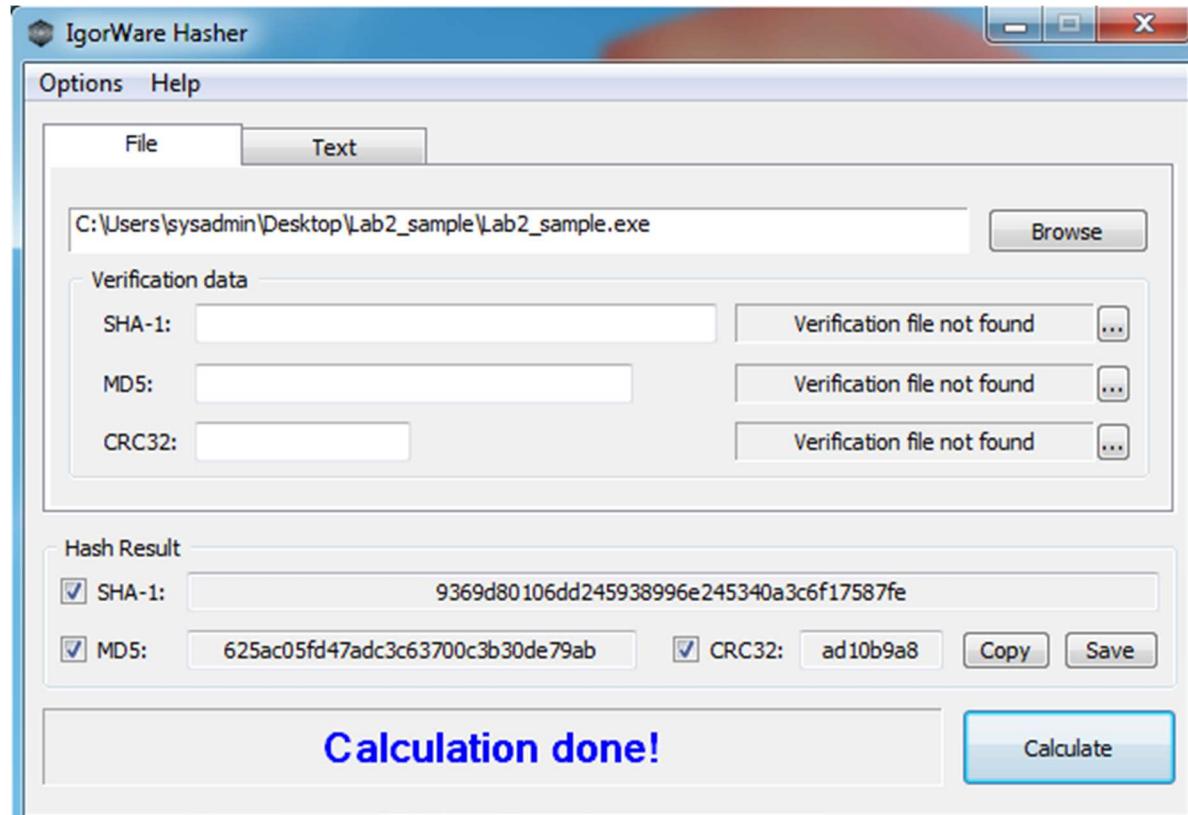


## Lab 2 – Dynamic Analysis

Gunnar Yonker

### Static Analysis – Preliminary Information

#### IgorWare Hasher



SHA-1: `9369d80106dd245938996e245340a3c6f17587fe`

#### VirusTotal

The screenshot shows the VirusTotal analysis page for the file `0fa1498340ca6c562cfa389ad3e9339544c72fd128d7ba08579a69aa3b126 test.exe`. The page displays a summary of 56 vendor detections, with a community score of 56/69. Below this, detailed detection tables for Alibaba, Anti-AVL, Avast, Avira, BitDefenderTheta, CrowdStrike Falcon, Cynet, DrWeb, Emsisoft, ESET-NOD32, and GData are shown, each listing threat labels, threat categories, family labels, and confidence levels.

## Lab 2 – Dynamic Analysis

Gunnar Yonker

### strings Utility

```
C:\Windows\System32\WindowsPowerShellV1.0\powershell.exe
GetModuleHandleA
GetWindowsDirectoryA
MoveFileA
GetTempPathA
KERNEL32.dll
ADVAPI32.dll
LookupPrivilegeValueA
OpenProcessToken
ADVAPI32.dll
_set_ntapi
MSVCRT.dll
_exit
_XcptFilter
exit
_p_initenv
_getmainargs
_inittern
_setusermathererr
_adjust_fdiv
_p_commode
_p_fnode
_set_app_type
_except_handler3
_controfip
_strincmp
objlogon.exe
!notreal!
SeDebugPrivilege
fc.exe
!System32\wupdngmgr.exe
zszs
BIN
H101
EndProcessModules
psapi.dll
GetModuleBaseNameA
psapi.dll
EndProcesses
psapi.dll
!System32\wupdngmgr.exe
zszs
!winup.exe
zszs
BIN
!This program cannot be run in DOS mode.
Rich
!text
!rdata
!data
!bdata
!BDA
!QDQE
!ZL
!D
!E
!WUW
!ZB
!E
!GetWindowsDirectoryA
WinExec
GetTempPathA
KERNEL32.dll
ADVAPI32.dll
urlmon.dll
_snprintf
MSVCRT.dll
_exit
_XcptFilter
exit
_p_initenv
_getmainargs
_inittern
_setusermathererr
_adjust_fdiv
_p_commode
_p_fnode
_set_app_type
_except_handler3
_controfip
!winup.exe
zszs
!System32\wupdngrd.exe
zszs
http://www.practicalwareanalysis.com/updater.exe
PS C:\Users\sysadmin\Desktop\Lab2_Sample> S_m
```

## Lab 2 – Dynamic Analysis

Gunnar Yonker

### MiTec EXE Explorer

MiTec EXE Explorer - [C:\Users\sysadmin\Desktop\Lab2\_sample\Lab2\_sample.exe]

File  
Free to use for private, educational and non-commercial purposes

C:\Users\sysadmin\Desktop\Lab2\_sample\Lab2\_sample.exe  
Portable Executable - PE32  
Intel 32-bit - Windows GUI

VirusTotal...

