Malware Analysis: Trojan Ransomware Static and Dynamic Analysis

NCI Post Graduate Diploma Cyber Security

Author: Jonathon Taaffe

Title: Malware Analysis: Trojan Ransomware Static and Dynamic Analysis
Author: Jonathon Taaffe

Contents

Executive Summary

Suspicious traffic was being generated by a Windows client on the client's office network and an alert was triggered by the production Network Firewall to the IT Network Operations team. There was outgoing network traffic routing to a suspicious domain called http://definitely-not-evil.com/.[1]

IT Network Operations identified the Microsoft Windows 7 [2] client by Internet Protocol (IP)[3] address which was generating the traffic and engaged IT PC Support to disconnect the PC from the network. IT PC Operations disconnected the potentially infected Windows client for further analysis.

Directed IT Network Operations to update the client's Cisco Network Firewall[4] Rules to DROP all traffic from the office network routing to the suspicious domain, ensuring any traffic to this suspicious domain will be DROPPED.

Directed IT PC Operations to update the client's Symantec Anti-Virus Definition Signatures[5] and to push the updated signatures to all Microsoft Windows 7 and 10 clients on the office network. Once all Windows clients are updated, further Microsoft Windows 7 or 10 client infection will be prevented.

This report outlines the steps taken to statically analyse the potentially infected Microsoft Windows 7 client and the steps taken to dynamically analyse the potentially infected Microsoft Windows 7 PC in a controlled, non-networked lab environment.

Further detailed recommendations have been provided to both the IT Network Operations and IT PC Operations teams on how to future protect the client's network against this malware.

[1] Robtex.com [2019] *definitely-not-evil.com Analysis* https://www.robtex.com/dns-lookup/definitely-not-evil.com [Accessed 1st August 2019]
[2] Microsoft.com [2019] *Microsoft Windows 7 Download* https://www.microsoft.com/en-us/software-download/windows7 [Accessed 1st August 2019]
[3] Wikipedia.com [2019] *IP address* https://en.wikipedia.org/wiki/IP_address [Accessed 1st August 2019]
[4] Cisco.com [2019] *What is a Firewall?* https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html [Accessed 1st August 2019]
[5] Symantec.com [2019] *Virus Definitions & Security Updates* https://www.symantec.com/security_response/definitions.jsp [Accessed 1st August 2019]

Malware Identification

Windows7-OfficePC Analysis

To access the OS Hard Disk Drive (HDD) of Windows7-OfficePC, the OS HDD was removed and connected to a Windows7 client which was not network connected. Windows7 client was fully updated with the latest Windows patches and Anti-Virus (AV) definitions. With the OS HDD of the potentially infected Windows7-OfficePC installed, a full AV scan was run. The AV scan identified the malware file as follows:

- File Name: Unknown.exe

With the file, file name and file location identified, the file was quarantined in a folder configured with read-only permissions. Static analysis tool Strings.exe[6] was run against the file to attempt to identify any useful data in the file Unknown.exe but no useful data was identified. This would point to the file being compressed and/or encrypted with a reasonable level of entropy. Static analysis tool HashMyFiles v2.35[7] was then run which gave the following hash values:

- MD5: 25d562f46c14c5267d56722f6a43b8ed
- SHA1: 7cd4d6f44bdb71d24574d0b4bc326abd006eb510

With the hash values documented, from a different network connected Windows client https://www.virustotal.com[8] was searched for the MD5 hash. In total 53 out of 70 Virus Scanning Engines identified this MD5 hash file as malicious. As there is no common malicious file/software naming convention between AV engines, this file was identified by multiple different names. The key words used by the various Virus Engines to identify this file give insight to the function of the file as follows: [9]

- Avast: Win32 Malware-gen
- Kaspersky: Trojan-Ransom.Win32.Blocker.jyqs
- Symantec: Ransom.TeslaCrypt
- ZoneAlarm: Trojan-Ransom.Win32.Blocker.jyqs

This file was identified as:

- Malware or Malicious Software: Software intentionally designed to cause damage to a computer, server, client, or computer network[10]
- Trojan: Malware that is disguised as legitimate software[11]
- Ransom or Ransomware: Prevents users from accessing their system or personal files and demands ransom payment in order to regain access[12]

Conclusion: Windows based Malware with Trojan and Ransomware features.

---

[6] Microsoft.com [2019] *Strings.exe* https://docs.microsoft.com/en-us/sysinternals/downloads/strings [Accessed 1st August 2019]
[7] NirSoft [2019] *HashMyFiles v2.35* https://www.nirsoft.net/utils/hash_my_files.html [Accessed 1st August 2019]
[8] VirusTotal.com [2019] *VirusTotal* https://www.virustotal.com [Accessed 1st August 2019]
[9] VirusTotal.com [2019] *Detection* https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/detection [Accessed 1st August 2019]
[10] Wikipedia.com [2019] *Malware* https://en.wikipedia.org/wiki/Malware [Accessed 1st August 2019]
[11] Kaspersky.com [2019] *What is a Trojan Virus?* https://usa.kaspersky.com/resource-center/threats/trojans [Accessed 1st August 2019]
[12] MalwareBytes.com [2019] *Ransomware* https://www.malwarebytes.com/ransomware/ [Accessed 1st August 2019]

VirusTotal.com[13] Analysis

Further analysis of the details of the file Unknown.exe at VirusTotal are summarised below which will assist in both static and dynamic analysis.

Basic Properties

- File type: Win32 EXE
- Magic: PE32 executable for MS Windows (console) Intel 80386 32-bit
- File size: 368 KB (376832 bytes)
- F-PROT: UPX

Conclusion: Windows 32-bit x86 Portable Executable (PE) file 368KB in size and is packed using UPX[14].

Names

- rainbowmagic.exe [15] [16]
- Trojan.Ransom.Alma.Blocker.exe [17]

Conclusion: These additional files names have provided further sources of research

Ultimate Packer for eXecutables (UPX) Sections

The following data outlines the UPX sections contained within the Unknown.exe file. This data will be useful during static analysis.

Name	Virtual Address	Virtual Size	Raw Size	Entropy
UPX0	4096	188416	0	0
UPX1	192512	335872	335872	7.71
.rsrc	528384	40960	39936	4.1

Table 1. Virus Total Unknown.exe Portable Execution Sections[18]

Conclusions:

- UPX0 has an entropy of 0 meaning it is not encrypted or compressed but also has a raw size of zero which is suspicious.
- UPX1 has an entropy of 7.71 which would suggest this section is encrypted as an anti-reverse engineering measure.
- .rsrc section which includes the top-level directory and sub-directories corresponding to the types of resources found in the file. It has an entropy of 4.1 which would also suggest this section is encrypted as an anti-reverse engineering measure.

[13] VirusTotal.com [2019] *Details* https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/details [Accessed 1st August 2019]

[14] UPX [2019] *Ultimate Packer for eXecutables* https://upx.github.io/ [Accessed 1st August 2019]

[15] Manalyzer.org [2019] *rainbowmagic.exe* https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed [Accessed 1st August 2019]

[16] Reverse.it [2019] *Analysis Overview* https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615 [Accessed 1st August 2019]

[17] Kaspersky.com [2019] *TROJAN-RANSOM.WIN32.BLOCKER* https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/ [Accessed 1st August 2019]

[18] Taaffe, Jonathon [2019] *Table 1. Virus Total Unknown.exe Portable Execution Sections* [Created 1st August 2019]

Imports

The file Unknown.exe imports the Windows Dynamic Link Library (DLL)[19] files below as part of its routine function. The functions Unknown.exe uses from each of the imported DLL files are also included below.

Imported DLL	Associated Functions	Associated Functions Description
ADVAPI32.dll	RegCloseKey	A handle to the open key to be closed[20]
CRYPT32.dll	CryptStringToBinaryA	Converts a formatted string into an array of bytes[21]
KERNEL32.DLL	VirtualProtect	Changes the protection on a region of committed pages in the virtual address space of the calling process[22]
	LoadLibraryA	Loads the specified module into the address space of the calling process. The specified module may cause other modules to be loaded[23]
	ExitProcess	Ends the calling process and all its threads[24]
	GetProcAddress	Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL)[25]
SHELL32.dll	ShellExecuteA	Performs an operation on a specified file[26]
USER32.dll	MessageBoxA	Displays a modal dialog box that contains a system icon, a set of buttons, and a brief application-specific message[27]
WININET.dll	InternetOpenA	Initializes an application's use of the WinINet functions[28]
OLE32.dll	CoTaskMemFree	Frees a block of task memory previously allocated through a call to the CoTaskMemAlloc or CoTaskMemRealloc function[29]

Table 2. Virus Total Unknown.exe Imports[30]

Conclusions

1. CRYPT32.dll: Encryption function
2. USER32.dll: Pop-up message displayed
3. WININET.dll: Access Windows Internet functions for network communication

[19] Microsoft.com [2019] *What is a DLL?* https://support.microsoft.com/en-us/help/815065/what-is-a-dll [Accessed 1st August 2019]
[20] Microsoft.com [2019] *WinRegCloseKey Function* https://docs.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regclosekey [Accessed 1st August 2019]
[21] Microsoft.com [2019] *CryptStringToBinaryA Function* https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptstringtobinarya [Accessed 1st August 2019]
[22] Microsoft.com [2019] *VirtualProtect Function* https://docs.microsoft.com/en-gb/windows/win32/api/memoryapi/nf-memoryapi-virtualprotect [Accessed 1st August 2019]
[23] Microsoft.com [2019] *LoadLibraryA Function* https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya [Accessed 1st August 2019]
[24] Microsoft.com [2019] *ExitProcess Function* https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-exitprocess [Accessed 1st August 2019]
[25] Microsoft.com [2019] *GetProcAddress Function* https://docs.microsoft.com/en-gb/windows/win32/api/libloaderapi/nf-libloaderapi-getprocaddress [Accessed 1st August 2019]
[26] Microsoft.com [2019] *ShellExecuteA Function* https://docs.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecutea [Accessed 1st August 2019]
[27] Microsoft.com [2019] *MessageBoxA Function* https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-messageboxa [Accessed 1st August 2019]
[28] Microsoft.com [2019] *InternetOpenA Function* https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopena [Accessed 1st August 2019]
[29] Microsoft.com [2019] *CoTaskMemFree Function* https://docs.microsoft.com/en-us/windows/win32/api/combaseapi/nf-combaseapi-cotaskmemfree [Accessed 1st August 2019]
[30] Taaffe, Jonathon [2019] *Table 2. Virus Total Unknown.exe Imports* [Created 1st August 2019]

Relations[31]

The following information from VirusTotal outlines the network elements related to Unknown.exe

URL	http://definitely-not-evil.com/ayy
Domain	definitely-not-evil.com
Registrar	Google LLC
IP Address	45.55.137.243
Autonomous System	14061 - DigitalOcean, LLC
Country	US

Table 3. Unknown.exe Network Elements Related[32]

Network Relations Graph Summary[33]

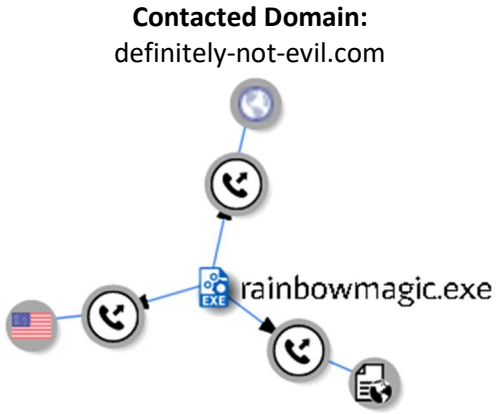


Diagram 1. VirusTotal Network Relations Graph[34]

Conclusions

- There is only 1 Domain contacted which has been added to the Network Firewall Rules
- There is only 1 IP address accessed which has be added to the Network Firewall Rules
- There is only 1 URL accessed which has been added to the Network Firewall Rules

[31] VirusTotal.com [2019] *Relations* https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/relations [Accessed 1st August 2019]
[32] Taaffe, Jonathon [2019] *Table 3. Unknown.exe Network Elements Related* [Created 1st August 2019]
[33] VirusTotal.com [2019] *Network Relations Graph Summary* https://www.virustotal.com/graph//drawer/node-summary/node/na635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/1565866169779 [Accessed 1st August 2019]
[34] Taaffe, Jonathon [2019] *Diagram 1. VirusTotal Network Relations Graph* [Created 1st August 2019]

Behaviour[35]

The following information from VirusTotal details the behaviour of Unknown.exe when it is executed. Behaviour includes:

- Files Opened, Written, Deleted and Copied
- Registry Keys Accessed and Configured
- Windows Processes Created and Shell Command Executed

Files Opened, Written, Deleted and Copied

The following File related actions will be very important when running dynamic analysis against Unknown.exe.

Opened	C:\Users\Administrator\AppData\Roaming\dope.exe \SystemRoot\AppPatch\sysmain.sdb C:\
Written	C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5 C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5 C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies C:\Users\Administrator\AppData\Roaming\dope.exe
Copied	From: C:\Users\Administrator\AppData\Roaming\dope.exe To: C:\analyse\1539912223.2694066_ee750dcb-1b3a-425c-926c-c87e4c201331 C:\analyse\1540046398.473315_4b722a59-4174-48bd-a030-a4543fe92b0b C:\analyse\1551674287.755578_cd02ed62-7212-4aca-a082-5abd0a929da5 C:\analyse\1555220237.3529565_fd6a4d25-0b70-4613-acc0-26ef2dd1a0cb C:\analyse\1564477572.824047_24575dba-4aef-4ac2-a041-27b96daf8984 C:\analyse\1565093853.3799548_6ea294d3-f419-405f-b27e-bf6bec08912b
Deleted	C:\analyse\1539912223.2694066_ee750dcb-1b3a-425c-926c-c87e4c201331 C:\analyse\1540046398.473315_4b722a59-4174-48bd-a030-a4543fe92b0b C:\analyse\1551674287.755578_cd02ed62-7212-4aca-a082-5abd0a929da5 C:\analyse\1555220237.3529565_fd6a4d25-0b70-4613-acc0-26ef2dd1a0cb C:\analyse\1564477572.824047_24575dba-4aef-4ac2-a041-27b96daf8984 C:\analyse\1565093853.3799548_6ea294d3-f419-405f-b27e-bf6bec08912b

Table 4. Files Opened, Written, Copied and Deleted[36]

[35] VirusTotal.com [2019] *Behaviour* https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/behavior [Accessed 1st August 2019]

[36] Taaffe, Jonathon [2019] *Table 4. Files Opened, Written, Copied and Deleted* [Created 1st August 2019]

Registry Keys Accessed and Configured

The following Registry related actions will be very important when running dynamic analysis against Unknown.exe.

Registry Keys Opened	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS

Table 5. Registry Keys Opened[37]

The following changes are made to the Registry by Unknown.exe and will be very important when running dynamic analysis.

Registry Keys Set	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	0
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\dope	C:\Users\Administrator\AppData\Roaming\dope.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\ConsoleTracingMask	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\EnableConsoleTracing	0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\EnableFileTracing	0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\FileDirectory	%windir%\tracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\FileTracingMask	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32\MaxFileSize	1048576
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\ConsoleTracingMask	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\EnableConsoleTracing	0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\EnableFileTracing	0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\FileDirectory	%windir%\tracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\FileTracingMask	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASMANCS\MaxFileSize	1048576
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\AdaptiveSqm\ManifestInfo\Version	0

[37] Taaffe, Jonathon [2019] *Table 5. Registry Keys Opened* [Created 1st August 2019]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\WSqmConsLastEventTimeStamp	
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\WSqmConsLastRunTime	

Table 6. Registry Changes Made[38]

Note: A registry value of 0 means the setting is disabled.

Conclusions

- Internet Proxy settings are disabled:
  Registry Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
  Value: 0

- Persistence is configured:
  Registry Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\dope
  Value: C:\Users\Administrator\AppData\Roaming\dope.exe

- Remote Access is configured:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\dope_RASAPI32

[38] Taaffe, Jonathon [2019] *Table 6. Registry Changes Made* [Created 1st August 2019]

Windows Processes Created and Shell Commands Executed

The following process is created by Unknown.exe and will be very important when running dynamic analysis.

C:\Users\Administrator\AppData\Roaming\dope.exe

And the following process is started by Unknown.exe:

C:\Windows\System32\schtasks.exe

And the following executables and associated commands are executed by Unknown.exe:

Executable/Command	Comment
dope.exe c:\analyse\1539912223.2694066_ee750dcb-1b3a-425c-926c-c87e4c201331	File created by dope.exe in c:\analyse
dope.exe c:\analyse\1540046398.473315_4b722a59-4174-48bd-a030-a4543fe92b0b	File created by dope.exe in c:\analyse
dope.exe c:\analyse\1551674287.755578_cd02ed62-7212-4aca-a082-5abd0a929da5	File created by dope.exe in c:\analyse
dope.exe c:\analyse\1555220237.3529565_fd6a4d25-0b70-4613-acc0-26ef2dd1a0cb	File created by dope.exe in c:\analyse
dope.exe c:\analyse\1564477572.824047_24575dba-4aef-4ac2-a041-27b96daf8984	File created by dope.exe in c:\analyse
dope.exe c:\analyse\1565093853.3799548_6ea294d3-f419-405f-b27e-bf6bec08912b	File created by dope.exe in c:\analyse
\??\C:\Windows\system32\conhost.exe	Console Windows Host[39]
C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"	Deletes the 'Microsoft\Windows\Customer Experience Improvement Program\Uploader' scheduled task
C:\Windows\System32\wsqmcons.exe	Windows SQM Consolidator for Customer Experience Improvement Program[40]
wmiadap.exe /F /T	Windows Management Interface Adapter used to access performance information in the WMI repository[41]

Table 7. Executables and Associated Commands[42]

Conclusions: Multiple files to be monitored during dynamic analysis.

[39] HowToGeek.com [2019] *What Is conhost.exe and Why Is It Running?* https://www.howtogeek.com/howto/4996/what-is-conhost.exe-and-why-is-it-running/ [Accessed 1st August 2019]
[40] Microsoft.com [2019] *Description of the scheduled tasks in Windows Vista* https://support.microsoft.com/en-us/help/939039/description-of-the-scheduled-tasks-in-windows-vista [Created 1st August 2019]
[41] Microsoft.com [2019] *wmiadap* https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmiadap [Accessed 1st August 2019]
[42] Taaffe, Jonathon [2019] *Table 7. Executables and Associated Commands* [Created 1st August 2019]

Further Research from Names Identified on VirusTotal

The following additional names were associated with the Unknown.exe file as per VirusTotal.com[43]:

Names

- rainbowmagic.exe [44] [45]
- Trojan.Ransom.Alma.Blocker.exe [46]

[43] VirusTotal.com [2019] *Detection* https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/detection [Accessed 1st August 2019]

[44] Manalyzer.org [2019] *rainbowmagic.exe* https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed [Accessed 1st August 2019]

[45] Reverse.it [2019] *Analysis Overview* https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615 [Accessed 1st August 2019]

[46] Kaspersky.com [2019] *TROJAN-RANSOM.WIN32.BLOCKER* https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/ [Accessed 1st August 2019]

Manalyzer.com[47] Analysis

This site has detailed analysis of the file rainbowmagic.exe which provided the following information relevant to Unknown.exe

Plugin Output

Libraries used to perform cryptographic operations:	Microsoft's Cryptography API
The PE is packed with UPX	Unusual section name found: UPX0 - Section UPX0 is both writable and executable. Unusual section name found: UPX1 - Section UPX1 is both writable and executable.
The PE contains common functions which appear in legitimate applications.	[!] The program may be hiding some of its imports: LoadLibraryA GetProcAddress Possibly launches other programs: ShellExecuteA Uses Microsoft's cryptographic API: CryptStringToBinaryA Has Internet access capabilities: InternetOpenA
The PE is possibly a dropper.	Resource 101 is possibly compressed or encrypted. Resources amount for 92.9417% of the executable.
Errors	[*] Warning: Section UPX0 has a size of 0!

Table 8. Manalyzer.com Plugin Output[48]

Conclusions

- UPX sections are both writeable and executable
- UPX0 has a size of 0
- Resource 101 is possibly compressed or encrypted

[47] Manalyzer.org [2019] *rainbowmagic.exe* https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed [Accessed 1st August 2019]

[48] Taaffe, Jonathon [2019] *Table 8. Manalyzer.org Plugin Output* [Created 1st August 2019]

Reverse.it[49] Analysis

This site has detailed analysis of the file rainbowmagic.exe which provided the following information relevant to Unknown.exe

Risk Assessment

Remote Access	Contains a remote desktop related string
Persistence	Modifies auto-execute functionality by setting/creating a value in the registry Writes data to a remote process
Fingerprint	Queries kernel debugger information Queries sensitive IE security settings Queries the internet cache settings Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date
Evasive	Marks file for deletion
Spyware	Accesses potentially sensitive information from local browsers
Spreading	Opens the MountPointManager

Table 9. Manalyzer.com rainbow.exe Risk Assessment[50]

Conclusions

- Remote Access/Remote Desktop related configuration
- Sets/creates auto-execute registry entry
- Accesses potentially sensitive information from local browsers
- Opens the MountPointManager to detect additional infection locations

[49] Reverse.it [2019] *Analysis Overview* https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615 [Accessed 1st August 2019]

[50] Taaffe, Jonathon [2019] *Table 9. Manalyzer.org rainbow.exe Risk Assessment* [Created 1st August 2019]

Kaspersky.com[51] Analysis

This site has detailed analysis of the file rainbowmagic.exe which provided the following information relevant to Unknown.exe

Description Key Points

Once Trojan-Ransom.Win32.Blocker is installed it:

1. Adds itself to the computer's startup routine
2. Blocks the operating system from loading normally
3. Takes control of the computer
4. Displays a pop-up requesting an SMS message with special text be sent to a specific number
5. The displayed pop-up states a malware deactivation code will be sent to unlock the computer

[51] Kaspersky.com [2019] *TROJAN-RANSOM.WIN32.BLOCKER* https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/ [Accessed 1st August 2019]

Robtex.com[52] Analysis

Suspicious URL: http://definitely-not-evil.com/

Robtex.com Suspicious Domain Results Summary

Fully Qualified Domain Name	definitely-not-evil.com
IP Address	45.55.137.243
Domain Name Servers	ns-cloud-a1.googledomains.com [216.239.32.106] ns-cloud-a2.googledomains.com [216.239.34.106] ns-cloud-a3.googledomains.com [216.239.36.106] ns-cloud-a4.googledomains.com [216.239.38.106]
Registered To	DigitalOcean, LLC (DO-13)
Location	DigitalOcean San Francisco, Clifton, United States
Web of Trust (WOT) Reputation Score	Trustworthiness - Very poor

Table 10. Robtex.com Results for definitely-not-evil.com[53]

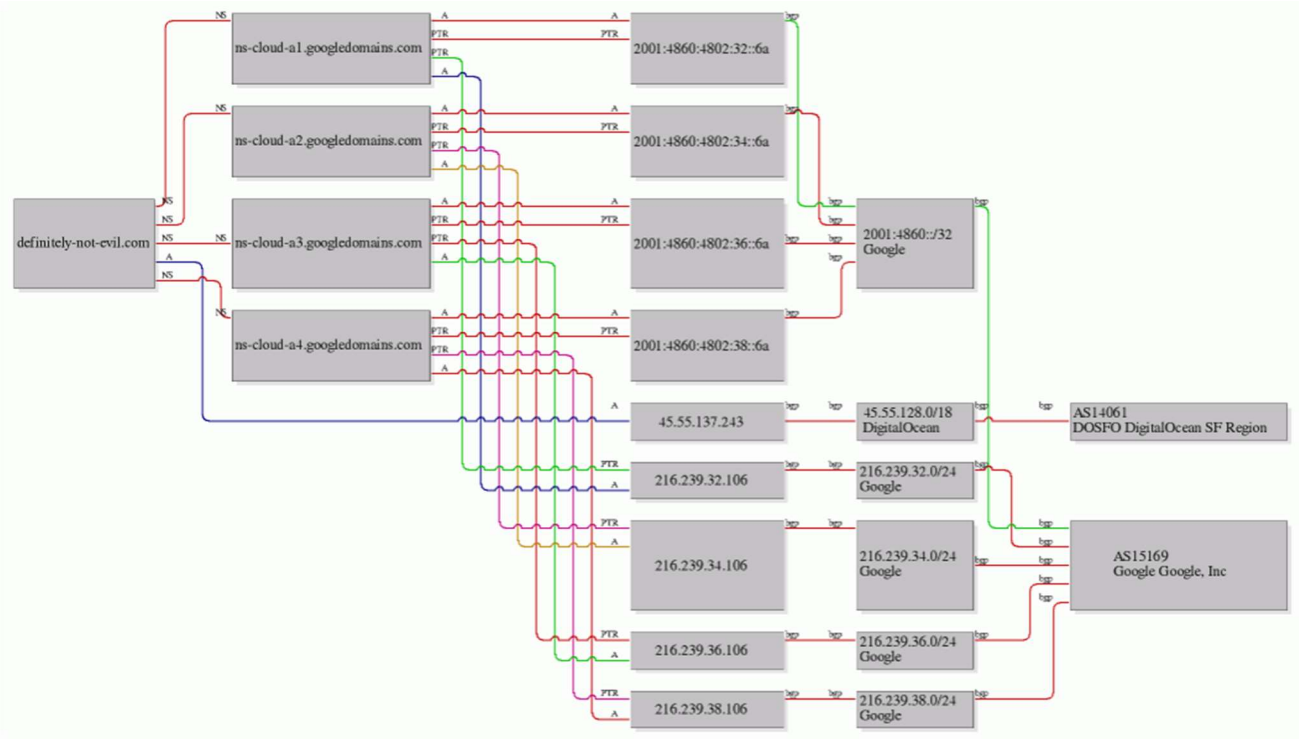


Diagram 2. Robtex.com Related Domain Name Services Graph[54]

Conclusion: Initial DNS related analysis reveals this site has a very poor trustworthiness score.

[52] Robtex.com (2019) *Robtex* https://www.robtex.com/ [Accessed 1st August 2019]

[53] Taaffe, Jonathon [2019] *Table 10. Robtex.com Results for definitely-not-evil.com* [Created 1st August 2019]

[54] Taaffe, Jonathon [2019] *Diagram 2. Robtex.com Related Domain Name Services Graph* [Created 1st August 2019]

Malware Identification Conclusion Summary

Below is a summary of the conclusions determined from the Malware Investigation

Conclusion	Page
Initial DNS related analysis reveals this site has very poor trustworthiness score	4
Windows based Malware with Trojan and Ransomware features	5
Windows 32-bit x86 Portable Executable (PE) file 368KB in size and is packed using UPX	6
UPX0 has an entropy of 0 meaning it is not encrypted or compressed but also has a raw size of zero which is suspicious.	6
UPX1 has an entropy of 7.71 which would suggest this section is encrypted as an anti-reverse engineering measure.	6
.rsrc section which includes the top-level directory and sub-directories corresponding to the types of resources found in the file. It has an entropy of 4.1 which would also suggest this section is encrypted as an anti-reverse engineering measure.	6
CRYPT32.dll: Unknown.exe encryption function	7
USER32.dll: Pop-up message displayed	7
WININET.dll: Access the Windows Internet function for network communication	7
Network Connectivity: 1 Domain, 1 IP address and 1 URL accessed	8
Internet Proxy settings are disabled	11
Persistence is configured	11
Remote Access is configured	11
UPX sections are both writeable and executable	13
UPX0 has a size of 0	13
Resource 101 is possibly compressed or encrypted	13
Remote Access/Remote Desktop related configuration	14
Sets/created auto-execute registry entry	14
Accesses potentially sensitive information from local browsers	14
Opens the MountPointManager to detect additional infection locations	14
Adds itself to the computer's startup routine	14
Blocks the operating system from loading normally	14
Takes control of the computer	14
Displays a pop-up requesting an SMS message with special text be sent to a specific number	14
The displayed pop-up states a malware deactivation code will be sent to unlock the computer	14

Table 11. Malware Identification Conclusion Summary[55]

[55] Taaffe, Jonathon [2019] Table 11. Malware Identification Conclusion Summary [Created 1st August 2019]

Malware Analysis Lab Configuration

Malware Analysis Utilities Selection

As detailed in Lecture 'Malware Types & Lab Setups File', Gateway OS - REMnux[56] and FakeNet-NG[57] were documented as utilities for Reverse-Engineering and Analyzing Malware.

From additional research iNetSim was identified as a useful network simulator. All 3 Malware Analysis Utilities VM's were installed and configured in the Malware Analysis Lab allowing for analysis from 3 different platforms. This will allow for confirmation and validation of analysis results.

To use these utilities, the TCP/IP Gateway IP of the Analysis Client needs to be set to the static IP of the analysis utility as follows

Utility	Static IP
Gateway OS – REMnux	10.0.0.20
FakeNet-NG	10.0.0.21
iNetSim	10.0.0.22

Table 12. Malware Analysis Utilities Static IP Assignment[58]

Gateway OS – REMnux VM Configuration

Downloaded REMnux Virtual Appliance OVA[59] and connected it to the NATNetwork for initial appliance install, update and configuration. Successfully updated using the '`update-remnux full`' command.

