

Malware Analysis

Basic Dynamic Analysis

Introduction

- Basic Dynamic Analysis is the next step after completion of basic static analysis, here the malware is executed in the controlled environment for monitoring its behaviour, functionality and characteristics.
- Dynamic analysis lets you observe the malware's true functionality, because, for example, the existence of an action string in a binary does not mean the action will actually execute.
- Dynamic analysis may put your system and network at risk.
- Dynamic techniques do have their limitations, because not all code paths may execute when a piece of malware is run.

Limitation(s)

- In the case of command-line malware that requires arguments, each argument could execute different program functionality, and without knowing the options you wouldn't be able to dynamically examine all of the program's functionality.
- Cannot identify its programming logic of malicious functions and behavior.



Executing DLL

- Because malicious DLLs frequently run most of their code in DLLMain (called from the DLL entry point), and because DLLMain is executed whenever the DLL is loaded, you can often get information dynamically by forcing the DLL to load using rundll32.exe.
- It can be tricky to launch malicious DLLs because Windows doesn't know how to run them automatically.
- Rundll32.exe provides a container for running a DLL using this syntax in cmd:
 - **>rundll32.exe Dllname, Functionname(Ordinal) argument**
 - Examples:
 - **>rundll32.exe rip.dll, Install**
 - **>rundll32.exe xyzzy.dll, #5**



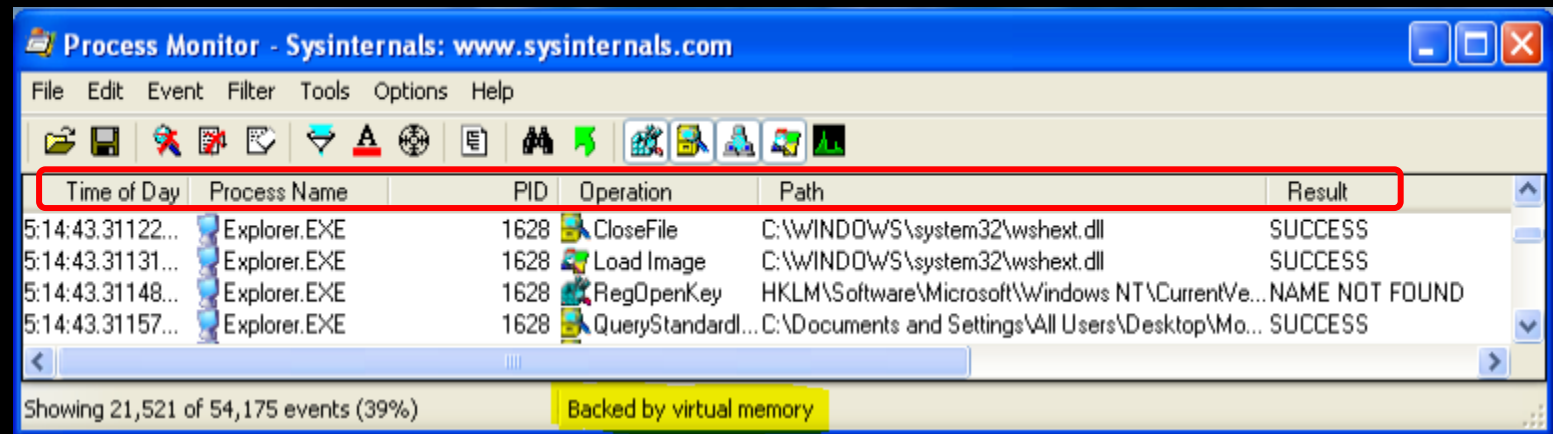
Process Monitor

- Procmon is an advanced monitoring tool for Windows that provides a way to monitor certain registry, file system, network, process, and thread activity.
- It combines and enhances the functionality of two legacy tools: FileMon and RegMon.
- Although procmon captures a lot of data, it doesn't capture everything.
- For example, it *can miss the device driver activity of a user-mode component* talking to a rootkit via device I/O controls, as well as certain GUI calls, such as SetWindowsHookEx.



Process Monitor

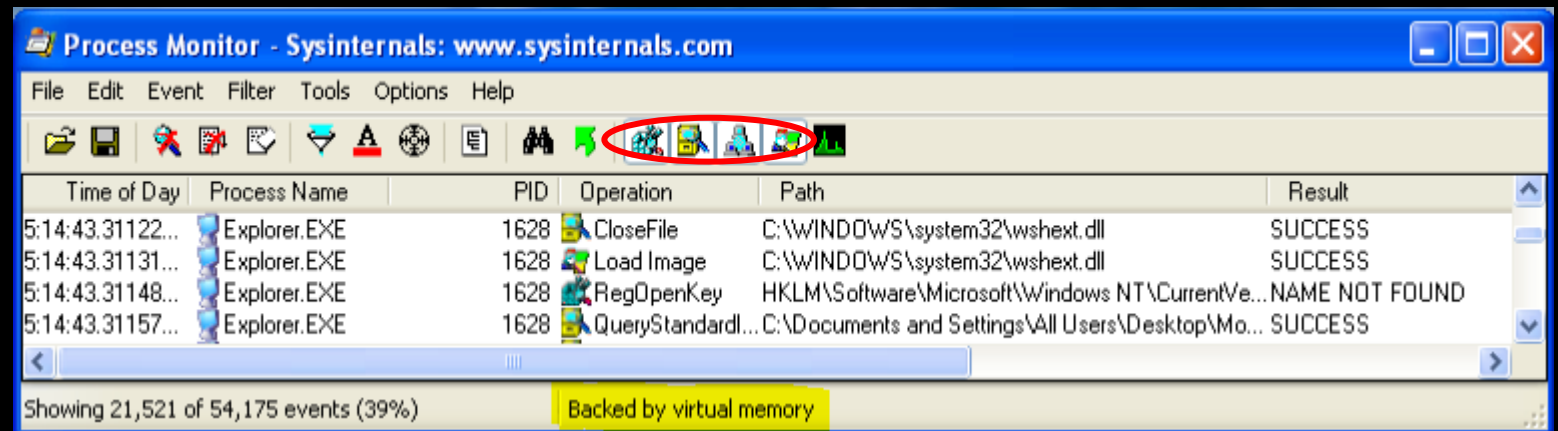
- Procmon monitors all system calls it can gather as soon as it is run.
- Because many system calls exist on a Windows machine (sometimes more than 50,000 events a minute), it's usually impossible to look through them all.
- As a result, because procmon uses RAM to log events until it is told to stop capturing, it can **crash a virtual machine** using all available memory.





Process Monitor

- **Automatic Filters of Procmon:**
- **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 you whether the malware spawned additional processes.
- **Network** Identifying network connections can show you any ports on which the malware is listening.





-



Process Monitor

- If your malware runs at boot time, use procmon's boot logging options to install procmon as a startup driver to capture startup events.

