Reverse Engineering: Towards Malware Analysis

Lecture – Basic Dynamic Analysis

Computer Science Practice

SPRING 2023

Outline

- Sandboxes
- Running malware
- Monitoring the malware
- Faking the network
- Tools in practice

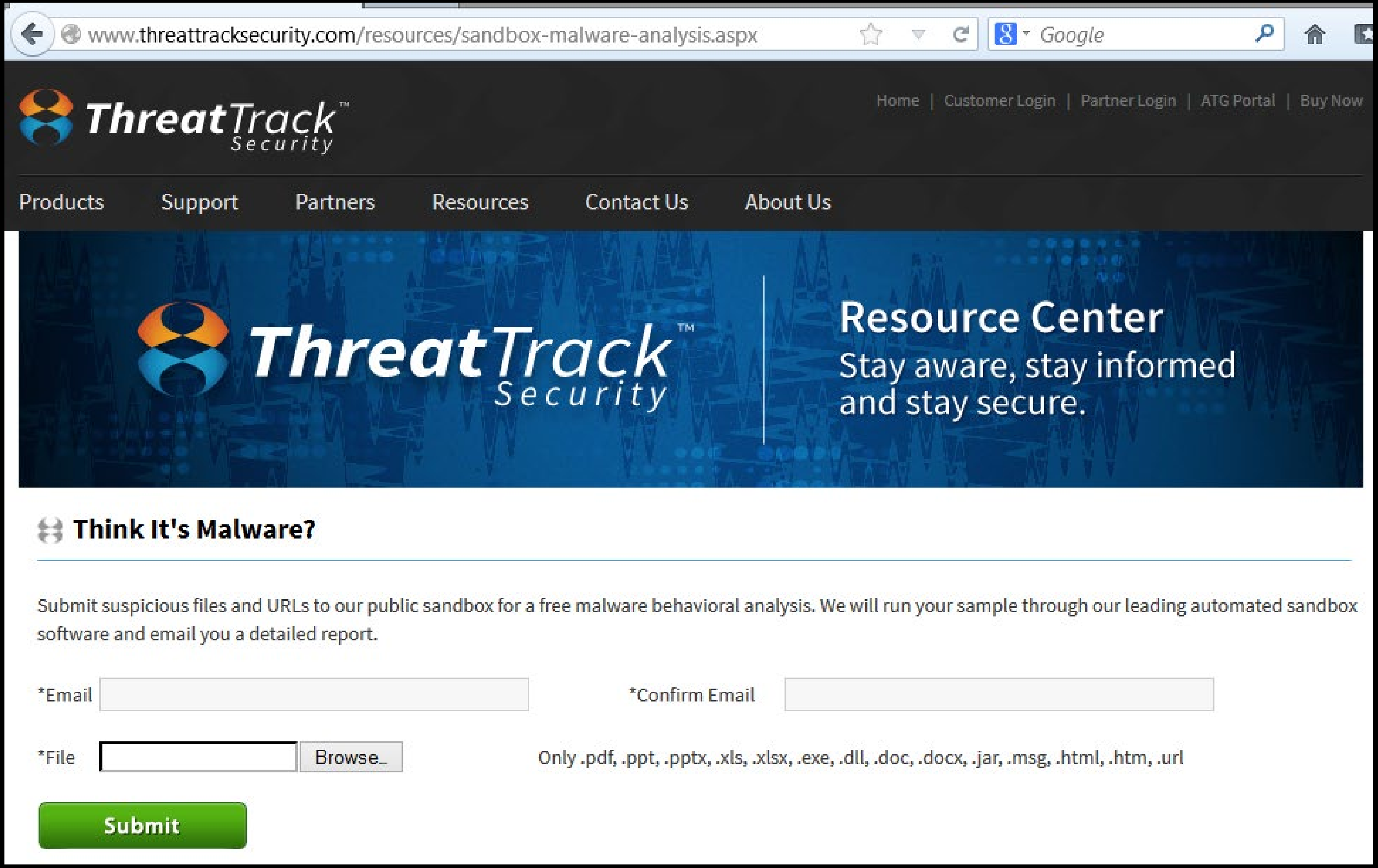
Dynamic Analysis

- Performed after static analysis
- Especially if static analysis reaches a dead-end, including due to obfuscation, packing, etc.
- Allows you to view the malware's functionality as it runs
- WARNING!!
- Not fool-proof: *code coverage* issue

Dynamic Analysis Sandboxes

- Norman
- CW Sandbox (GFI Sandbox)
- Anubis
- Joe Sandbox
- ThreatExpert
- BitBlaze
- Comodo Instant Malware Analysis
- *Great for initial analysis, but …*

GFI ThreatTrack



www.threattracksecurity.com/resources/sandbox-malware-analysis.aspx

Resource Center

Stay aware, stay informed and stay secure.

Think It's Malware?

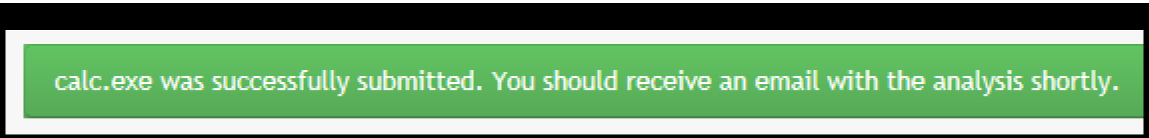
Submit suspicious files and URLs to our public sandbox for a free malware behavioral analysis. We will run your sample through our leading automated sandbox software and email you a detailed report.