Once the VM was updated and operational, the VM's network connection was changed to the isolated Internal Network 'malware-analysis-network01' and set a static IP address of 10.0.0.20/24 with no Gateway specified. Summary of the Gateway OS – REMnux VM configuration is as follows:

Name	Remnux Gateway OS	
Type	Linux	
Version	Ubuntu 14.04 (64-bit)	
RAM	1024MB	
Disk	VDI Dynamic	
Disk Size	25GB	
Network Details	Initial Install and Configuration	Isolated Network
Adapter 1	NATNetwork	Internal Network
Adapter 1 Network	NATNetwork	malware-analysis-network01
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:93:01:19	08:00:27:93:01:19
Adapter 1 IP	DHCP	10.0.0.20

Table 13. Gateway OS – REMnux VM Configuration[60]

[56] REMnux.org (2019) *REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware* https://remnux.org/ [Accessed 1st July 2019].
[57] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]
[58] Taaffe, Jonathon [2019] *Table 12. Malware Analysis Utilities Static IP Assignment* [Created 2nd August 2019]
[59] REMnux 6.0 OVA Public [2019] *remnux-6.0-ova-public.ova (2.0G)* https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download [Accessed 2nd August 2019]
[60] Taaffe, Jonathon [2019] *Table 13. Gateway OS – REMnux VM Configuration* [Created 2nd August 2019]

FakeNet-NG VM Configuration[61]

Downloaded Ubuntu 18.04 ISO and installed a new VM connected to the NATNetwork for initial appliance install, update and configuration as per the following VM configuration:

Name	FakeNet-NG	
Type	Linux Ubuntu (64-bit)	
RAM	1024MB	
Disk	VDI Dynamic	
Disk Size	50GB	
Network Details	Initial Install and Configuration	Isolated Network
Adapter 1	NATNetwork	Internal Network
Adapter 1 Network	NATNetwork	malware-analysis-network01
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:65:65:4F	08:00:27:65:65:4F
Adapter 1 IP	DHCP	10.0.0.21

Table 14. FakeNet-NG VM Configuration[62]

FakeNet-NG Installation – Pre-Requisites[63]

Completed an `apt-get update` and `apt-get upgrade` and installed all FakeNet-NG prerequisites including:

Package	Command
Git package manager	apt install git
Python 2.7 pip package manager	apt install python-pip
Python file transfer package	pip install pysendfile
Python FPTS package	pip install pyopenssl
Python 2.7 development files	apt install python-dev
OpenSSL development files	apt install libssl-dev
libffi development files	apt install libffi-dev
libnetfilterqueue development files	apt install libnetfilter-queue-dev

Table 15. FakeNet-NG Pre-Requisites[64]

FakeNet-NG Installation – Installation[65]

Once all pre-requisites were installed, fakenet-ng was cloned into the /opt directory and ran the python installer as follows:

```
fakenet@FakeNet-NG:/$ cd /opt
fakenet@FakeNet-NG:/opt$ git clone https://github.com/fireeye/flare-fakenet-ng/
fakenet@FakeNet-NG:/opt$ cd flare-fakenet-ng
fakenet@FakeNet-NG:/opt/flare-fakenet-ng$ python setup.py install
```

The Network Adapter was changed to Internet Network 'malware-analysis-network01', configured a static IP address of 10.0.0.21/24 with no Gateway specified.

---

[61] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]

[62] Taaffe, Jonathon [2019] *Table 14. Gateway OS – REMnux VM Configuration* [Created 2nd August 2019]

[63] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]

[64] Taaffe, Jonathon [2019] *Table 15. FakeNet-NG Pre-Requisites* [Created 2nd August 2019]

[65] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]

iNetSim VM Configuration[66]

Downloaded Ubuntu 18.04 ISO and installed a new VM connected to the NATNetwork for initial appliance install, update and configuration as per the following VM configuration:

Name	iNetSim	
Type	Linux Ubuntu (64-bit)	
RAM	1024MB	
Disk	VDI Dynamic	
Disk Size	50GB	
Network Details	Initial Install and Configuration	Isolated Network
Adapter 1	NATNetwork	Internal Network
Adapter 1 Network	NATNetwork	malware-analysis-network01
Adapter 1 Type	Intel PRO/1000MT Server (82545EM)	Intel PRO/1000MT Server (82545EM)
Adapter 1 MAC	08:00:27:E9:1A:F5	08:00:27:E9:1A:F5
Adapter 1 IP	DHCP	10.0.0.22

Table 16. iNetSim VM Configuration[67]

iNetSim – Installation[68]

Updated /etc/apt/sources.list.d/ to include inetsim.list and ran `apt install inetsim` as follows:

```
root@inetsim: echo "deb http://www.inetsim.org/debian/ binary/" >
/etc/apt/sources.list.d/inetsim.list
root@inetsim: wget -O - http://www.inetsim.org/inetsim-archive-signing-key.asc |
apt-key add -
root@inetsim: apt update
root@inetsim: apt install inetsim
```

iNetSim – Configuration

The default Linux DNS resolver must be disabled prior to configuring iNetSim as follows:

```
root@inetsim: systemctl disable systemd-resolved.service
root@inetsim: service systemd-resolved stop
```

Next the default inetsim.conf must be backed up and configured as follows:

```
root@inetsim: cp /etc/inetsim/inetsim.conf /etc/inetsim/inetsim.conf.orig
root@inetsim: nano /etc/inetsim/inetsim.conf
```

Change	`#service_bind_address 10.10.10.1`
To	`service_bind_address 0.0.0.0`
Change	`#dns_default_ip 10.10.10.1`
To	`dns_default_ip 10.0.0.22`

iNetSim uses the following directories and files:

```
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
```

[66] INetSim.org [2019] *INetSim: Internet Services Simulation Suite* https://www.inetsim.org [Accessed 2nd August 2019]

[67] Taaffe, Jonathon [2019] *Table 16. iNetSim VM Configuration* [Created 2nd August 2019]

[68] TechAnarchy.net [2019] *Installing and Configuring InetSim* https://techanarchy.net/blog/installing-and-configuring-inetsim [Accessed 2nd August 2019]

Virtual Network Configuration

Oracle VirtualBox[69] was chosen as the virtual platform for the Malware Analysis Lab with the following configurations:

- **VirtualBox Host-Only Adapter:** Configured from the File Server to local host to allow for initial file transfer from local host to the Analysis Client on the isolated Internal Network.

- **VirtualBox Internal Network:** Configured an isolated Internal Network called 'malware-analysis-network01' which the Analysis Client would be connected to and assigned static IP addresses on the 'malware-analysis-network01' as follows:

Category	Type	Interface	Adapter	IP Range
Utilities	File Server	LAN	Host-Only Adapter	192.168.202.10
Utilities	File Server	LAN	Internal Network	10.0.0.10-19/24
Utilities	Malware Analysis	LAN	Internal Network	10.0.0.20-29/24
Client	Windows 7	LAN	Internal Network	10.0.0.70-79/24

Table 17. malware-analysis-network01 Static Assignments[70]

[69] VirtualBox.org [2019] *VirtualBox* https://www.virtualbox.org/ [Accessed 2nd August 2019]
[70] Taaffe, Jonathon [2019] *Table 17. malware-analysis-network01 Static Assignments* [Created 2nd August 2019]

Utilities VM Configuration

File Transfer: Windows Server 2016[71] File Server

With Automatic Windows Updates, Virus Protection and Windows Firewall disabled on the Analysis Client on which the Malware was to be executed, the client was isolated from the Internet. To facilitate the transfer of the Malware sample and required Analysis Tools as documented in Lecture 'Malware Types & Lab Setups File',a Windows Server 2016 File Server was installed and configured.

The File Server had 2 Network Adapters configured, a Host-Only Adapter with a static IP assigned and an Internal Network static IP assigned. This facilitated downloading the Malware sample to local host, transferring the files to the File Server over the Host-Only adapter and connecting the Analysis Client to the File Server from the Internal Network to download the Malware sample.

Once the malware sample was copied to the Analysis Client, the File Server was powered off to ensure the Internal Network was fully isolated. Summary of the File Server VM configuration is as follows:

Name	WS2016-File-Server01		
Type	Microsoft		
Version	Windows 2016 (64-bit)		
RAM	2048MB		
Disk	VDI Dynamic		
Disk Size	C:50GB D:50GB		
Network Details	Initial VM Install	Upload from Host	Transfer to Analysis Client
Adapter Number	01	01	02
Adapter	NATNetwork	Host-Only Adapter	Internal Network
Network	NATNetwork	Host-Only Adapter	malware-analysis-network01
Type	Intel PRO/1000MT	Intel PRO/1000MT	Intel PRO/1000MT
MAC	08:00:27:63:60:FB	08:00:27:18:93:FF	08:00:27:13:9B:15
IP	DHCP	192.168.202.10	10.0.0.20
Share Name	n/a	mw_client_files	mw_client_files
Share Location	n/a	D:\mw_client_files	D:\mw_client_files
Share Account	n/a	Administrator	MWUser01
Share Permissions	n/a	Full	Read

Table 18. Windows Server 2016 File Server VM Configuration[72]

Configuring File and Storage Services[73]

Added the File and Storage Services\ File Server Role and created an SMB Share called MW_Client_Files granting WS2016_File_Server\mwclient permissions to the share

[71] Portal.Azure.com [2019] *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd August 2019]
[72] Taaffe, Jonathon [2019] *Table 18. Windows Server 2016 File Server VM Configuration* [Created 2nd August 2019]
[73] Tactig.com [2019] *How to Share Files and Folders in Windows Server 2016* https://www.tactig.com/share-files-folders-windows-server-2016/ [Accessed 2nd August 2019]

Analysis Client VM Configuration

As determined in the Malware Investigation section of this report, the malware sample was created to run on Microsoft Windows 7 32-bit[74]

The Analysis Client was installed with Automatic Windows Updates, Virus Protection and Windows Firewall disabled, and was connected to the isolated Internal Network 'malware-analysis-network01'. Analysis Client configuration as follows:

Client Name	Windows7-01
Type	Microsoft Windows
OS Version	Windows 7 Pro 32bit
OS Build	6.1.7601 SP1
RAM	1024MB
Disk	VDI Dynamic
Disk Size	50GB
Adapter 1	Internal Network
Network	malware-analysis-network01
MAC	08:00:27:1E:0F:51
IP	10.0.0.70
Subnet	255.255.255.0
Gateway	10.0.0.20 (Remnux Gateway OS) 10.0.0.21 (FakeNet-NG) 10.0.0.22 (iNetSim)

Table 19. Windows 7 VM Client Configuration[75]

Analysis Client Network Configuration

To ensure the Analysis Client is optimally configured for TCP/IPv4 on the malware-analysis-network01 the following network settings were configured:

Client	Windows7-01
Client for MS Networks	Enabled
QoS Packet Scheduler	Enabled
TCP/IPv4	Enabled
Register connection in DNS	Disabled
Enable LMHOSTS Lookup	Disabled
Disable NetBIOS over TCPIP	Selected
Microsoft ISATAP Adapter	Disabled
ISATAP Adapter	Uninstalled from Device Manager
ISATAP Adapter Disabled	netsh interface isatap set state disabled

Table 20. Windows 7 Network Configuration[76]

[74] Microsoft.com [2019] *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd August 2019]
[75] Taaffe, Jonathon [2019] *Table 19. Windows 7 VM Client Configuration* [Created 2nd August 2019]
[76] Taaffe, Jonathon [2019] *Table 20. Windows 7 Network Configuration* [Created 2nd August 2019]

Analysis Client OS Configuration

To ensure the Analysis Client was optimally configured as per Lecture 'Malware Types & Lab Setups File' and is ready for malware analysis, the following OS settings were configured:

Client	Windows7-01
Automatic Updates	Off
Virus Protection	Off
Windows Firewall	Off
User Account Control	Off
Show File Extensions	Enabled
Show Hidden Files	Enabled
Disable Zone Checking*	Configured
CMD Shortcut on Desktop	Configured
c:\tools\bin Created	Configured
c:\tools\bin added to %PATH%	Configured

Table 21. Windows 7 OS Configuration[77]

***Note on Disabling Internet Explorer Zone Checking[78]:** To disable Zone Checking in Internet Explorer add the following Windows registry keys:

reg add "HKCU\Environment" /V SEE_MASK_NOZONECHECKS /T REG_SZ /D 1 /F

reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1" /v "Flags" /t REG_DWORD /d 219 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /V SEE_MASK_NOZONECHECKS /T REG_SZ /D 1 /F

[77] Taaffe, Jonathon [2019] *Table 21. Windows 7 OS Configuration* [Created 2nd August 2019]

[78] Microsoft.com [2019] *Internet Explorer security zones registry entries for advanced users* https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users [Accessed 2nd August 2019]

Malware Analysis Lab Configuration

Phase 1: Installation and Configuration

The following diagram details Phase 1 configuration of the Malware Analysis Lab which includes the Windows Server 2016[79] File Server, Gateway OS – REMnux[80], FakeNet-NG[81] and iNetSim[82] Malware Analysis Utilities and Windows 7[83] Analysis Client network Configuration.

This configuration allows for:

1. OS install, update and configuration of the File Server and Malware Analysis Utility VM's
2. OS install and configuration of the Analysis Client

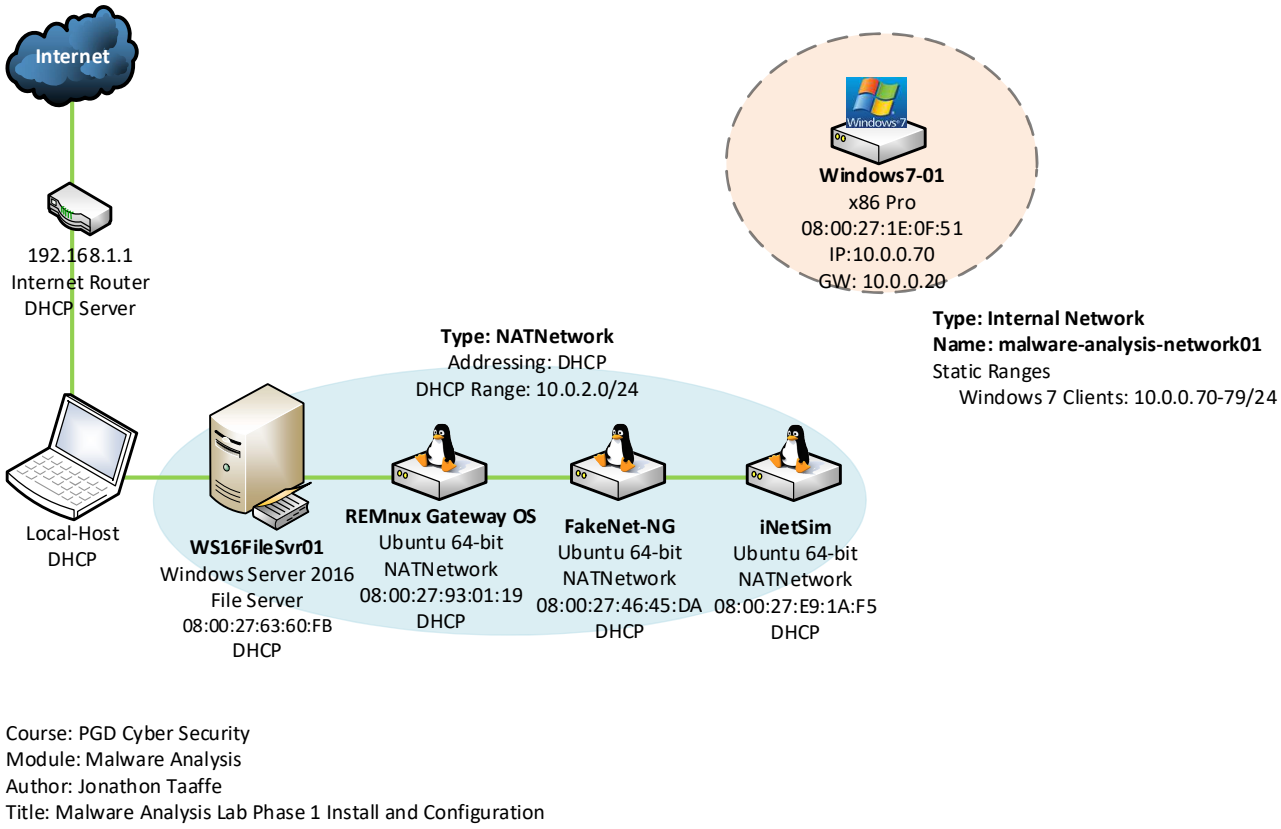


Diagram 3. Phase 1 Installation and Configuration [84]

[79] Portal.Azure.com [2019] *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd August 2019]
[80] REMnux 6.0 OVA Public [2019] *remnux-6.0-ova-public.ova (2.0G)* https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download [Accessed 2nd August 2019]
[81] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]
[82] INetSim.org [2019] *INetSim: Internet Services Simulation Suite* https://www.inetsim.org [Accessed 2nd August 2019]
[83] Microsoft.com [2019] *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd August 2019]
[84] Taaffe, Jonathon [2019] *Diagram 3. Lab 1 Phase 1 Installation and Configuration* [Created 2nd August 2019]

Phase 2: File Transfer

The following diagram details Phase 2 configuration of the Malware Analysis Lab which includes the Windows Server 2016[85] File Server, Network File Share for File Transfer and the Windows 7[86] Analysis Client network configuration.

This configuration allows for

1. Download of all required Analysis files from the Internet to the host
2. Transfer of files from the host to the Windows Server 2016 File Server share mw_client_files
3. Download of Analysis files from the network share mw_client_files to the Analysis Client

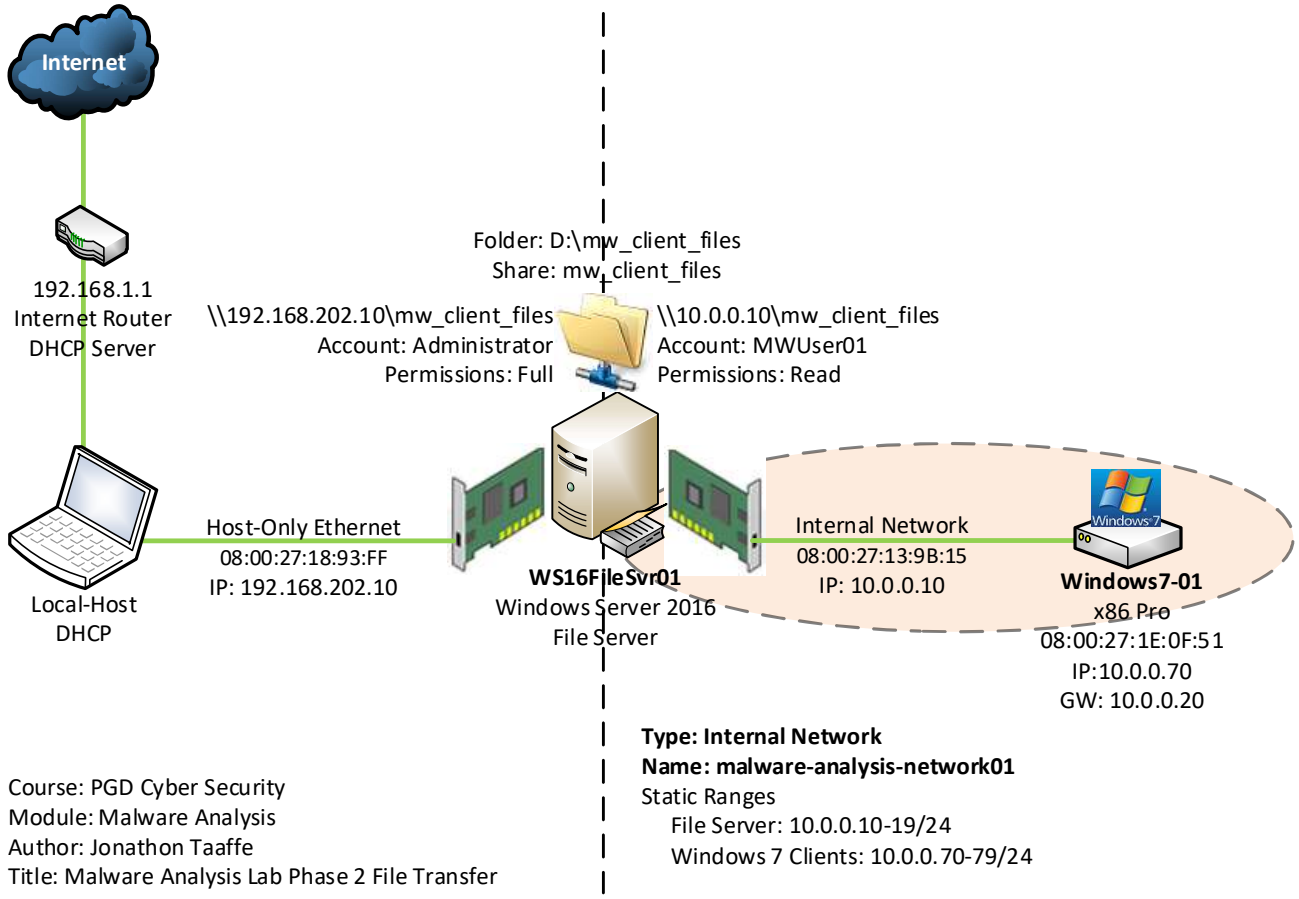


Diagram 4. Phase 2 File Transfer[87]

[85] Portal.Azure.com [2019] *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd August 2019]
[86] Microsoft.com [2019] *Download Virtual Machines* https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ [Accessed 2nd August 2019]
[87] Taaffe, Jonathon [2019] *Diagram 4. Lab 1 Phase 2 File Transfer* [Created 2nd August 2019]

Phase 3: Client Application File Transfer

With the File Server configured allowing for File Transfer from local host to the Analysis Client on the Internal 'malware-analysis-network01' Network, the following Application Files were transferred as per Lecture 'Malware Types & Lab Setups File', to C:\Temp on the Analysis Client:

Application	**File**
Microsoft .NET Framework 4	Microsoft_.NET_Framework_4_x86_x64.exe
Adobe Reader 2019.012.20034	Adobe_Reader_2019.012.20034.exe
Chrome 1.3.34.7	ChromeStandaloneSetup_x86.exe
Firefox Setup 67.0.1 x86	Firefox_Setup_67.0.1_x86.exe
Java JRE 8u211 Windows i586	Java_JRE_8u211_Windows_i586.exe
Microsoft Office 365 Home x86 x64	Office\Setup32.exe
Microsoft PowerShell 1.0 KB926139-v2	Microsoft_PowerShell_1.0_(KB926139-v2)_x86_WinXP
Python 2.7.9 and 3.4.3 x86	Python_2.7.9_x86.msi and Python_3.4.3_x86.msi
Python 3.7.3 x86	Python_3.7.3_x86.exe
WinRAR 561 and 571 x86	WinRAR561.exe and WinRAR571.exe

Table 22. Analysis Client Application File Transfer[88]

Phase 4: Client Application Installation

VirtualBox snapshots were used before and after each application installation as follows

Action	**Details**
Snapshot 01	VM Snapshot
Application Install	Active Perl, Adobe Reader, Chrome
Snapshot 02	Post Application Install Snapshot
Application Install	Firefox, Java, Microsoft .NET
Snapshot 03	Post Application Install Snapshot
Application Install	Microsoft Office, Microsoft PowerShell
Snapshot 04	Post Application Install Snapshot
Application Install	Microsoft Visual C++ 2008, C++ 2010
Snapshot 06	Post Application Install Snapshot
Application Install	Python, WinRAR
VM Clone	OS, Files and Installed Applications

Table 23. Analysis Client Application Installation[89]

[88] Taaffe, Jonathon [2019] *Table 22. Analysis Client Application File Transfer* [Created 2nd August 2019]

[89] Taaffe, Jonathon [2019] *Table 23.. Analysis Client Application Installation* [Created 2nd August 2019]

Phase 5: Malware Analysis Tools File Transfer

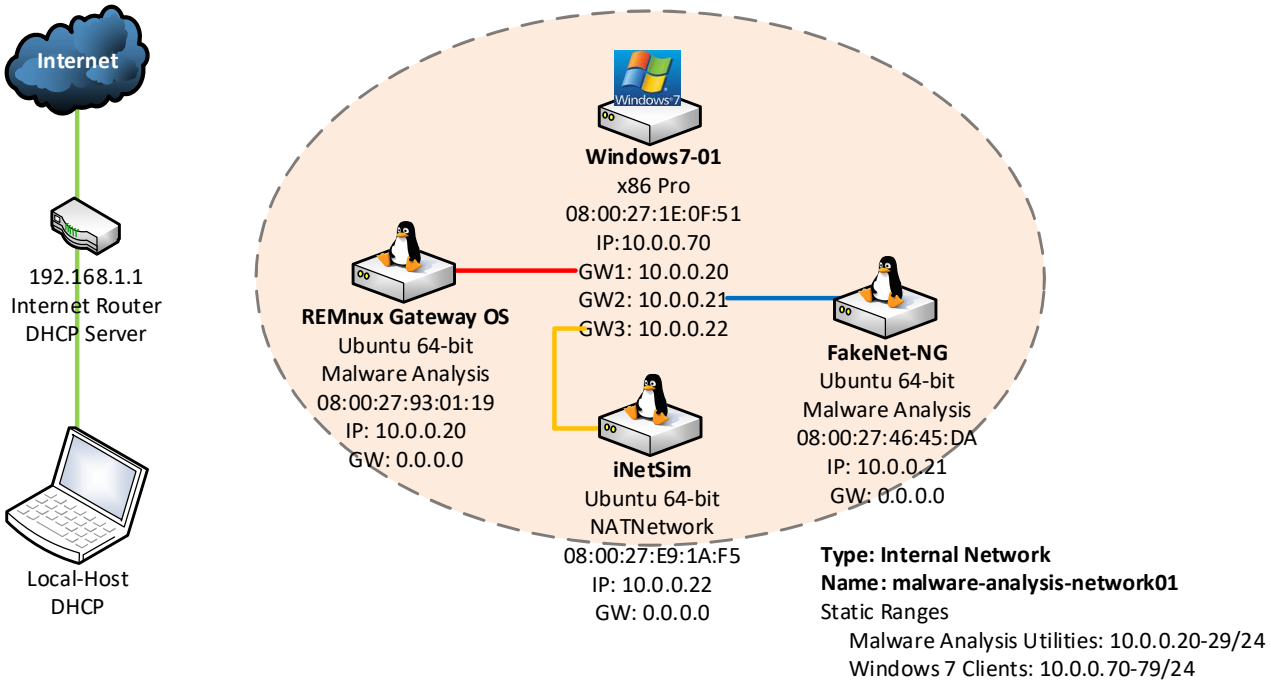
As per Lecture 'Malware Types & Lab Setups File', the current versions of each of the Malware Analysis tools listed were downloaded. All tools were transferred to the Windows Analysis Client and located at C:\Temp\Tools.

Phase 6: Dynamic Malware Analysis Configuration

With the 2 Malware Analysis Utility VM's and all client VM's configured with required applications installed and all analysis tools copied, the Internal 'malware-analysis-network01' Network was completely isolated by powering off the Windows Server 2016[90] File Server.

Note: Malware Analysis Utility Selection

- Setting Client Gateway IP to 10.0.0.20, Client will communicate with REMnux (red line)
- Setting Client Gateway IP to 10.0.0.21, Client will communicate with FakeNet-NG (blue line)
- Setting Client Gateway IP to 10.0.0.22, Client will communicate with iNetSim (yellow line)



Course: PGD Cyber Security
Module: Malware Analysis
Author: Jonathon Taaffe
Title: Malware Analysis Lab Phase 6 Dynamic Malware Analysis Configuration

Diagram 5. Phase 6 Dynamic Malware Analysis Configuration[91]

[90] Portal.Azure.com [2019] *Windows Server 2016 Standard* http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso [Accessed 2nd August 2019]
[91] Taaffe, Jonathon [2019] *Diagram 5. Lab 1 Phase 6 Dynamic Malware Analysis Configuration* [Created 2nd August 2019]

Malware Analysis Methodology

To develop this in-depth report, the following Malware Analysis Methods were used:

- Internet Investigations
- Static Analysis
- Dynamic Analysis

Internet Resources

The following Internet resources were used for the initial information gathering analysis

URL	Justification
https://www.robtex.com[92]	Online analysis of: • Public Internet IP Addresses • DNS Domain Names • DNS Record Types • Host Names • Autonomous Systems • Network Routes
https://www.virustotal.com[93]	1. Data aggregator offering independent services 2. Online analysis of • Uploaded files • URL/Domain Blacklists • File hash values 3. Online analysis against: • 70 Anti-Virus scanning engines • Numerous website scanners • Numerous file and URL analysis tools • Numerous user contributions 4. In-depth online analysis providing: • Detection results • Details of the analysed file/URL • Network related connections • File/URL behavioural data 5. Online Tools to extract data from uploaded files 6. Results shared to improve cyber security 7. Emerging cyber threats and malware behaviour analysis 8. Signatures updated in-line with Anti-Virus signature distribution

Table 24. Internet Investigations Justifications[94]

[92] Robtex.com [2019] *Robtex.com* https://www.robtex.com/ [Accessed 2nd August 2019]
[93] VirusTotal.com [2019] *VirusTotal* https://www.virustotal.com [Accessed 2nd August 2019]
[94] Taaffe, Jonathon [2019] *Table 24. Internet Investigations Justifications* [Created 2nd August 2019]

Internet Investigations (Continued)

URL	Justification
https://manalyzer.org [95]	1. Portable executable static analysis 2. Anti-Virus signature analysis 3. Import combination analysis 4. Resources extraction 5. Cryptographic algorithm identification 6. Hashes submitted to VirusTotal 7. Authenticode signature verification
https://www.reverse.it[96]	1. Online malware analysis using Hybrid Analysis 2. Utilises CrowdStrike Falcon Sandbox for Static Analysis 3. Detect unknown/zero-day threats and evasive malware 4. Full attack lifecycle analysis 5. Online analysis of: • Uploaded files • URL/Domain Blacklists • File hash values 6. Online analysis against: • +10Million Indicators of Compromise (IOCs) • Reputation lookups • Anti-Virus engines
https://threats.kaspersky.com[97]	1. In-depth cyber security analysis of • Vulnerabilities • Threats

Table 25. Internet Investigations Justifications [98]

[95] Manalyzer.org [2019] *Manalyzer.org* https://manalyzer.org [Accessed 2nd August 2019]
[96] Reverse.it [2019] *Reverse.it* https://www.reverse.it [Accessed 2nd August 2019]
[97] Kaspersky.com [2019] *Threats.Kaspersky.com* https://threats.kaspersky.com [Accessed 2nd August 2019]
[98] Taaffe, Jonathon [2019] *Table 25. Internet Investigations Justifications* [Created 2nd August 2019]

Static Malware Analysis Tool Selection

The following static analysis tools were used to further analyse the malware sample:

Tool	Justification
7-zip[99]	Extract password protected zip archives
HashMyFiles v2.35[100]	Calculate the MD5 and SHA1 hash values for files
PEView[101]	View the internals of 32-bit Portable Executable (PE) files View the following content of EXE files: 1. Headers 2. Sections 3. Directories 4. Import table 5. Export table 6. Resource information
PEiD 0.95[102]	View and analyse PE executable files including: 1. Packers 2. Encryptors 3. Decryptors 4. Compilers
BinText3.03[103]	File data extraction View and analyse ASCII code, Unicode and Resource strings
DependencyWalker 2.2[104]	Windows DLL/EXE file scanner Builds a diagram of all dependent modules
UPX 3.95[105]	Pack and update executable files
Resource Hacker 5.1.7[106]	Windows application resource editor
IDA Pro v7.0[107]	Interactive DisAssembler for static decompiling
OllyDbg 1.10[108]	Microsoft Windows assembly analysis debugger

Table 26. Static Analysis Tools Justifications[109]

[99] 7-Zip.org [2019] *7-zip* https://www.7-zip.org/ [Accessed 2nd August 2019]
[100] NirSoft.net [2019] *HashMyFiles v2.35* https://www.nirsoft.net/utils/hash_my_files.html [Accessed 2nd August 2019]
[101] WJRadburn.com [2019] *PEView* http://wjradburn.com/software/ [Accessed 2nd August 2019]
[102] Softpedia.com [2019] *PEiD 0.95* http://www.softpedia.com/ [Accessed 2nd August 2019]
[103] Softpedia.com [2019] *BinText3.03* https://www.softpedia.com/get/System/File-Management/BinText.shtml [Accessed 2nd August 2019]
[104] DependencyWalker.com [2019] *DependencyWalker 2.2* http://www.dependencywalker.com/ [Accessed 2nd August 2019]
[105] UPX.github.com [2019] *UPX 3.95* https://upx.github.io/ [Accessed 2nd August 2019]
[106] AngusJ.com [2019] *Resource Hacker 5.1.7* http://www.angusj.com/resourcehacker/ [Accessed 2nd August 2019]
[107] Hex-Rays.com [2019] *IDA Pro v7.0* https://www.hex-rays.com/products/ida/support/download_freeware.shtml [Accessed 2nd August 2019]
[108] OllyDBG.de [2019] *OllyDbg 1.10* http://www.ollydbg.de/download.htm [Accessed 2nd August 2019]
[109] Taaffe, Jonathon [2019] *Table 26. Static Analysis Tools Justifications* [Created 2nd August 2019]

Dynamic Malware Analysis Tool Selection

The following dynamic analysis tools were used to further analyse the malware sample:

Tool	Justification
RegShot[110]	Windows registry comparison tool
SysInternals Process Monitor v3.50[111]	Monitor real-time file system, Registry and process/thread activity in Windows
SysInternals Process Explorer v 16.21[112]	Display active processes in Windows Display handles of active processes Display DLL of active processes
Wireshark[113]	Advanced network protocol analyser
Gateway OS - REMnux[114]	Distribution to reverse-engineer malicious software Analyse Windows and Linux malware Examine browser-based threats Intercept network traffic in an isolated lab
FakeNet-NG[115]	Dynamic network analysis tool for malware analysis Intercept/redirect network traffic Capture network signatures Identify malware's functionality

Table 27. Dynamic Analysis Tools Justifications[116]

[110] RegShot [2019] *RegShot* https://sourceforge.net/projects/regshot/ [Accessed 2nd August 2019]
[111] Microsoft.com [2019] *SysInternals Process Monitor v3.50* https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon [Accessed 2nd August 2019]
[112] Microsoft.com [2019] *SysInternals Process Explorer v 16.21* https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer [Accessed 2nd August 2019]
[113] Wireshark.org [2019] *Download Wireshark* https://www.wireshark.org/download.html [Accessed 2nd August 2019]
[114] REMnux 6.0 OVA Public [2019] *remnux-6.0-ova-public.ova (2.0G)* https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download [Accessed 2nd August 2019]
[115] FireEye/Flare-FakeNet-NG [2019] *FakeNet-NG - Next Generation Dynamic Network Analysis Tool* https://github.com/fireeye/flare-fakenet-ng [Accessed 2nd August 2019]
[116] Taaffe, Jonathon [2019] *Table 27. Dynamic Analysis Tools Justifications* [Created 2nd August 2019]

Malware Analysis

Static Malware Analysis

As documented in section 2 'Malware Identification', extensive online analysis of the malware sample has already been completed. In this section static analysis will be preformed on the malware sample in an isolated VirtualBox VM environment.

