CSec15233
Malicious Software Analysis

Basic Dynamic Analysis

Qasem Abu Al-Haija

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

Dynamic analysis

- It can involve
  - ✓ Monitoring malware as it runs or
  - ✓ Examining the system after the malware has been executed.

- It observes the malware's true functionality,
  - ✓ e.g., locate the keylogger's log file on the system.

Advantages of Dynamic Analysis

- Observe the malware's true functionality
  - Existence of an action string in a binary does not mean the action will actually execute
- Identify malware functionality
  - Example: For Keyloggers, you can:
    - Locate the keylogger's log file on the system.
    - Discover the kinds of records it keeps.
    - Decipher where it sends its information, and so on.

Disadvantages of Dynamic Analysis

- Dynamic analysis can put your network and system at risk.
  - Malware can leak to your host (if no proper protection at host).

- Not all code paths may execute when malware is run.
  - E.g., in case of command-line malware that requires arguments
  - Each argument could execute different program functionality.
  - Without knowing the options, you wouldn't be able to examine all of the program's functionality dynamically.
  - Your best bet will be to use advanced dynamic or static techniques to figure out how to force the malware to execute all its functionality.

Sandboxes:

The Quick-and-Dirty Approach

Sandboxes: The Quick-and-Dirty Approach

- *sandbox* is a security mechanism for running untrusted programs in a safe environment without fear of harming "real" systems.

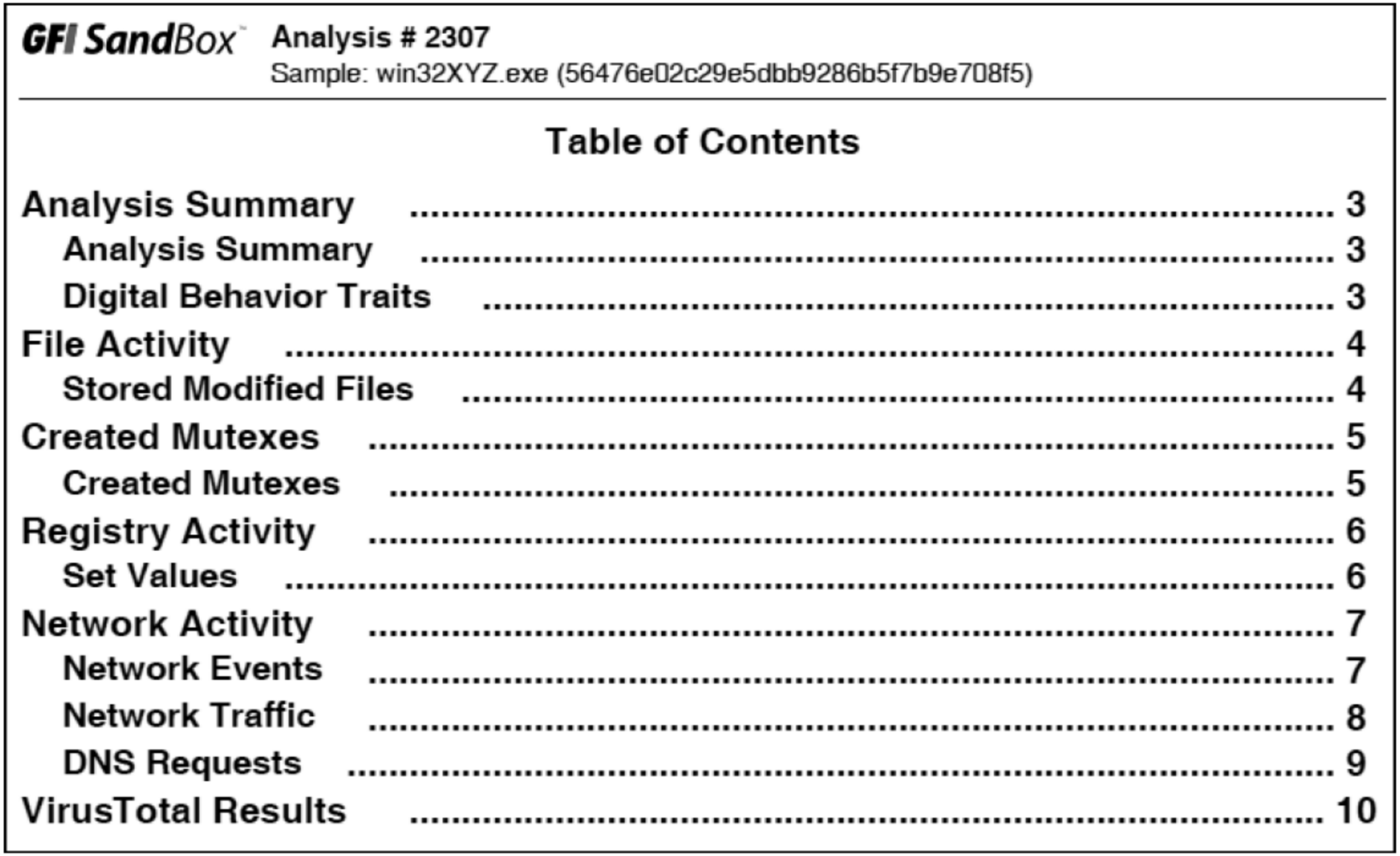
- Sandboxes comprise virtualized environments that
  - Simulate network services to ensure that the software or malware being tested will function normally.

Using a Malware Sandbox

- Many malware sandboxes– will analyze malware for free.
  - Such as Norman SandBox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, and Comodo Instant Malware Analysis
  - These provide easy-to-understand output and are great for initial triage if you are willing to submit your malware to the sandbox websites.

- Even though the sandboxes are automated:
  - you might choose not to submit malware that contains company information to a public website.

GFI Sandbox



GFI SandBox **Analysis # 2307**
Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

Analysis Summary 3
- Analysis Summary 3
- Digital Behavior Traits 3

File Activity 4
- Stored Modified Files 4

Created Mutexes 5
- Created Mutexes 5

Registry Activity 6
- Set Values 6

Network Activity 7
- Network Events 7
- Network Traffic 8
- DNS Requests 9

VirusTotal Results 10

Figure 3-1: GFI Sandbox sample results for win32XYZ.exe

Free Online Automated Malware Analysis

- Hybrid Analysis. Note: good
- sandbox.pikker.ee. Note: good
- Akana (Android files)
- Binary Guard True Bare Metal
- Intezer Analyze (Community Edition)
- Comodo Valkyrie
- Detux Sandbox (Linux binaries)
- Joe Sandbox Cloud (Community Edition)
- Malwr (also see MalwareViz). Note: down
- SecondWrite (free version)
- ThreatExpert
- ThreatTrack
- ViCheck

Sandbox Drawbacks (1)

- Sandbox simply runs the executable, without command-line options.
  - If the malware executable requires command-line options, it will not execute any code that runs only when an option is provided.
  - If your subject malware is waiting for a command-and-control packet to be returned before launching a backdoor, the backdoor will not be launched in the sandbox.

- The sandbox may not record all events, because neither you nor the sandbox may wait long enough.
  - For example, if the malware is set to sleep for a day before it performs malicious activity, you may miss that event.
  - Most sandboxes hook the Sleep function and set it to sleep only briefly, but there is more than one way to sleep, and the sandboxes cannot account for all of these.

Sandbox Drawbacks (2)

- Malware often detects when it is running in a VM.
  - If a VM is detected, the malware might stop running or behave differently.
  - Not all sandboxes take this issue into account.

- Some malware requires the presence of certain registry keys or files on the system that might not be found in the sandbox.
  - legitimate data, such as commands or encryption keys.