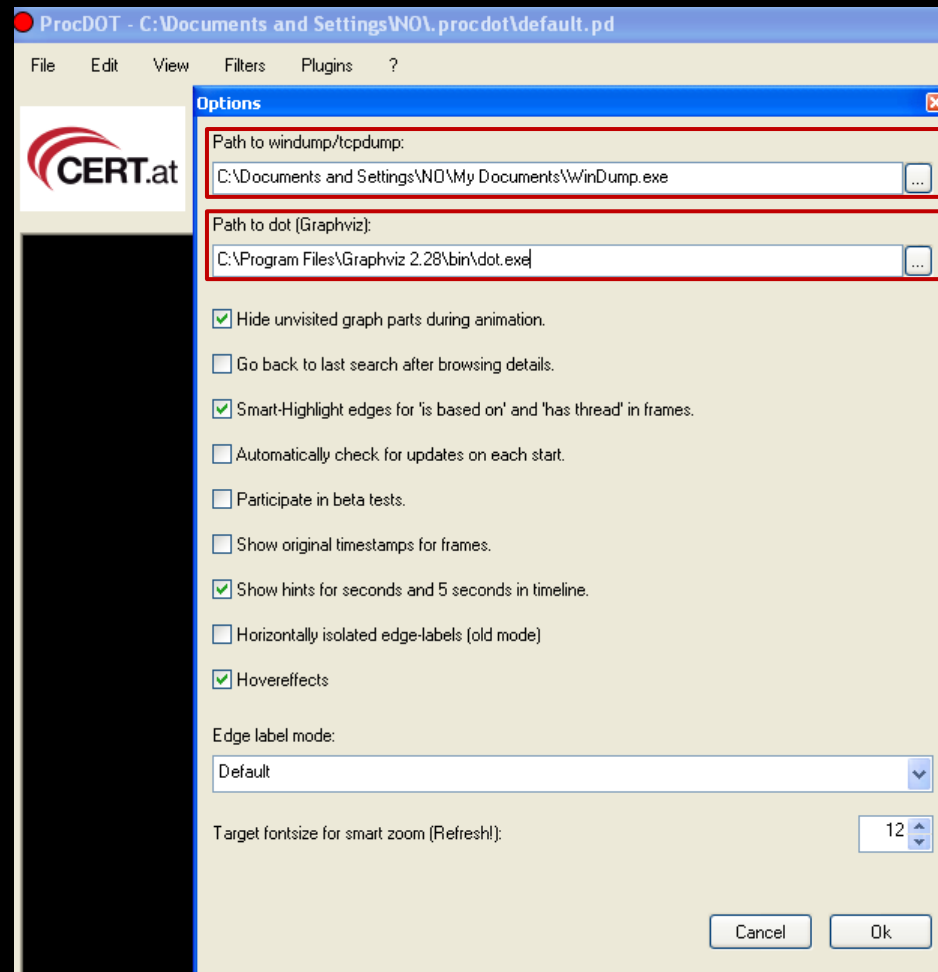


ProcDOT

- ProcDOT is not necessarily a malware analysis tool. **ProcDOT is a tool that visualizes system activities in a very convenient way.**
- ProcDOT has some of the below features:
- something that lets us get an overall guts feeling for an entire situation within a glance,
- something that enables us to spot relevant parts and understand the correlation between them in minutes, and finally
- something that provides us a perfect starting point for deeper, detailed and even code level analysis if necessary.



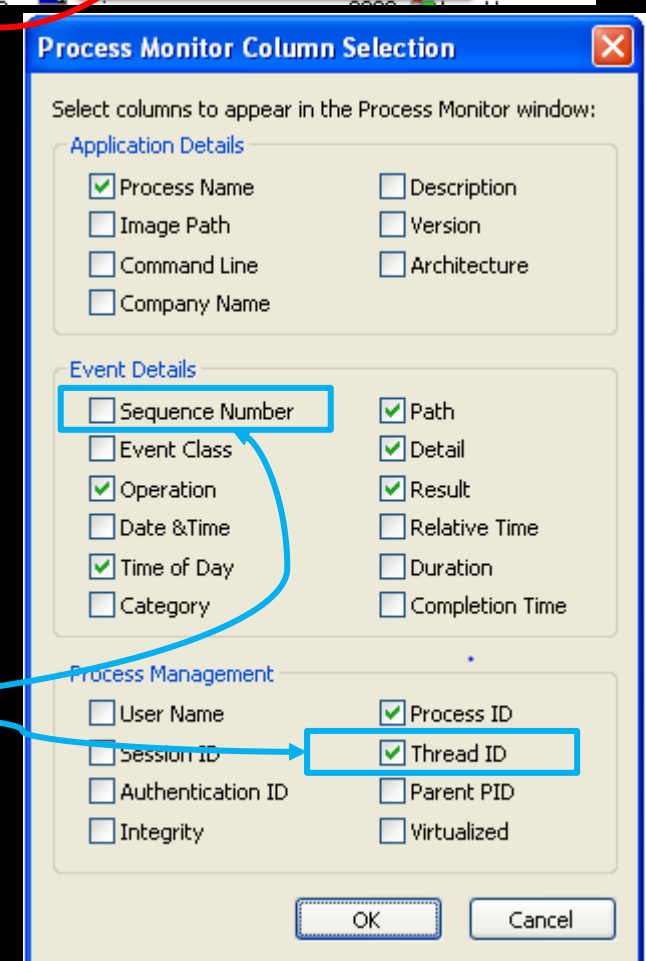
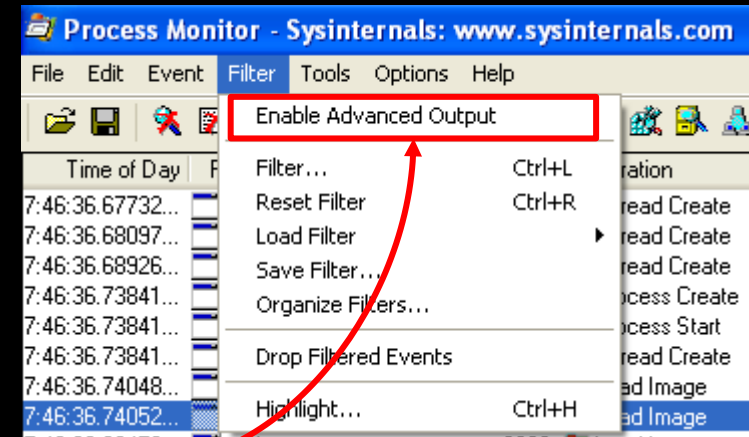
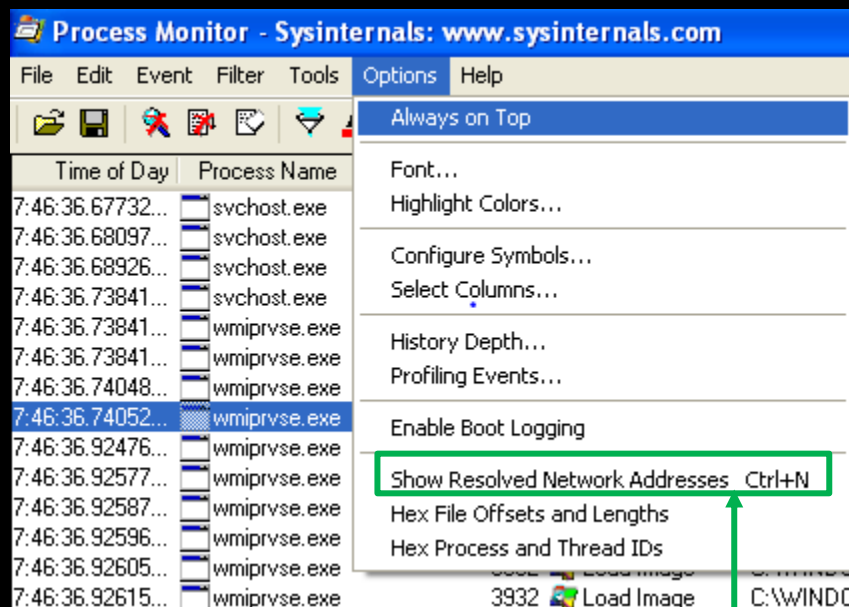
ProcDOT



