SCHOOL OF COMPUTING

Diploma in Infocomm Security Management

<u>Malware Reverse Engineering Assignment 1</u>
ST2617

DISM/FT/3A/04

Submitted By (Student ID):

Yeo Yu Jun (2143341)

Muhammad Amirul Adeeb Bin Rizal (2107095)

Lecturer: Soh Yong Sheng

Submission Date: 03/06/2023

Table of content

Executive Summary

The Sample 66 was an email worm that caused widespread damage in 1999 created by “Spanska”. It spread via email attachments, infecting Windows 95, 98 and NT systems. It is regarded as the first virus to spread over email and serves as a model for other viruses that reproduce themselves. Happy99 is unlikely to ever inflict any harm because it lacks a dangerous payload, but it did slow down system performance and cause other unwanted effects.

Happy99 will arrive in an email with a subject line of "Happy New Year," along with an attachment called "Happy99.exe." When the attachment was opened, the worm would install itself on the user's system and modify the email settings to send copies of itself to other email addresses.

WSOCK32.DLL is copied and given the name WSOCK32.SKA. Happy99 will alter WSOCK32.DLL in such a way that SKA.EXE will launch each time WSOCK32.DLL is launched. If it is already running, the worm changes the registry key so that it can be launched once when the computer starts. The worm also keeps track of the addresses to which it has sent copies of itself. This data is kept in a file with the name “LISTE.SKA”.

1. Introduction

In this document we present our findings on sample 66 malware on 32-bit Virtual Machine. The analysis of static , behaviour and memory properties will be the main topics of the document. The virtual machine's specifications include an image of Windows XP (32 bit) and Linux REMnux.The Happy99 virus, also known as "Ska," was a significant computer virus that caused widespread damage in 1999. Its emergence highlighted the vulnerability of computer systems to malicious attacks and the potential damage that could be caused by malware. Our analysis provides valuable insights into the behaviour and impact of the Happy99 virus on computer systems.

2. Online Information

2.1. Virus Variant Name

After uploading this malware to VirusTotal, It returned various names of the malware from various different anti-virus providers. The results often associated terms such as 'Worm`,`Happy99` ,`Ska` & `Email` with the malware. With the result, there is the assumption that the malware is an email worm. After performing research online, It is known that the name of the malware is Happy99 which is a type of worm that is used to infect email as shown in the [Table] below

Anti-Virus Vendor	Malware Name
Avast	Win32:Happy-B [Wrm]
Symantec	Happy99.Worm
VirIT	Happy99
Fortinet	W32/Ska.A@m
Alibaba	Worm:Win32/Happy.d8dd0504
Microsoft	Worm:Win32/Ska.A@m
McAfee	W32/Ska@M

2.2. Background Information

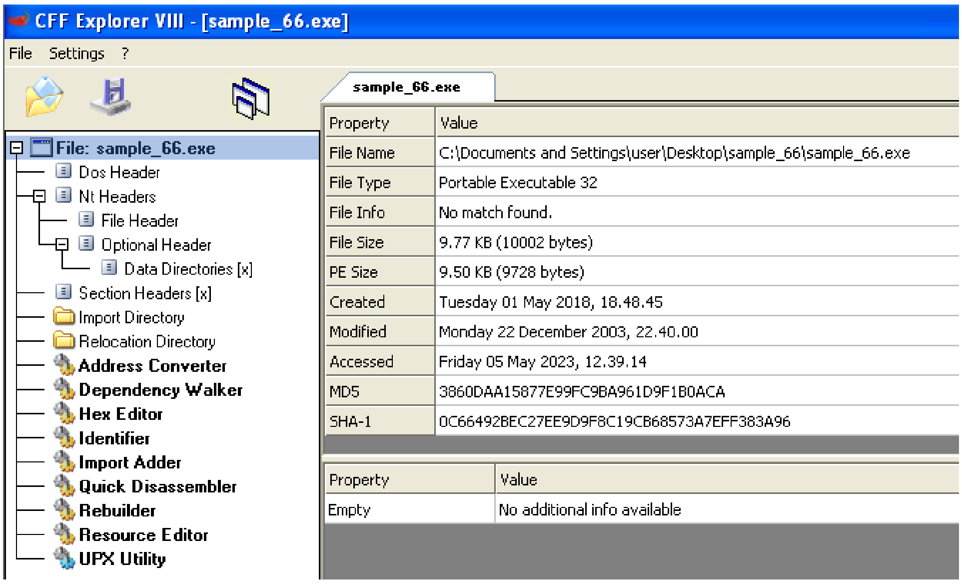
The Happy99 virus, also known as "Ska," is a computer virus that caused widespread damage in 1999. It is a type of email-based malware that spreads rapidly via email attachments, infecting Windows 95 and 98 systems. The virus would arrive in an email with a subject line of "Happy New Year," along with an attachment called "Happy99.exe." When the attachment was opened, the virus would install itself on the user's system and modify the email settings to send copies of itself to other email addresses. (Wikipedia , 2022)

The Happy99 virus also had a payload that would display fireworks on the user's computer screen. While the virus did not cause any significant damage to the infected computer, it did slow down system performance and cause other unwanted effects. (Wikipedia , 2022)

The emergence of the Happy99 virus highlighted the vulnerability of computer systems to malicious attacks and the potential damage that could be caused by malware. It also demonstrated the importance of implementing security measures and educating computer users about safe computing practices to prevent future malware outbreaks. (Wikipedia ,2022)

3. Static Analysis

3.1. General Information



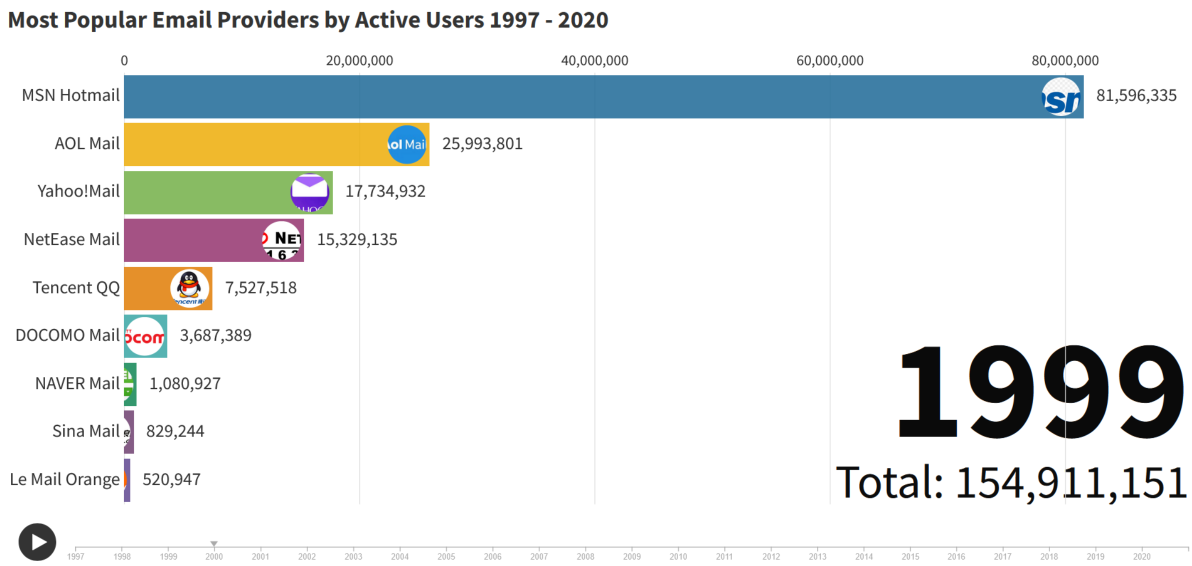
While using CFF Explorer, we conducted analysis on Happy99 which provided us with data of the static properties.

Firstly, we noticed the hashed values of both MD5 & SHA1 according to [fig]

These hashes act as digital fingerprints for the files. Security researchers and antivirus vendors maintain databases of known malicious file hashes. When a new file is suspected of being malware, its hash can be calculated and compared against the database to determine if it matches any known malicious files. This allows for quick identification and classification of malware.

Malware authors may employ various techniques to evade detection by modifying their code or payload. Hash values can be used as a defense mechanism to detect such tampering. For instance, some antivirus software and security systems calculate the hash of critical processes or components during runtime. If the calculated hash differs from the expected value, it may indicate that the process or component has been modified, potentially signalling the presence of malware.

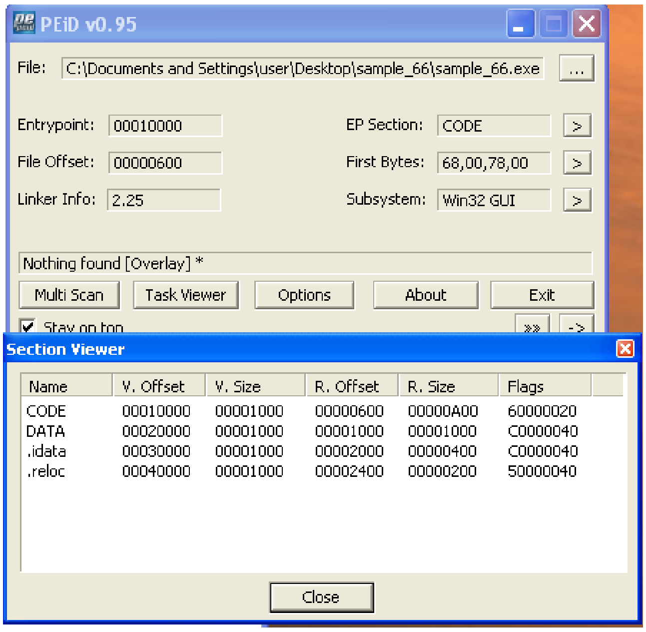
Secondly, the file type is a “Portable Executable 32”. The .exe extension typically indicates that the file is an executable file on Windows operating systems. PE is the file format used for executable files, object code, and DLLs (Dynamic Link Libraries) on Windows systems..EXE (Executable) files have the potential to trigger malware attacks because they are executable binary files that can contain malicious code.



https://flo.uri.sh/visualisation/3070061/embed

Thirdly, we notice the file size of Happy99 is “9.77KB”. The attachment size limit for MSN Hotmail in 1999 was 10 MB (megabytes) which is equivalent to 10,00KB as shown in [fig] assuming the sender uses MSN Hotmail. Happy99 needs to be small in size in order to spread through email attachment.

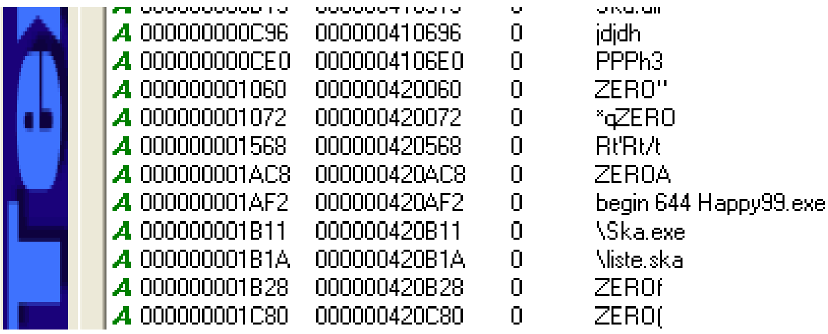
3.2. Packers



In order to determine how the malware is packaged, PEid is used. There does not appear to be any packers being used to conceal Happy99 so that it cannot be found.Upon clicking the ep section it will show the code of Happy99.

3.3. Strings

While using BinText, We manage to get a whole list of strings related to Happy 99 Malware.



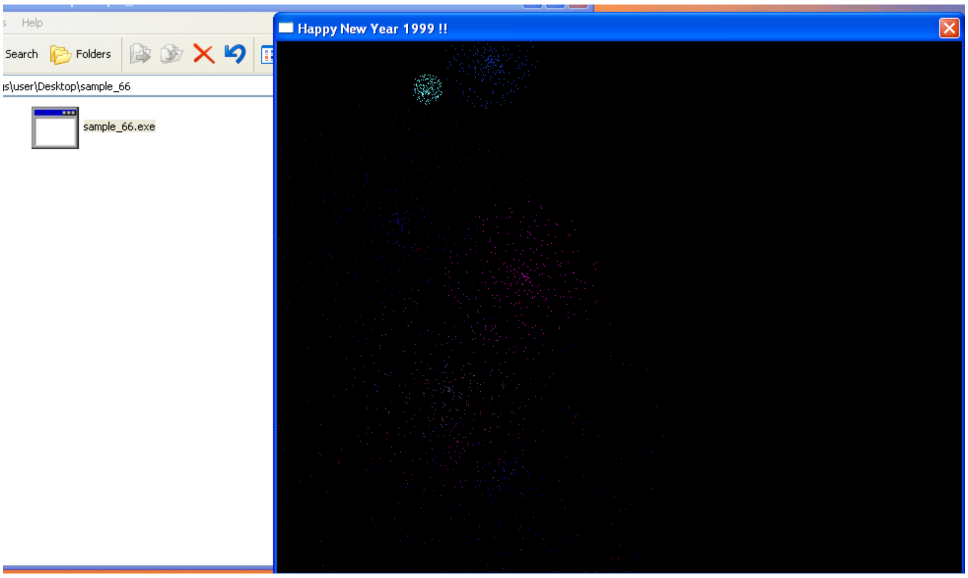
Firstly, we found the strings related to executing the program. The strings are “begin 644 Happy99.exe” & “\Ska.exe”. Happy99 and Ska is the actual name of malware sample 66.