*Email

*Confirm Email

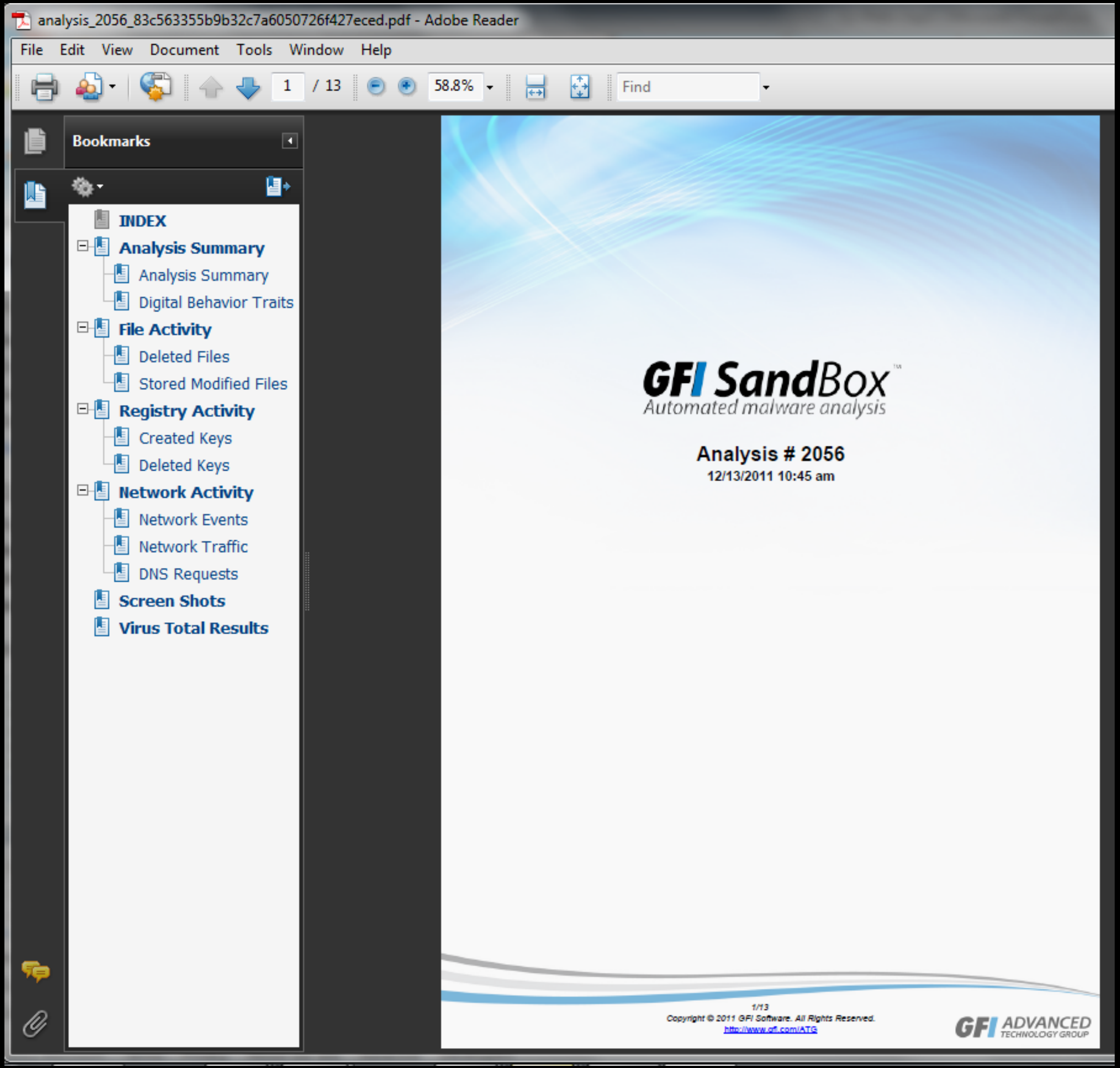
*File

Only .pdf, .ppt, .pptx, .xls, .xlsx, .exe, .dll, .doc, .docx, .jar, .msg, .html, .htm, .url



calc.exe was successfully submitted. You should receive an email with the analysis shortly.

Sample Report



analysis_2056_83c563355b9b32c7a6050726f427eced.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 13
58.8%
Find
Bookmarks

- INDEX
- Analysis Summary
  - Analysis Summary
  - Digital Behavior Traits
- File Activity
  - Deleted Files
  - Stored Modified Files
- Registry Activity
  - Created Keys
  - Deleted Keys
- Network Activity
  - Network Events
  - Network Traffic
  - DNS Requests
- Screen Shots
- Virus Total Results

GFI SandBox™
Automated malware analysis

Analysis # 2056
12/13/2011 10:45 am

1/13
Copyright © 2011 GFI Software. All Rights Reserved.
http://www.gfi.com/ATG

GFI ADVANCED TECHNOLOGY GROUP

Drawbacks to Using a Sandbox

- Execution & payload delivery must be quick
  - Sandbox won’t wait forever
  - Malware sleeps
- Most sandboxes use VMs: Can be detectable
- Sandbox environments may be missing required DLLs or environment variables
- Incompatible OS
- External inputs required

Running Malware

- Be careful!
- Running EXEs == easy enough
- What about DLLs?
    - `rundll32.exe`: requires a target export
    - `rundll32.exe [DLLname], [Export] [arguments]`
    - `rundll32.exe rip.dll, Install`
    - `rundll32.exe xyzzy.dll, #5`
- Converting the DLL to an EXE
    - Bit flip on `IMAGE_FILE_DLL` flag inside `IMAGE_FILE_HEADER`
    - Run `DLLMain` method:
      it may crash, but hopefully run enough to execute the payload

Running Malware - Services

- Service DLLs are common

```
>rundll32 ipr32x.dll, InstallService ServiceName
>net start ServiceName
```

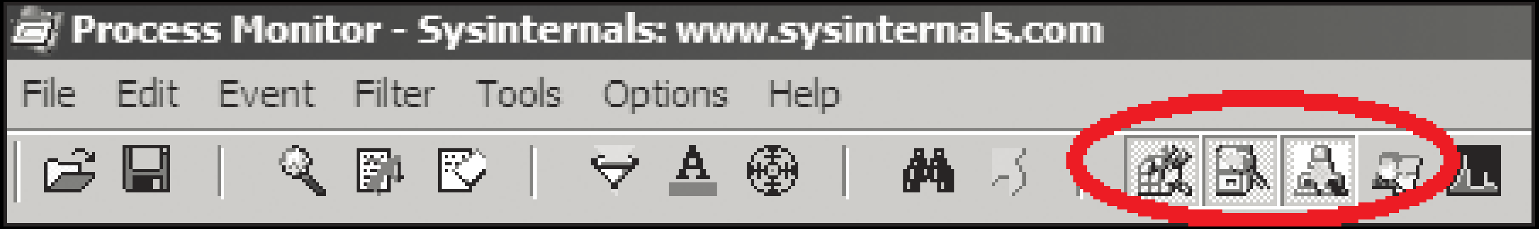
- Manual Installation

  Regedit (unused service HKLM\SYSTEM\CurrentControlSet\Service\AppMgmt\Parameters\ServiceDLL)

```
>net start AppMgmt
```