- **ProcDOT Prerequisites:**
- Read the readme file and follow it.
- Installing Windump (*Copy the downloaded executable (WinDump.exe) to a place of your taste (presumption: you need to provide this location in ProcDOT's options later)*)
- Installing Graphviz



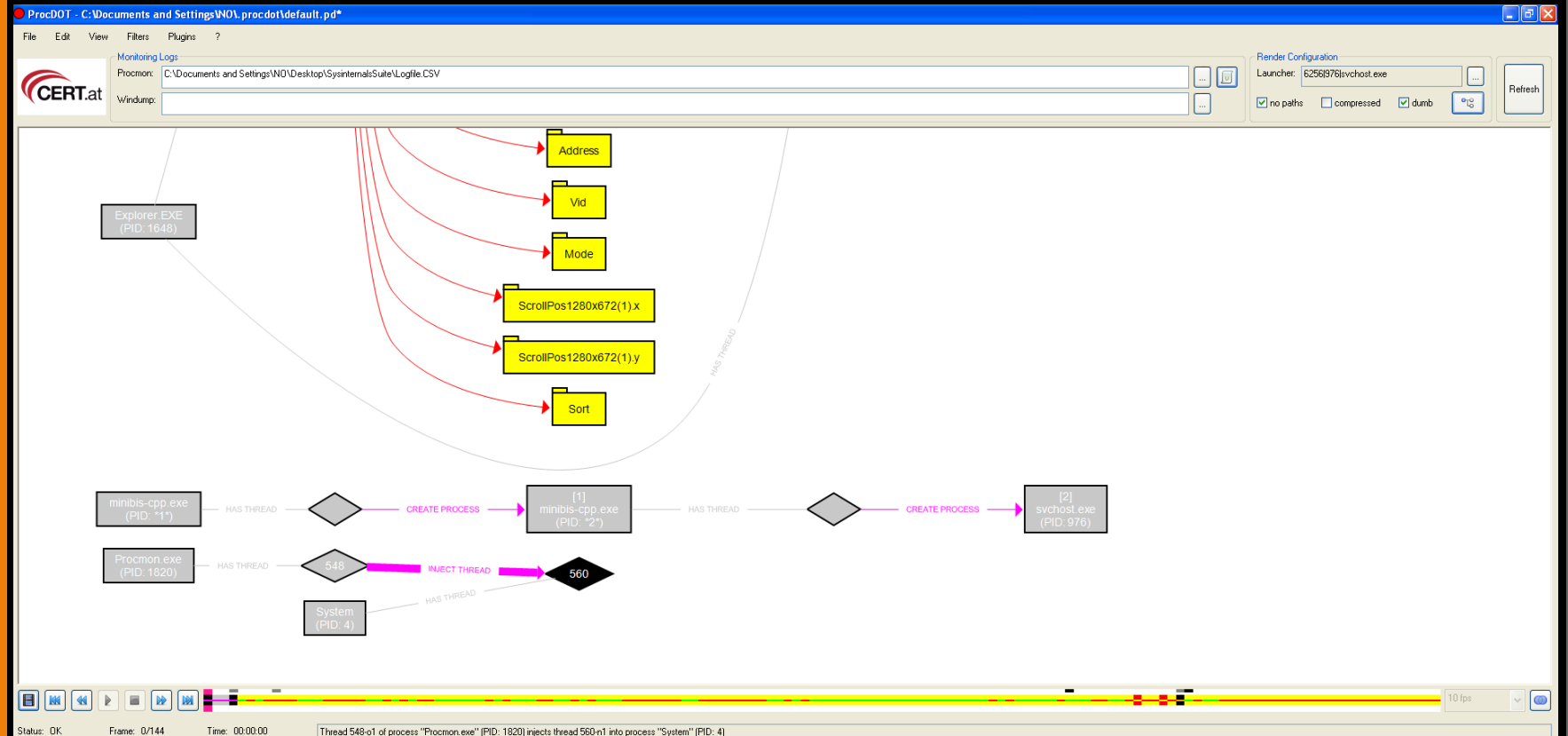
ProcDOT



- You need to adjust Procmon's configuration
Therefore, in Procmon ...
- disable (uncheck) "Show Resolved Network Addresses" (Options)
- disable (uncheck) "Enable Advanced Output" (Filter)
- adjust the displayed columns (Options > Select Columns ...)
 - to not show the "Sequence" column
 - to show the "Thread ID" column



ProcDOT



Save Procmon file and open in ProcDOT to visualize the system activities



Process Explorer

- Process explorer is an extremely powerful task manager. It can provide valuable insight into the processes currently running on a system.
- Process Explorer can be used to list active processes, DLLs loaded by a process, various process properties, and overall system information.
- It can also be used it to kill a process, log out users, and launch and validate processes.
- Process Explorer shows five columns: Process (the process name), PID (the process identifier), CPU (CPU usage), Description, and Company Name.