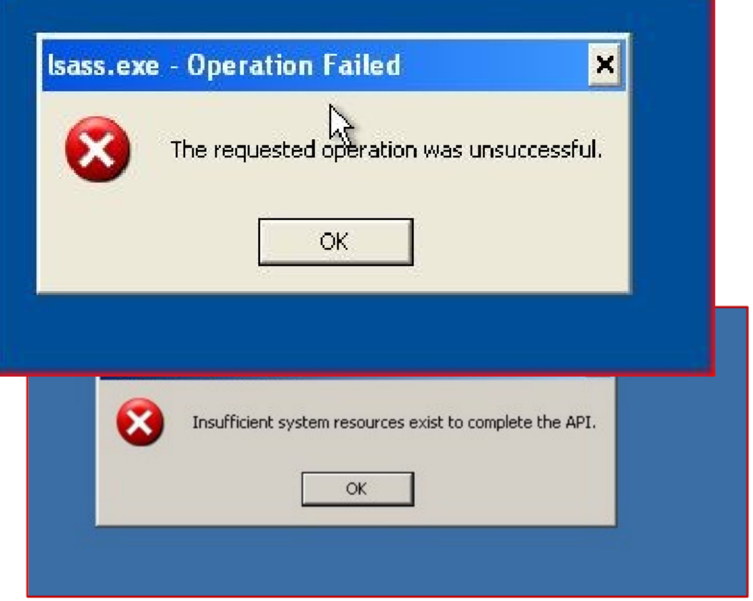
Sandbox Drawbacks (3)

- If the malware is a DLL, certain exported functions will not be invoked properly.
  - Because a DLL will not run as easily as an executable.

- Sandbox environment OS may not be correct for malware.
  - For example, the malware might crash on Win XP but run correctly in Win 7.

- A sandbox cannot tell you what the malware does.
  - It may report basic functionality, but it cannot tell you, for example, if the malware is a custom Security Accounts Manager (SAM) hash dump utility.
  - Those are conclusions that you must draw on your own.

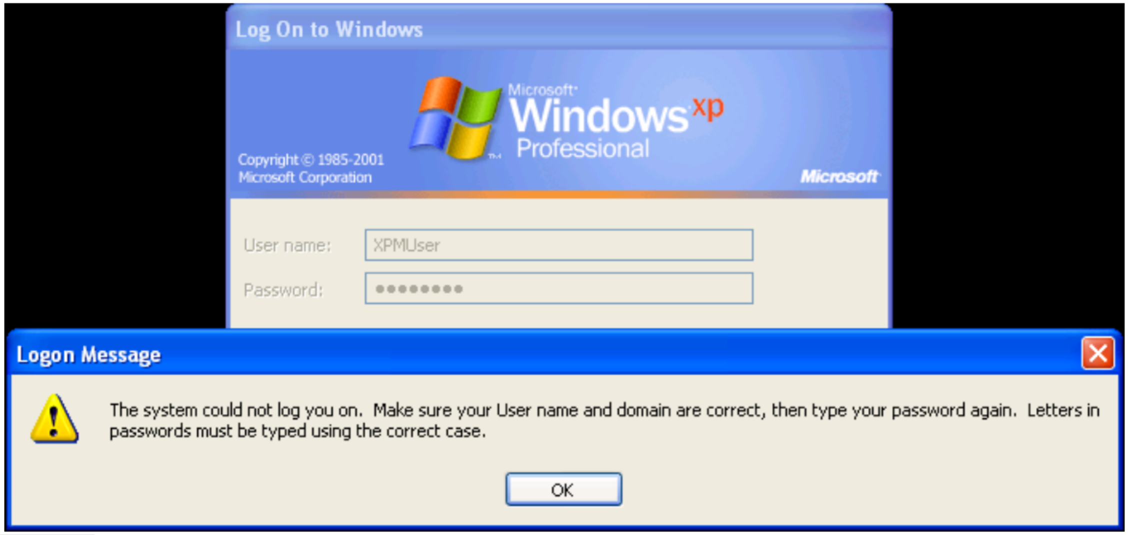
SAM



lsass.exe - Operation Failed

The requested operation was unsuccessful.

Insufficient system resources exist to complete the API.



Log On to Windows

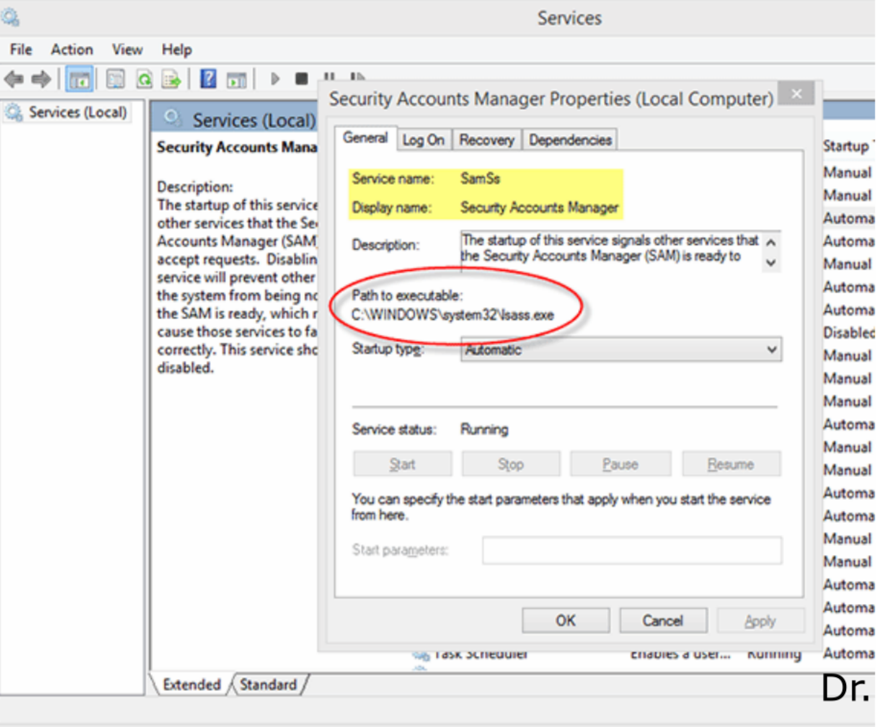
Copyright © 1985-2001 Microsoft Corporation

User name: XPMUser

Password: ●●●●●●●●

Logon Message

The system could not log you on. Make sure your User name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.



Services

Security Accounts Manager Properties (Local Computer)

Service name: SamSs

Display name: Security Accounts Manager

Description: The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to

Path to executable:
C:\WINDOWS\system32\lsass.exe

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Security Accounts Mana

Description:
The startup of this service other services that the Se Accounts Manager (SAM accept requests. Disablin service will prevent other the system from being nc the SAM is ready, which r cause those services to fa correctly. This service shc disabled.

Lsass.exe
Local Security Authority
Subsystem Service

Running Malware

Running Malware

- EXE files can be run directly, but DLLs can't

- Use **Rundll32.exe** (included in Windows)

  ➔ *rundll32.exe DLLname, Export arguments*

- The Export value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer.

Running Malware

- Example: rip.dll has these exports: Install and Uninstall: **rundll32.exe rip.dll, Install**

- Some functions use ordinal values instead of names, like: **rundll32.exe xyzzy.dll, #5**

- It's also possible to modify the PE header and convert a DLL into an EXE

Monitoring with Process Monitor

Monitoring with Process Monitor (procmon)

- Advanced monitoring tool for Windows
  - Monitor certain registry, file system, network, process, and thread activity.
  - Combines two legacy tools: FileMon and RegMon.

- 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
  - Procmon monitors all system calls it can gather as soon as it is run.
  - Procmon uses RAM to log events!

