Basic Dynamic Analysis

Monitors everything!

Fareed

- Interested in Malware Analysis, Incident Response and Reverse Engineering.
- Currently focus on WannaCry analysis
- ~2 years in exploring reverse engineering
- Played/Won CTFs in the past

Note that…

- This icon  meaning that we going to have some practical on the subtopic after the lecture.

Let’s recap some important points

Malware definition

“Software intentionally designed to harm user’s computer or data”

Goals of Malware Analysis

Description
To provide information in a need to response to a network intrusion
To evaluate the damage
To find the root cause
To discover indicator of compromise
To evaluate the level of intruder
To increase level of security perimeter
Business justification

Business Justification

Description
What type of data the malware access?
Did the malware steal anything?
How it passed the security perimeter?
What are we lacked of?
Can our vendor detect this?
How to prevent this?
and many more…

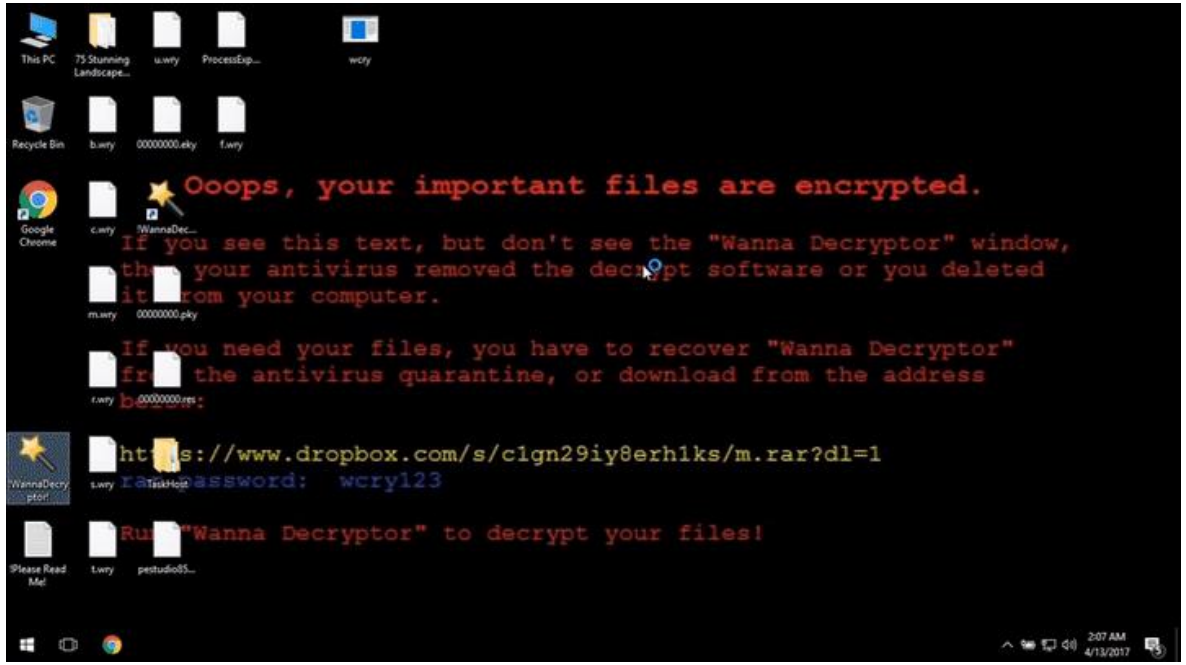
Static vs Dynamic Analysis

- Static Analysis
  - Code is not executed
  - Whitebox
- Dynamic Analysis
  - Observing and controlling running “live” program.
  - Blackbox
- The best way is to combine them

Dynamic Behavior Analysis

What it is?

- Running malware deliberately, while monitoring the results
- Observing and monitoring its behavior of the malware
- Requires a safe environment



Real Machines

- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so reimaging the machine will be necessary
- Advantage
  - Some malware detects virtual machines and won't run properly in one

Virtual Machines

- The most common method
- We'll do it that way
- This protects the host machine from the malware
- Except for a few very rare cases of malware that escape the virtual machine and infect the host
- We will use VirtualBox

What it is? (cont.)

- Analyse a sample in an isolate environment
- As soon as we run an unknown piece of code on our system, nothing writable can be trusted
- Setup our own environment
  - With various of tools installed
  - Our nice and safe environment wasn't important during static analysis.
  - Snapshot is a must!
    - Makes life easier and safer
    - We will need to run the malware many times

Snapshots

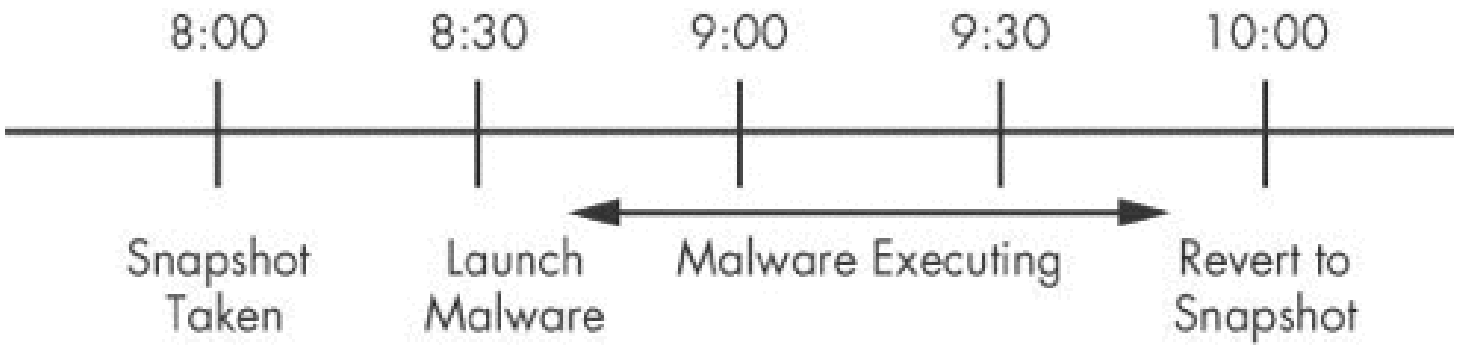


Figure 3-5. Snapshot timeline

What it is? (cont.)