Process Explorer

Process Explorer - Sysinternals - www.sysinternals.com [NFSU-4DD5B68025W0]

File Options View Process End DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		3,220 K	5,104 K	900	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		2,016 K	5,060 K	420	WMI	Microsoft Corporation
svchost.exe		1,900 K	4,572 K	976	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		14,368 K	24,840 K	1072	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		676 K	2,580 K	1996	Windows Security Center No...	Microsoft Corporation
svchost.exe		1,484 K	3,792 K	1116	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,704 K	4,268 K	1212	Generic Host Process for Wi...	Microsoft Corporation
explorer.exe		16,752 K	2,492 K	1628	Windows Explorer	Microsoft Corporation
VBxTray.exe		2,116 K	4,036 K	1924	VirtualBox Guest Additions Tr...	Oracle Corporation
ctfmon.exe		1,000 K	3,524 K	1940	CTF Loader	Microsoft Corporation
procexp.exe	0.99	11,184 K	15,716 K	400	Sysinternals Process Explorer	Sysinternals - www.sysinter
spoolsv.exe		3,184 K	4,908 K	1724	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,380 K	3,860 K	204	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,260 K	2,716 K	1300	Application Layer Gateway S...	Microsoft Corporation

Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\WINDOWS\system32\advapi32.dll
comctl32.dll	Common Controls Library	Microsoft Corporation	C:\WINDOWS\system32\comctl32.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-...
ctype.nls			C:\WINDOWS\system32\ctype.nls
davclnt.dll	Web DAV Client DLL	Microsoft Corporation	C:\WINDOWS\system32\davclnt.dll
drprov.dll	Microsoft Terminal Server Network...	Microsoft Corporation	C:\WINDOWS\system32\drprov.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\WINDOWS\system32\gdi32.dll
hnetcfg.dll	Home Networking Configuration M...	Microsoft Corporation	C:\WINDOWS\system32\hnetcfg.dll
imm32.dll	Windows XP IMM32 API Client DLL	Microsoft Corporation	C:\WINDOWS\system32\imm32.dll
iphlpapi.dll	IP Helper API	Microsoft Corporation	C:\WINDOWS\system32\iphlpapi.dll

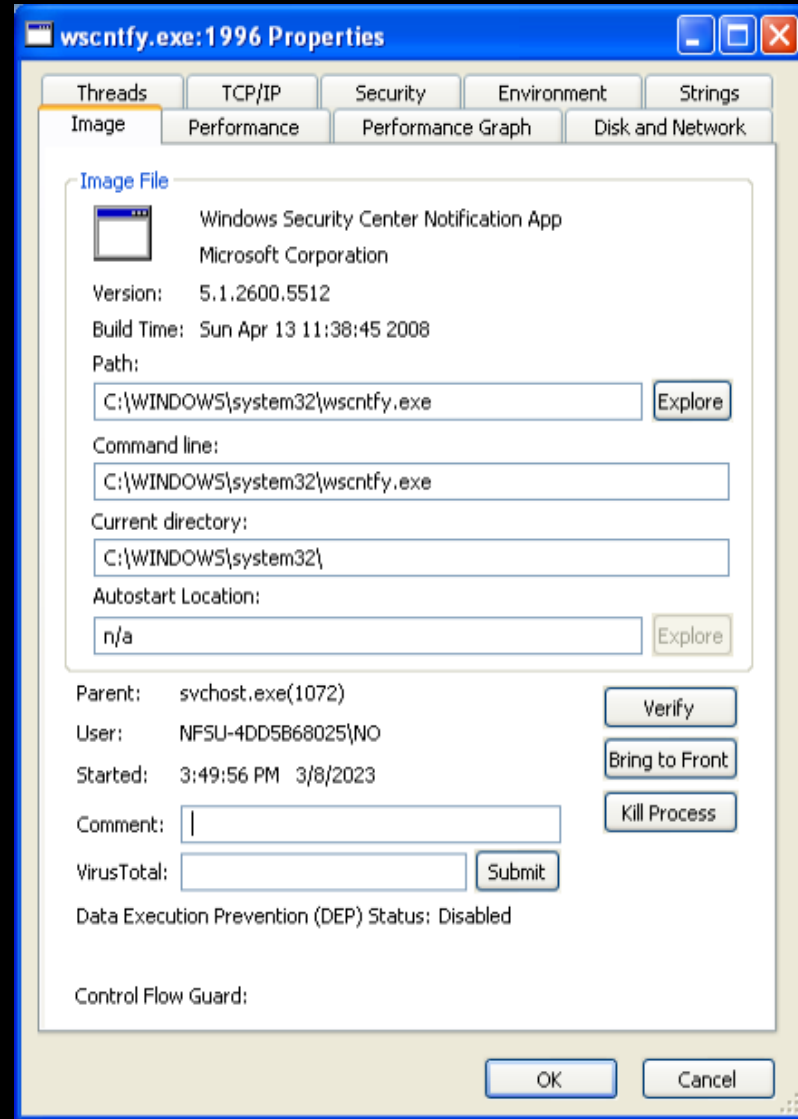
CPU Usage: 0.99% Commit Charge: 2.44% Processes: 22 Physical Usage: 8.62%

Change the lower Panel details either **DLL** display OR **Handles** window.

services are highlighted in pink, processes in blue, new processes in green, and terminated processes in red.



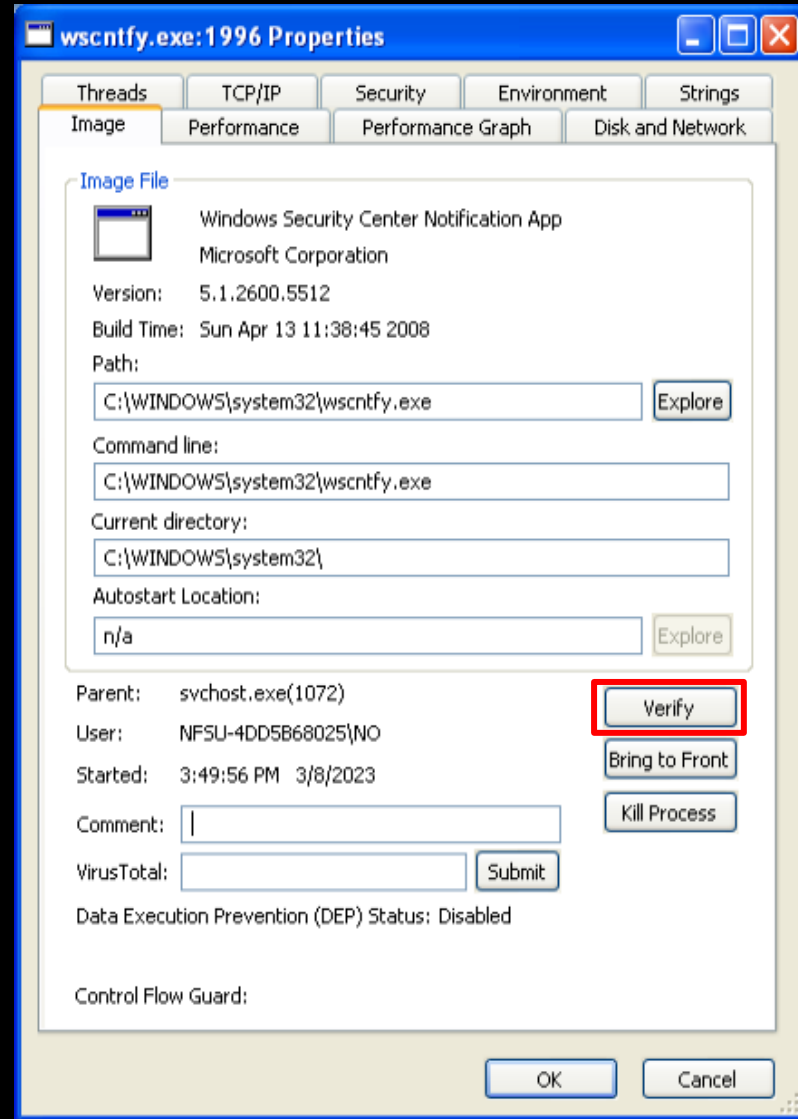
Process Explorer



- This window (Property of Process) can provide some particularly useful information about the subject malware.
- The Threads tab shows all active threads
- The TCP/IP tab displays active connections or ports on which the process is listening, and
- the Image tab (opened in the figure) shows the path on disk to the executable.