Headers Sections Directories Imports Resources Strings Hex View

Property	Value
Signature	0x00004550 (Portable Executable)
Machine	Intel 32-bit
Number of sections	4
Timestamp	8/30/2019 5:26:59 PM
Pointer to symbol table	0x00000000
Number of symbols	0
Size of optional header	224
Characteristics	0x10F
Relocations stripped	YES
Debugging information stripped	NO
Application can handle addresses larger than 2 GB	NO
Image can handle a high entropy 64-bit virtual address sp...	NO
Code Integrity checks are enforced	NO
Data Execution Prevention	NO
Address Space Layout Randomization	NO
Control Flow Guard	NO
Safe Structured Exception Handling	YES
WDM Driver	NO
Operating system	Windows NT 4
Size	36.00 KB (36864 B)
Entry point section	.text
File offset	0x000015CF
Created	3/27/2023 7:15:13 PM
Modified	7/5/2011 8:16:15 PM
Accessed	3/27/2023 7:15:13 PM
Entropy	1.177
Correct Checksum	0x0000D3EE
Compiler	Microsoft Visual Studio 6.0 (RTM, SP1 or SP2)

Checksums DOS File Optional Rich

Version Info

Search tool

MiTec EXE Explorer - [C:\Users\sysadmin\Desktop\Lab2\_sample\Lab2\_sample.exe]

File  
Free to use for private, educational and non-commercial purposes

C:\Users\sysadmin\Desktop\Lab2\_sample\Lab2\_sample.exe  
Portable Executable - PE32  
Intel 32-bit - Windows GUI

VirusTotal...

Headers Sections Directories Imports Resources Strings Hex View

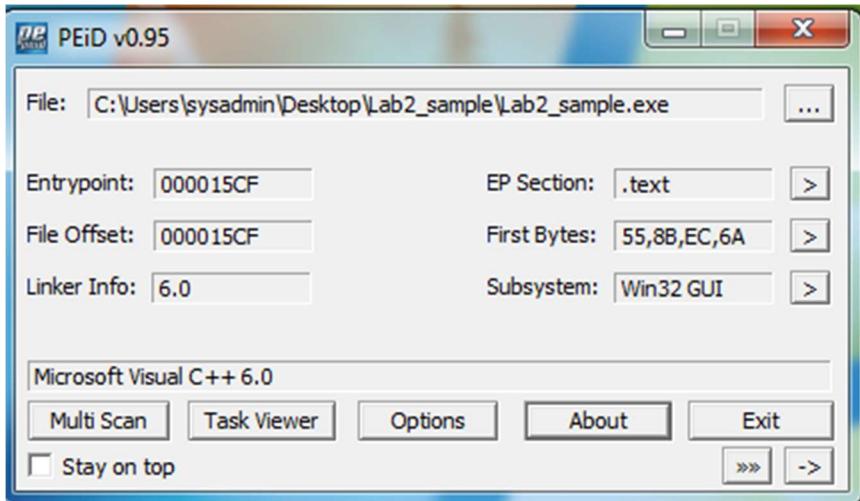
Name	Ordinal	Address	Delayed
ADVAPI32.dll (3)			
KERNEL32.dll (16)			
MSVCRT.dll (15)			

## Lab 2 – Dynamic Analysis

Gunnar Yonker

MiTeC EXE Explorer - [C:\Users\sysadmin\Desktop\Lab2_sample\Lab2_sample.exe]											
Free to use for private, educational and non-commercial purposes											
C:\Users\sysadmin\Desktop\Lab2_sample\Lab2_sample.exe											
Headers	Sections	Directories	Imports	Resources	Strings	Hex View					
Name	Virtual Address	Virtual Size	Raw Data Offset	Raw Data Size	Flags		Entropy	Executable	Readable	Writable	Shareable
.text	0x00001000	1824	0x00001000	4096	0x60000020		3.123	YES	YES		YES
.rdata	0x00002000	978	0x00002000	4096	0x40000040		1.591	YES	YES		YES
.data	0x00003000	332	0x00003000	4096	0xC0000040		0.508	YES	YES	YES	YES
.rsrc	0x00004000	16480	0x00004000	20480	0x40000040		0.713	YES	YES		YES

## PEiD



## Lab 2 – Dynamic Analysis

Gunnar Yonker

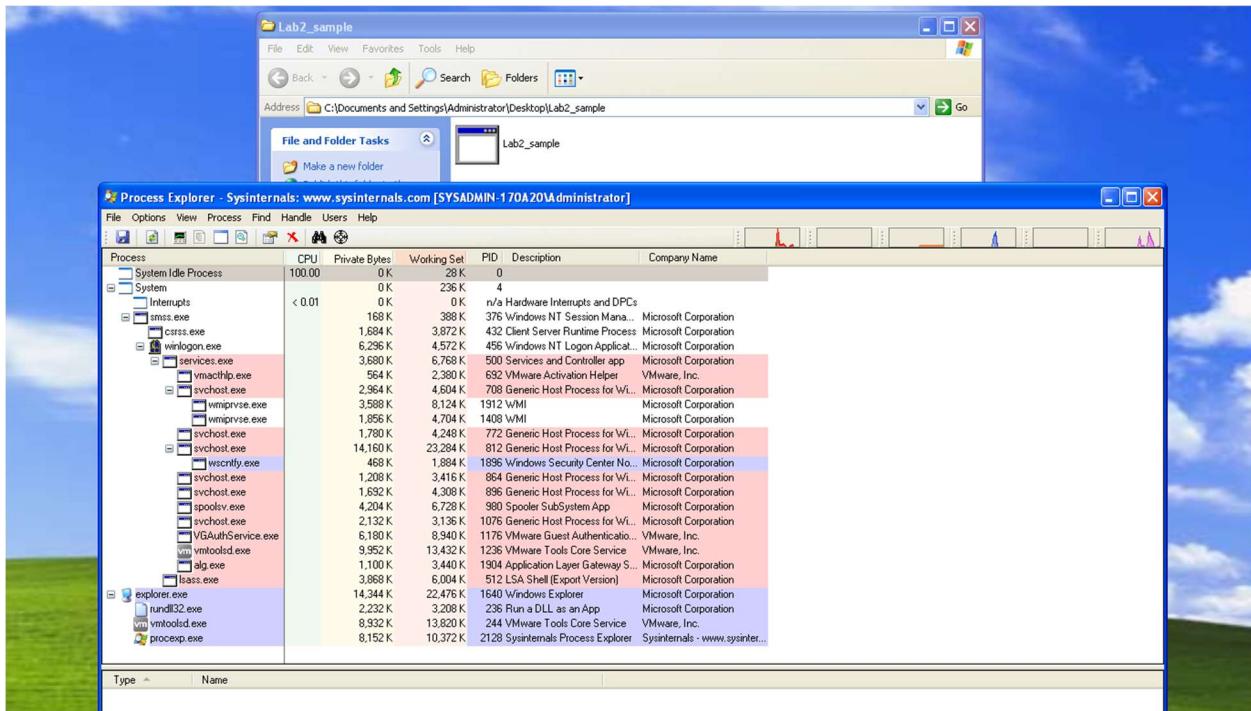
### Lab 2 Dynamic Analysis Tools:

#### Tool: Process Explorer

**Purpose of Tool:** The Process Explorer tool allows the users to view detailed information about running processes, including the ability to see which processes have loaded specific DLLs. It also gives the user information on which processes have opened certain files or registry keys and also gives the user the ability to terminate processes. It is a more powerful version of the Windows task manager giving the user information such as DLLs loaded, child processes spawned, TCP/IP ports used by the process, resource consumption and signature verification.

