Introduction to Dynamic Malware Analysis

David Shaw
dshaw@dshaw.net

Who am I?

- David Shaw
- Senior Director of Engineering at Redspin
- Application and Network Security
- Technical Editor: *Nmap 6: Network Exploration and Security Auditing Cookbook*
- @dshaw_

What you’ll learn

- How to setup an Analysis Lab
- Detection of Malicious Processes
- System-level Change Detection
- Malicious Traffic Analysis

What you’ll learn

- How to setup an Analysis Lab
- Detection of Malicious Processes
- System-level Change Detection
- Malicious Traffic Analysis
- Bonus! Dealing with Dead C&Cs

What you won’t

- Static Code Analysis
- Crackmes
  - (But you should check those out anyway)
- How to be a wizard with IDA Pro, OllyDbg, etc.
- Any assembly whatsoever

Mal-what? Why do I care?

- Computers are faster; malware can do more

- System and security admins must maintain data and network integrity

- Anti-virus is a game of cat-and-mouse

- Malware analysis is fun!

Getting Started

- Virtualization software (VirtualBox)
- Windows ISO or disc
- Analysis toolchain
- Malware samples (malware.lu, VirusShare, any shady web site...)

Meet the Tools

- Sysinternals: best thing ever

- Process Explorer
  - Task Manager improved

- Process Monitor
  - System-level change monitoring

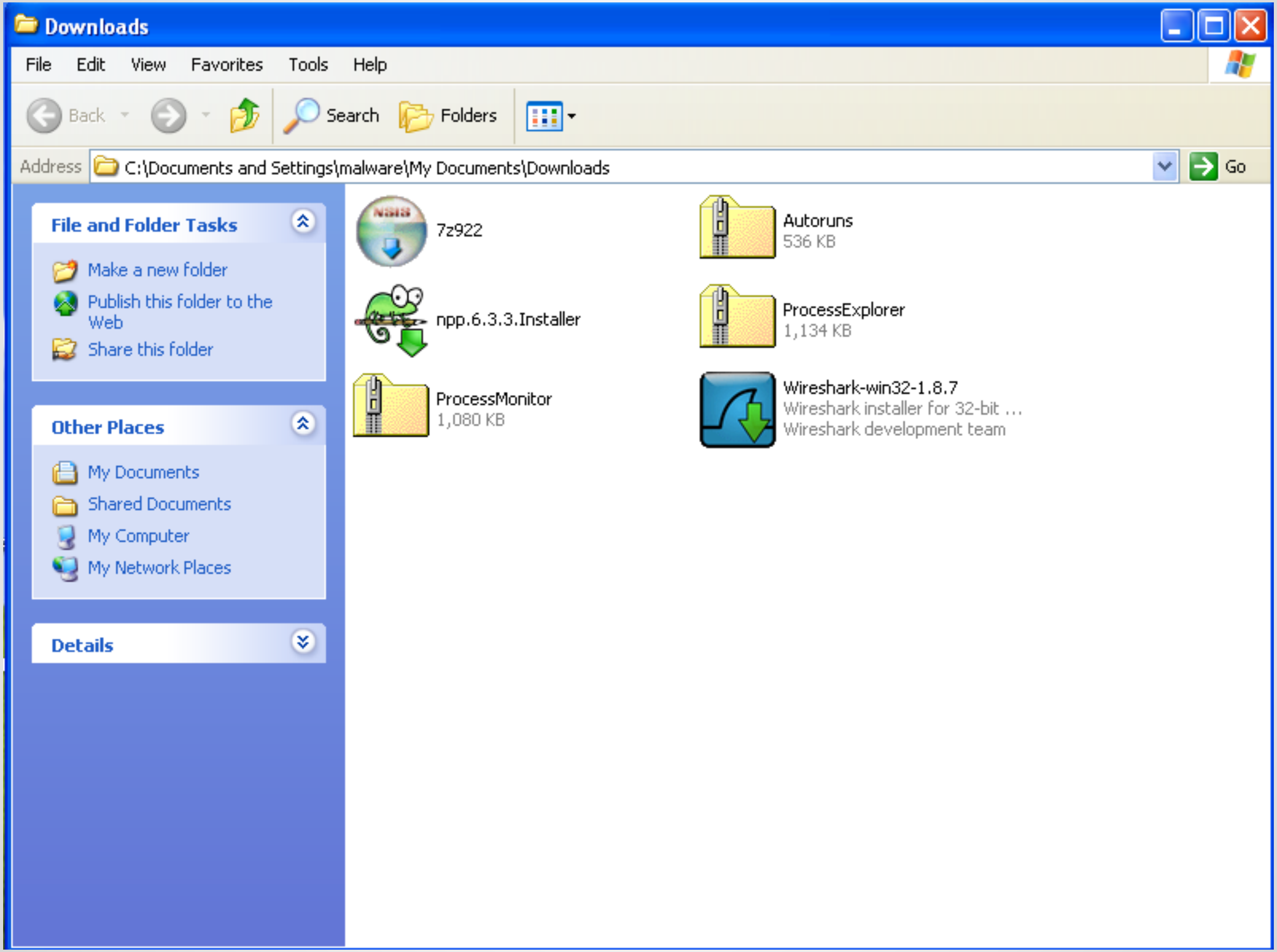
- Autoruns
  - Basic malware persistence analysis

- Wireshark

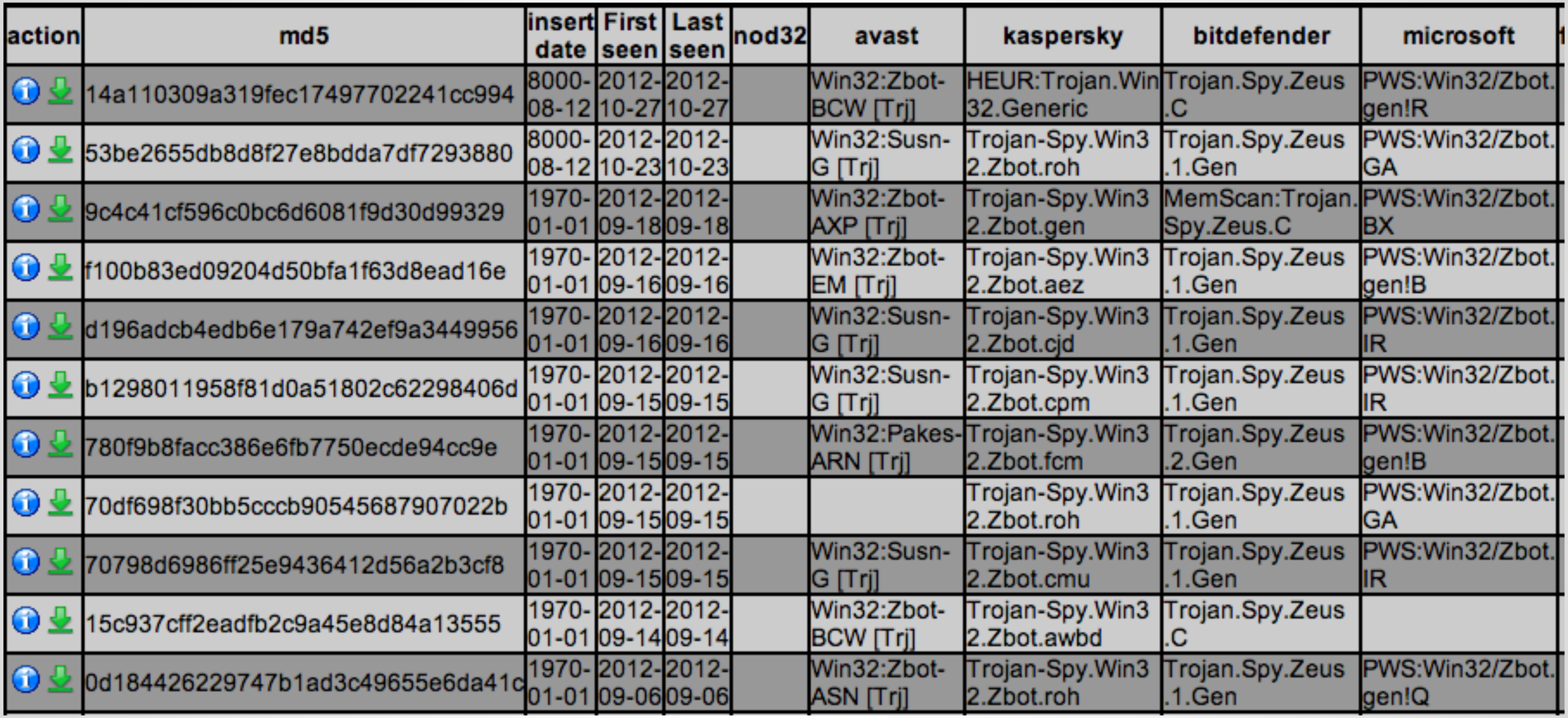
Before we start

- Create a new analysis VM
- Install the toolchain
- Take a snapshot
- Install malware
- Take a snapshot (INFECTED)