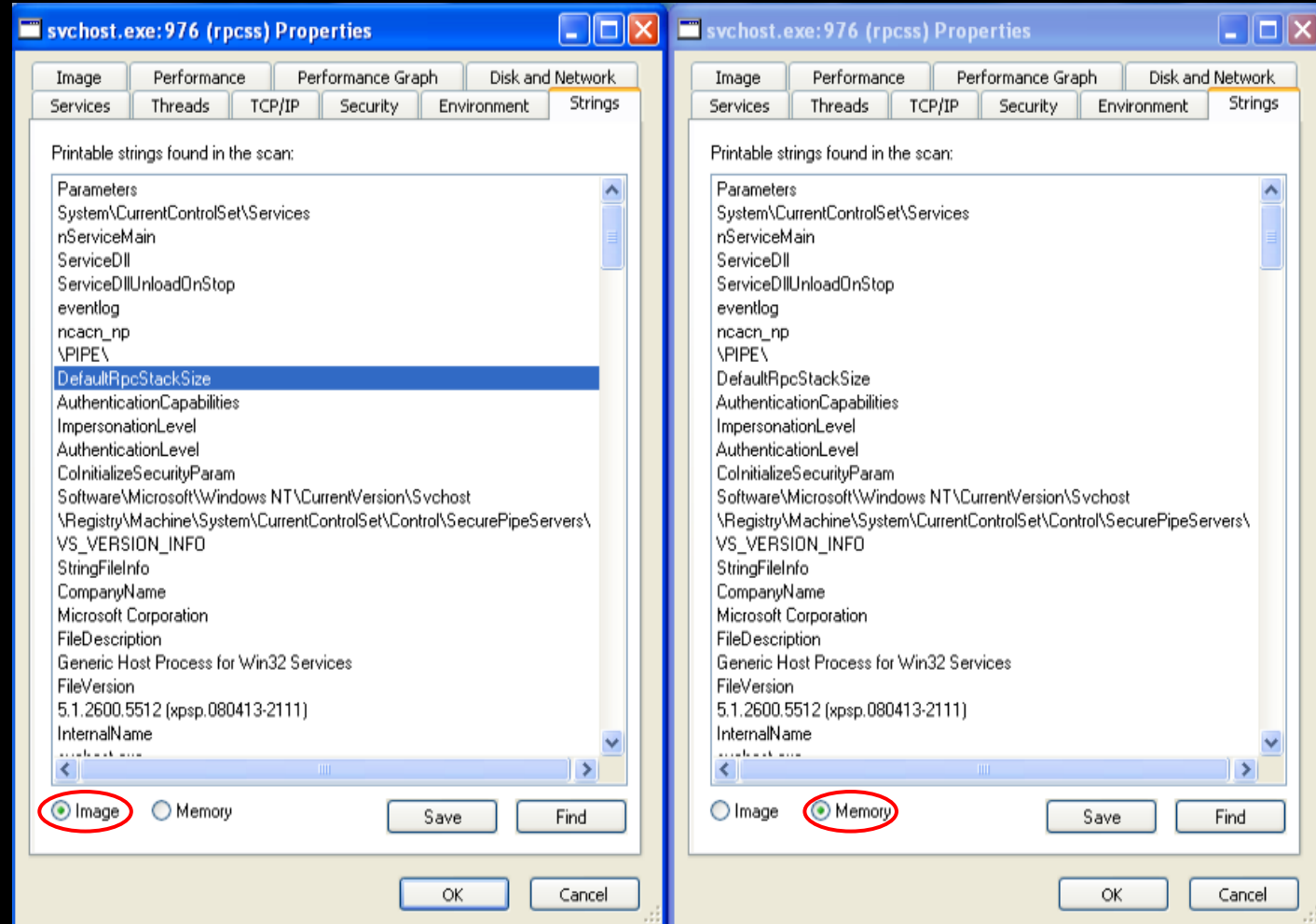
Process Explorer



- Click this button to verify that the image on disk is, in fact, the **Microsoft signed binary**. Because Microsoft uses digital signatures for most of its core executables.
- The Verify button verifies the image on disk rather than in memory, and it is useless **if an attacker uses process replacement**, which involves running a process on the system and overwriting its memory space with a malicious executable.



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 observed drastically different then likely chance of process replacement.



Analyse Malicious Document Process Explorer

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

RegShot

- Regshot is an open source registry comparison tool that allows you to take and compare two registry snapshots.
- 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.
- You will find the difference between first shot and second shot for any modification, addition or deletion in the registry.

Faking Internet

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\N0>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.56.101
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

C:\Documents and Settings\N0>
```

```
ubuntu@ubuntu: ~
docker0  Link encap:Ethernet  HWaddr 02:42:01:cb:38:02
         inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