A	[illegible]	[illegible]	0	[illegible]
A	00000000212A	00000043012A	0	WriteFile
A	000000002136	000000430136	0	UnmapViewOfFile
A	000000002148	000000430148	0	GetWindowsDirectoryA
A	000000002160	000000430160	0	GetModuleHandleA
A	000000002174	000000430174	0	CopyFileA
A	000000002180	000000430180	0	GetProcAddress
A	000000002192	000000430192	0	ExitProcess
A	0000000021A0	0000004301A0	0	GetFileSize
A	0000000021AE	0000004301AE	0	GetModuleFileNameA
A	0000000021C4	0000004301C4	0	LocalAlloc
A	0000000021D2	0000004301D2	0	CreateFileMappingA
A	0000000021E8	0000004301E8	0	GetVersionExA
A	0000000021F8	0000004301F8	0	GetSystemDirectoryA
A	00000000220E	00000043020E	0	CreateFileA
A	00000000221C	00000043021C	0	CloseHandle
A	00000000222A	00000043022A	0	LocalFree
A	000000002236	000000430236	0	MapViewOfFile
A	000000002246	000000430246	0	ReadFile
A	000000002252	000000430252	0	RegSetValueExA
A	000000002264	000000430264	0	RegCreateKeyExA
A	000000002276	000000430276	0	RegCloseKey
A	000000002284	000000430284	0	ReleaseDC
A	000000002290	000000430290	0	RegisterClassA
A	0000000022A2	0000004302A2	0	PostQuitMessage
A	0000000022B4	0000004302B4	0	PeekMessageA
A	0000000022C4	0000004302C4	0	GetDC
A	0000000022CC	0000004302CC	0	DispatchMessageA
A	0000000022E0	0000004302E0	0	DefWindowProcA

Secondly, we found strings related to modifications of the registry by creating keys. The strings are “RegCreateKeyExA”, “RegSetValueExA” & “CreateFileA”.

4. Behavioural Analysis

This section will cover the possible finding through performing behaviour analysis on the targeted malware. As mentioned previously when running the malware, it popped up an animated window of fireworks.



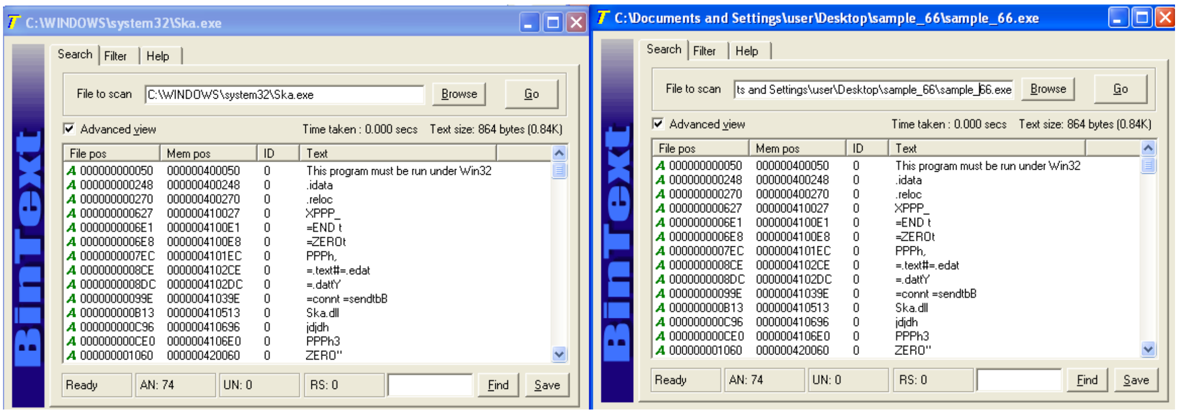
4.1. File Activity

By utilising Procmon, the malware actions can be monitored after being executed. As shown in the image below after the malware is executed, multiple Dynamic Link Library (DLL) are used to display the window of fireworks and modified Windows registry values. A DLL such as advapi32.dll is used to perform various functions such as RegOpenKeyExA and RegSetValueExA to create new Registry Keys and values. (Chappell, 2010)

:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS
:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS
:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS

As shown in [figure] below, the worm self-propagates itself to Windows system32 folder as Ska.exe which contains most of the worm functionality besides being unable to open the file to display the fireworks window.

:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	QueryAttributeInformationVolu	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	QueryBasicInformationFile	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	QueryAttributeInformationVolu	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	SetEndOfFileInformationFile	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	CreateFileMapping	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	QueryStandardInformationFile	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	FASTIO_RELEASE_FOR_SECTION	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	CreateFileMapping	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	FASTIO_RELEASE_FOR_SECTION	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	WriteFile	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	SetBasicInformationFile	C:\WINDOWS\system32\Ska.exe	SUCCESS
:41.0	sample_66.exe	432	CloseFile	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	IRP_MJ_CLOSE	C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe	SUCCESS
:41.0	sample_66.exe	432	CloseFile	C:\WINDOWS\system32\Ska.exe	SUCCESS



It appears that a DLL is packed into Ska.exe. After it is executed, the DLL is extracted from the executable file called Ska.dll into Windows 32 folder. This DLL has two exported APIs ‘mail’ and ‘news’ that cause the worm to send itself to any email (if the email client supports SMTP) or newsgroup postings the user sends.

:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\Ska.dll	SUCCESS
:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32	SUCCESS
:41.0	sample_66.exe	432	CloseFile	C:\WINDOWS\system32	SUCCESS
:41.0	sample_66.exe	432	IRP_MJ_CLOSE	C:\WINDOWS\system32	SUCCESS
:41.0	sample_66.exe	432	WriteFile	C:\WINDOWS\system32\Ska.dll	SUCCESS

After Ska.dll is created, the worm creates a copy of wsock32.dll and names it as wsock32.ska in the system directory. Wsock32.dll file contains Windows Sockets API used by most Internet and network applications to handle network connections (Process Library, no date). It can be seen that wsock32.dll is being modified in a way that allows SKA.exe to run whenever winsock32.dll is in use or started.

:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryAttributeTagFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryStandardInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryBasicInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryStreamInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryBasicInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryEaInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	QueryAttributeInformationVolu	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	QueryBasicInformationFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	QueryAttributeInformationVolu	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	SetEndOfFileInformationFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	CreateFileMapping	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	QueryStandardInformationFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	FASTIO_RELEASE_FOR_SECTION	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	CreateFileMapping	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	FASTIO_RELEASE_FOR_SECTION	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	WriteFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	SetBasicInformationFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS
:41.0	sample_66.exe	432	CloseFile	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	IRP_MJ_CLOSE	C:\WINDOWS\system32\wsock32.dll	SUCCESS
:41.0	sample_66.exe	432	CloseFile	C:\WINDOWS\system32\wsock32.ska	SUCCESS

4.2. Registry Activity

Happy99 malware is known to modify winsock32.dll to allow it to be triggered whenever a connect or send activity is detected. When this online activity occurs, the modified code loads and executes the worm's SKA.DLL file. It is also stated that the worm checks if WSOCK32.DLL is being used in memory. If it is not, the malware will modify WSOCK32.DLL in a way that causes SKA.EXE to run whenever WSOCK32.DLL is started as mentioned previously. If it is in use, the worm modifies the Local Machine registry key that allows it to run once when the machine is started.(Virus Encyclopedia, no date)

As the image shown below, it seems that the worm tried to modify the wsock32.dll file and was unsuccessful due to the wsock32.dll being in use by another program thus sharing violation error occurred. As such, the worm attempted to add an entry to the registry file to execute Ska.exe the next time Windows will be started but access was denied.

59:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\wsock32.dll	SHARING VIOLATION	Desired Access: Generic Read/Write, Disposit
59:41.0	sample_66.exe	432	RegCreateKey	HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce	ACCESS DENIED	Desired Access: All Access, Synchronize
59:41.0	sample_66.exe	432	RegCreateKey	HKLM\Software	SUCCESS	Desired Access: Maximum Allowed

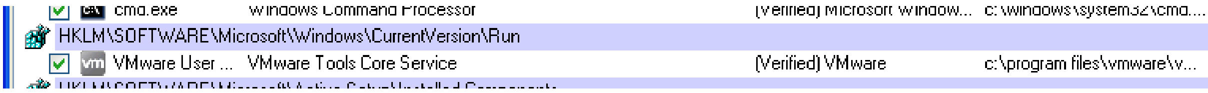
Regshot

By using regshot, any modification made to the registry can be detected. As mentioned previously, the worm tried to create a new key in the registry but was denied access thus no registry keys or value was changed or modified by the worm as shown in the image below. Most key added and modified file paths are \ShellNoRoam\BagMRU which does not spark much suspicious intention as these are to store accessed folder settings.

```
Regshot 1.8.2
Comments:
Datetime:2023/5/7 12:56:00  ,  2023/5/7 12:56:42
Computer:USER-07446B9AB3 , USER-07446B9AB3
Username:user , user

----------------------------------
Keys added:3
----------------------------------
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\43
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\164
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\164\Shell

----------------------------------
Values added:6
----------------------------------
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\hfre\Qrfxgbc\
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\43: 42 00 31 00 00 00 00 00 A1 4C 17 56 10 00 53 41 4D 50 4C 45 7E 31 00 00 2A 00 03 00 04 00 EF BE A1 4C 17 56
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\43\NodeSlot: 0x000000A4
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\43\MRUListEx: FF FF FF FF
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\164\Shell\FolderType: "Documents"
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\user\Desktop\sample_66\sample_66.exe: "sample_66"

----------------------------------
Values modified:5
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 98 9D 53 61 F8 D2 59 F1 67 41 35 01 3D E9 4A 2B 38 72 16 DF EF AF 00 31 B4 88 D0 58 57 11 0C 56 BD 1E 1E E7 CC DD E8 31 2F F0 36 83 3C 8D F5 F8 5F 99 FC 85 40 E7
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 48 FE 08 78 86 2D DE D3 9F 8C B5 95 70 A1 E7 E5 8D C7 4A 50 AC 10 9A B0 3D A4 CD 86 90 43 17 94 14 A2 2F DC 91 DB BC B7 FA 14 C5 97 A0 4E 84 4E 1B 77 00 8D 7C FF
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 15 00 00 00 B1 00 00 00 A0 19 42 42 E3
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 15 00 00 00 B2 00 00 00 E0 67 78 50 E3
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG: 13 00 00 00 5B 00 00 00 E0 7D 52 FB E0
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG: 15 00 00 00 5C 00 00 00 F0 40 08 50 E3
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 00 00 00 00 2A 00 00 00 29 00 00 00 25 00 00 00 28 00 00 00 27 00 00 00 26 00 00 00 24 00 00 00 23 00
HKU\S-1-5-21-2052111302-823518204-682003330-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 2B 00 00 00 00 00 00 00 2A 00 00 00 29 00 00 00 25 00 00 00 28 00 00 00 27 00 00 00 26 00 00 00 24 00

----------------------------------
Total changes:14
----------------------------------
```

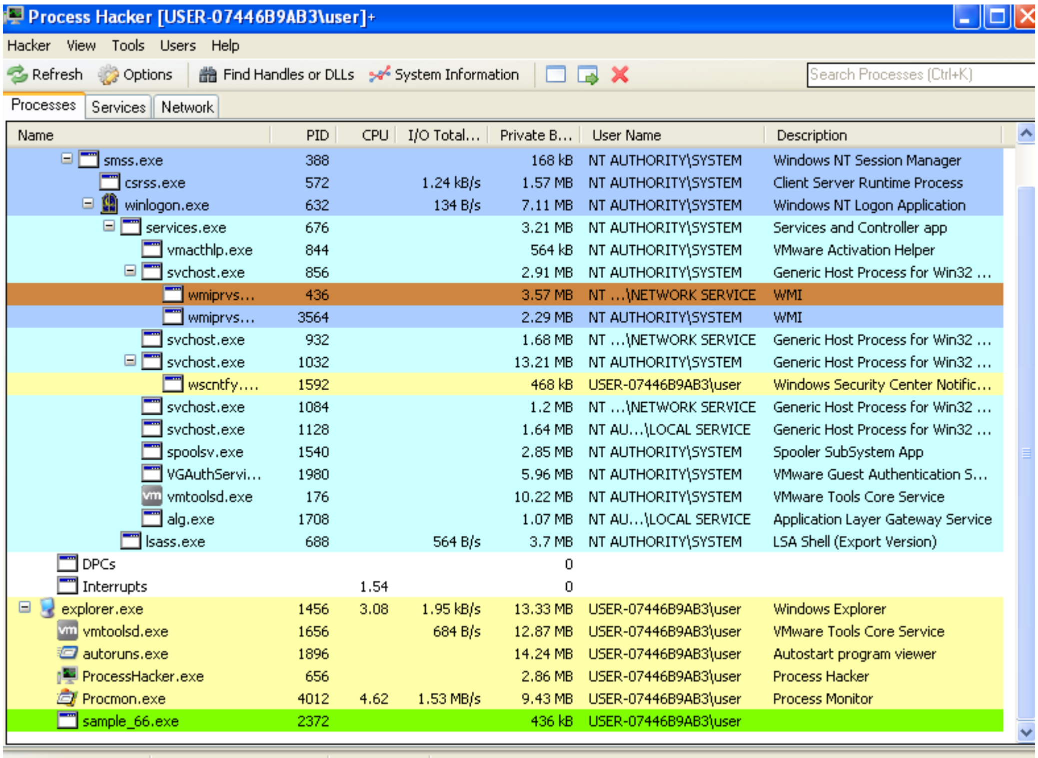
Autorun

Using autorun, a comparison of a before image and a after image can be performed to determine whether the worm is able to successfully create a new registry key to remain persistent after it has been executed. From the image shown below, the malware was unsuccessful in creating a registry key after being executed as mentioned previously and no additional services were added when the malware was executed.