- FlareVM
  - The windows malware analysis distribution you've (malware analyst) always needed!
  - Freely available and open sourced Windows-based security distribution
  - Fully installed collection of tools
  - Designed for
    - reverse engineers,
    - malware analysts,
    - incident responders,
    - forensicates,
    - and penetration testers.

What it is? (cont.)

- Monitoring
  - Activities of the malware
  - Interaction of network communication
  - Effect on the system

Why perform Dynamic Analysis?

- Static analysis can reach a dead-end, due to
  - Obfuscation
  - Packing
  - Examiner has exhausted the available static analysis techniques
- Dynamic analysis is efficient and will show you exactly what the malware does

Sandbox

- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

Let’s have a quick and short quiz on kahoot.it

Types of monitoring

- Process monitoring
  - process activity
  - examining the properties of the process
- File system monitoring
  - real-time file system activity
- Registry monitoring
  - registry keys accessed/modified
  - registry data that is being read/written
- Network monitoring
  - live traffic in and out of the system

System And Network Monitoring

- Monitoring malware's interaction help us gaining better understanding about the malware.
- Observe the malware's true functionality
  - Example, locate the keylogger's log file on the system
  - Try to change execute cmd command

System and Network Monitoring

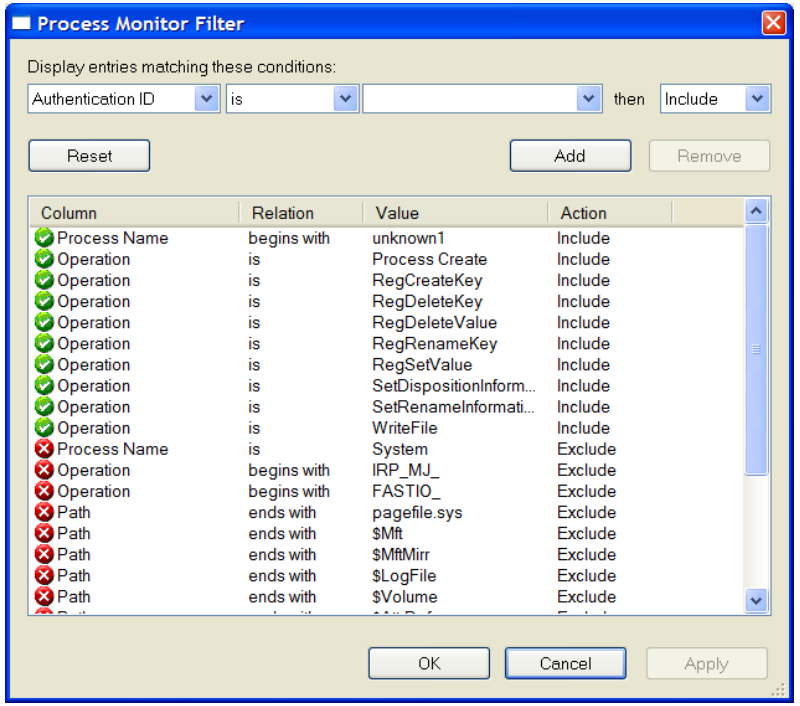
- It interact with a system in various ways and perform different activities.
  - spawn a child process
  - drop additional files
  - create registry keys and values for its persistence
  - download other components
- The objective is
  - to gather real-time data related to malware behaviour
  - and its the impact on the system.

Tools

- Process Monitor
  - registry, file system, network, process, and thread activity.
  - All recorded events are kept, but you can filter the display to make it easier to find items of interest
  - Don't run it too long or it will fill up all RAM and crash the machine

Process Monitor

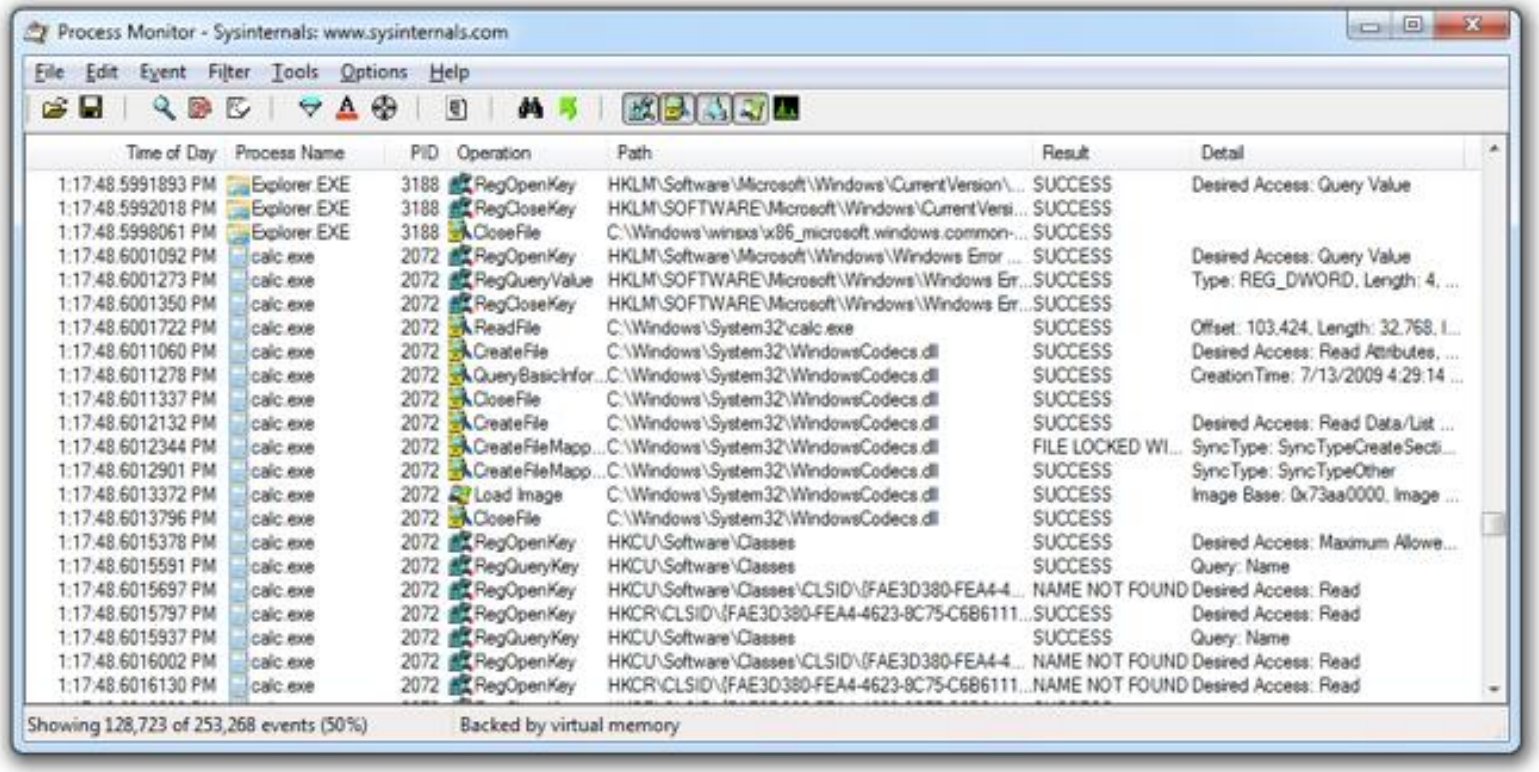
- Procmon is a SysInternal tool that records information about file system, registry and Process/Thread activity
- The key effective use of ProcMon for malware analysis is their filter feature