enp0s3   Link encap:Ethernet  HWaddr 08:00:27:9a:57:0a
         inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
         inet6 addr: fe80::4396:5a4d:bbc6:ce6e/64  Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:102 errors:0 dropped:0 overruns:0 frame:0
         TX packets:580 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:15469 (15.4 KB)  TX bytes:58914 (58.9 KB)
```

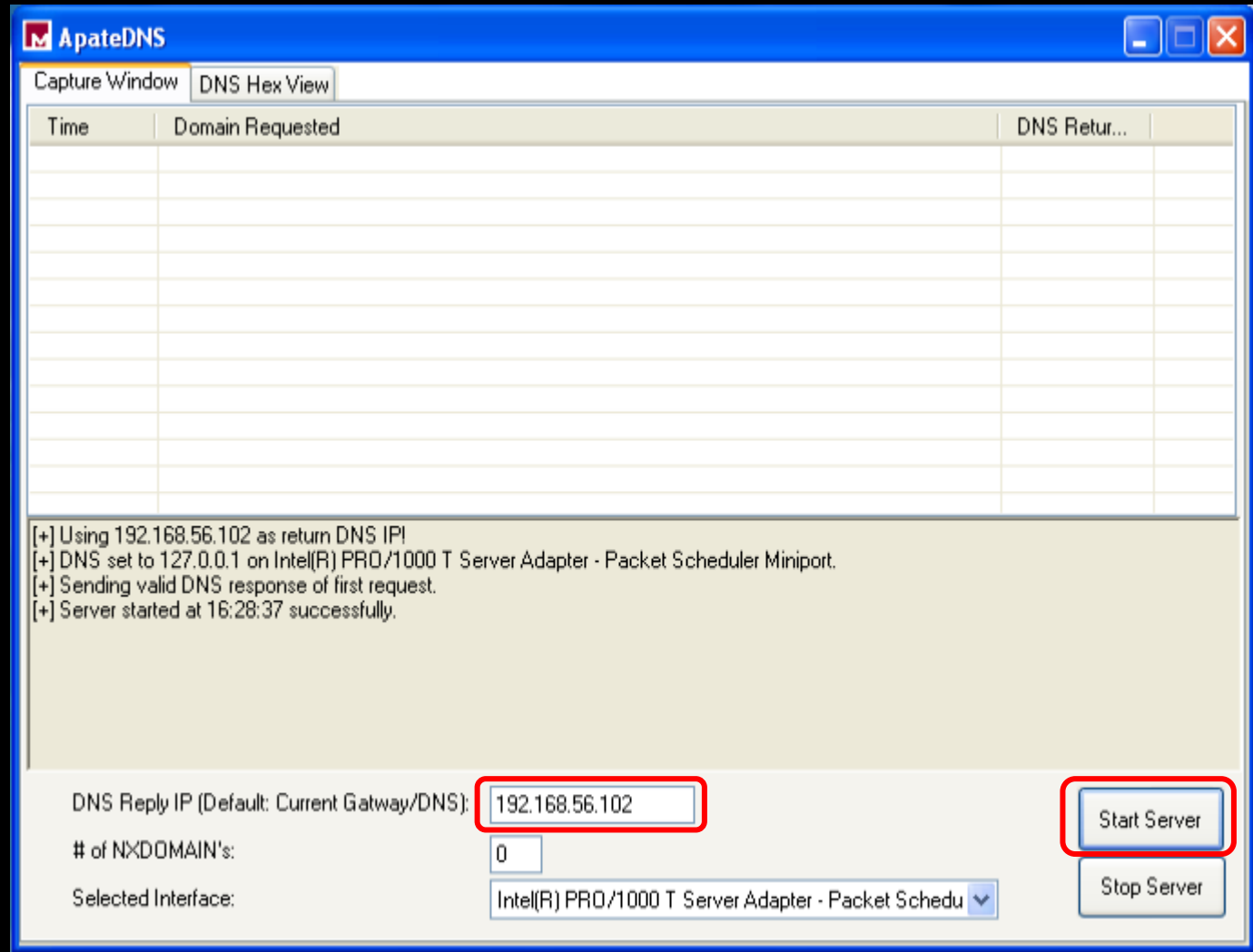
Faking Internet (inetsim)

- Install inetsim > apt-get install inetsim
- Make Changes in the inetsim.conf file:
 - #service_bind_address 10.10.10.1 Win Machine IP OR 0.0.0.0
 - #dns_default_ip 10.10.10.1 Linux Machine IP
 - #dns_default_domainname some.domain
 - #dns_static www.foo.com 10.10.10.10
- Remove # while changing the inetsim.conf file.

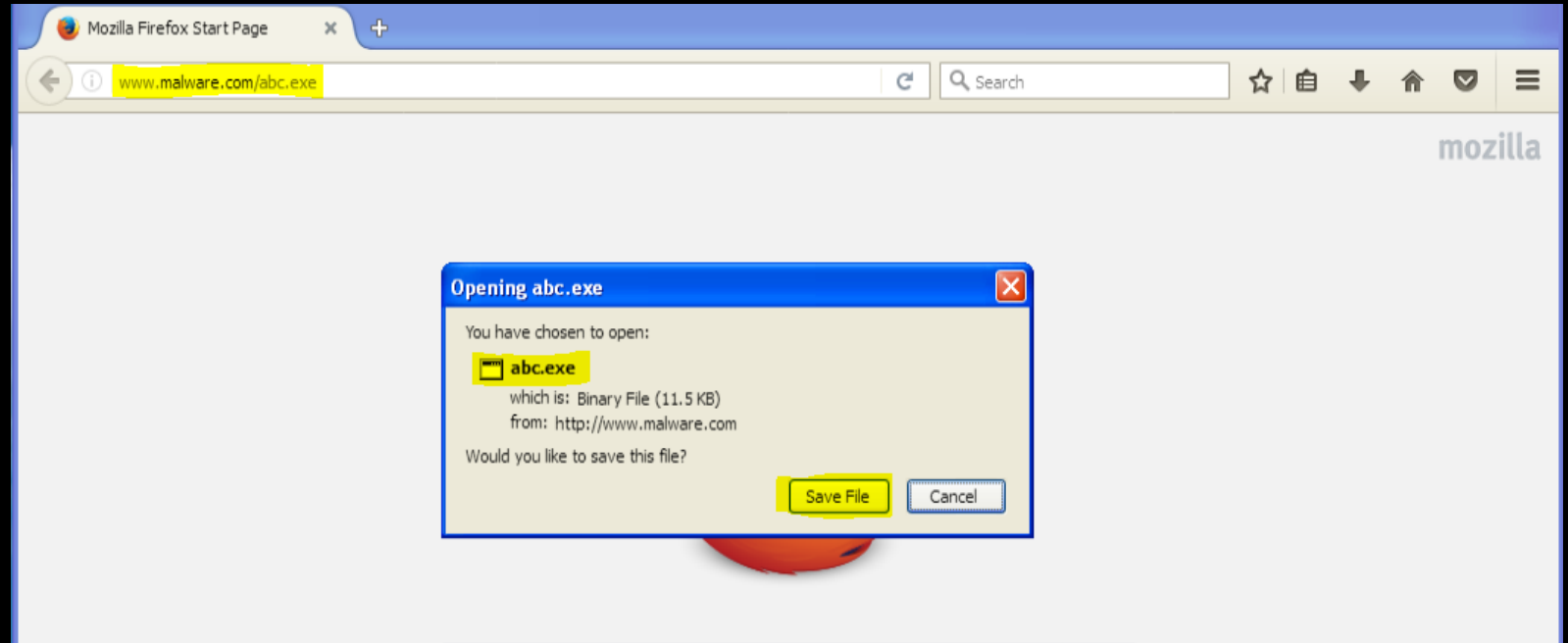
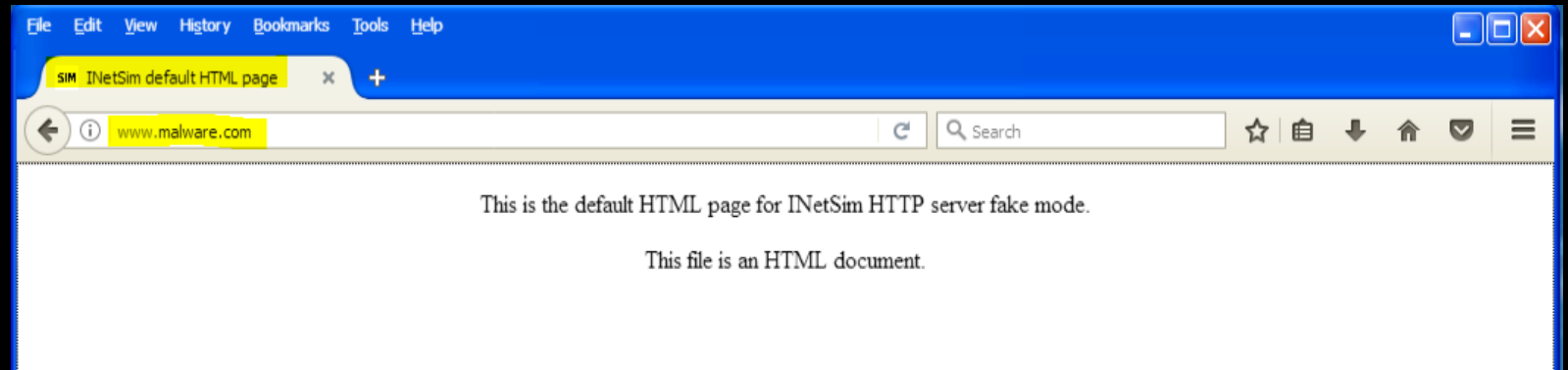
Faking Internet (inetsim)