#### Relevant information from tool:

Before malware:



## Lab 2 – Dynamic Analysis

Gunnar Yonker

After malware:

The screenshot shows a Windows desktop environment. In the foreground, there is a Microsoft Internet Explorer window with the URL <http://windowsupdate.microsoft.com>. The page displays an error message: "The page cannot be displayed" with the subtext: "The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings." A red box highlights this error message. Below the browser, a Process Explorer window titled "Process Explorer - Sysinternals: www.sysinternals.com [SYSADMIN-170A20\Administrator]" lists numerous processes. Several processes are highlighted in red, including "svchost.exe", "services.exe", "vmservice.exe", "vmpvservice.exe", "IEXPLORE.EXE", "svchost.exe", "explorer.exe", and "process.exe". The "IEXPLORE.EXE" process is shown with a PID of 2608 and a description of "2608 Internet Explorer". The "explorer.exe" process is also highlighted. The Process Explorer interface includes columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. At the bottom of the Process Explorer window, it says "CPU Usage: 0.77%", "Commit Charge: 4.70%", "Processes: 26", and "Physical Usage: 16.30%".

**IEXPLORE.EXE:2608 Properties**

**Threads** **TCP/IP** **Security** **Environment** **Disk and Network** **Strings**

Printable strings found in the scan:

- ADVAPI32.dll
- IstrlenW
- MultiByteToWideChar
- CreateEventA
- GetCurrentThreadId
- IstrcatA
- IstrlencA
- IstrcpyA
- GetModuleFileNameA
- FreeLibrary
- GetProcAddress
- LoadLibraryA
- GetVersionExA
- UnmapViewOfFile
- CloseHandle
- ReleaseMutex
- SetEvent
- WaitForSingleObject
- CreateProcessA
- IstrcpyA
- GetCurrentProcessId
- DuplicateHandle

Image  Memory  Threads  TCP/IP  Security  Environment  Disk and Network  Strings

Save Find OK Cancel

**IEXPLORE.EXE:2608 Properties**

**Image** **Threads** **TCP/IP** **Security** **Environment** **Disk and Network** **Strings**

**Image File**

Internet Explorer  
Microsoft Corporation  
Version: 6.0.2900.5512  
Build Time: Sun Apr 13 13:34:13 2008  
Path: C:\Program Files\Internet Explorer\IEXPLORE.EXE

Command line:  
"C:\Program Files\Internet Explorer\iexplore.exe" -Embedding

Current directory:  
C:\Documents and Settings\Administrator\Desktop

Autostart Location:  
n/a

Parent: svchost.exe(708)   
User: SYSADMIN-170A20\Administrator   
Started: 10:04:04 PM 3/27/2023   
Comment:   
VirusTotal:

Data Execution Prevention (DEP) Status:

## Lab 2 – Dynamic Analysis

Gunnar Yonker

Name	Description	Company Name	Path
soribls.nls			C:\WINDOWS\system32\soribls.nls
sxs.dll	Fusion 2.5	Microsoft Corporation	C:\WINDOWS\system32\sxs.dll
tap32.dll	Microsoft® Windows(TM) Telepho...	Microsoft Corporation	C:\WINDOWS\system32\tap32.dll
unicode.nls			C:\WINDOWS\system32\unicode.nls
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	C:\WINDOWS\system32\urlmon.dll
use32.dll	Windows XP USER API Client DLL	Microsoft Corporation	C:\WINDOWS\system32\use32.dll
userenv.dll	Userenv	Microsoft Corporation	C:\WINDOWS\system32\userenv.dll
uxtheme.dll	Microsoft LxTheme Library	Microsoft Corporation	C:\WINDOWS\system32\uxtheme.dll
version.dll	Version Checking and File Installati...	Microsoft Corporation	C:\WINDOWS\system32\version.dll
wininet.dll	Internet Extensions for Win32	Microsoft Corporation	C:\WINDOWS\system32\wininet.dll
wmmm.dll	MCI API DLL	Microsoft Corporation	C:\WINDOWS\system32\wmmm.dll
wintrust.dll	Microsoft Trust Verification APIs	Microsoft Corporation	C:\WINDOWS\system32\wintrust.dll
wldap32.dll	Win32 LDAP API DLL	Microsoft Corporation	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Windows Socket 2.0 Helper for Wi...	Microsoft Corporation	C:\WINDOWS\system32\ws2help.dll
wshtcpip.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshtcpip.dll
wssock32.dll	Windows Socket 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\wssock32.dll
xpsp2res.dll	Service Pack 2 Messages	Microsoft Corporation	C:\WINDOWS\system32\xpsp2res.dll

CPU Usage: 3.79% | Commit Charge: 4.48% | Processes: 25 | Physical Usage: 16.03%

**Insights gained:** When the malware is run, Process Manager briefly shows the sample malware running before it closes and the new program that is running is a IEXPLORE.EXE program under svchost.exe. When this program is looked into further some of the DLL libraries that are imported deal with the Windows Socket for connection. The mshtml.dll, shdocvw.dll, and wininet.dll references are commonly used with Internet Explorer. The strings found in the memory of the file show that the malware is creating a new process for browsing with BrowseNewProcess and this means it may be attempting to execute code within this new process. The references to KERNEL32.dll, NTDLL.DLL, USER32.dll, SHLWAPI.dll can also indicate that the malware might be attempting to interact with operating system components. The strings related to error handling and debugging also suggest that the malware is attempting to avoid detection and analysis. There are also references to cryptography packages which means the malware may be trying to do operations that require encryption. In strings, CreateWindowExA and CreateMenu both suggest that the malware may be trying to display a fake or misleading user interface to trick the user into interacting with it.