Monitoring with Process Monitor

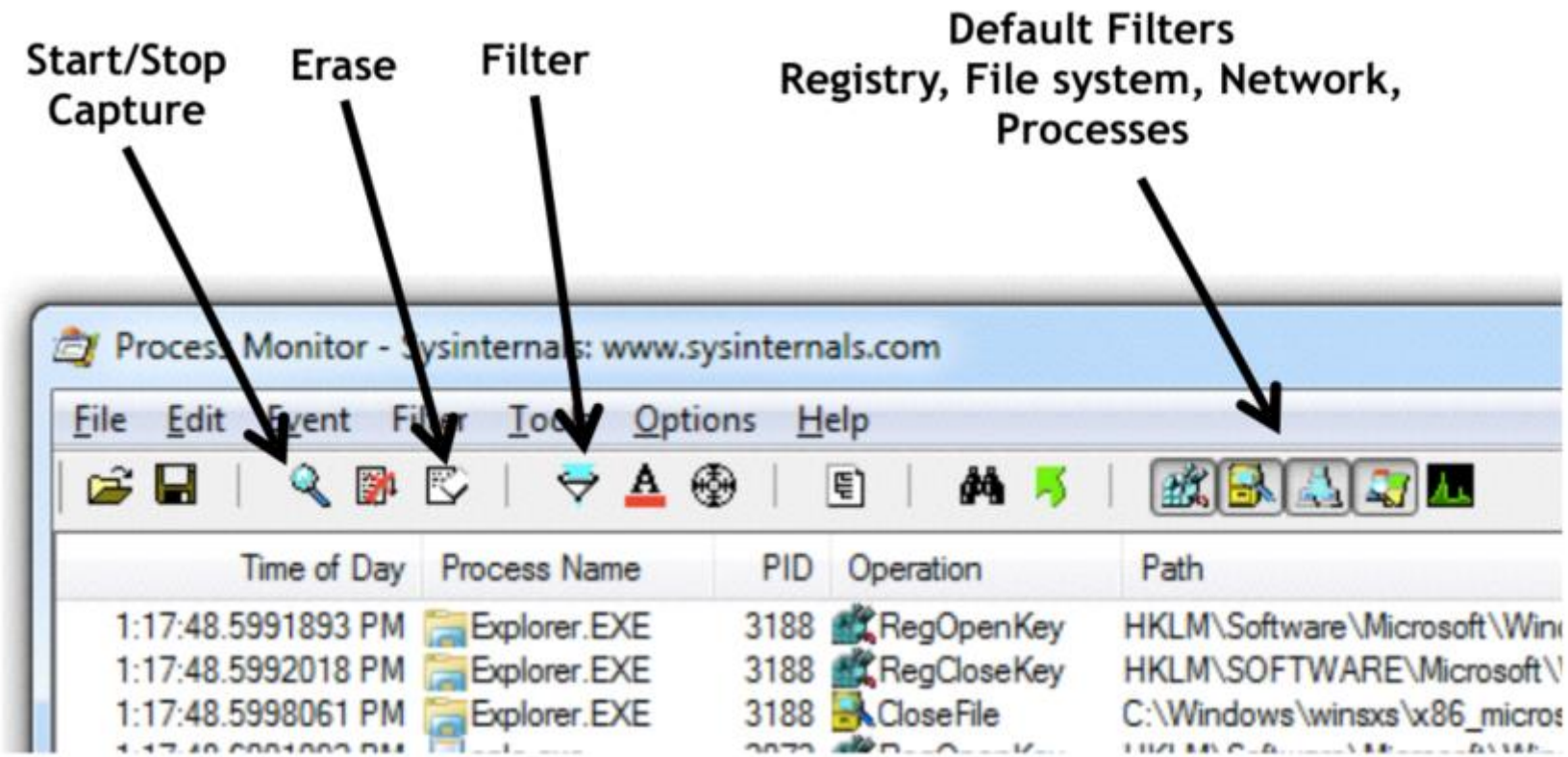
Launching Calc.exe

- Many, many events recorded



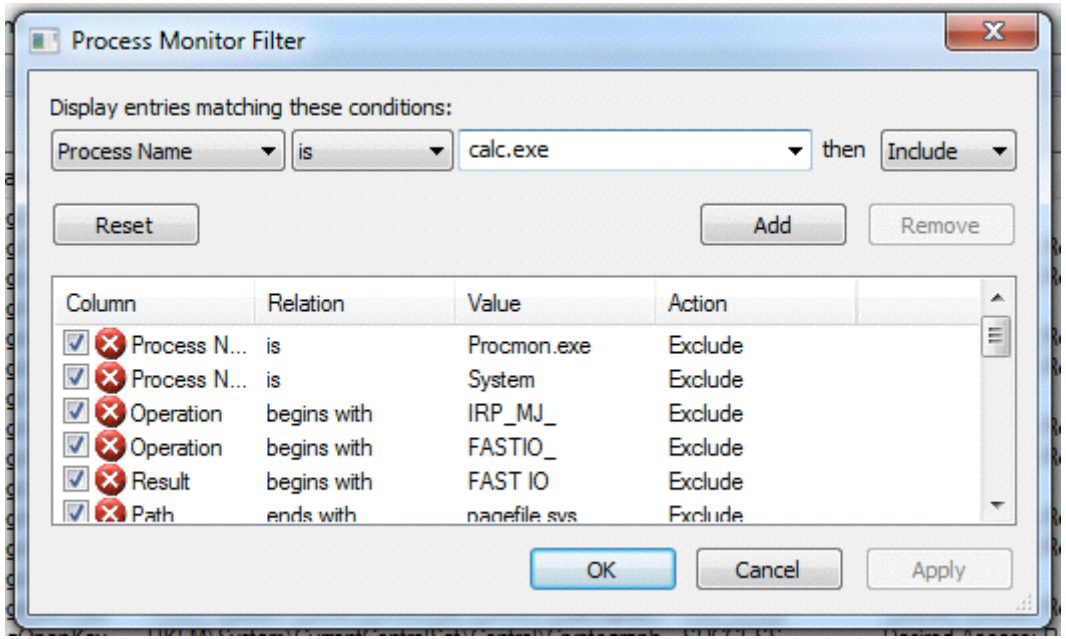
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: Query Value
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi...	SUCCESS	
1:17:48.5998061 PM	Explorer.EXE	3188	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-...	SUCCESS	
1:17:48.6001092 PM	calc.exe	2072	RegOpenKey	HKLM\Software\Microsoft\Windows\Windows Error ...	SUCCESS	Desired Access: Query Value
1:17:48.6001273 PM	calc.exe	2072	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\Windows Er...	SUCCESS	Type: REG_DWORD, Length: 4, ...
1:17:48.6001350 PM	calc.exe	2072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Windows Er...	SUCCESS	
1:17:48.6001722 PM	calc.exe	2072	ReadFile	C:\Windows\System32\calc.exe	SUCCESS	Offset: 103,424, Length: 32,768, I...
1:17:48.6011060 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Attributes, ...
1:17:48.6011278 PM	calc.exe	2072	QueryBasicInfor...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	CreationTime: 7/13/2009 4:29:14 ...
1:17:48.6011337 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6012132 PM	calc.exe	2072	CreateFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Desired Access: Read Data/List ...
1:17:48.6012344 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSecti...
1:17:48.6012901 PM	calc.exe	2072	CreateFileMapp...	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	SyncType: SyncTypeOther
1:17:48.6013372 PM	calc.exe	2072	Load Image	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	Image Base: 0x73aa0000, Image ...
1:17:48.6013796 PM	calc.exe	2072	CloseFile	C:\Windows\System32\WindowsCodecs.dll	SUCCESS	
1:17:48.6015378 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: Maximum Allowe...
1:17:48.6015591 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6015697 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6015797 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	SUCCESS	Desired Access: Read
1:17:48.6015937 PM	calc.exe	2072	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
1:17:48.6016002 PM	calc.exe	2072	RegOpenKey	HKCU\Software\Classes\CLSID\{FAE3D380-FEA4-4...	NAME NOT FOUND	Desired Access: Read