Important Note: In preparation for both the static and dynamic analysis of this malware sample, the following precautions have been taken:

1. All malware analysis tools copied to the Windows 7 Analysis Client
2. Malware sample copied to the Windows 7 Analysis Client
3. Shared Folders: Disabled
4. Drag' n 'Drop: Disabled
5. Shared Clipboard: Disabled
6. Disabled network adapter 1 connected to Windows 7 Analysis Client
7. Cloned the Windows 7 Analysis Client
8. Powered off the Windows 2016 File Server

Malware Sample File Location: C:\Temp\Virus_Files\Unknown.exe

PEView[117] Analysis

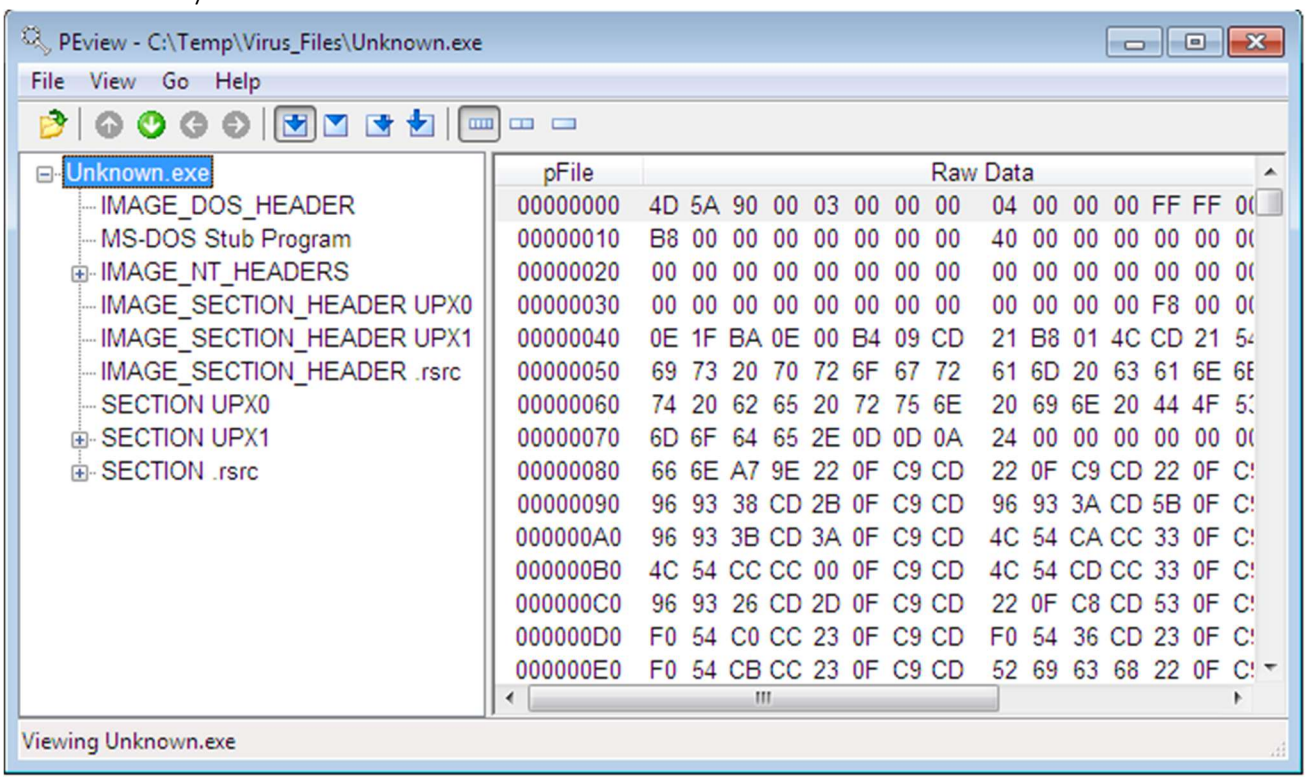


Image 1. PEView Analysis[118]

[117] Radburn, Wayne J. (2018) *PEview version 0.9.9 (.zip 31KB)* http://wjradburn.com/software/ [Accessed 2nd August 2019]
[118] Taaffe, Jonathon [2019] *Image 1. PEView Analysis* [Created 2nd August 2019]

PEView SECTION UPX0 Analysis

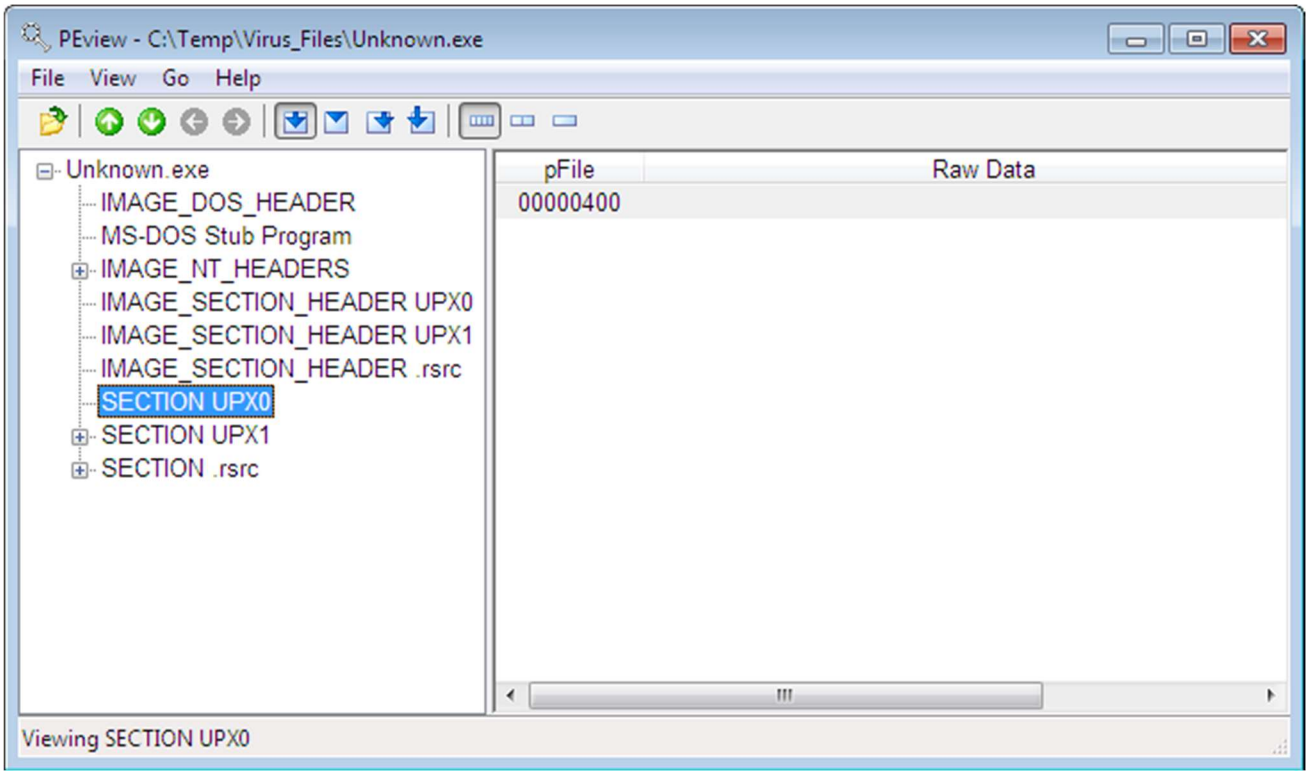


Image 2. Sections Analysis - SECTION UPX0[119]

Conclusion: No viewable data available

[119] Taaffe, Jonathon [2019] *Image 2. Sections Analysis - SECTION UPX0* [Created 2nd August 2019]

PEView SECTION UPX1 Analysis

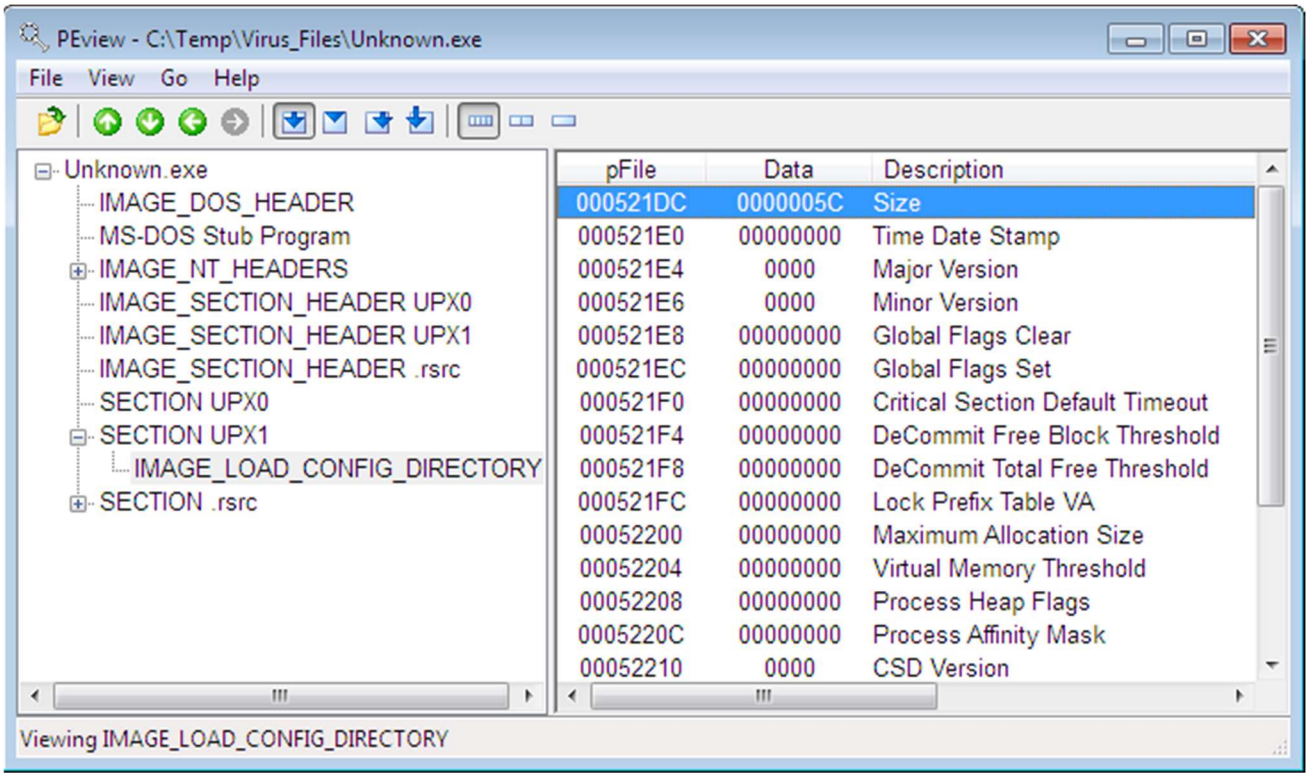


Image 3. Sections Analysis - SECTION UPX1[120]

Conclusion: Key information relating to the Directory Load Configuration, but no data listed in Value column

[120] Taaffe, Jonathon [2019] *Image 3. Sections Analysis - SECTION UPX1* [Created 2nd August 2019]

PEView SECTION .rsrc Analysis

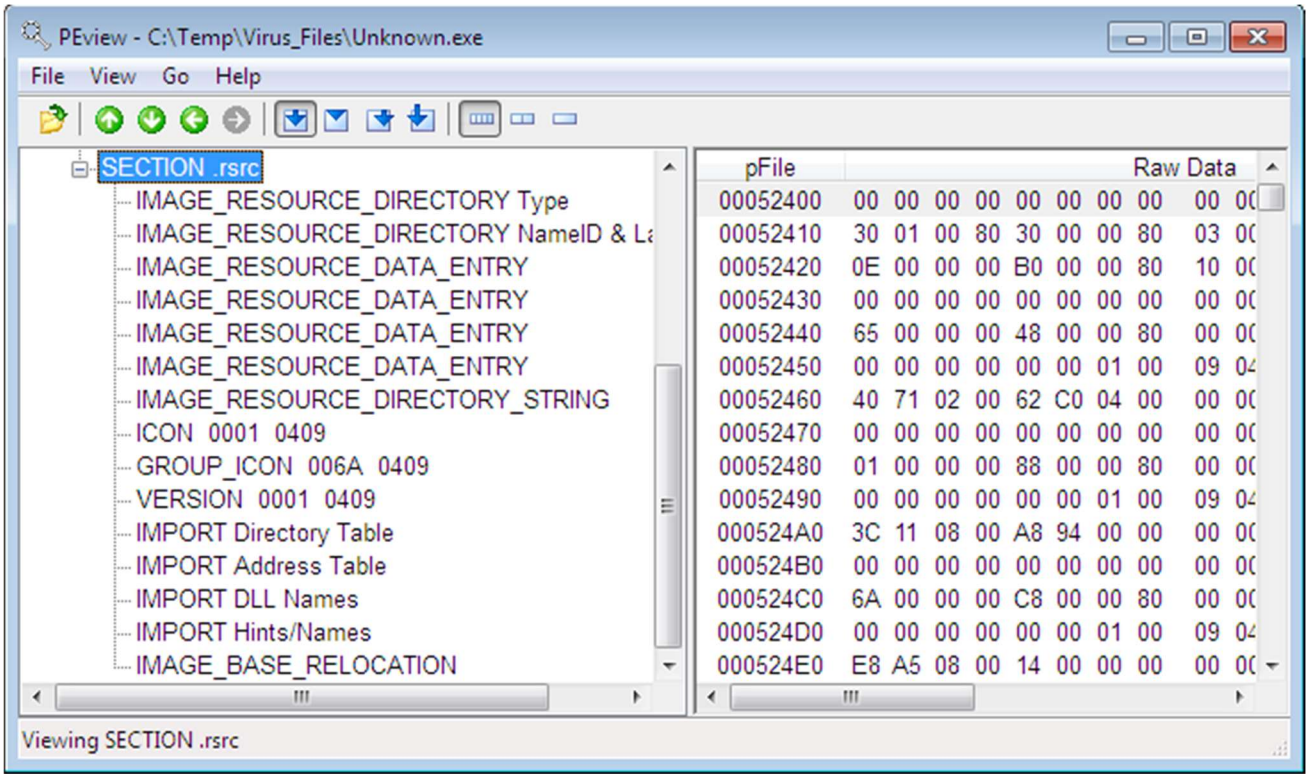


Image 4. Section Analysis - SECTION .rsrc[121]

Conclusion: Extensive resource data available as follows

[121] Taaffe, Jonathon [2019] *Image 4. Section Analysis - SECTION .rsrc* [Created 2nd August 2019]

PEView SECTION .rsrc – IMAGE_RESOURCE_DIRECORY Type Analysis

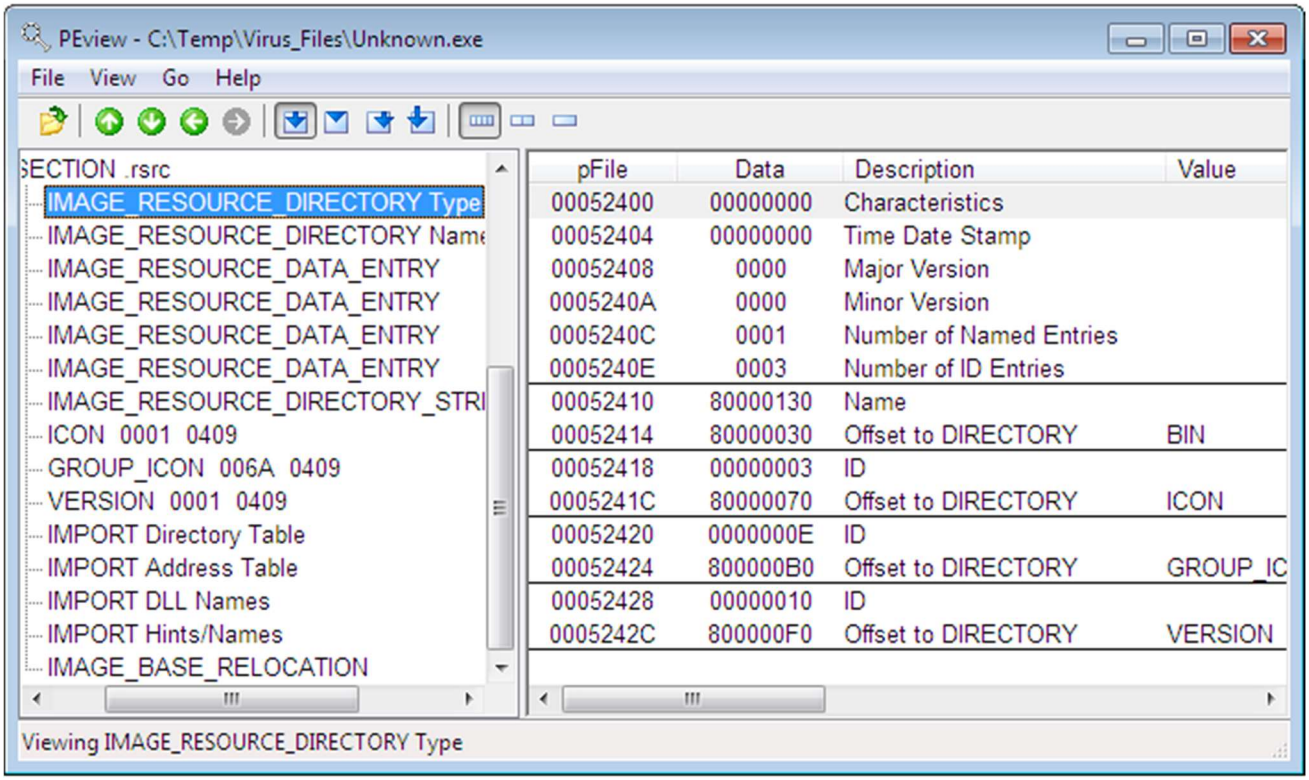


Image 5. SECTION .rsrc - IMAGE_RESOURCE_DIRECORY Type[122]

Analysis: This shows there are Bin, Icon, Group_Icon and Version directories associated to the sample.

[122] Taaffe, Jonathon [2019] *Image 5. SECTION .rsrc - IMAGE_RESOURCE_DIRECORY Type* [Created 2nd August 2019]

PEView SECTION .rsrc – IMPORT Directory Table Analysis

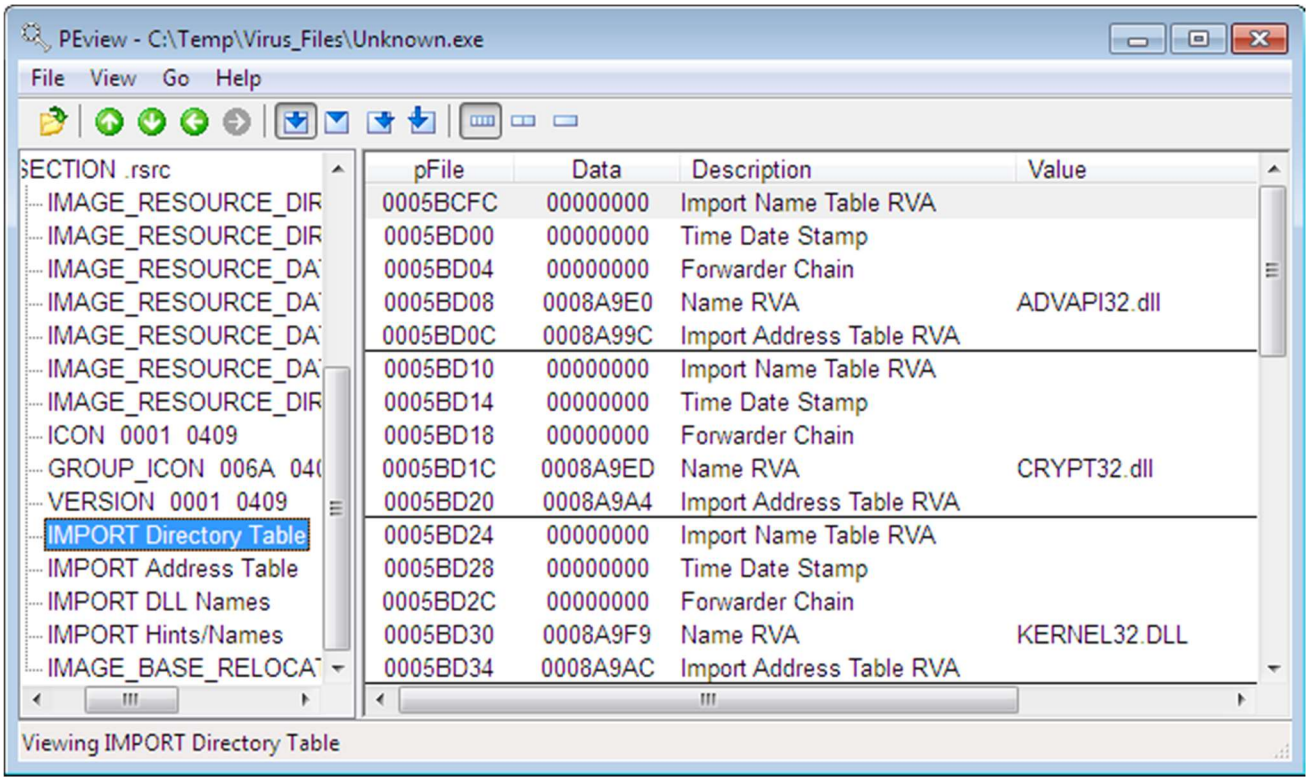


Image 6. SECTION .rsrc – IMPORT Directory Table[123]

Analysis: This section shows the Dynamic Link Library files imported by this malware sample.

Imported Windows DLL's

- ADVAPI32.dll
- CRYPT32.dll
- KERNEL32.DLL
- SHELL32.dll
- USER32.dll
- WININET.dll
- ole32.dll

[123] Taaffe, Jonathon [2019] *Image 6. SECTION .rsrc – IMPORT Directory Table* [Created 2nd August 2019]

PEView SECTION .rsrc – IMPORT Address Table Analysis

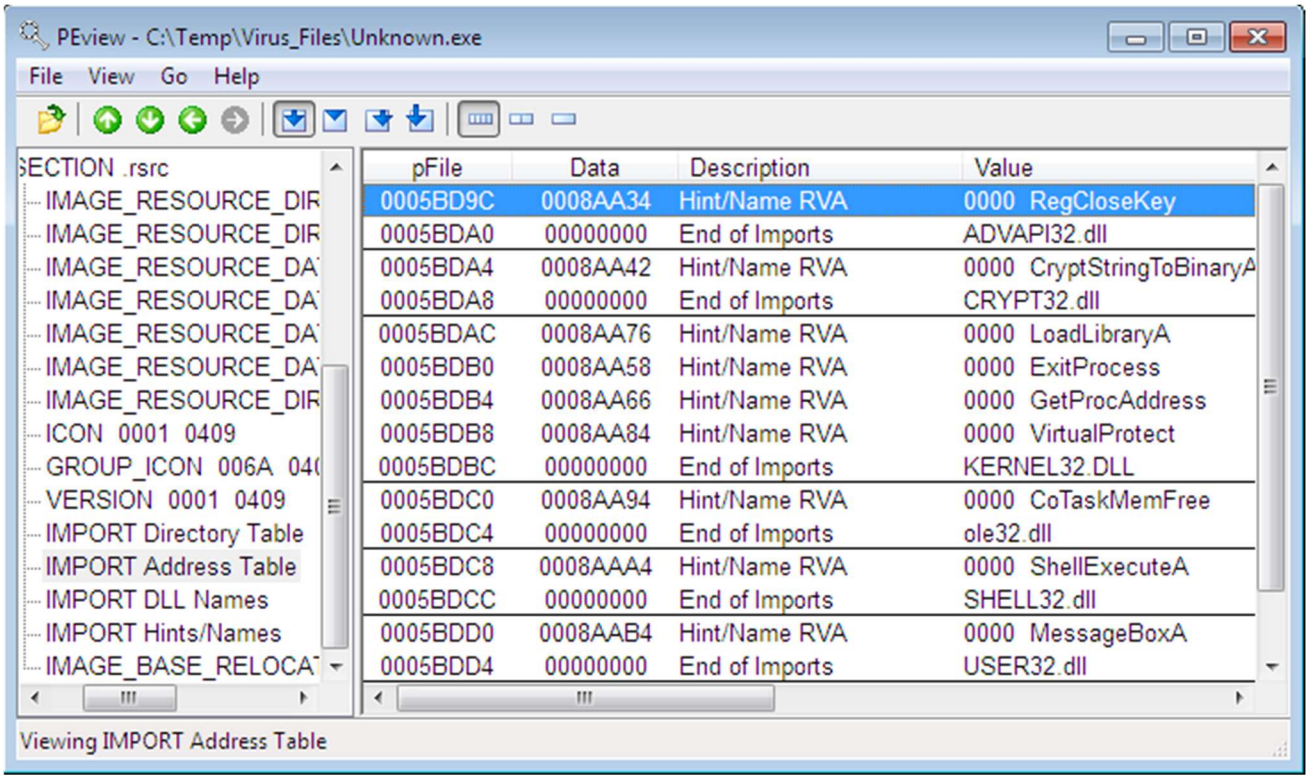


Image 7. SECTION .rsrc – IMPORT Address Table[124]

Analysis: This section shows the functions used in the Dynamic Link Library files imported by this malware sample.