```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ sudo inetsim  
[sudo] password for ubuntu:  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Using log directory:      /var/log/inetsim/  
Using data directory:     /var/lib/inetsim/  
Using report directory:   /var/log/inetsim/report/  
Using configuration file: /etc/inetsim/inetsim.conf  
Parsing configuration file.  
Configuration file parsed successfully.  
=== INetSim main process started (PID 5079) ===  
Session ID:      5079  
Listening on:    0.0.0.0  
Real Date/Time:  2023-03-08 16:18:24  
Fake Date/Time:  2023-03-08 16:18:24 (Delta: 0 seconds)  
Forking services...  
* dns_53_tcp_udp - started (PID 5081)  
* finger_79_tcp  - started (PID 5093)  
* syslog_514_udp - started (PID 5095)  
* ident_113_tcp  - started (PID 5094)  
* time_37_tcp    - started (PID 5096)  
* irc_6667_tcp   - started (PID 5091)  
* time_37_udp    - started (PID 5097)  
* ntp_123_udp    - started (PID 5092)  
* chargen_19_tcp - started (PID 5106)
```

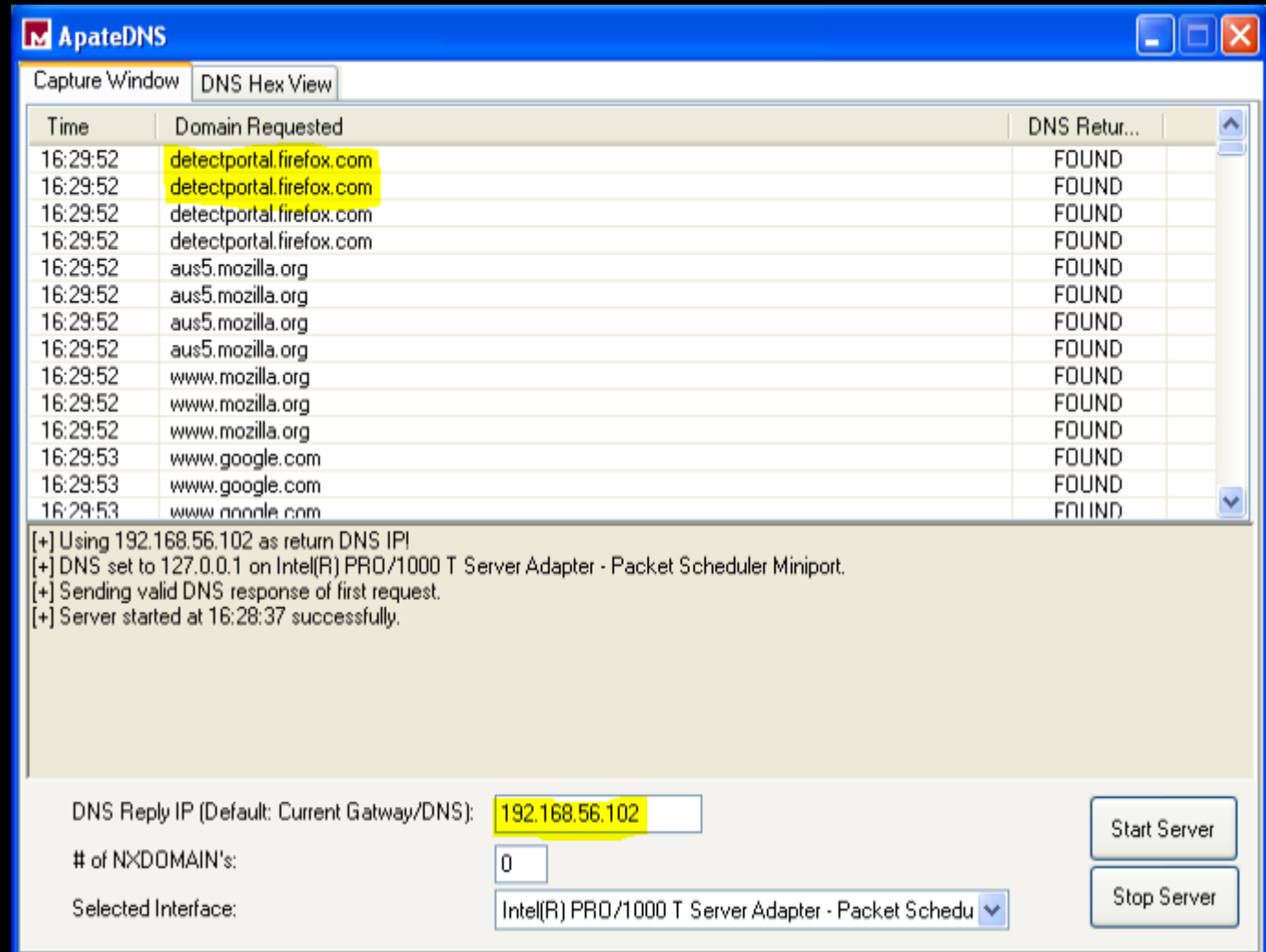

Faking Internet (ApateDNS)



Faking Internet



Faking Internet (ApateDNS)



The screenshot shows the ApateDNS application window. It has a title bar with the ApateDNS logo and standard window controls. Below the title bar are two tabs: 'Capture Window' and 'DNS Hex View'. The main area displays a table of DNS requests and responses.

Time	Domain Requested	DNS Return...
16:29:52	detectportal.firefox.com	FOUND
16:29:52	detectportal.firefox.com	FOUND
16:29:52	detectportal.firefox.com	FOUND
16:29:52	detectportal.firefox.com	FOUND
16:29:52	aus5.mozilla.org	FOUND
16:29:52	aus5.mozilla.org	FOUND
16:29:52	aus5.mozilla.org	FOUND
16:29:52	aus5.mozilla.org	FOUND
16:29:52	www.mozilla.org	FOUND
16:29:52	www.mozilla.org	FOUND
16:29:52	www.mozilla.org	FOUND
16:29:52	www.mozilla.org	FOUND
16:29:53	www.google.com	FOUND
16:29:53	www.google.com	FOUND
16:29:53	www.google.com	FOUND

Below the table, there is a log area with the following messages:

- [+] Using 192.168.56.102 as return DNS IP!
- [+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport.
- [+] Sending valid DNS response of first request.
- [+] Server started at 16:28:37 successfully.

At the bottom of the window, there are configuration options:

- DNS Reply IP (Default: Current Gateway/DNS): 192.168.56.102
- # of NXDOMAIN's: 0
- Selected Interface: Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport

There are two buttons on the right side: 'Start Server' and 'Stop Server'.




Sandbox

- “A system that allows an untrusted application to run in a highly controlled environment where the application’s permissions are restricted to an essential set of computer permissions.” – NIST
- “A sandbox is a security mechanism for running untrusted programs in a safe environment without fear of harming “real” systems.”
- *The isolation metaphor is taken from the idea of children who do not play well together, so each is given their own sandbox to play in alone.*
- Ex. Norman SandBox, GFI Sandbox, Joe Sandbox, ThreatExpert, BitBlaze, Cuckoo and Comodo Instant Malware Analysis.



Sandbox (Cuckoo Sandbox)

cuckoo  [Dashboard](#) [Recent](#) [Pending](#) [Search](#) [Submit](#) [Import](#)

Insights

Cuckoo Installation

Version	2.0.7
You are up to date.	

Usage statistics

reported	5659394
completed	0
total	5700356
running	0
pending	0


From the press:

No blogposts have been loaded (this indicates version_check has been disabled in cuckoo.conf).

[Click here for more](#)

Cuckoo

SUBMIT A FILE FOR ANALYSIS



Drag your file into the left field or click the icon to select a file.

SUBMIT URLS/HASHES


Submit URLs/hashes

[Submit](#)

System info

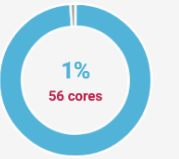
free used total

FREE DISK SPACE



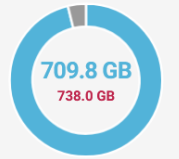
10.9 TB
90.0 TB

CPU LOAD



1%
56 cores

MEMORY USAGE



709.8 GB
738.0 GB

<https://sandbox.pikker.ee/>



Sandbox (Cuckoo Sandbox)

Dashboard

Recent

Pending

Search

Submit

Import

Summary

Static Analysis

Extracted Artifacts 1

Behavioral Analysis 8

Network Analysis

Dropped Files 2

Dropped Buffers

IntelMQ 10

Process Memory

Compare Analysis

Export Analysis

Reboot Analysis

Options

Feedback

Lock sidebar