1:17:48.6016130 PM	calc.exe	2072	RegOpenKey	HKCR\CLSID\{FAE3D380-FEA4-4623-8C75-C6B6111...	NAME NOT FOUND	Desired Access: Read

Process Monitor Toolbar



Filtering with Include

- Most useful filters: Process Name, Operation, and Detail



Viewing Processes with Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [W7\student]

File Options View Process Find Users Help

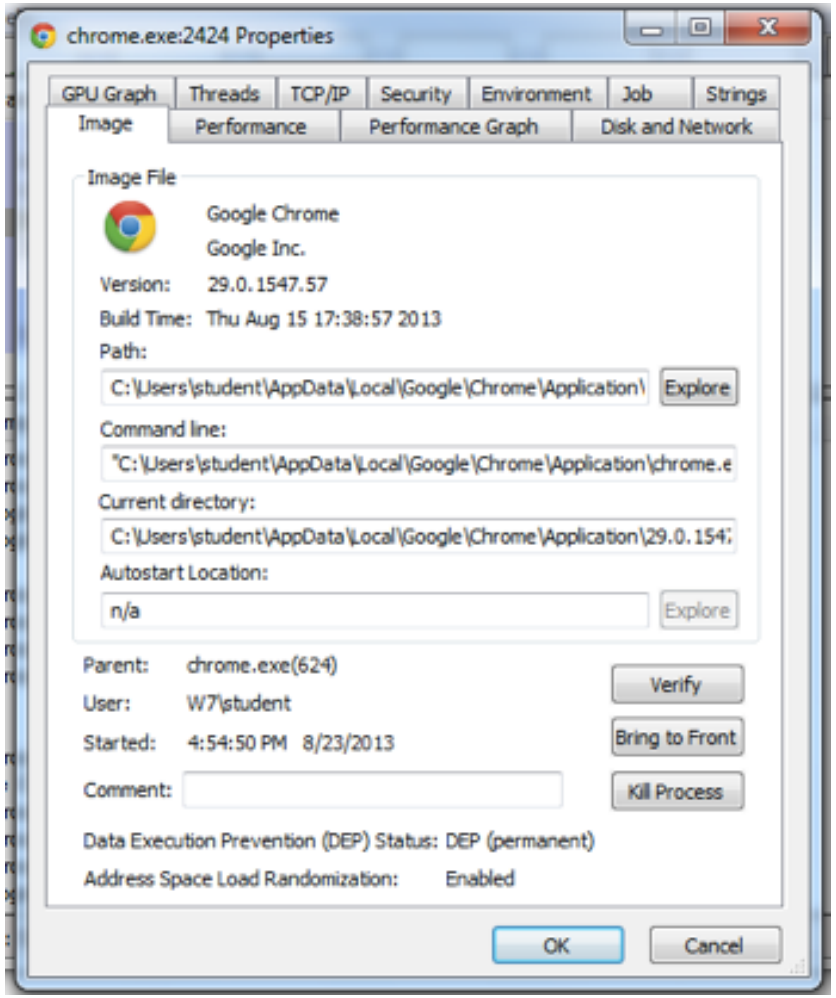
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	96.81	0 K	24 K		
System	4	0.09	48 K	560 K		
Interrupts	n/a	0.88	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	260		224 K	748 K	Windows Session Manager	Microsoft Corporation
csrss.exe	348	< 0.01	1,252 K	3,164 K	Client Server Runtime Process	Microsoft Corporation
wininit.exe	400		892 K	3,084 K	Windows Start-Up Application	Microsoft Corporation
services.exe	504	0.01	3,972 K	6,640 K	Services and Controller app	Microsoft Corporation
svchost.exe	652		2,700 K	6,024 K	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	1716		6,176 K	4,804 K	COM Surrogate	Microsoft Corporation
WmiPrvSE.exe	740		1,804 K	4,736 K	WMI Provider Host	Microsoft Corporation
svchost.exe	724	< 0.01	2,972 K	6,012 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	772		13,776 K	11,760 K	Host Process for Windows S...	Microsoft Corporation
audiodg.exe	3200		14,960 K	13,972 K	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe	912		37,940 K	42,292 K	Host Process for Windows S...	Microsoft Corporation
dwm.exe	3248	0.74	61,892 K	27,976 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	936	0.02	20,836 K	29,900 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1116	0.03	5,136 K	8,340 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1260	0.06	10,840 K	11,960 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1352		5,392 K	7,436 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1388		6,752 K	8,720 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1500		2,472 K	4,712 K	Host Process for Windows S...	Microsoft Corporation
gogoc.exe	1592	< 0.01	1,216 K	3,920 K	gogoCLIENT	gogo6, Inc.
vmtoolsd.exe	1728	0.07	7,260 K	10,368 K	VMware Tools Core Service	VMware, Inc.
svchost.exe						