Associated Functions	Associated Functions Description
RegCloseKey	A handle to the open key to be closed
CryptStringToBinaryA	Converts a formatted string into an array of bytes
VirtualProtect	Changes the protection on a region of committed pages in the virtual address space of the calling process
LoadLibraryA	Loads the specified module into the address space of the calling process. The specified module may cause other modules to be loaded
ExitProcess	Ends the calling process and all its threads
GetProcAddress	Retrieves the address of an exported function or variable from the specified dynamic-link library (DLL)
ShellExecuteA	Performs an operation on a specified file
MessageBoxA	Displays a modal dialog box that contains a system icon, a set of buttons, and a brief application-specific message
InternetOpenA	Initializes an application's use of the WinINet functions
CoTaskMemFree	Frees a block of task memory previously allocated through a call to the CoTaskMemAlloc or CoTaskMemRealloc function

Table 28. Unknown.exe DLL File Imports[125]

[124] Taaffe, Jonathon [2019] *Image 7. SECTION .rsrc – IMPORT Address Table* [Created 2nd August 2019]
[125] Taaffe, Jonathon [2019] *Table 28. Unknown.exe DLL File Imports* [Created 2nd August 2019]

PEiD[126] Analysis

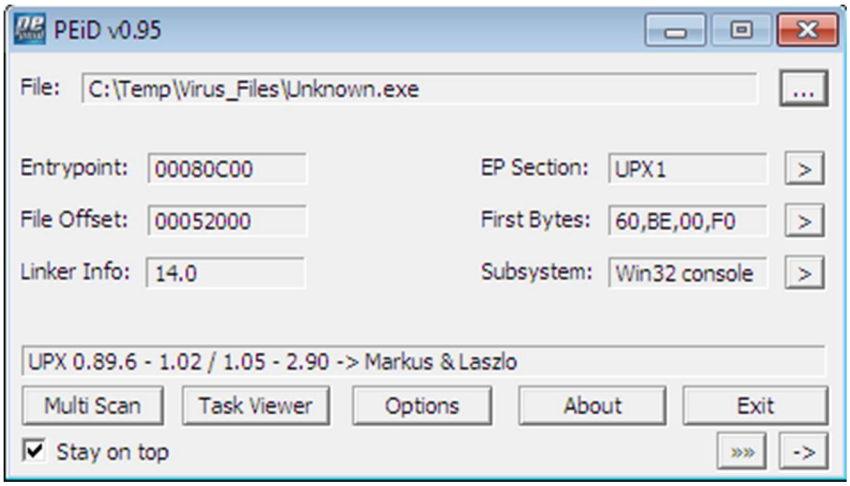


Image 8. PEiD Analysis[127]

Conclusion: Shows that this malware sample was packed using UPX 0.89.6 - 1.02 / 1.05 – 2.90 -> Markus & Laszlo

PEiD - Section Viewer

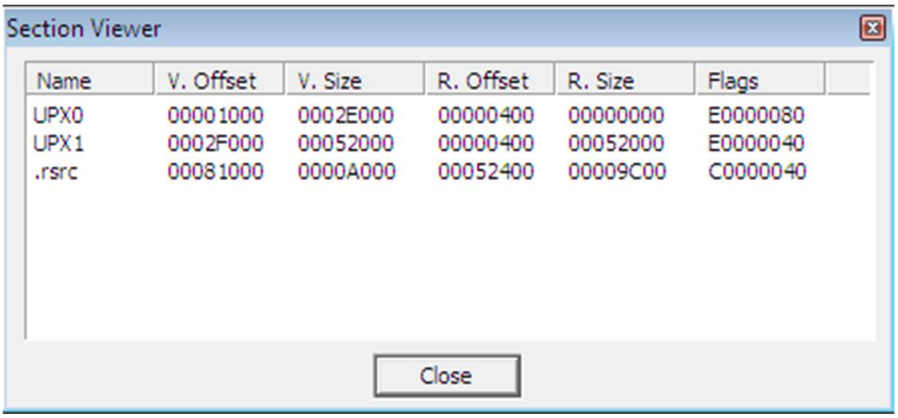


Image 9. PEiD - Section Viewer[128]

Conclusion: Same 3 sections identified as PEView – UPX0, UPX1 and .rsrc

[126] Softpedia.com [2019] *PEiD 0.95* https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 2nd August 2019]
[127] Taaffe, Jonathon [2019] *Image 8. PEiD Analysis* [Created 2nd August 2019]
[128] Taaffe, Jonathon [2019] *Image 9. PEiD - Section Viewer* [Created 2nd August 2019]

BinText3.03[129] Analysis

BinText Analysis01

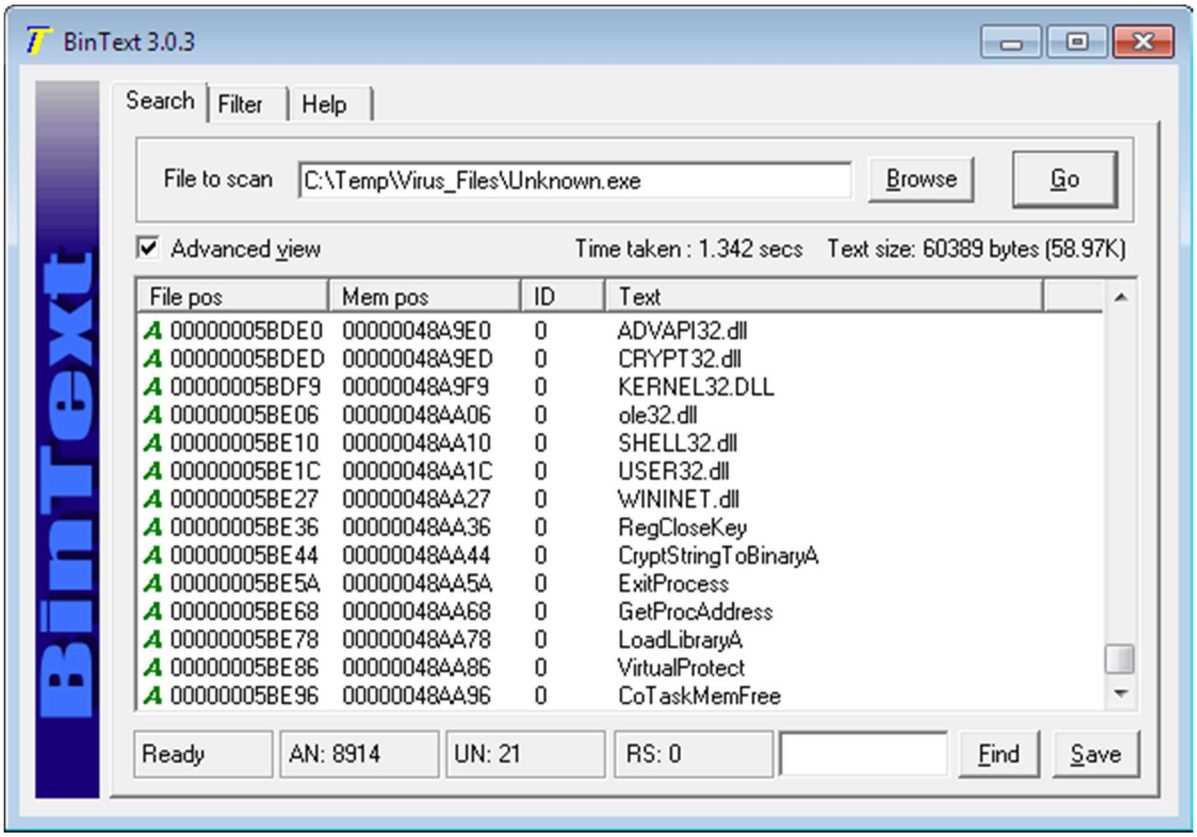


Image 10. BinText3.03 Analysis01[130]

Conclusion: Towards the end of the BinText display the Dynamic Link Library files imported by, and the associated functions used in the DLL files imported by this malware sample are listed.

These are the same results as PEView.

[129] Softpedia.com [2019] *BinText 3.03* https://www.softpedia.com/get/System/File-Management/BinText.shtml [Accessed 2nd August 2019]

[130] Taaffe, Jonathon [2019] *Image 10. BinText3.03 Analysis01* [Created 2nd August 2019]

BinText Analysis02

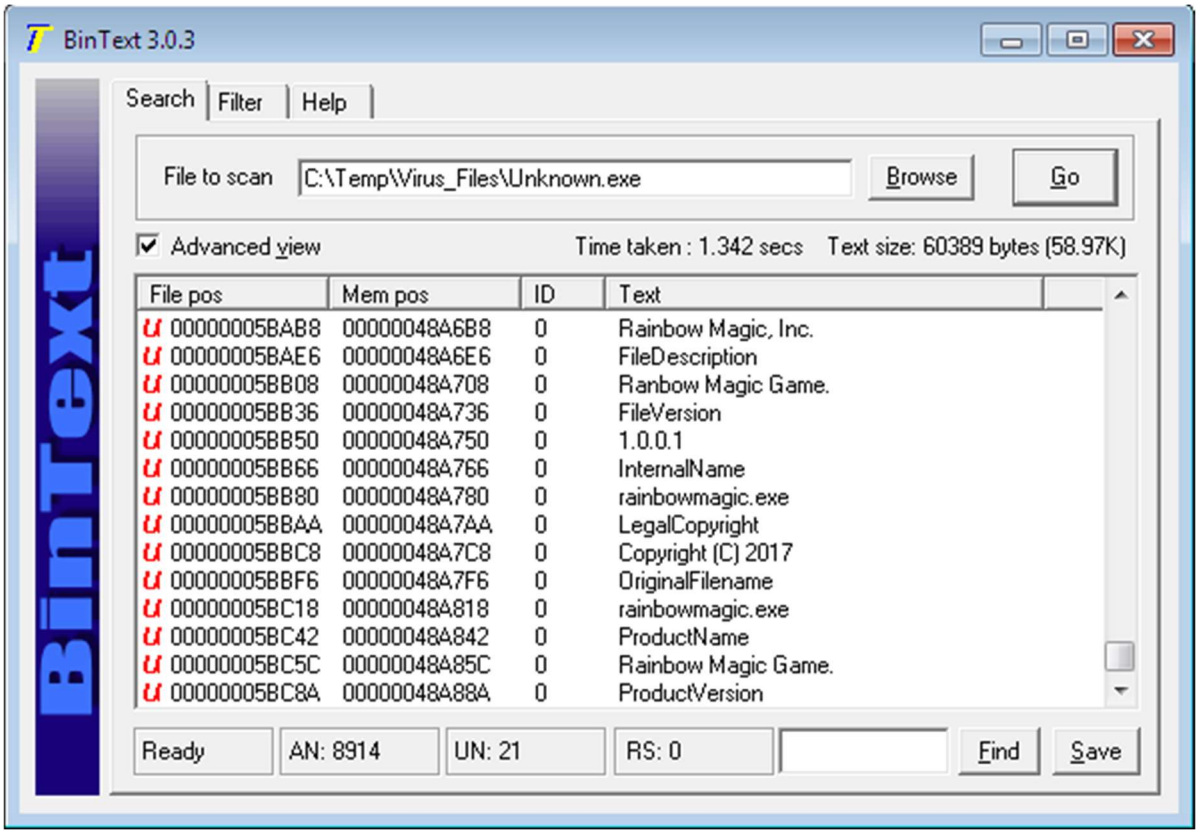


Image 11. BinText3.03 Analysis02[131]

Conclusion: Here we can see the Product Name 'RainBow Magic Game' and Original File name of 'rainbowmagix.exe ' listed.

This confirms the Malware Identification internet results

[131] Taaffe, Jonathon [2019] *Image 11. BinText3.03 Analysis02* [Created 2nd August 2019]

Dependency Walker 2.2[132] Analysis

Dependency Walker Analysis01

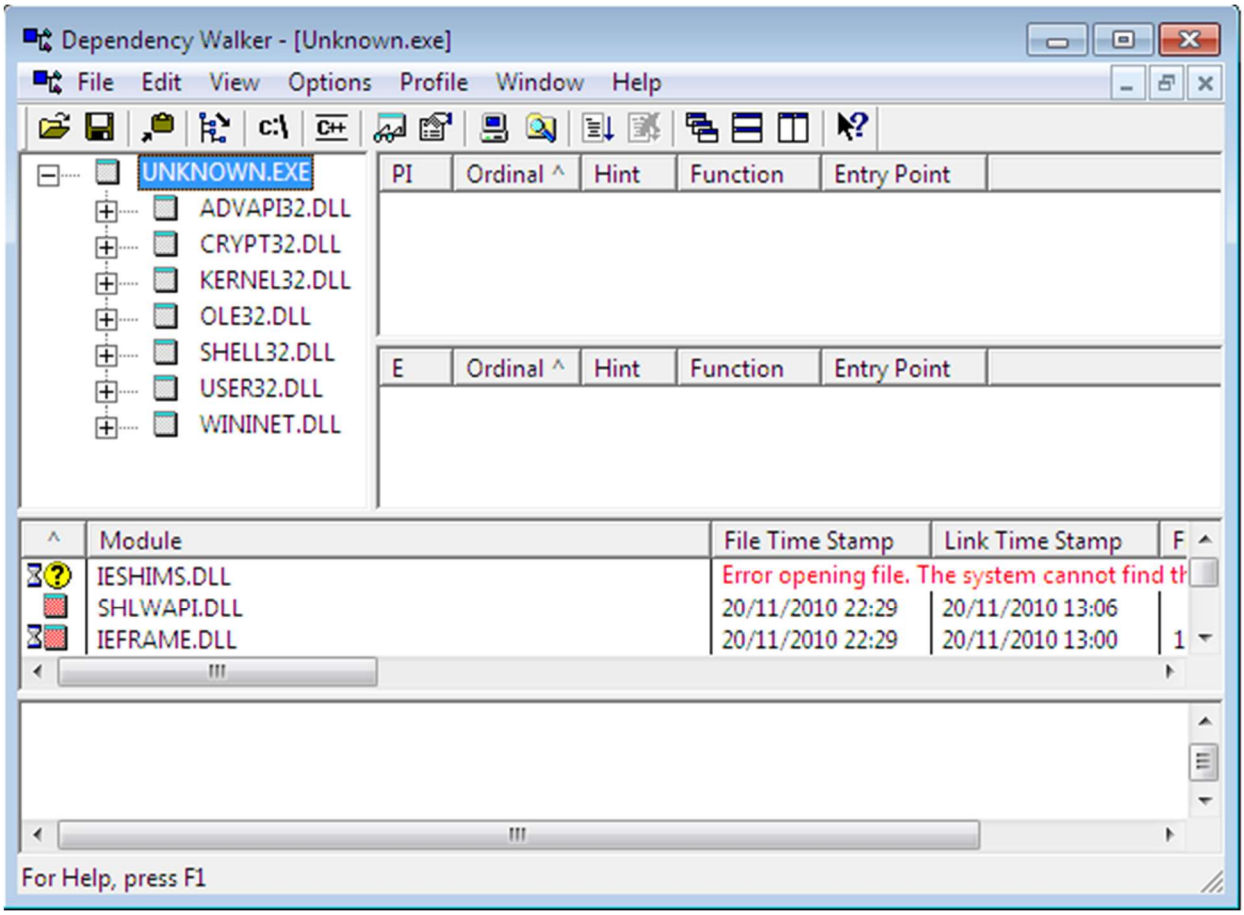


Image 12. Dependency Walker 2.2 Analysis01[133]

Analysis: This section shows the Dynamic Link Library files imported by this malware sample.

Imported Windows File

- ADVAPI32.dll
- CRYPT32.dll
- KERNEL32.DLL
- SHELL32.dll
- USER32.dll
- WININET.dll
- ole32.dll

These imports are the same as PEView

Conclusion: Import data not obfuscated

[132] Dependency Walker 2.2 [2019] *Dependency Walker 2.2* http://www.dependencywalker.com/ [Accessed 2nd August 2019]
[133] Taaffe, Jonathon [2019] *Image 12. Dependency Walker 2.2 Analysis01* [Created 2nd August 2019]

Dependency Walker Analysis02

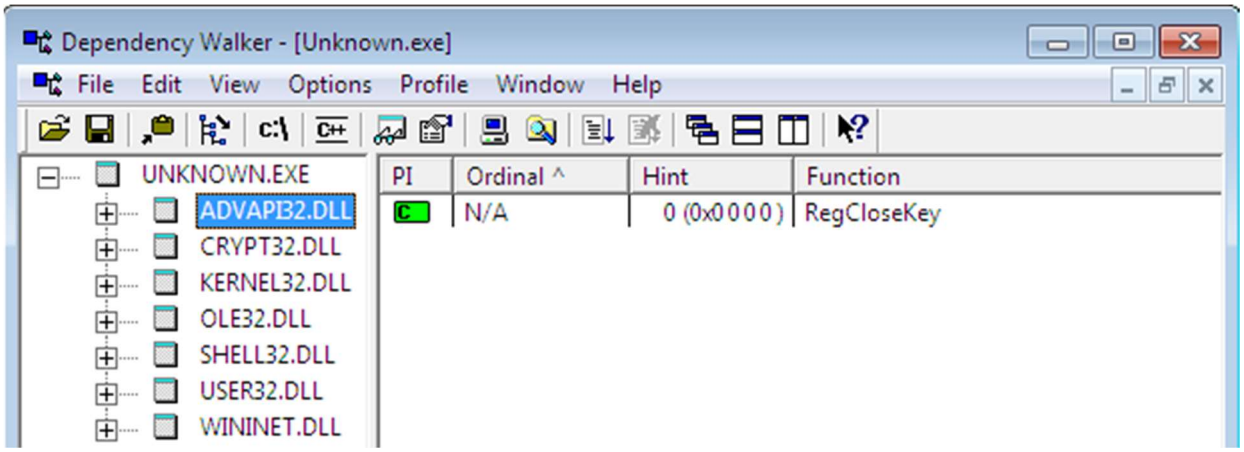


Image 13. Dependency Walker 2.2 Analysis02[134]

Conclusion: ADVAPI32.DLL imported and RegCloseKey function used.

Dependency Walker Analysis03

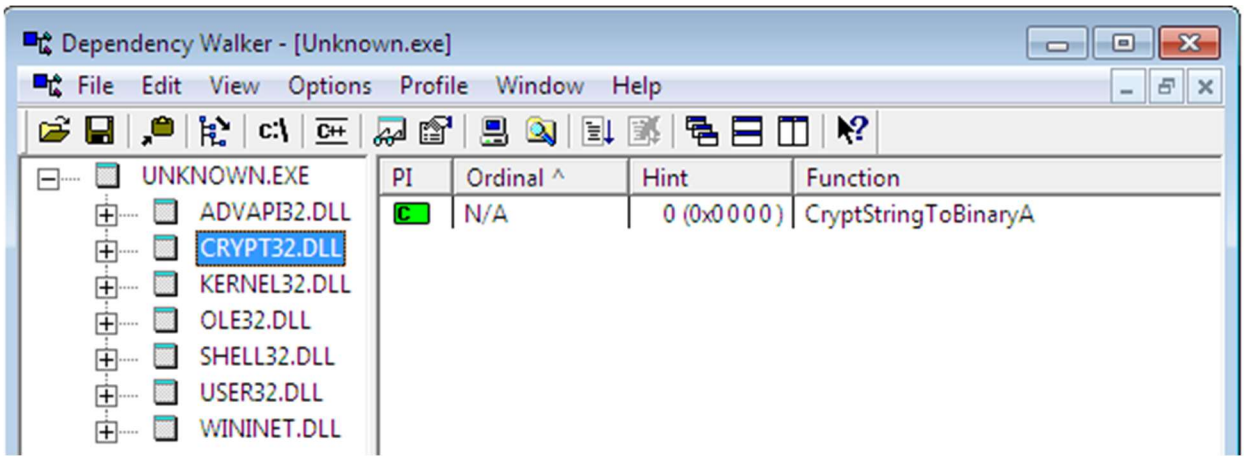


Image 14. Dependency Walker 2.2 Analysis03[135]

Conclusion: CRYPT32.dll imported and CryptStringToBinaryA function used.

[134] Taaffe, Jonathon [2019] *Image 13. Dependency Walker 2.2 Analysis02* [Created 2nd August 2019]
[135] Taaffe, Jonathon [2019] *Image 14. Dependency Walker 2.2 Analysis03* [Created 2nd August 2019]

Dependency Walker Analysis04

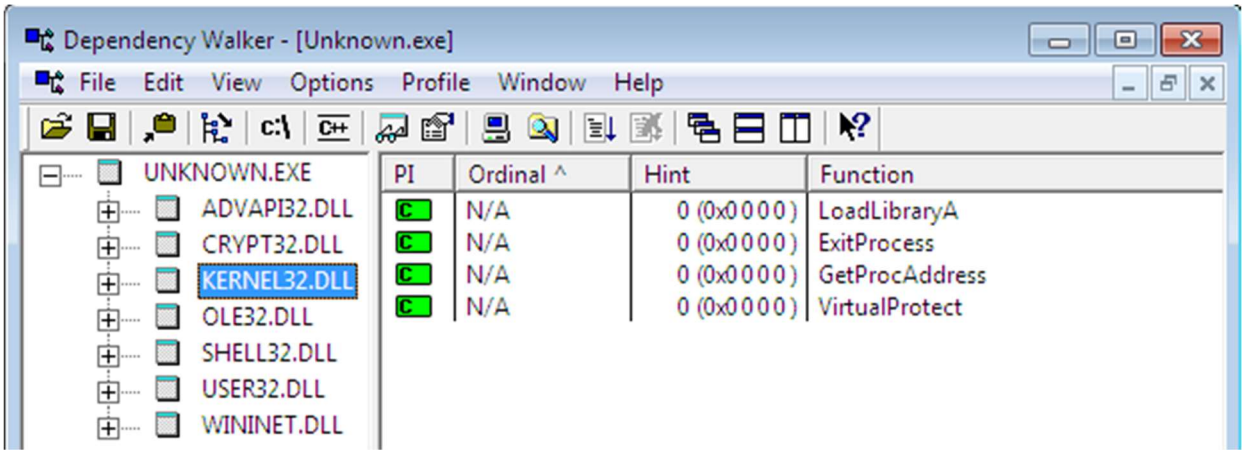


Image 15. Dependency Walker 2.2 Analysis04[136]

Conclusion: KERNEL32.DLL imported and the following functions are used:

- VirtualProtect
- LoadLibraryA
- ExitProcess
- GetProcAddress

Dependency Walker Analysis05

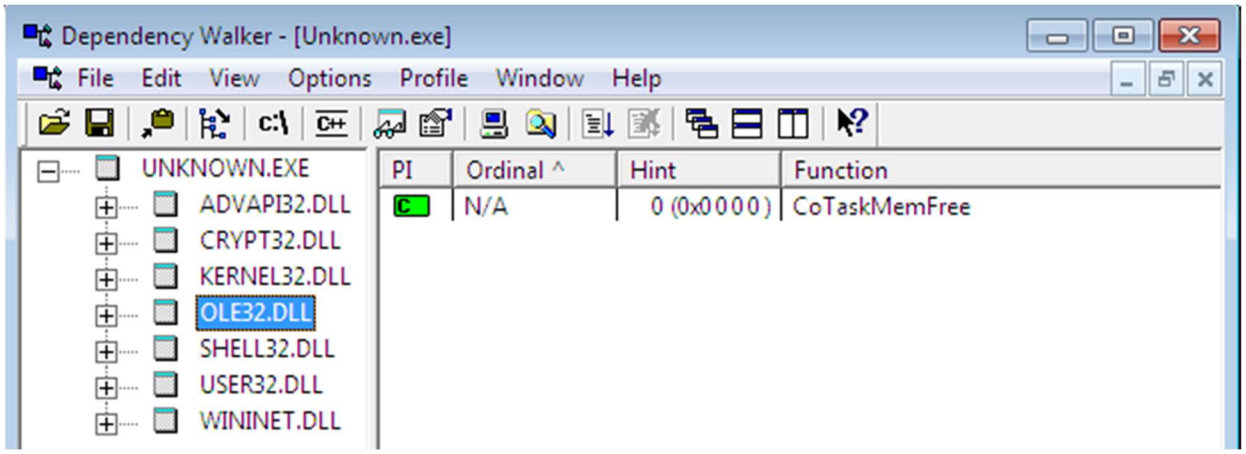


Image 16. Dependency Walker 2.2 Analysis05[137]

Conclusion: OLE32.dll imported and the CoTaskMemFree function used.

[136] Taaffe, Jonathon [2019] *Image 15. Dependency Walker 2.2 Analysis04* [Created 2nd August 2019]
[137] Taaffe, Jonathon [2019] *Image 16. Dependency Walker 2.2 Analysis05* [Created 2nd August 2019]

Dependency Walker Analysis06

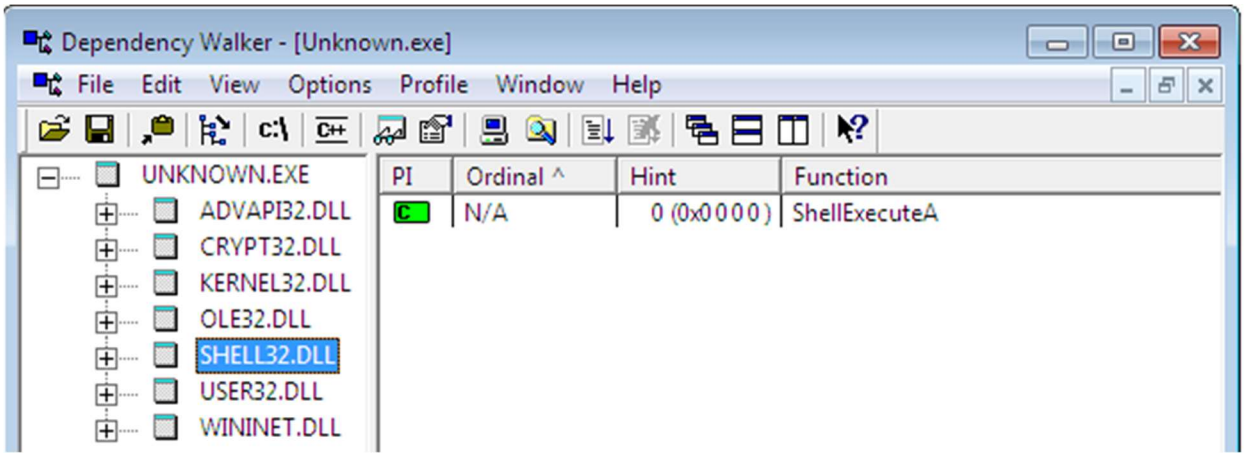


Image 17. Dependency Walker 2.2 Analysis06[138]

Conclusion: SHELL32.dll imported and the ShellExecuteA function used.

Dependency Walker Analysis07

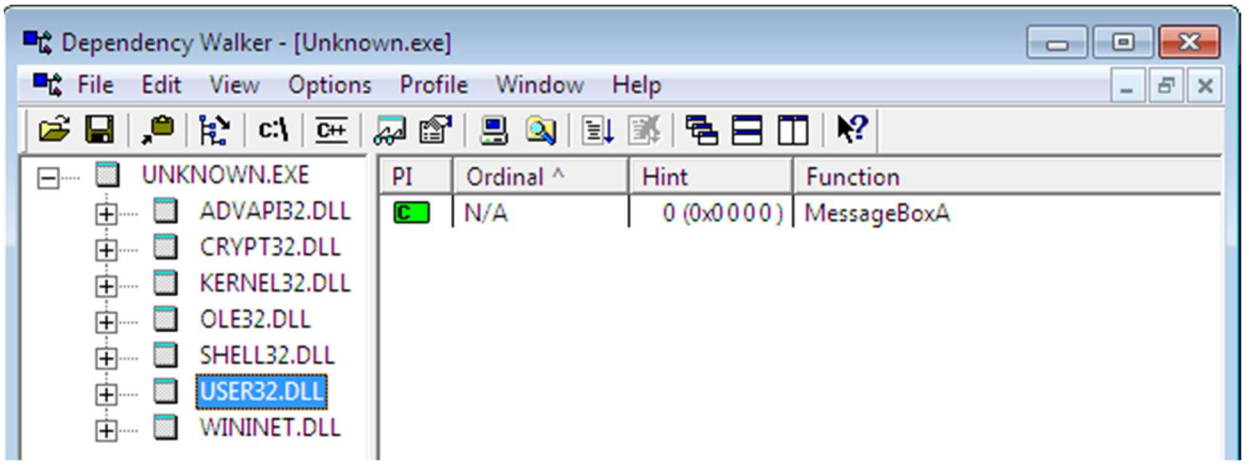
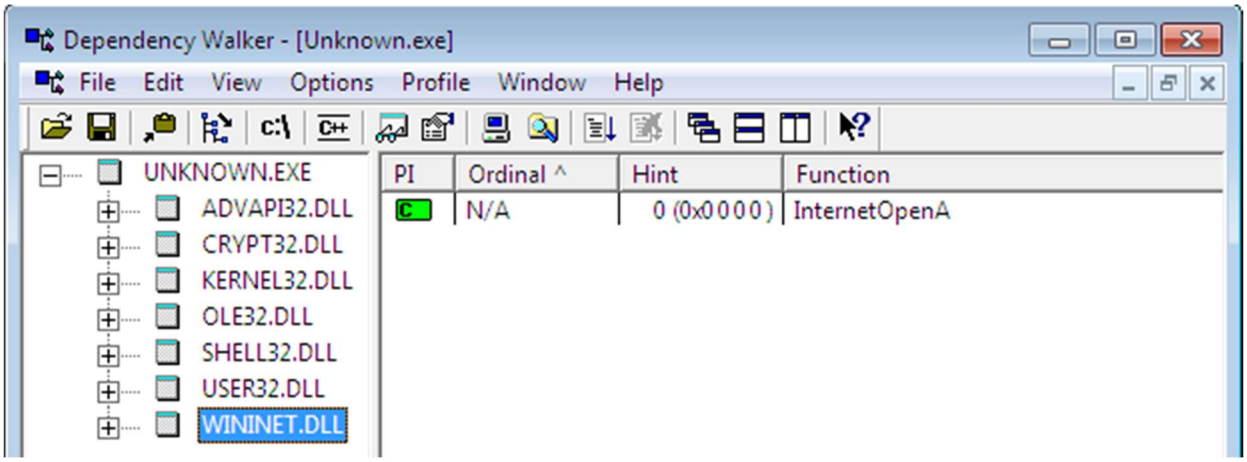


Image 18. Dependency Walker 2.2 Analysis07[139]

Conclusion: USER32.dll imported and the MessageBoxA function used.

[138] Taaffe, Jonathon [2019] *Image 17. Dependency Walker 2.2 Analysis06* [Created 2nd August 2019]
[139] Taaffe, Jonathon [2019] *Image 18. Dependency Walker 2.2 Analysis07* [Created 2nd August 2019]

Dependency Walker Analysis08



[140]**Image 19. Dependency Walker 2.2 Analysis08**

Conclusion: WININET.dll imported and the InternetOpenA function used.