## Lab 2 – Dynamic Analysis

Gunnar Yonker

### Tool: Regshot

**Purpose of Tool:** Regshot is a tool that can take snapshots of the system registry and then they can be used to compare the system registry before and after malware execution. This is extremely useful to be able to identify any registry entries that have been modified by the malware execution.

### Relevant information from tool:

The screenshot shows the Regshot interface comparing two registry snapshots. The left pane displays the 'Changes' section, listing 230 modifications. The right pane shows the 'Compare logs save as' options and the output path 'C:\DOCUMENTS\ADMIN\11'. The bottom pane lists deleted values, added keys, modified values, and total changes (230).

**Changes:**

- Keys added: 17
- Values deleted: 194

**Values modified: 7**

**Total changes: 230**

**Output Path:** C:\DOCUMENTS\ADMIN\11

**Insights gained:** By using this tool I was able to see that the malware made a lot of changes to the registry, 230 in total. There were 17 keys added and 7 values modified that were related to system settings such as Download Manager, Internet Explorer extensions, Explorer menu order, and Internet Connection Wizard. There were modifications made to the UserAssist registry which could be an indication that the malware is trying to monitor the user's activity on the system. There were 194 values deleted from the registry that was removing the language values for system functions such as My Computer and My Documents. It also was deleting values related to file operations such as renaming,

## Lab 2 – Dynamic Analysis

Gunnar Yonker

moving, and copying file. There were also modifications to values associated with web publishing. With all of the deletions and modifications by the malware I suspect that it was attempting to disrupt or disable system functions to make the user believe that they needed to update their windows system by then opening the windowsupdate.microsoft.com/ webpage in the Internet Explorer window.

## Lab 2 – Dynamic Analysis

Gunnar Yonker

### Tool: Process Monitor

**Purpose of Tool:** The Process Monitor tool is used to monitor registry, filesystem, network, process and thread activities. With this tool network activity may not be reliably logged across the different versions of windows. It will monitor all systems calls when it is run and the event logs consume memory leading to the potential of exhausting all system RAM quickly. This tool can capture detailed information about these events, the timestamp of the event, and any relevant details about the event.

#### Relevant information from tool:

The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations like Open, Save, Print, and various monitoring and filtering options. The main pane displays a table of event logs. The columns are: Time..., Process Name, PID, Operation, Path, Result, and Detail. The table lists numerous events for the process "iexplore.exe" with PID 2980. The operations include Process Start, Thread Create, QueryNameInfo, Load Image, CreateFile, RegOpenKey, CreateFile, FileSystemControl, QueryOpen, Load Image, RegOpenKey, RegQueryValue, RegCloseKey, Load Image, RegOpenKey, RegOpenKey, and RegQueryValue. The paths are mostly within the Windows system directory (C:\Windows\system32). The results are mostly "SUCCESS", with some "NAME NOT FOUND" or "Desired Access: R...". The details column provides specific information like Parent PID, Thread ID, and image base addresses.

Time...	Process Name	PID	Operation	Path	Result	Detail
9:50:2...	iexplore.exe	2980	Process Start		SUCCESS	Parent PID: 708, C...
9:50:2...	iexplore.exe	2980	Thread Create		SUCCESS	Thread ID: 2996
9:50:2...	iexplore.exe	2980	QueryNameInfo	C:\Program Files\Internet Explorer\EXP... SUCCESS	Name: \Program Fil...	
9:50:2...	iexplore.exe	2980	Load Image	C:\Program Files\Internet Explorer\EXP... SUCCESS	Image Base: 0x400...	
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
9:50:2...	iexplore.exe	2980	QueryNameInfo	C:\Program Files\Internet Explorer\EXP... SUCCESS	Name: \Program Fil...	
9:50:2...	iexplore.exe	2980	CreateFile	C:\WINDOWS\Prefetch\IEXPLORE.EXE..NAME NOT FOUND	Desired Access: G...	
9:50:2...	iexplore.exe	2980	RegOpenKey	HKEY\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
9:50:2...	iexplore.exe	2980	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: E...
9:50:2...	iexplore.exe	2980	FileSystemControl	C:\WINDOWS\system32	SUCCESS	Control: FSCTL_IS...
9:50:2...	iexplore.exe	2980	QueryOpen	C:\Program Files\Internet Explorer\expl... NAME NOT FOUND		
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
9:50:2...	iexplore.exe	2980	RegOpenKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Desired Access: R...
9:50:2...	iexplore.exe	2980	RegQueryValue	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	Type: REG_DWORD
9:50:2...	iexplore.exe	2980	RegCloseKey	HKEY\SYSTEM\CurrentControlSet\Contro...	SUCCESS	
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\msvcr7.dll	SUCCESS	Image Base: 0x77c...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\gd32.dll	SUCCESS	Image Base: 0x7f1...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x7f1...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS	Image Base: 0x77e...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	Image Base: 0x7e2...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\crypt32.dll	SUCCESS	Image Base: 0x77a...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\msasn1.dll	SUCCESS	Image Base: 0x77b...
9:50:2...	iexplore.exe	2980	Load Image	C:\WINDOWS\system32\cryptui.dll	SUCCESS	Image Base: 0x754...
9:50:2...	iexplore.exe	2980	RegOpenKey	HKEY\Software\Policies\Microsoft\Con...	NAME NOT FOUND	Desired Access: R...
9:50:2...	iexplore.exe	2980	RegOpenKey	HKEY\Control Panel\Desktop	SUCCESS	Desired Access: R...
9:50:2...	iexplore.exe	2980	RegQueryValue	HKEY\Control Panel\Desktop\Icon\MultiII	NAMF NOT FOUND Length: 256	

