Dynamic Analysis

Why Dynamic Analysis?

- We want malware's IoCs such as the following quickly:
  - C2 server information (host names, IP addresses, user agent …)
  - File (e.g. dropped file names and hashes) and registry activities
  - Notable strings in memory spaces of malware processes
  - Mutex
  - …

- Dynamic analysis is suitable for this purpose.

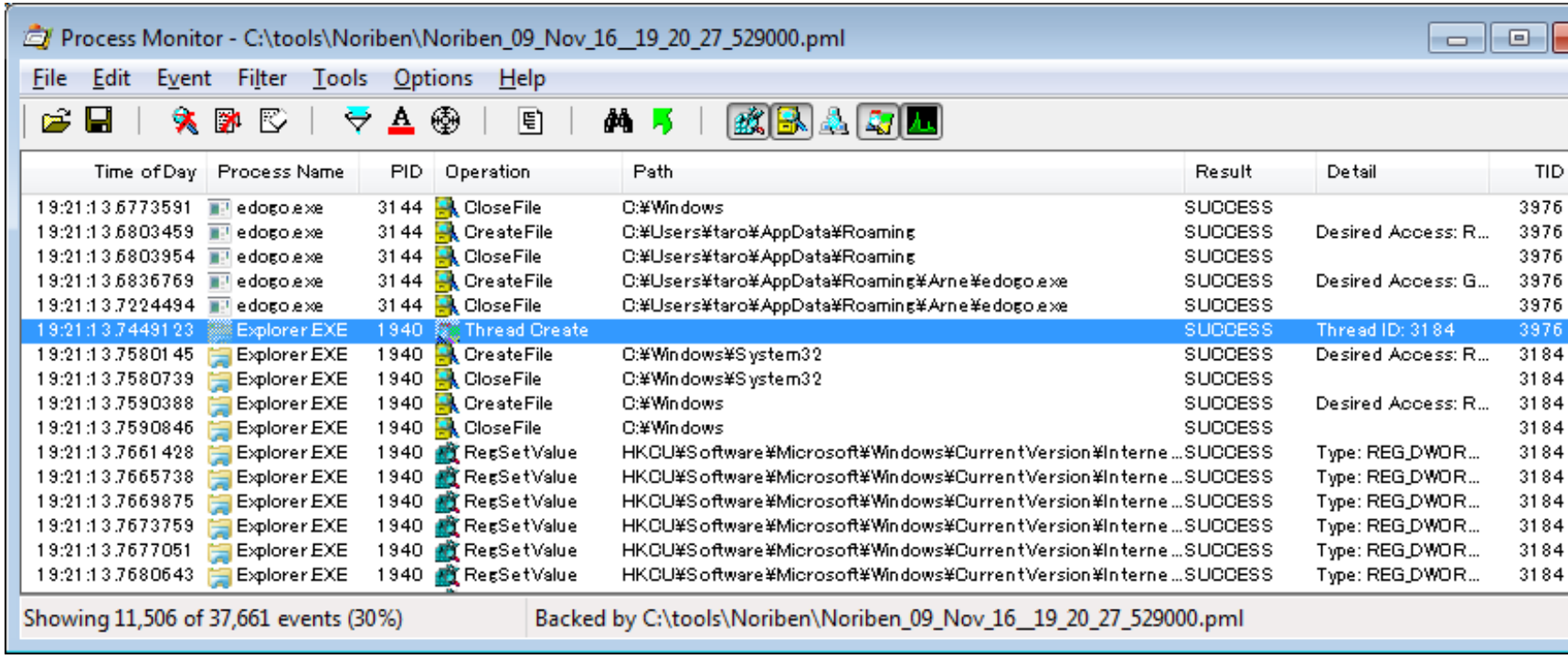
Dynamic Analysis Tools

Dynamic Analysis Tools (1)

- We will use these tools in this section.
  - Process Monitor (Procmon)
  - Noriben
  - Fakenet-NG
  - Process Hacker
  - Wireshark
  - glogg

Dynamic Analysis Tools (2)

- Process Monitor (Procmon)
  - It is a monitoring tool. It can monitor:
    - Process Activities
    - File activities
    - Registry Activities
    - Network Activities



Time of Day	Process Name	PID	Operation	Path	Result	Detail	TID
19:21:13.6773591	edogo.exe	3144	CloseFile	C:¥Windows	SUCCESS		3976
19:21:13.6803459	edogo.exe	3144	CreateFile	C:¥Users¥taro¥AppData¥Roaming	SUCCESS	Desired Access: R...	3976
19:21:13.6803954	edogo.exe	3144	CloseFile	C:¥Users¥taro¥AppData¥Roaming	SUCCESS		3976
19:21:13.6836769	edogo.exe	3144	CreateFile	C:¥Users¥taro¥AppData¥Roaming¥Arne¥edogo.exe	SUCCESS	Desired Access: G...	3976
19:21:13.7224494	edogo.exe	3144	CloseFile	C:¥Users¥taro¥AppData¥Roaming¥Arne¥edogo.exe	SUCCESS		3976
19:21:13.7449123	Explorer.EXE	1940	Thread Create		SUCCESS	Thread ID: 3184	3976
19:21:13.7580145	Explorer.EXE	1940	CreateFile	C:¥Windows¥System32	SUCCESS	Desired Access: R...	3184
19:21:13.7580739	Explorer.EXE	1940	CloseFile	C:¥Windows¥System32	SUCCESS		3184
19:21:13.7590388	Explorer.EXE	1940	CreateFile	C:¥Windows	SUCCESS	Desired Access: R...	3184
19:21:13.7590846	Explorer.EXE	1940	CloseFile	C:¥Windows	SUCCESS		3184
19:21:13.7661428	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184
19:21:13.7665738	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184
19:21:13.7669875	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184
19:21:13.7673759	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184
19:21:13.7677051	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184
19:21:13.7680643	Explorer.EXE	1940	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Interne...	SUCCESS	Type: REG_DWOR...	3184

Dynamic Analysis Tools (3)

- Noriben
  - Noriben is a simple python script. It summarizes Procmon's log.

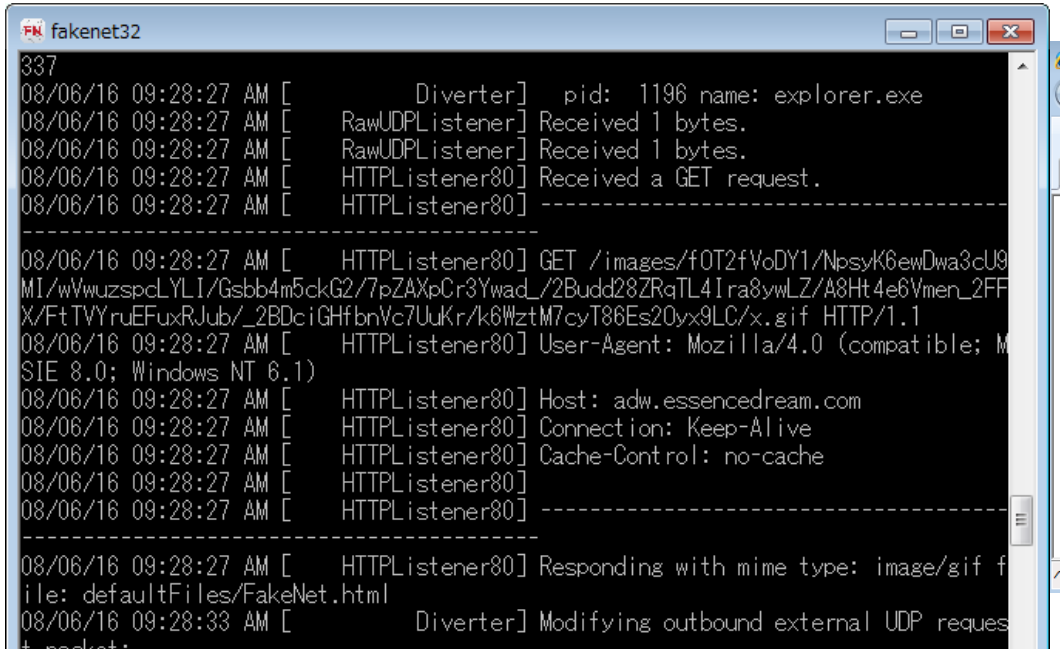
Noriben_04_Jul_18__17_21_078980.txt - Notepad