CPU Usage: 3.19% Commit Charge: 21.92% Processes: 57 Physical Usage: 30.24%

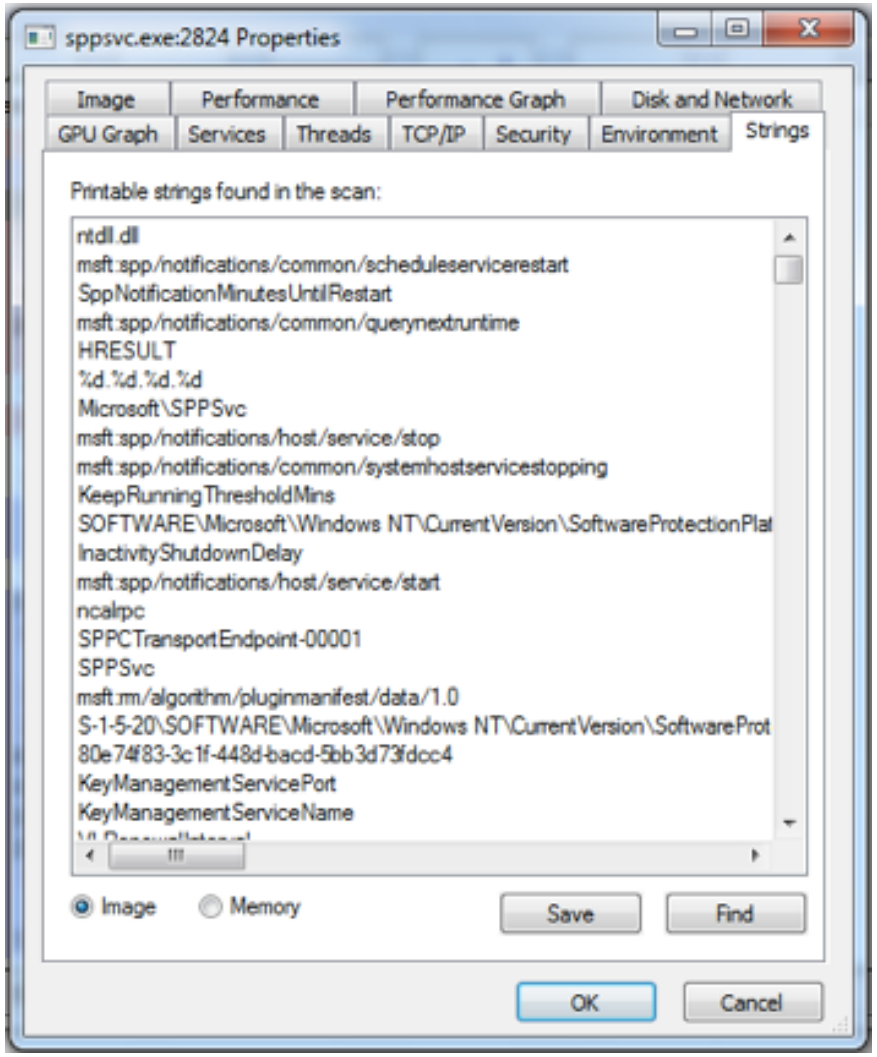
Coloring

- Services are pink
- Processes are blue
- New processes are green briefly
- Terminated processes are red

Properties


chrome.exe:2424 Properties
GPU Graph
Threads
TCP/IP
Security
Environment
Job
Strings
Image
Performance
Performance Graph
Disk and Network
Image File
Google Chrome
Google Inc.
Version: 29.0.1547.57
Build Time: Thu Aug 15 17:38:57 2013
Path:
C:\Users\student\AppData\Local\Google\Chrome\Application\
Explore
Command line:
"C:\Users\student\AppData\Local\Google\Chrome\Application\chrome.e
Current directory:
C:\Users\student\AppData\Local\Google\Chrome\Application\29.0.154
Autostart Location:
n/a
Explore
Parent: chrome.exe(624)
User: W7\student
Started: 4:54:50 PM 8/23/2013
Comment:
Verify
Bring to Front
Kill Process
Data Execution Prevention (DEP) Status: DEP (permanent)
Address Space Load Randomization: Enabled
OK
Cancel