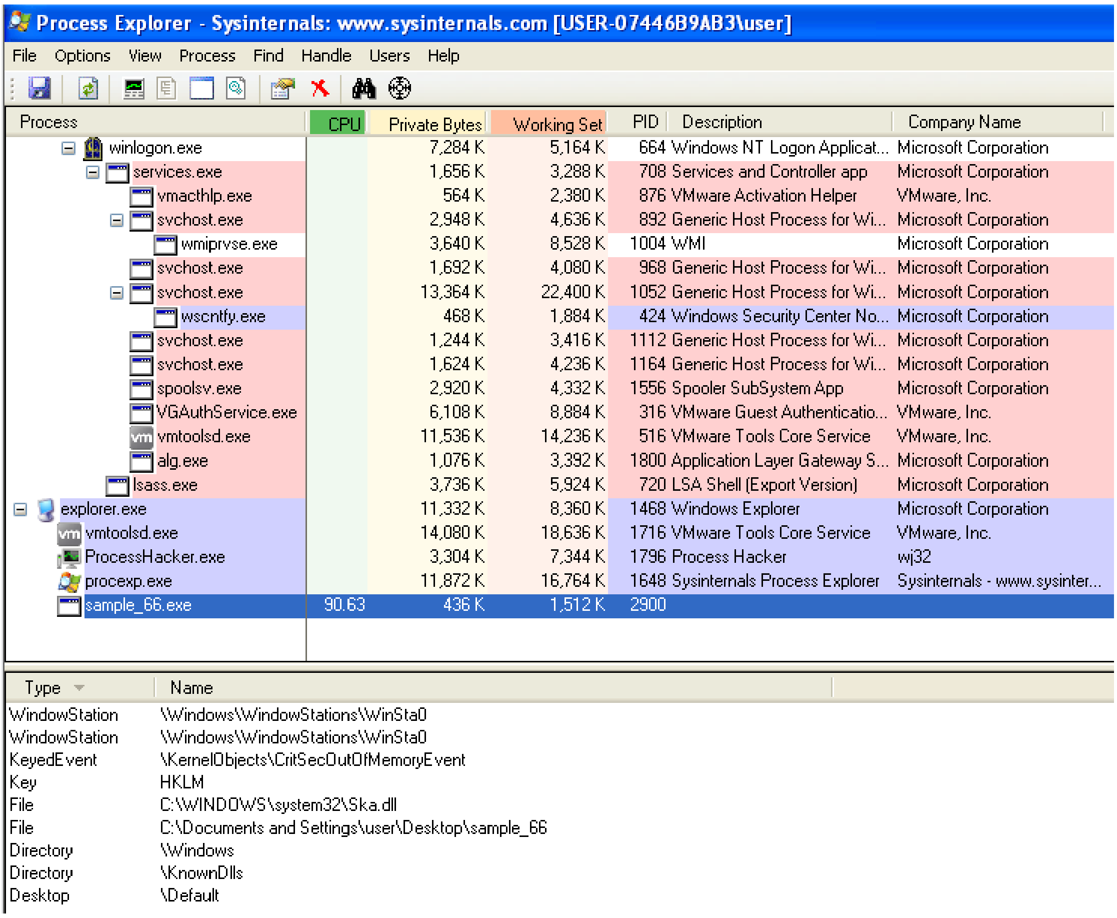
4.3. Process activity

Using Process Hacker, it can be seen that the malware did not run additional processes or services after it has been executed. When the firework window is closed, the process will automatically end.



Mutex

With the use of process explorer, there wasn't any mutex that was used by the malware when it was executed.



Dynamic Link Library (DLL)

Through Process Hacker and Process Monitor, any DLLs used by the malware can be identified and according to [figure number], the malware uses quite a few DLL to load firework pop-up windows and perform other functions. Some **notable** DLLs that the malware uses will be:

- Advapi32.dll: An essential Window process that supports several APIs including security and registry calls. (File.net, no date)
- Rpcrt4.dll: A Remote Procedure Call (RPC) API used by Windows applications for network and Internet communication. Process Library (no date)
- Kernel32.dll: It is a Windows kernel module that runs as a background process and carries out important functions like memory management, I/O operations and interruptions. (Rouse, M., 2016)
- Uxtheme.dll: Responsible for handling the visual themes and appearance customization in windows

Some additional DLL that the malware created and used are wsock32.dll and Ska.dll as mentioned previously about their purpose sample_66.exe (2900) Properties

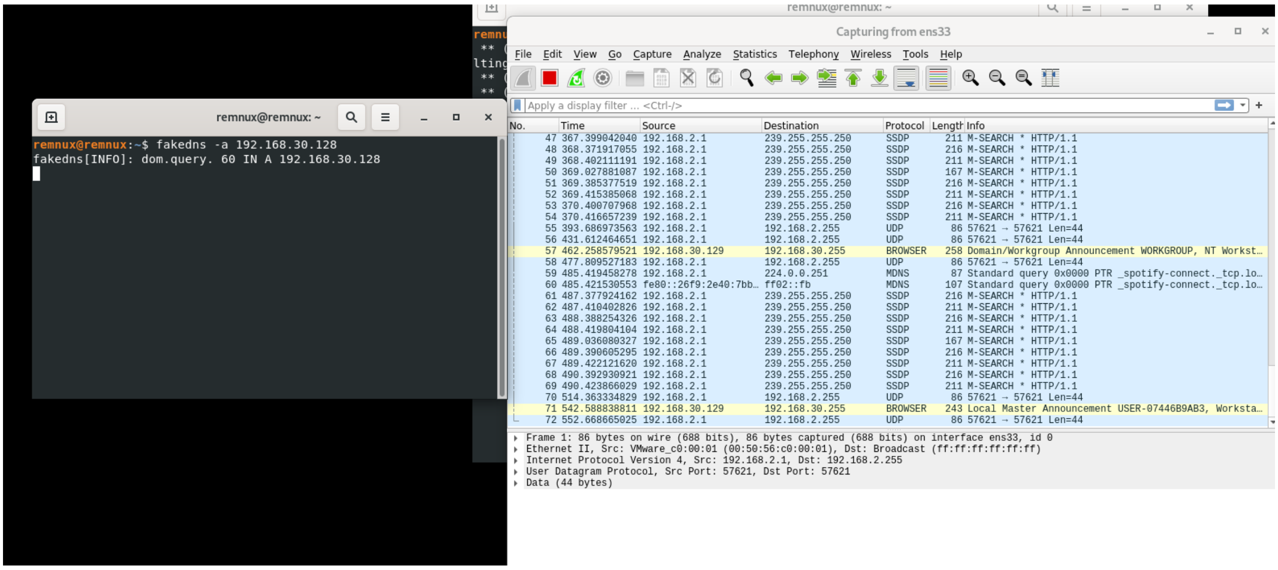
General | Statistics | Performance | Threads | Token | Modules | Memory | Environment | Handles | Comment

Name	Base Address	Size	Description
sample_66.exe	**0x400000**	**320 kB**	
advapi32.dll	0x77dd0000	620 kB	Advanced Windows 32 Base...
ctype.nls	0x890000	12 kB	
gdi32.dll	0x77f10000	292 kB	GDI Client DLL
kernel32.dll	0x7c800000	984 kB	Windows NT BASE API Clien...
locale.nls	0x280000	260 kB	
msvcrt.dll	0x77c10000	352 kB	Windows NT CRT DLL
ntdll.dll	0x7c900000	700 kB	NT Layer DLL
rpcrt4.dll	0x77e70000	584 kB	Remote Procedure Call Runt...
secur32.dll	0x77fe0000	68 kB	Security Support Provider In...
sortkey.nls	0x2d0000	260 kB	
sorttbls.nls	0x320000	24 kB	
unicode.nls	0x260000	88 kB	
user32.dll	0x7e410000	580 kB	Windows XP USER API Clien...
uxtheme.dll	0x5ad70000	224 kB	Microsoft UxTheme Library

Time of	Process Name	PID	Operation	Path	Result
59:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\wsock32.dll	SHARING \
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
59:41.0	sample_66.exe	432	CreateFile	C:\WINDOWS\system32\Ska.dll	SUCCESS
59:41.0	sample_66.exe	432	WriteFile	C:\WINDOWS\system32\Ska.dll	SUCCESS
00:42.6	sample_66.exe	432	CloseFile	C:\WINDOWS\system32\Ska.dll	SUCCESS
00:42.6	sample_66.exe	432	IRP_MJ_CLOSE	C:\WINDOWS\system32\Ska.dll	SUCCESS
59:41.0	sample_66.exe	432	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS
59:41.0	sample_66.exe	432	QueryOpen	C:\WINDOWS\system32\uxtheme.dll	SUCCESS

4.4. Network Activity

Through the use of wireshark and fakedns, any transmission through the network can be identified. The malware did not show any signs of spreading through the network and as mentioned previously the possible cause could be because the malware is not able to modify wsock32.dll file due to sharing violation and was denied access to create a registry key.

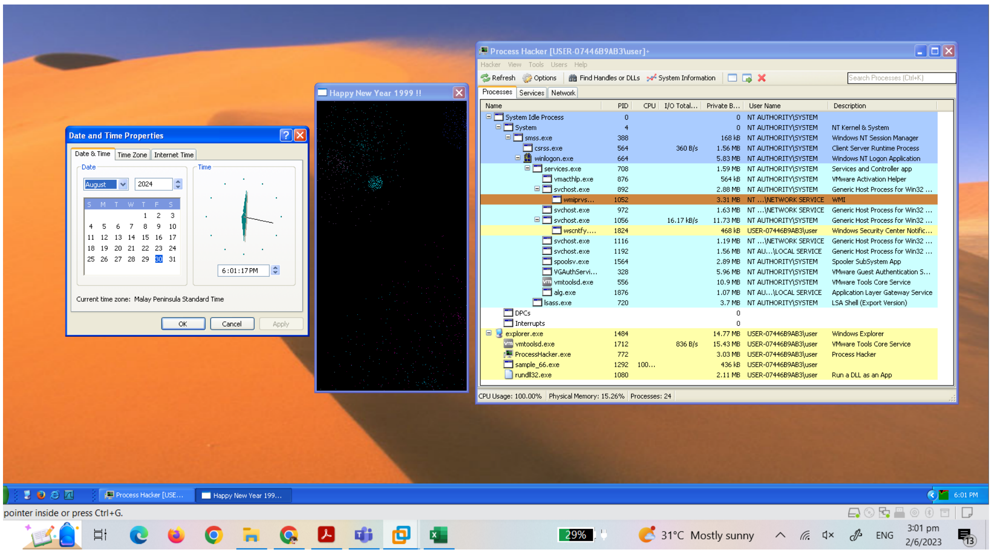


5. Malware Fuzzing

This section will cover the fuzzing of the malware to determine whether it can run normally after changing a few inputs.

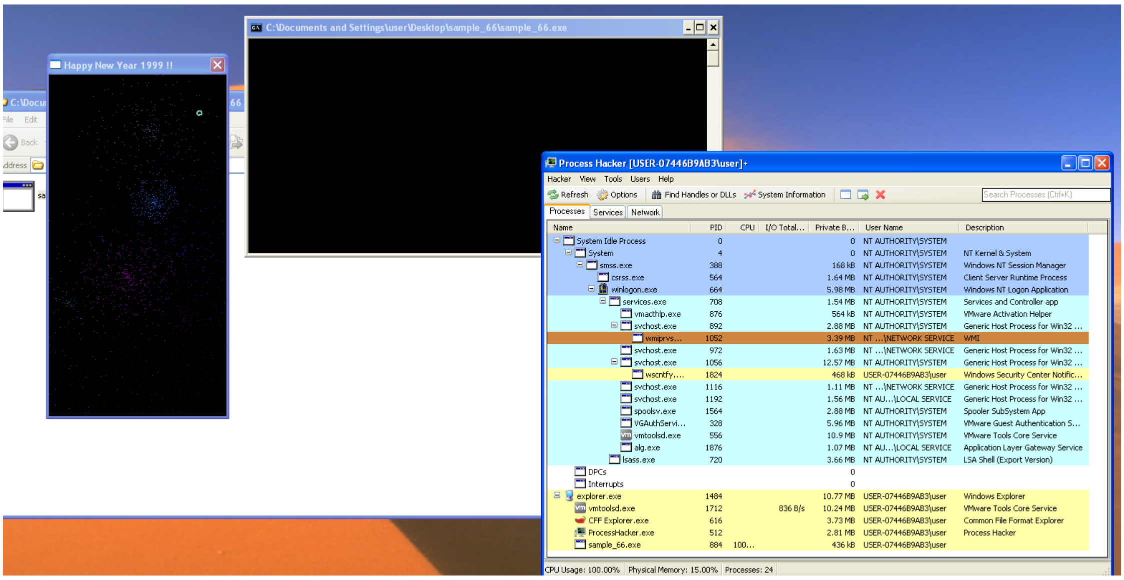
5.1. System time

From the image shown below, we can see that the malware can still be executed and will display an animated window of fireworks even after changing the system time to a different time and a different time zone from the host pc. It should not affect the malware because the malware does not depend on the time to be able to run.