[140] Taaffe, Jonathon [2019] *Image 19. Dependency Walker 2.2 Analysis08* [Created 2nd August 2019]

UPX 3.95[141] Unpacking

```
C:\Temp\MW_Analysis\UPX-3.95>upx.exe -d -o C:\Temp\Virus_Files\Unknown-Unpacked.
exe C:\Temp\Virus_Files\Unknown.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95w       Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    433152 <-    376832   87.00%    win32/pe     Unknown-Unpacked.exe

Unpacked 1 file.

C:\Temp\MW_Analysis\UPX-3.95>
```

Image 20. UPX Unpacking[142]

Conclusion: Unpacked Unknow.exe to a new file Unknown-Unpacked.exe for further analysis

PEiD[143] Post UPX Unpacking Analysis

File: Unknown-Unpacked.exe

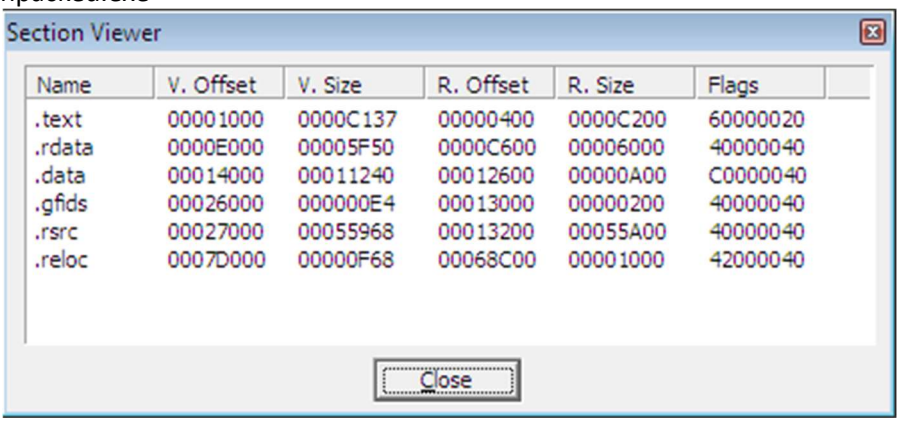


Image 21. PEiD Post UPX Unpacking Analysis[144]

Conclusion: Unpacking the file shows changes to the Resources Sections compared to the original PEiD Analysis (copy of screen shot below)

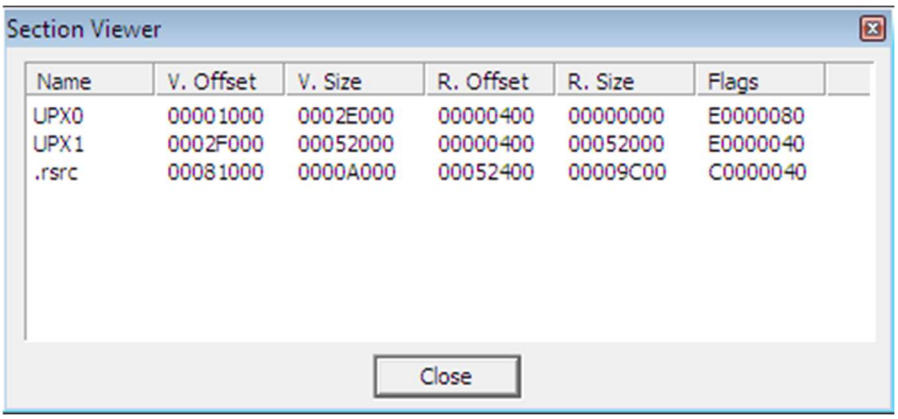


Image 22. PEiD Post UPX Unpacking Section Analysis[145]

[141] UPX Ultimate Packer for eXecutables [2019] *UPX 3.95* https://github.com/upx/upx/releases/tag/v3.95 [Accessed 2nd August 2019]
[142] Taaffe, Jonathon [2019] *Image 20. UPX Unpacking* [Created 2nd August 2019]
[143] Softpedia.com [2019] *PEiD 0.95* https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml [Accessed 2nd August 2019]
[144] Taaffe, Jonathon [2019] *Image 21. PEiD Post UPX Unpacking Section Analysis* [Created 2nd August 2019]
[145] Taaffe, Jonathon [2019] *Image 22. PEiD Post UPX Unpacking Section Analysis* [Created 2nd August 2019]

BinText Post UPX Unpacking Analysis

A BinText visual comparison of the 2 files shows that data was unpacked, uncompressed and/or unobfuscated when unpacked with UPX. Analysis as follows

File Position: 00000000C815
File1: Unknown.exe

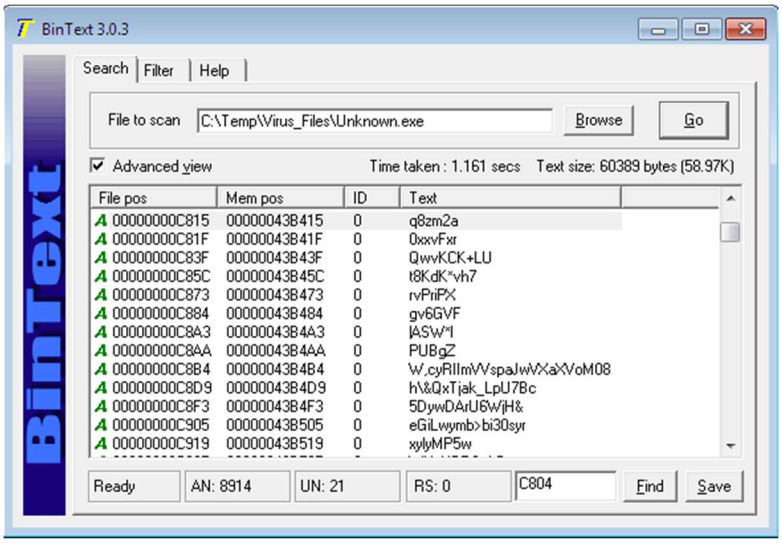


Image 23. BinText Post UPX Unpacking Analysis01[146]

File2: Unknown-Unpacked.exe

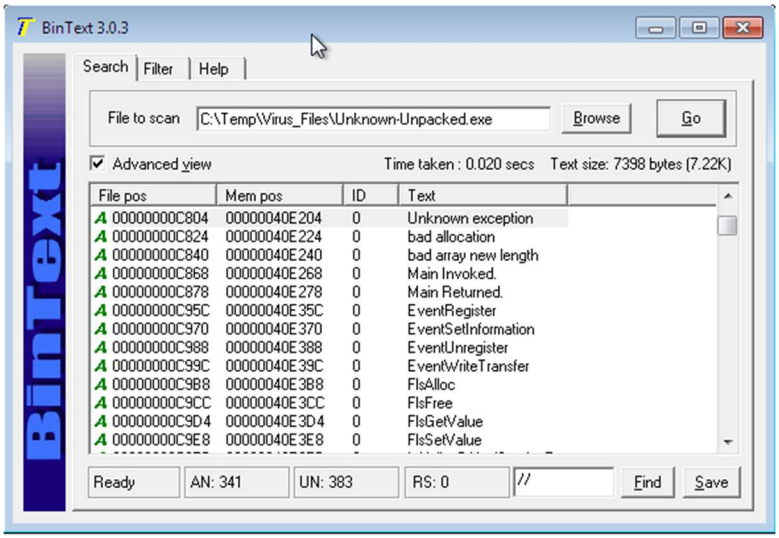


Image 24. BinText Post UPX Unpacking Analysis02[147]

[146] Taaffe, Jonathon [2019] *Image 23. BinText Post UPX Unpacking Analysis01* [Created 2nd August 2019]
[147] Taaffe, Jonathon [2019] Image 24. *BinText Post UPX Unpacking Analysis02* [Created 2nd August 2019]

File Position: 000000011108
File1: Unknown.exe

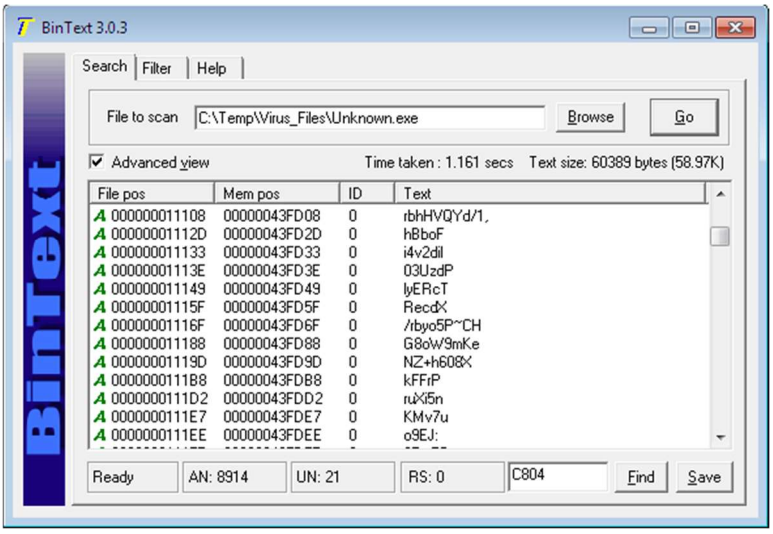


Image 25. BinText Post UPX Unpacking Analysis03[148]

File2: Unknown-Unpacked.exe

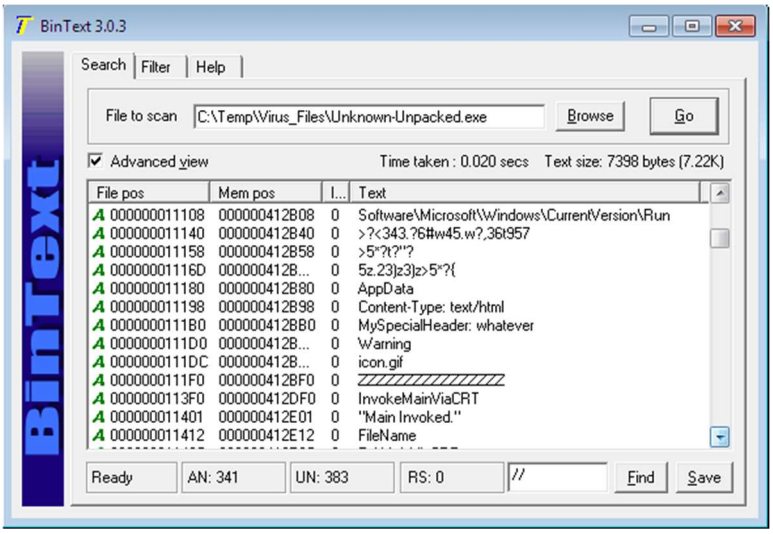


Image 26. BinText Post UPX Unpacking Analysis04[149]

Conclusion: Persistence Registry key visible - Software\Microsoft\Windows\CurrentVersion\Run

[148] Taaffe, Jonathon [2019] *Image 25. BinText Post UPX Unpacking Analysis03* [Created 2nd August 2019]
[149] Taaffe, Jonathon [2019] *Image 26. BinText Post UPX Unpacking Analysis04* [Created 2nd August 2019]

File Position: 000000011E1A
File1: Unknown.exe

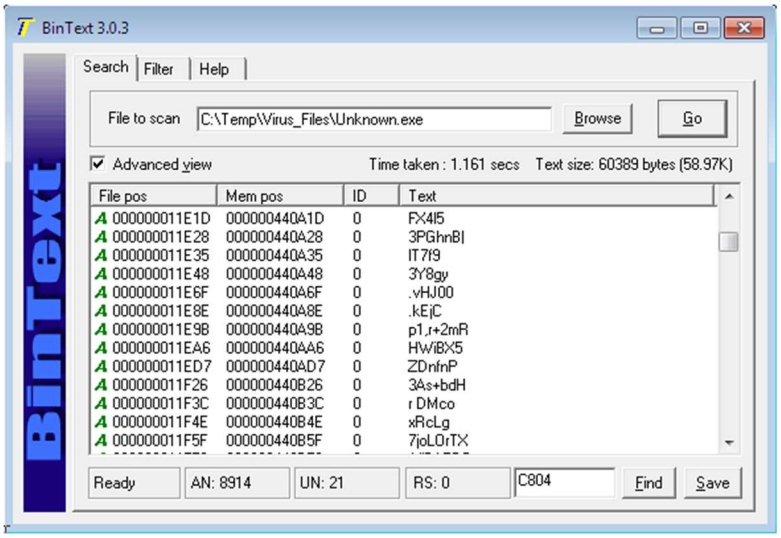


Image 27. BinText Post UPX Unpacking Analysis05[150]

File2: Unknown-Unpacked.exe

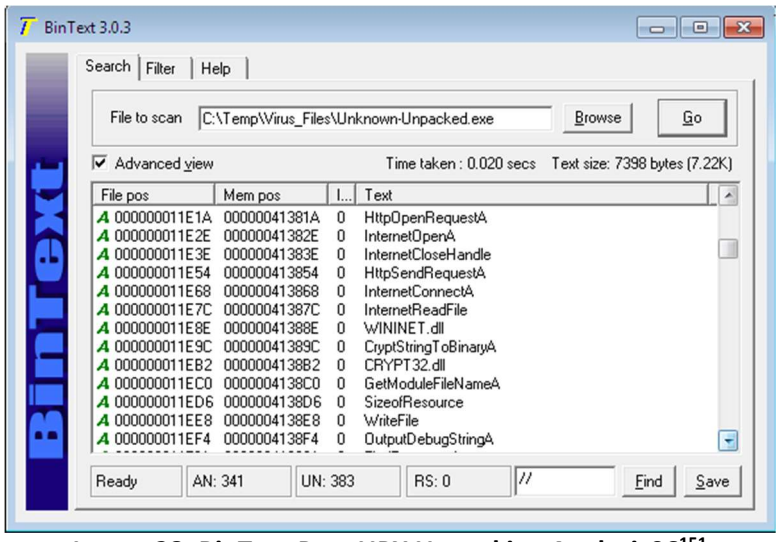


Image 28. BinText Post UPX Unpacking Analysis06[151]

Conclusion: Internet Connectivity configuration

[150] Taaffe, Jonathon [2019] *Image 27. BinText Post UPX Unpacking Analysis05* [Created 2nd August 2019]
[151] Taaffe, Jonathon [2019] *Image 28. BinText Post UPX Unpacking Analysis06* [Created 2nd August 2019]

File Position: 0000000C0FB
File1: Unknown.exe

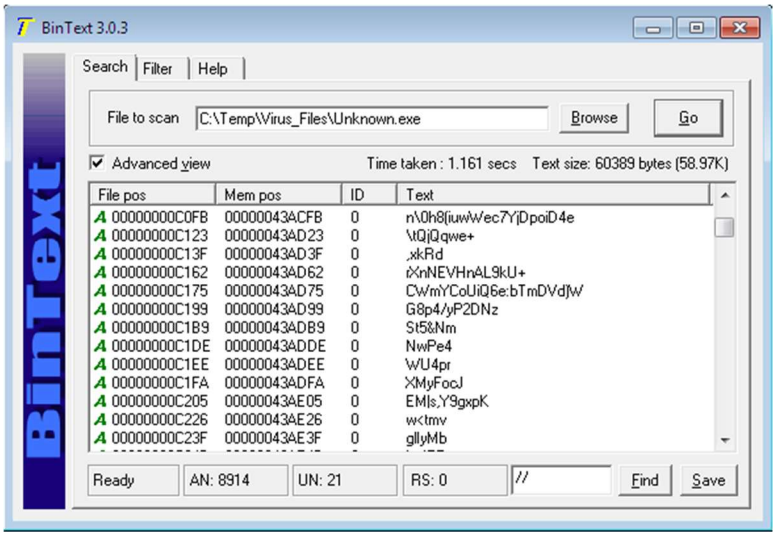


Image 29. BinText Post UPX Unpacking Analysis07[152]

File2: Unknown-Unpacked.exe

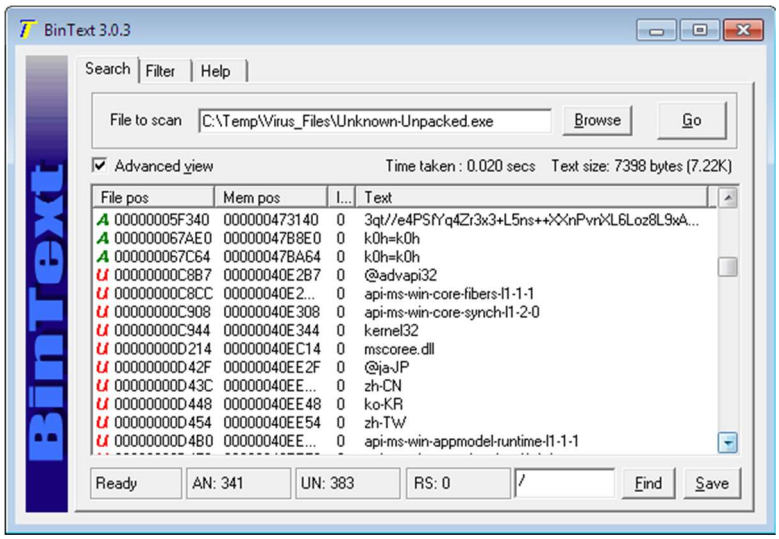


Image 30. BinText Post UPX Unpacking Analysis08[153]

Conclusion: Potentially the Internet address but encrypted/obfuscated.

[152] Taaffe, Jonathon [2019] *Image 29. BinText Post UPX Unpacking Analysis07* [Created 2nd August 2019]
[153] Taaffe, Jonathon [2019] *Image 30. BinText Post UPX Unpacking Analysis08* [Created 2nd August 2019]

IDA Pro[154] Analysis

New > PE Dynamic Library > OK > C:\Temp\Virus_Files\Unknown.exe > Open

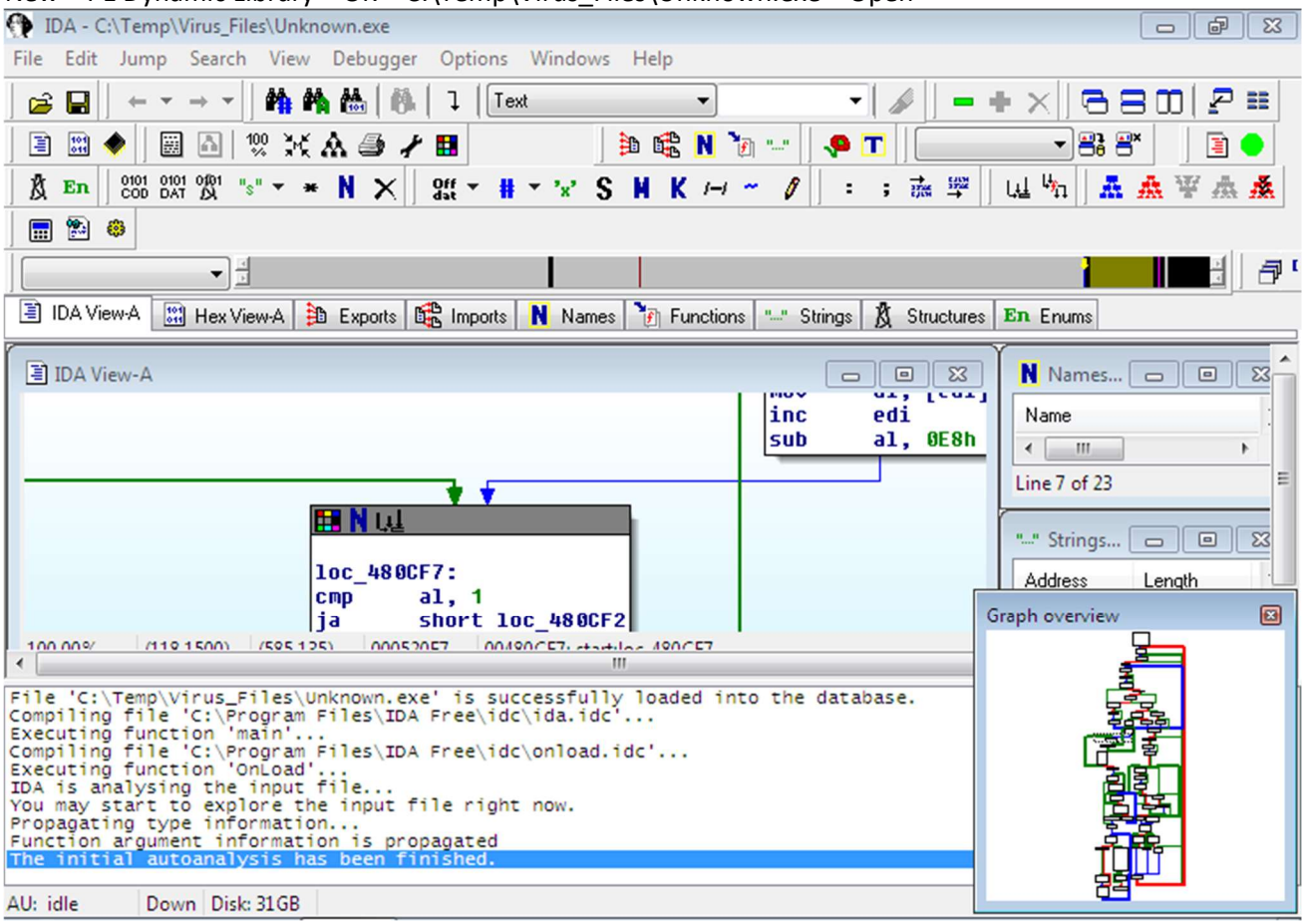


Image 31. IDA Pro Analysis[155]

IDA Pro Imports Section

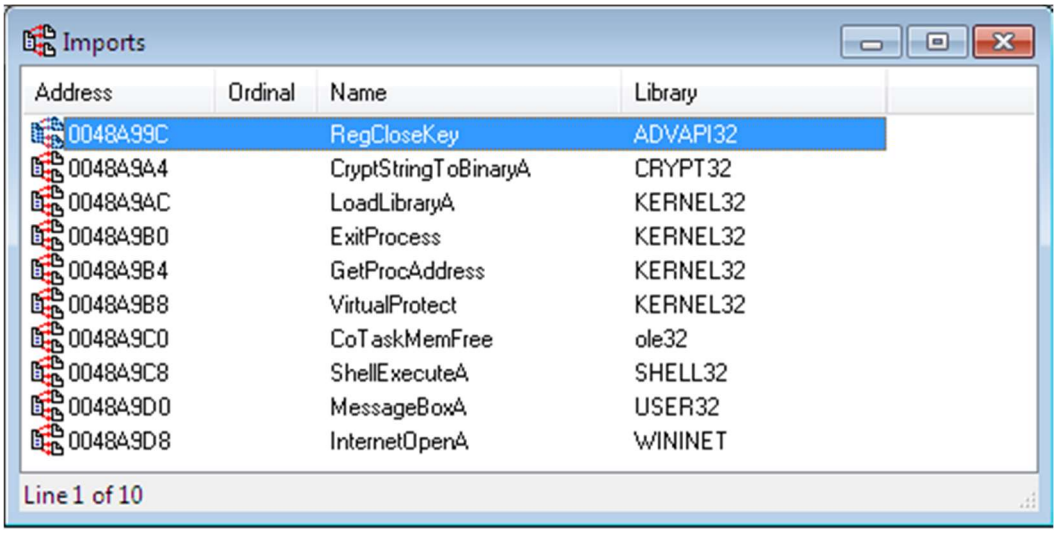


Image 32. IDA Pro Imports Section[156]

[154] Hex-Rays [2019] *IDA Freeware for Windows (48 MB)* https://www.hex-rays.com/products/ida/support/download_freeware.shtml [Accessed 2nd August 2019]

[155] Taaffe, Jonathon [2019] *Image 31. IDA Pro Analysis* [Created 2nd August 2019]

[156] Taaffe, Jonathon [2019] *Image 32. IDA Pro Imports Section* [Created 2nd August 2019]

IDA Pro Stings Section

IDA Pro > Windows > Strings > sort by String

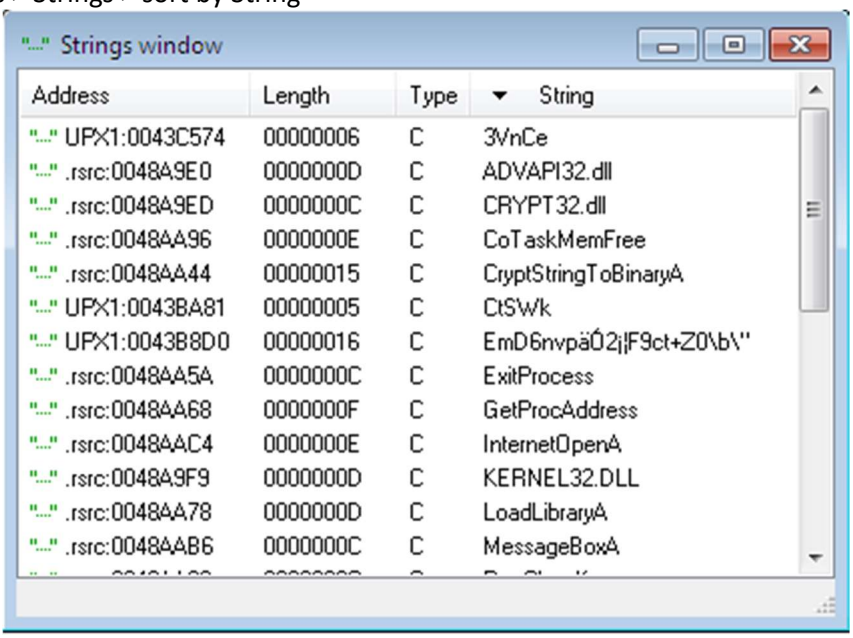


Image 33. IDA Pro Stings Section[157]

Double-clicked CRYPT32.DLL to view DLL load section in IDA-View A

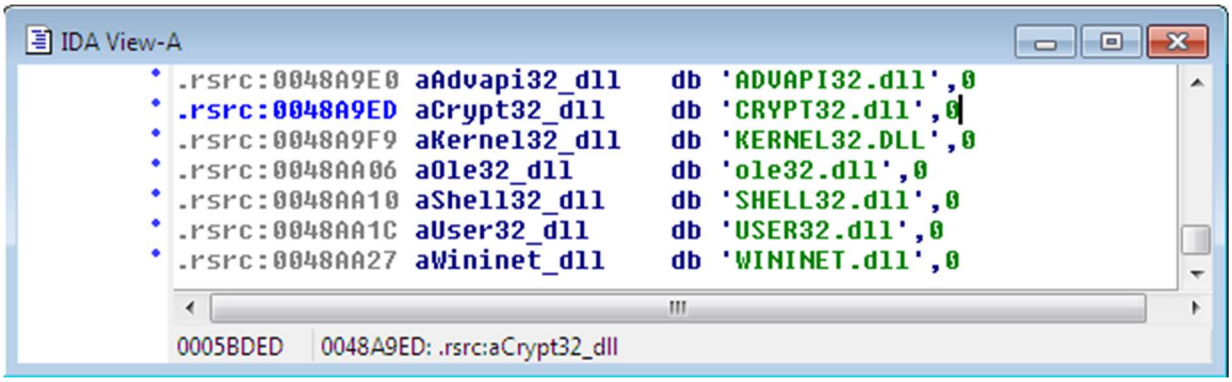


Image 34. IDA Pro CRYPT32.DLL DLL Load Section[158]

Conclusion: No further details relating to DLL's or functions loaded

[157] Taaffe, Jonathon [2019] *Image 33. IDA Pro Stings Section* [Created 2nd August 2019]
[158] Taaffe, Jonathon [2019] *Image 34. IDA Pro CRYPT32.DLL DLL Load Section* [Created 2nd August 2019]

Resource Hacker 5.1.7[159] Analysis

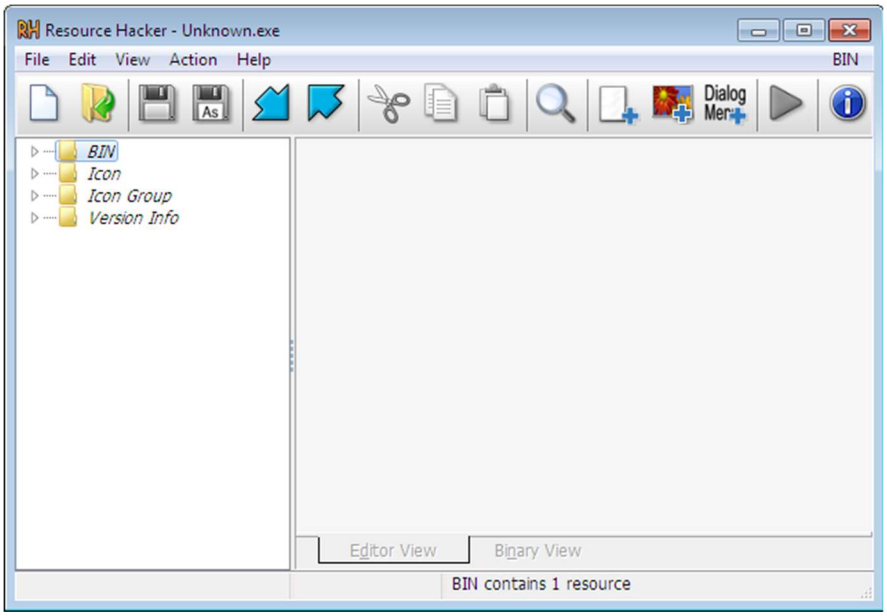


Image 35. Resource Hacker Analysis01[160]

Conclusion: No data viewable in BIN\101 : 1033

Resource Hacker Analysis02

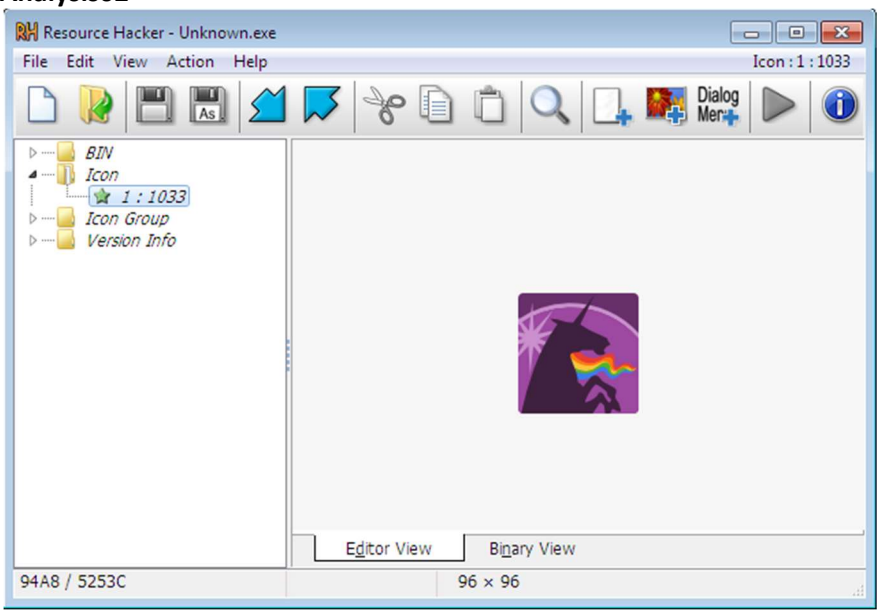


Image 36. Resource Hacker Analysis02[161]

Conclusion: Icon image for 'rainbowmagic.exe' displayed in Icon\ 1 : 1033

[159] Resource Hacker [2019] *Resource Hacker 5.1.7* http://www.angusj.com/resourcehacker/ [Accessed 2nd August 2019]
[160] Taaffe, Jonathon [2019] *Image 35. Resource Hacker Analysis01* [Created 2nd August 2019]
[161] Taaffe, Jonathon [2019] *Image 36. Resource Hacker Analysis02* [Created 2nd August 2019]

Resource Hacker Analysis03

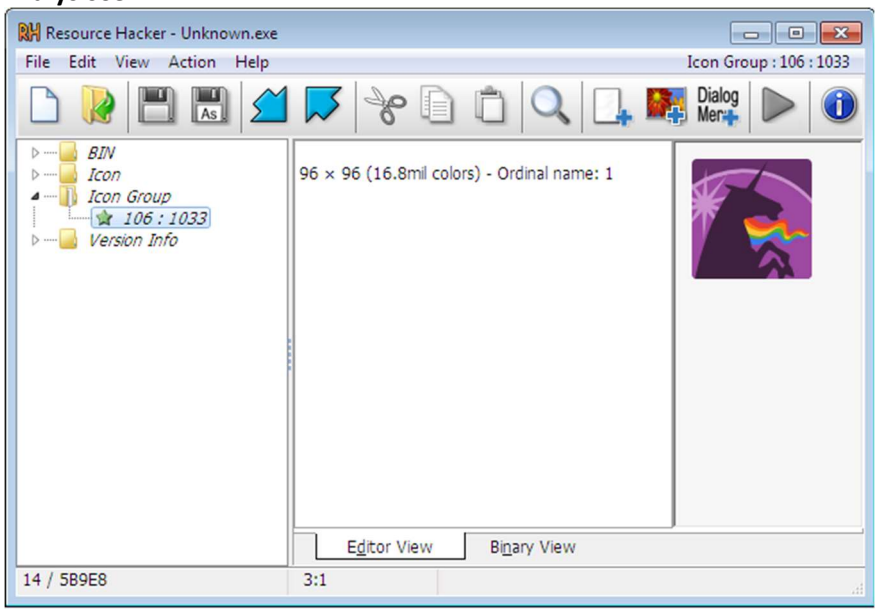


Image 37. Resource Hacker Analysis03[162]

Conclusion: Additional information on the icon image for 'rainbowmagic.exe' displayed in Icon\ 106 : 1033

Resource Hacker Analysis04

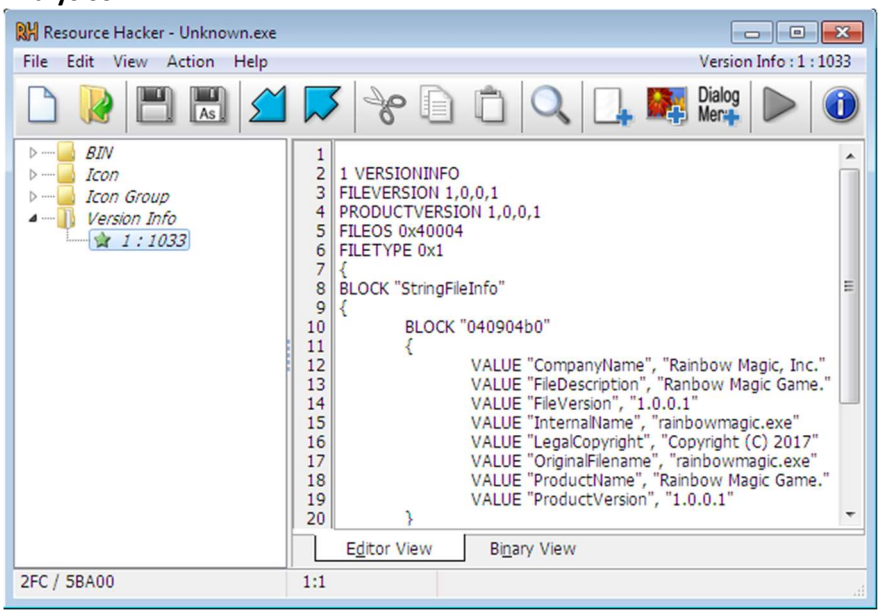


Image 38. Resource Hacker Analysis04[163]

Conclusion: File information but no additional information

[162] Taaffe, Jonathon [2019] *Image 37. Resource Hacker Analysis03* [Created 2nd August 2019]
[163] Taaffe, Jonathon [2019] *Image 38. Resource Hacker Analysis04* [Created 2nd August 2019]

Dynamic Malware Analysis

This section documents the dynamic analysis performed against the malware sample in the isolated VirtualBox VM environment.