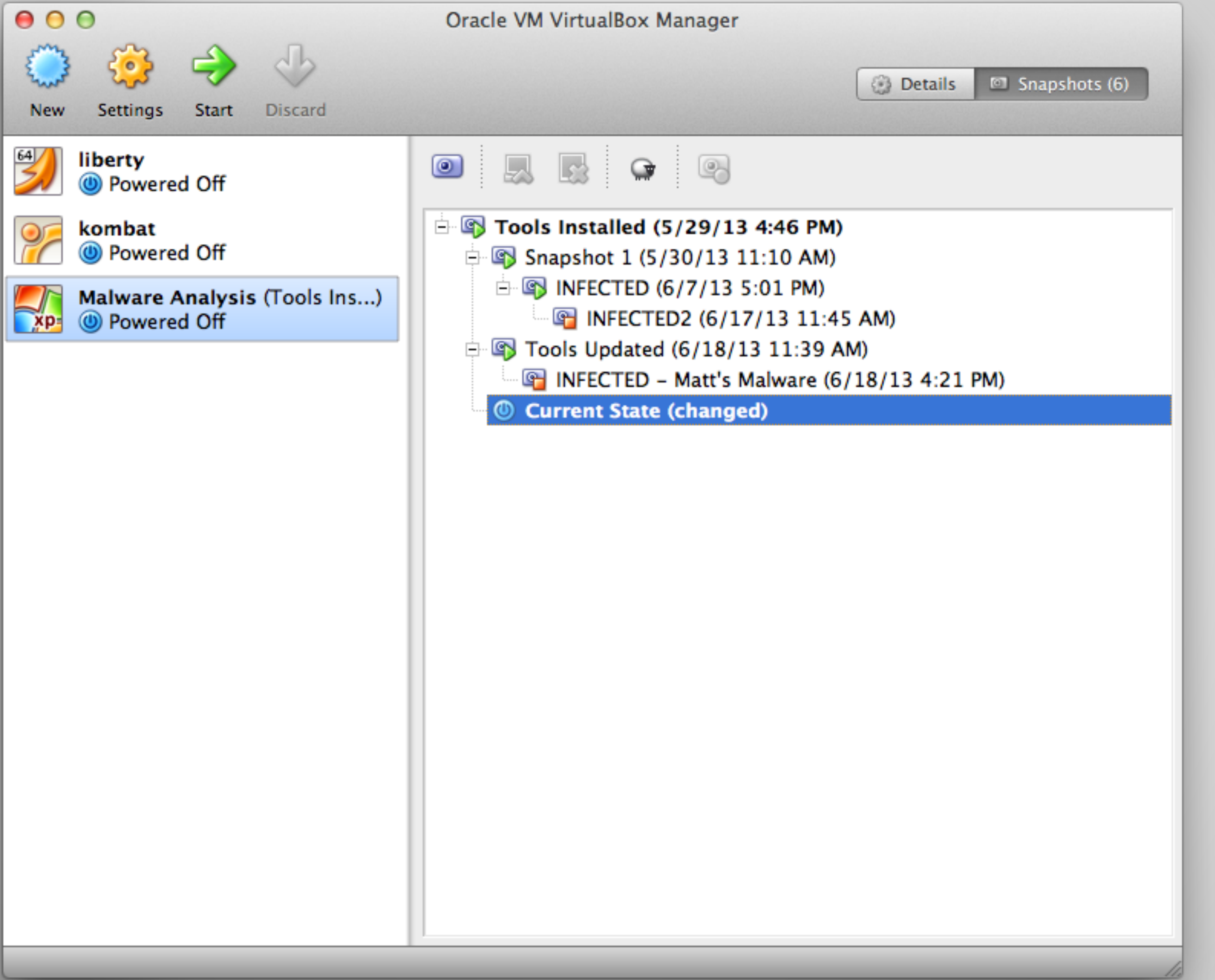
Install the toolchain



Install the malware



action	md5	insert date	First seen	Last seen	nod32	avast	kaspersky	bitdefender	microsoft
ⓘ ⬇	14a110309a319fec17497702241cc994	8000-08-12	2012-10-27	2012-10-27		Win32:Zbot-BCW [Trj]	HEUR:Trojan.Win32.Generic	Trojan.Spy.Zeus.C	PWS:Win32/Zbot.gen!R
ⓘ ⬇	53be2655db8d8f27e8bdda7df7293880	8000-08-12	2012-10-23	2012-10-23		Win32:Susn-G [Trj]	Trojan-Spy.Win32.Zbot.roh	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.GA
ⓘ ⬇	9c4c41cf596c0bc6d6081f9d30d99329	1970-01-01	2012-09-18	2012-09-18		Win32:Zbot-AXP [Trj]	Trojan-Spy.Win32.Zbot.gen	MemScan:Trojan.Spy.Zeus.C	PWS:Win32/Zbot.BX
ⓘ ⬇	f100b83ed09204d50bfa1f63d8ead16e	1970-01-01	2012-09-16	2012-09-16		Win32:Zbot-EM [Trj]	Trojan-Spy.Win32.Zbot.aez	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.gen!B
ⓘ ⬇	d196adcb4edb6e179a742ef9a3449956	1970-01-01	2012-09-16	2012-09-16		Win32:Susn-G [Trj]	Trojan-Spy.Win32.Zbot.cjd	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.IR
ⓘ ⬇	b1298011958f81d0a51802c62298406d	1970-01-01	2012-09-15	2012-09-15		Win32:Susn-G [Trj]	Trojan-Spy.Win32.Zbot.cpm	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.IR
ⓘ ⬇	780f9b8facc386e6fb7750ecde94cc9e	1970-01-01	2012-09-15	2012-09-15		Win32:Pakes-ARN [Trj]	Trojan-Spy.Win32.Zbot.fcm	Trojan.Spy.Zeus.2.Gen	PWS:Win32/Zbot.gen!B
ⓘ ⬇	70df698f30bb5cccb90545687907022b	1970-01-01	2012-09-15	2012-09-15			Trojan-Spy.Win32.Zbot.roh	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.GA
ⓘ ⬇	70798d6986ff25e9436412d56a2b3cf8	1970-01-01	2012-09-15	2012-09-15		Win32:Susn-G [Trj]	Trojan-Spy.Win32.Zbot.cmu	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.IR
ⓘ ⬇	15c937cff2eadfb2c9a45e8d84a13555	1970-01-01	2012-09-14	2012-09-14		Win32:Zbot-BCW [Trj]	Trojan-Spy.Win32.Zbot.awbd	Trojan.Spy.Zeus.C	
ⓘ ⬇	0d18442622974 7b1ad3c49655e6da41c	1970-01-01	2012-09-06	2012-09-06		Win32:Zbot-ASN [Trj]	Trojan-Spy.Win32.Zbot.roh	Trojan.Spy.Zeus.1.Gen	PWS:Win32/Zbot.gen!Q



liberty
Powered Off

kombat
Powered Off

Malware Analysis (Tools Ins...)
Powered Off

- Tools Installed (5/29/13 4:46 PM)
  - Snapshot 1 (5/30/13 11:10 AM)
    - INFECTED (6/7/13 5:01 PM)
      - INFECTED2 (6/17/13 11:45 AM)
  - Tools Updated (6/18/13 11:39 AM)
    - INFECTED – Matt's Malware (6/18/13 4:21 PM)
  - Current State (changed)

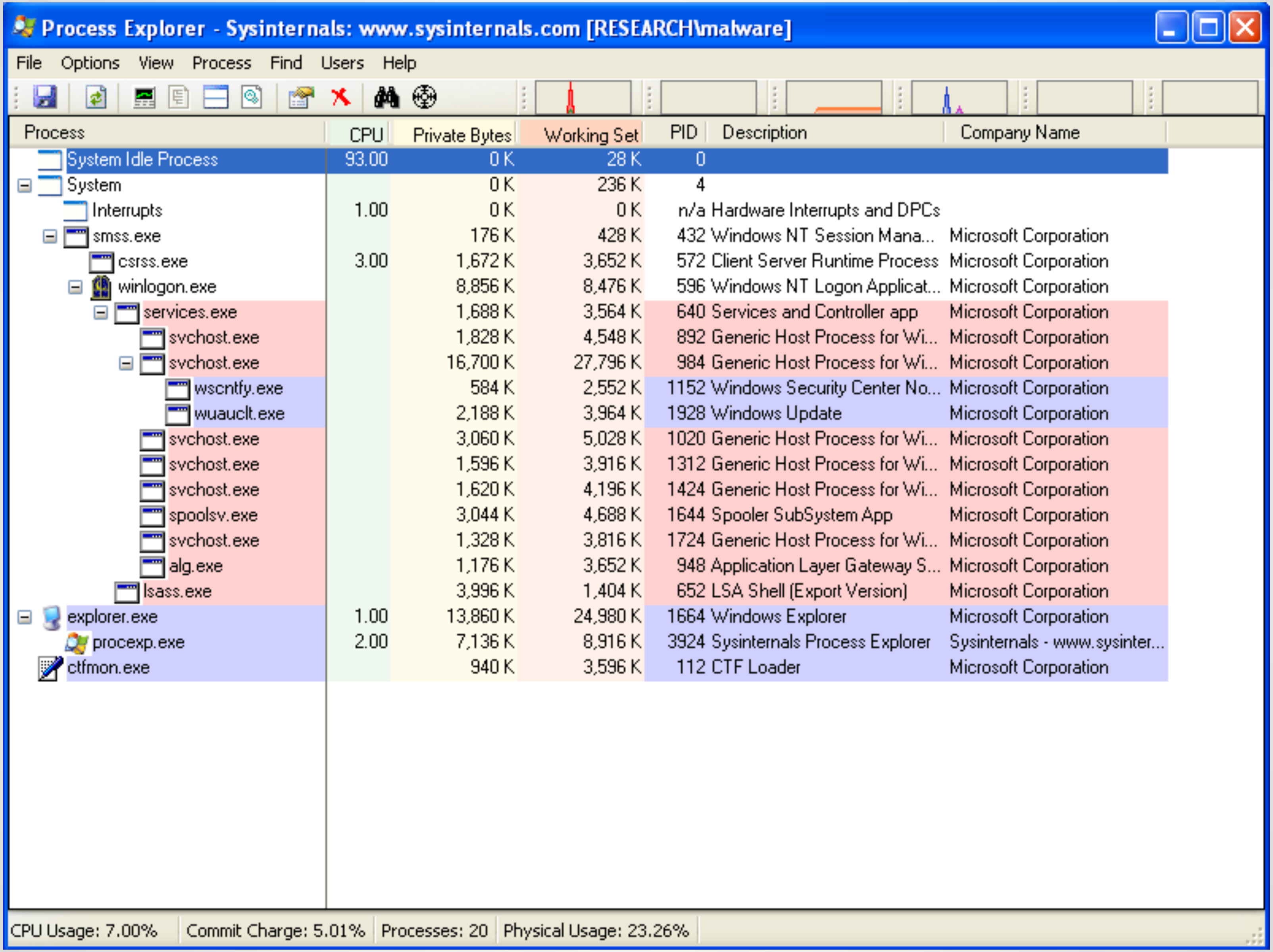
Part I
What’s Running?