Process Monitor

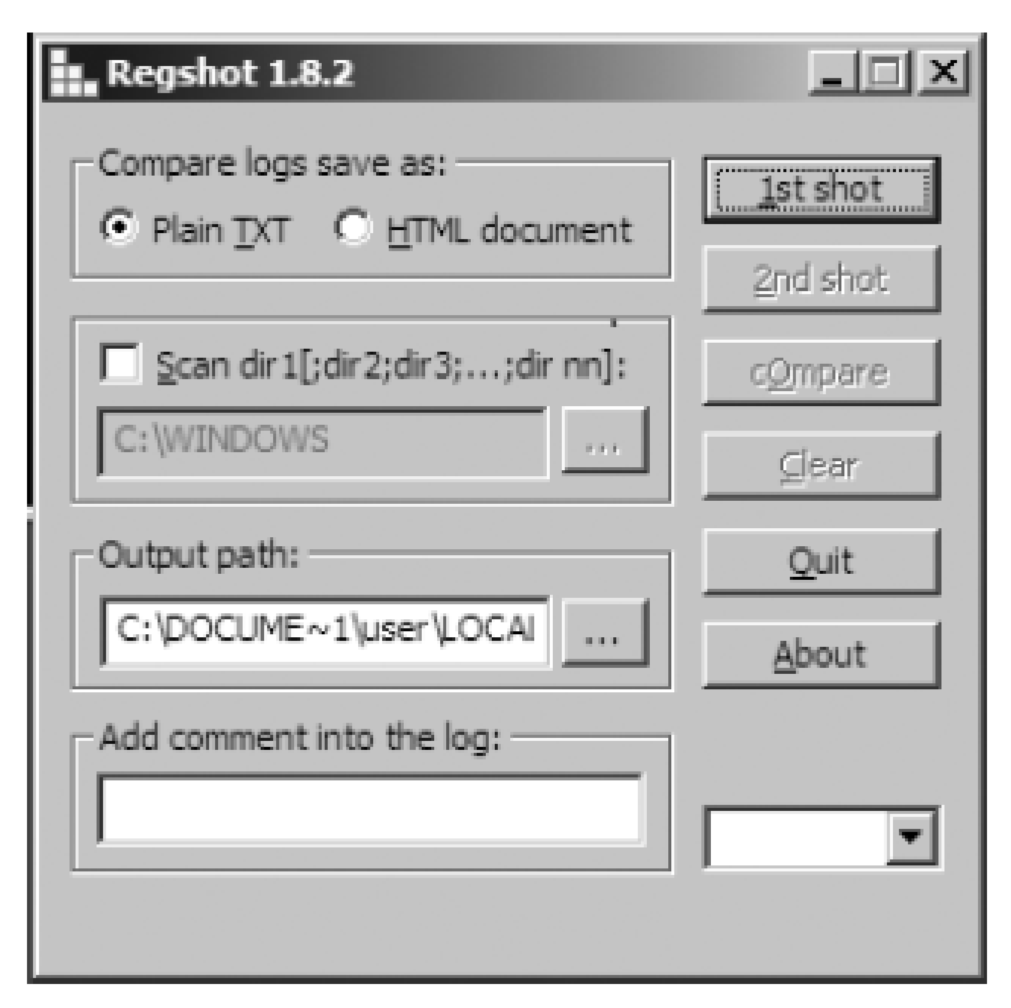
- WARNING!
- (Display) Filter, Filter, Filter: Include, Exclude
- Included automatic filters
  - Registry, File system, Network, Process Activity



- Don't run it too long:
  The RAM will be filled up, and your machine will crash!

Regshot

- Take the first shot
- Run malware
  (or do something)
- Take the second shot
- Inspect what registry keys are changed!



Regshot 1.8.2

Compare logs save as:

● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:

C:\WINDOWS

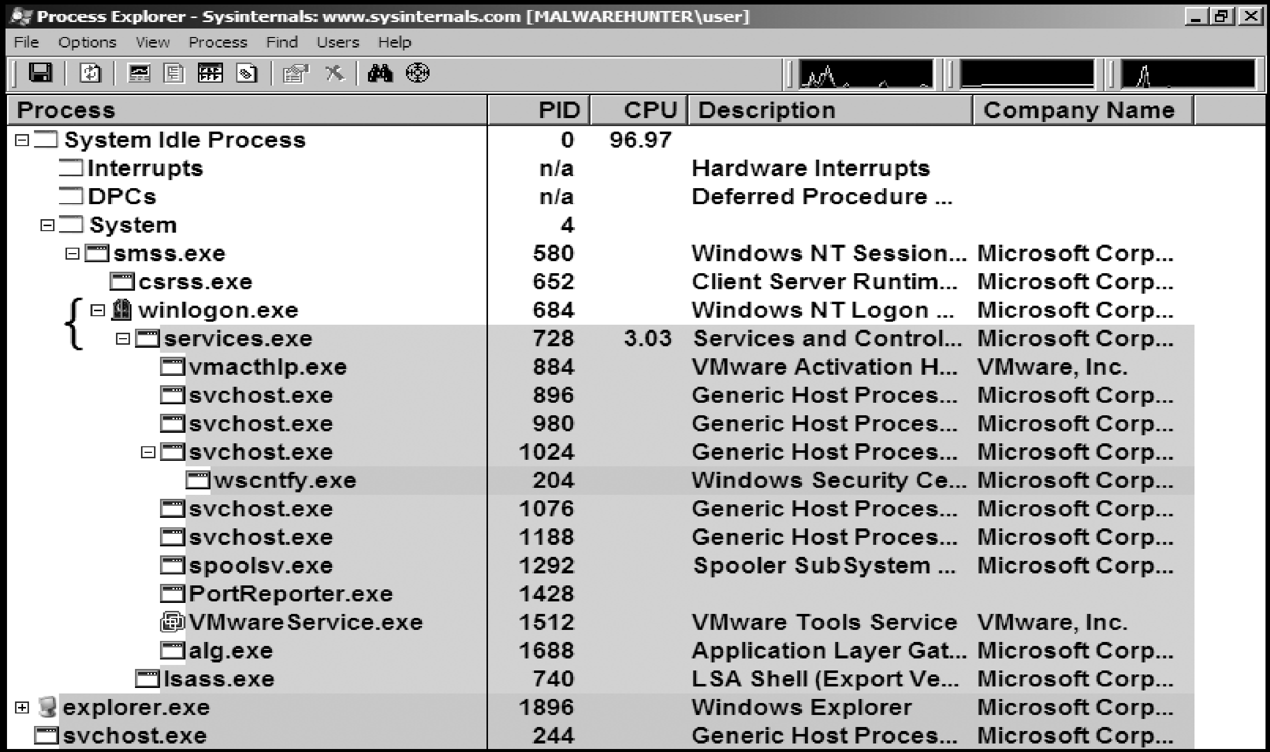
Output path:

C:\DOCUME~1\user\LOCAl

Add comment into the log:

Process Explorer

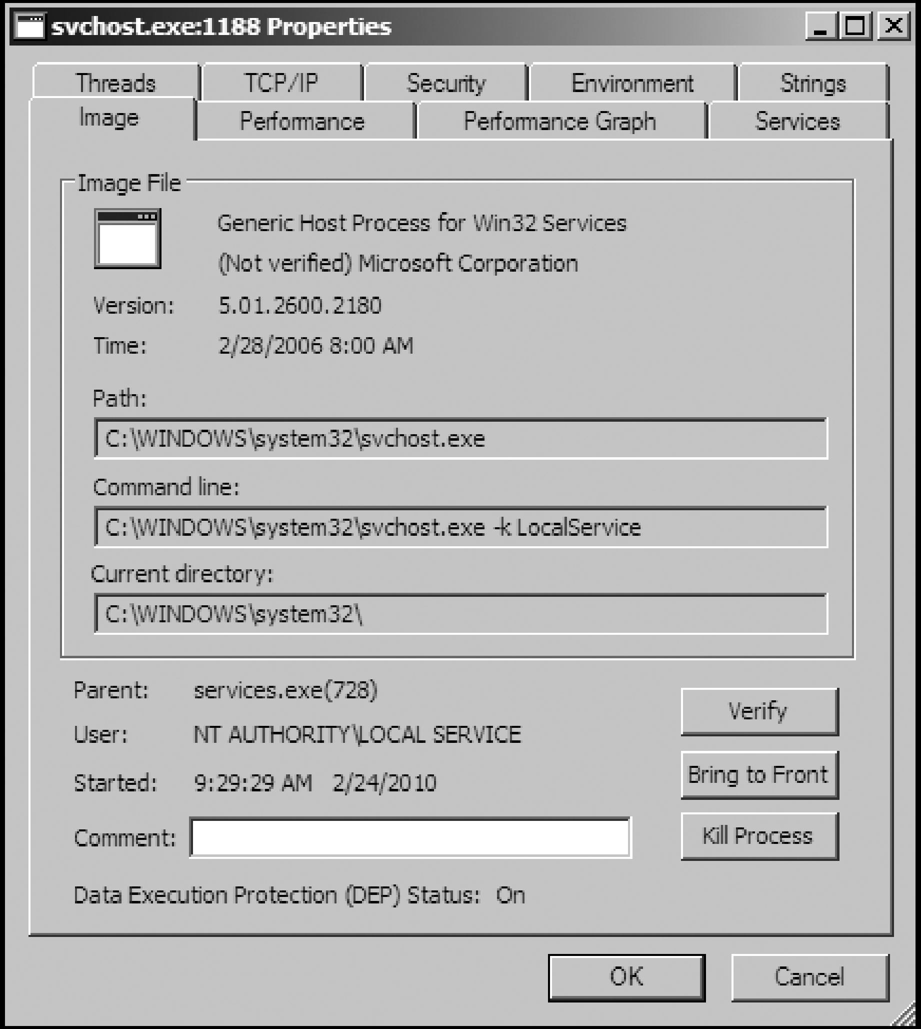
- Displays processes running on a system in a tree-structure
  - Shows child → parent relationship


Process Explorer - Sysinternals: www.sysinternals.com [MALWAREHUNTER\user]
File
Options
View
Process
Find
Users
Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	96.97		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure ...	
System	4			
smss.exe	580		Windows NT Session...	Microsoft Corp...
csrss.exe	652		Client Server Runtim...	Microsoft Corp...
winlogon.exe	684		Windows NT Logon ...	Microsoft Corp...
services.exe	728	3.03	Services and Control...	Microsoft Corp...
vmacthlp.exe	884		VMware Activation H...	VMware, Inc.
svchost.exe	896		Generic Host Proces...	Microsoft Corp...
svchost.exe	980		Generic Host Proces...	Microsoft Corp...
svchost.exe	1024		Generic Host Proces...	Microsoft Corp...
wscntfy.exe	204		Windows Security Ce...	Microsoft Corp...
svchost.exe	1076		Generic Host Proces...	Microsoft Corp...
svchost.exe	1188		Generic Host Proces...	Microsoft Corp...
spoolsv.exe	1292		Spooler SubSystem ...	Microsoft Corp...
PortReporter.exe	1428			
VMwareService.exe	1512		VMware Tools Service	VMware, Inc.
alg.exe	1688		Application Layer Gat...	Microsoft Corp...
lsass.exe	740		LSA Shell (Export Ve...	Microsoft Corp...
explorer.exe	1896		Windows Explorer	Microsoft Corp...
svchost.exe	244		Generic Host Proces...	Microsoft Corp...

Process Explorer

- Double click on a process to see its properties:



Generic Host Process for Win32 Services

(Not verified) Microsoft Corporation

Version: 5.01.2600.2180

Time: 2/28/2006 8:00 AM

Path: C:\WINDOWS\system32\svchost.exe

Command line: C:\WINDOWS\system32\svchost.exe -k LocalService

Current directory: C:\WINDOWS\system32\

Parent: services.exe(728)

User: NT AUTHORITY\LOCAL SERVICE

Started: 9:29:29 AM 2/24/2010

Comment:

Data Execution Protection (DEP) Status: On

Verify: A Signed Binary (On the Disk)?