5.2. Subsystem

Other possible fuzzing inputs is to change the subsystem of the malware. Instead of using Windows GUI as the subsystem, it will be changed to Windows Console to determine whether the malware will be able to run. From the image shown below, we can see that the malware is still able to be executed even after changing the subsystem to Windows Console. The window of animated fireworks will still appear but additionally a Window Command prompt is appearing as well. The process for the malware is also shown in process hacker. Upon terminating the command prompt, the malware will be terminated as well and vice versa.



6. Memory Analysis

This section will cover the memory analysis on the malware which will include the different functions, ports, connections and processes used by the malware.

6.1.1. Functions (API)

From the image shown below, some of the main functions that the malware uses are shown such as “CreateFileA” which could possibly for to create Ska.exe in the system directory, “RegCreateKeyExA” which is to create a registry key when Ska.exe is run the next time, “CreateWindowExA” and “ShowWindow” would be used to create and display the animated fireworks window.

Function name	Segment	Start	Length	R	F	L	S	B	T	=
start	CODE	00410000	00000520	R	.	.	.	.	.	.
sub_4105AD	CODE	004105AD	000002E7	R	.	.	.	.	.	.
sub_410894	CODE	00410894	00000018	R	.	.	.	.	.	.
WriteFile	CODE	004108AC	00000006	R	.	.	.	.	T	.
UnmapViewOfFile	CODE	004108B2	00000006	R	.	.	.	.	T	.
GetModuleHandleA	CODE	004108BE	00000006	R	.	.	.	.	T	.
CopyFileA	CODE	004108C4	00000006	R	.	.	.	.	T	.
GetProcAddress	CODE	004108CA	00000006	R	.	.	.	.	T	.
ExitProcess	CODE	004108D0	00000006	R	.	.	.	.	T	.
GetModuleFileNameA	CODE	004108DC	00000006	R	.	.	.	.	T	.
LocalAlloc	CODE	004108E2	00000006	R	.	.	.	.	T	.
CreateFileMappingA	CODE	004108E8	00000006	R	.	.	.	.	T	.
GetVersionExA	CODE	004108EE	00000006	R	.	.	.	.	T	.
GetSystemDirectoryA	CODE	004108F4	00000006	R	.	.	.	.	T	.
CreateFileA	CODE	004108FA	00000006	R	.	.	.	.	T	.
CloseHandle	CODE	00410900	00000006	R	.	.	.	.	T	.
LocalFree	CODE	00410906	00000006	R	.	.	.	.	T	.
MapViewOfFile	CODE	0041090C	00000006	R	.	.	.	.	T	.
RegSetValueExA	CODE	00410918	00000006	R	.	.	.	.	T	.
RegCreateKeyExA	CODE	0041091E	00000006	R	.	.	.	.	T	.
RegCloseKey	CODE	00410924	00000006	R	.	.	.	.	T	.
ReleaseDC	CODE	0041092A	00000006	R	.	.	.	.	T	.
RegisterClassA	CODE	00410930	00000006	R	.	.	.	.	T	.
PostQuitMessage	CODE	00410936	00000006	R	.	.	.	.	T	.
PeekMessageA	CODE	0041093C	00000006	R	.	.	.	.	T	.
GetDC	CODE	00410942	00000006	R	.	.	.	.	T	.
DispatchMessageA	CODE	00410948	00000006	R	.	.	.	.	T	.
DefWindowProcA	CODE	0041094E	00000006	R	.	.	.	.	T	.
CreateWindowExA	CODE	00410954	00000006	R	.	.	.	.	T	.
ShowWindow	CODE	0041095A	00000006	R	.	.	.	.	T	.
UpdateWindow	CODE	00410960	00000006	R	.	.	.	.	T	.
TranslateMessage	CODE	00410966	00000006	R	.	.	.	.	T	.
SetPixelV	CODE	0041096C	00000006	R	.	.	.	.	T	.

6.2. Processes

With kernel detective, an analysis of the physical memory dump of the WinXP infected by the malware can be performed. As the image shown below, the malware process named sample_66.exe does not attempt to hide itself from the EPROCESS list.

```
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTi
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- ------
0x02475da0 winlogon.exe            632 True   True   True     True   True  True    True
0x02503da0 services.exe            676 True   True   True     True   True  True    True
0x02396a48 vmtoolsd.exe           1656 True   True   True     True   True  True    True
0x0238c650 wscntfy.exe            1592 True   True   True     True   True  True    True
0x021c5020 svchost.exe             856 True   True   True     True   True  True    True
0x02380c88 svchost.exe             932 True   True   True     True   True  True    True
0x023a07a0 wmiprvse.exe            436 True   True   True     True   True  True    True
0x020aa020 firefox.exe            1232 True   True   True     True   True  True    True
0x024924e0 VGAuthService.e        1980 True   True   True     True   True  True    True
0x0204eb28 spoolsv.exe            1540 True   True   True     True   True  True    True
0x024e8c10 vmacthlp.exe            844 True   True   True     True   True  True    True
0x024c7570 svchost.exe            1084 True   True   True     True   True  True    True
0x02365980 explorer.exe           1456 True   True   True     True   True  True    True
0x0242bda0 svchost.exe            1032 True   True   True     True   True  True    True
0x02299540 zzzzzz.exe             4028 True   True   True     True   True  True    True
0x0204dda0 svchost.exe            1128 True   True   True     True   True  True    True
0x0238fa78 alg.exe                1708 True   True   True     True   True  True    True
0x02046da0 vmtoolsd.exe            176 True   True   True     True   True  True    True
0x02169508 sample_66.exe          2656 True   True   True     True   True  True    True
```

6.3. Connections

As shown in the image below, after running a connection scan, it shows that the malware did not attempt to make any connection to another remote address as all connections are made from PID 1232 which is from firefox.exe and not PID 2656 which is the malware executable. As such, all the connections shown below are web browsing attempts made by browsing through firefox.

```
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01f68008 127.0.0.1:1145            127.0.0.1:1144            1232
0x02087008 192.168.30.129:1174       192.168.30.128:443        1232
0x02216008 192.168.30.129:1177       192.168.30.128:443        1232
0x02285a68 127.0.0.1:1144            127.0.0.1:1145            1232
0x02352c08 192.168.30.129:1151       192.168.30.128:443        1232
0x0238b008 192.168.30.129:1173       192.168.30.128:443        1232
0x024573e0 3.0.132.2:25185           0.153.228.129:21353       2178403168
0x0752da68 127.0.0.1:1144            127.0.0.1:1145            1232
0x08dcf008 192.168.30.129:1173       192.168.30.128:443        1232
0x0defec08 192.168.30.129:1151       192.168.30.128:443        1232
0x0efbd008 192.168.30.129:1177       192.168.30.128:443        1232
0x10cf1c08 192.168.30.129:1151       192.168.30.128:443        1232
0x16869008 192.168.30.129:1173       192.168.30.128:443        1232
```

6.4. Ports

Running a sock scan allows us to determine whether any ports are opened by the malware to perform unauthorised tasks or access. The image below shows the list of ports that are opened by the different executable and none of them are opened by the malware with a PID 2656 because the malware was not able to create the registry key mentioned above.

Offset(P)	PID	Port	Proto	Protocol	Address	Create Time
0x01f67e98	1232	1172	6	TCP	0.0.0.0	2023-05-15 09:47:34 UTC+0000
0x01f69950	1032	123	17	UDP	127.0.0.1	2023-04-25 07:46:13 UTC+0000
0x01f71e98	4	138	17	UDP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x01f7e438	1232	1144	6	TCP	127.0.0.1	2023-05-15 09:46:25 UTC+0000
0x01f83e68	1232	1171	6	TCP	0.0.0.0	2023-05-15 09:47:34 UTC+0000
0x02055610	1232	1165	6	TCP	0.0.0.0	2023-05-15 09:47:29 UTC+0000
0x021c1c08	4	445	6	TCP	0.0.0.0	2023-04-18 06:17:12 UTC+0000
0x021c2e98	4	445	17	UDP	0.0.0.0	2023-04-18 06:17:12 UTC+0000
0x021de008	1084	1050	17	UDP	0.0.0.0	2023-04-18 06:20:54 UTC+0000
0x021e7da0	1232	1166	6	TCP	0.0.0.0	2023-05-15 09:47:30 UTC+0000
0x0221b008	1084	1051	17	UDP	0.0.0.0	2023-04-18 06:20:55 UTC+0000
0x0221ce98	4	139	6	TCP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x0227ba10	1128	1900	17	UDP	127.0.0.1	2023-04-25 07:46:13 UTC+0000
0x022bfa48	1032	123	17	UDP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x0233d768	1128	1900	17	UDP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x02349878	1232	1169	6	TCP	0.0.0.0	2023-05-15 09:47:33 UTC+0000
0x023556f0	688	0	255	Reserved	0.0.0.0	2023-04-18 06:17:28 UTC+0000
0x0238c2c8	1032	1026	17	UDP	127.0.0.1	2023-04-18 06:17:50 UTC+0000
0x023a0d88	1708	1030	6	TCP	127.0.0.1	2023-04-18 06:17:51 UTC+0000
0x023a48f8	688	4500	17	UDP	0.0.0.0	2023-04-18 06:17:28 UTC+0000
0x023b1688	1232	1168	6	TCP	0.0.0.0	2023-05-15 09:47:33 UTC+0000
0x023b3708	1232	1167	6	TCP	0.0.0.0	2023-05-15 09:47:31 UTC+0000
0x0240dd98	1232	1174	6	TCP	0.0.0.0	2023-05-15 09:47:36 UTC+0000
0x024128a0	1232	1145	6	TCP	0.0.0.0	2023-05-15 09:46:25 UTC+0000
0x02426b90	1084	1025	17	UDP	0.0.0.0	2023-04-18 06:17:35 UTC+0000
0x02497750	688	500	17	UDP	0.0.0.0	2023-04-18 06:17:28 UTC+0000
0x024c8e98	932	135	6	TCP	0.0.0.0	2023-04-18 06:17:14 UTC+0000
0x024d6008	1232	1176	6	TCP	0.0.0.0	2023-05-15 09:47:37 UTC+0000
0x02518540	4	137	17	UDP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x07775878	1232	1169	6	TCP	0.0.0.0	2023-05-15 09:47:33 UTC+0000
0x0778eda0	1232	1166	6	TCP	0.0.0.0	2023-05-15 09:47:30 UTC+0000
0x0c19b708	1232	1167	6	TCP	0.0.0.0	2023-05-15 09:47:31 UTC+0000
0x0e1c16f0	688	0	255	Reserved	0.0.0.0	2023-04-18 06:17:28 UTC+0000
0x0eac3e98	4	139	6	TCP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x0f0c4008	1084	1050	17	UDP	0.0.0.0	2023-04-18 06:20:54 UTC+0000
0x12de2708	1232	1167	6	TCP	0.0.0.0	2023-05-15 09:47:31 UTC+0000
0x1be5de98	4	139	6	TCP	192.168.30.129	2023-04-25 07:46:13 UTC+0000
0x1c737708	1232	1167	6	TCP	0.0.0.0	2023-05-15 09:47:31 UTC+0000

7. Conclusion

7.1. Spreading method

Happy99, also known as the Happy99 worm, was a malware that spread primarily through email attachments. It utilised social engineering techniques to entice users into opening the infected attachment, which was often disguised as a harmless fireworks animation or screensaver file named "Happy99.exe." The worm would infect the victim's computer upon execution, modifying the WSOCK32.DLL file responsible for network communication. Once installed, Happy99 had the ability to automatically send itself to the user's email contacts by attaching itself to outgoing email messages. By leveraging email as its primary propagation method, Happy99 quickly spread to other users who unknowingly executed the infected attachment.

7.2. Detection method

The Happy99 worm could be detected using antivirus software that had specific signatures for identifying the worm. Additionally, network intrusion detection systems could potentially spot the worm's activity by analysing network traffic for suspicious patterns or known signatures associated with Happy99.

7.3. Patches and updates (Removal)

As an old and outdated malware from the late 1990s, the Happy99 worm did not have official patches or updates released by its creators. However, antivirus companies and security researchers have developed signatures and updates for their software to detect and remove the worm from infected systems.