Running Processes

- Process Explorer shows great information

- Task Manager, but way better

- Lets us look for suspicious processes
  - Also: a nice way to get to know your system



Process Explorer - Sysinternals: www.sysinternals.com [RESEARCH\malware]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	93.00	0 K	28 K	0		
System		0 K	236 K	4		
Interrupts	1.00	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		176 K	428 K	432	Windows NT Session Mana...	Microsoft Corporation
csrss.exe	3.00	1,672 K	3,652 K	572	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		8,856 K	8,476 K	596	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,688 K	3,564 K	640	Services and Controller app	Microsoft Corporation
svchost.exe		1,828 K	4,548 K	892	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		16,700 K	27,796 K	984	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		584 K	2,552 K	1152	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		2,188 K	3,964 K	1928	Windows Update	Microsoft Corporation
svchost.exe		3,060 K	5,028 K	1020	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,596 K	3,916 K	1312	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,620 K	4,196 K	1424	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,044 K	4,688 K	1644	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,328 K	3,816 K	1724	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,176 K	3,652 K	948	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,996 K	1,404 K	652	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1.00	13,860 K	24,980 K	1664	Windows Explorer	Microsoft Corporation
procexp.exe	2.00	7,136 K	8,916 K	3924	Sysinternals Process Explorer	Sysinternals - www.sysinter...
ctfmon.exe		940 K	3,596 K	112	CTF Loader	Microsoft Corporation

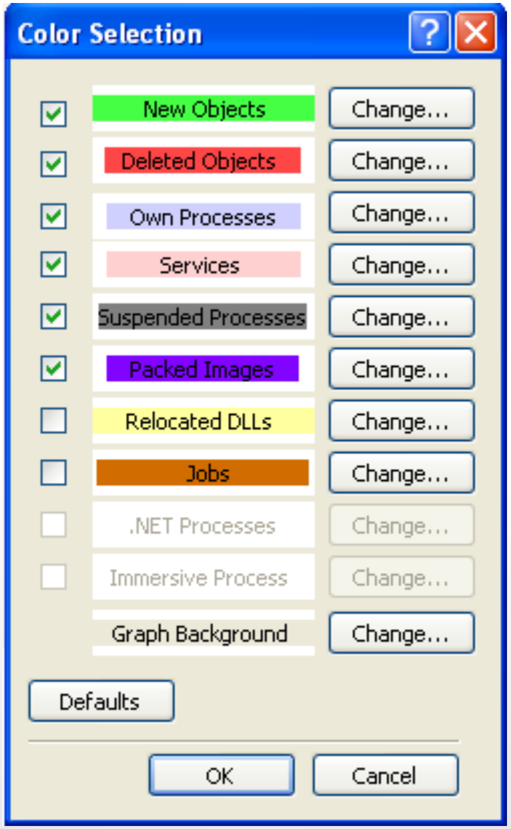
CPU Usage: 7.00% Commit Charge: 5.01% Processes: 20 Physical Usage: 23.26%

So many colors!

- Process Explorer is color coded!
  - Green: New Object
  - Red: Killed Object
  - Salmon: Service Process
  - Blue: Own (user) process
  - Deep Purple: Packed Image

So many colors!

- Easily configurable via Options -> Color Selector



Color Selection

☑ New Objects

☑ Deleted Objects

☑ Own Processes

☑ Services

☑ Suspended Processes

☑ Packed Images

☐ Relocated DLLs

☐ Jobs

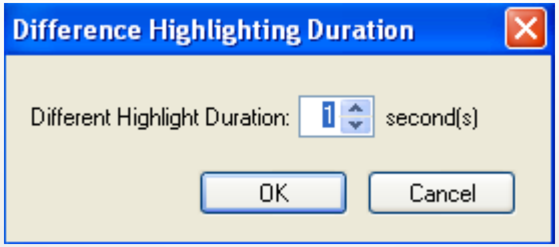
☐ .NET Processes

☐ Immersive Process

Graph Background

What was that blip?

- By default, Process Explorer shows new/killed processes for only a second
- Not really enough time for in-depth analysis
- Can be handily changed via Options -> Difference Highlighting Duration

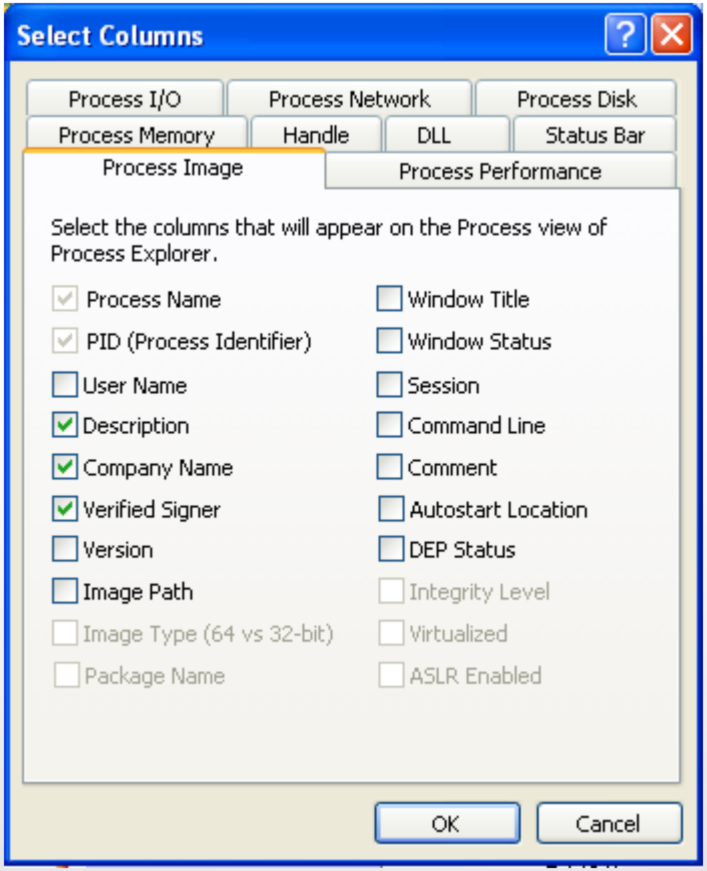


Difference Highlighting Duration

Different Highlight Duration: 1 second(s)

Customized Column Reporting

- Display particularly relevant information immediately



Select Columns

Select the columns that will appear on the Process view of Process Explorer.

☑ Process Name
☑ PID (Process Identifier)
☐ User Name
☑ Description
☑ Company Name
☑ Verified Signer
☐ Version
☐ Image Path
☐ Image Type (64 vs 32-bit)
☐ Package Name
☐ Window Title
☐ Window Status
☐ Session
☐ Command Line
☐ Comment
☐ Autostart Location
☐ DEP Status
☐ Integrity Level
☐ Virtualized
☐ ASLR Enabled

Process Identification

- Are there red flags?
  - Unsigned or unverified processes (fake svchost.exe, etc.)
  - Packed processes (generally not a good sign)
- When does the process run?
  - Right after you run the potential malware?

A Deeper Look

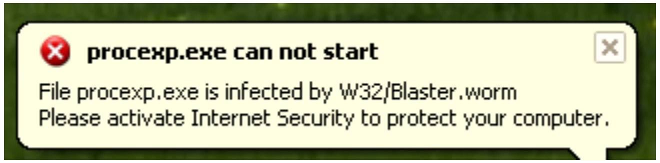
- Is the process persistent?
  - If not, what is it doing? File or network I/O?
- Is this from a trusted source?
- Are there hardcoded strings?

Potential Pitfalls

- Some malware tries to stop our analysis:

Potential Pitfalls

- Some malware tries to stop our analysis:

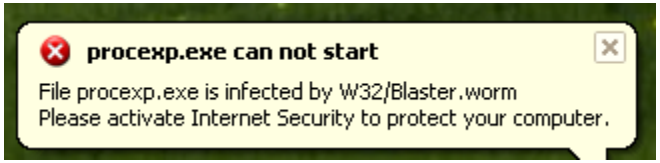


procexp.exe can not start

File procexp.exe is infected by W32/Blaster.worm
Please activate Internet Security to protect your computer.