Strings


sppsvc.exe:2824 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Services
Threads
TCP/IP
Security
Environment
Strings
Printable strings found in the scan:
ntdll.dll
msft:spp/notifications/common/scheduleservicerestart
SppNotificationMinutesUntilRestart
msft:spp/notifications/common/querynextruntime
HRESULT
%d.%d.%d.%d
Microsoft\SPPSvc
msft:spp/notifications/host/service/stop
msft:spp/notifications/common/systemhostservicestopping
KeepRunningThresholdMins
SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlat
InactivityShutdownDelay
msft:spp/notifications/host/service/start
ncalrpc
SPPCTransportEndpoint-00001
SPPSvc
msft:rm/algorithm/pluginmanifest/data/1.0
S-1-5-20\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProt
80e74f83-3c1f-448d-bacd-5bb3d73fdcc4
KeyManagementServicePort
KeyManagementServiceName
Image
Memory
Save
Find
OK
Cancel

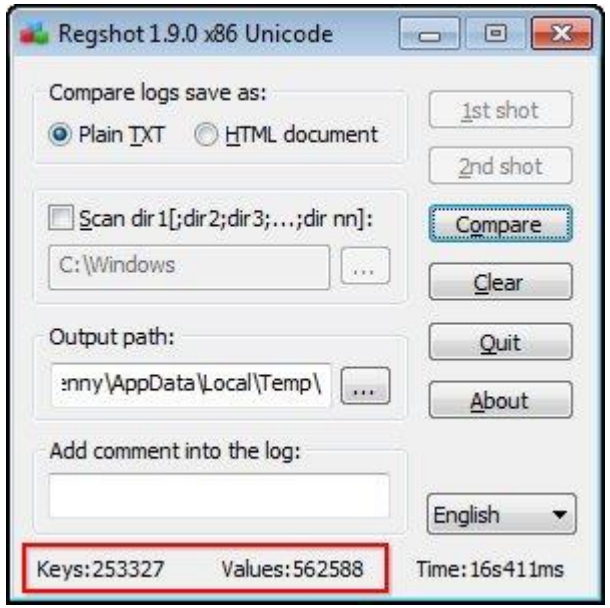
Detecting Malicious Documents

- Open the document (e.g. PDF) on a system with a vulnerable application
- Watch Process Explorer to see if it launches a process
- The Image tab of that process's Properties sheet will show where the malware is

Comparing Registry Snapshots with Regshot

Tools (cont.)

- Regshot
  - open source registry comparison tool that allows you to take and compare two registry snapshots.

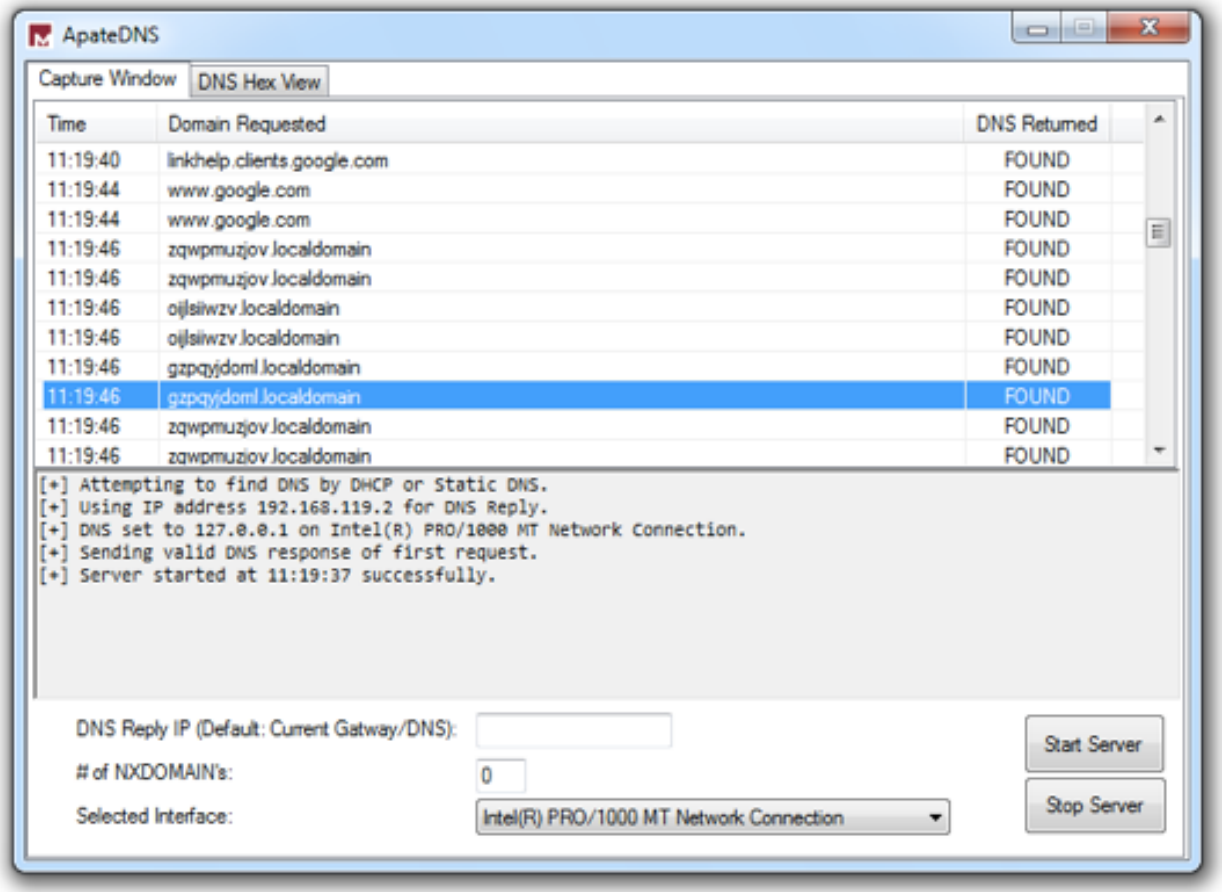


Regshot

- Take 1st shot
- Run malware
- Take 2nd shot
- Compare them to see what registry keys were changed

Faking a Network

Using ApateDNS to Redirect DNS Resolutions



Tools (cont.)