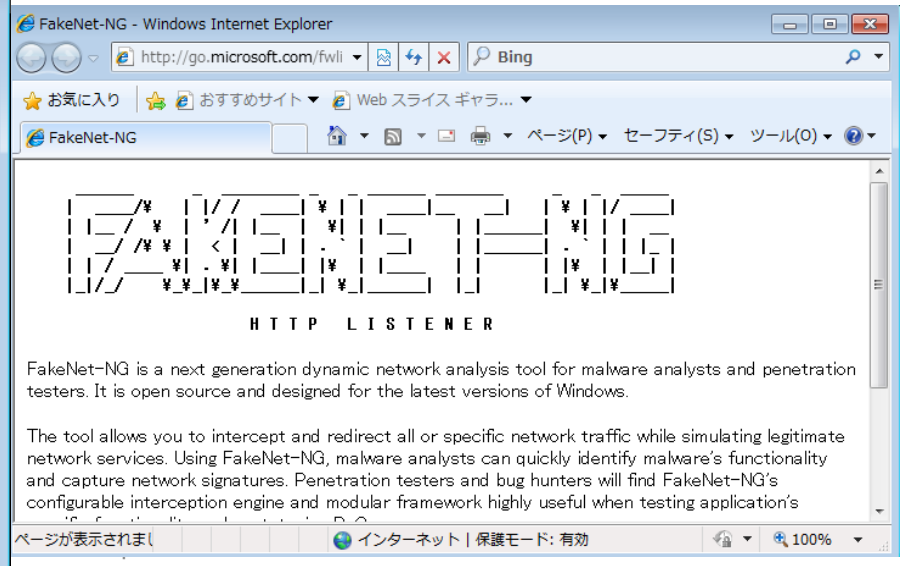
File Edit Format View Help

```
-=] Sandbox Analysis Report generated by Noriben v1.8.1
-=] Developed by Brian Baskin: brian @@ thebaskins.com  @bbaskin
-=] The latest release can be found at https://github.com/Rurik/Noriben

-=] Execution time: 431.68 seconds
-=] Processing time: 5.03 seconds
-=] Analysis time: 55.22 seconds

Processes Created:
==================
[CreateProcess] Explorer.EXE:2324 > "%ProgramFiles%\NTCore\Explorer Suite\CFF Explorer.exe
%UserProfile%\Desktop\malware\AddinsManager_dump.dll"   [Child PID: 4236]
[CreateProcess] Explorer.EXE:2324 > "%UserProfile%\Desktop\malware\AddinsManager.exe "
[Child PID: 3884]
[CreateProcess] Explorer.EXE:2324 > "%ProgramFiles%\Wireshark\Wireshark.exe C:\shortcuts
\07_MalwareAnalysis\tools\fakenet\packets_20180704_172120.pcap" [Child PID: 5768]
[CreateProcess] Wireshark.exe:5768 > "%ProgramFiles%\Wireshark\dumpcap.exe -D -Z none"
[Child PID: 5520]
[CreateProcess] dumpcap.exe:5520 > "\??\%WinDir%\system32\conhost.exe 0xffffffff -ForceV1"
[Child PID: 4516]
[CreateProcess] cmd.exe:3168 > "netsh  interface ip set address name=Ethernet0 dhcp"
```

Dynamic Analysis Tools (4)

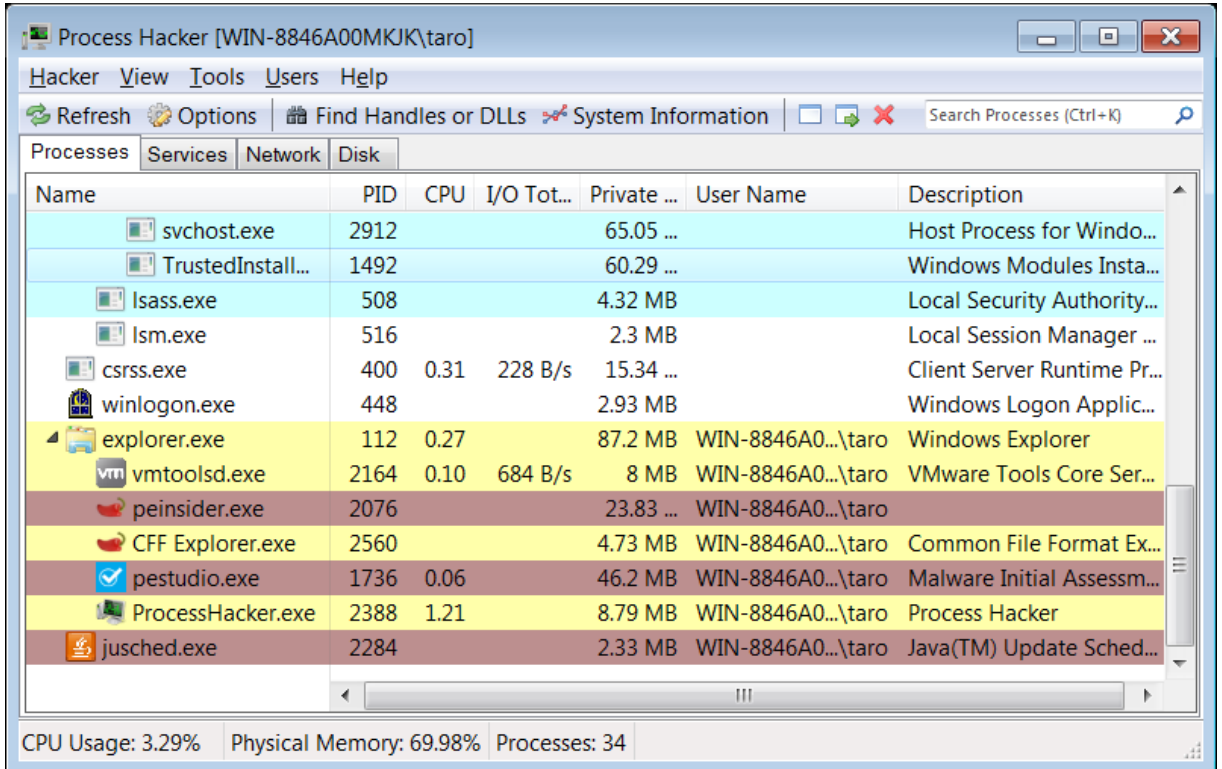
- Fakenet-NG
  - It is an Internet emulator
    - Maintained by FireEye (Flare team)
    - This software redirects communications from malware to this software, and records host names and/or IP addresses of C2 servers, and HTTP headers.
    - It has a packet capture feature as well.