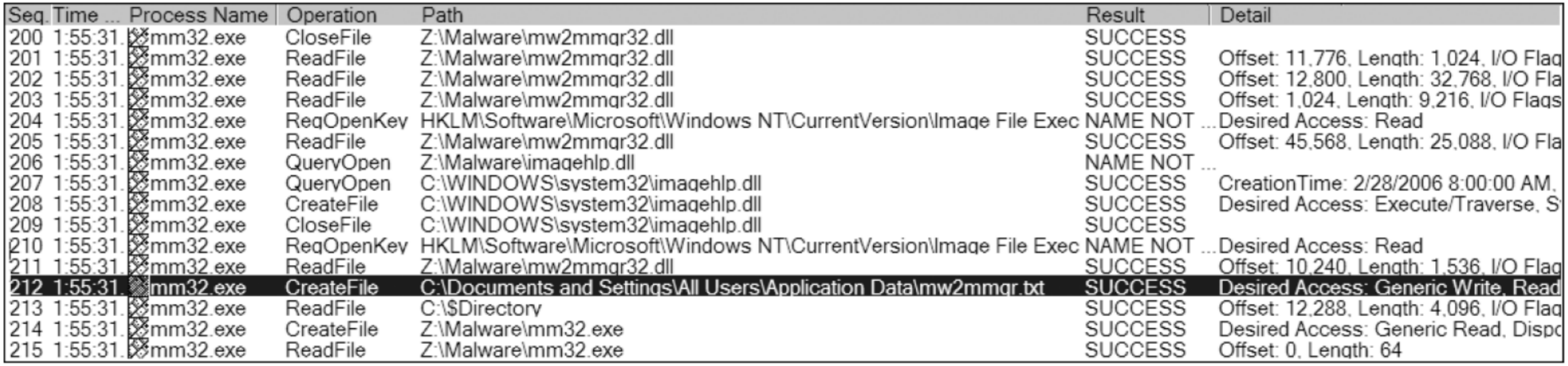
Monitoring with Process Monitor (procmon)

Procmon captures much data but doesn't capture everything.

- For example, It can miss:
  - Device driver activity of a user-mode component
    - talking to a rootkit via *device I/O controls*,
  - Certain GUI calls, such as *SetWindowsHookEx*.

Procmon Display

- Procmon displays configurable columns containing information about individual events, including the event's
  - sequence number,
  - timestamp,
  - name of the process causing the event,
  - event operation,
  - path used by the event, and
  - result of the event.

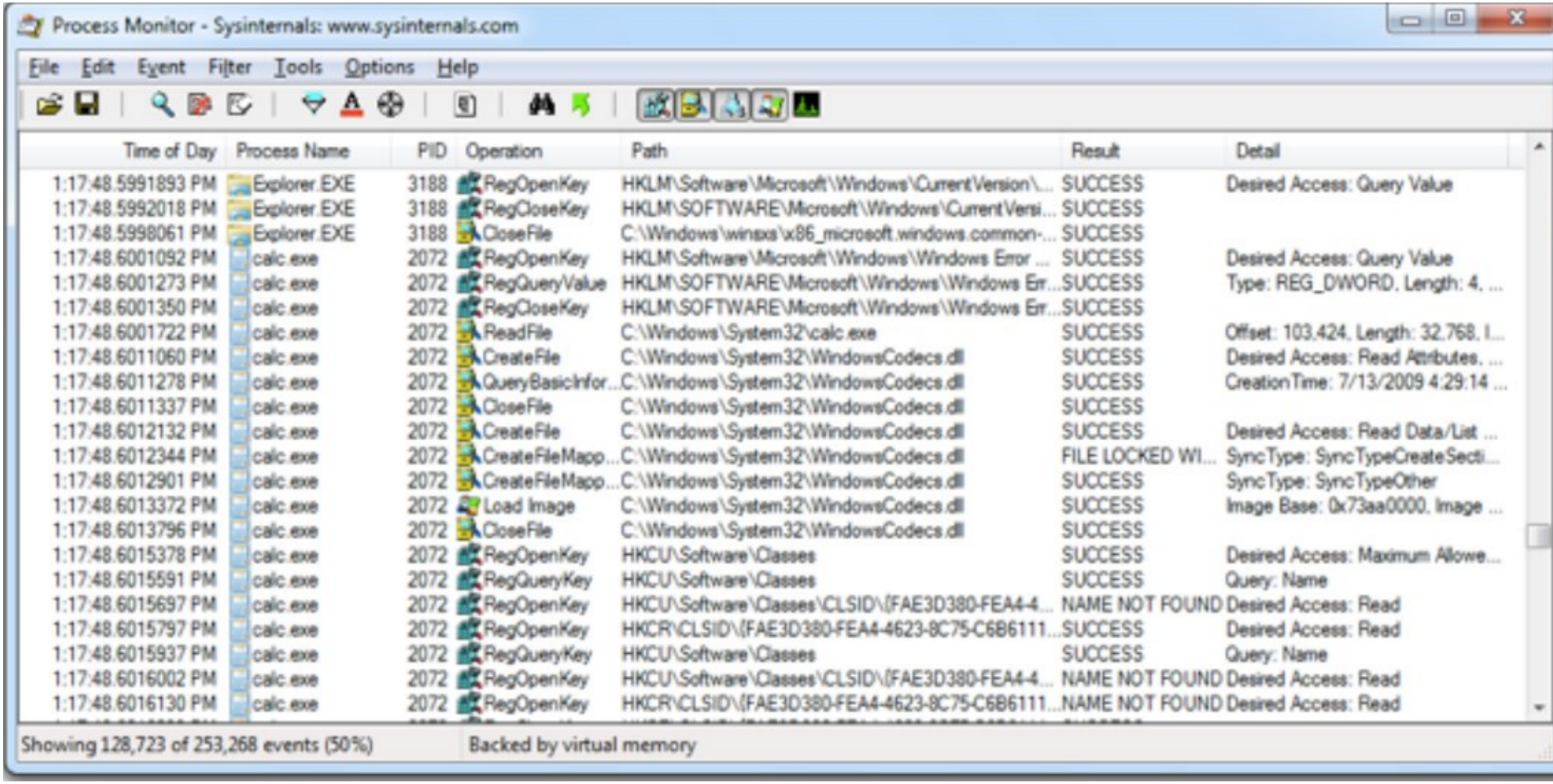


Seq.	Time ...	Process Name	Operation	Path	Result	Detail
200	1:55:31.	mm32.exe	CloseFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	
201	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 11,776, Length: 1,024, I/O Flag
202	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 12,800, Length: 32,768, I/O Fla
203	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 1,024, Length: 9,216, I/O Flags
204	1:55:31.	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT ...	Desired Access: Read
205	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 45,568, Length: 25,088, I/O Fla
206	1:55:31.	mm32.exe	QueryOpen	Z:\Malware\imagehlp.dll	NAME NOT ...	
207	1:55:31.	mm32.exe	QueryOpen	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	CreationTime: 2/28/2006 8:00:00 AM,
208	1:55:31.	mm32.exe	CreateFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	Desired Access: Execute/Traverse, S
209	1:55:31.	mm32.exe	CloseFile	C:\WINDOWS\system32\imagehlp.dll	SUCCESS	
210	1:55:31.	mm32.exe	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT ...	Desired Access: Read
211	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mw2mmgr32.dll	SUCCESS	Offset: 10,240, Length: 1,536, I/O Flag
212	1:55:31.	mm32.exe	CreateFile	C:\Documents and Settings\All Users\Application Data\mw2mmgr.txt	SUCCESS	Desired Access: Generic Write, Read
213	1:55:31.	mm32.exe	ReadFile	C:\$Directory	SUCCESS	Offset: 12,288, Length: 4,096, I/O Flag
214	1:55:31.	mm32.exe	CreateFile	Z:\Malware\mm32.exe	SUCCESS	Desired Access: Generic Read, Dispo
215	1:55:31.	mm32.exe	ReadFile	Z:\Malware\mm32.exe	SUCCESS	Offset: 0, Length: 64