Important Note: In preparation for this dynamic analysis of this malware sample the following precautions have been taken:

1. All malware analysis tools copied to the Windows 7 Analysis Client
2. Malware sample copied to the Windows 7 Analysis Client
3. Shared Folders: Disabled
4. Drag' n 'Drop: Disabled
5. Shared Clipboard: Disabled
6. Disabled network adapter 1 connected to Windows 7 Analysis Client
7. Cloned the Windows 7 Analysis Client
8. Powered off the Windows 2016 File Server

Malware Sample File Location: C:\Temp\Virus_Files\Unknown.exe

SysInternals Process Monitor[164]

Configuration: Open Process Monitor > click Filter > click Reset Filter
Click Filter > then Filter and set the following

- Filter for: Process Name
- Condition: is
- Filter:Unknown.exe

Click Add

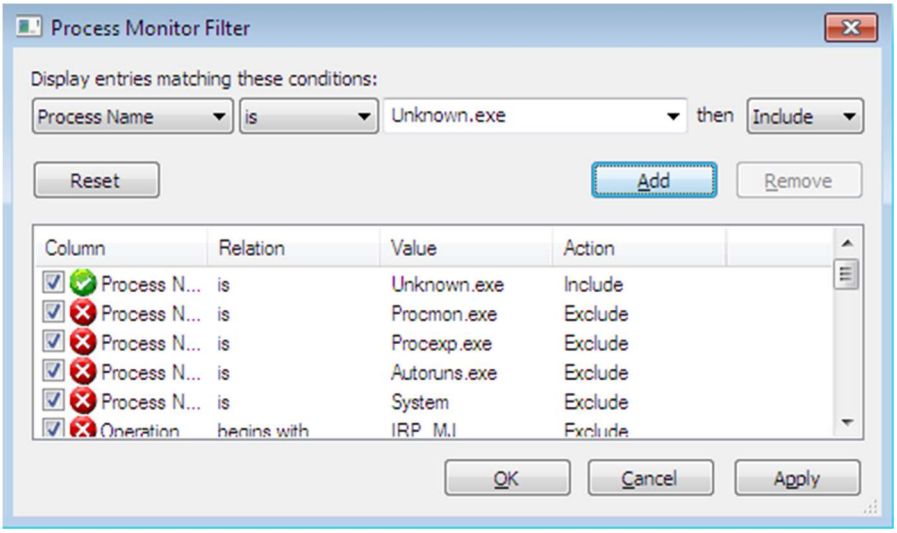


Image 39. Process Monitor Filter[165]

VM Snapshot: Prior to running Unknown.exe a VM Snapshot named 'Snapshot 1' was taken

[164] Microsoft.com [2019] *Process Monitor v3.52* https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon [Accessed 2nd August 2019]
[165] Taaffe, Jonathon [2019] *Image 39. Process Monitor Filter* [Created 2nd August 2019]

CAUTION: Execution of Unknown.exe Malware Sample

Important: Ensure 'Snapshot 1' has successfully completed prior to proceeding

File Location: C:\Temp\Virus_Files\Unknown.exe

Initial Observations

1. Multiple new entries were recorded in Process Monitor.
2. Changes were bring made to the Registry, File System, Processes and Threads.
3. No network activity reported as the Malware Analysis Client did not have a network adapter connected
4. Full capture of the event using the filter above saved to:

   C:\Temp\MW_Analysis\Unknown_ProcessMonitor_Logfile01.CSV

Process Monitor

Initial Process Monitor Screen Filtered for Process: Unknown.exe

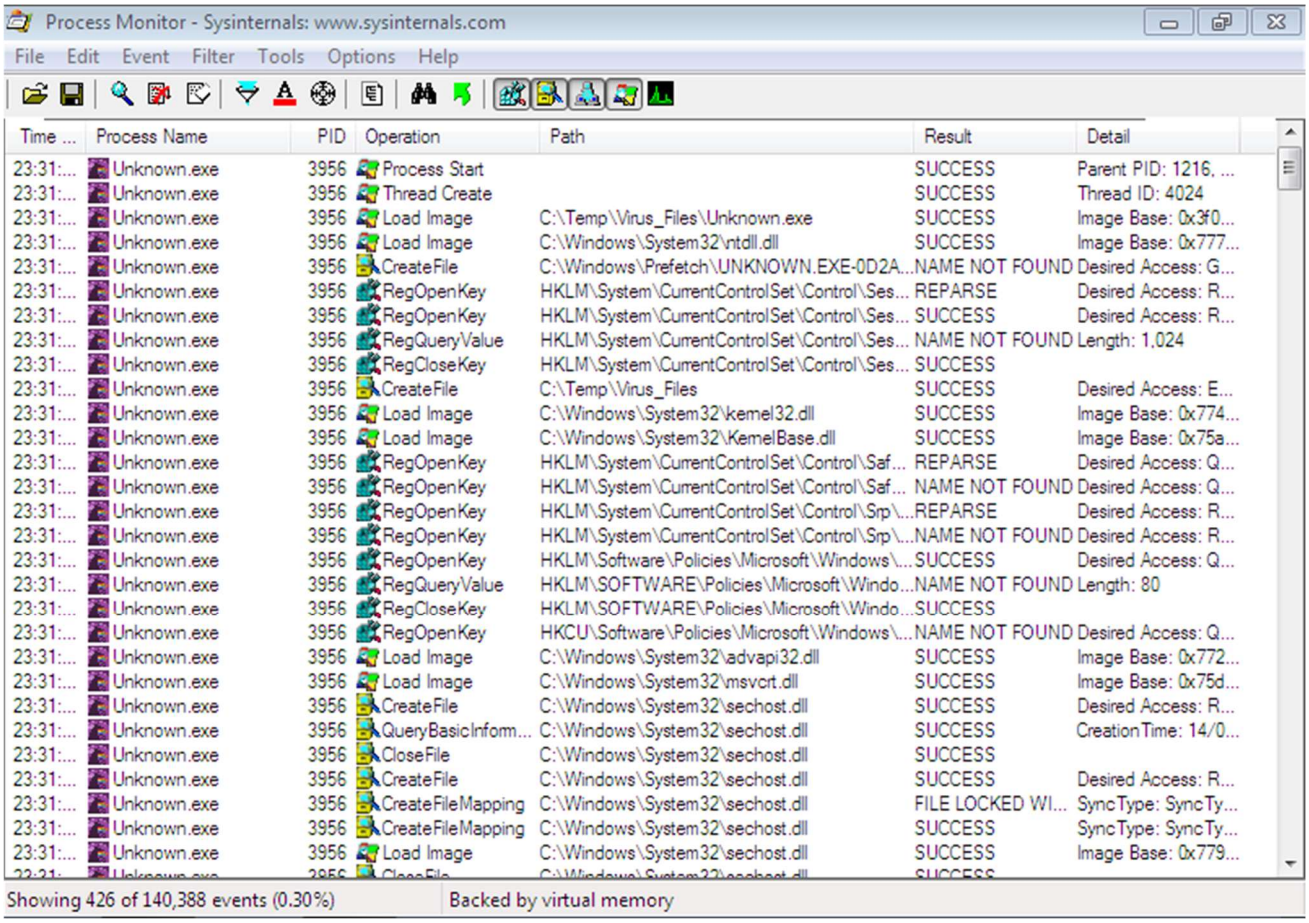


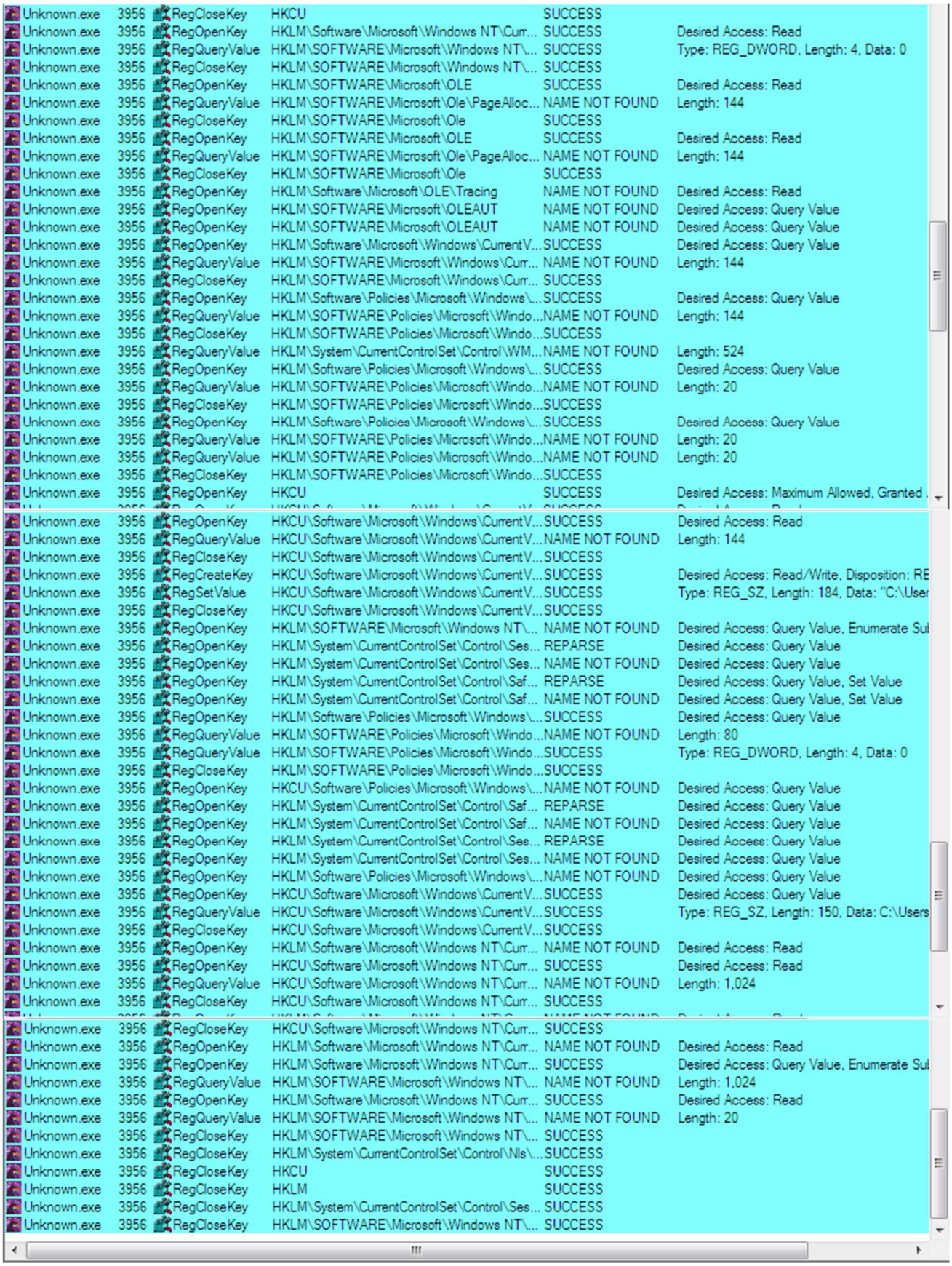
Image 40. Process Monitor[166]

[166] Taaffe, Jonathon [2019] *Image 40. Process Monitor* [Created 2nd August 2019]

Process Monitor - Registry Activity Results

Note: Screen shots of Process Monitor as the Malware Analysis Client is completely isolated

Process Name	PID	Operation	Path	Result	Detail
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	REPARSE	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\System\CurrentControlSet\Control\Ses...	NAME NOT FOUND	Length: 1,024
Unknown.exe	3956	RegCloseKey	HKLM\System\CurrentControlSet\Control\Ses...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	REPARSE	Desired Access: Query Value, Set Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	NAME NOT FOUND	Desired Access: Query Value, Set Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\...	REPARSE	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 80
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\...	REPARSE	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\...	SUCCESS	Type: REG_SZ, Length: 36, Data: 00060101
Unknown.exe	3956	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\...	REPARSE	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Services\cr...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\System\CurrentControlSet\services\cry...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKLM\System\CurrentControlSet\services\cry...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	REPARSE	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\System\CurrentControlSet\Control\Ses...	NAME NOT FOUND	Length: 16
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Erro...	REPARSE	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Erro...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND	Length: 172
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted
Unknown.exe	3956	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached\M...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegCloseKey	HKCU	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Setti...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted
Unknown.exe	3956	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Pa...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU\Control Panel\Desktop\LanguageConfi...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegEnumValue	HKCU\Control Panel\Desktop\LanguageConfi...	NO MORE ENTRIES	Index: 0, Length: 512
Unknown.exe	3956	RegCloseKey	HKCU\Control Panel\Desktop\LanguageConfi...	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKCU	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Setti...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted
Unknown.exe	3956	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Pa...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKCU\Control Panel\Desktop\PreferredUILan...	NAME NOT FOUND	Length: 12
Unknown.exe	3956	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKCU	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\MUI\Setti...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted
Unknown.exe	3956	RegOpenKey	HKCU\Control Panel\Desktop\MuiCached	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\M...	BUFFER OVERFLOW	Length: 12
Unknown.exe	3956	RegQueryValue	HKCU\Control Panel\Desktop\MuiCached\M...	SUCCESS	Type: REG_MULTI_SZ, Length: 12, Data: er
Unknown.exe	3956	RegCloseKey	HKCU\Control Panel\Desktop\MuiCached	SUCCESS	



Unknown.exe	3956	RegCloseKey	HKCU	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\PageAlloc...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLE	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\PageAlloc...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\OLE\Tracing	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLEAUT	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\SOFTWARE\Microsoft\OLEAUT	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentV...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\Curr...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\Curr...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	
Unknown.exe	3956	RegQueryValue	HKLM\System\CurrentControlSet\Control\WM...	NAME NOT FOUND	Length: 524
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 20
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 20
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 20
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed, Granted ...
Unknown.exe	3956	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentV...	NAME NOT FOUND	Length: 144
Unknown.exe	3956	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	
Unknown.exe	3956	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	Desired Access: Read/Write, Disposition: RE
Unknown.exe	3956	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	Type: REG_SZ, Length: 184, Data: "C:\User
Unknown.exe	3956	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	REPARSE	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	REPARSE	Desired Access: Query Value, Set Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	NAME NOT FOUND	Desired Access: Query Value, Set Value
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	NAME NOT FOUND	Length: 80
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windo...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	REPARSE	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Saf...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	REPARSE	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ses...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\...	NAME NOT FOUND	Desired Access: Query Value
Unknown.exe	3956	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	Desired Access: Query Value
Unknown.exe	3956	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	Type: REG_SZ, Length: 150, Data: C:\Users
Unknown.exe	3956	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentV...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKCU\Software\Microsoft\Windows NT\Curr...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKCU\Software\Microsoft\Windows NT\Curr...	NAME NOT FOUND	Length: 1,024
Unknown.exe	3956	RegCloseKey	HKCU\Software\Microsoft\Windows NT\Curr...	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKCU\Software\Microsoft\Windows NT\Curr...	SUCCESS	
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NAME NOT FOUND	Desired Access: Read
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Desired Access: Query Value, Enumerate Sub
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND	Length: 1,024
Unknown.exe	3956	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Desired Access: Read
Unknown.exe	3956	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND	Length: 20
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\...	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKCU	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKLM	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKLM\System\CurrentControlSet\Control\Ses...	SUCCESS	
Unknown.exe	3956	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	

Image 41. Registry Activity Results [167]

[167] Taaffe, Jonathon [2019] *Image 41. Registry Activity Results* [Created 2nd August 2019]

Process and Tree Activity Results

Note: Screen shots of Process Monitor as the Analysis Client is completely isolated

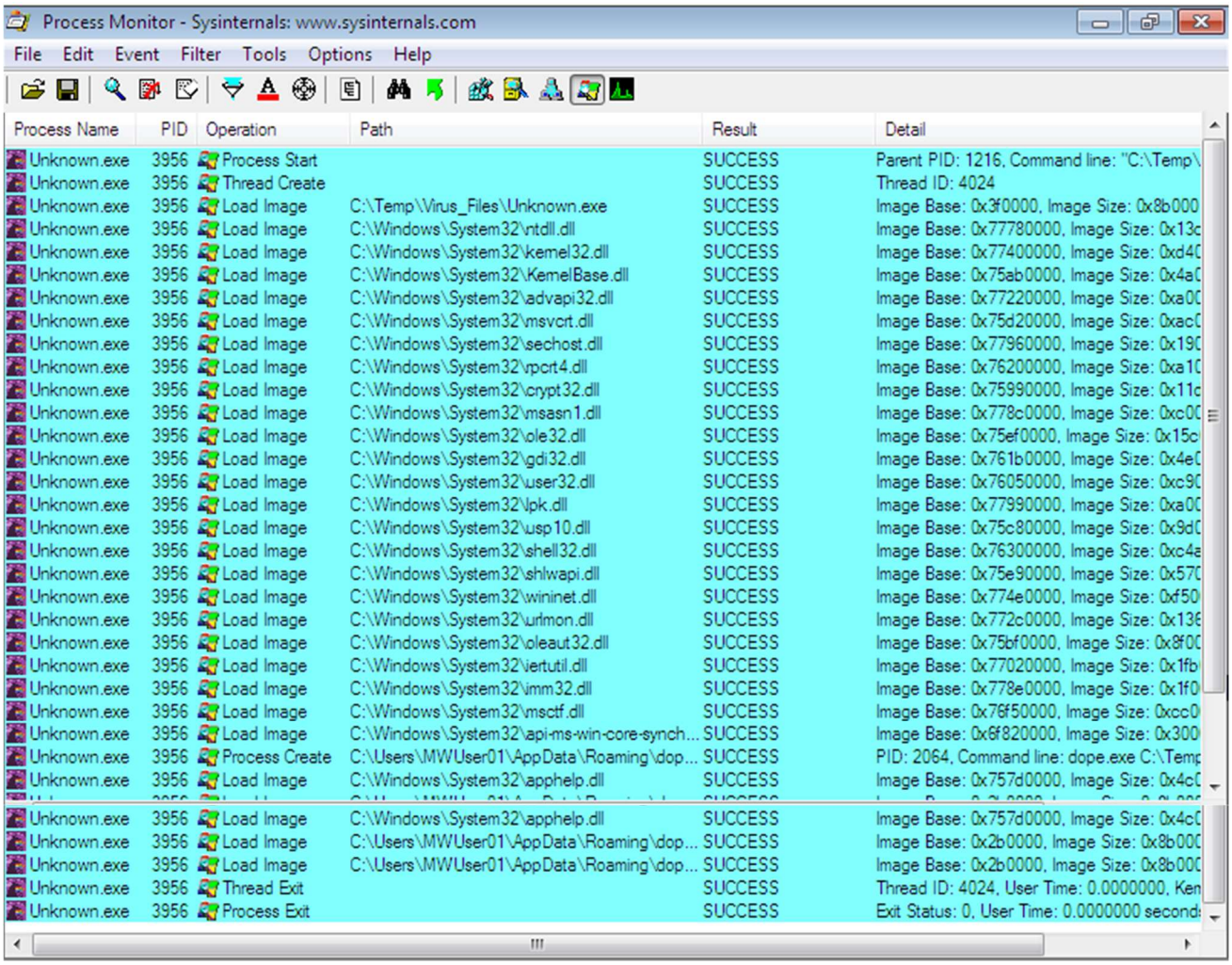


Image 42. Process and Tree Activity Results[168]

[168] Taaffe, Jonathon [2019] *Image 42. Process and Tree Activity Results* [Created 2nd August 2019]

Process Monitor Analysis
The Process Monitor log file C:\Temp\MW_Analysis\Unknown_ProcessMonitor_Logfile01.CSV was copied from the Analysis VM to the local host for analysis ensuring to virus scan the file prior to opening.

The Process monitor log file has a total of 427-line entries and took just under 1 second to complete all actions. The detailed log file is attached below for reference.

Unknown.exe Operations Summary
Below is a summary of the actions Unknown.exe took after being executed

Operation	Path	Description
Process Start		System and User environment information accessed
Load Image	C:\Temp\Virus_Files\Unknown.exe	Imaged loaded into memory
Load Image	C:\Windows\System32\ntdll.dll	DLL Imported
RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	Registry key read
CreateFile	C:\Temp\Virus_Files	Created file to confirm permissions
Load Image	C:\Windows\System32\kernel32.dll	DLL Imported
Load Image	C:\Windows\System32\KernelBase.dll	DLL Imported
RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	Registry key read
Load Image	C:\Windows\System32\advapi32.dll	DLL Imported
Load Image	C:\Windows\System32\msvcrt.dll	DLL Imported
CreateFile	C:\Windows\System32\sechost.dll	File created for malware to function
Load Image	C:\Windows\System32\rpcrt4.dll	DLL Imported
Load Image	C:\Windows\System32\crypt32.dll	DLL Imported
Load Image	C:\Windows\System32\msasn1.dll	DLL Imported
Load Image	C:\Windows\System32\ole32.dll	DLL Imported
Load Image	C:\Windows\System32\gdi32.dll	DLL Imported
Load Image	C:\Windows\System32\user32.dll	DLL Imported
Load Image	C:\Windows\System32\lpk.dll	DLL Imported
Load Image	C:\Windows\System32\usp10.dll	DLL Imported
Load Image	C:\Windows\System32\shell32.dll	DLL Imported
Load Image	C:\Windows\System32\shlwapi.dll	DLL Imported
Load Image	C:\Windows\System32\wininet.dll	DLL Imported
Load Image	C:\Windows\System32\urlmon.dll	DLL Imported
Load Image	C:\Windows\System32\oleaut32.dll	DLL Imported
Load Image	C:\Windows\System32\iertutil.dll	DLL Imported
RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	Registry key read
CreateFile	C:\Windows\System32\imm32.dll	File created for malware to function
Load Image	C:\Windows\System32\msctf.dll	DLL Imported

CreateFile	C:\Windows\System32\api-ms-win-core-synch-l1-2-0.dll	File created for malware to function
CreateFile	C:\Users\MWUser01\AppData\Roaming\dope.exe	File created for malware to function
WriteFile	C:\Users\MWUser01\AppData\Roaming\dope.exe	Data written to created file
RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Persistence configured in registry
CreateFile	C:\Users\MWUser01\AppData\Roaming	Persistence configured in file system
QueryNetworkOpenInformationFile	C:\Program Files\Common Files\Oracle\Java\javapath	Network configuration check
Process Exit		End of process
RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	Registry keys closed
RegCloseKey	HKCU	Registry keys closed
RegCloseKey	HKLM	Registry keys closed
RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	Registry keys closed
RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Registry keys closed

Table 29. Unknown.exe Operations Summary[169]

[169] Taaffe, Jonathon [2019] *Table 29. Unknown.exe Operations Summary* [Created 2nd August 2019]

Process Explorer

Files Created Summary

Below is a list of the files Unknown.exe created

C:\Users\MWUser01\AppData\Roaming\dope.exe
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\api-ms-win-core-synch-l1-2-0.dll
C:\Windows\System32\apphelp.dll
C:\Windows\System32\imm32.dll
C:\Windows\System32\sechost.dll
C:\Program Files\Common Files\Oracle\Java\javapath_target_5829021\
api-ms-win-appmodel-runtime-l1-1-1.DLL
api-ms-win-core-fibers-l1-1-1.DLL
api-ms-win-core-localization-l1-2-1.DLL
ext-ms-win-kernel32-package-current-l1-1-0.DLL

DLL's Imported Summary

Below is a list of the DLL's Unknown.exe imported to function:

Section	Content	Page
Malware Identification	Table 2. Virus Total Unknown.exe Imports	7
Static Malware Analysis	Image 6. SECTION .rsrc – IMPORT Directory Table	38

DLL's Imported Summary

Imaged Loaded	DLL
C:\Temp\Virus_Files\Unknown.exe	
C:\Users\MWUser01\AppData\Roaming\dope.exe	
C:\Windows\System32\advapi32.dll	ADVAPI32.dll
C:\Windows\System32\api-ms-win-core-synch-l1-2-0.dll	
C:\Windows\System32\apphelp.dll	
C:\Windows\System32\crypt32.dll	CRYPT32.dll
C:\Windows\System32\gdi32.dll	
C:\Windows\System32\iertutil.dll	
C:\Windows\System32\imm32.dll	
C:\Windows\System32\kernel32.dll	KERNEL32.DLL
C:\Windows\System32\KernelBase.dll	
C:\Windows\System32\lpk.dll	
C:\Windows\System32\msasn1.dll	
C:\Windows\System32\msctf.dll	
C:\Windows\System32\msvcrt.dll	
C:\Windows\System32\ntdll.dll	
C:\Windows\System32\ole32.dll	OLE32.dll
C:\Windows\System32\oleaut32.dll	
C:\Windows\System32\rpcrt4.dll	
C:\Windows\System32\sechost.dll	
C:\Windows\System32\shell32.dll	SHELL32.dll
C:\Windows\System32\shlwapi.dll	

C:\Windows\System32\urlmon.dll	
C:\Windows\System32\user32.dll	USER32.dll
C:\Windows\System32\usp10.dll	
C:\Windows\System32\wininet.dll	WININET.dll

Table 30. DLL's Imported Summary[170]

Process Explorer – Process Created
Unknown.exe created and started the following single process:

Path: C:\Users\MWUser01\AppData\Roaming\dope.exe
Command line: dope.exe C:\Temp\Virus_Files\Unknown.exe

Process Explorer – Persistence Configuration
Unknown.exe created the following registry key with the following registry value to ensure persistence:

Registry Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Registry Key Value:
Type: REG_SZ
Length: 184
Data: "C:\Users\MWUser01\AppData\Roaming\dope.exe"

Conclusion: The information gathered during Malware Identification and Malware Static Analysis has been validated after Dynamic Analysis.

[170] Taaffe, Jonathon [2019] *Table 30. DLL's Imported Summary* [Created 2nd August 2019]

Network Traffic Analysis

So far in this report an extensive Malware Identification, Static Analysis and Dynamic Analysis actions have been performed. The following section includes a full Dynamic Analysis including Network traffic investigation.