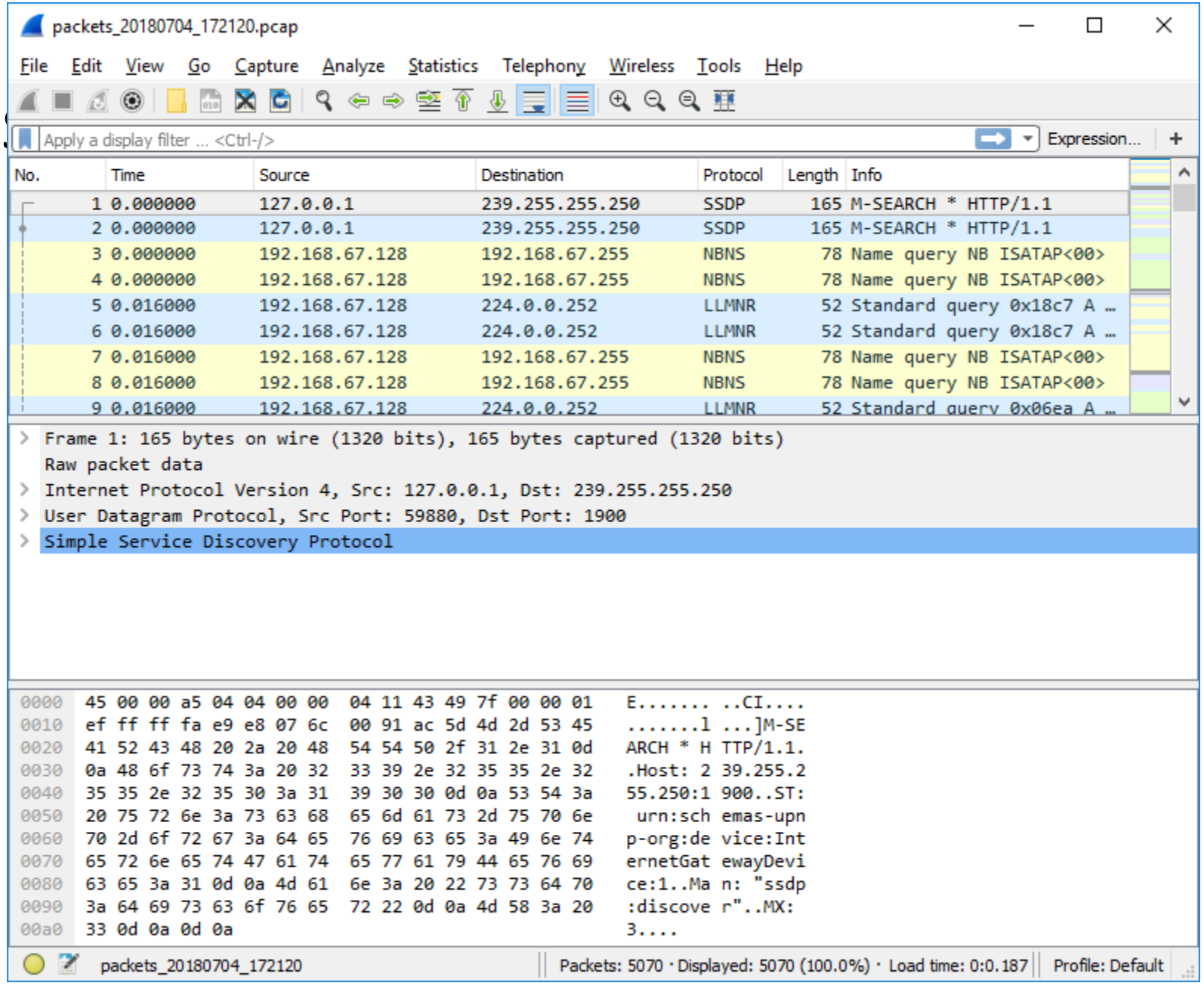
Dynamic Analysis Tools (5)

- Process Hacker
  - It is similar to Process Explorer. In addition, this tool can read/write on memory regions, show memory access rights, and dump them.
    - It is useful for analyzing malware with a process hollowing technique, and for finding malicious processes.



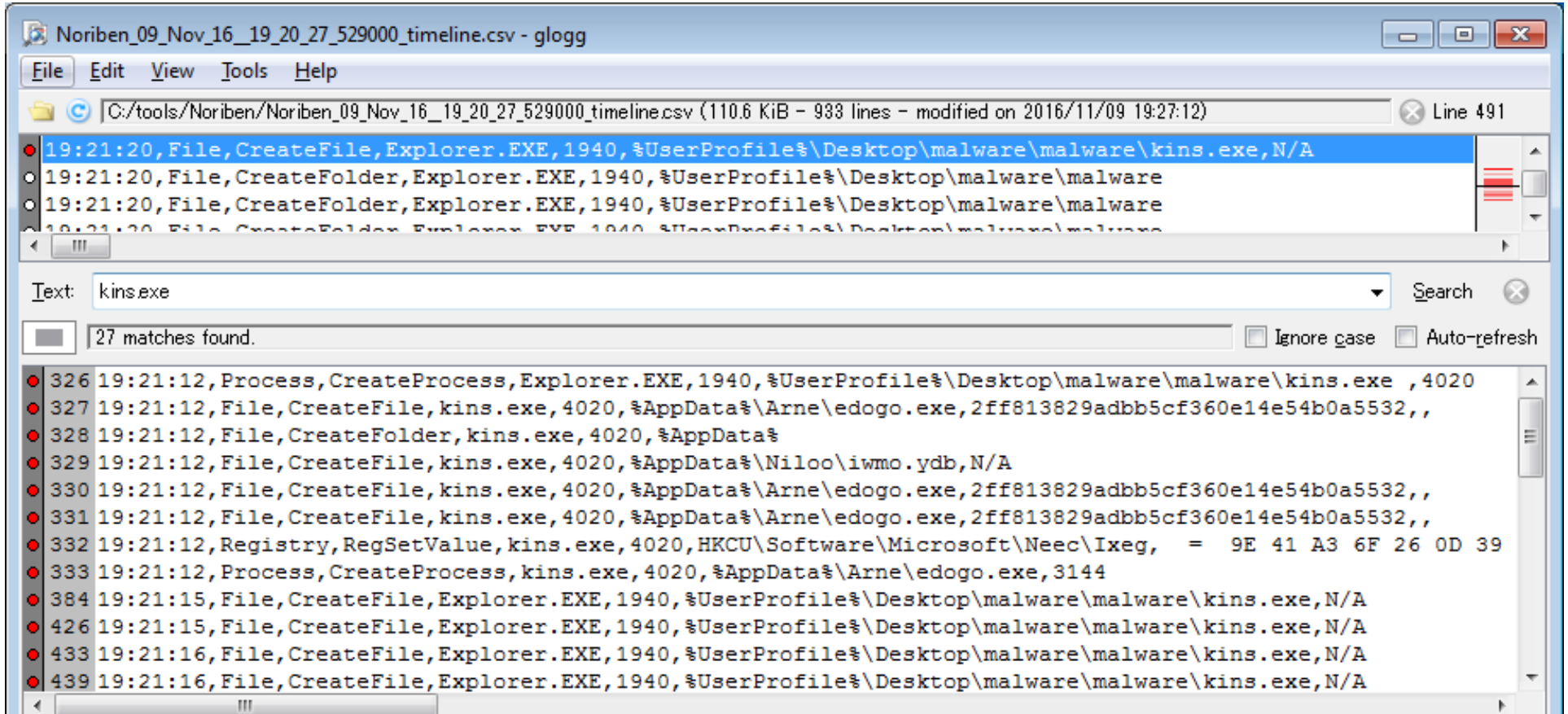
Dynamic Analysis

- Wireshark
  - It is a de facto standard packet capture and parser tool.



Dynamic Analysis Tools (7)

- glogg
  - It is a grep tool with GUI. It can handle very large files.



Preparation for Dynamic Analysis

Preparation for Dynamic Analysis

- Extract malware from the zip file below.
  - Path:
    - E:\Artifacts\other_malware\dynamic_analysis_malware.zip
  - Password: infected

- Then, take a snapshot of your VM with a name “before dynamic analysis”.

Practice Exercise 1

Dynamic Analysis using Noriben, Procmon, and Fakenet-ng

Practice Exercise 1 (1)

- Open shortcuts folder and navigate to 04_MalwareAnalysis. Then, you can find the analysis tools.
- Double-click Fakenet.exe
  - Press “Yes” when the UAC dialog shows up
- Double-click Noriben.bat
  - When you see a license agreement dialog for procmon, press “Agree”.
  - Press “Yes” when the UAC dialog shows up
- Then, double-click OceanLotus.exe (malware) in dynamic_malware_analysis folder.