## Lab 2 – Dynamic Analysis

Gunnar Yonker

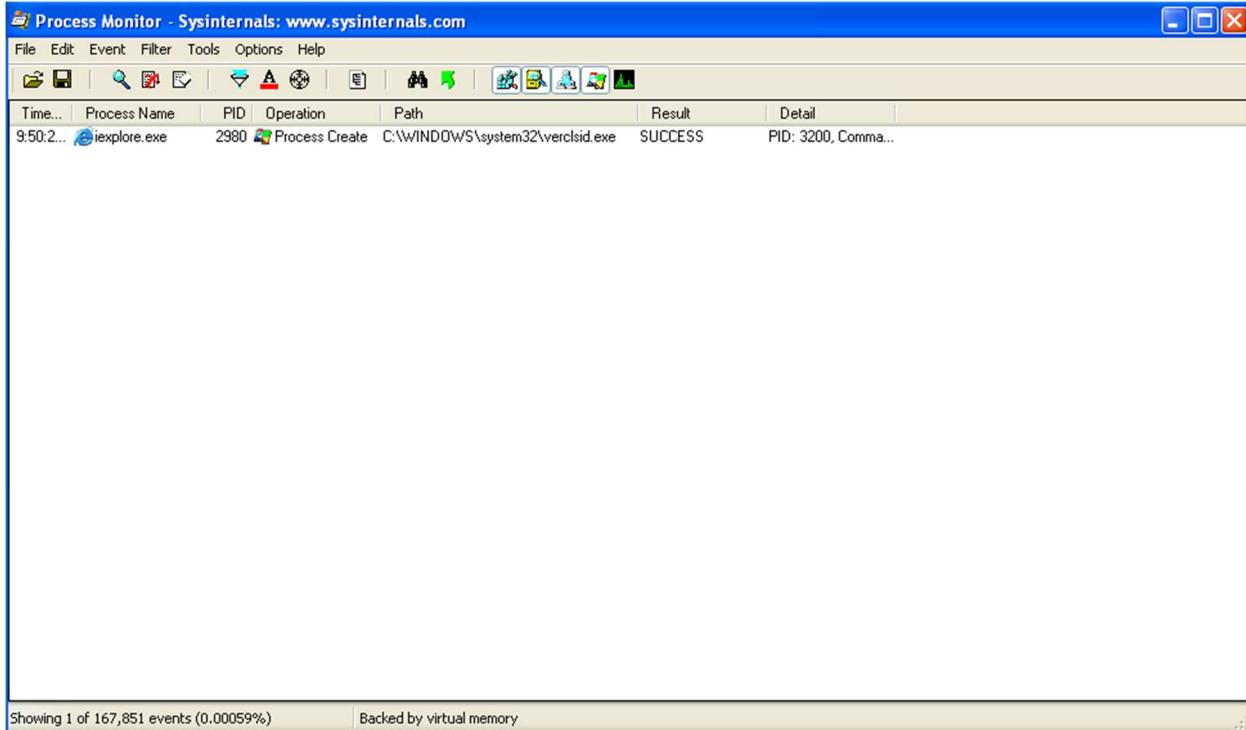
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time... Process Name PID Operation Path Result Detail

9:50:2... iexplore.exe 2980 Process Create C:\WINDOWS\system32\verclsid.exe SUCCESS PID: 3200, Comma...

Show 1 of 167,851 events (0.00059%) Backed by virtual memory



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time... Process Name PID Operation Path Result Detail

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\S... SUCCESS Type: REG\_BINA...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Internet Expl... SUCCESS Type: REG\_DWO...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_DWO...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_DWO...

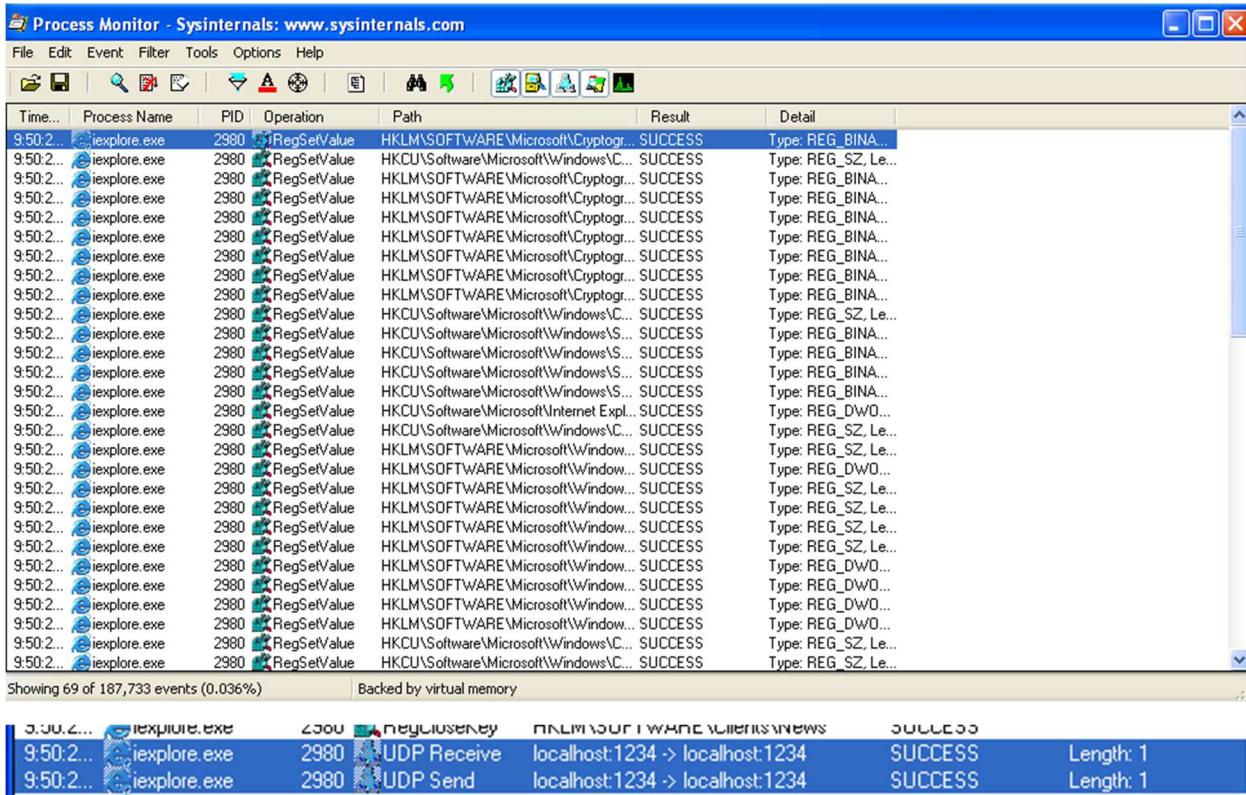
9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_DWO...

9:50:2... iexplore.exe 2980 RegSetValue HKLM\SOFTWARE\Microsoft\Window... SUCCESS Type: REG\_DWO...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_SZ, Le...

9:50:2... iexplore.exe 2980 RegSetValue HKCU\Software\Microsoft\Windows\... SUCCESS Type: REG\_SZ, Le...

