.828501	10.2.23.2	445 10.2.23.231	49561 TCP	55 [TCP Keep-Alive] 445 → 49561 [ACK] Seq=1073 Ack=4086 Win=64
28872	2019-02-23 20:09:31.828707	10.2.23.231	49561 10.2.23.2	445 TCP	66 [TCP Keep-Alive ACK] 49561 → 445 [ACK] Seq=4086 Ack=1074 Wi

Conclusion of the analysis

In conclusion, for this project we have collected and discover all the possible evidence by record and analyse the activity or malware behaviour that may help us to figure out our investigation by using difference forensics tools. We additionally analyse all the file one by one and compare the evidence to detect any anomalies, suspicious and misuse of assets. Besides, this report has pointed out pieces of information relating the attackers and victims may be in the same network or has been infected with trojan. Attacker send executable files to target IP address and try to access server throughout the analysis that we conduct using Wireshark and NetworkMiner 2.4.

Recommendation

- 1) The addition tools use for investigate would help in discovering evidence and identify anomalies.
- 2) Determine significance evidence that may be related to the crime and preserve for detail examination.
- 3) Create the proper procedure and guidelines to perform the forensic task.

Reference

1. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>
2. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/8f11e0f3-d545-46cc-97e6-f00569e3e1bc
3. <https://www.speedguide.net/port.php?port=445>
4. <https://securityonline.info/introduction-to-binwalk-firmware-analysis-tool/>