Practice Exercise 1 (2)

- Wait for a few minutes. If you see suspicious communications on Fakenet-ng window, press Ctrl + c to quit Fakenet-ng.

fakenet.exe

```
07/07/19 03:53:05 PM [          Diverter]   pid:  796 name: rastlsc.exe
07/07/19 03:53:05 PM [          Diverter] [DPF] Redirecting TCP 192.168.67.128:49698->192.0.2.123:25123 to go to port
80
07/07/19 03:53:05 PM [          Diverter] [DPF] MASQUERADING TCP 192.168.67.128:8080->192.168.67.128:49698 to come fr
port 25123
07/07/19 03:53:05 PM [          Diverter]   pid:  796 name: rastlsc.exe
07/07/19 03:53:05 PM [          Diverter] [DPF] Redirecting TCP 192.168.67.128:49698->192.0.2.123:25123 to go to port
80
07/07/19 03:53:05 PM [          Diverter] [DPF] MASQUERADING TCP 192.168.67.128:8080->192.168.67.128:49698 to come fr
port 25123
07/07/19 03:53:05 PM [          Diverter] [DPF] MASQUERADING TCP 192.168.67.128:8080->192.168.67.128:49698 to come fr
port 25123
07/07/19 03:53:05 PM [          Diverter] [DPF] Redirecting TCP 192.168.67.128:49698->192.0.2.123:25123 to go to port
80
```

Practice Exercise 1 (3)

- Press “Ctrl + c” on the Noriben window as well and wait few minutes for reports to be created.
  - When you see a UAC dialog of procmon, press “Yes”.
  - When terminating Noriben, you would see a message “Terminate batch job (Y/N)?”. Enter “y” and press Enter key on your keyboard.

- Fakenet saves captured packet data in the Fakenet folder as well. Let’s open the latest pcap file with Wireshark by double-clicking it.

Practice Exercise 1 (4)

- When filtered with “dns”, you can find some DNS queries with a long FQDN.

packets_20180704_114047.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Proto	Lengt	Info
249	38.070000	192.168.67.128	192.168.67.128	DNS	118	Standard query response 0xcc18 PTR f.f.f.f.a.d.3.0.7.a.e.6.0.1.8.f.c.4.8.2.4.2.c.5.0.8.3.4.8.a.0.c.ip6.arpa
250	46.851000	192.168.67.128	192.168.67.128	DNS	130	Standard query 0x7bf2 A mkggmlggnjggmbggnkggmfggngggidggngggjkggmoggmdggmbggjgggnjgg.iknlbkgp.traveroyce.com
251	46.883000	192.168.67.128	192.168.67.128	DNS	146	Standard query response 0x7bf2 A mkggmlggnjggmbggnkggmfggngggidggngggjkggmoggmdggmbggjgggnjgg.iknlbkgp.traveroyce.com A 192.0.2.123
277	48.258000	192.168.67.128	192.168.67.128	DNS	70	Standard query 0xbab2 PTR 123.2.0.192.in-addr.arpa
278	48.304000	192.168.67.128	192.168.67.128	DNS	70	Standard query response 0xbab2 PTR 123.2.0.192.in-addr.arpa
279	56.117000	192.168.67.128	192.168.67.128	DNS	69	Standard query 0x46a2 A www.msftconnecttest.com
280	56.133000	192.168.67.128	192.168.67.128	DNS	85	Standard query response 0x46a2 A www.msftconnecttest.com A 192.0.2.123

```
> Frame 251: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.67.128, Dst: 192.168.67.128
> User Datagram Protocol, Src Port: 53, Dst Port: 55521
> Domain Name System (response)
```

```
0000  45 00 00 92 5f df 00 00  80 11 d2 2a c0 a8 43 80   E..._... ...*..C.
0010  c0 a8 43 80 00 35 d8 e1  00 7e 7a d4 7b f2 85 80   ..C..5.. .~z.{...
0020  00 01 00 01 00 00 00 00  3c 6d 6b 67 67 6d 6c 67   ........ <mkggmlg
0030  67 6e 6a 67 67 6d 62 67  67 6e 6b 67 67 6d 66 67   gnjggmbg gnkggmfg
```

Practice Exercise 1 (5)

- When you see “Conversations”, you will find many 25123/TCP communications.
  - You can open “Conversations” window by clicking “Statistics” on the menu and choosing “Conversations”. Then, select “TCP” tab.

Wireshark · Conversations · packets_20180704_114047

Ethernet | IPv4 · 6 | IPv6 | TCP · 286 | UDP · 46

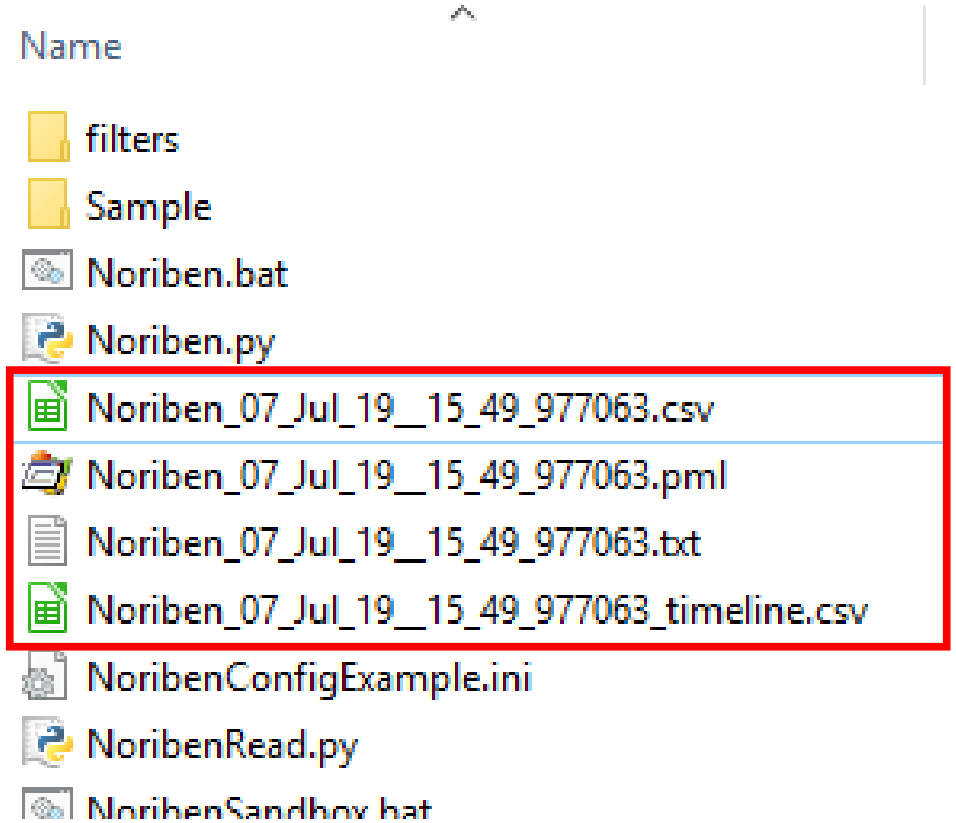
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.67.128	49819	192.0.2.123	25123	6	281	6	281	0	0	1019.07800(	0.1250	17 k	
192.168.67.128	49819	192.168.67.12	8080	12	562	6	281	6	281	1019.09300(	0.1250	17 k	
192.168.67.128	49821	192.0.2.123	25123	6	281	6	281	0	0	1029.26500(	0.0790	28 k	
192.168.67.128	49821	192.168.67.12	8080	12	562	6	281	6	281	1029.26500(	0.0790	28 k	
192.168.67.128	49823	192.0.2.123	25123	6							0	20 k	
192.168.67.128	49823	192.168.67.12	8080	12							0	23 k	
192.168.67.128	49825	192.0.2.123	25123	6							0	16 k	
192.168.67.128	49825	192.168.67.12	8080	12							0	20 k	
192.168.67.128	49827	192.0.2.123	25123	7							0	18 k	
192.168.67.128	49827	192.168.67.12	8080	14							0	20 k	
192.168.67.128	49829	192.0.2.123	25123	6							0	24 k	
192.168.67.128	49829	192.168.67.12	8080	12							0	28 k	
192.168.67.128	49831	192.0.2.123	25123	6	281	6	281	0	0	1080.12500(	0.1250	17 k	
192.168.67.128	49831	192.168.67.12	8080	12	562	6	281	6	281	1080.14000(	0.1260	17 k	
192.168.67.128	49833	192.0.2.123	25123	6	281	6	281	0	0	1090.34400(	0.1250	17 k	
192.168.67.128	49833	192.168.67.12	8080	12	562	6	281	6	281	1090.34400(	0.1250	17 k	
192.168.67.128	49835	192.0.2.123	25123	6	281	6	281	0	0	1100.51500(	0.1410	15 k	

8080/TCP is used for the proxy server and communication redirection port of fakenet in this environment.
You should ignore them.