Figure 3-2: Procmon mm32.exe *example*

Launching Calc.exe

- Many, many events recorded



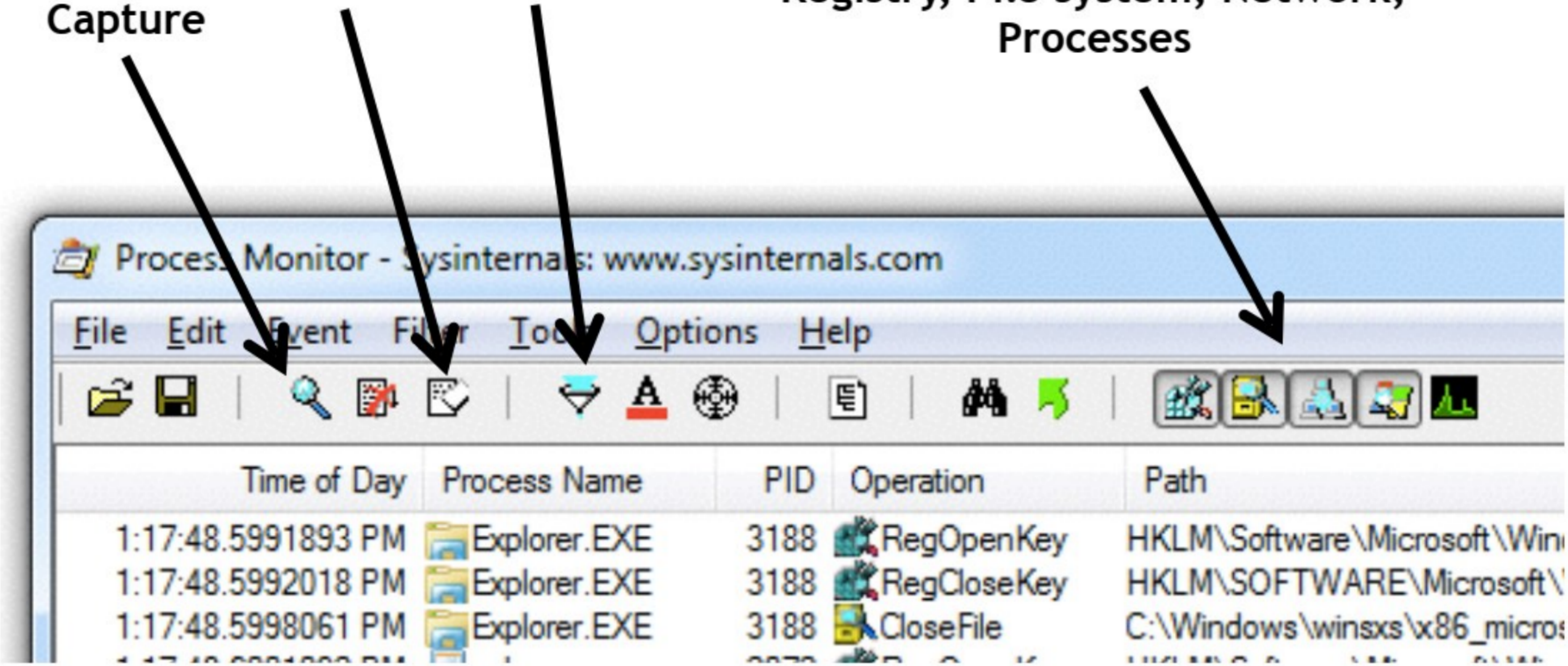
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:17:48.5991893 PM	Explorer.EXE	3188	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\...	SUCCESS	Desired Access: Query Value
1:17:48.5992018 PM	Explorer.EXE	3188	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersi...	SUCCESS	
1:17:48.5998061 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 Err...	SUCCESS	Type: REG_DWORD, Length: 4, ...
1:17:48.6001350 PM	calc.exe	2072	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Windows Err...	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

Showing 128,723 of 253,268 events (50%)

Backed by virtual memory

Process Monitor Toolbar

- Many, many events recorded



Start/Stop Capture

Erase

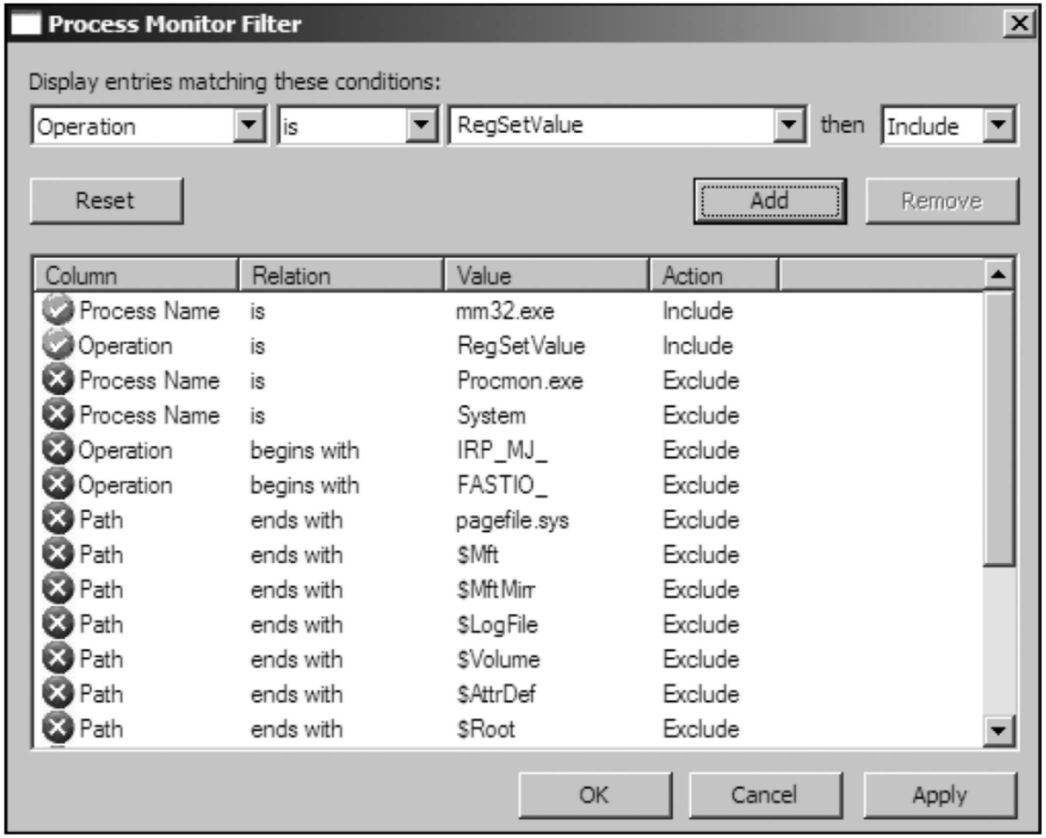
Filter

Default Filters
Registry, File system, Network, Processes

```
Time of Day          Process Name   PID   Operation     Path
1:17:48.5991893 PM   Explorer.EXE   3188  RegOpenKey    HKLM\Software\Microsoft\Win
1:17:48.5992018 PM   Explorer.EXE   3188  RegCloseKey   HKLM\SOFTWARE\Microsoft\
1:17:48.5998061 PM   Explorer.EXE   3188  CloseFile     C:\Windows\winsxs\x86_micros
```

Procmon Filtering

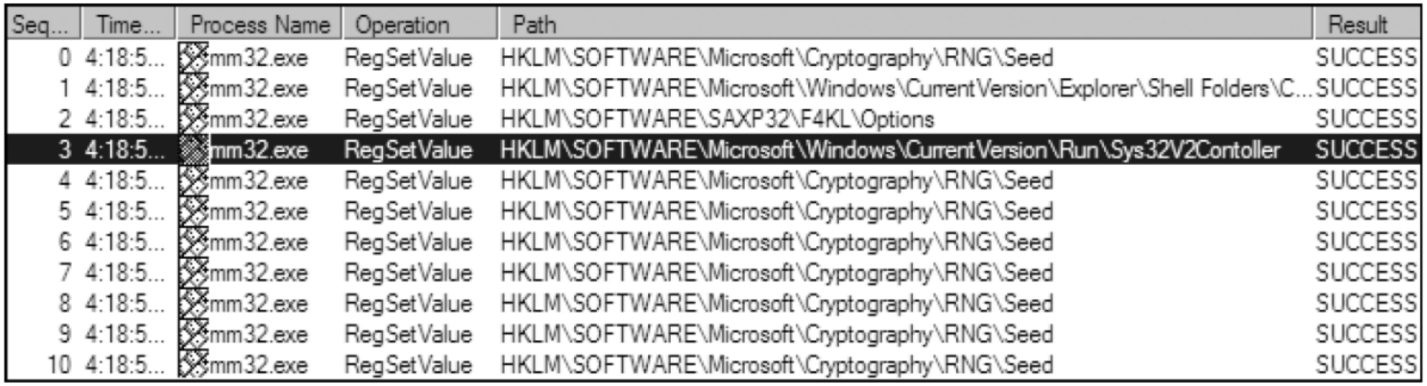
- You can set procmon to filter on one executable running on the system.
- This feature is particularly useful for malware analysis because you can set a filter on the piece of malware you are running.
- You can filter on individual system calls such as RegSetValue, CreateFile, WriteFile, or other suspicious or destructive calls.
- The most important filters for malware analysis are Process Name, Operation, and Detail