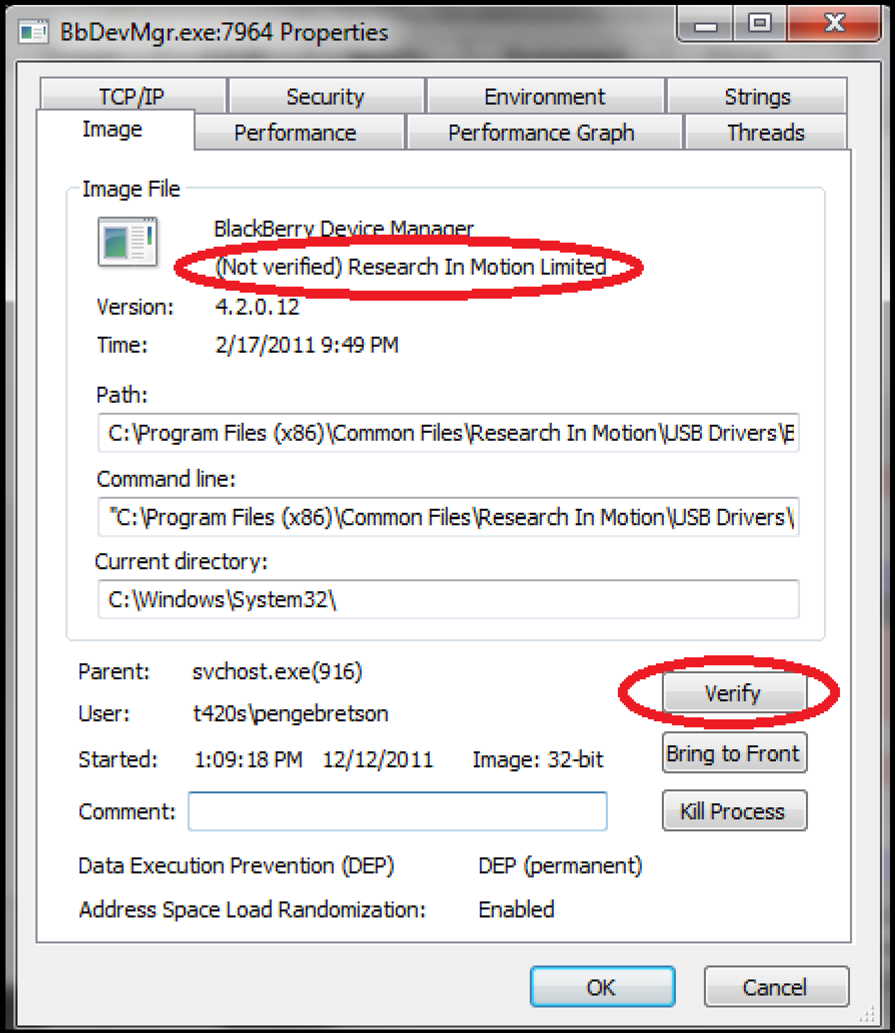


Image File

BlackBerry Device Manager

(Not verified) Research In Motion Limited

Version: 4.2.0.12

Time: 2/17/2011 9:49 PM

Path:

C:\Program Files (x86)\Common Files\Research In Motion\USB Drivers\E

Command line:

"C:\Program Files (x86)\Common Files\Research In Motion\USB Drivers\

Current directory:

C:\Windows\System32\

Parent: svchost.exe(916)

User: t420s\pengebretson

Started: 1:09:18 PM 12/12/2011 Image: 32-bit

Comment:

Data Execution Prevention (DEP) DEP (permanent)

Address Space Load Randomization: Enabled

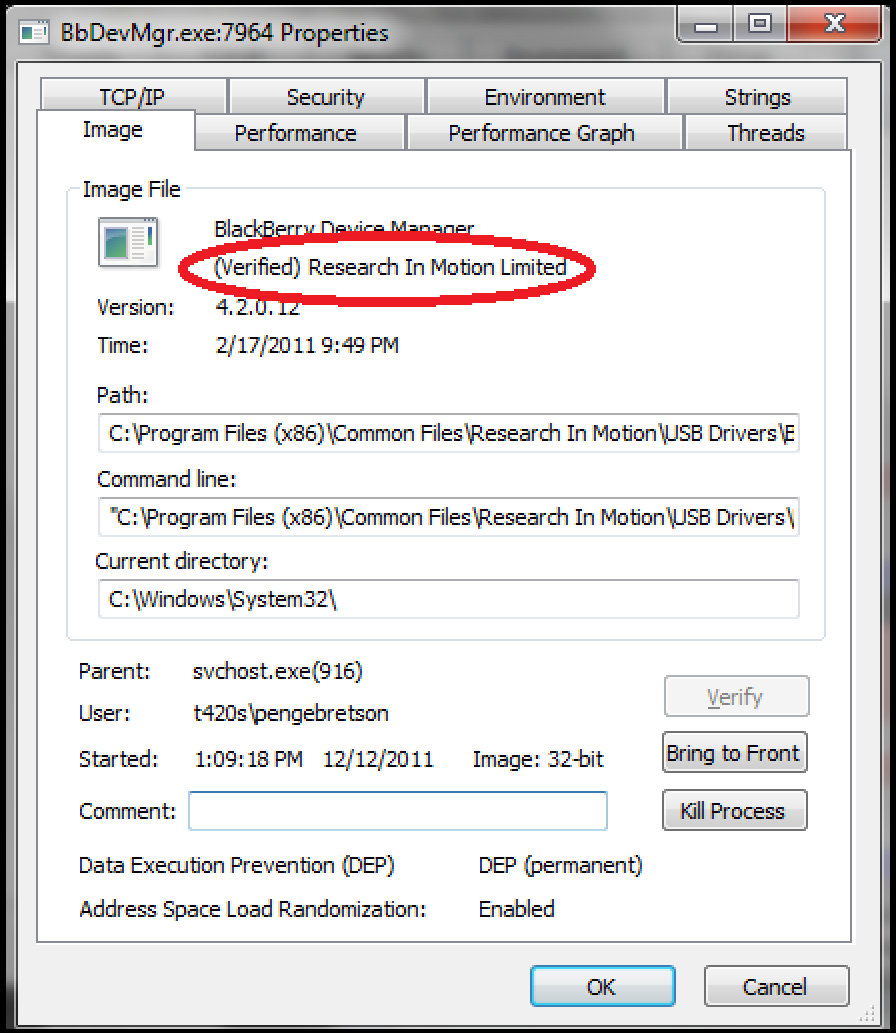


Image File

BlackBerry Device Manager

(Verified) Research In Motion Limited

Version: 4.2.0.12

Time: 2/17/2011 9:49 PM

Path:

C:\Program Files (x86)\Common Files\Research In Motion\USB Drivers\E

Command line:

"C:\Program Files (x86)\Common Files\Research In Motion\USB Drivers\

Current directory:

C:\Windows\System32\

Parent: svchost.exe(916)

User: t420s\pengebretson

Started: 1:09:18 PM 12/12/2011 Image: 32-bit

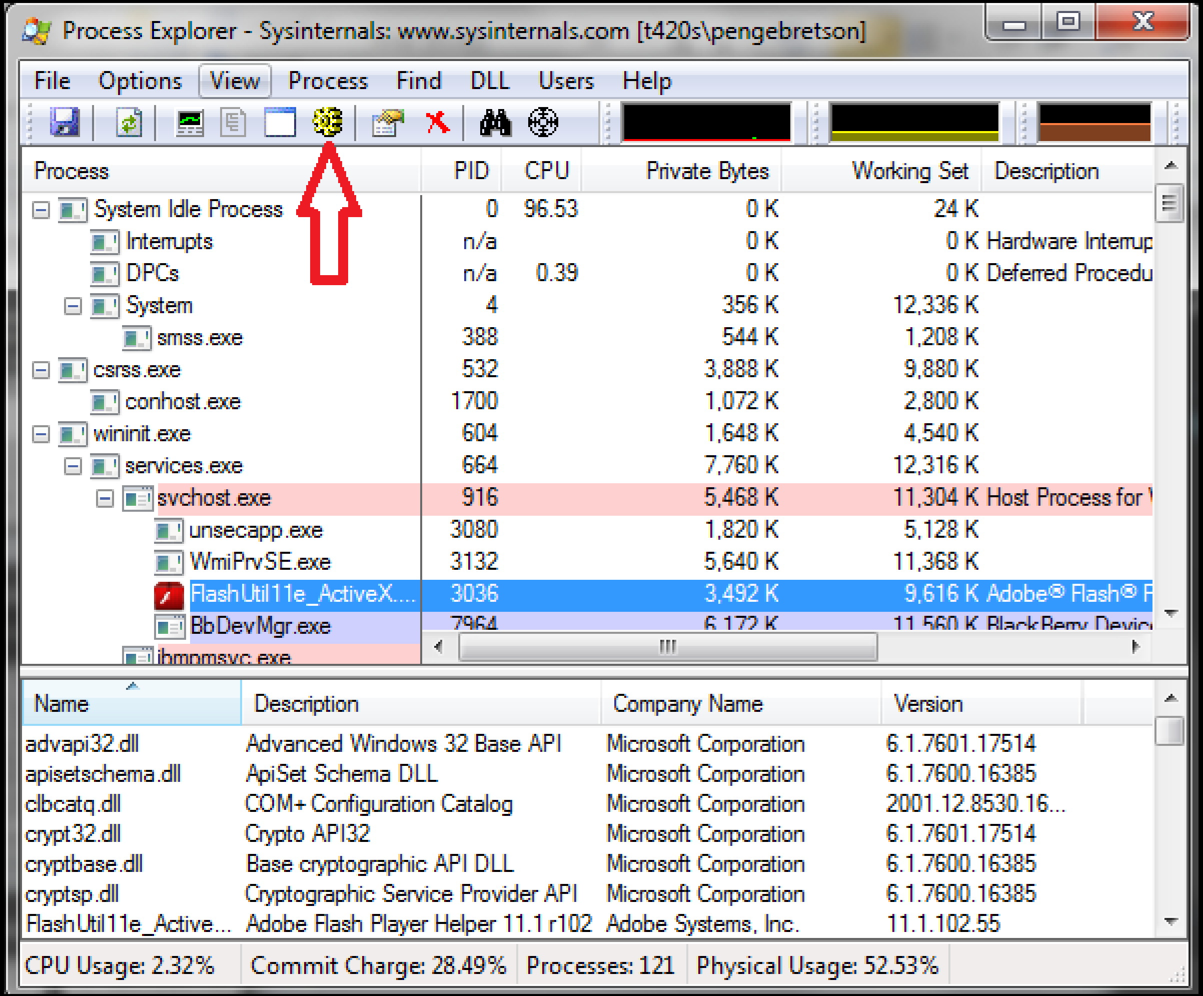
Comment:

Data Execution Prevention (DEP) DEP (permanent)

Address Space Load Randomization: Enabled

View DLLs

- CTRL+D
  (or click the shown icon)



Process Explorer - Sysinternals: www.sysinternals.com [t420s\pengebretson]

Process	PID	CPU	Private Bytes	Working Set	Description
System Idle Process	0	96.53	0 K	24 K	
Interrupts	n/a		0 K	0 K	Hardware Interrup
DPCs	n/a	0.39	0 K	0 K	Deferred Procedu
System	4		356 K	12,336 K	
smss.exe	388		544 K	1,208 K	
csrss.exe	532		3,888 K	9,880 K	
conhost.exe	1700		1,072 K	2,800 K	
wininit.exe	604		1,648 K	4,540 K	
services.exe	664		7,760 K	12,316 K	
svchost.exe	916		5,468 K	11,304 K	Host Process for \
unsecapp.exe	3080		1,820 K	5,128 K	
WmiPrvSE.exe	3132		5,640 K	11,368 K	
FlashUtil11e_ActiveX....	3036		3,492 K	9,616 K	Adobe® Flash® F
BbDevMgr.exe	7964		6,172 K	11,560 K	BlackBerry Devic
ibmpmsvc.exe					

Name	Description	Company Name	Version
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.1.7601.17514
apisetschema.dll	ApiSet Schema DLL	Microsoft Corporation	6.1.7600.16385
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	2001.12.8530.16...
crypt32.dll	Crypto API32	Microsoft Corporation	6.1.7601.17514
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	6.1.7600.16385
cryptsp.dll	Cryptographic Service Provider API	Microsoft Corporation	6.1.7600.16385
FlashUtil11e_Active...	Adobe Flash Player Helper 11.1 r102	Adobe Systems, Inc.	11.1.102.55