Name resolution | Limit to display filter | Absolute start time

Practice Exercise 1 (6)

- Next, let's analyze a Noriben report.
  - When you open Noriben folder, you can find four report files created by Noriben.
    - A csv log (csv file converted from Procmon's binary log data)
    - PML (binary log data from Procmon)
    - A text report (Noriben displays this file automatically after a report is created.)
    - A timeline report (csv file)



Practice Exercise 1 (7)

- Load the “Noriben” timeline report into “glogg”.
  - Then type “OceanLotus.exe” to collect its activities.

Noriben_07_Jul_19__15_49_977063_timeline.csv - glogg

File Edit View Tools Encoding Help

C:/shortcuts/07_MalwareAnalysis/tools/noriben/Noriben_07_Jul_19__15_49_977063_timeline.csv (35.5 KiB - 208 lines - modified on 7/7/2019 3:54 PM - UTF-8) Line 132

```
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\ws2_32.dll,SHA256,7f660a552cf7146a72381b736f844b60af94a6f358baf36905536fcbd3cec0c2,,
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\winhttp.dll,SHA256,6d860e000cf6aba7084223f794f41cb293509dd360beee41ce3eef3bd84076c3,,
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\IPHLPAPI.DLL,SHA256,9cc7e1a2216f69142336975045d41570d52a11be6dcf6be9a273548cd25c33e3,,
```

Text: OceanLotus.exe Search

45 matches found. Ignore case Auto-refresh

```
77 3:49:53,File,CreateFile,OceanLotus.exe,3                                   3d83d82b0f28799cf20,,
78 3:49:53,File,CreateFile,OceanLotus.exe,3                                   ae59210de90a721ad68,,
79 3:49:53,File,CreateFolder,OceanLotus.exe
80 3:49:53,File,CreateFolder,OceanLotus.exe
81 3:49:53,File,CreateFile,OceanLotus.exe,3                                   966ecad65b73cda3be,,
82 3:49:53,File,CreateFile,OceanLotus.exe,3160,%WinDir%\SysWOW64\rsaenh.dll,SHA256,a1d957de47e671d76669deea59616225799ee00e08e897c7eec946cb86150fd,,
83 3:49:53,File,CreateFile,OceanLotus.exe,3160,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastlsc.exe,SHA256,
84 3:49:53,File,CreateFile,OceanLotus.exe,3160,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\SyLog.bin,SHA256,71
85 3:49:53,File,CreateFile,OceanLotus.exe,3160,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastls.dll,SHA256,0
86 3:49:53,Registry,RegSetValue,OceanLotus.exe,3160,HKCU\Software\Microsoft\Windows\CurrentVersion\Run\DeviceAssociationService,  =  C:\Users\taro\A
88 3:49:53,Process,CreateProcess,OceanLotus.exe,3160,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastlsc.exe,7
```

You can see that OceanLotus.exe created three files, registered rastlsc.exe to an auto-start location, and executed it when you filter with the keyword “OceanLotus.exe”.

Practice Exercise 1 (8)

- Add files and registry keys related to “OceanLotus.exe”.
  - Then, you can find another activities related to this malware.

Text: OceanLotus.exe|rastlsc.exe|SyLog.bin|rastls.dll|DeviceAssociationService

90 matches found.

```
116 3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\imm32.dll,SHA256,cda412fdcf28503d0b9dd78c8e969a61f4b79ca4a8cc2721f
117 3:49:53,File,CreateFile,rastlsc.exe,796,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\r
118 3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\bcrypt.dll,SHA256,6978f42157714ae031a5a31b9f3f8725d0dbb220f0f7db96
119 3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\rsaenh.dll,SHA256,afd957de47e67fd766698deea596f62257992e00e08e897c
120 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\ole32.dll,SHA256,319fc1e318f3f2f094c0447acdc6e181c479c6f54601c83eb
121 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\oleaut32.dll,SHA256,f132a5225ded6531383e766a5705a48123fb9c2211cabf
122 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\ws2_32.dll,SHA256,7f660a552cf7146a72381b736f844b60af94a6f358baf369
123 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\winhttp.dll,SHA256,6d860e000cf6aba7084223f794f41cb293509dd360beee4
124 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\IPHLPAPI.DLL,SHA256,9cc7e1a2216f69142336975045d41570d52a11be6dcf6b
125 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\mswsock.dll,SHA256,dd51257116f07c4a683a0e95a084e2f9d5860d7c0a6d928
126 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\nsi.dll,SHA256,86eb506bc706dbeb0eb9234a2c1d4ba7589b1abe0a9ca83d49a
127 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\dnsapi.dll,SHA256,2042e62b3585aa54ed8d284625fefa98086c0860dd768ca0
130 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\FWPUCLNT.DLL,SH                                          c6f3d68d4791
131 3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\rasadhlp.dll,SH                                          d3bbbd4c14f9
132 3:49:54,Network,TCP Send,rastlsc.exe,796,192.0.2.123:25123
133 3:49:54,Network,TCP Receive,rastlsc.exe,796
141 3:51:43,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\OnDemandConnRouteHelper.dll,SHA256,b0b77179455cab1a704b63db705d61e
142 3:51:44,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\OnDemandConnRouteHelper.dll,SHA256,b0b77179455cab1a704b63db705d61e
```

Rastlsc.exe communicated with an external server with 25123/TCP.

Practice Exercise 1 (9)

Summary of malicious activities

Activities		Value	Source
Network activities	TCP, DNS	mkggmlggnjggmbggnkggmfggngggidggngggjkggmoggmdggmbggjgggnjgg.iknlbkgp.traveroyce.com:25123	Fakenet
File activities	Create	%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastlsc.exe	Noriben/procmon
		%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\SyLog.bin	
		%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastls.dll	
Process activities	Execute	%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastlsc.exe	Noriben/procmon
Registry activities	Create	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\DeviceAssociationService	Noriben/procmon

Practice Exercise 1 (10)

- We can get various results like the previous slide even if we do not have commercial sandboxes. These free tools we mentioned earlier help us to find out information such as:
  - Network activities
    - C2 servers
  - File activities
  - Registry activities
  - Process activities

- We can do the first response using the information.
  - e.g. Finding other infected machines in your network

Practice Exercise 1 (11)

- By the way, you should know that a CreateFile event is not for “creating a file”. It is for “creating a file handle or a descriptor”. It occurs on all file-related events such as read/write/create/delete…

OceanLotus.exe|rastlsc.exe|SyLog.bin|rastls.dll|DeviceAssociationService

90 matches found.

```
3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\imm32.dll,SHA256,cda412fdcf28503d0b9dd78c8e969a61f4b79ca4a8cc2721f8d05
3:49:53,File,CreateFile,rastlsc.exe,796,%AppData%\Symantec Endpoint Protection\12.1.671.4971.104a\DeviceAssociationService\rastl
3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\bcrypt.dll,SHA256,
3:49:53,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\rsaenh.dll,SHA256,
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\ole32.dll,SHA256,3
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\oleaut32.dll,SHA25
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\ws2_32.dll,SHA256,
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\winhttp.dll,SHA256
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\IPHLPAPI.DLL,SHA25
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\mswsock.dll,SHA256
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\nsi.dll,SHA256,86e
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\dnsapi.dll,SHA256,2042e62b3585aa54ed8d284625fefa98086c0860dd768ca0cce3
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\FWPUCLNT.DLL,SHA256,cf245be448c7a4f1043a12e32d3e80d53fc6f3d68d47919807
3:49:54,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\rasadhlp.dll,SHA256,6a5379dc710f55f7b2aa92f28826885a07d3bbbd4c14f91353
3:49:54,Network,TCP Send,rastlsc.exe,796,192.0.2.123:25123
3:49:54,Network,TCP Receive,rastlsc.exe,796
3:51:43,File,CreateFile,rastlsc.exe,796,%WinDir%\SysWOW64\OnDemandConnRouteHelper.dll,SHA256,b0b77179455cab1a704b63db705d61ec970
```

You can typically ignore “CreateFile” events for DLLs under SysWOW64 and System32 because the target executable file depends on them and these DLL files were loaded from the target executable file.