Potential Pitfalls

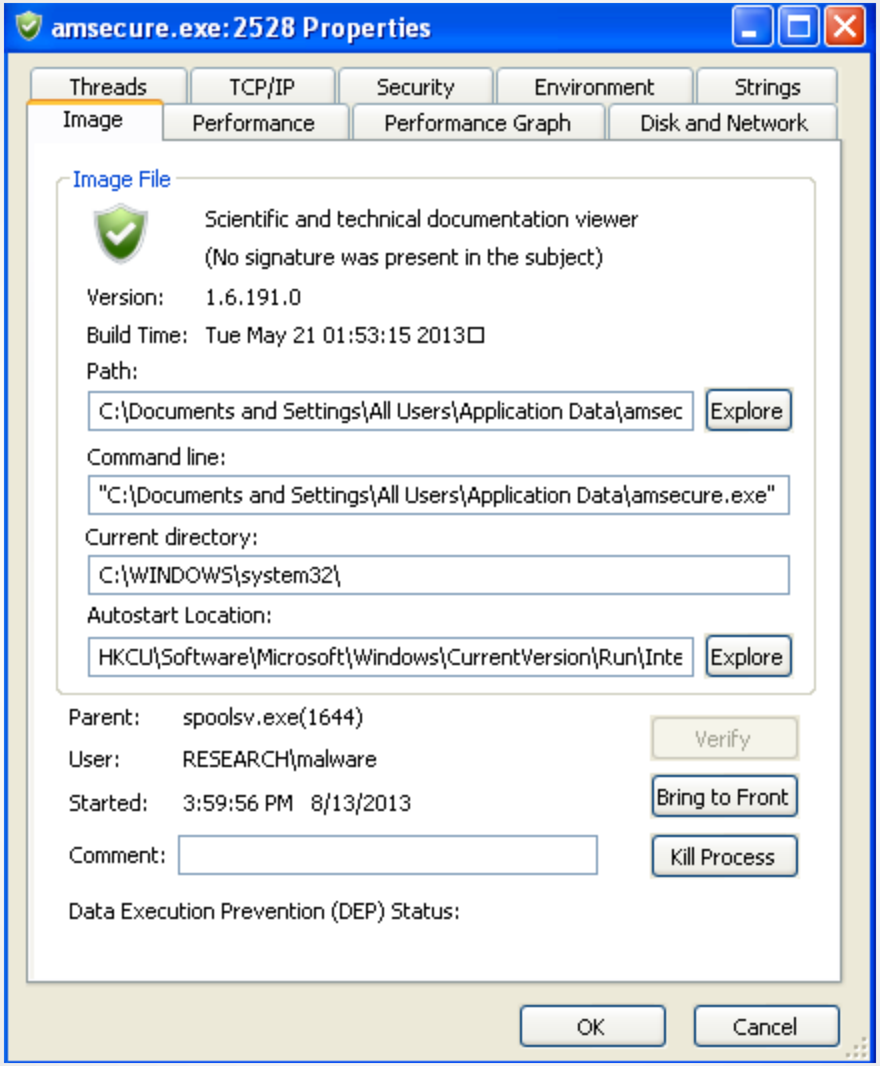
- Some malware tries to stop our analysis:



procexp.exe can not start

File procexp.exe is infected by W32/Blaster.worm
Please activate Internet Security to protect your computer.

- Fortunately, we can simply run as a privileged user
    - Unless the malware beats us to it
- Consequence: “own process” changes



amsecure.exe:2528 Properties

Image File

Scientific and technical documentation viewer
(No signature was present in the subject)

Version: 1.6.191.0

Build Time: Tue May 21 01:53:15 2013□

Path:

C:\Documents and Settings\All Users\Application Data\amsec

Command line:

"C:\Documents and Settings\All Users\Application Data\amsecure.exe"

Current directory:

C:\WINDOWS\system32\

Autostart Location:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Inte

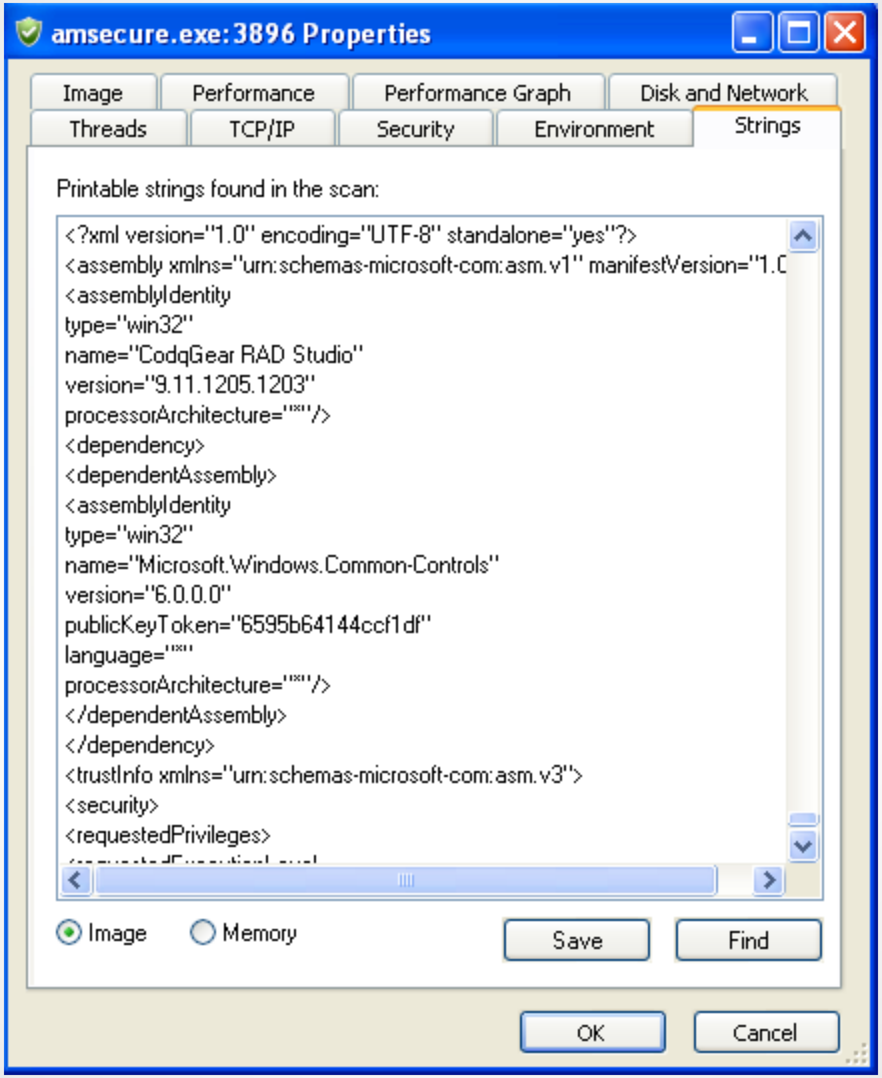
Parent: spoolsv.exe(1644)

User: RESEARCH\malware

Started: 3:59:56 PM 8/13/2013

Comment:

Data Execution Prevention (DEP) Status:



Printable strings found in the scan:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0
<assemblyIdentity
type="win32"
name="CodqGear RAD Studio"
version="9.11.1205.1203"
processorArchitecture="*"/>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
publicKeyToken="6595b64144ccf1df"
language="*"
processorArchitecture="*"/>
</dependentAssembly>
</dependency>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
<requestedPrivileges>
```

● Image ○ Memory

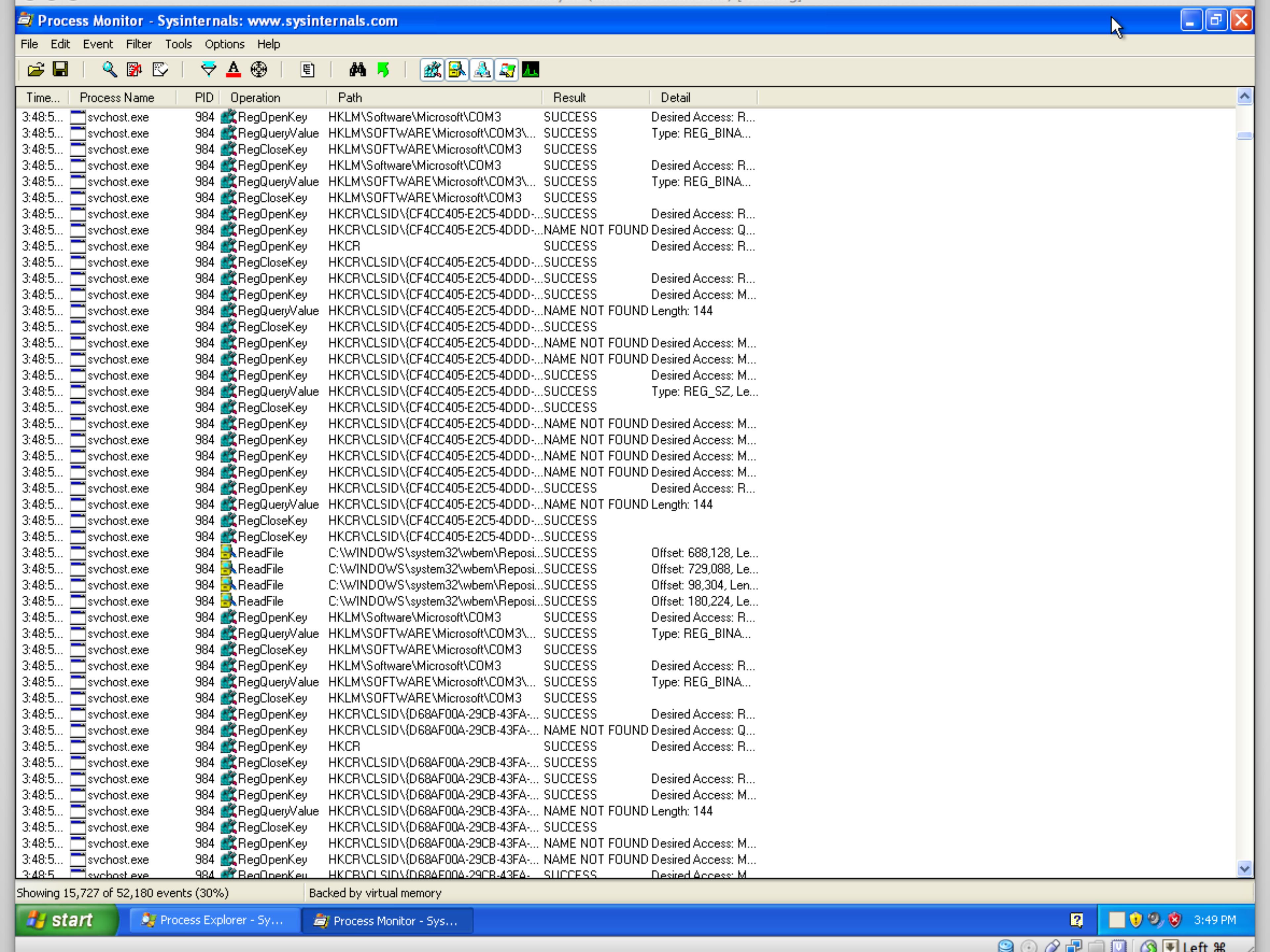
Strings Analysis

- Command and Control servers (C&Cs) must be hardcoded somehow
- Sometimes (due to laziness), we get lucky
- `grep -iE '\d+\.\d+\.\d+\.\d+|https?:'`
- But what is the malware *doing?*

Part II
What’s it Doing?

System-level changes

- Process Monitor hooks into the Windows Event Tracing functionality
- All file system changes are logged to a constantly scrolling window
- Produce a huge amount of data



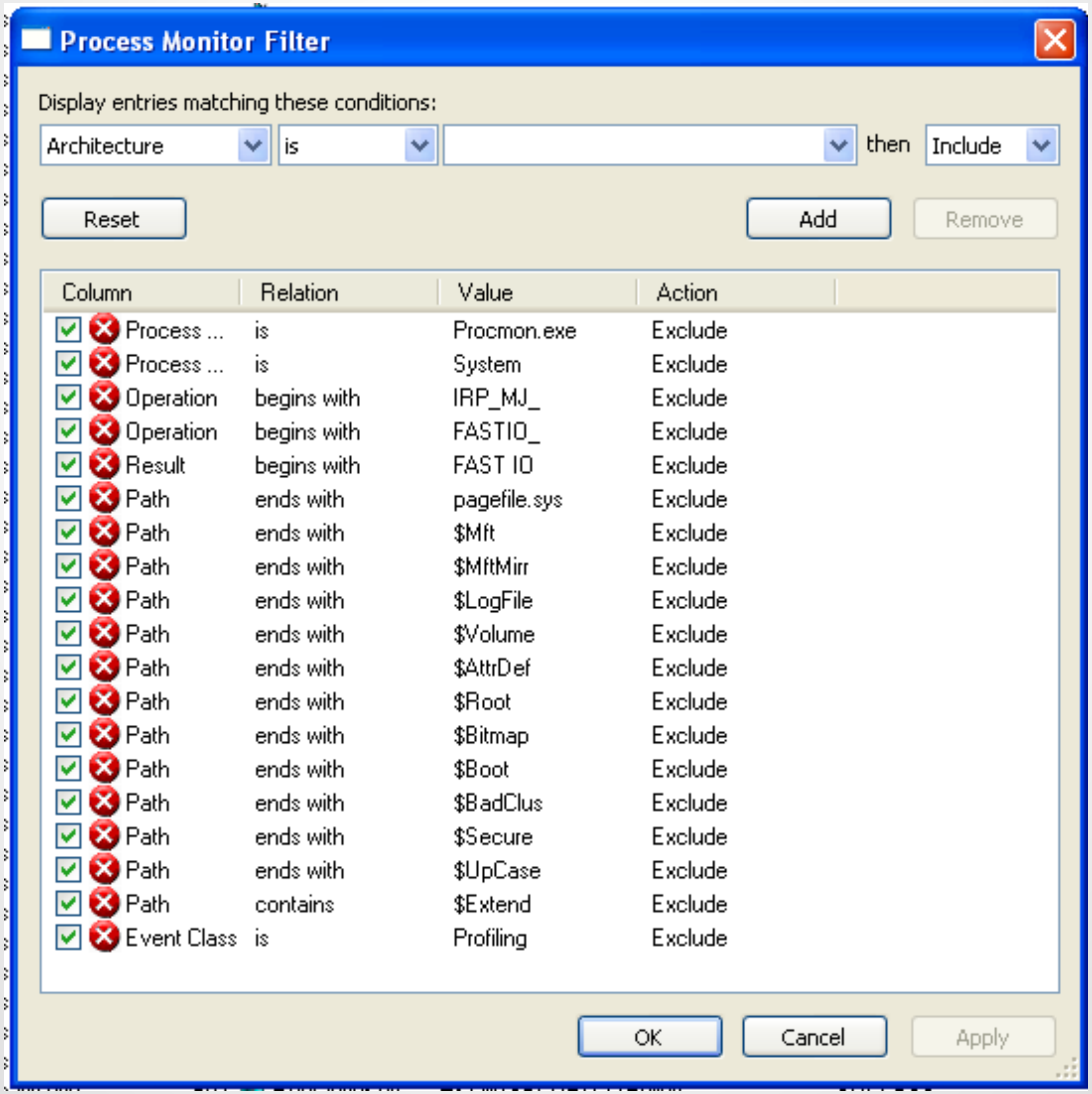
```
Time...  Process Name  PID  Operation      Path                                Result          Detail
3:48:5... svchost.exe  984  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\...    SUCCESS         Type: REG_BINA...
3:48:5... svchost.exe  984  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\...    SUCCESS         Type: REG_BINA...
3:48:5... svchost.exe  984  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: Q...
3:48:5... svchost.exe  984  RegOpenKey     HKCR                                SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Desired Access: M...
3:48:5... svchost.exe  984  RegQueryValue  HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Length: 144
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Desired Access: M...
3:48:5... svchost.exe  984  RegQueryValue  HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Type: REG_SZ, Le...
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegQueryValue  HKCR\CLSID\{CF4CC405-E2C5-4DDD-...NAME NOT FOUND  Length: 144
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{CF4CC405-E2C5-4DDD-...SUCCESS
3:48:5... svchost.exe  984  ReadFile       C:\WINDOWS\system32\wbem\Reposi...SUCCESS         Offset: 688,128, Le...
3:48:5... svchost.exe  984  ReadFile       C:\WINDOWS\system32\wbem\Reposi...SUCCESS         Offset: 729,088, Le...
3:48:5... svchost.exe  984  ReadFile       C:\WINDOWS\system32\wbem\Reposi...SUCCESS         Offset: 98,304, Len...
3:48:5... svchost.exe  984  ReadFile       C:\WINDOWS\system32\wbem\Reposi...SUCCESS         Offset: 180,224, Le...
3:48:5... svchost.exe  984  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\...    SUCCESS         Type: REG_BINA...
3:48:5... svchost.exe  984  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKLM\Software\Microsoft\COM3        SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegQueryValue  HKLM\SOFTWARE\Microsoft\COM3\...    SUCCESS         Type: REG_BINA...
3:48:5... svchost.exe  984  RegCloseKey    HKLM\SOFTWARE\Microsoft\COM3        SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... NAME NOT FOUND  Desired Access: Q...
3:48:5... svchost.exe  984  RegOpenKey     HKCR                                SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS         Desired Access: R...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS         Desired Access: M...
3:48:5... svchost.exe  984  RegQueryValue  HKCR\CLSID\{D68AF00A-29CB-43FA-... NAME NOT FOUND  Length: 144
3:48:5... svchost.exe  984  RegCloseKey    HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... NAME NOT FOUND  Desired Access: M...
3:48:5... svchost.exe  984  RegOpenKey     HKCR\CLSID\{D68AF00A-29CB-43FA-... SUCCESS         Desired Access: M...
```