Show 69 of 187,733 events (0.036%) Backed by virtual memory



Time...	Process Name	PID	Operation	Path	Result	Detail
9:50:2...	iexplore.exe	2980	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Verclsid	SUCCESS	Length: 1
9:50:2...	iexplore.exe	2980	UDP Receive	localhost:1234 > localhost:1234	SUCCESS	Length: 1
9:50:2...	iexplore.exe	2980	UDP Send	localhost:1234 > localhost:1234	SUCCESS	Length: 1

### Insights gained:

No WriteFile operations are taking place so that means that the malware is not creating any files.  
ProcessCreate operation is found and creating the verclsid.exe file. It also appears that there are many

## Lab 2 – Dynamic Analysis

Gunnar Yonker

operations involving the registry such as RegSetValue. Towards the end of the Process Monitor list after the malware is run there is a UDP Receive and UDP send operation. There are also many operations where files are being read. There are many events that are taking place with many of them pertaining to the registry being modified to some capacity. I had difficulty filtering through the noise with this tool and need to expand my knowledge of what operations I should pay particular attention to so that I can filter through the noise more efficiently. I also noted that there was a Thread Create event that was then followed by a Thread Exit at the end of the Process Monitor List.

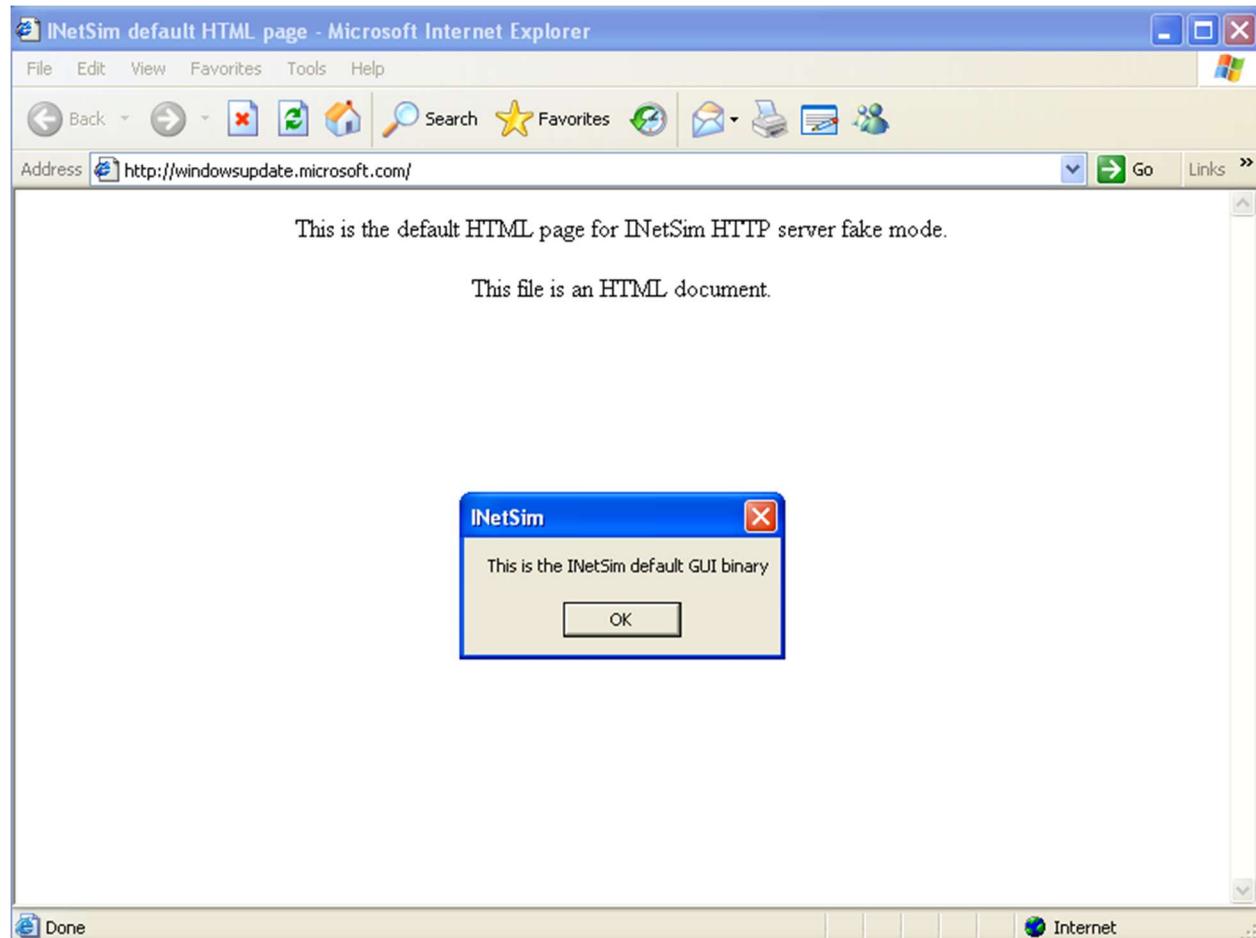
## Lab 2 – Dynamic Analysis

Gunnar Yonker

### Tool: INetSim

**Purpose of Tool:** INetSim is a Linux-based software package for simulating various internet services such as providing fake services to incoming requests such as HTTP, DNS, SMTP, and HTTPS. It also records all incoming requests and connections which is useful for dissecting network behavior of a malware.