7.4. Manual Removal

Most virus scanning tools will detect and clean Happy99 from a system. Happy99 can be manually removed from affected systems. You must update your scanning tools with the most recent virus signatures or definitions in order to identify and eliminate current viruses. Setting the WSOCK32.DLL file attributes to "read only" will stop the Happy99 from spreading. Additionally, we advise you to get in touch with everyone on the LISTE.SKA file's list. This file contains a list of additional individuals who may have been given the Happy99 Trojan horse by you. (Kasperky, no date)

7.5. FixHappy Tool

The FIXHAPPY tool is specifically designed to safely remove Happy99.Worm (also known as W32.Ska) files and restore the WSOCK32.DLL in Windows systems. It performs several important tasks to achieve this. First, it deletes the SKA.EXE and SKA.DLL files from the Windows System directory, typically located at C:\WINDOWS\SYSTEM. These files are inserted by the Happy99.Worm during its installation on the system. (Symantec, no date)

Furthermore, FIXHAPPY restores the original WSOCK32.DLL file. The Happy99.Worm modifies this file to intercept and control the mail-sending and newsgroup article-posting routines. (Symantec, no date)

In addition to file operations, FIXHAPPY removes a specific Windows Registry modification made by the worm. It deletes the following entry: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce=SKA.EXE. The Happy99.Worm adds this entry to the Windows Registry if the worm's attempt to modify WSOCK32.DLL is unsuccessful due to the file being in use (for example, when a user is online or connected to a network). (Symantec, no date)

It's important to note that while FIXHAPPY addresses the removal of Happy99.Worm-related files and the restoration of the WSOCK32.DLL, the tool does not delete the actual Happy99.Worm file itself. It's recommended to manually delete the HAPPY99.EXE file (the file recognized by NAV as "Happy99.Worm") separately. By utilizing FIXHAPPY and removing the associated files, users can effectively eliminate the Happy99.Worm and its modifications from their Windows systems. (Symantec, no date)

7.6. Malware Mitigation

Happy99, also known as the Happy99 worm, was a malware that spread via email attachments in the late 1990s. While Happy99 is an outdated and obsolete malware, there are different ways to prevent the system from being infected. A few ways mentioned below are ways that can help to prevent infected by the malware on your machine:

1. **Use Reliable Security Software:** Install and regularly update a reputable antivirus or anti-malware program to detect and block known malware.
2. **Keep Software Updated:** Maintain up-to-date operating systems, web browsers, plugins, and other software to ensure you have the latest security patches that address known vulnerabilities.
3. **Exercise Caution with Email:** Be cautious when opening email attachments or clicking on links in emails, especially if they are unexpected, suspicious, or from unknown senders.
4. **Enable Firewall:** Enable and configure a firewall to filter incoming and outgoing network traffic, providing an additional layer of protection.
5. **Educate Yourself:** Stay informed about the latest malware threats, techniques, and common indicators of compromise to enhance your ability to identify and avoid potential risks.

8. Recommendations

8.1. Security Policies

Strict security procedures will make it less likely for businesses to fall victim to social engineering or phishing attacks that install backdoors. These regulations protect the business's security and shield it from malware assaults. Businesses must spend time and money educating their staff about these security procedures. Users who are familiar with the security policies are less likely to start an outbreak in the company, despite the fact that this is not a completely foolproof method.

8.2. Advanced email & collaboration security

Companies should use Mimecast which is a cloud-based email security and management service. It provides varieties of features that can help prevent risk related with malware like Happy99. Although Happy 99 is outdated , email security measures from Mimecast can still help with overall security. A further line of defence is offered by Mimecast's URL and link protection feature, which scans and examines links within emails to find any potential phishing attempts or malicious websites.

9. Fileless Malware

In an ever-evolving landscape of cyber threats, malware is constantly adapting and evolving posing significant challenges to cyber security professionals. Among the various types of malware, fileless malware has emerged as an elusive and stealthy form of malicious software.

Introduction

Malware is a malicious software or program that exploits a computer system and obtains the user's information stored in the system. Fileless malware is a type of malicious software that utilises legitimate programs to execute a cybersecurity attack and was developed by attackers to make it hard for antivirus to detect one that might be in the system. Unlike traditional malware, fileless malware does not require an attacker to install any code or files on the target's system and leave no footprint, making it a challenge to detect and remove. (Baker, K., 2023) While attackers do not need install codes to launch an fileless attack, the attackers still need access to the environment so that they can modify its native tools to serve their purpose. The few common tactics attackers use to gain access are:

- Social engineering schemes like phishing emails.
- Using compromised credentials, using password-cracking tools or other methods to obtain them.

During fileless attack, threat actors will infiltrate, take control, and perform malicious activities by exploiting vulnerable software that end users might use daily such as Microsoft Word, browser or software that is pre-installed on the computer. (Aqua, no date)

9.1. Type of fileless malware attack

With the evolution of fileless malware, many different types of fileless malware have been developed. These are some of the fileless malware types:

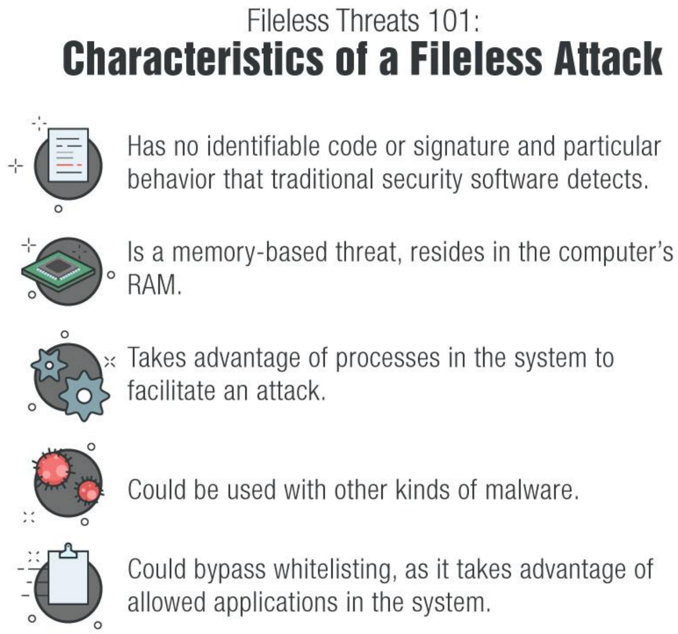
- **Windows Registry Manipulation Malware:** It involves the use of a malicious file that takes advantage of a trusted Windows process. When clicked on the file or link, it uses a normal windows process to write and execute the fileless code into the registry. By manipulating the registry instead of working through an application, the malware can remain persistent and hide from detection tools. (Fortinet, no date)
- **Memory-Only Malware:** This technique involves hiding malicious code in the memory of legitimate applications. The malware will distribute and reinject itself into processes that are running and are critical to Windows activity. These attacks leverage known vulnerabilities in browsers and programs such as Java, Flash and phishing campaigns to gain entry and run the malicious code in the target's computer memory. **(**Johansen, A.G., no date)
- **Fileless Ransomware:** With the evolution of malware, ransomware attackers are leveraging fileless techniques to embed malicious code into existing documents using native languages such as macros or writing the malicious code directly into the memory through the use of an exploit. This enables the ransomware to hijack native tools like Powershell to encrypt and hold files hostage without writing any line to the disk. (Baker, K., 2023)

- **Exploit Kits:** Exploit kits are a collection of exploits which includes exploits for a number of vulnerabilities and a management console that the attacker can use to control the system.. Adversaries use these tools to take advantage of vulnerabilities on a victim's computer. It is an efficient way for an attacker to launch a fileless malware attack because it can be injected directly into the memory without writing any line to the disk. The attack generally begins through social engineering or phishing email. Once the malware infiltrates the machine, the exploit kit can scan the system to determine the vulnerability and it can craft and launch a customised exploit. Oftentimes the malware is able to go undetected and gain extensive access to system and data. (Baker, K., 2023)
- **Script-based malware:** Scripts is a popular attack vector for compromising a system. Script-based malware is used to exploit the vulnerability in MS Office, Windows applications and Windows Powershell. (Khushali, V., 2020) With scripts, it can provide an initial point of access to a computer, which allows payload delivery and lateral movement. The payload will carry out desired actions such as collecting information and encrypting files. To prevent it from being detected, the hackers will usually lean on trusted Windows applications for their attack. (Uzer, S., 2021)

Characteristics of Fileless malware

Fileless malware exhibits several unique characteristics that can distinguish itself from traditional malware. Understanding these characteristics is crucial in recognizing and defending against fileless malware attacks. Below are some of the characteristics of fileless malware:

- **Memory-Based Malware**: Unlike traditional malware that relies on executable files that are stored on the hard drive, fileless malware resides primarily in a computer's volatile memory (RAM). (Zhang, E., 2018)
- **Exploit of legitimate tools**: Fileless malware uses trusted applications, scripts, system utilities that are already on the targeted system to carry out the attack. (Zhang, E., 2018)
- **Evasion of Anti-Virus**: Fileless malware has no identifiable code or signature that standard anti virus tools are able to detect it. It does not exhibit a particular behaviour therefore, a heuristic scanner cannot identify it as a malicious software. (Zhang, E., 2018)
- **Pairing with another malware:** Fileless malware can be combined with other types of malware to facilitate a complex cyberattack. (Zhang, E., 2018)

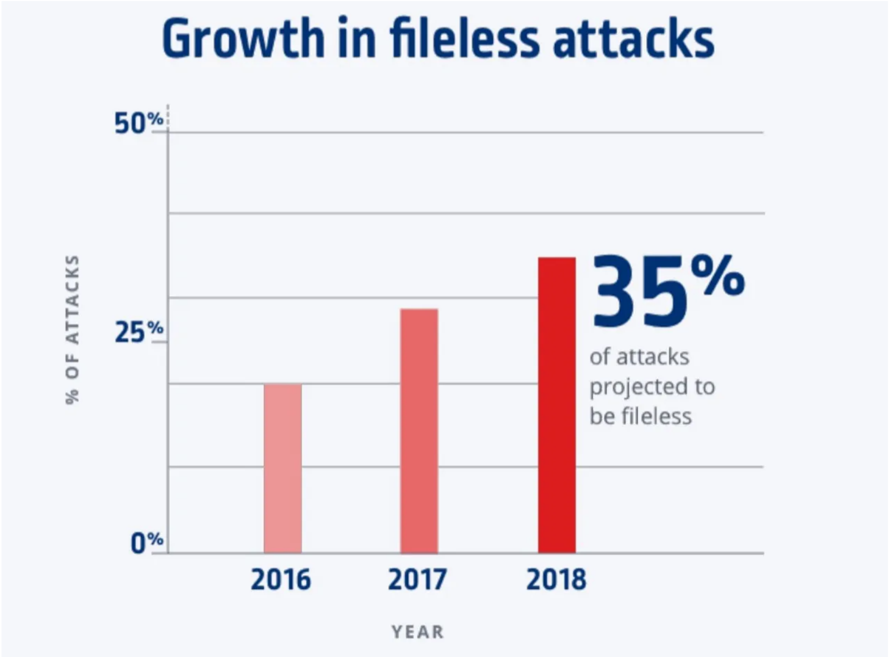


(Image link for characteristics https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems)

Development of Fileless Malware

The term fileless malware made its first appearance in 2001 with the Code Red worm. This worm exploited a buffer overflow vulnerability in Microsoft IIS web server and was the first code to be categorised as fileless malware. The worm was found to be run only in the memory of the infected machine. (Prevost, S., 2023)

In 2017, Fileless malware emerged as a mainstream type of attack, but many of these attack methods have been around for a while. Frodo, Number of the Beast, and The Dark Avenger were all early examples of this type of malware. (Trelix, no date) Mainly the reason fileless malware has become more prevalent was because of the exfiltration of data from 150 million Equifax customers through a vulnerability in the Apache Struts web application framework.



(Image link reference https://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/)

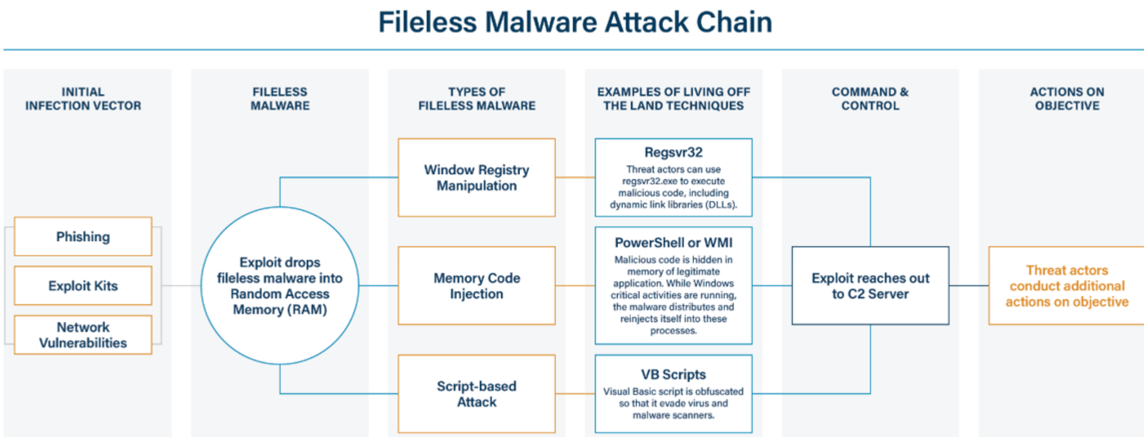
Fileless malware attacks have been seen to hide their code in benign files or invisible registry keys. Some of the fileless attacks use a framework called CactusTorch in a malicious document. (Arntz, P., 2021) CactusTorch is a framework for payload generation in adversary simulation engagements based on James Forshaw's DotNetToJScript tool. (MDSec Research, no date)

Other techniques that attackers have to consider when developing a fileless malware to execute and operate in the system memory are:

- **Payload:** The payload in the malware is the most important component as it consists of the scripts and commands that are being executed on the memory. The payload can be written in scripting languages such as Javascript, Visual Basic and Powershell. (Buckbee, M., 2022)
- **Code Obfuscation:** To evade any detection and analysis, malware developers would obfuscate the code within the malware. Obfuscation techniques can include encryption, code splitting, encode and data masking. These methods make it harder to detect the intent behind the program and hides the actual code.
- **Persistence techniques:** To allow the malware to be able to remain in the victim system, malware developers would develop the malware to tamper with the registry keys, leverage system services and exploit startup keys. (Daulaguphu, S., 2022)
- **Evasion techniques:** Malware developers implement various evasion techniques to avoid security solutions. These techniques include antivirus evasion such as packers to hide the content of the files; network security evasion such as firewall,intrusion detection system (IDS), intrusion prevention system (IPS); sandbox evasion.