```
Showing 15,727 of 52,180 events (30%)     Backed by virtual memory
```

Drilling Down

- Too much data becomes useless
  - Much like other kinds of security monitoring...
- What are we looking for?
- File creation, file deletion, registry edits
- Persistence mechanisms
  - More on that soon

Process Monitor Filters



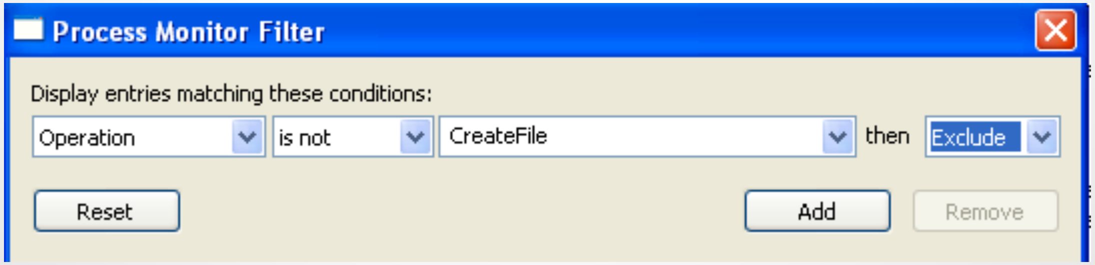
Display entries matching these conditions:

Architecture | is | | then | Include

	Column	Relation	Value	Action
☑	Process ...	is	Procmon.exe	Exclude
☑	Process ...	is	System	Exclude
☑	Operation	begins with	IRP_MJ_	Exclude
☑	Operation	begins with	FASTIO_	Exclude
☑	Result	begins with	FAST IO	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
☑	Path	ends with	$Bitmap	Exclude
☑	Path	ends with	$Boot	Exclude
☑	Path	ends with	$BadClus	Exclude
☑	Path	ends with	$Secure	Exclude
☑	Path	ends with	$UpCase	Exclude
☑	Path	contains	$Extend	Exclude
☑	Event Class	is	Profiling	Exclude

Custom Filters

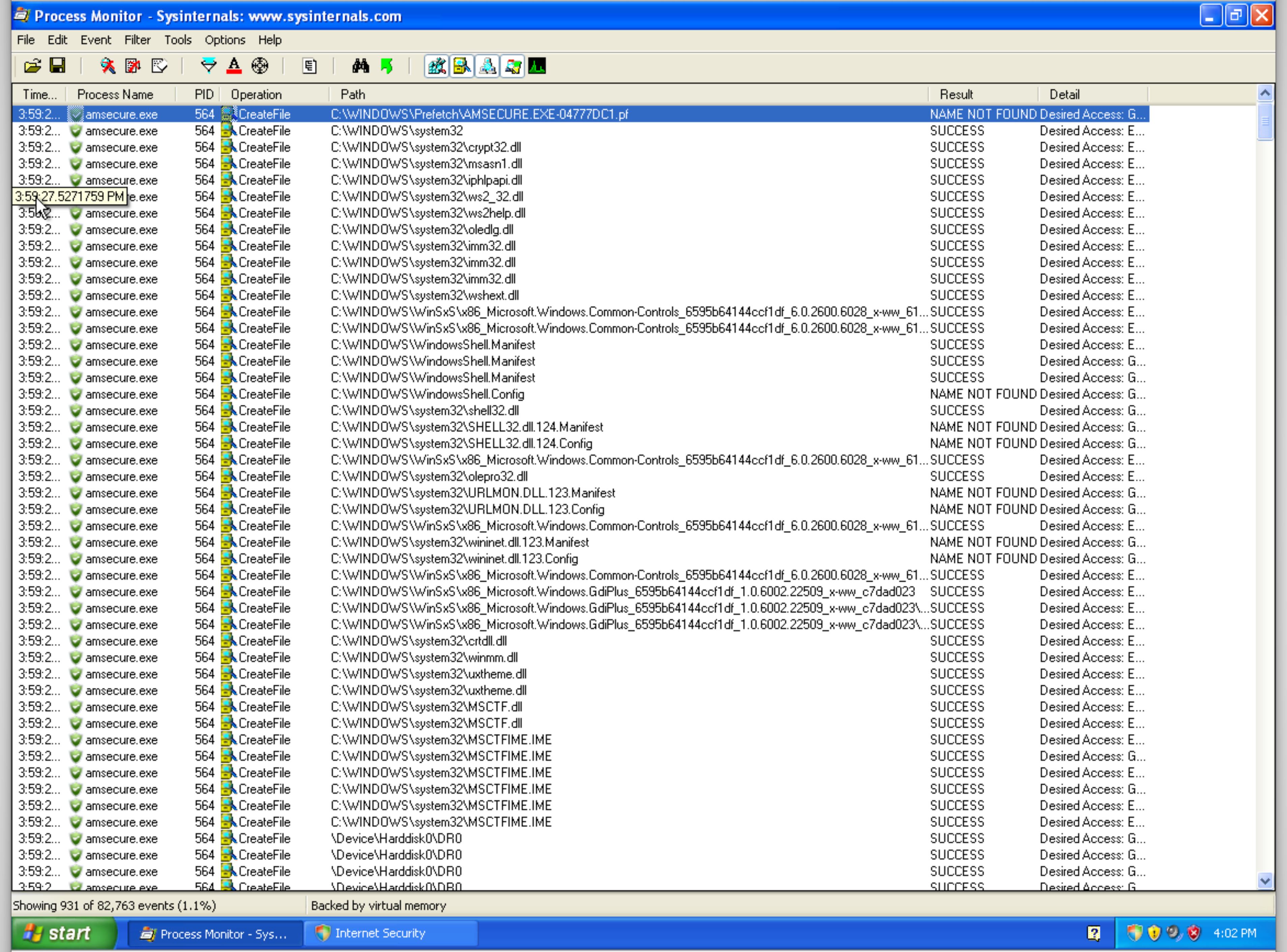
- Several approaches (inclusive vs. exclusive)
- Depends on what you’re looking for!
- For example:



Process Monitor Filter

Display entries matching these conditions:

Operation | is not | CreateFile | then | Exclude



Time...	Process Name	PID	Operation	Path	Result	Detail
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\Prefetch\AMSECURE.EXE-04777DC1.pf	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\crypt32.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\msasn1.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\iphlpapi.dll	SUCCESS	Desired Access: E...
3:59:27.5271759 PM	e.exe	564	CreateFile	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	Desired Access: E...
3:5...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\ws2help.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\oledlg.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\wshext.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WindowsShell.Config	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\SHELL32.dll.124.Manifest	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\SHELL32.dll.124.Config	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\olepro32.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\URLMON.DLL.123.Manifest	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\URLMON.DLL.123.Config	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\wininet.dll.123.Manifest	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\wininet.dll.123.Config	NAME NOT FOUND	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-ww_61...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.6002.22509_x-ww_c7dad023	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.6002.22509_x-ww_c7dad023\...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.6002.22509_x-ww_c7dad023\...	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\crtdll.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\winmm.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTF.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTF.dll	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	C:\WINDOWS\system32\MSCTFIME.IME	SUCCESS	Desired Access: E...
3:59:2...	amsecure.exe	564	CreateFile	\Device\Harddisk0\DR0	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	\Device\Harddisk0\DR0	SUCCESS	Desired Access: G...
3:59:2...	amsecure.exe	564	CreateFile	\Device\Harddisk0\DR0	SUCCESS	Desired Access: G...
3:59:2	amsecure.exe	564	CreateFile	\Device\Harddisk0\DR0	SUCCESS	Desired Access: G

Showing 931 of 82,763 events (1.1%)

Backed by virtual memory

What can this tell us?

- All file system operations
- Easy way to detect changing (or new) executables
- Filters allow fine-tuned results from a massive data set
- Can detect persistence mechanisms before they activate

Part III
Does it Stick Around?

Autoruns

- Ever used `msconfig`?

- It’s like that, except better in every way
    - Process Explorer : taskman :: Autoruns : msconfig

- Can easily view many different types of persistence mechanisms
    - Also useful for general system administration

- Also has a nice CLI mode (autorunsc.exe)

Interpreting Autoruns

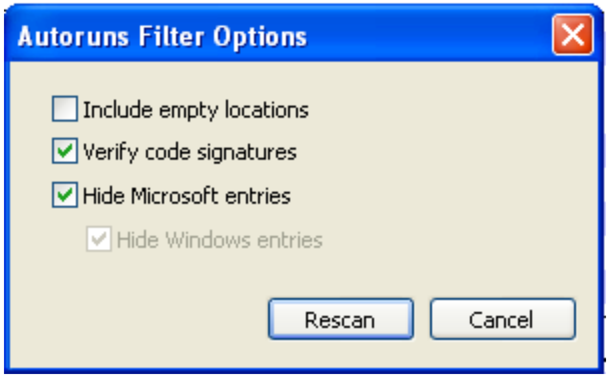
- Also color coded

- Like many other Sysinternals tools, can verify code signatures

- Can be used as a “run once” tool or `diff`ed
    - autorunsc.exe -c

Interpreting Autoruns

- Filters help



Autoruns Filter Options

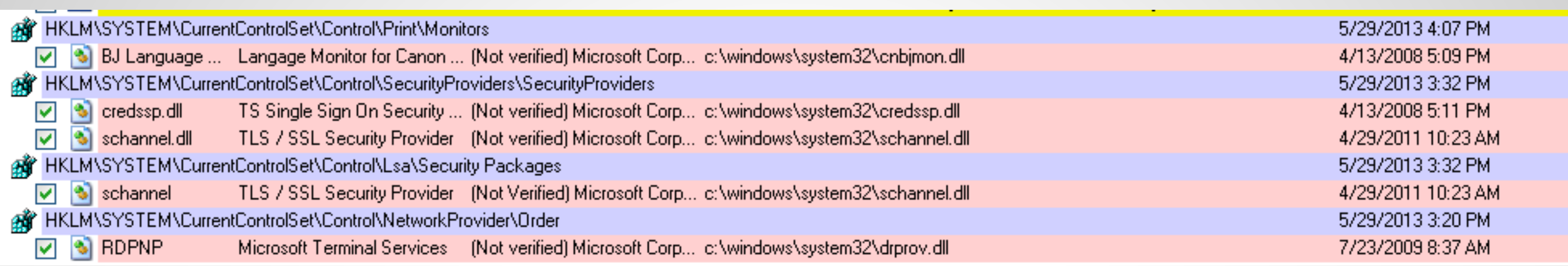
□ Include empty locations

☑ Verify code signatures

☑ Hide Microsoft entries

☑ Hide Windows entries

- Combining results with Process Monitor is usually a good idea, too



	Entry	Description	Publisher	Image Path	Timestamp
	HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors				5/29/2013 4:07 PM
☑	BJ Language ...	Langage Monitor for Canon ...	(Not verified) Microsoft Corp...	c:\windows\system32\cnbjmon.dll	4/13/2008 5:09 PM
	HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders				5/29/2013 3:32 PM
☑	credssp.dll	TS Single Sign On Security ...	(Not verified) Microsoft Corp...	c:\windows\system32\credssp.dll	4/13/2008 5:11 PM
☑	schannel.dll	TLS / SSL Security Provider	(Not verified) Microsoft Corp...	c:\windows\system32\schannel.dll	4/29/2011 10:23 AM
	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages				5/29/2013 3:32 PM
☑	schannel	TLS / SSL Security Provider	(Not Verified) Microsoft Corp...	c:\windows\system32\schannel.dll	4/29/2011 10:23 AM
	HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order				5/29/2013 3:20 PM
☑	RDPNP	Microsoft Terminal Services	(Not verified) Microsoft Corp...	c:\windows\system32\drprov.dll	7/23/2009 8:37 AM

Common Pitfalls

- Watch out for tricky malware
- Malware will often be redundant *many times over*
    - This is why anti-malware can have such a hard time
- Be wary of run-once (on reboot) entries
- Be wary of cmd.exe calls to write/delete/run other files

Part IV
What’s it saying?

Wireshark

- Wireshark is industry-standard GUI packet sniffer

- Very robust, includes filters, etc.

- Process Explorer & Process Monitor may already flag network connections

- Who is it talking to?

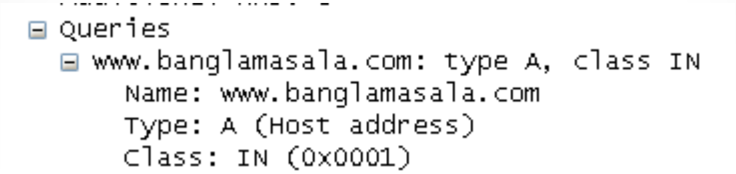
- What is it saying?

Who is it talking to?

- Malware almost always “calls home.”
    - If not, it’s going to send you somewhere (scareware/ransomware)
- C&Cs get shut down *constantly,* so malware likes to keep its network current
- This can also make analysis harder (more on that later)
- So what do we see?

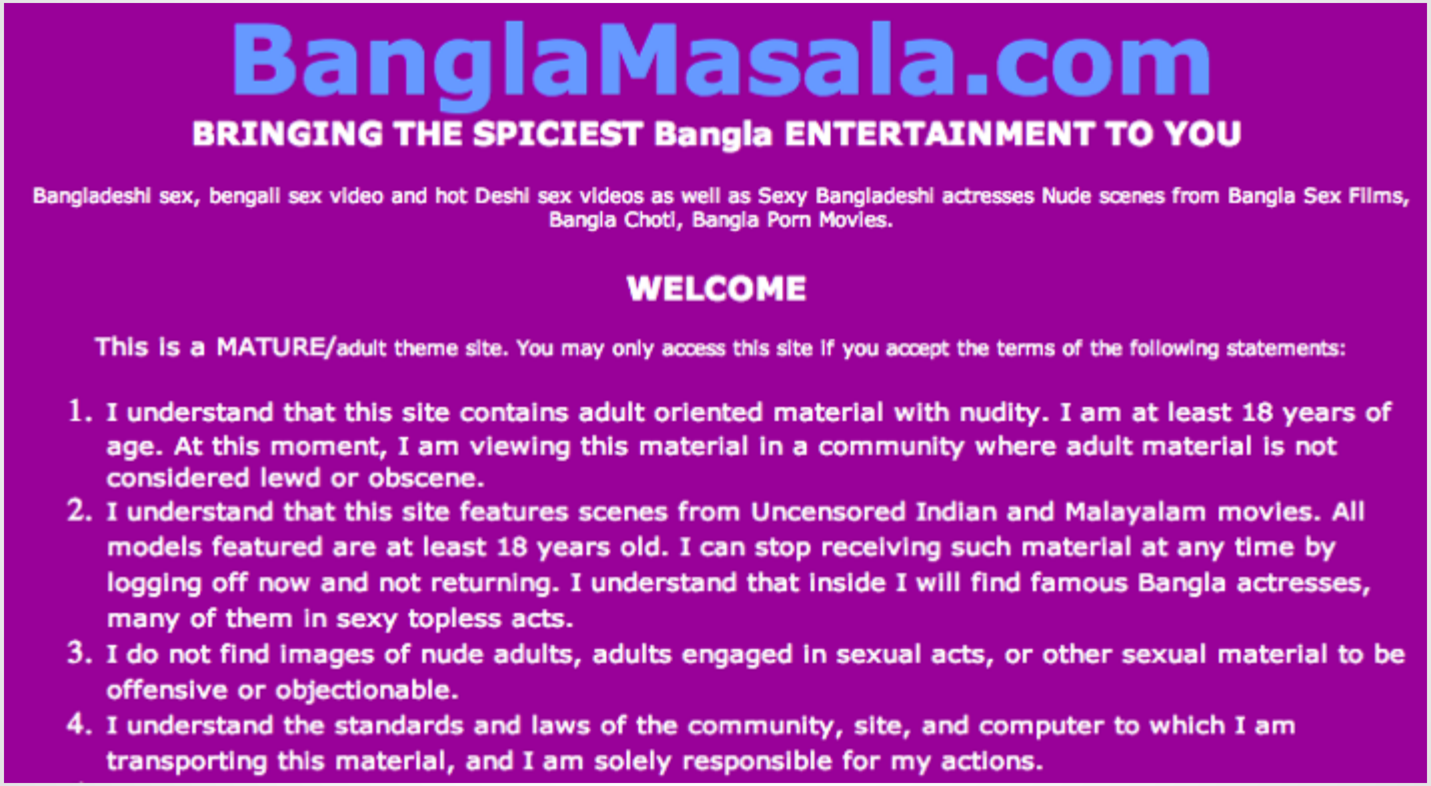
Who is it talking to?

- First thing we see is a DNS query:



```
⊟ Queries
  ⊟ www.banglamasala.com: type A, class IN
      Name: www.banglamasala.com
      Type: A (Host address)
      Class: IN (0x0001)
```

- I wonder what that is?



BanglaMasala.com

BRINGING THE SPICIEST Bangla ENTERTAINMENT TO YOU

Bangladeshi sex, bengali sex video and hot Deshi sex videos as well as Sexy Bangladeshi actresses Nude scenes from Bangla Sex Films, Bangla Choti, Bangla Porn Movies.

WELCOME

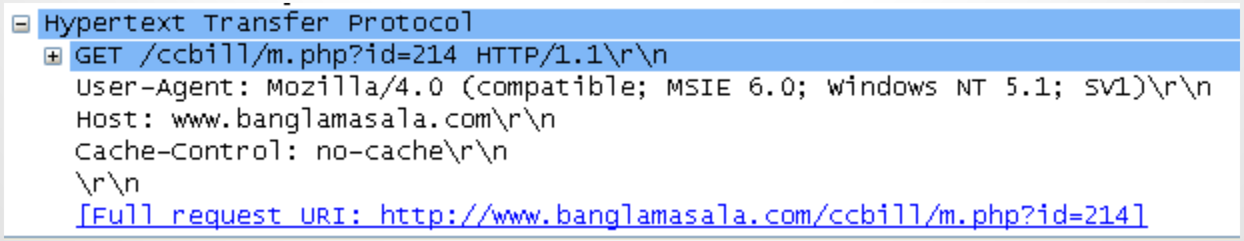
This is a MATURE/adult theme site. You may only access this site if you accept the terms of the following statements:

1. I understand that this site contains adult oriented material with nudity. I am at least 18 years of age. At this moment, I am viewing this material in a community where adult material is not considered lewd or obscene.
2. I understand that this site features scenes from Uncensored Indian and Malayalam movies. All models featured are at least 18 years old. I can stop receiving such material at any time by logging off now and not returning. I understand that inside I will find famous Bangla actresses, many of them in sexy topless acts.
3. I do not find images of nude adults, adults engaged in sexual acts, or other sexual material to be offensive or objectionable.
4. I understand the standards and laws of the community, site, and computer to which I am transporting this material, and I am solely responsible for my actions.

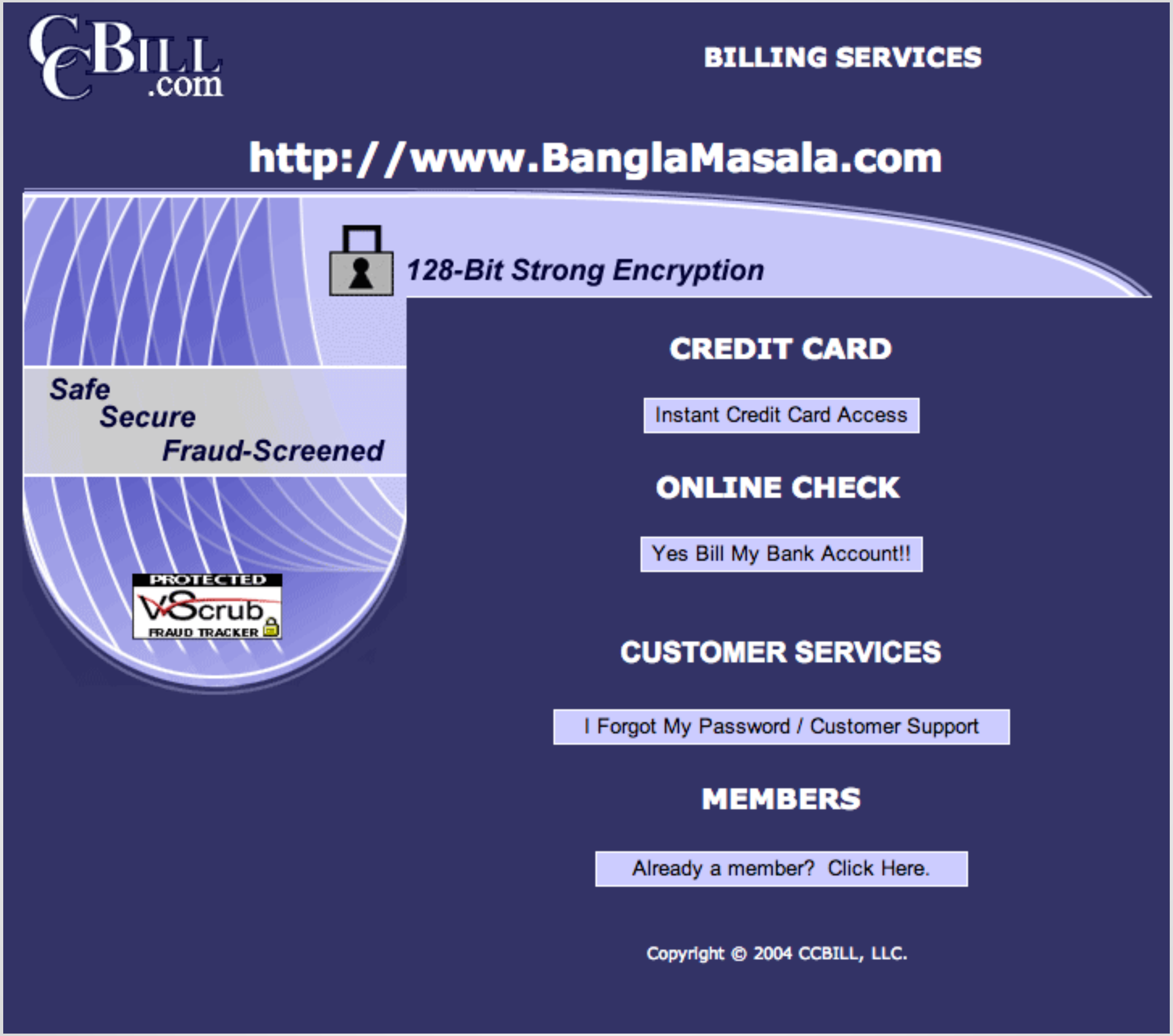
We’ll just call this “NSFW media.”

What else?

- “Sketchy,” but doesn’t appear to be blatantly malicious
- Probably a compromised host
- What does the malware do next?