#### Relevant information from tool:



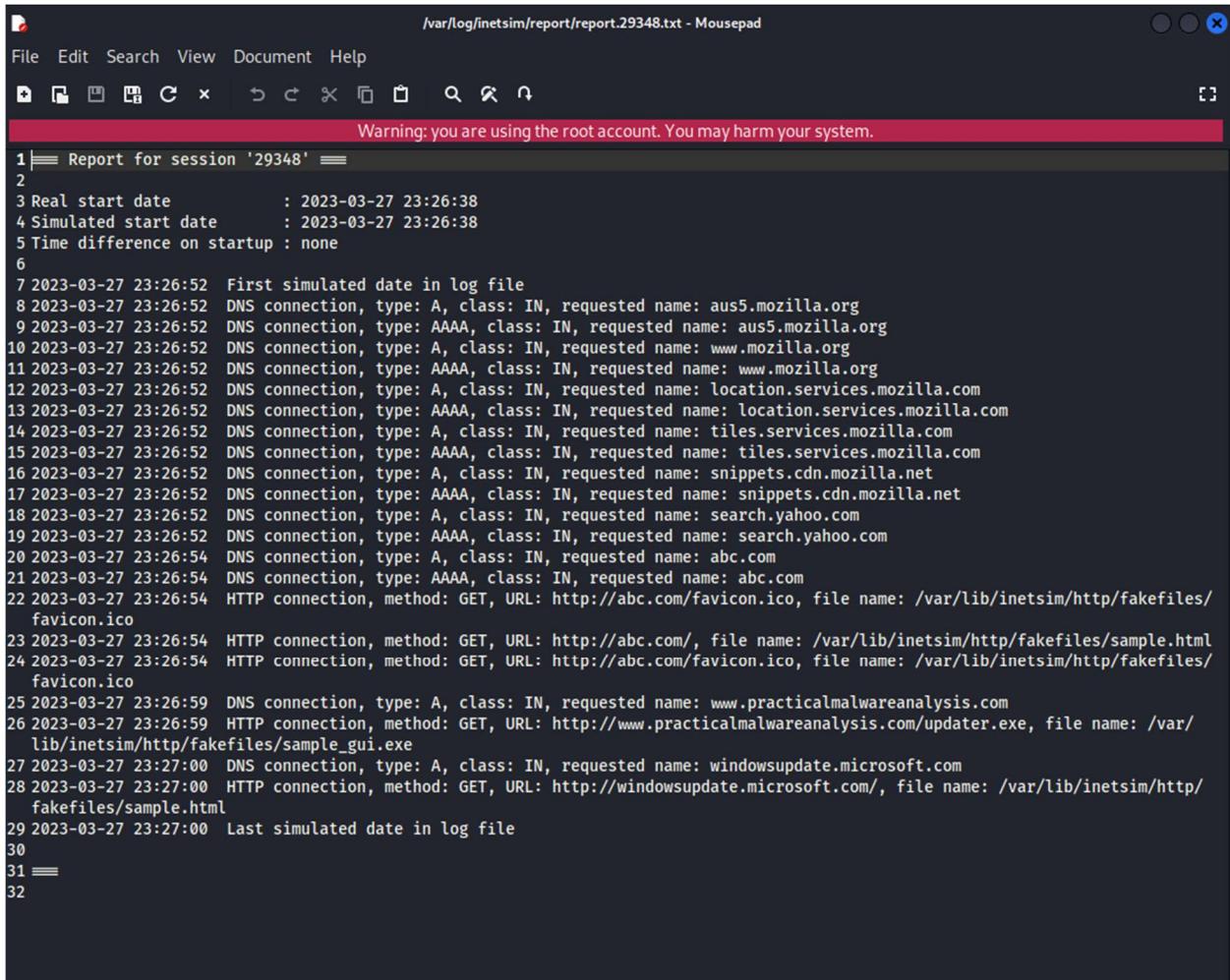
## Lab 2 – Dynamic Analysis

Gunnar Yonker

```
kali@kali:~  
File Actions Edit View Help  
* echo_7_tcp - stopped (PID 29369)  
* quotd_17_udp - stopped (PID 29374)  
* echo_7_udp - stopped (PID 29370)  
* quotd_17_tcp - stopped (PID 29373)  
* daytime_13_udp - stopped (PID 29368)  
* daytime_13_tcp - stopped (PID 29367)  
* ftp_21_tcp - stopped (PID 29357)  
* discard_9_tcp - stopped (PID 29371)  
* syslog_514_udp - stopped (PID 29364)  
* pop3s_995_tcp - stopped (PID 29356)  
* time_37_tcp - stopped (PID 29365)  
* finger_79_tcp - stopped (PID 29362)  
* pop3_110_tcp - stopped (PID 29355)  
* smtps_465_tcp - stopped (PID 29354)  
* smtp_25_tcp - stopped (PID 29353)  
* https_443_tcp - stopped (PID 29352)  
* http_80_tcp - stopped (PID 29351)  
* http_80_tcp - stopped (PID 29351)  
* tftp_69_udp - stopped (PID 29359)  
* irc_6667_tcp - stopped (PID 29360)  
Simulation stopped.  
Report written to '/var/log/inetsim/report/report.29348.txt' (31 lines)  
==== INetSim main process stopped (PID 29348) ====  
.  
└─(kali㉿kali)-[~]  
$ █
```

## Lab 2 – Dynamic Analysis

Gunnar Yonker



/var/log/netsim/report/report.29348.txt - Mousepad

File Edit Search View Document Help

Warning: you are using the root account. You may harm your system.

```
1 Report for session '29348' ===
2
3 Real start date      : 2023-03-27 23:26:38
4 Simulated start date : 2023-03-27 23:26:38
5 Time difference on startup : none
6
7 2023-03-27 23:26:52 First simulated date in log file
8 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: aus5.mozilla.org
9 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: aus5.mozilla.org
10 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: www.mozilla.org
11 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: www.mozilla.org
12 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: location.services.mozilla.com
13 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: location.services.mozilla.com
14 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: tiles.services.mozilla.com
15 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: tiles.services.mozilla.com
16 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: snippets.cdn.mozilla.net
17 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: snippets.cdn.mozilla.net
18 2023-03-27 23:26:52 DNS connection, type: A, class: IN, requested name: search.yahoo.com
19 2023-03-27 23:26:52 DNS connection, type: AAAA, class: IN, requested name: search.yahoo.com
20 2023-03-27 23:26:54 DNS connection, type: A, class: IN, requested name: abc.com
21 2023-03-27 23:26:54 DNS connection, type: AAAA, class: IN, requested name: abc.com
22 2023-03-27 23:26:54 HTTP connection, method: GET, URL: http://abc.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico
23 2023-03-27 23:26:54 HTTP connection, method: GET, URL: http://abc.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html
24 2023-03-27 23:26:54 HTTP connection, method: GET, URL: http://abc.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico
25 2023-03-27 23:26:59 DNS connection, type: A, class: IN, requested name: www.practicalmalwareanalysis.com
26 2023-03-27 23:26:59 HTTP connection, method: GET, URL: http://www.practicalmalwareanalysis.com/updater.exe, file name: /var/lib/inetsim/http/fakefiles/sample_gui.exe
27 2023-03-27 23:27:00 DNS connection, type: A, class: IN, requested name: windowsupdate.microsoft.com
28 2023-03-27 23:27:00 HTTP connection, method: GET, URL: http://windowsupdate.microsoft.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html
29 2023-03-27 23:27:00 Last simulated date in log file
30
31 ===
32
```