As documented in the Malware Analysis Lab Setup section, the following has been configured:

- Isolated Internal Network 'malware-analysis-network01
- Windows7 Analysis Client with all required Tools and Malware Sample copied

The following Malware Analysis Utility VM's have also been configured:

- Gateway OS – REMnux
- FakeNet-NG
- iNetSim

For Network Traffic Analysis, iNetSim will be used to:

- Simulate network services including HTTP and DNS
- Gather all network traffic from the Windows 7 Analysis client

Network Configuration

The following diagram shows the Dynamic Analysis network Configuration:

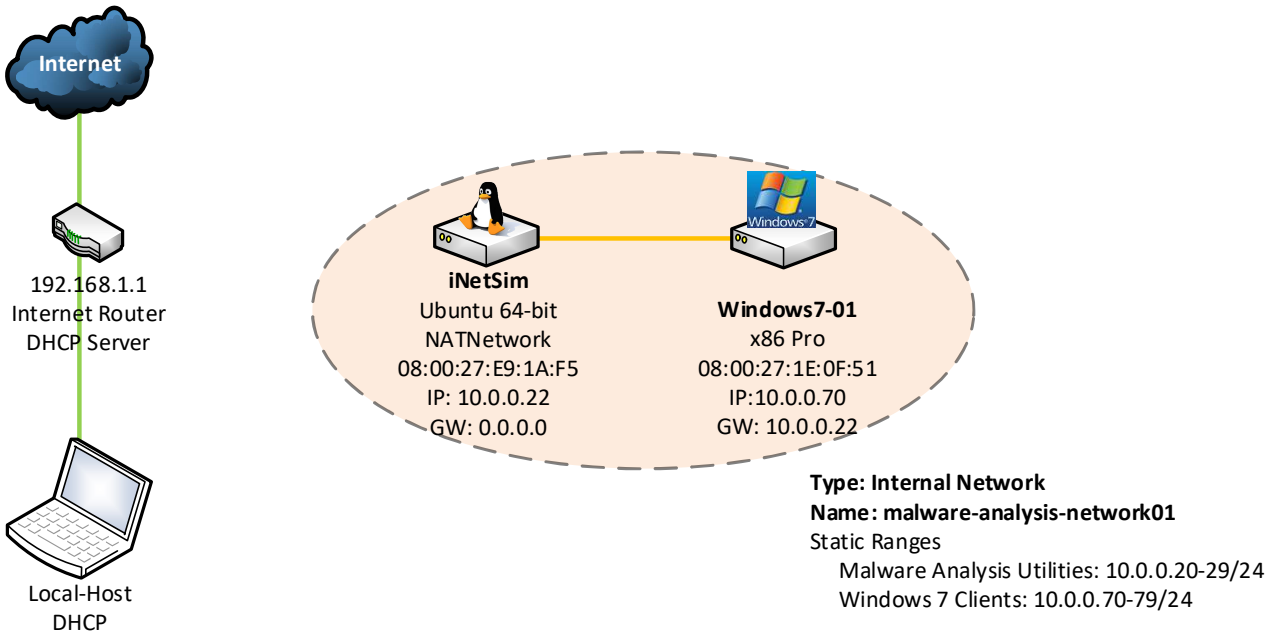


Diagram 6. Dynamic Analysis Network Configuration[171]

[171] Taaffe, Jonathon [2019] *Diagram 6. Lab 1 Phase 6 Dynamic Malware Analysis Configuration* [Created 2nd August 2019]

iNetSim Configuration[172]

iNetSim VM is configured with a static IP address of 10.0.0.22 and is configured to the use the following directory and file locations:

```
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
```

To start iNetSim run `inetsim` from the `/etc/inetsim` directory

Windows7 Analysis VM Configuration

The Windows 7 Analysis VM has also been configured with a static IP address of 10.0.0.70 and it's Gateway IP address is configured as 10.0.0.22 (iNetSim static IP).

Connectivity from Windows 7 VM to iNetSim Network Services

Network ping from Windows 7 (10.0.0.70) to iNetSim VM (10.0.0.22) : OK
Network ping from iNetSim VM (10.0.0.22) to Windows 7 (10.0.0.70) : OK

Starting iNetSim

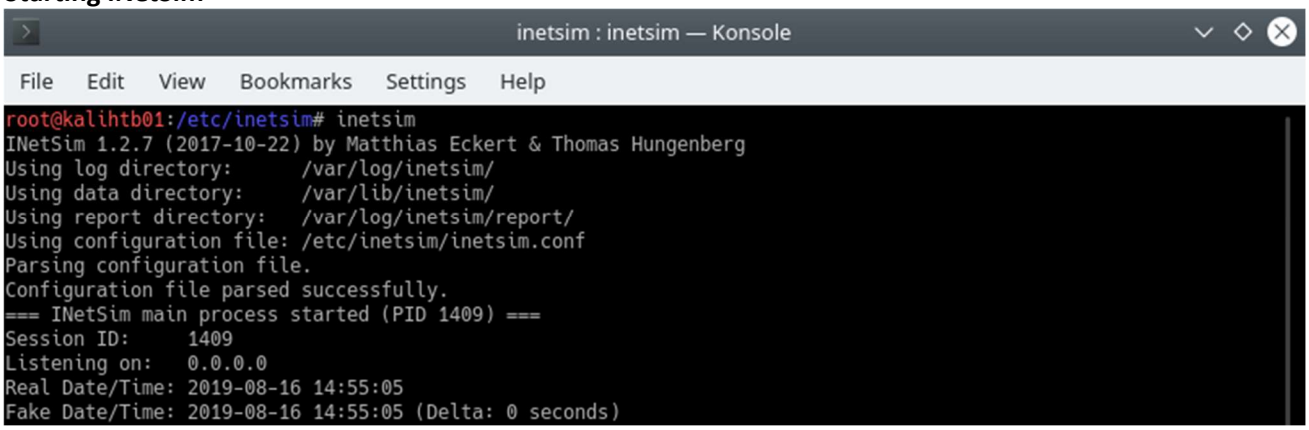


Image 43. Starting iNetSim[173]

[172] INetSim.org [2019] *INetSim: Internet Services Simulation Suite* https://www.inetsim.org [Accessed 2nd August 2019]
[173] Taaffe, Jonathon [2019] *Image 43. Starting iNetSim* [Created 2nd August 2019]

Network Services Created (Forked) by iNetSim

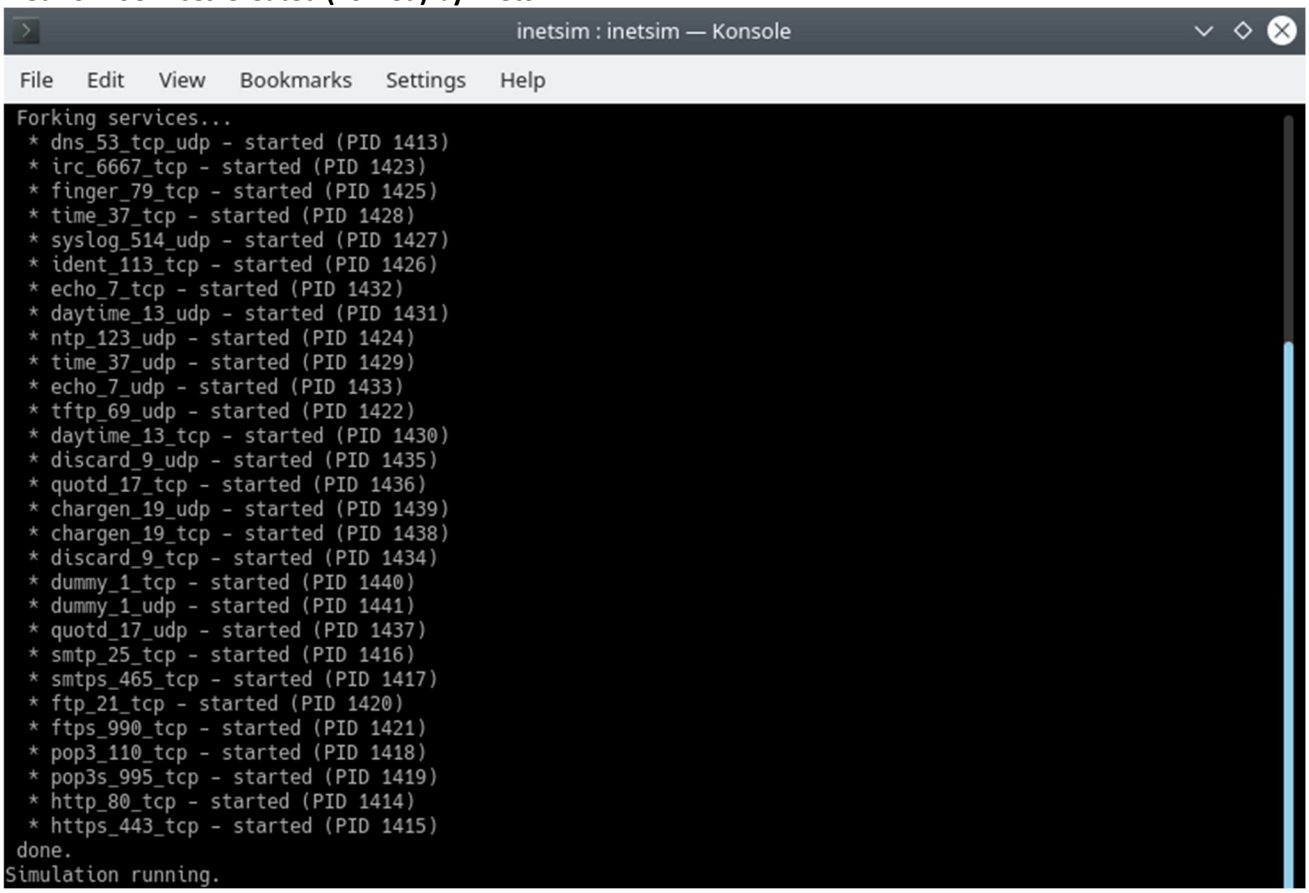


Image 44. Network Serviced Created (Forked) by iNetSim[174]

Services to Note:

```
dns_53_tcp_udp - started (PID 1413)
http_80_tcp - started (PID 1415)
```

DNS and HTTP Connection from Windows 7 VM to iNetSim

Test URL: http://www.test101.com : OK

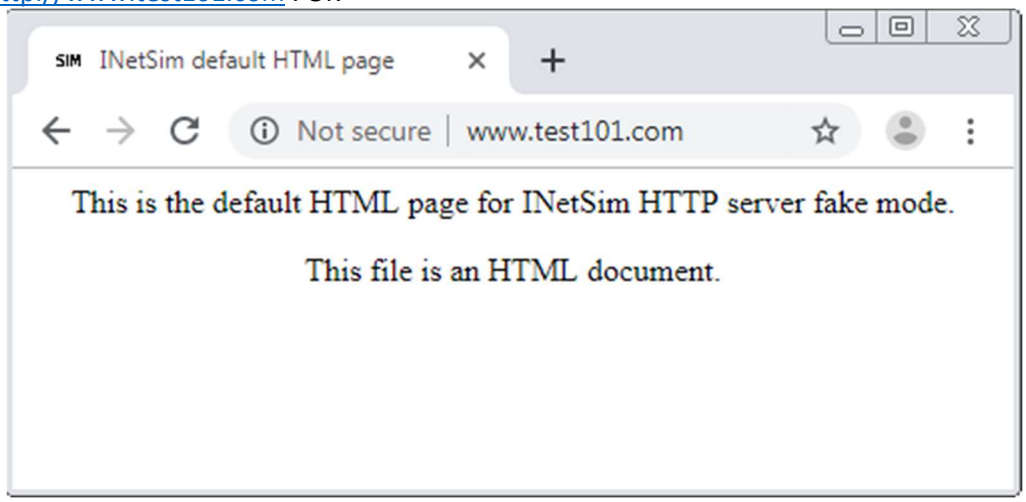


Image 45. iNetSim Default HTML Page[175]

[174] Taaffe, Jonathon [2019] *Image 44. Network Serviced Created (Forked) by iNetSim* [Created 2nd August 2019]
[175] Taaffe, Jonathon [2019] *Image 45. iNetSim Default HTML Page* [Created 2nd August 2019]

Wireshark Network Monitoring[176]

Wireshark configured to capture network packets on eth0. Once the DNS request was received by iNetSim it captured it in Wireshark as follows:

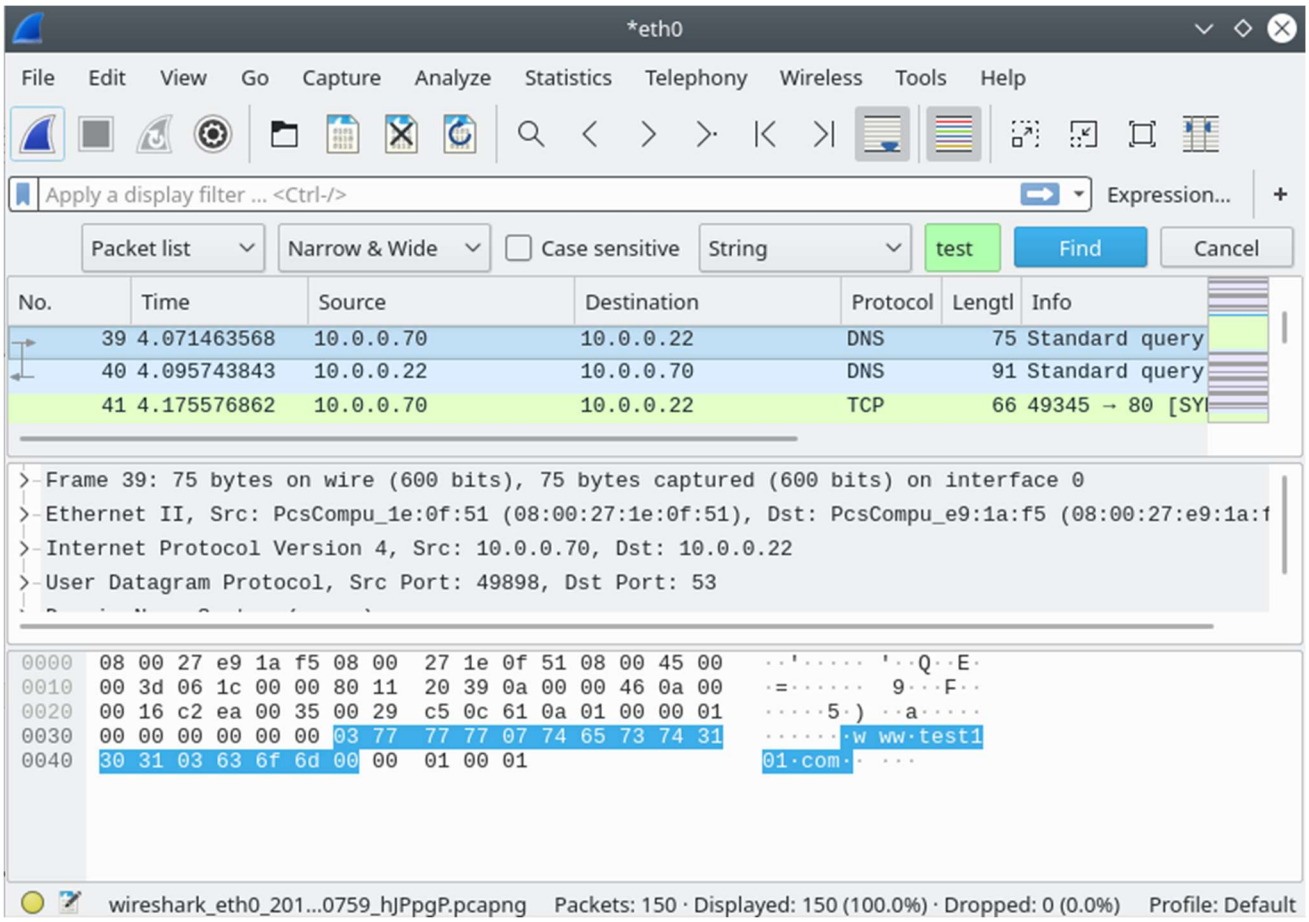


Image 46. Wireshark Network Monitoring[177]

Network Traffic Investigation Checks

Prior to running a full Network Traffic Investigation, here are the checks completed so far:

1. Windows 7 Analysis VM Static IP 10.0.0.70 : OK
2. Windows 7 Analysis VM Gateway IP 10.0.0.22 : OK
3. iNetSim static IP 10.0.0.22 : OK
4. Windows 7 VM to iNetSim Connectivity : OK
5. iNetSim Started : OK
6. iNetSim DNS Service 'dns_53_tcp_udp – started (PID 1413)' started : OK
7. iNetSim HTTP Service 'http_80_tcp – started (PID 1415)' started : OK
8. Browser Connection (http://www.test101.com) from Windows 7 VM to iNetSim : OK
9. Wireshark Network Monitoring : OK

[176] Wireshark.org [2019] Download Wireshark *https://www.wireshark.org/download.html* [Accessed 2nd August 2019]

[177] Taaffe, Jonathon [2019] *Image 46. Wireshark Network Monitoring* [Created 2nd August 2019]

Dynamic Network Traffic Investigation

Started Process Monitor on the Windows 7 VM and have set a filter to only monitor for Process Name: Unknown.exe.

Executed C:\Temp\Virus_Files\Unknown.exe

Process Monitor Network Activity

Again Unknown.exe generated multiple Registry, File System and Processes; 2,166 in total
But this time Unknown.exe generated the following Network Activity:

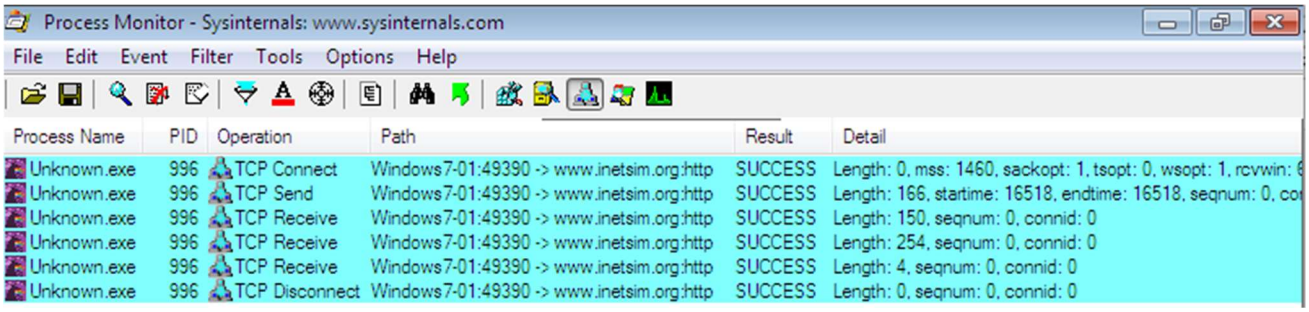


Image 47. Unknown.exe Process Monitor Network Activity[178]

Below is the details of the Network Activity generated

Operation	Path	Details
TCP Connect	Windows7-01:49390 -> www.inetsim.org:http	Length:0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 65700, rcvwinscale: 2, sndwinscale: 7, seqnum: 0, connid: 0
TCP Send	Windows7-01:49390 -> www.inetsim.org:http	Length: 166, startime:16518, endtime: 16518, seqnum: 0, connid: 0
TCP Receive	Windows7-01:49390 -> www.inetsim.org:http	Length: 150, seqnum: 0, connid: 0
TCP Receive	Windows7-01:49390 -> www.inetsim.org:http	Length: 254, seqnum: 0, connid: 0
TCP Receive	Windows7-01:49390 -> www.inetsim.org:http	Length: 4, seqnum: 0, connid: 0
TCP Disconnect	Windows7-01:49390 -> www.inetsim.org:http	Length: 0, seqnum: 0, connid: 0

Table 31. Unknown.exe Process Monitor Network Activity[179]

Conclusion: This shows Unknown.exe successfully connected to iNetSim VM over port TCP 49390 using HTTP.

[178] Taaffe, Jonathon [2019] Image 47. Unknown.exe Process Monitor Network Activity [Created 2nd August 2019]
[179] Taaffe, Jonathon [2019] Table 31. Unknown.exe Process Monitor Network Activity [Created 2nd August 2019]

Wireshark Capture Analysis

Wireshark captured Unknown.exe DNS request for definitely-not-evil.com as shown below

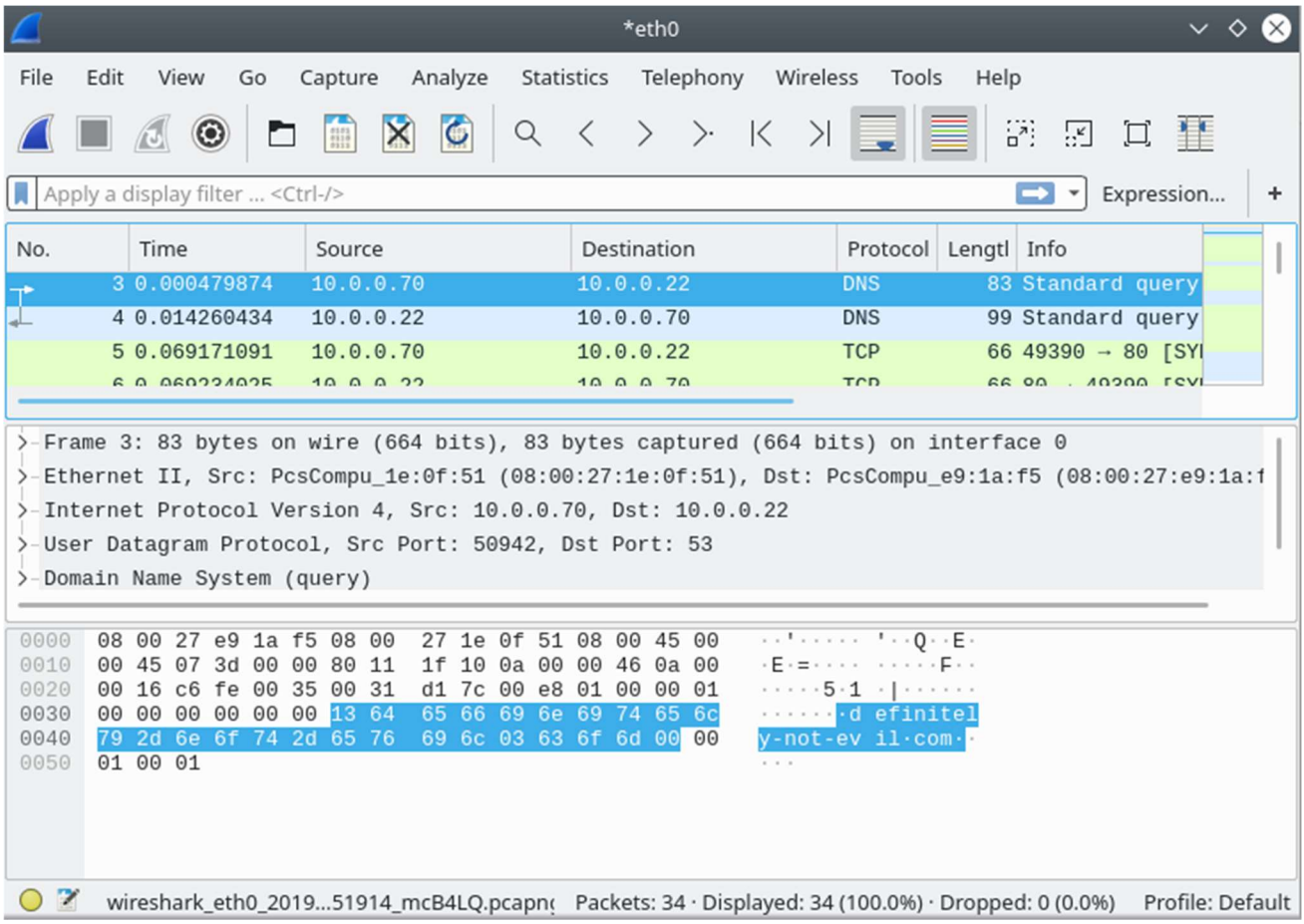


Image 48. Wireshark Capture Analysis[180]

Wireshark Capture saved to iNetSim VM /root/documents

[180] Taaffe, Jonathon [2019] *Image 48. Wireshark Capture Analysis* [Created 2nd August 2019]

Packets: 5 to 15

Source	Destination	Protocol	Details
10.0.0.70	10.0.0.22	DNS	DNS request from W7 for definitely-not-evil.com
10.0.0.22	10.0.0.70	DNS	DNS reply from iNetSim for definitely-not-evil.com
10.0.0.22	10.0.0.70	TCP	HTTP GET Request on Port 49390
10.0.0.70	10.0.0.22	TCP	HTTP GET Request
10.0.0.22	10.0.0.70	TCP	HTTP/1.1 200 OK

Table 32. Wireshark Network Packets Analysis01[181]

Follow TCP Stream

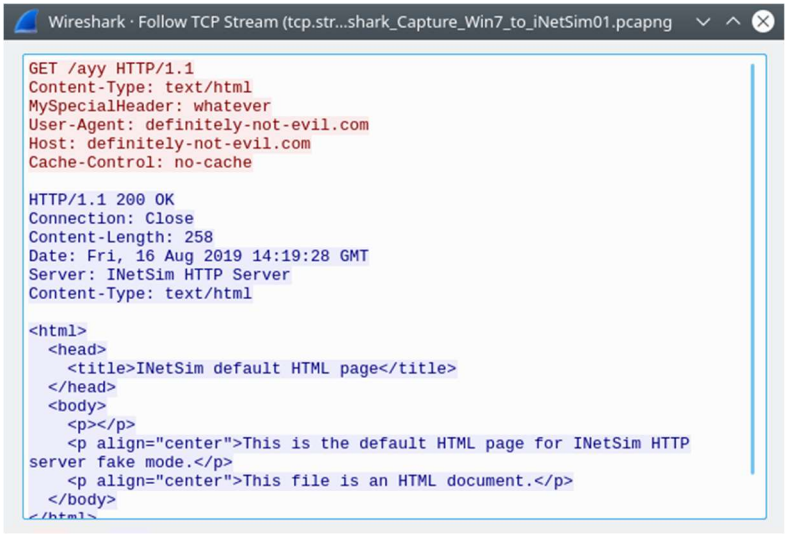


Image 49. Wireshark Follow TCP Stream[182]

Packets: 16 to 18

Packet	Source	Destination	Protocol	Details
16	10.0.0.70	244.0.0.252	LLMNR	Link-local Multicast Name Resolution

Table 33. Wireshark Network Packets Analysis02[183]

Conclusion: Unknown.exe sent a multicast for additional host name resolution.