How Fileless Malware Works

Fileless malware can be effective in performing malicious activity because it is hiding a victim system without having the need to use a malicious software or files as an entry point and does not need a cybercriminal to install harmful code onto a victim's machine since it is not a file based malware but a memory malware. In figure[] shows an example of how a fileless malware attack will occur in a computer system.
(this link is for the image below https://www.cisecurity.org/insights/blog/only-in-memory-fileless-malware-an-elusive-ttp) Fileless malware attack chain with examples



The few evasion techniques that are mentioned below are commonly used techniques that fileless malware uses to prevent detection by detection techniques such as antivirus.

- **Malicious Documents**
    - Most documents downloaded by adversary supplies and email attachment. Scripts abilities to launch programs and download malicious code and run directly in the memory to be a part of the fileless injection. (Khushali, V., 2020)
- **Malicious scripts**
    - Adversaries are able to utilise Microsoft Windows script interpreters for Powershell, VBScript, batch files and Javascript. (Khushali, V., 2020) With the advantages of using scripts, the attackers are able to interact with the OS without restrictions that some applications such as web browsers might impose on the scripts.
- **Living off the land**
    - Attackers only utilise already installed software on the machine to conduct attacks. Once the malicious code can interact with the local programs, it will start with infecting a document, and misuse the OS to download malicious artifacts, launch malicious programs and steal data, move laterally and maintain persistence. (Khushali, V., 2020)
- **Malicious code in memory**
    - Memory is volatile and dynamic and gives an opportunity to malware to change in its shape and operate at a blind spot of antivirus and other detection technologies. When an attacker executes malicious

codes on the endpoint, the adversary can unpack the malware into the memory without writing any files to the disk. (Khushali, V., 2020)

These are a few scenarios in which a fileless malware can utilise your system's software, applications and protocol to install and execute malicious activities on your system. **(**Johansen, A.G., no date)

- **Phishing emails, malicious downloads, and links that look legitimate as a point of entry. (**Johansen, A.G., no date)
    - When a user clicks on these links, the malware is loaded into the user's PC memory, which enables the hacker to remotely load codes via scripts that are able to capture and share confidential data within the system. **(**Johansen, A.G., no date)
- **Utilise applications that you've already installed such as Microsoft Word, Excel or Javascript. (**Johansen, A.G., no date)
    - Malicious code can be injected into already-installed, trusted programs that reside within the user's system which can be hijacked and executed. **(**Johansen, A.G., no date)
- **Native and highly trusted applications like Windows Management Instrumentation (WMI) and Windows Powershell. (**Johansen, A.G., no date)
    - Fileless malware targets these applications remotely. It makes it more challenging for security programs and analysis to catch. In a powershell attack, fileless malware embeds malicious scripts into legitimate powershell scripts which essentially run together with the normal process. **(**Johansen, A.G., no date)
- **Lateral Infiltration (**Johansen, A.G., no date)
    - Fileless malware attacks are widespread due to tools like Windows Powershell which can be used to infiltrate other machines. **(**Johansen, A.G., no date)

A fileless malware attack is fairly unique in the way its function. Understanding how it operates allows the organisations to protect against the attack. The key stages of a fileless malware attacks are: (Aqua, no date)

1. **Malware gains access to the machine**
   Before an attacker is able to perform the malware attack fully, they must first gain access to a machine. Oftentimes the attacker will use social engineering tactics or phishing email to gain access to the machine. (Aqua, no date)

2. **Execution**
   After the fileless malware gains access to the machine, it will use various techniques such as manipulating software, libraries or other pre-installed programs to steal credentials within the environment it infiltrated. This allows the attacker to freely navigate to other systems in the environment. (Aqua, no date)

3. **Establish Persistence**

After gaining access, the malware would establish a backdoor to allow the hacker to access the machine at any time they want. The main purpose is to avoid losing access to the device so information gathering can be over a long period of time. (Aqua, no date)

4. **Data Exfiltration**
   In this last step, the attacker will steal or intercept data and exfiltrate it to another environment. This allows the attacker to procure sensitive data over a long period of time. (Aqua, no date)

Tools used in behavioural analysis

The following are some tools that can be used and are effective against fileless malware.

- **Process Monitor:** Procmon is a tool that can monitor and capture system level activity in real time such as process creations and registry changes. It can provide detailed information on processes, registry activity, file system operations and network connections. It is great for spotting persistent malware and comes with several filters that will enable you to see parent/child relationship between executable. (Cirelly, J., 2022) As fileless malware can utilise registry keys to maintain persistence, procmon is able to identify modified registry keys that fileless malware might modified.

- **Procdot:** Procdot allows a malware analyst to ingest input from Procmon and generate a graphical presentation of the captured data. It allows security analysts to analyse recorded malware activity easily rather than creating filters and navigating through thousands of events. (Fox, N., 2022)

- **Autoruns:** Autorun is a Microsoft tool that will display any installed software or processes that is configured to run when a machine is powered on. Fileless malware is configured to remain persistent after reboot and by doing so, it has to create or modify the registry values. By using autorun, it can detect and highlight the persistent software and technique the fileless malware implemented. (Fox, N., 2022)

- **Wireshark:** Wireshark is a tool for capturing and analysing network traffic. It allows deep packet inspection of multiple protocols at multiple layers. Using wireshark, analysts can look for patterns and anomalies that might indicate the presence of a fileless attack. However even fileless malware cannot avoid being stored in the network traffic logs if the initial infection is via a network connection. (Howard Poston, 2019) Some fileless malware attacks often establish connections with a command & control (C&C) server to receive instructions or exfiltrate data. Analysts can use wireshark to follow conversations between the C&C and the malware.

Behavioural Analysis on fileless malware

Since fileless malware is not like a traditional malware, traditional antivirus software might not be effective in trying to detect fileless malware. In addition, detection based on signatures, rules and scan cannot catch fileless attacks. Instead of looking for malicious files, anomalous behaviour should be used to identify activities that might indicate a fileless attack is occuring. (Aqua, no date) Behavioural analysis can help in identifying abnormal and suspicious activities that might have evaded detection tools or software. (Aqua, no date) Using behavioural analysis has its pros and cons. Some pros and cons are mentioned below.

Pros:

- **Keep track of unusual modifications:** Keep track of unusual modifications to software and applications like PowerShell and WMI. (Trend Micro, 2020)
- **Few false negatives**: Indicators that are marked as non-suspicious, but could be a suspicious malware performing unauthorised actions. (Oliver Rochford, 2021)
- **Detect hidden malware:** Behaviour analysis will be able to detect abnormal and suspicious activities that have evaded other detection technologies. (Aqua, no date)
- **Real time monitoring:** Behavioural analysis tools can provide real time monitoring capabilities which allows for immediate detections and response of fileless malware threats.
- **Detecting unknown malware:** Behavioural analysis tools can detect previously unknown malware based on its behaviour. By running the malicious code in a sandbox, security experts are able to observe the malware behaviour.

Cons:

- **High false positive rate:** Indicators that are marked as suspicious, might not be an attack but a normal thread process. (Oliver Rochford, 2021)
- **Evasion techniques:** Malware is able to behave like a legitimate process which makes it hard to detect.
- **Excessive analysis time:** The analysis can be time consuming as it might be hard for the SOC team or in-house engineer to track the damage done,the scope of the attack and trace of the infected malware. (Hioureas, V., 2018)
-

Others ways and tools the malware can be analysed

Apart from performing behavioural analysis on a fileless malware, there are several other analysis methods that can be used to analyse fileless malware. The few methods are:

- **Memory analysis:** Memory analysis can examine malware hooks and codes outside the function normal scope. (Khushali, V., 2020) Memory forensics techniques can analyse, detect malware that solely reside in the memory and monitor malware behaviours such as API hooking, DLL injection and hidden process. (Ilker Kara, 2022)
- **Endpoint Detection and Response (EDR):** EDR solution can monitor all activities in the information system. Custom rules can be created to hunt or

stop any threats. EDR can perform real-time monitoring of outgoing and incoming network traffic, phishing emails and suspicious activities in programs like Powershell and Windows Management Instrumentation (WMI). (Fakhar Imam, 2019)

- **Indicator of attacks (IOA):** IOA is an efficient method for locating fileless malware because you can detect the behaviour associated with the malware as opposed to a specific file that has been introduced to your computer. IOA looks for signs that an attack may be in progress. Signs such as code execution, lateral movements and actions that seem to be intended to cloak the intruder's true intent. (Baker, K., 2023)

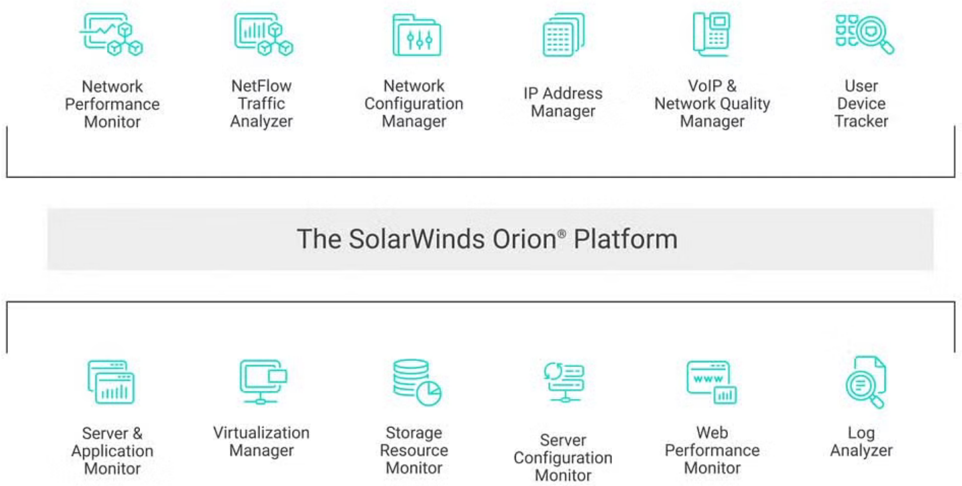
10. Dropper Malware

10.1. Introduction

A malicious application called a Trojan dropper is made to spread other viruses to a victim's computer or phone. Most often, droppers are Trojans which are programs that imitate or contain a useful application for the user. A key generator (also known as a keygen) for a counterfeit copy of a suite of commercial software serves as an example. (Oladimeji, S. and Kerner, S.M, 2022)

One of the largest cybersecurity attacks to happen in the 21st century was the SolarWinds hack. The SolarWinds hack was a big deal since thousands of companies, including the US government, were harmed by a much bigger supply chain disaster than the intrusion of just one corporation. (Oladimeji, S. and Kerner, S.M, 2022)

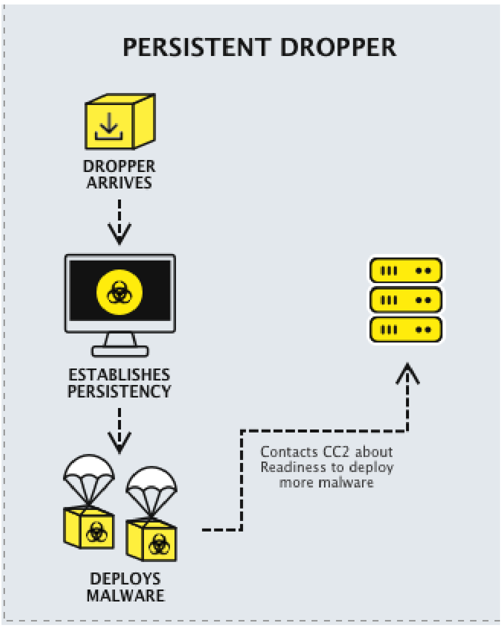
The Orion IT monitoring and management software from SolarWinds, used by thousands of businesses and government organisations worldwide, was compromised by hackers with a dropper. (Oladimeji, S. and Kerner, S.M, 2022)



https://www.solarwinds.com/orion-platform.