✖ Uses suspicious command line tools or Windows utilities (1 event)

✖ Performs 579 file moves indicative of a ransomware file encryption process (50 out of 579 events)

✖ Appends a new file extension or content to 579 files indicative of a ransomware file encryption process (50 out of 579 events)

✖ File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)

✖ File has been identified by 67 AntiVirus engines on VirusTotal as malicious (50 out of 67 events)

Screenshots

Name	Response	Post-Analysis Lookup
		No hosts contacted.

IP Address	Status	Action	VT
		No hosts contacted.	

<https://sandbox.pikker.ee/>



Sandbox (Any Run)

ANY RUN
INTERACTIVE MALWARE ANALYSIS

[+ New analysis](#)
[Reports](#)
[Teamwork](#)
[History](#)
[Threat Intelligence](#)
[Windows 10 64 bit](#)
[Windows 10 64 bit](#)
[Profile](#)
[Pricing](#)
[Contacts](#)
[FAQ](#)

Start your analysis

Interact with the OS directly from the browser window, and immediately see the feedback from your actions.

Deep interactive investigation in full environment

Submit File / Email

Detonate an object to observe its malicious activity

Submit URL

Investigate malicious and phishing activity and inspect downloaded files

Check Suspicious Links

Open any URL to verify its content fast and easily

Safebrowsing

free beta

Explore Links Faster!

Speed up routine link checks and get real-time threat alerts.

[Okay](#)

<https://any.run/>



Sandbox (Any Run)

The screenshot displays the AnyRun web interface, which provides a remote Windows 10 desktop environment for analysis. The desktop shows various applications like Microsoft Edge, Recycle Bin, and several PDF files. A taskbar at the bottom includes a search bar and system icons. On the right side, a 'Malicious activity' panel is active, showing a list of processes. The top of this panel indicates a URL: <https://idoxaby.sufydely.com/quicksand-regular.woff2>, which is identified as 'phishing' and 'github'. Below this, there are tabs for 'Text report', 'Graph', 'ATT&CK', 'Summary', and 'Export'. A 'Processes' table lists running applications with their PIDs, process names, and network activity.

PID	Process name	Content
1064	msedge.exe	"https://idoxaby.sufydely.com/quicksand-regular.woff2"
6160	msedge.exe	-type=crashpad-handler *-user-data-dir=C:\Users\admin\AppData\Local\Micros...
6364	msedge.exe	-type=gpu-process -no-appcompat-clear -gpu-preferences=WAAAAAAAAADgA...
6372	msedge.exe	-type=utility -utility-sub-type=network.mojom.NetworkService -lang=en-US -ser...
6392	msedge.exe	-type=utility -utility-sub-type=storage.mojom.StorageService -lang=en-US -servi...
6612	msedge.exe	-type=renderer -no-appcompat-clear -lang=en-US -js-flags=-ms-user-locale=-d...
6636	msedge.exe	-type=renderer -no-appcompat-clear -lang=en-US -js-flags=-ms-user-locale=-d...
6716	msedge.exe	-type=renderer -extension-process -renderer-sub-type=extension -no-appcomp...
6724	msedge.exe	-type=utility -utility-sub-type=data_decoder.mojom.DataDecoderService -lang=e...

At the bottom of the interface, a 'FREE trial' banner is visible, and a 'View more' button is present.

<https://any.run/>



Sandbox



Triage by Recorded Future

<https://tria.ge/>



Hybrid Analysis

<https://www.hybrid-analysis.com/>



Joe Sandbox

<https://www.joesandbox.com/>

Sandbox Drawbacks

- The 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 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.
- It may not record all events, because neither you nor the sandbox may wait long enough. Ex. if the malware is **set to sleep** for a day before it performs malicious activity, you may miss that event.

Sandbox Drawbacks

- Malware often detects when it is running in a virtual machine, and if a virtual machine is detected, the malware might stop running or behave differently.
- Some malware requires the presence of certain registry keys or files on the system that might not be found in the sandbox. These might be required to contain legitimate data, such as commands or encryption keys.
- 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.
- The sandbox environment OS may not be correct for the malware.
- A sandbox cannot tell you what the malware does.

References

- Practical Malware Analysis by Michael Sikorski