```
⊟ Hypertext Transfer Protocol
  ⊞ GET /ccbill/m.php?id=214 HTTP/1.1\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
    Host: www.banglamasala.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://www.banglamasala.com/ccbill/m.php?id=214]
```



BILLING SERVICES

http://www.BanglaMasala.com

128-Bit Strong Encryption

Safe
Secure
Fraud-Screened

PROTECTED
VScrub
FRAUD TRACKER

CREDIT CARD

Instant Credit Card Access

ONLINE CHECK

Yes Bill My Bank Account!!

CUSTOMER SERVICES

I Forgot My Password / Customer Support

MEMBERS

Already a member? Click Here.

Spread that ‘net!

- `m.php` 404’d
- Further evidence of compromised (then fixed host)
- Malware doesn’t usually give up easily; when one server doesn’t work, the sample keeps trying
- When there’s nothing left and no response, it’s dead

Dealing with Dead Malware

- Malware (and C&Cs) have a very short lifespan

- By the time samples are easily available, this lifespan is usually over
  - Unless you found some 0day malware!

- Many researchers are working on this problem (it’s harder for dynamic analysts)

FakeNet

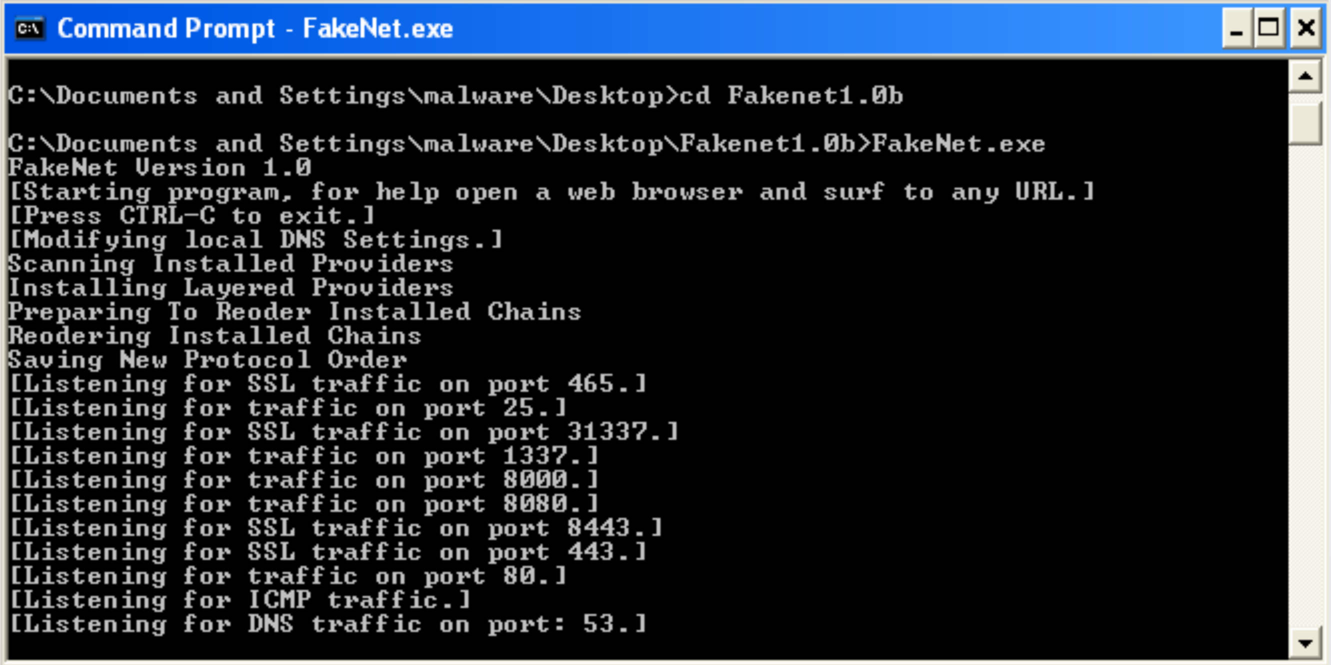
- FakeNet can simulate a “live” host that’s actually dead

- Very useful for seeing what malware does once commands are received

- Still not 100% effective if you can’t model traffic

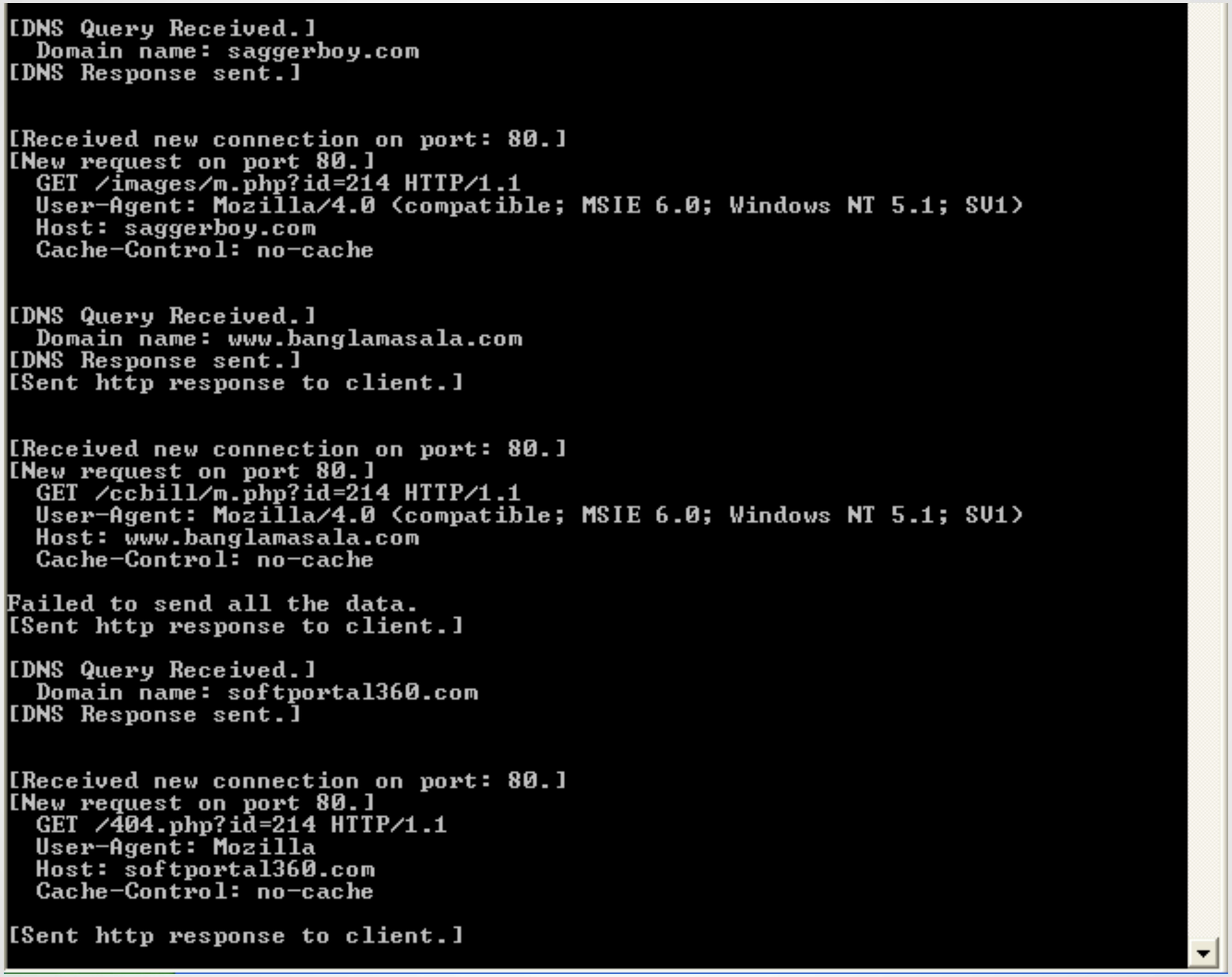
FakeNet

- Some major advantages:
  - Can view SSL-encrypted requests easily
  - Traps all traffic going out
  - Can usually lead to effective modeling of traffic
- http://sourceforge.net/projects/fakenet/



```
C:\Documents and Settings\malware\Desktop>cd Fakenet1.0b

C:\Documents and Settings\malware\Desktop\Fakenet1.0b>FakeNet.exe
FakeNet Version 1.0
[Starting program, for help open a web browser and surf to any URL.]
[Press CTRL-C to exit.]
[Modifying local DNS Settings.]
Scanning Installed Providers
Installing Layered Providers
Preparing To Reoder Installed Chains
Reodering Installed Chains
Saving New Protocol Order
[Listening for SSL traffic on port 465.]
[Listening for traffic on port 25.]
[Listening for SSL traffic on port 31337.]
[Listening for traffic on port 1337.]
[Listening for traffic on port 8000.]
[Listening for traffic on port 8080.]
[Listening for SSL traffic on port 8443.]
[Listening for SSL traffic on port 443.]
[Listening for traffic on port 80.]
[Listening for ICMP traffic.]
[Listening for DNS traffic on port: 53.]
```



```
[DNS Query Received.]
  Domain name: saggerboy.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /images/m.php?id=214 HTTP/1.1
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
  Host: saggerboy.com
  Cache-Control: no-cache


[DNS Query Received.]
  Domain name: www.banglamasala.com
[DNS Response sent.]
[Sent http response to client.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /ccbill/m.php?id=214 HTTP/1.1
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
  Host: www.banglamasala.com
  Cache-Control: no-cache

Failed to send all the data.
[Sent http response to client.]

[DNS Query Received.]
  Domain name: softportal360.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /404.php?id=214 HTTP/1.1
  User-Agent: Mozilla
  Host: softportal360.com
  Cache-Control: no-cache

[Sent http response to client.]
```

Further Research

- Practice on known malware

- Read up on static vs. dynamic analysis
  - CrackMe’s

- *Practical Malware Analysis*

- Find and analyze new malware!

Thank You!