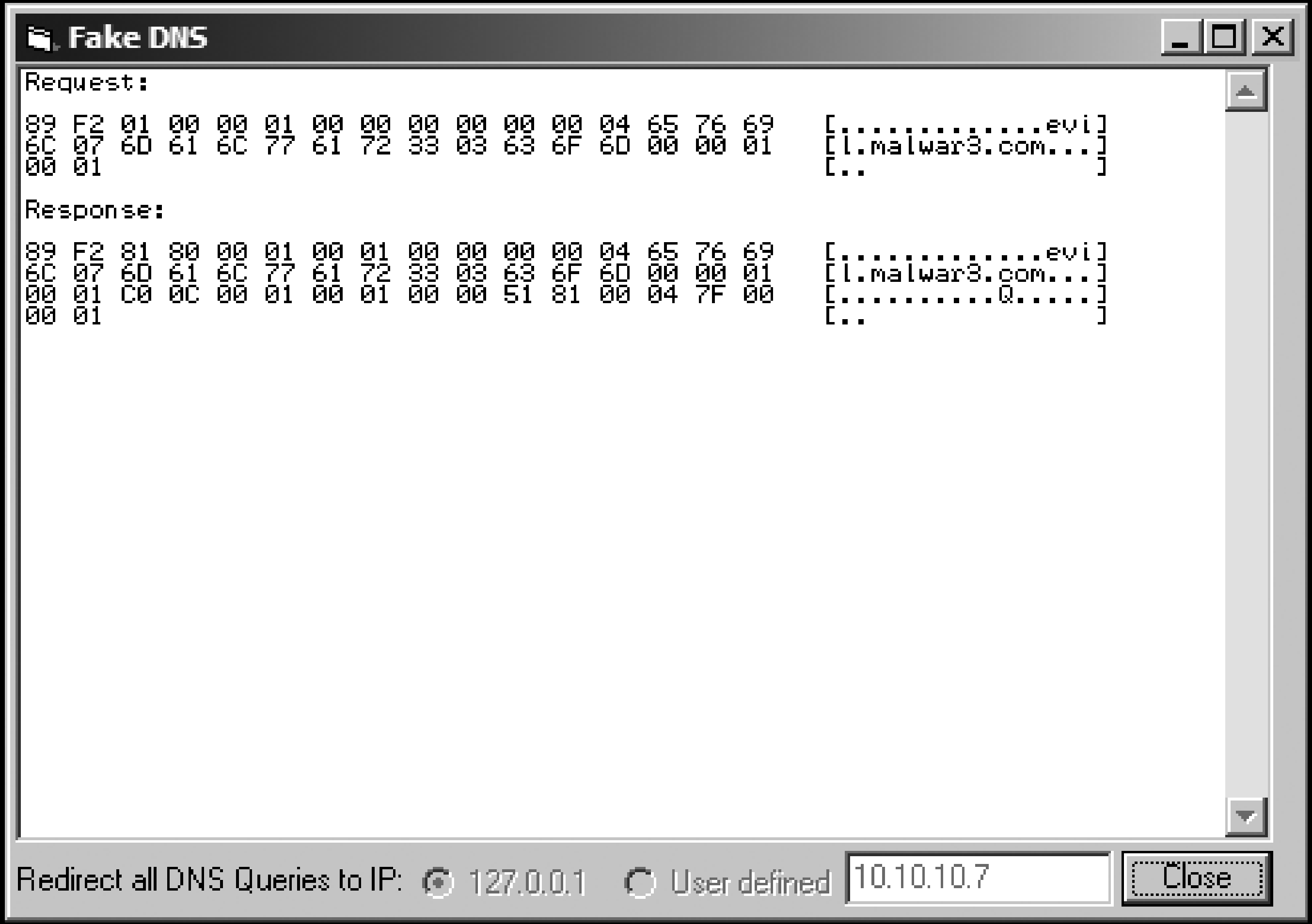
CPU Usage: 2.32% | Commit Charge: 28.49% | Processes: 121 | Physical Usage: 52.53%

Faking the Network

FakeDNS

- Included with iDefense Malcode Analysis Pack
  - Installed on the local machine
  - Responds to DNS requests from the malware
  - Displays the hex and ASCII results of all requests/responses
- To use
  - Install FakeDNS
  - Set the local DNS server to `127.0.0.1`
  - Start FakeDNS

FakeDNS Example

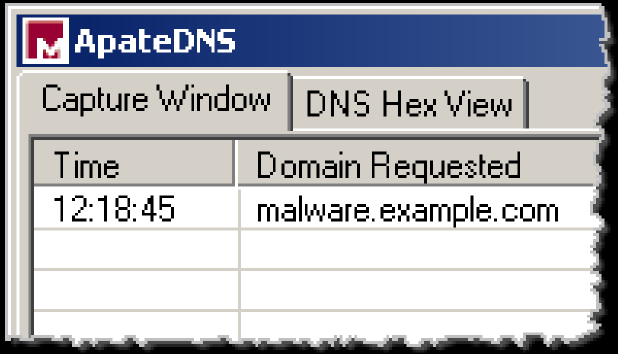


```
Request:

89 F2 01 00 00 01 00 00 00 00 00 00 04 65 76 69    [.............evi]
6C 07 6D 61 6C 77 61 72 33 03 63 6F 6D 00 00 01    [l.malwar3.com...]
00 01                                              [..              ]

Response:

89 F2 81 80 00 01 00 01 00 00 00 00 04 65 76 69    [.............evi]
6C 07 6D 61 6C 77 61 72 33 03 63 6F 6D 00 00 01    [l.malwar3.com...]
00 01 C0 0C 00 01 00 01 00 00 51 81 00 04 7F 00    [..........Q.....]
00 01                                              [..              ]
```