## Lab 2 – Dynamic Analysis

Gunnar Yonker

```
/var/log/inetnsim/service.log - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.

report.29348.txt x service.log x

327 [2023-03-27 23:26:59] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] connect
328 [2023-03-27 23:26:59] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] recv: Query Type A, Class IN, Name www.practicalmalwareanalysis.com
329 [2023-03-27 23:26:59] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] send: www.practicalmalwareanalysis.com 3600 IN A 192.168.60.129
330 [2023-03-27 23:26:59] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] disconnect
331 [2023-03-27 23:26:59] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] stat: 1 qtype=A qclass=IN qname=www.practicalmalwareanalysis.com
332 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] connect
333 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: GET /updater.exe HTTP/1.1
334 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: Accept: */*
335 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: Accept-Encoding: gzip, deflate
336 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
337 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: Host: www.practicalmalwareanalysis.com
338 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] recv: Connection: Keep-Alive
339 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] info: Request URL: http://www.practicalmalwareanalysis.com/updater.exe
340 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] info: Sending fake file configured for extension 'exe'.
341 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: HTTP/1.1 200 OK
342 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: Content-Type: x-msdos-program
343 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: Date: Tue, 28 Mar 2023 03:26:59 GMT
344 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: Content-Length: 12814
345 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: Server: InetSim HTTP Server
346 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] send: Connection: Close
347 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] info: Sending file: /var/lib/inetnsim/http/fakefiles/sample_gui.exe
348 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] stat: 1 method=GET url=http://www.practicalmalwareanalysis.com/updater.exe sent=/var/lib/inetnsim/http/fakefiles/sample_gui.exe postdata=
349 [2023-03-27 23:26:59] [29348] [http_80_tcp 29580] [192.168.60.130:1243] disconnect
350 [2023-03-27 23:27:00] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] connect
351 [2023-03-27 23:27:00] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] recv: Query Type A, Class IN, Name windowsupdate.microsoft.com
352 [2023-03-27 23:27:00] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] send: windowsupdate.microsoft.com 3600 IN A 192.168.60.129
353 [2023-03-27 23:27:00] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] disconnect
354 [2023-03-27 23:27:00] [29348] [dns_53_tcp_udp 29350] [192.168.60.130] stat: 1 qtype=A qclass=IN qname=windowsupdate.microsoft.com
355 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] connect
356 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: GET / HTTP/1.1
357 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: Accept: */
358 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: Accept-Language: en-us
359 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: Accept-Encoding: gzip, deflate
360 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
361 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: Host: windowsupdate.microsoft.com
362 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] recv: Connection: Keep-Alive
363 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] info: Request URL: http://windowsupdate.microsoft.com/
364 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] info: No matching file extension configured. Sending default fake file.
365 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: HTTP/1.1 200 OK
366 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: Content-Type: text/html
367 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: Connection: Close
368 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: Content-Length: 258
369 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: Date: Tue, 28 Mar 2023 03:27:00 GMT
370 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] send: Server: InetSim HTTP Server
371 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] info: Sending file: /var/lib/inetnsim/http/fakefiles/sample.html
372 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] stat: 1 method=GET url=http://windowsupdate.microsoft.com/ sent=/var/lib/inetnsim/http/fakefiles/sample.html postdata=
373 [2023-03-27 23:27:00] [29348] [http_80_tcp 29589] [192.168.60.130:1245] disconnect
374
```

### Insights gained:

This tool provider a lot of valuable information about the nature of this malware. The malware attempts to get a file called `updater.exe` from `practicalmalwareanalysis` using a DNS connection and then a HTTP connection to retrieve the `updater.exe` file which is suspected to be a malicious file. It then requests the host of `windowsupdate.microsoft.com/` to make the user think that the file is from Microsoft and that they need to update their windows.

## Lab 2 – Dynamic Analysis

Gunnar Yonker

### **Conclusion:**

The tools used in this lab to analyze the Lab 2 malware sample provided valuable insights into what processes the malware created using Process Explorer. I was able to see that the malware executed, started a internet explorer process, and then exited so that I would not be able to see that the malware was executed and still running. Using this tool I was also able to see the string that was accompanied by the malware created process, this section provided information as to what the malware was attempting to do with this process with functions such as CreateWindowExA and BrowseNewProcess. From this tool I knew which process to track when using the Process Monitor tool. Using the Regshot tool I was able to see what registry files were deleted/modified/created by comparing the windows registry before the malware was executed, and then after. This malware made a number of changes to the registry, with 230 operations taking place and a majority of them being deletions. Many of the modifications, deletions, and additions appeared to deal with system settings and system operations which gave me insight into the idea that the malware was attempting to change or hide system settings to then trick the user into further actions. Next, using the Process Monitor tool to look at events pertaining to the process created by the malware that I found using Process Explorer I was able to see all of the registry events taking place and other events such as a UDP connection attempt and ProcessCreate. Using the INetSim tool by setting up a Kali Linux VM that could run the tool and routing the network connection of my Windows XP infected system through the Kali Linux VM running INetSim I was able to get what I think is some of the most valuable information about this malware. I was able to see that when the malware was run that it was creating a DNS connection to practicalmalwareanalysis.com and then an HTTP connection to retrieve a file called updater.exe. It then tried to connect to the windowsupdate.microsoft.com/ url and that is the page that would be displayed to the user.

Taking all of these insights gathered from the use of the dynamic tools used, I think that the objective of the malware was to modify the system settings to make the user believe that their system needs a critical windows update and trick them into believing that. At the same time the malware would run, and then execute the Internet Explorer process which would first retrieve the updater.exe file from the original connection of practicalmalwareanalysis.com, then it would display to the user the windowsupdate.microsoft.com/ page in the Internet Explorer program that was opened. This combined with the modification of the windows system settings would trick the user into believing that the update was needed and that the updater.exe file was from the Microsoft page that was opened, and they would run it which would further infect the system. Once that file was executed, I am unsure as to what would happen after that file was executed, but if it was the goal of the malware to have the user update using the retrieved file then I would assume it would further infect the system in some capacity.

### **Key Takeaways:**

I think that this reinforced the idea for me that first the static malware analysis should be completed because now with an understanding of the tools for the static analysis, it is a very quick process and can provide some initial insights. The malware can be further analyzed using dynamic analysis tools that we learned about in this module. One of my key takeaways is that I found it difficult to filter through the noise events in Process Monitor, and that as I use it more and understand more of the commonly used operations that it will become a powerful tool in analyzing malware samples. I really enjoyed learning about the use of INetSim by having the infected system route the connection to the Kali Linux VM running the INetSim. This is a very useful tool if it is observed that the malware is trying to connect to

## Lab 2 – Dynamic Analysis

Gunnar Yonker

the internet and retrieve any files or if the malware is trying to communicate with a Command & Control center by sending sensitive information that was gathered from the infected system. It was also interesting to see how the tools can be used with each other such as pairing Process Explorer and Process Monitor together to make sure that the correct process is being analyzed.