Display entries matching these conditions:

Operation | is | RegSetValue | then | Include

Column	Relation	Value	Action
Process Name	is	mm32.exe	Include
Operation	is	RegSetValue	Include
Process Name	is	Procmon.exe	Exclude
Process Name	is	System	Exclude
Operation	begins with	IRP_MJ_	Exclude
Operation	begins with	FASTIO_	Exclude
Path	ends with	pagefile.sys	Exclude
Path	ends with	$Mft	Exclude
Path	ends with	$MftMirr	Exclude
Path	ends with	$LogFile	Exclude
Path	ends with	$Volume	Exclude
Path	ends with	$AttrDef	Exclude
Path	ends with	$Root	Exclude



Seq...	Time...	Process Name	Operation	Path	Result
0	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
1	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\C...	SUCCESS
2	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\SAXP32\F4KL\Options	SUCCESS
3	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Sys32V2Contoller	SUCCESS
4	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
5	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
6	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
7	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
8	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
9	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS
10	4:18:5...	mm32.exe	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS

Figure 3-3: Setting a procmon filter

Automatic filters on its toolbar

- **Registry** By examining registry operations, you can tell how a piece of malware installs itself in the registry.
- **File system** Exploring file system interaction can show all files that the malware creates or configuration files it uses.
- **Process activity** Investigating process activity can tell whether the malware spawned additional processes.
- **Network** Identifying network connections can show you any ports on which the malware is listening.

Procmon – notes

- Analysis of procmon's recorded events takes practice and patience since many events are simply part of the standard way executables startup.

- The more you use procmon, the easier you will find it to review the event listing quickly.

Viewing Processes with Process Explorer

Viewing Processes with Process Explorer

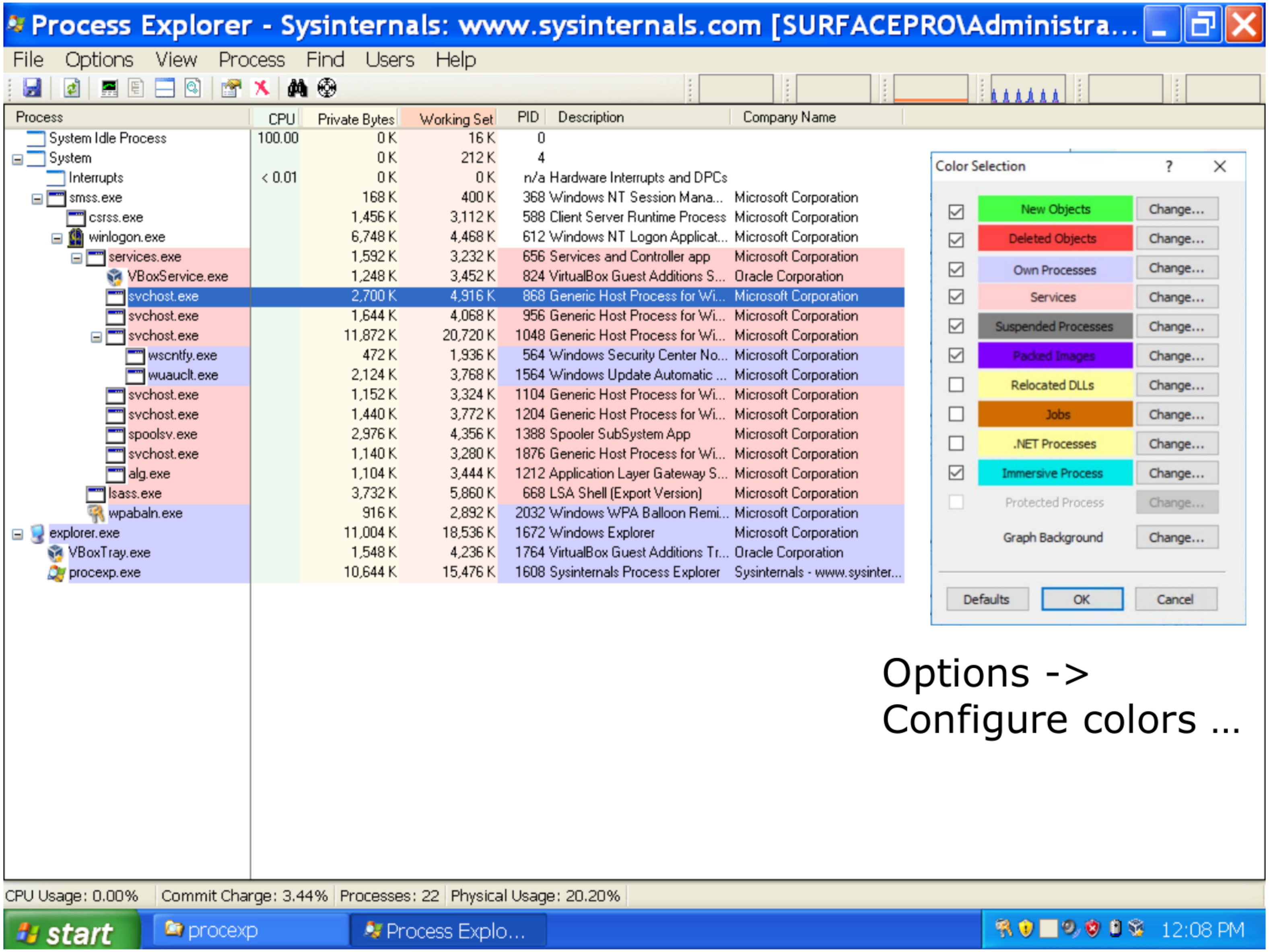
- The Process Explorer, free from Microsoft, is an extremely powerful task manager that should be running when you are performing dynamic analysis.

- It can provide valuable insight into the processes currently running on a system.

- You can use Process Explorer to list
  - active processes,
  - DLLs loaded by a process,
  - various process properties, and
  - overall system information.

- You can also use it to kill a process, log out users, and launch and validate processes.

Process Explorer Interface


Process Explorer - Sysinternals: www.sysinternals.com [SURFACEPRO\Administra...
File Options View Process Find Users Help
start
procexp
Process Explo...
12:08 PM

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	400 K	368	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,456 K	3,112 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,748 K	4,468 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,592 K	3,232 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,248 K	3,452 K	824	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,700 K	4,916 K	868	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,644 K	4,068 K	956	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		11,872 K	20,720 K	1048	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		472 K	1,936 K	564	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,124 K	3,768 K	1564	Windows Update Automatic ...	Microsoft Corporation
svchost.exe		1,152 K	3,324 K	1104	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,440 K	3,772 K	1204	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2,976 K	4,356 K	1388	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,140 K	3,280 K	1876	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,104 K	3,444 K	1212	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,732 K	5,860 K	668	LSA Shell (Export Version)	Microsoft Corporation
wpabaln.exe		916 K	2,892 K	2032	Windows WPA Balloon Remi...	Microsoft Corporation
explorer.exe		11,004 K	18,536 K	1672	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,548 K	4,236 K	1764	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		10,644 K	15,476 K	1608	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Color Selection

- ☑ New Objects — Change...
- ☑ Deleted Objects — Change...
- ☑ Own Processes — Change...
- ☑ Services — Change...
- ☑ Suspended Processes — Change...
- ☑ Packed Images — Change...
- □ Relocated DLLs — Change...
- □ Jobs — Change...
- □ .NET Processes — Change...
- ☑ Immersive Process — Change...
- □ Protected Process — Change...
- Graph Background — Change...