Redirect all DNS Queries to IP: ● 127.0.0.1 ○ User defined 10.10.10.7

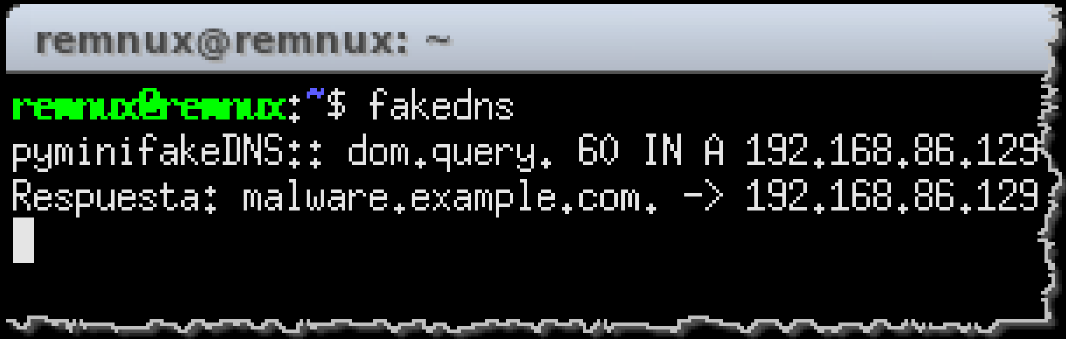
Other Options for Faking DNS

- ApateDNS
  - Mandiant GUI tool



Time	Domain Requested
12:18:45	malware.example.com

- fakeDNS.py
  - Linux tool
  - With REMnux



```
remnux@remnux:~$ fakedns
pyminifakeDNS:: dom.query. 60 IN A 192.168.86.129
Respuesta: malware.example.com. -> 192.168.86.129
```

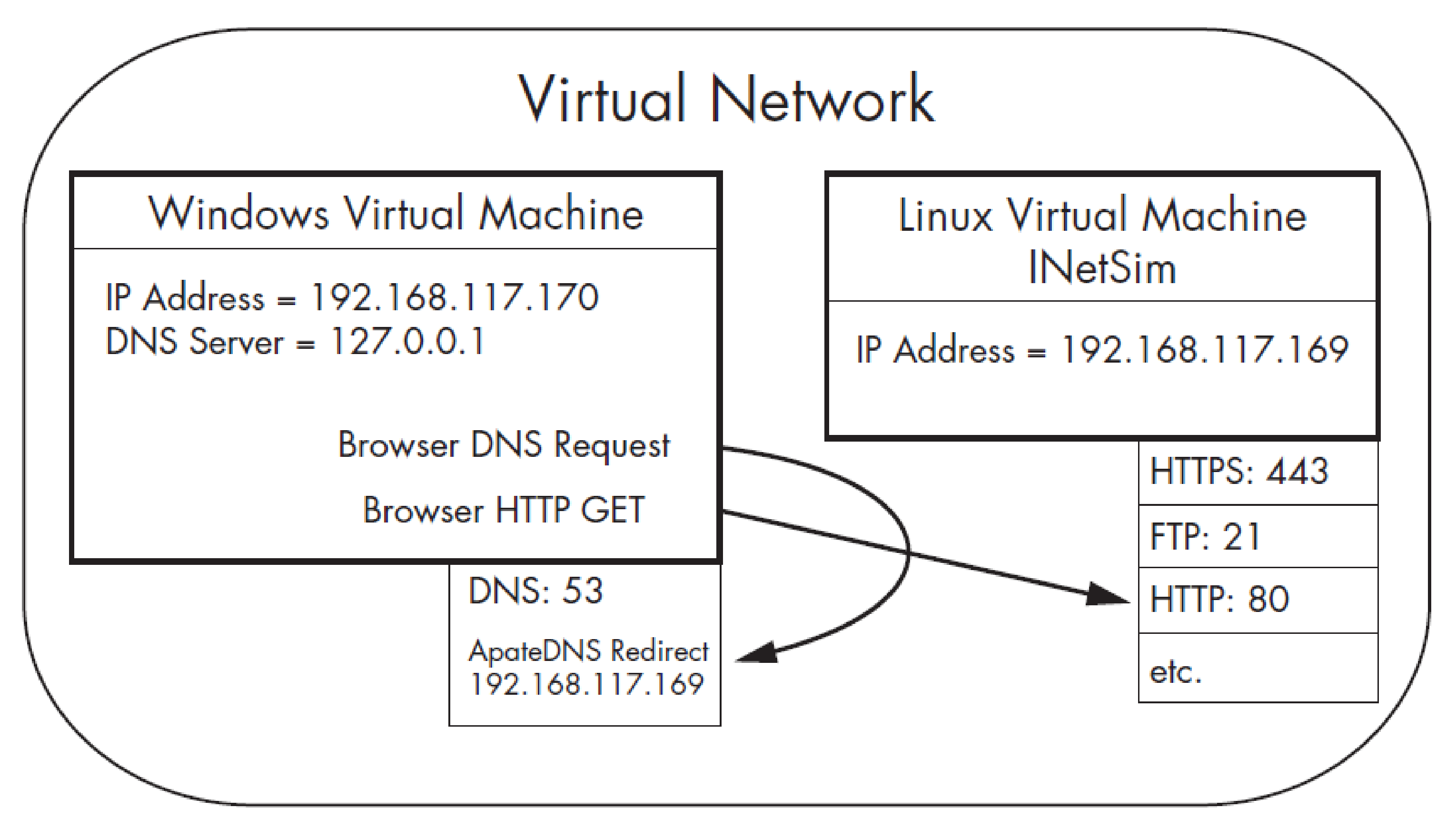
Netcat for Network Monitoring

- Redirect traffic by manipulating DNS, e.g. using FakeDNS
- Run NC in listen mode to accept connections on monitored ports
- Usage:
  - `nc -l -p 80`

INetSim

- Free, Linux-based VM
- Emulates common services
  - HTTP, HTTPS, FTP, IRC, DNS. etc.
- Serves up what it can to look like a real server
- Fully configurable
- *Dummy Services*: log all data regardless of the port

INetSim: Set-Up Example



FakeNet

- Allows you to completely trick the malware’s networking operations
  - Continue execution – malware might do more
  - HTTP serving
- Layered Service Provider (LSP)
  - Winsock hooking - any `send() & connect()` calls are hooked
- Protocols: DNS, HTTP, SSL
- DNS module
  - Allows you to resolve any DNS name to any IP Address in the configuration file
  - NXDomain

FakeNet (Cntd.)

- Supports pcap based capturing for offline analysis
  - Built-in localhost packer capture
- Python extensions
  - SMTP plug-in
  - Custom plugin support:
    Create a custom C2 script for a given piece of malware
- Dummy listener to listen for traffic on any port
- Works for DNS or direct IP connections
- Available at practicalmalwareanalysis.com

Summary

- Covered basic dynamic analysis tools & techniques
- Used to confirm static findings
- Generate leads for future analysis
- Faking the network is important
- Be careful!
- Still doesn’t tell the whole story
- That’s why, *to be continued*….!

?