- ApateDNS (Faking a network)
  - ApateDNS™ is a tool for controlling DNS responses though an easy-to-use GUI.
- Flare Fakenet-ng

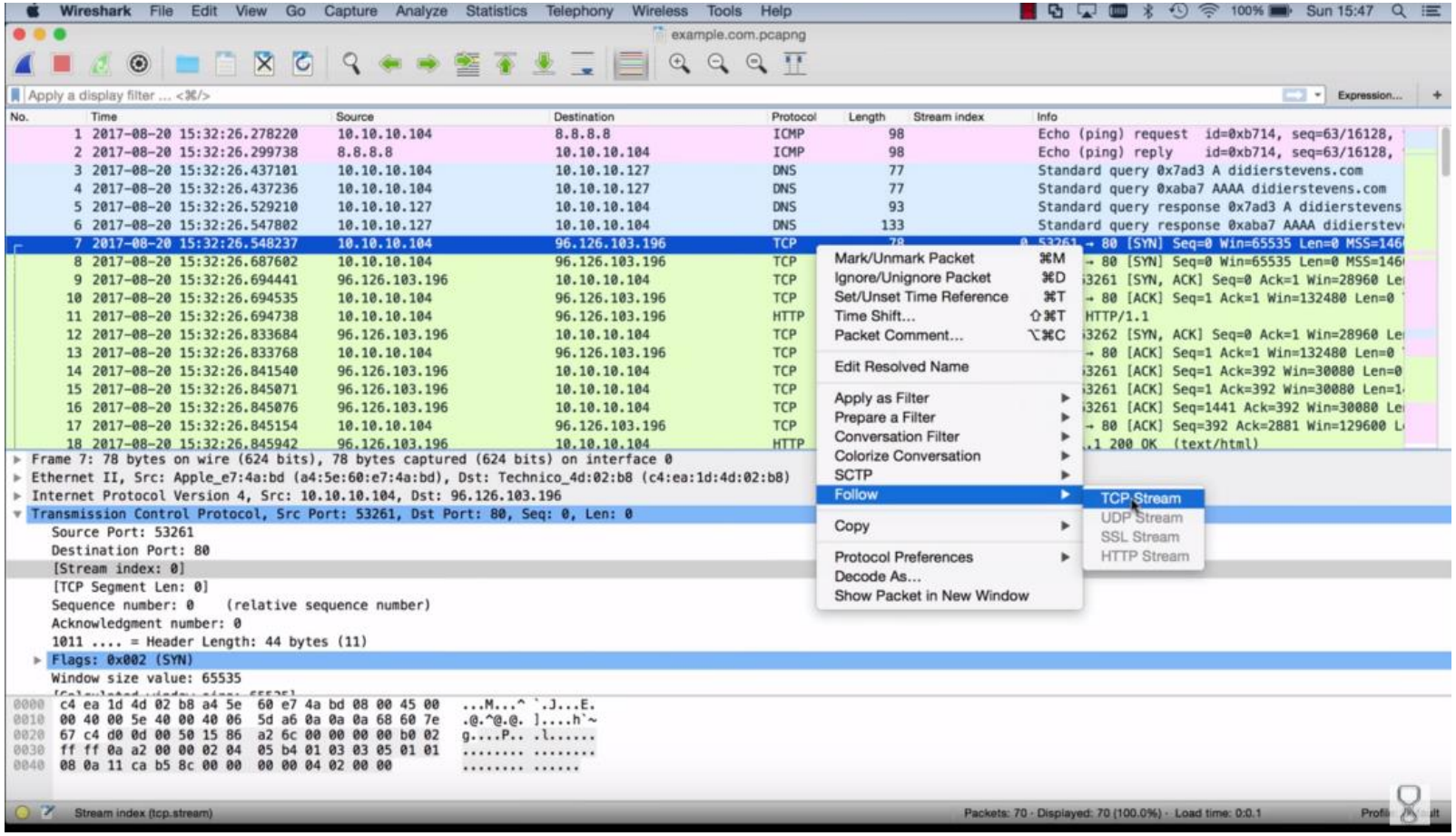
Packet Sniffing with Wireshark

Wireshark

- Protocol analyzer that captures and decodes network traffic
- As with Process Monitor, the key is using filters to focus on what is relevant

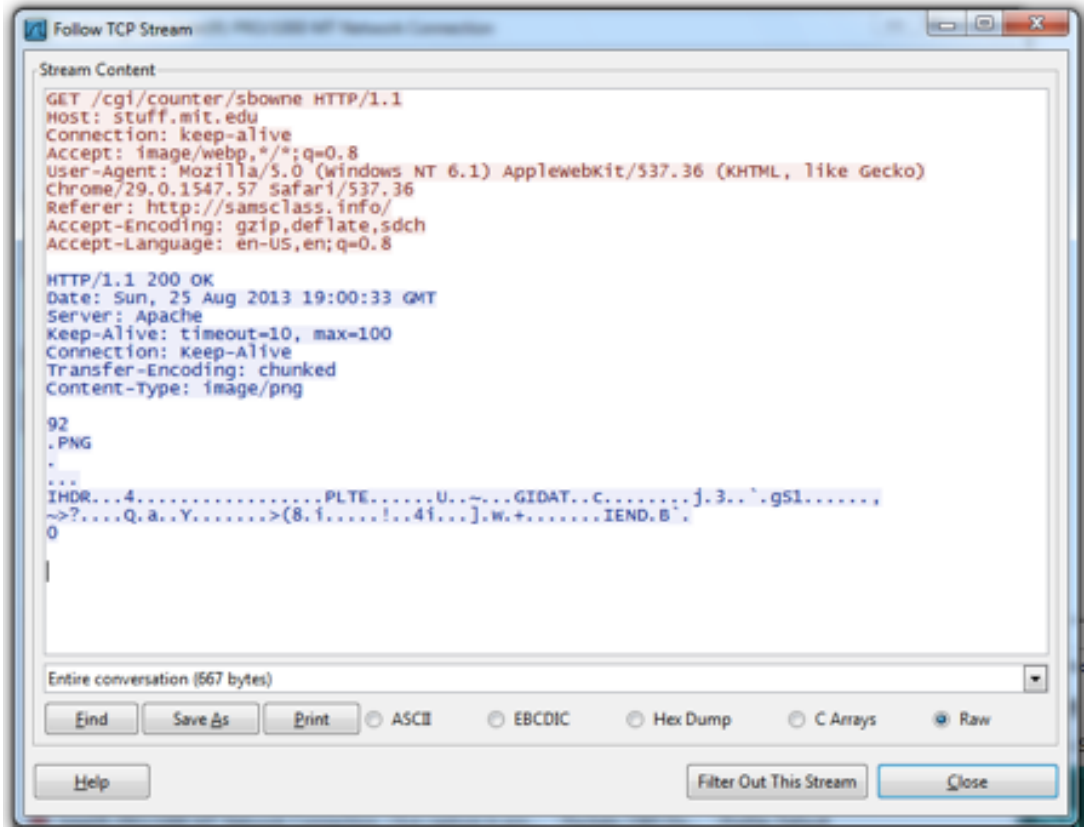
Tools (cont.)