Scenario 1 Labs

The Result of Persistence Analysis

- We have found two binaries from the host Client-Win10-1.

	Persistence Type	Name	Image to Execute	Registered Date	Access Rights
Persistence A	Scheduled Task	SxS	C:\Windows\SvS.DLL,GnrkQr	2018-03-14 22:50:28 (JST)	Privileged
Persistence B	WMI	AddinManager Monitor	C:\Windows\addins\Addins Manager.exe	2018-03-20 18:40:27 (JST)	Privileged

Scenario 1 Labs:
Lab 1 - Dynamic Analysis SvS.DLL

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (1)

- Revert your VM to “before dynamic analysis” first if you have not done yet.

- Double-click Fakenet.exe
  - Press “Yes” when the UAC dialog shows up

- Double-click Noriben.bat
  - Press “Yes” when the UAC dialog shows up

- Open cmd.exe and execute the command below. The command line is what you have found from the Task Scheduler, and is suspected to execute the malware.

```
rundll32 C:\Users\taro\Desktop\malware\SvS.DLL,GnrkQr
```

- Wait for about three minutes…

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (2)

```
rundll32 C:\Users\taro\Desktop\malware\SvS.DLL,GnrkQr
```

- Goals:
  - Find any suspicious communications first.
    - What was the host name of the C2 server, the method of HTTP protocol and the port number?
    - Are there remarkable HTTP headers?
  - Can you find any suspicious entries of file activities, registry activities and process activities on the Noriben report?
  - Identify the malware name **without using any external sandboxes and services such as VirusTotal**.
- Hints:
  - The customer's proxy server name is proxy.ninja-motors.net. It is not a malicious server.
  - You will need to check pcap data. Filter with "dns or http".
  - You will need to check files that have filenames starting with http* on Fakenet-NG folder.
  - In order to specify its name, use web search engines with the specific strings such as remarkable HTTP headers.

```
/07/19 05:11:44 PM [          IRCServer] Starting...
/07/19 05:11:44 PM [       TFTPListener] Starting...
/07/19 05:11:44 PM [          POPServer] Starting...
/07/19 05:11:44 PM [           Diverter] Starting...
/07/19 05:11:44 PM [           Diverter] Set DNS server 192.168.67.128 on the adapter: Ethernet0
/07/19 05:11:44 PM [           Diverter] Failed to notify adapter change on {C2E2C235-7DE5-48B9-96EA-FCE359318682}
/07/19 05:11:44 PM [           Diverter] Failed to call OpenService
/07/19 05:11:44 PM [           Diverter] Diverting ports:
/07/19 05:11:44 PM [           Diverter] Flushed DNS cache.
/07/19 05:12:49 PM [           Diverter]   pid:  4796 name: rundll32.exe
/07/19 05:12:49 PM [        DNS Server] Received A request for domain 'proxy.ninja-motors.net'.
/07/19 05:12:49 PM [        DNS Server] Responding with '192.0.2.123'
/07/19 05:12:49 PM [           Diverter]   pid:  4796 name: rundll32.exe
/07/19 05:12:49 PM [  ProxyTCPListener] Received 33 bytes.
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:49674 -> 127.0.0.1:80
/07/19 05:12:49 PM [
/07/19 05:12:49 PM [
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:49674 -> 127.0.0.1:80
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:49674 -> 127.0.0.1:80
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:80 -> 127.0.0.1:49674
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:80 -> 127.0.0.1:49674
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
/07/19 05:12:49 PM [           Diverter]   127.0.0.1:80 -> 127.0.0.1:49674
/07/19 05:12:49 PM [           Diverter] Ignoring loopback packet
```

This malware communicated with an external host via the customer's proxy server.

packets_20180704_153054.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns or http

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
947	97.455000	192.168.67.128	192.168.67.128	DNS	62	Standard query 0x57f3 A time.windows.com
949	97.518000	192.168.67.128	192.168.67.128	DNS	78	Standard query response 0x57f3 A time.windows.com A 192.0.2.123
965	106.799000	192.168.67.128	8.8.8.8	DNS	68	Standard query 0xfb98 A proxy.ninja-motors.net
966	106.799000	192.168.67.128	192.168.67.128	DNS	68	Standard query 0xfb98 A proxy.ninja-motors.net
967	106.831000	192.168.67.128	192.168.67.128	DNS	84	Standard query response 0xfb98 A proxy.ninja-motors.net A 192.0.…
973	106.893000	192.168.67.128	192.0.2.123	HTTP	73	CONNECT 1ive.net:443 HTTP/1.0
974	106.893000	192.168.67.128	192.168.67.128	HTTP	73	CONNECT 1ive.net:443 HTTP/1.0
979	106.940000	127.0.0.1	127.0.0.1	HTTP	73	CONNECT 1ive.net:443 HTTP/1.0
982	106.956000	127.0.0.1	127.0.0.1	HTTP	379	HTTP/1.0 501 Unsupported method ('CONNECT') (text/html)
991	107.034000	192.168.67.128	192.0.2.123	HTTP	111	Continuation
992	107.034000	192.168.67.128	192.168.67.128	HTTP	111	Continuation
994	107.799000	192.168.67.128	192.168.67.128	DNS	118	Standard query 0x4a39 PTR 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.4.0.0.0.…
995	107.831000	192.168.67.128	192.168.67.128	DNS	66	Standard query 0xbe49 PTR 8.8.8.8.in-addr.arpa

```
> Frame 967: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.67.128, Dst: 192.168.67.128
> User Datagram Protocol, Src Port: 53, Dst Port: 62405
```

```
0000  45 00 00 54 60 9c 00 00  80 11 d1 ab c0 a8 43 80   E..T`... ......C.
0010  c0 a8 43 80 00 35 f3 c5  00 40 cd 21 fb 98 85 80   ..C..5.. .@.!....
0020  00 01 00 01 00 00 00 00  05 70 72 6f 78 79 0c 6e   ........ .proxy.n
0030  69 6e 6a 61 2d 6d 6f 74  6f 72 73 03 6e 65 74 00   inja-mot ors.net.
0040  00 01 00 01 c0 0c 00 01  00 01 00 00 00 00 00 04   ........ ........
0050  c0 00 02 7b                                         ...{
```

We found that this malware connected to 1ive.net:443 via the customer's proxy server (proxy.ninja-motors.net) with CONNECT method when we filter with "dns or http".