[181] Taaffe, Jonathon [2019] *Table 32. Wireshark Network Packets Analysis01* [Created 2nd August 2019]
[182] Taaffe, Jonathon [2019] *Image 49. Wireshark Follow TCP Stream* [Created 2nd August 2019]
[183] Taaffe, Jonathon [2019] *Table 33. Wireshark Network Packets Analysis02* [Created 2nd August 2019]

Packets: 19 to 28

Packet	Source	Destination	Protocol	Details
19	10.0.0.70	10.0.0.22	TCP	GET /fwlink/?LinkID=121721&clcid=0
24	10.0.0.22	10.0.0.70	TCP	HTTP/1.1 200 OK

Table 34. Wireshark Network Packets Analysis03[184]

Follow TCP Stream

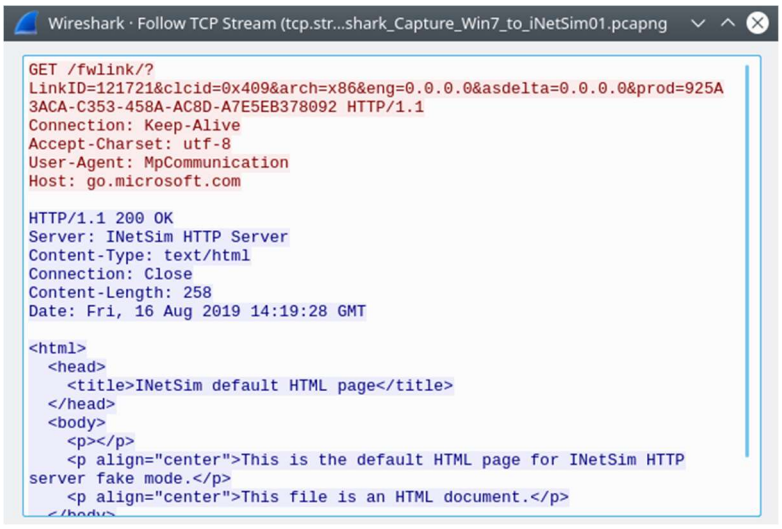


Image 50. Wireshark Follow TCP Stream[185]

Packets: 29 to 30

Packet	Source	Destination	Protocol	Details
29	10.0.0.70	10.0.0.22	DNS	252.0.0.224-in-addr.arpa
30	10.0.0.22	10.0.0.70	DNS	252.0.0.224-in-addr.arpa……www.inetsim.org

Table 35. Wireshark Network Packets Analysis04[186]

Follow TCP Stream

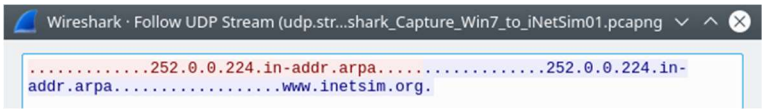


Image 51. Wireshark Follow UDP Stream[187]

[184] Taaffe, Jonathon [2019] *Table 34. Wireshark Network Packets Analysis03* [Created 2nd August 2019]
[185] Taaffe, Jonathon [2019] *Image 50. Wireshark Follow TCP Stream* [Created 2nd August 2019]
[186] Taaffe, Jonathon [2019] *Table 35. Wireshark Network Packets Analysis04* [Created 2nd August 2019]
[187] Taaffe, Jonathon [2019] *Image 51. Wireshark Follow UDP Stream* [Created 2nd August 2019]

Packets: 31 to 34

Packet	Source	Destination	Protocol	Details
31	10.0.0.70	255.255.255.250	SSDP	Simple Service Discovery Protocol

Table 36. Wireshark Network Packets Analysis05[188]

Follow UDP Stream

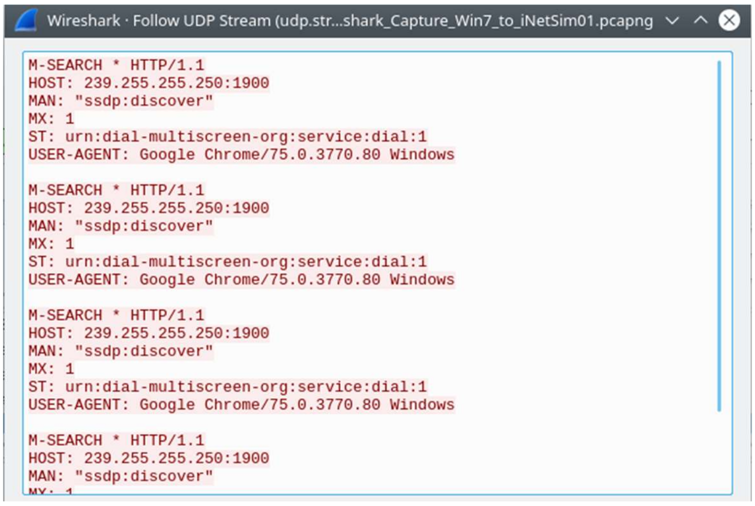


Image 52. Wireshark Follow UDP Stream[189]

Wireshark Network Packets Analysis - Conclusion

1. Unknown.exe requests to connect to definitely-not-evil.com
2. Unknown.exe then send a network Multicast for additional host name resolution
3. Unknown.exe then requests a link: GET /fwlink/?LinkID=121721&clcid=0
4. Unknown.exe the performs a PTR/Reverse lookup: 252.0.0.224-in-addr.arpa
5. Unknown.exe performs an SSDP Simple Service Discovery Protocol for Browser Versions on the network

iNetSim Report

2019-08-16 15:17:55 DNS connection, type: PTR, class: IN, requested name: 250.255.255.239.in-addr.arpa
2019-08-16 15:17:57 DNS connection, type: PTR, class: IN, requested name: 22.0.0.10.in-addr.arpa
2019-08-16 15:19:28 DNS connection, type: A, class: IN, requested name: definitely-not-evil.com
2019-08-16 15:19:28 HTTP connection, method: GET, URL: http://definitely-not-evil.com/ayy
2019-08-16 15:19:28 DNS connection, type: PTR, class: IN, requested name: 252.05.05.224.in-addr.arpa

[188] Taaffe, Jonathon [2019] *Table 36. Wireshark Network Packets Analysis05* [Created 2nd August 2019]
[189] Taaffe, Jonathon [2019] Image 52. Wireshark Follow UDP Stream [Created 2nd August 2019]

Detailed Recommendations

For this specific malware sample, the following recommendations have been provided to the IT Network Operations, Server Operations and PC Support teams:

Network Filtering

All Network Firewall Filters to updated to DROP any network traffic containing any of the following data:

Fully Qualified Domain Name	definitely-not-evil.com
URLs	http://definitely-not-evil.com/ http://definitely-not-evil.com/ayy
IP Address	45.55.137.243

Table 37. Network Firewall Filters Updates[190]

Email Filtering

Malicious Email Attachment and Spam Email Filters to be updated to DELETE any email attachments containing any of the following data:

File Name	Unknown.exe rainbowmagic.exe re101.exe dope.exe Trojan.Ransom.Alma.Blocker.exe a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615.bin a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615.exe
File Version Information	Copyright: Copyright (C) 2017 Product: Rainbow Magic Game Description: Rainbow Magic Game Original Name: rainbowmagic.exe Internal Name: rainbowmagic.exe File Version: 1.0.0.1
File Hashes	MD5: 25d562f46c14c5267d56722f6a43b8ed SHA-1:7cd4d6f44bdb71d24574d0b4bc326abd006eb510 SHA-256: a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615
File Sections MD5 Hashes	UPX0: d41d8cd98f00b204e9800998ecf8427e UPX1: 16257d5acfdbed7dca880991bf0418ff .rsrc: 567c038240474732cc9dbc92402dd111

Table 38. Email Protection Updates[191]

Server and PC Protection

1. Ensure Symantec Enterprise Protection Suite[192] (Anti-Virus solution) is updated with the latest virus signatures as and when Symantec publish new signatures.
2. Ensure Symantec Anti-Virus client on ALL Servers and PC's are fully functioning and are receiving updates from on-site Symantec Anti-Virus
3. Ensure ALL Servers and PC's are configured for Real-Time Anti-Virus scanning.

[190] Taaffe, Jonathon [2019] *Table 37. Network Firewall Filters Updates* [Created 2nd August 2019]
[191] Taaffe, Jonathon [2019] *Table 38. Email Protection Updates* [Created 2nd August 2019]
[192] Symantec.com (2019) *Symantec Protection Suite Enterprise Edition* https://www.symantec.com/products/protection-suite [Accessed 2nd August 2019]

Conclusions

This malware sample is a piece of ransomware and its core functionality is:

1. Analyse the system on which it is being run
2. Create registry keys to ensure persistence
3. Imports CRYPT32.dll to enable encryption functionality
4. Imports WININET.dll to enable network/internet connectivity
5. Create files and folders
6. Present a dialogue box to the user informing them their data had been encrypted

The original sample had been Packed using UPX which made it difficult to analyse the code of the sample. Unpacking the sample using UPX decrypted the malware code for analysis.

Once network/internet connectivity is established, the ransomware attempts to connect to 1 domain and 1 IP address, thus making it easy to block at the Network Firewalls.

It has been in the wild since 2017 and is well documented.

Anti-Virus vendors have a virus signature for this ransomware so it should be detected and quarantined prior to execution.

References

1	Robtex.com	[2019]	definitely-not-evil.com Analysis	https://www.robtex.com/dns-lookup/definitely-not-evil.com	[Accessed 1st August 2019]
2	Microsoft.com	[2019]	Microsoft Windows 7 Download	https://www.microsoft.com/en-us/software-download/windows7	[Accessed 1st August 2019]
3	Wikipedia.com	[2019]	IP address	https://en.wikipedia.org/wiki/IP_address	[Accessed 1st August 2019]
4	Cisco.com	[2019]	What is a Firewall?	https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html	[Accessed 1st August 2019]
5	Symantec.com	[2019]	Virus Definitions & Security Updates	https://www.symantec.com/security_response/definitions.jsp	[Accessed 1st August 2019]
6	Microsoft.com	[2019]	Strings.exe	https://docs.microsoft.com/en-us/sysinternals/downloads/strings	[Accessed 1st August 2019]
7	NirSoft	[2019]	HashMyFiles v2.35	https://www.nirsoft.net/utils/hash_my_files.html	[Accessed 1st August 2019]
8	VirusTotal.com	[2019]	VirusTotal	https://www.virustotal.com	[Accessed 1st August 2019]
9	VirusTotal.com	[2019]	Detection	https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/detection	[Accessed 1st August 2019]
10	Wikipedia.com	[2019]	Malware	https://en.wikipedia.org/wiki/Malware	[Accessed 1st August 2019]
11	Kaspersky.com	[2019]	What is a Trojan Virus?	https://usa.kaspersky.com/resource-center/threats/trojans	[Accessed 1st August 2019]
12	MalwareBytes.com	[2019]	Ransomware	https://www.malwarebytes.com/ransomware/	[Accessed 1st August 2019]
13	VirusTotal.com	[2019]	Details	https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/details	[Accessed 1st August 2019]
14	UPX	[2019]	Ultimate Packer for eXecutables	https://upx.github.io/	[Accessed 1st August 2019]
15	Manalyzer.org	[2019]	rainbowmagic.exe	https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed	[Accessed 1st August 2019]
16	Reverse.it	[2019]	Analysis Overview	https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615	[Accessed 1st August 2019]
17	Kaspersky.com	[2019]	TROJAN-RANSOM.WIN32.BLOCKER	https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/	[Accessed 1st August 2019]
18	Taaffe, Jonathon	[2019]	Table 1. Virus Total Unknown.exe Portable Execution Sections		[Created 1st August 2019]
19	Microsoft.com	[2019]	What is a DLL?	https://support.microsoft.com/en-us/help/815065/what-is-a-dll	[Accessed 1st August 2019]
20	Microsoft.com	[2019]	WinRegCloseKey Function	https://docs.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regclosekey	[Accessed 1st August 2019]
21	Microsoft.com	[2019]	CryptStringToBinaryA Function	https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptstringtobinarya	[Accessed 1st August 2019]
22	Microsoft.com	[2019]	VirtualProtect Function	https://docs.microsoft.com/en-gb/windows/win32/api/memoryapi/nf-memoryapi-virtualprotect	[Accessed 1st August 2019]
23	Microsoft.com	[2019]	LoadLibraryA Function	https://docs.microsoft.com/en-us/windows/win32/api/libloaderapi/nf-libloaderapi-loadlibrarya	[Accessed 1st August 2019]
24	Microsoft.com	[2019]	ExitProcess Function	https://docs.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-exitprocess	[Accessed 1st August 2019]
25	Microsoft.com	[2019]	GetProcAddress Function	https://docs.microsoft.com/en-gb/windows/win32/api/libloaderapi/nf-libloaderapi-getprocaddress	[Accessed 1st August 2019]
26	Microsoft.com	[2019]	ShellExecuteA Function	https://docs.microsoft.com/en-us/windows/win32/api/shellapi/nf-shellapi-shellexecutea	[Accessed 1st August 2019]
27	Microsoft.com	[2019]	MessageBoxA Function	https://docs.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-messageboxa	[Accessed 1st August 2019]
28	Microsoft.com	[2019]	InternetOpenA Function	https://docs.microsoft.com/en-us/windows/win32/api/wininet/nf-wininet-internetopena	[Accessed 1st August 2019]

29	Microsoft.com	[2019]	CoTaskMemFree Function	https://docs.microsoft.com/en-us/windows/win32/api/combaseapi/nf-combaseapi-cotaskmemfree	[Accessed 1st August 2019]
30	Taaffe, Jonathon	[2019]	Table 2. Virus Total Unknown.exe Imports		[Created 1st August 2019]
31	VirusTotal.com	[2019]	Relations	https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/relations	[Accessed 1st August 2019]
32	Taaffe, Jonathon	[2019]	Table 3. Unknown.exe Network Elements Related		[Created 1st August 2019]
33	VirusTotal.com	[2019]	Network Relations Graph Summary	https://www.virustotal.com/graph//drawer/node-summary/node/na635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/1565866169779	[Accessed 1st August 2019]
34	Taaffe, Jonathon	[2019]	Diagram 1. VirusTotal Network Relations Graph		[Created 1st August 2019]
35	VirusTotal.com	[2019]	Behaviour	https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/behavior	[Accessed 1st August 2019]
36	Taaffe, Jonathon	[2019]	Table 4. Files Opened, Written, Copied and Deleted		[Created 1st August 2019]
37	Taaffe, Jonathon	[2019]	Table 5. Registry Keys Opened		[Created 1st August 2019]
38	Taaffe, Jonathon	[2019]	Table 6. Registry Changes Made		[Created 1st August 2019]
39	HowToGeek.com	[2019]	What Is conhost.exe and Why Is It Running?	https://www.howtogeek.com/howto/4996/what-is-conhost.exe-and-why-is-it-running/	[Accessed 1st August 2019]
40	Microsoft.com	[2019]	Description of the scheduled tasks in Windows Vista	https://support.microsoft.com/en-us/help/939039/description-of-the-scheduled-tasks-in-windows-vista	[Created 1st August 2019]
41	Microsoft.com	[2019]	wmiadap	https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmiadap	[Accessed 1st August 2019]
42	Taaffe, Jonathon	[2019]	Table 7. Executables and Associated Commands		[Created 1st August 2019]
43	VirusTotal.com	[2019]	Detection	https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/detection	[Accessed 1st August 2019]
44	Manalyzer.org	[2019]	rainbowmagic.exe	https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed	[Accessed 1st August 2019]
45	Reverse.it	[2019]	Analysis Overview	https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615	[Accessed 1st August 2019]
46	Kaspersky.com	[2019]	TROJAN-RANSOM.WIN32.BLOCKER	https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/	[Accessed 1st August 2019]
47	Manalyzer.org	[2019]	rainbowmagic.exe	https://manalyzer.org/report/25d562f46c14c5267d56722f6a43b8ed	[Accessed 1st August 2019]
48	Taaffe, Jonathon	[2019]	Table 8. Manalyzer.org Plugin Output		[Created 1st August 2019]
49	Reverse.it	[2019]	Analysis Overview	https://www.reverse.it/sample/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615	[Accessed 1st August 2019]
50	Taaffe, Jonathon	[2019]	Table 9. Manalyzer.org rainbow.exe Risk Assessment		[Created 1st August 2019]
51	Kaspersky.com	[2019]	TROJAN-RANSOM.WIN32.BLOCKER	https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Blocker/	[Accessed 1st August 2019]
52	Robtex.com	[2019]	Robtex	https://www.robtex.com/	[Accessed 1st August 2019]
53	Taaffe, Jonathon	[2019]	Table 10. Robtex.com Results for definitely-not-evil.com		[Created 1st August 2019]
54	Taaffe, Jonathon	[2019]	Diagram 2. Robtex.com Related Domain Name Services Graph		[Created 1st August 2019]
55	Taaffe, Jonathon	[2019]	Table 11. Malware Identification Conclusion Summary		[Created 1st August 2019]
56	REMnux.org	[2019]	REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware	https://remnux.org/	[Accessed 1st July 2019]
57	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
58	Taaffe, Jonathon	[2019]	Table 12. Malware Analysis Utilities Static IP Assignment		[Created 2nd August 2019]
59	REMnux 6.0 OVA Public	[2019]	remnux-6.0-ova-public.ova (2.0G)	https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download	[Accessed 2nd August 2019]
60	Taaffe, Jonathon	[2019]	Table 13. Gateway OS – REMnux VM Configuration		[Created 2nd August 2019]

61	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
62	Taaffe, Jonathon	[2019]	Table 14. Gateway OS – REMnux VM Configuration		[Created 2nd August 2019]
63	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
64	Taaffe, Jonathon	[2019]	Table 15. FakeNet-NG Pre-Requisites		[Created 2nd August 2019]
65	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
66	INetSim.org	[2019]	INetSim: Internet Services Simulation Suite	https://www.inetsim.org	[Accessed 2nd August 2019]
67	Taaffe, Jonathon	[2019]	Table 16. iNetSim VM Configuration		[Created 2nd August 2019]
68	TechAnarchy.net	[2019]	Installing and Configuring InetSim	https://techanarchy.net/blog/installing-and-configuring-inetsim	[Accessed 2nd August 2019]
69	VirtualBox.org	[2019]	VirtualBox	https://www.virtualbox.org/	[Accessed 2nd August 2019]
70	Taaffe, Jonathon	[2019]	Table 17. malware-analysis-network01 Static Assignments		[Created 2nd August 2019]
71	Portal.Azure.com	[2019]	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd August 2019]
72	Taaffe, Jonathon	[2019]	Table 18. Windows Server 2016 File Server VM Configuration		[Created 2nd August 2019]
73	Tactig.com	[2019]	How to Share Files and Folders in Windows Server 2016	https://www.tactig.com/share-files-folders-windows-server-2016/	[Accessed 2nd August 2019]
74	Microsoft.com	[2019]	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd August 2019]
75	Taaffe, Jonathon	[2019]	Table 19. Windows 7 VM Client Configuration		[Created 2nd August 2019]
76	Taaffe, Jonathon	[2019]	Table 20. Windows 7 Network Configuration		[Created 2nd August 2019]
77	Taaffe, Jonathon	[2019]	Table 21. Windows 7 OS Configuration		[Created 2nd August 2019]
78	Microsoft.com	[2019]	Internet Explorer security zones registry entries for advanced users	https://support.microsoft.com/en-us/help/182569/internet-explorer-security-zones-registry-entries-for-advanced-users	[Accessed 2nd August 2019]
79	Portal.Azure.com	[2019]	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd August 2019]
80	REMnux 6.0 OVA Public	[2019]	remnux-6.0-ova-public.ova (2.0G)	https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download	[Accessed 2nd August 2019]
81	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
82	INetSim.org	[2019]	INetSim: Internet Services Simulation Suite	https://www.inetsim.org	[Accessed 2nd August 2019]
83	Microsoft.com	[2019]	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd August 2019]
84	Taaffe, Jonathon	[2019]	Diagram 3. Lab 1 Phase 1 Installation and Configuration		[Created 2nd August 2019]
85	Portal.Azure.com	[2019]	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd August 2019]
86	Microsoft.com	[2019]	Download Virtual Machines	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/	[Accessed 2nd August 2019]
87	Taaffe, Jonathon	[2019]	Diagram 4. Lab 1 Phase 2 File Transfer		[Created 2nd August 2019]
88	Taaffe, Jonathon	[2019]	Table 22. Analysis Client Application File Transfer		[Created 2nd August 2019]
89	Taaffe, Jonathon	[2019]	Table 23.. Analysis Client Application Installation		[Created 2nd August 2019]
90	Portal.Azure.com	[2019]	Windows Server 2016 Standard	http://dl.msdn.com/pr/en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso	[Accessed 2nd August 2019]
91	Taaffe, Jonathon	[2019]	Diagram 5. Lab 1 Phase 6 Dynamic Malware Analysis Configuration		[Created 2nd August 2019]
92	Robtex.com	[2019]	Robtex.com	https://www.robtex.com/	[Accessed 2nd August 2019]
93	VirusTotal.com	[2019]	VirusTotal	https://www.virustotal.com	[Accessed 2nd August 2019]
94	Taaffe, Jonathon	[2019]	Table 24. Internet Investigations Justifications		[Created 2nd August 2019]
95	Manalyzer.org	[2019]	Manalyzer.org	https://manalyzer.org	[Accessed 2nd August 2019]
96	Reverse.it	[2019]	Reverse.it	https://www.reverse.it	[Accessed 2nd August 2019]
97	Kaspersky.com	[2019]	Threats.Kaspersky.com	https://threats.kaspersky.com	[Accessed 2nd August 2019]
98	Taaffe, Jonathon	[2019]	Table 25. Internet Investigations Justifications		[Created 2nd August 2019]

99	7-Zip.org	[2019]	7-zip	https://www.7-zip.org/	[Accessed 2nd August 2019]
100	NirSoft.net	[2019]	HashMyFiles v2.35	https://www.nirsoft.net/utils/hash_my_files.html	[Accessed 2nd August 2019]
101	WJRadburn.com	[2019]	PEView	http://wjradburn.com/software/	[Accessed 2nd August 2019]
102	Softpedia.com	[2019]	PEiD 0.95	http://www.softpedia.com/	[Accessed 2nd August 2019]
103	Softpedia.com	[2019]	BinText3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml	[Accessed 2nd August 2019]
104	DependencyWalker.com	[2019]	DependencyWalker 2.2	http://www.dependencywalker.com/	[Accessed 2nd August 2019]
105	UPX.github.com	[2019]	UPX 3.95	https://upx.github.io/	[Accessed 2nd August 2019]
106	AngusJ.com	[2019]	Resource Hacker 5.1.7	http://www.angusj.com/resourcehacker/	[Accessed 2nd August 2019]
107	Hex-Rays.com	[2019]	IDA Pro v7.0	https://www.hex-rays.com/products/ida/support/download_freeware.shtml	[Accessed 2nd August 2019]
108	OllyDBG.de	[2019]	OllyDbg 1.10	http://www.ollydbg.de/download.htm	[Accessed 2nd August 2019]
109	Taaffe, Jonathon	[2019]	Table 26. Static Analysis Tools Justifications		[Created 2nd August 2019]
110	RegShot	[2019]	RegShot	https://sourceforge.net/projects/regshot/	[Accessed 2nd August 2019]
111	Microsoft.com	[2019]	SysInternals Process Monitor v3.50	https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon	[Accessed 2nd August 2019]
112	Microsoft.com	[2019]	SysInternals Process Explorer v 16.21	https://docs.microsoft.com/en-gb/sysinternals/downloads/process-explorer	[Accessed 2nd August 2019]
113	Wireshark.org	[2019]	Download Wireshark	https://www.wireshark.org/download.html	[Accessed 2nd August 2019]
114	REMnux 6.0 OVA Public	[2019]	remnux-6.0-ova-public.ova (2.0G)	https://docs.google.com/uc?id=0B6fULLT_NpxMampUWlBCQXVJZzA&export=download	[Accessed 2nd August 2019]
115	FireEye/Flare-FakeNet-NG	[2019]	FakeNet-NG - Next Generation Dynamic Network Analysis Tool	https://github.com/fireeye/flare-fakenet-ng	[Accessed 2nd August 2019]
116	Taaffe, Jonathon	[2019]	Table 27. Dynamic Analysis Tools Justifications		[Created 2nd August 2019]
117	Radburn, Wayne J.	[2018]	PEview version 0.9.9 (.zip 31KB)	http://wjradburn.com/software/	[Accessed 2nd August 2019]
118	Taaffe, Jonathon	[2019]	Image 1. PEView Analysis		[Created 2nd August 2019]
119	Taaffe, Jonathon	[2019]	Image 2. Sections Analysis - SECTION UPX0		[Created 2nd August 2019]
120	Taaffe, Jonathon	[2019]	Image 3. Sections Analysis - SECTION UPX1		[Created 2nd August 2019]
121	Taaffe, Jonathon	[2019]	Image 4. Section Analysis - SECTION .rsrc		[Created 2nd August 2019]
122	Taaffe, Jonathon	[2019]	Image 5. SECTION .rsrc - IMAGE_RESOURCE_DIRECORY Type		[Created 2nd August 2019]
123	Taaffe, Jonathon	[2019]	Image 6. SECTION .rsrc – IMPORT Directory Table		[Created 2nd August 2019]
124	Taaffe, Jonathon	[2019]	Image 7. SECTION .rsrc – IMPORT Address Table		[Created 2nd August 2019]
125	Taaffe, Jonathon	[2019]	Table 28. Unknown.exe DLL File Imports		[Created 2nd August 2019]
126	Softpedia.com	[2019]	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 2nd August 2019]
127	Taaffe, Jonathon	[2019]	Image 8. PEiD Analysis		[Created 2nd August 2019]
128	Taaffe, Jonathon	[2019]	Image 9. PEiD - Section Viewer		[Created 2nd August 2019]
129	Softpedia.com	[2019]	BinText 3.03	https://www.softpedia.com/get/System/File-Management/BinText.shtml	[Accessed 2nd August 2019]
130	Taaffe, Jonathon	[2019]	Image 10. BinText3.03 Analysis01		[Created 2nd August 2019]
131	Taaffe, Jonathon	[2019]	Image 11. BinText3.03 Analysis02		[Created 2nd August 2019]
132	Dependency Walker 2.2	[2019]	Dependency Walker 2.2	http://www.dependencywalker.com/	[Accessed 2nd August 2019]
133	Taaffe, Jonathon	[2019]	Image 12. Dependency Walker 2.2 Analysis01		[Created 2nd August 2019]
134	Taaffe, Jonathon	[2019]	Image 13. Dependency Walker 2.2 Analysis02		[Created 2nd August 2019]
135	Taaffe, Jonathon	[2019]	Image 14. Dependency Walker 2.2 Analysis03		[Created 2nd August 2019]
136	Taaffe, Jonathon	[2019]	Image 15. Dependency Walker 2.2 Analysis04		[Created 2nd August 2019]
137	Taaffe, Jonathon	[2019]	Image 16. Dependency Walker 2.2 Analysis05		[Created 2nd August 2019]

138	Taaffe, Jonathon	[2019]	Image 17. Dependency Walker 2.2 Analysis06		[Created 2nd August 2019]
139	Taaffe, Jonathon	[2019]	Image 18. Dependency Walker 2.2 Analysis07		[Created 2nd August 2019]
140	Taaffe, Jonathon	[2019]	Image 19. Dependency Walker 2.2 Analysis08		[Created 2nd August 2019]
141	UPX Ultimate Packer for eXecutables	[2019]	UPX 3.95	https://github.com/upx/upx/releases/tag/v3.95	[Accessed 2nd August 2019]
142	Taaffe, Jonathon	[2019]	Image 20. UPX Unpacking		[Created 2nd August 2019]
143	Softpedia.com	[2019]	PEiD 0.95	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml	[Accessed 2nd August 2019]
144	Taaffe, Jonathon	[2019]	Image 21. PEiD Post UPX Unpacking Section Analysis		[Created 2nd August 2019]
145	Taaffe, Jonathon	[2019]	Image 22. PEiD Post UPX Unpacking Section Analysis		[Created 2nd August 2019]
146	Taaffe, Jonathon	[2019]	Image 23. BinText Post UPX Unpacking Analysis01		[Created 2nd August 2019]
147	Taaffe, Jonathon	[2019]	Image 24. BinText Post UPX Unpacking Analysis02		[Created 2nd August 2019]
148	Taaffe, Jonathon	[2019]	Image 25. BinText Post UPX Unpacking Analysis03		[Created 2nd August 2019]
149	Taaffe, Jonathon	[2019]	Image 26. BinText Post UPX Unpacking Analysis04		[Created 2nd August 2019]
150	Taaffe, Jonathon	[2019]	Image 27. BinText Post UPX Unpacking Analysis05		[Created 2nd August 2019]
151	Taaffe, Jonathon	[2019]	Image 28. BinText Post UPX Unpacking Analysis06		[Created 2nd August 2019]
152	Taaffe, Jonathon	[2019]	Image 29. BinText Post UPX Unpacking Analysis07		[Created 2nd August 2019]
153	Taaffe, Jonathon	[2019]	Image 30. BinText Post UPX Unpacking Analysis08		[Created 2nd August 2019]
154	Hex-Rays	[2019]	IDA Freeware for Windows (48 MB)	https://www.hex-rays.com/products/ida/support/download_freeware.shtml	[Accessed 2nd August 2019]
155	Taaffe, Jonathon	[2019]	Image 31. IDA Pro Analysis		[Created 2nd August 2019]
156	Taaffe, Jonathon	[2019]	Image 32. IDA Pro Imports Section		[Created 2nd August 2019]
157	Taaffe, Jonathon	[2019]	Image 33. IDA Pro Stings Section		[Created 2nd August 2019]
158	Taaffe, Jonathon	[2019]	Image 34. IDA Pro CRYPT32.DLL DLL Load Section		[Created 2nd August 2019]
159	Resource Hacker	[2019]	Resource Hacker 5.1.7	http://www.angusj.com/resourcehacker/	[Accessed 2nd August 2019]
160	Taaffe, Jonathon	[2019]	Image 35. Resource Hacker Analysis01		[Created 2nd August 2019]
161	Taaffe, Jonathon	[2019]	Image 36. Resource Hacker Analysis02		[Created 2nd August 2019]
162	Taaffe, Jonathon	[2019]	Image 37. Resource Hacker Analysis03		[Created 2nd August 2019]
163	Taaffe, Jonathon	[2019]	Image 38. Resource Hacker Analysis04		[Created 2nd August 2019]
164	Microsoft.com	[2019]	Process Monitor v3.52	https://docs.microsoft.com/en-gb/sysinternals/downloads/procmon	[Accessed 2nd August 2019]
165	Taaffe, Jonathon	[2019]	Image 39. Process Monitor Filter		[Created 2nd August 2019]
166	Taaffe, Jonathon	[2019]	Image 40. Process Monitor		[Created 2nd August 2019]
167	Taaffe, Jonathon	[2019]	Image 41. Registry Activity Results		[Created 2nd August 2019]
168	Taaffe, Jonathon	[2019]	Image 42. Process and Tree Activity Results		[Created 2nd August 2019]
169	Taaffe, Jonathon	[2019]	Table 29. Unknown.exe Operations Summary		[Created 2nd August 2019]
170	Taaffe, Jonathon	[2019]	Table 30. DLL's Imported Summary		[Created 2nd August 2019]
171	Taaffe, Jonathon	[2019]	Diagram 6. Lab 1 Phase 6 Dynamic Malware Analysis Configuration		[Created 2nd August 2019]
172	INetSim.org	[2019]	INetSim: Internet Services Simulation Suite	https://www.inetsim.org	[Accessed 2nd August 2019]
173	Taaffe, Jonathon	[2019]	Image 43. Starting iNetSim		[Created 2nd August 2019]
174	Taaffe, Jonathon	[2019]	Image 44. Network Serviced Created (Forked) by iNetSim		[Created 2nd August 2019]
175	Taaffe, Jonathon	[2019]	Image 45. iNetSim Default HTML Page		[Created 2nd August 2019]

176	Wireshark.org	[2019]	Download Wireshark	https://www.wireshark.org/download.html	[Accessed 2nd August 2019]
177	Taaffe, Jonathon	[2019]	Image 46. Wireshark Network Monitoring		[Created 2nd August 2019]
178	Taaffe, Jonathon	[2019]	Image 47. Unknown.exe Process Monitor Network Activity		[Created 2nd August 2019]
179	Taaffe, Jonathon	[2019]	Table 31. Unknown.exe Process Monitor Network Activity		[Created 2nd August 2019]
180	Taaffe, Jonathon	[2019]	Image 48. Wireshark Capture Analysis		[Created 2nd August 2019]
181	Taaffe, Jonathon	[2019]	Table 32. Wireshark Network Packets Analysis01		[Created 2nd August 2019]
182	Taaffe, Jonathon	[2019]	Image 49. Wireshark Follow TCP Stream		[Created 2nd August 2019]
183	Taaffe, Jonathon	[2019]	Table 33. Wireshark Network Packets Analysis02		[Created 2nd August 2019]
184	Taaffe, Jonathon	[2019]	Table 34. Wireshark Network Packets Analysis03		[Created 2nd August 2019]
185	Taaffe, Jonathon	[2019]	Image 50. Wireshark Follow TCP Stream		[Created 2nd August 2019]
186	Taaffe, Jonathon	[2019]	Table 35. Wireshark Network Packets Analysis04		[Created 2nd August 2019]
187	Taaffe, Jonathon	[2019]	Image 51. Wireshark Follow UDP Stream		[Created 2nd August 2019]
188	Taaffe, Jonathon	[2019]	Table 36. Wireshark Network Packets Analysis05		[Created 2nd August 2019]
189	Taaffe, Jonathon	[2019]	Image 52. Wireshark Follow UDP Stream		[Created 2nd August 2019]
190	Taaffe, Jonathon	[2019]	Table 37. Network Firewall Filters Updates		[Created 2nd August 2019]
191	Taaffe, Jonathon	[2019]	Table 38. Email Protection Updates		[Created 2nd August 2019]
192	Symantec.com	[2019]	Symantec Protection Suite Enterprise Edition	https://www.symantec.com/products/protection-suite	[Accessed 2nd August 2019]