- Wireshark (Capture network)
  - Intercepts and logs network traffic.
  - Help us in understand the communication channel used by the malware
  - Help in determining network-based indicator
  - To use Wireshark for this purpose
    - connect to the Internet or simulate an Internet connection
    - and then start Wireshark's packet capture
    - and run
    - the malware.


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
example.com.pcapng
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Stream index Info
1 2017-08-20 15:32:26.278220 10.10.10.104 8.8.8.8 ICMP 98 Echo (ping) request id=0xb714, seq=63/16128,
2 2017-08-20 15:32:26.299738 8.8.8.8 10.10.10.104 ICMP 98 Echo (ping) reply id=0xb714, seq=63/16128,
3 2017-08-20 15:32:26.437101 10.10.10.104 10.10.10.127 DNS 77 Standard query 0x7ad3 A didierstevens.com
4 2017-08-20 15:32:26.437236 10.10.10.104 10.10.10.127 DNS 77 Standard query 0xaba7 AAAA didierstevens.com
5 2017-08-20 15:32:26.529210 10.10.10.127 10.10.10.104 DNS 93 Standard query response 0x7ad3 A didierstevens
6 2017-08-20 15:32:26.547802 10.10.10.127 10.10.10.104 DNS 133 Standard query response 0xaba7 AAAA didierstev
7 2017-08-20 15:32:26.548237 10.10.10.104 96.126.103.196 TCP 78 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=146
8 2017-08-20 15:32:26.687602 10.10.10.104 96.126.103.196 TCP → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=146
9 2017-08-20 15:32:26.694441 96.126.103.196 10.10.10.104 TCP 3261 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
10 2017-08-20 15:32:26.694535 10.10.10.104 96.126.103.196 TCP → 80 [ACK] Seq=1 Ack=1 Win=132480 Len=0
11 2017-08-20 15:32:26.694738 10.10.10.104 96.126.103.196 HTTP HTTP/1.1
12 2017-08-20 15:32:26.833684 96.126.103.196 10.10.10.104 TCP 3262 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
13 2017-08-20 15:32:26.833768 10.10.10.104 96.126.103.196 TCP → 80 [ACK] Seq=1 Ack=1 Win=132480 Len=0
14 2017-08-20 15:32:26.841540 96.126.103.196 10.10.10.104 TCP 3261 [ACK] Seq=1 Ack=392 Win=30080 Len=0
15 2017-08-20 15:32:26.845071 96.126.103.196 10.10.10.104 TCP 3261 [ACK] Seq=1 Ack=392 Win=30080 Len=1
16 2017-08-20 15:32:26.845076 96.126.103.196 10.10.10.104 TCP 3261 [ACK] Seq=1441 Ack=392 Win=30080 Le
17 2017-08-20 15:32:26.845154 10.10.10.104 96.126.103.196 TCP → 80 [ACK] Seq=392 Ack=2881 Win=129600 L
18 2017-08-20 15:32:26.845942 96.126.103.196 10.10.10.104 HTTP .1 200 OK (text/html)
Frame 7: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: Apple_e7:4a:bd (a4:5e:60:e7:4a:bd), Dst: Technico_4d:02:b8 (c4:ea:1d:4d:02:b8)
Internet Protocol Version 4, Src: 10.10.10.104, Dst: 96.126.103.196
Transmission Control Protocol, Src Port: 53261, Dst Port: 80, Seq: 0, Len: 0
Source Port: 53261
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
1011 .... = Header Length: 44 bytes (11)
Flags: 0x002 (SYN)
Window size value: 65535
0000 c4 ea 1d 4d 02 b8 a4 5e 60 e7 4a bd 08 00 45 00 ...M...^ `.J...E.
0010 00 40 00 5e 40 00 40 06 5d a6 0a 0a 0a 68 60 7e .@.^@.@.]....h`~
0020 67 c4 d0 0d 00 50 15 86 a2 6c 00 00 00 00 b0 02 g....P.. .l......
0030 ff ff 0a a2 00 00 02 04 05 b4 01 03 03 05 01 01 ....
0040 08 0a 11 ca b5 8c 00 00 00 00 04 02 00 00 ....
Mark/Unmark Packet ⌘M
Ignore/Unignore Packet ⌘D
Set/Unset Time Reference ⌘T
Time Shift... ⇧⌘T
Packet Comment... ⌥⌘C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
Stream index (tcp.stream)
Packets: 70 · Displayed: 70 (100.0%) · Load time: 0:0.1

Follow TCP Stream

- Can save files from streams here too



Basic dynamic analysis in practice

1. Reverting to the clean snapshot
2. Running the monitoring/dynamic analysis tools
   - Running Procmon
     - Setting a filter on the malware executable name and clearing out all events just before running.
   - Starting Process Explorer
   - Gathering a first snapshot of the registry using Regshot.
   - Setup fake network simulation
   - Run Wireshark
3. Executing the malware specimen
4. Stopping the monitoring tools
5. Analysing the results