Defaults | OK | Cancel

CPU Usage: 0.00% | Commit Charge: 3.44% | Processes: 22 | Physical Usage: 20.20%

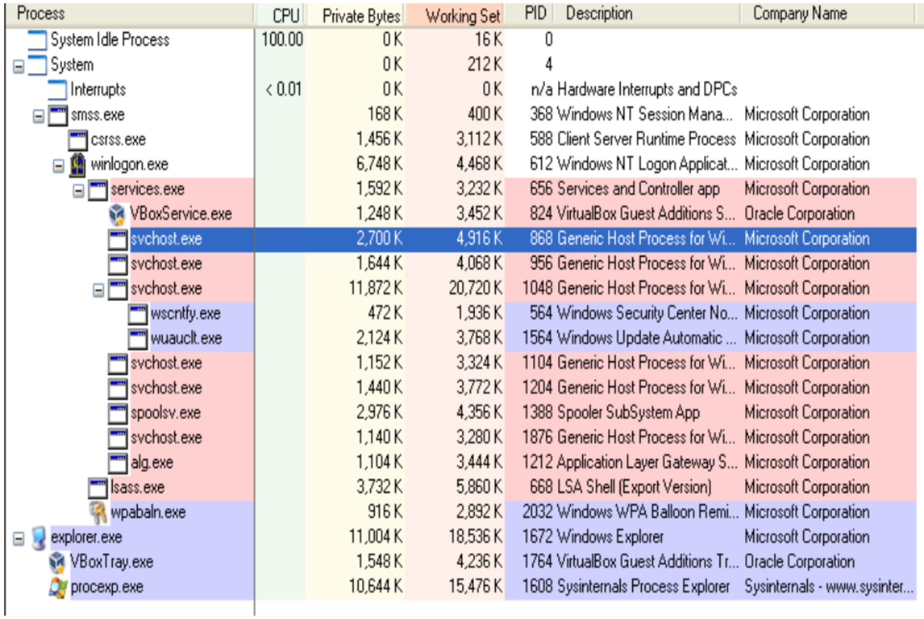
Options -> Configure colors …

Process Explorer Coloring

- Monitors the processes running on a system and shows them in a tree structure that displays child and parent relationships.
  - Services are highlighted in **pink**,
  - Processes in **blue**,
  - New processes in **green.**
  - Terminated processes in **red**.

Process Explorer (PExp) Coloring

- PExp view five main columns:
  - Process (the process name).
  - PID (the process identifier).
  - CPU (CPU usage).
  - Description.
  - Company Name.

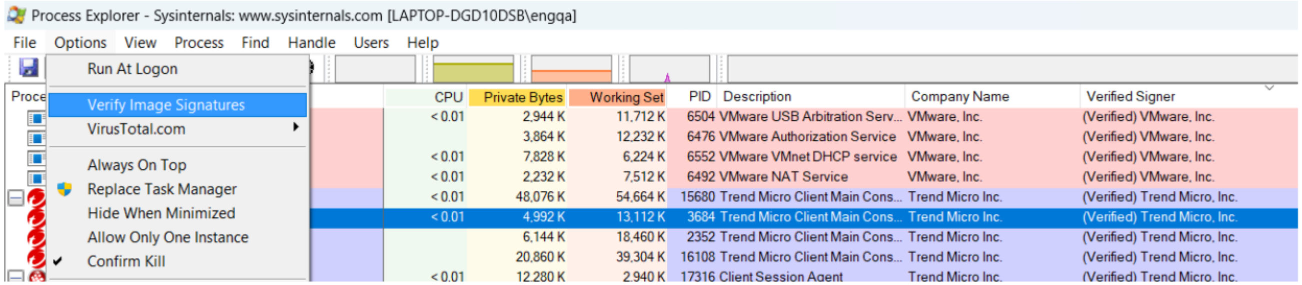


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	400 K	368	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,456 K	3,112 K	588	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,748 K	4,468 K	612	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,592 K	3,232 K	656	Services and Controller app	Microsoft Corporation
VBoxService.exe		1,248 K	3,452 K	824	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		2,700 K	4,916 K	868	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,644 K	4,068 K	956	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		11,872 K	20,720 K	1048	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		472 K	1,936 K	564	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,124 K	3,768 K	1564	Windows Update Automatic ...	Microsoft Corporation
svchost.exe		1,152 K	3,324 K	1104	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,440 K	3,772 K	1204	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2,976 K	4,356 K	1388	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,140 K	3,280 K	1876	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,104 K	3,444 K	1212	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,732 K	5,860 K	668	LSA Shell (Export Version)	Microsoft Corporation
wpabaln.exe		916 K	2,892 K	2032	Windows WPA Balloon Remi...	Microsoft Corporation
explorer.exe		11,004 K	18,536 K	1672	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,548 K	4,236 K	1764	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		10,644 K	15,476 K	1608	Sysinternals Process Explorer	Sysinternals - www.sysinter...

- When analyzing malware, watch the Process Explorer window for changes or new processes, and be sure to investigate them thoroughly.

Using the Verify Option on the Image tab

- This verifies that the image on disk is Microsoft signed.
  - Microsoft digitally signs most of its core executables.
  - PExp verifies that a signature is valid, and you can be sure that the file is executable from Microsoft.
  - This is useful to verify that the Windows file on disk has not been corrupted;
  - Since Malware often replaces authentic Windows files with its own in an attempt to hide.



Proce	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
	< 0.01	2,944 K	11,712 K	6504	VMware USB Arbitration Serv...	VMware, Inc.	(Verified) VMware, Inc.
		3,864 K	12,232 K	6476	VMware Authorization Service	VMware, Inc.	(Verified) VMware, Inc.
	< 0.01	7,828 K	6,224 K	6552	VMware VMnet DHCP service	VMware, Inc.	(Verified) VMware, Inc.
	< 0.01	2,232 K	7,512 K	6492	VMware NAT Service	VMware, Inc.	(Verified) VMware, Inc.
	< 0.01	48,076 K	54,664 K	15680	Trend Micro Client Main Cons...	Trend Micro Inc.	(Verified) Trend Micro, Inc.
	< 0.01	4,992 K	13,112 K	3684	Trend Micro Client Main Cons...	Trend Micro Inc.	(Verified) Trend Micro, Inc.
		6,144 K	18,460 K	2352	Trend Micro Client Main Cons...	Trend Micro Inc.	(Verified) Trend Micro, Inc.
		20,860 K	39,304 K	16108	Trend Micro Client Main Cons...	Trend Micro Inc.	(Verified) Trend Micro, Inc.
	< 0.01	12,280 K	2,940 K	17316	Client Session Agent	Trend Micro Inc.	(Verified) Trend Micro, Inc.

Using the Verify Option on the Image tab

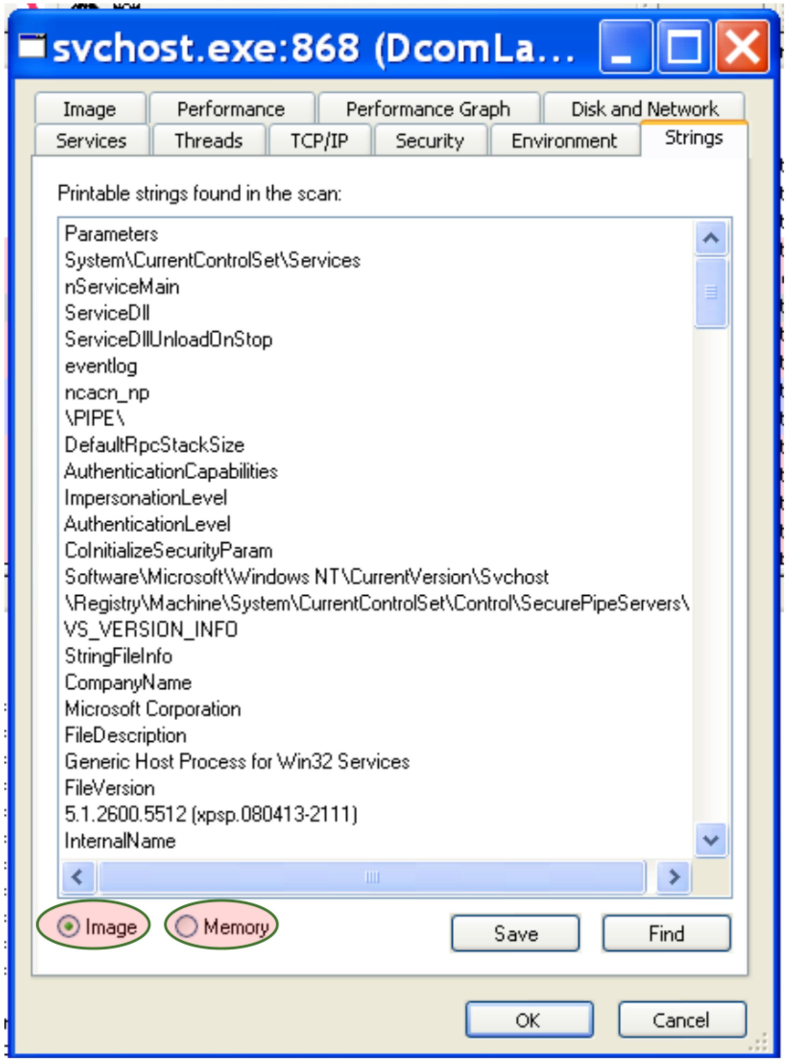
- This verifies the image on disk rather than in memory