Hypertext Transfer Protocol: Protocol | Packets: 4678 · Displayed: 730 (15.6%) · Load time: 0:0.374 | Profile: Default

fakenet.exe

```
07/07/19 05:16:26 PM [          Diverter]   127.0.0.1:49678 -> 127.0.0.1:80
07/07/19 05:16:26 PM [     HTTPListener80] Received a POST request
07/07/19 05:16:26 PM [          Diverter] Ignoring loopback packet
07/07/19 05:16:26 PM [     HTTPListener80] ----------------------------------------------------------------------------
--
07/07/19 05:16:26 PM [          Diverter]   127.0.0.1:80 -> 127.0.0.1:49678
07/07/19 05:16:26 PM [     HTTPListener80] POST /update?id=1b4e1e22 HTTP/1.1
07/07/19 05:16:26 PM [     HTTPListener80] Accept: */*
07/07/19 05:16:26 PM [     HTTPListener80] X-Session: 0
07/07/19 05:16:26 PM [     HTTPListener80] X-Status: 0
07/07/19 05:16:26 PM [     HTTPListener80] X-Size: 61456
07/07/19 05:16:26 PM [     HTTPListener80] X-Sn: 1
07/07/19 05:16:26 PM [     HTTPListener80] User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
07/07/19 05:16:26 PM [     HTTPListener80] Host: 192.0.2.123:8080
07/07/19 05:16:26 PM [     HTTPListener80] Content-Length: 0
07/07/19 05:16:26 PM [     HTTPListener80] Connection: Keep-Alive
07/07/19 05:16:26 PM [     HTTPListener80] Cache-Control: no-cache
07/07/19 05:16:26 PM [     HTTPListener80]
07/07/19 05:16:26 PM [     HTTPListener80]
07/07/19 05:16:26 PM [     HTTPListener80] ----------------------------------------------------------------------------
--
07/07/19 05:16:26 PM [     HTTPListener80] Storing HTTP POST headers and data to http_20190707_171626.txt.
07/07/19 05:16:26 PM [     HTTPListener80] Responding with mime type: text/html file: C:\Tools\FakeNet\defaultFiles\FakeN
et.html
07/07/19 05:16:26 PM [          Diverter] Ignoring loopback packet
07/07/19 05:16:26 PM [
07/07/19 05:16:26 PM [
07/07/19 05:16:26 PM [
07/07/19 05:16:26 PM [
07/07/19 05:16:26 PM [          Diverter]   TCP 127.0.0.1:80->127.0.0.1:49678
```

This malware also performed a POST request with non standard HTTP headers such as “X-Session”, “X-Status”, “X-Size” and “X-Sn”. The user-agent string looks like hard-coded.

fakenet

File Home Share View

« 07_MalwareAnalysis › tools › fakenet

Search fakenet

Name	Date modified	Type	Size
configs	7/2/2018 7:07 PM	File folder	
defaultFiles	10/17/2017 8:42 AM	File folder	
listeners			
CHANGELOG.txt			
fakenet.exe			
fakenet.exe.manifest	10/17/2017 8:47 AM	MANIFEST File	1 KB
packets_20180704_153054.pcap			
README.txt			
http_20180704_155216.txt			
http_20180704_155229.txt			
http_20180704_155601.txt			
http_20180704_155602.txt			
http_20180704_155603.txt			

Quick access
Desktop
Downloads
Documents
Pictures
fakenet
tools
OneDrive
This PC
Network
Homegroup

13 items

Fakenet-NG saves http requests in the fakenet folder.
We can verify the requests.

http_20180704_155603.txt - Notepad

File Edit Format View Help

```
POST /update?id=1e6a44f1 HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
Host: 192.0.2.123:8080
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (7)

- If we search with these characteristic keywords in a search engine…,
  - "X-Session" "X-Status" "X-Size" "X-Sn"
  - We will find that these characteristics imply the use of PlugX!!

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (8)

- Once the communications are logged, stop Fakenet-NG and Noriben.

Noriben_04_Jul_18__16_27_674066_timeline.csv - glogg

File Edit View Tools Encoding Help

C:/shortcuts/07_MalwareAnalysis/tools/noriben/Noriben_04_Jul_18_

```
4:31:34,Registry,RegSetValue,rundll32.exe,340,
4:31:34,Registry,RegSetValue,rundll32.exe,340,
4:31:35,Registry,RegSetValue,rundll32.exe,340,
4:31:35,Registry,RegSetValue,rundll32.exe,340,
```

1. Load the Noriben timeline report with glogg.
2. Filter with “rundll32|SvS.DLL”.
3. We can see that this malware changed several IE settings.
   - disable and delete proxy settings
   - lower Internet zone settings

Line 740

```
anet,  =  1
t,  =  0
\CachePrefix,  =
\CachePrefix,  =  Cookie:
```

Text: rundll32|SvS.DLL Search

83 matches found. Ignore case Auto-refresh

```
724 1:34,File,CreateFile,rundll32.exe,340,%WinDir%\SysWOW64\winhttp.dll,SHA256,07193f6c70e1bbd07a2591b409d9155ce84a5a62cd30f26771920f5baf7aab16,,
725 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable,  =  0
726 1:34,Registry,RegDeleteVal ue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
727 1:34,Registry,RegDeleteVal ue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
728 1:34,Registry,RegDeleteVal ue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
729 1:34,Registry,RegDeleteVal ue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\AutoDetect
730 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings,  =  46 00 0
731 1:34,File,CreateFile,rundll32.exe,340,%WinDir%\SysWOW64\urlmon.dll,SHA256,9d18d8a88a7b5dfdd44e5e371e96a3fac90df9a901aa22ddf55d6774a9a3b811,,
732 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass,  =  1
733 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName,  =  1
734 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet,  =  1
735 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect,  =  0
736 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass,  =  1
737 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName,  =  1
738 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet,  =  1
739 1:34,Registry,RegSetValue,rundll32.exe,340,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect,  =  0
```

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (9)

- Summary for this analysis
  - It connects to “1ive.net” with CONNECT method via the customer’s proxy server.
    - Note that the first character of the domain name is “one”, not “L”.
  - There are several remarkable HTTP headers, and some of them are not standard headers.
    - POST /update\?id=[a-z0-9]{8} HTTP/1.1
    - X-Session: 0
    - X-Status: 0
    - X-Size: 61456
    - X-Sn: 1
    - User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
  - There are no significant entries in file system activities.
  - There are several entries related to changing IE & proxy settings in registry activities.

Scenario 1 Labs: Lab 1
Dynamic Analysis SvS.DLL (10)

- Revert the VM to “before dynamic analysis” after you finished this exercise.
  - In case you want to save some data (logs and outputs of the tools), copy them to your host machine before reverting the VM.

Scenario 1 Labs:
Lab 2 - Dynamic Analysis
AddinsManager.exe

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (1)

- Revert your VM first if you have not done it.

- Double-click Fakenet.exe
  - Press “Yes” when the UAC dialog shows up

- Double-click Noriben.bat
  - Press “Yes” when the UAC dialog shows up

- Double-click AddinsManager.exe (malware)

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (2)

- Goal:
  - First, find suspicious communications. In this exercise, you should focus on the communication information.
    - What was the host name of the C2 server, the method of HTTP protocol and the port number?
- Hint
  - The customer’s proxy server name is proxy.ninja-motors.net. It is not a malicious server.
  - You will need to check pcap data. Filter with “dns or http”.

```
[          Diverter] Ignoring loopback packet
[          Diverter]   127.0.0.1:80 -> 127.0.0.1:49678
[          Diverter]   pid:  1948 name: svchost.exe
[        DNS Server] Received A request for domain 'proxy.ninja-motors.net'.
[        DNS Server] Responding with '192.0.2.123'
[          Diverter]   pid:  4836 name: AddinsManager.exe
[  ProxyTCPListener] Received 36 bytes.
[          Diverter] Ignoring loopback packet
[          Diverter]
[          Diverter]
[          Diverter]
[          Diverter]
```

We found that this malware accessed out1ook.net:443 via the customer's proxy server (proxy.ninja-motors.net).

packets_20180704_172120.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns or http

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1269	89.214000	192.168.67.128	192.168.67.128	DNS	68	Standard query 0xe2bd A proxy.ninja-motors.net
1270	89.261000	192.168.67.128	192.168.67.128	DNS	84	Standard query response 0xe2bd A proxy.ninja-motors.net A 192.0.2.123
1276	89.323000	192.168.67.128	192.0.2.123	HTTP	76	CONNECT out1ook.net:443 HTTP/1.1
1277	89.323000	192.168.67.128	192.168.67.128	HTTP	76	CONNECT out1ook.net:443 HTTP/1.1
1282	89.354000	127.0.0.1	127.0.0.1	HTTP	76	CONNECT out1ook.net:443 HTTP/1.1
1285	89.354000	127.0.0.1	127.0.0.1	HTTP	379	HTTP/1.0 501 Unsupported method ('CONNECT') (text/html)
1296	89.573000	192.168.67.128	192.168.67.128	DNS	69	Standard query 0xdb0d A www.msftconnecttest.com
1297	89.604000	192.168.67.128	192.168.67.128	DNS	85	Standard query response 0xdb0d A www.msftconnecttest.com A 192.0.2.123
1303	89.651000	192.168.67.128	192.0.2.123	HTTP	151	GET /connecttest.txt HTTP/1.1
1304	89.651000	192.168.67.128	192.168.67.128	HTTP	151	GET /connecttest.txt HTTP/1.1
1308	89.729000	192.168.67.128	192.168.67.128	HTTP	182	HTTP/1.0 200 OK (text/plain)
1325	96.682000	192.168.67.128	192.168.67.128	DNS	70	Standard query 0x07e1 A win10.ipv6.microsoft.com