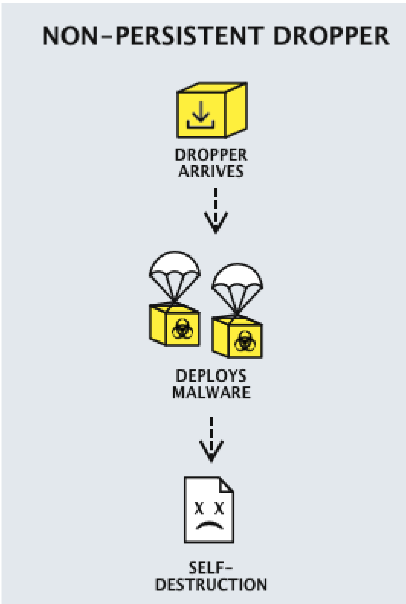
10.2. Types of Dropper malware

- **Persistent Dropper**: As soon as the malware is run, it hides itself on the device, making it extremely dangerous. The system registry keys are then changed. Even if the malware is removed, the hidden file will run when the system reboots. This enables it to reinstall the malware even after it has been taken down. (Kaspersky, no date)



https://gridinsoft.com/dropper

- **Non-Persistent dropper**: Because it leaves the system after delivering its payload, it is less dangerous. In this manner, the malware won't be able to reinstall itself after being removed.(Kaspersky, no date)



https://gridinsoft.com/dropper

10.3. How Dropper Malware works

Most of the time, droppers don't carry out any malicious actions. A dropper's main objective is to covertly install additional malicious software, or its "payload," on the target device. A dropper already has the necessary components, as opposed to a downloader, which gets them from the attackers' server. It extracts the payload before launch and stores it in the device memory. Malware installers can also be launched by a dropper. (Kaspersky, no date)

10.4. Case study

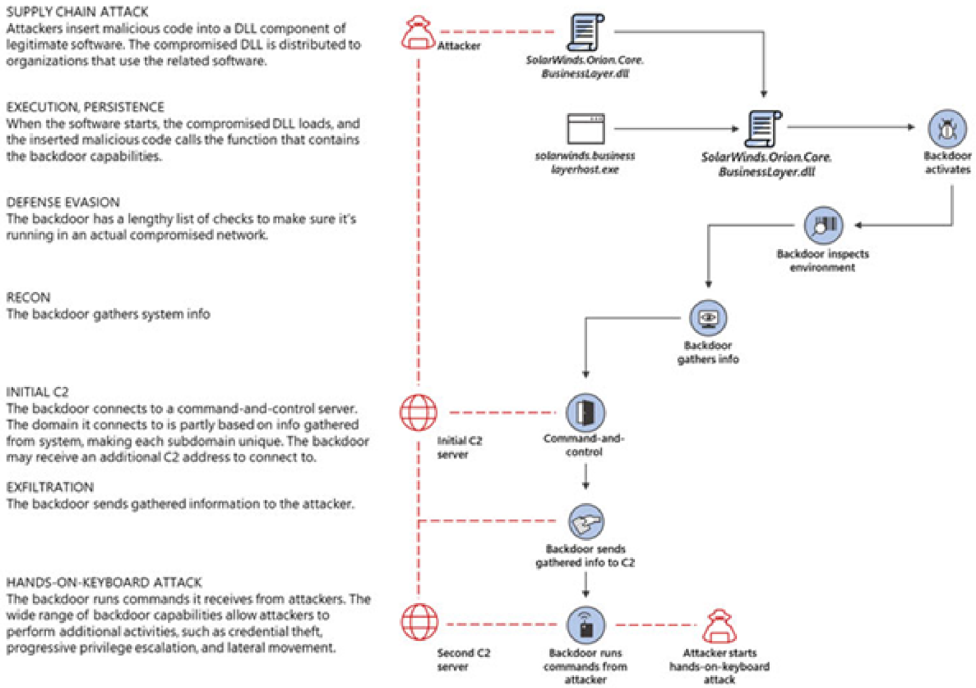
10.4.1. SolarWinds Supply Chain Attack

One notable cybersecurity incident that caused a significant disruption is the SolarWinds supply chain attack. SolarWinds is a prominent software provider and has a headquarters located in Tulsa, Oklahoma. It offers system management tools for network and infrastructure monitoring as well as other technical services to millions of businesses worldwide. One of the company's services is the Orion IT performance monitoring system. (TechTarget Contributor, 2020)

In late 2020, The networks, systems, and data of thousands of SolarWinds customers were compromised by suspected nation-state hackers who were identified as a group by Microsoft under the name Nobelium. The Orion Software has affected more than 30,000 public and private organisations when SolarWinds unintentionally distributed the backdoor malware as an update to the Orion software, the hack compromised the data, networks, and systems of thousands of people. (TechTarget Contributor, 2020)

Clients of SolarWinds weren't the only ones impacted. As a result of the hack, which revealed Orion users' internal workings, the hackers might have had access to the data and networks of their clients and partners. This would result in the number of victims increasing dramatically. (TechTarget Contributor, 2020)

10.4.2. How does it affect SolarWinds?



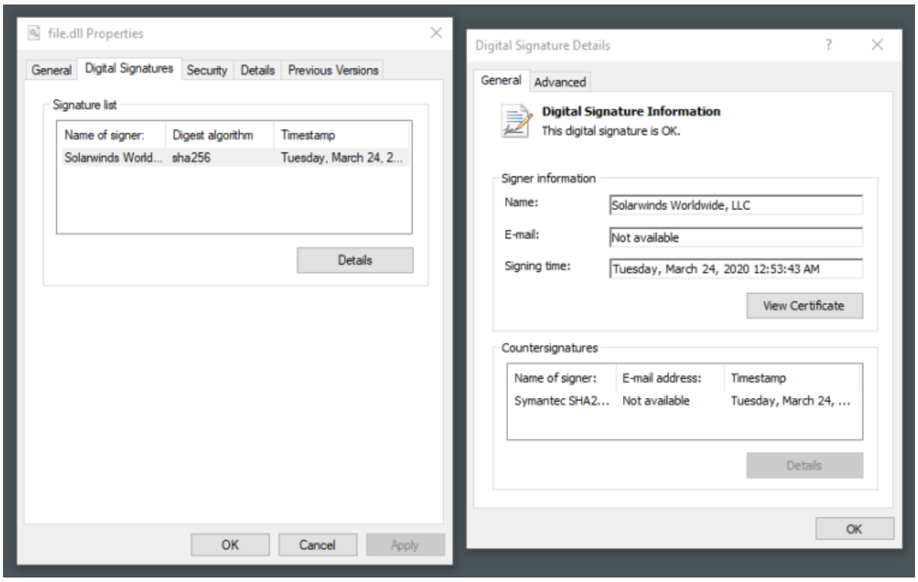
https://www.ecloudcontrol.com/analysis-of-solarwinds-hack/

FireEye, a top cybersecurity company has discovered a widespread campaign. They are involved in tracking UNC2452 which refers to "SolarWinds supply chain attack" or "Sunburst attack" . Attackers used various methods, according to FireEye, to evade being found by multiple scanners. In order to make them appear real and normal, virus activity was mixed in with regular Orion business operations. (TechTarget Contributor, 2020)

The threat actors were also clever enough to remain unnoticed for several months. They had enough time to set up backdoors and gain access to various systems and data. (TechTarget Contributor, 2020)

10.4.3. SUNBURST Backdoor

The Orion software framework contains a backdoor that communicates with outside servers via HTTP and is digitally signed by SolarWinds known as "SolarWinds.Orion.Core.BusinessLayer.dll."(www.varonis.com)



(www.varonis.com)

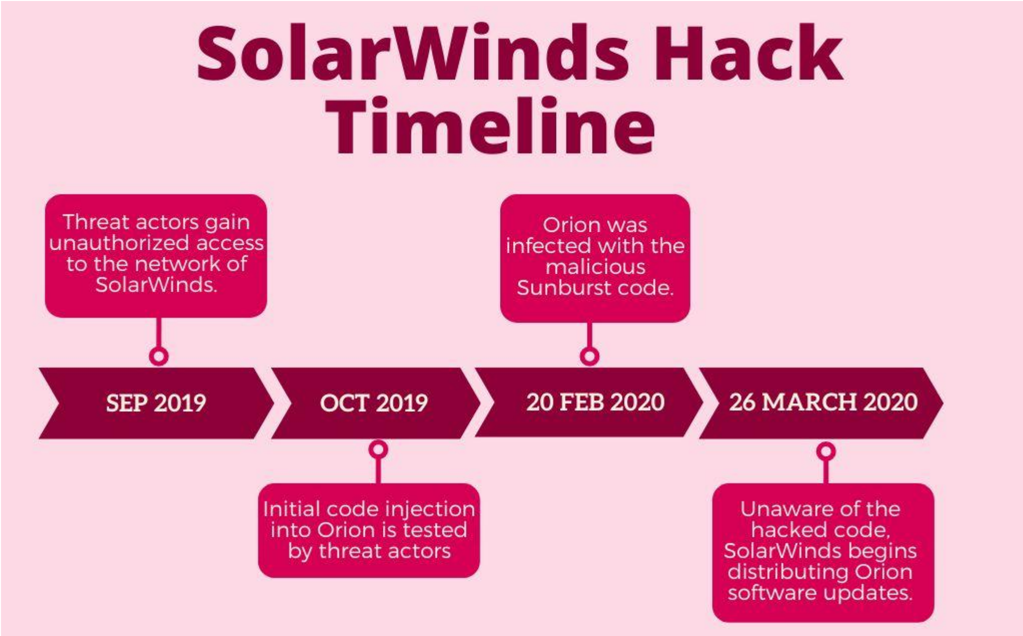
The malicious DLL would have been downloaded and run by any company using SolarWinds and receiving updates from their servers. It would be extremely hard to recognize the malicious content because the DLL was signed and distributed via the official SolarWinds update servers.(www.varonis.com)

A lightweight malware dropper, known as “TEARDROP" by FireEye was delivered using the backdoor. This dropper does not leave a trail on the disk and loads immediately in memory. According to researchers, it was used to launch a modified Cobalt Strike BEACON payload. Red Team Ethical Hackers use Cobalt Strike, a commercial penetration testing framework and post-exploitation agent. Hackers and sophisticated cybercriminal organisations have also adapted it. (www.varonis.com)

Systems Affected

- SolarWinds Orion Platform Version 2019.4 HF 5
- SolarWinds Orion Platform Version 2020.2
- SolarWinds Orion Platform Version 2020.2 HF 1

Here is a timeline of the SolarWinds hack:



https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

10.5. Comparative analysis of attack growth in the past 5 years

As we can see from the table below, it shows the percentage of trojan-dropper attacks over the past 5 years and we can see that the number of trojan-droppers detected each year has been decreasing.

Year	Overall, the number of mobile malware installation packages detected	% of detected packages which is a Trojan-Dropper	Article by
2021	3 464 756	2.55% (88,351)	Tatyana Shishkova Anton Kivva (Mobile malware evolution 2021)
2020	5 683 694	4.51% (256,334)	Victor Chebyshev (Mobile malware evolution 2020)
2019	3 503 952	16.09% (563,785)	Victor Chebyshev (Mobile malware evolution 2019)
2018	5 321 142	16.85%	Victor Chebyshev

			(Mobile malware evolution 2019)
2017	5 730 916	8.63%	Victor Chebyshev (Mobile malware evolution 2018)

11. Conclusion

In conclusion,

AI Tools Used

Name of AI tool	ChatGTP
Input prompt	Persistent Dropper vs Non-Persistent dropper
Date generated	1/6/2023
Output generated	Persistent Dropper: A persistent dropper is a type of dropper malware that is designed to establish a long-term presence on the compromised system. Once executed, a persistent dropper deploys its payload and implements mechanisms to ensure that the payload remains active and functional even after system reboots or security measures are applied. The primary goal of a persistent dropper is to maintain a persistent backdoor or entry point into the compromised system. It achieves this by modifying system settings, creating startup entries, or installing malicious services or drivers. These modifications allow the dropper's payload to be automatically executed during system boot-up, ensuring continuous access for the attackers. Persistent droppers often employ advanced techniques to evade detection and removal. They may use code obfuscation, encryption, or anti-analysis techniques to make it harder for security solutions to detect their presence. Additionally, they may employ rootkit capabilities to hide their presence

	from traditional security tools and maintain their persistence undetected. Non-Persistent Dropper: In contrast, a non-persistent dropper is designed to execute its payload only once and does not establish long-term persistence on the compromised system. Once the payload is delivered and executed, the dropper's task is complete, and it does not take further action to maintain its presence. Non-persistent droppers are typically used in specific attack scenarios where a one-time execution of the payload is sufficient to achieve the attacker's objectives. For example, they may be used in targeted attacks or spear-phishing campaigns where the attackers aim to gain immediate access to sensitive information or execute a specific malicious action. Unlike persistent droppers, non-persistent droppers do not make changes to system settings or create startup entries. They rely on social engineering tactics or exploit specific vulnerabilities to trick users into executing the dropper or exploit the system to run the payload. Once executed, the payload carries out its intended malicious activities, but it does not establish persistence on the compromised system. Non-persistent droppers are often easier to detect and remove compared to persistent droppers. However, they can still cause significant damage or lead to the installation of additional malware if their payload is designed to execute further actions or deliver subsequent stages of the attack.
Impact on submission	I will have a better understanding between Persistent Dropper vs Non-Persistent dropper

Name of AI tool	ChatGTP
Input prompt	Mitigation on happy99
Date generated	26/5/2023
Output generated	Mitigation measures for the Happy99 worm involve steps to prevent its spread and to minimize its impact if it does infect a system. Here are some mitigation strategies: 1. User Education: Educate users about the risks associated with email attachments and the importance of exercising caution when opening or executing files from unknown or suspicious sources. Teach them to

	recognize common indicators of the Happy99 worm, such as unexpected emails with attachments or unusual behavior on their systems. 2. Updated Antivirus Software: Ensure that antivirus software is installed and regularly updated on all systems. Antivirus programs with updated signatures can detect and remove the Happy99 worm if it is present on a system. 3. Email Filtering: Employ email filtering systems or services that can identify and block emails containing the Happy99 worm or similar malware. This helps prevent infected emails from reaching users' inboxes. 4. Network Monitoring: Implement network monitoring solutions to detect unusual network behavior or traffic patterns associated with the propagation of the Happy99 worm. This can help identify infected systems and prevent the worm from spreading further. 5. System Hardening: Apply appropriate system hardening measures such as disabling unnecessary services or features that could be exploited by the Happy99 worm. Regularly update and patch the operating system and applications to address known vulnerabilities. 6. Incident Response: Establish an incident response plan to promptly address and contain any infections by the Happy99 worm. This includes isolating infected systems, removing the worm, and conducting thorough system scans to ensure complete remediation. Remember, these mitigation measures are specific to the Happy99 worm, which is an older malware. It is important to stay updated with the latest security practices and technologies as malware evolves over time. Regularly consulting reputable security sources and following best practices will help protect against newer and more sophisticated malware threats.
Impact on submission	I will get info on the best way to mitigate happy99 malware.