- It is useless if an attacker uses *process replacement*,
  - Running a process on the system and overwriting its memory space with a malicious executable.
  - This provides malware with the same privileges as the process it is replacing (to appear as a legitimate process).
  - But it leaves a fingerprint: **The image in memory will differ from the image on disk**.

Comparing Strings within Process Explorer

- One way to recognize process replacement is to use the Strings tab in the Process Properties window to compare the strings contained in the disk executable (image) against the strings in memory for that same executable running in memory.

- If the two string listings are drastically different, process replacement may have occurred



Printable strings found in the scan:

```
Parameters
System\CurrentControlSet\Services
nServiceMain
ServiceDll
ServiceDllUnloadOnStop
eventlog
ncacn_np
\PIPE\
DefaultRpcStackSize
AuthenticationCapabilities
ImpersonationLevel
AuthenticationLevel
CoInitializeSecurityParam
Software\Microsoft\Windows NT\CurrentVersion\Svchost
\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\
VS_VERSION_INFO
StringFileInfo
CompanyName
Microsoft Corporation
FileDescription
Generic Host Process for Win32 Services
FileVersion
5.1.2600.5512 (xpsp.080413-2111)
InternalName
```

● Image ○ Memory

Using "Find DLL" within Process Explorer

- It also lets you search for a handle or DLL by choosing **Find | Find Handle or DLL**
- The Find DLL option is particularly useful when you find a malicious DLL on disk and want to know if any running processes use that DLL.
- To determine whether a DLL is loaded into a process after load time, you can compare the DLL list in Process Explorer to the imports shown in Dependency Walker.

Analyzing Malicious Documents within Process Explorer

- You can also use Process Explorer to analyze malicious documents, such as PDFs and Word documents.

- A quick way to determine whether a document is malicious is to open Process Explorer and open the suspected malicious document.

- If the document launches any processes, you should see them in Process Explorer and be able to locate the malware on disk via the Image tab of the Properties window.

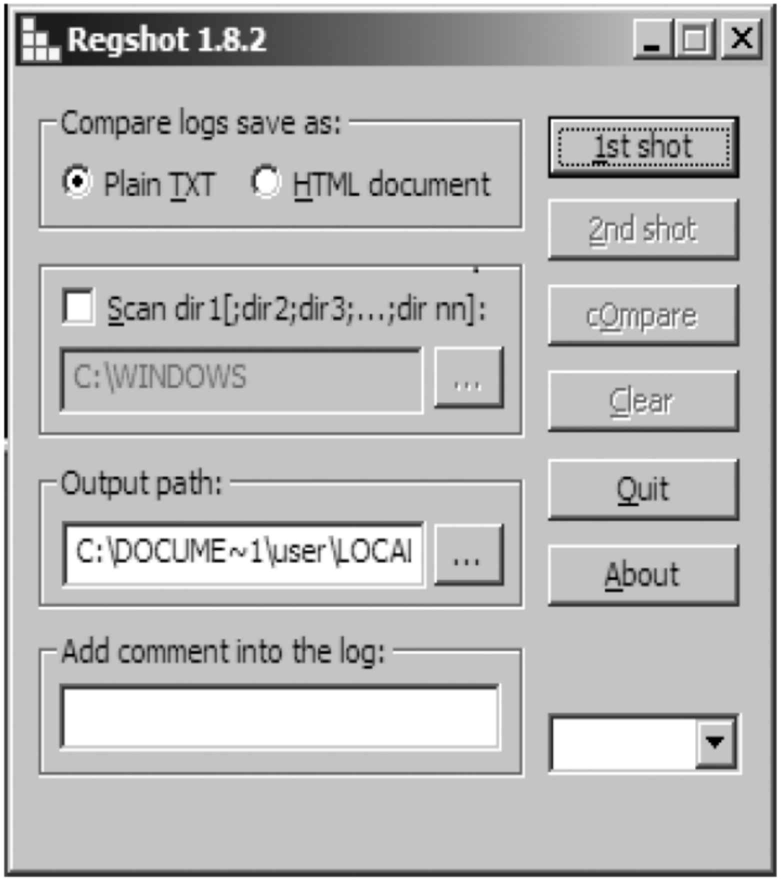
Comparing Registry Snapshots with Regshot

Comparing Registry Snapshots with Regshot

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

- To use Regshot for malware analysis, simply take the first shot by clicking the **1st Shot** button, and then run the malware and wait for it to finish making any system changes. Next, take the second shot by clicking the **2nd Shot** button. Finally, click the **Compare** button to compare the two snapshots.

- As with procmon, your analysis of these results requires patient scanning to find nuggets of interest



Compare logs save as: ● Plain TXT ○ HTML document

☐ Scan dir1[;dir2;dir3;...;dir nn]: C:\WINDOWS

Output path: C:\DOCUME~1\user\LOCAl

Add comment into the log:

Figure 3-8: Regshot window

Faking a Network

Faking a Network

- Malware often beacons out and eventually communicates with a command-and-control server

- You can create a fake network and quickly obtain network indicators without actually connecting to the Internet.

- These indicators can include
  - DNS names,
  - IP addresses, and
  - packet signatures.

- To fake a network successfully, you must prevent the malware from realizing that it is executing in a virtualized environment

Using ApateDNS

- ApateDNS, a free tool from Mandiant (*www.mandiant.com/products/research/mandiant_apatedns/download*), is the quickest way to see DNS requests made by malware.
  - Needs .Net Framework 4.0/3.5?

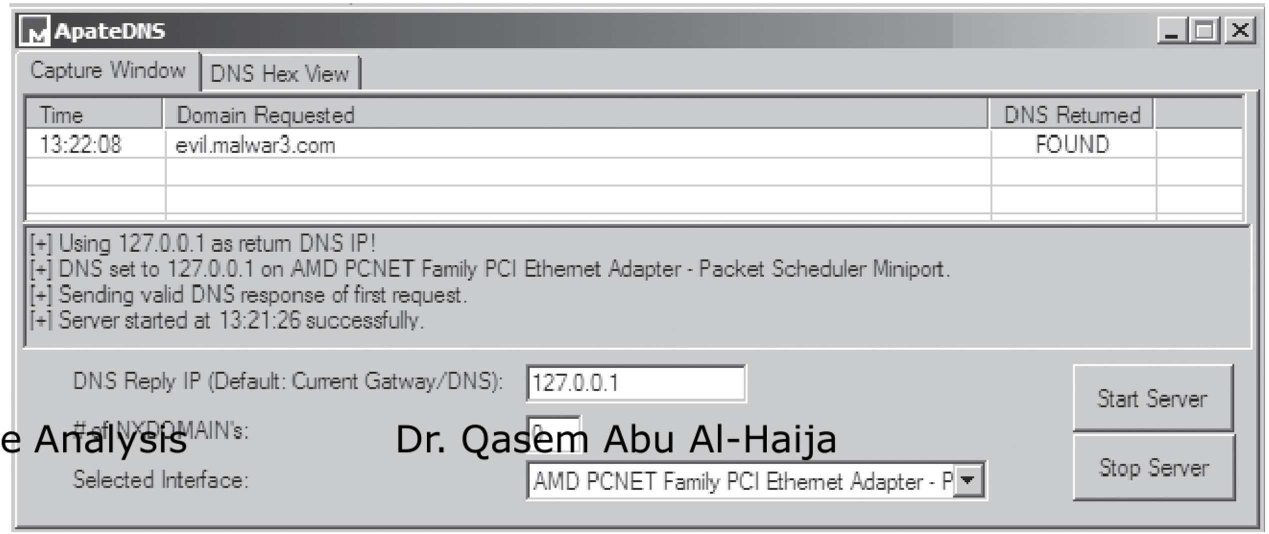
- ApateDNS spoofs DNS responses to a user-specified IP address by listening on UDP port 53 on the local machine.