```
> Frame 1451: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.67.128, Dst: 192.168.67.128
> User Datagram Protocol, Src Port: 53, Dst Port: 52370
> Domain Name System (response)

0000  45 00 00 54 62 3f 00 00  80 11 d0 08 c0 a8 43 80   E..Tb?.. ......C.
0010  c0 a8 43 80 00 35 cc 92  00 40 2d d3 c2 1a 85 80   ..C..5...@-.....
```

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (4)

- Quit Noriben and Fakenet-NG.

- Then check the Noriben’s timeline report with glogg.

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (5)

Noriben_04_Jul_18__17_21_078980_timeline.csv - glogg

File Edit View Tools Encoding Help

C:/shortcuts/07_MalwareAnalysis/tools/noriben/Noriben_04_Jul_18__17_21_078980_timeli

```
5:22:02,File,CreateFolder,OneDriveStandaloneUpdater.exe,3212
5:22:02,File,CreateFile,OneDriveStandaloneUpdater.exe,3212,
5:22:02,File,CreateFolder,OneDriveStandaloneUpdater.exe,3212
```

Text: AddinsManager.exe

7 matches found.

Ignore case Auto-refresh

```
110 5:22:20,Process,CreateProcess,Explorer.EXE,2324,%UserProfile%\Desktop\malware\AddinsManager.exe ,3884
111 5:22:20,Registry,RegSetValue,svchost.exe,948,HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibi
113 5:22:20,Registry,RegSetValue,Explorer.EXE,2324,HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{9E3971
115 5:22:20,Network,UDP Send,AddinsManager.exe,3884,c0a8:4380:0:0:0:0:0:0:53
116 5:22:20,Network,UDP Receive,AddinsManager.exe,3884
117 5:22:20,Network,TCP Send,AddinsManager.exe,3884,192.0.2.123:8080
118 5:22:20,Network,TCP Receive,AddinsManager.exe,3884
```

Unfortunately, there are no remarkable entries in process, file and registry activities.

Note that the entries surrounded by the red line are logged when we executed a file from explorer. Therefore, it is not related to the malware.

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (7)

- Summary of the analysis:
  - It accesses “out1ook.net” with CONNECT method via the customer’s proxy server.
    - Note that the fourth character of the domain name is “one”, not “L”.
  - There were no significant entries in file system and registry activities.
  - We could not find any characteristics in the communication. Therefore, we could not identify the malware name at this time.

Scenario 1 Labs: Lab 2
Dynamic Analysis AddinsManager.exe (8)

- Revert the VM to “before dynamic analysis”.
  - Do not forget to save important data before reverting.

Wrap Up

What We Get in This Chapter for Scenario 1

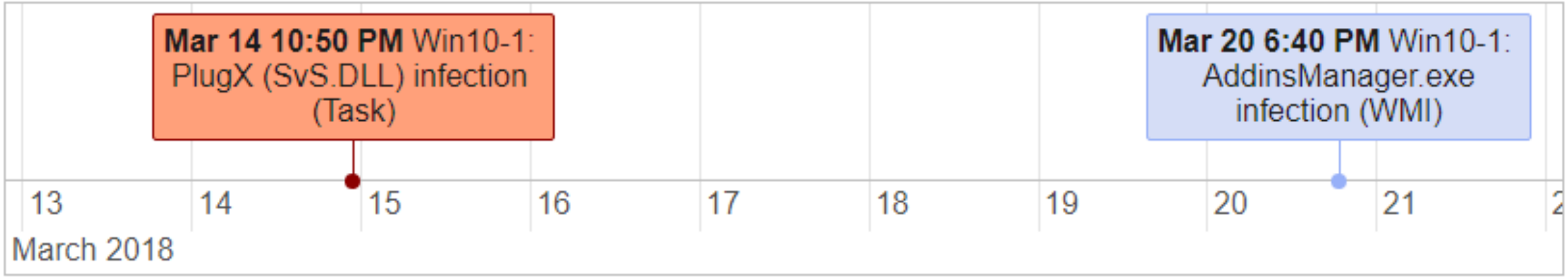
- We got several IoCs.

Malware	Destination	Type	Content (method, header, body...)
PlugX (SvS.DLL)	proxy.ninja-motors.net*	CONNECT METHOD	CONNECT 1ive.net
	1ive.net	POST METHOD	POST /update?id=[a-z0-9]{8} HTTP/1.1
		HTTP Header	X-Session: 0
		HTTP Header	X-Status: 0
		HTTP Header	X-Size: 61456
		HTTP Header	X-Sn: 1
		HTTP Header	User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
unknown malware (AddinsManager.exe)	proxy.ninja-motors.net*	CONNECT METHOD	CONNECT out1ook.net
	out1ook.net		-

*proxy.ninja-motors.net is a legitimate HTTP proxy server of the victim environment.

What We Get in This Chapter for Scenario 1

- PlugX is used in targeted attacks frequently. Therefore, there is a possibility that this incident was a targeted attack.



- We will need to perform network forensics such as proxy log analysis using the information to see if there are any other infected machines in the network.
  - It is likely to happen as they were able to put the malware in “C:\Windows” and execute it with SYSTEM privilege on Client-Win10-1.

What We Learned in This Chapter

- We can get the effective and efficient results required for incident response in a short period by performing surface and dynamic analysis.
  - Finding important IoCs is essential for investigating how far the infection had spread at the initial phase of the incident response.
  - For this purpose, we need to perform this quick analysis.

Appendix 1: Change Log of Fakenet Configuration

fakenet\configs\default.ini

```
--- default.ini.orig 2019-02-02 01:57:06.000000000 +0900
+++ default.ini  2019-07-05 15:35:48.570152816 +0900
@@ -46,7 +46,7 @@
 #    NFQUEUE    NetfilterQueue activity (Linux only)
 #    PROCFS     Procfs read/write activity (Linux only)
 #    IPTABLES   iptables firewall rule activity (Linux only)
-DebugLevel:            Off
+DebugLevel:            DPF

 # MultiHost mode only: Specify what interfaces the Linux Diverter should create
 # an iptables rule for to redirect traffic destined for other hosts to the
@@ -207,7 +207,7 @@
 Enabled:    True
 Protocol:   TCP
 Listener:   ProxyListener
-Port:       38926
+Port:       8080
 Listeners:  HTTPListener, RawListener, FTPListener, DNSListener, POPListener, SMTPListener,
TFTPListener, IRCListener, BITSListener
 Hidden:     False
```

Tools

- Process Monitor (Procmon)
  - https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
- Noriben
  - https://github.com/Rurik/Noriben
- Fakenet-NG
  - https://github.com/fireeye/flare-fakenet-ng
- Process Hacker
  - https://processhacker.sourceforge.io/
- Wireshark
  - https://www.wireshark.org/
- glogg
  - https://glogg.bonnefon.org/download.html