Name of AI tool	ChatGTP
Input prompt	mimecast against happy99
Date generated	26/5/2023

Output generated	Mimecast, as a cloud-based email security and management service, can provide some level of protection against email-borne threats, including malware like Happy 99. However, it's important to note that Happy 99 is a very old and outdated malware, and modern antivirus solutions are generally effective in detecting and removing it. Here's how Mimecast's email security features can help mitigate the risks associated with Happy 99 or similar malware: 1. Advanced Threat Protection: Mimecast employs various security measures, such as content filtering and attachment sandboxing, to detect and block malicious email content. While Happy 99 is an old malware strain, Mimecast's threat protection capabilities can help identify and block any related malicious email attachments or links. 2. Anti-Malware Scanning: Mimecast includes anti-malware scanning capabilities that can detect and prevent the delivery of known malware, including potentially any remnants of Happy 99 that may still be circulating. Regular updates to Mimecast's malware definitions ensure that it can recognize and block known malware strains effectively. 3. URL and Link Protection: Mimecast scans and analyzes URLs and links within emails to identify potential phishing attempts or malicious websites. If a link is found to be malicious or suspicious, Mimecast can block access to that URL, preventing users from inadvertently downloading or accessing malware. 4. Attachment Protection: Mimecast can sandbox and analyze email attachments in a secure environment to detect any malicious behavior or code. If a malicious attachment is identified, Mimecast can block its delivery or strip off the attachment to prevent users from accessing it. While Mimecast provides robust email security features, it's important to note that the effectiveness of any security solution against specific malware strains, especially outdated ones like Happy 99, depends on the timely detection and recognition of such threats. Regularly updating and maintaining your antivirus software and applying security best practices across your organization are crucial for comprehensive protection against a wide range of malware threats, including those from the past and present.
Impact on submission	Chatgpt will generate a response on how

	this mimecast software is good against malware like happy99 & other types

References:

Aqua (no date), *How fileless attacks work and how to detect and prevent them*, *Aqua*. Available at: https://www.aquasec.com/cloud-native-academy/application-security/fileless-attacks/ (Accessed: 18 May 2023).

Arntz, P. (2021), What is fileless malware?, Malwarebytes. Available at: https://www.malwarebytes.com/blog/news/2021/10/what-is-fileless-malware (Accessed: 27 May 2023).

Buckbee, M. (2022), What is fileless malware? PowerShell exploited, Varonis. Available at: https://www.varonis.com/blog/fileless-malware#:~:text=Fileless%20malware%20most%20commonly%20uses,detectable)%20binaries%20into%20your%20systems. (Accessed: 27 May 2023).

Baker, K. (2023), What is fileless malware? - crowdstrike, crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/ (Accessed: 25 May 2023).

Chappell, G. (2010), *Advapi32 functions*. Available at: https://www.geoffchappell.com/studies/windows/win32/advapi32/api/index.htm (Accessed: May 7, 2023).

Cirelly, J. (2022) 10 best malware analysis tools - updated 2023! (paid & free), Comparitech. Available at: https://www.comparitech.com/net-admin/best-malware-analysis-tools/#:~:text=8.-,PeStudio,Searchers%20for%20signatures (Accessed: 30 May 2023).

Daulaguphu, S. (2022), 11 critical malware persistence mechanisms you must know, Tech Zealots. Available at: https://tech-zealots.com/malware-analysis/malware-persistence-mechanisms/ (Accessed: 27 May 2023).

Fakhar Imam (2019), Malware spotlight: Fileless malware, Infosec Resources. Available at: https://resources.infosecinstitute.com/topic/malware-spotlight-fileless-malware/#:~:text=Fileless%20malware%20often%20relies%20on,while%20shortening%20the%20investigation%20timelines. (Accessed: 28 May 2023).

File.net (no date), *What is advapi32.dll?*, *advapi32.dll Windows process - What is it?* Available at: https://www.file.net/process/advapi32.dll.html (Accessed: 10 May 2023).

Fortinet (no date), What is fileless malware? examples, detection and prevention, Fortinet. Available at:

https://www.fortinet.com/resources/cyberglossary/fileless-malware#:~:text=Fileless%20malware%20is%20malicious%20code,downloaded%20to%20your%20hard%20drive. (Accessed: 01 June 2023).

Fox, N. (2022) 11 best malware analysis tools and their features, Varonis. Available at: https://www.varonis.com/blog/malware-analysis-tools (Accessed: 30 May 2023).

Hioureas, V. (2018), Fileless malware: Getting the lowdown on this insidious threat, Malwarebytes. Available at: https://www.malwarebytes.com/blog/news/2018/08/fileless-malware-getting-the-lowdown-on-this-insidious-threat (Accessed: 27 May 2023).

Howard Poston (2019) Network Traffic Analysis for IR: Analyzing fileless malware, Infosec Resources. Available at: https://resources.infosecinstitute.com/topic/network-traffic-analysis-for-ir-analyzing-fileless-malware/ (Accessed: 30 May 2023).

Ilker Kara (2022) Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges, Expert Systems with Applications. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0957417422021510#:~:text=We%20suggest%20a%20memory%2Dbased,detecting%20and%20analyzing%20fileless%20malware.&text=This%20proposed%20method%20offers%20useful,experts%20working%20in%20this%20field.&text=The%20proposed%20method%CA%BCs%20applicability%20was%20demonstrated%20using%20a%20real%20case%20study%20sample. (Accessed: 28 May 2023).

Johansen, A.G., (no date) *What is fileless malware and how does it work?*, *Norton*. Available at: https://us.norton.com/blog/malware/what-is-fileless-malware# (Accessed: 21 May 2023).

Kasperky (no date), Happy, Kaspersky Threats. Available at: https://threats.kaspersky.com/en/threat/Email-Worm.Win32.Happy/ (Accessed: 26 May 2023).

Kaspersky (no date), Trojan droppers, Kaspersky IT Encyclopedia. Available at: https://encyclopedia.kaspersky.com/glossary/trojan-droppers/ (Accessed: 02 June 2023).

Khushali, V. (2020), A review on Fileless Malware Analysis Techniques, International Journal of Engineering Research & Technology. Available at: https://www.ijert.org/a-review-on-fileless-malware-analysis-techniques (Accessed: 28 May 2023).

MDSec Research (no date), Payload generation with CACTUSTORCH, MDSec. Available at: https://www.mdsec.co.uk/2017/07/payload-generation-with-cactustorch/#:~:text=CACTUSTORCH%20is%20a%20framework%20for,to%20bypass%20many%20common%20defences. (Accessed: 27 May 2023).

Oliver Rochford (2021), *Thwarting evasive attacks with behavioral analysis*, *Securonix*. Available at:

https://www.securonix.com/blog/thwarting-evasive-attacks-with-behavioral-analysis/ (Accessed: 24 May 2023).

Prevost, S. (2023), Fileless Malware & Cybersecurity Solutions, Stormshield. Available at: https://www.stormshield.com/news/fileless-malware-how-does-it-work/#undefined (Accessed: 27 May 2023).

Process Library (no date), *Wsock32.dll*, *What is wsock32.dll?* Available at: https://www.processlibrary.com/en/directory/files/wsock32/24607/ (Accessed: May 7, 2023).

Process Library (no date), *What is rpcrt4.dll doing on my computer?*, *What is rpcrt4.dll?* Available at: https://www.processlibrary.com/en/directory/files/rpcrt4/23580/ (Accessed: 10 May 2023).

Rouse, M. (2016), *Kernel32.dll*, *Techopedia*. Available at: https://www.techopedia.com/definition/3379/kernel32dll (Accessed: 10 May 2023).

Symantec (no date), Happy99.Worm removal tool, Symantec Security Response - Happy99.Worm Removal Tool. Available at: https://web.archive.org/web/20040710034245/www.sarc.com/avcenter/venc/data/fix.happy99.worm.html (Accessed: 02 June 2023).

TechTarget Contributor (2020) What is Dropper?: Definition from TechTarget, WhatIs.com. Available at: https://www.techtarget.com/whatis/definition/dropper (Accessed: 02 June 2023).

Trend Micro (2020), *Security 101: How fileless attacks work and persist in Systems*, *Security News*. Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems (Accessed: 24 May 2023).

Trelix (no date), What is fileless malware?, Trellix. Available at: https://www.trellix.com/en-sg/security-awareness/ransomware/what-is-fileless-malware.html#:~:text=Fileless%20malware%20emerged%20in%202017,of%20this%20type%20of%20malware. (Accessed: 27 May 2023).

Uzer, S. (2021), *What is script-based malware?*, *Paubox*. Available at: https://www.paubox.com/blog/what-is-script-based-malware (Accessed: 01 June 2023).

Virus Encyclopedia, V. (no date), *The Virus Encyclopedia*, *Happy99 - The Virus Encyclopedia*. Available at: http://virus.wikidot.com/happy99 (Accessed: May 7, 2023).

Zhang, E. (2018), *What is fileless malware (or a non-malware attack)? definition and best practices for fileless malware protection*, *Digital Guardian*. Available at: https://www.digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices-fileless-malware (Accessed: 18 May 2023).

flo.uri.sh. (n.d.), *Most Popular Email Providers by Active Users 1997 - 2020*. [online] Available at: https://flo.uri.sh/visualisation/3070061/embed [Accessed 21 May 2023].

Wikipedia. (2022), Happy99. [online] Available at: https://en.wikipedia.org/wiki/Happy99.[Accessed 21 May 2023].

kb.iu.edu. (n.d.), What is the Happy99 virus, and how do I remove it? [online] Available at: https://kb.iu.edu/d/agyo [Accessed 21 May 2023].

www.f-secure.com. (n.d.). *Ska | F-Secure Labs*. [online] Available at: https://www.f-secure.com/v-descs/ska.shtml [Accessed 2 Jun. 2023].

www.softlookup.com. (n.d.). *Download FixHappy Freeware*. [online] Available at: https://www.softlookup.com/display.asp?id=10488 [Accessed 2 Jun. 2023].

vuls.cert.org. (n.d.). *CERT Incident Note IN-99-02: Happy99.exe Trojan Horse - Historical - VulWiki*. [online] Available at: https://vuls.cert.org/confluence/display/historical/CERT+Incident+Note+IN-99-02%3A+Happy99.exe+Trojan+Horse [Accessed 2 Jun. 2023].

securelist.com. (n.d.). *Author: David Emm | Securelist*. [online] Available at: https://securelist.com/author/davidemm/ [Accessed 2 Jun. 2023].

Oladimeji, S. and Kerner, S.M. (2022). *SolarWinds hack explained: Everything you need to know*. [online] WhatIs.com. Available at: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Accessed 2 Jun. 2023].

Center for Internet Security (2021). *The SolarWinds Cyber-Attack: What You Need to Know*. [online] CIS. Available at: https://www.cisecurity.org/solarwinds [Accessed 2 Jun. 2023]..

FIREEYE (2020). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. [online] Mandiant. Available at: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor [Accessed 2 Jun. 2023]..

Ramesan, R. (2021). *ANALYSIS OF SOLARWINDS HACK*. [online] CLOUDCONTROL. Available at: https://www.ecloudcontrol.com/analysis-of-solarwinds-hack/ [Accessed 2 Jun. 2023]..

www.varonis.com. (n.d.). *SolarWinds SUNBURST Backdoor: Inside the Stealthy APT Campaign*. [online] Available at: https://www.varonis.com/blog/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign [Accessed 2 Jun. 2023]..

Guidepointsecurity.com. (2021). Available at: https://www.guidepointsecurity.com/blog/analysis-of-the-solarwinds-supply-chain-attack/.

Constantin, L. (2020). *SolarWinds attack explained: And why it was so hard to detect*. [online] CSO Online. Available at: https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html [Accessed 2 Jun. 2023]..

Simplilearn.com. (n.d.). *SolarWinds Attack & Details You Need To Know About It | Simplilearn*. [online] Available at: https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack#what_is_solarwinds [Accessed 2 Jun. 2023].

LLC, G. (n.d.). *Dropper Malware | Gridinsoft*. [online] Gridinsoft LLC. Available at: https://gridinsoft.com/dropper [Accessed 2 Jun. 2023].

securelist.com. (n.d.). Mobile malware evolution 2021. [online] Available at: https://securelist.com/mobile-malware-evolution-2021/105876/ [Accessed 2 Jun. 2023]..

securelist.com. (n.d.). Mobile malware evolution 2020. [online] Available at: https://securelist.com/mobile-malware-evolution-2020/101029/ [Accessed 2 Jun. 2023]..

securelist.com. (n.d.). *Mobile malware evolution 2019*. [online] Available at: https://securelist.com/mobile-malware-evolution-2019/96280/ [Accessed 2 Jun. 2023]..

securelist.com. (2019). *Mobile malware evolution 2018*. [online] Available at: https://securelist.com/mobile-malware-evolution-2018/89689/ [Accessed 2 Jun. 2023].

www.solarwinds.com. (n.d.). *Orion Platform | SolarWinds*. [online] Available at: https://www.solarwinds.com/orion-platform [Accessed 2 Jun. 2023].