- It responds to DNS requests with the DNS response set to an IP address you specify.

- ApateDNS can display the hexadecimal and ASCII results of all requests it receives.

ApateDNS Capturing Malware DNS Requests

- Set the IP address you want sent in DNS responses and select the interface.
- Press the **Start Server** button
- This will automatically start the DNS server and change the DNS settings to localhost.
- Run your malware and watch as DNS requests appear in the ApateDNS window.
- You can catch additional domains used by a malware sample through the use of the nonexistent domain (NXDOMAIN) option.
  - Malware will often loop through the different domains it has stored if the first or second domains are not found.
  - Using this NXDOMAIN option can trick malware into giving you additional domains it has in its configuration.



Time	Domain Requested	DNS Returned
13:22:08	evil.malwar3.com	FOUND

```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 13:21:26 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS): 127.0.0.1

# of NXDOMAIN's: 0

Selected Interface: AMD PCNET Family PCI Ethernet Adapter - P

Monitoring with Netcat

- Netcat, the “TCP/IP Swiss Army knife,” can be used over both inbound and outbound connections for port scanning, tunneling, proxying, port forwarding, and much more.
- In listen mode, Netcat acts as a server, while in connect mode it acts as a client.
- Netcat takes data from standard input for transmission over the network.
- All the data it receives is output to the screen via standard output.

NetCat Capturing Malware Packets

- Using ApateDNS, we redirect the DNS request for *evil.malwar3.com* to our local host.

- Assuming that the malware is going out over port 80 (a common choice), we can use Netcat to listen for connections before executing the malware.

- Malware frequently uses port 80 or 443 (HTTP or HTTPS traffic, respectively), because these ports are typically not blocked or monitored as outbound connections.

- The malware connects to our Netcat listener because we're using ApateDNS for redirection.

Packet Sniffing with Wireshark

- Wireshark is an *open-source sniffer*, a packet capture tool that intercepts and logs network traffic.

- Wireshark provides visualization, packet-stream analysis, and in-depth analysis of individual packets.

Using INetSim

- INetSim is a free, Linux-based software suite for simulating common Internet services.

- The easiest way to run INetSim if your base operating system is Microsoft Windows is to install it on a Linux virtual machine and set it up on the same virtual network as your malware analysis virtual machine.

- INetSim is the best free tool for providing fake services, allowing you to analyze the network behavior of unknown malware samples by emulating services such as HTTP, HTTPS, FTP, IRC, DNS, SMTP, and others.

- INetSim does its best to look like a real server
  - INetSim can serve almost any file requested in the case of http, https

- INetSim can also record all inbound requests and connections

Notes: Install inetsim over Ubuntu Desktop 16.04

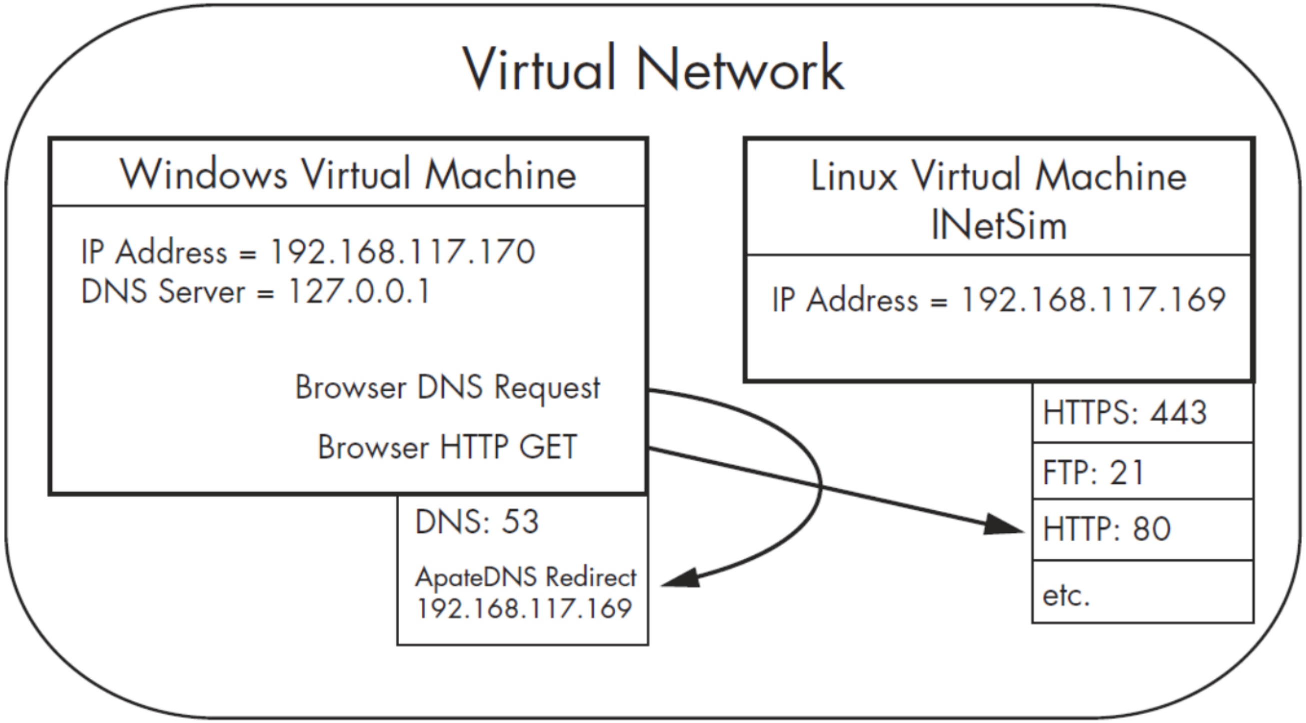
- Install VirtualBox guest additions
- Refer to INetSim installation using apt

- sudo touch /etc/apt/sources.list.d/inetsim.list
- sudo chmod 755 /etc/apt/sources.list.d/inetsim.list
- echo "deb http://www.inetsim.org/debian/ binary/" > /etc/apt/sources.list.d/inetsim.list
- wget -O - http://www.inetsim.org/inetsim-archive-signing-key.asc | sudo apt-key add -
- sudo find / -name inetsim

- Refer INetSim
- Log files are stored in the /var/log/inetsim/ directory:
  - debug.log: debug information in case inetsim is run in debug mode
  - main.log: information logs (services started, stopped, ...)
  - service.log: when connections are made against the services, logs are added to this file

Example Malware Analysis Setup

- This virtual network contains two hosts: the malware analysis Windows virtual machine and the Linux virtual machine running INetSim.
- The Linux virtual machine is listening on many ports.
- The Windows virtual machine is listening on port 53 for DNS requests through ApateDNS.
- The DNS server for the Windows virtual machine has been configured to localhost (127.0.0.1).
- ApateDNS is configured to redirect you to the Linux virtual machine (192.168.117.169).



Main Sources for these slides

- *Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"; ISBN-10: 1593272901.*
- *Xinwen Fu, “Introduction to Malware Analysis,” University of Central Florida*
- *Sam Bowne, “Practical Malware Analysis,” City College San Francisco*
- *Abhijit Mohanta and Anoop Saldanha, “Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware,” ISBN: 1484261925.*

Thank you