CEOINDUSTRIES, INC.

Reversing Challenge Winter 2024

DePaul University

Corinne Otten
Section: 801
March 29, 2024

.danger file malware analysis

DePaul University

1111 Main Street
Chicago, Illinois 36636
United States of America

Tel: 212-365-3653
Email: info@depaul.com
Web: https://depauluni.edu

Notification

This report is provided "as is" for informational purposes only. CEOIndustries, Inc. (CEO, Inc.) does not provide any warranties of any kind regarding any information contained herein. The CEO, Inc. does not endorse any commercial product or service referenced in this report or otherwise.

Summary

Description

CEO, Inc. received 1 Windows Portable Executable (PE) file for analysis. DePaul University (Client) received several alerts on or about March 11, 2024. These alerts presumably came from an employee's desktop: JCortes_PC01. The alerts reported that the desktop was downloading a suspected suspicious file. Client has requested that CEO, Inc. perform Malware Analysis on this file and report its findings, which are provided herein.

Submitted File(s) (1)

I) 9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87.danger
(9a00f.danger)

Analysis Tools Used

CEO, Inc. has performed its analysis using industry-standard professional tools:

- BinaryNinja
- Capa
- CFF Explorer
- DetectItEasy
- Fiddler
- Floss
- HxD
- IDA Pro
- PE Browser
- PE-Studio
- Radare2
- Regshot
- SysInternals: strings; Process Monitor; Process Explorer
- Wireshark
- X32dbg

Findings

I) Filename: 9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87.danger

Determination

It is the professional opinion of CEO, Inc. that this file is malicious. Please see Appendices A through D for screenshots and additional technical information.

VirusTotal Information

Please see the following website for more information:

VirusTotal - File - 9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87

Details

Filename	9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87.danger
Microsoft Known Malware Name	Trojan:Win32/CobaltStrike!rfn
MD5	C9B105EC2412AC0E2ACE20BFA71E1450
SHA1	3CEF1CA36A78CBA308FB29A46B20E5CA22D03289
SHA256	9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87
Imphash	7698a47cb1463adc6420e55f320386c
TimeDateStamp	Friday, June 26, 2015 9:12:52 PM GMT
Number of Sections	5
List of Section Names	.text .rdata .data .rsrc .reloc
EntryPoint	000028D8 .text
Intended CPU	Intel
32bit or 64bit	32-bit
Dll or Exe	Exe
Compiler Information	Operation system: Windows(XP)[I386, 32-bit, GUI] Linker: Microsoft Linker(11.00.60610) Compiler: Microsoft Visual C/C++(17.00.60610)[C++] Language: C/C++

	Tool: Visual Studio(2012)
Interesting Strings	CloseHandle CreateFileA GetProcAddress LocalAlloc WININET.dll CRYPT32.dll urlmon.dll gdiplus.dll CryptAcquireContextA CryptReleaseContext CryptGenKey CryptEncrypt CryptDecrypt InternetOpenA InternetConnectA HttpOpenRequestA GetSystemDirectoryA GetComputerNameA GetVersionExA GetUserNameA GetAdaptersInfo CreateProcessA CreateThread VirtualAlloc VirtualProtect SetFileAttributeA DeleteFileA CopyFileA MoveFileExA CreateMutexA CreateToolhelp32Snapshot Process32First Process32Next ZwAllocateVirtualMemory ZwWriteVirtualMemory ZwResumeThread ZwSetContextThread
Verdict Determination	Malicious. Please see Description Section below.

Description

The provided file is 100% malicious malware. It is a Trojan virus created to establish persistence on the host system, indicated by the creation of startup items (**funefyza.exe**, **wveqaga.exe**) in the user's startup directory, ensuring it is executed upon every system startup. It employs network communication to contact a remote server (**http://adobe-dns-3-adobe.com/eojysoyx.php**), likely for Command and Control (C2) purposes, as well as DNS resolutions and HTTP requests that

indicate its capability to receive instructions and/or exfiltrate data. It interacts with critical system components, including processes (**svchost.exe**), and engages in file system manipulation such as creating, copying, and deleting files, indicative of an attempt to modify system behavior or cover its tracks. The malware also accesses and modifies registry entries, which could be used to change configuration settings or disable security features. Additionally, the use of cryptographic functions suggests attempts to encrypt data or communications to avoid detection. Windows Defender antivirus software also flagged this file and the additional files created as being malicious.

Recommendations

CEO, Inc. recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.

  Enforce a strong password policy and implement regular password changes.

  Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.

  Disable unnecessary services on agency workstations and servers.

  Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Appendix A – Basic Static Analysis

I) Filename: 9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87.danger

PE-Studio – Screenshot Results

The results from PE-Studio flag those items that are suspicious and provide the category of and hints regarding the techniques being used.

Strings Output:

encoding ...	size ...	location	flag (36)	label (96)	group (10)	technique (10)	value
ascii	10	section:.rdata	x	import	file	T1485 | Data Destruction	DeleteFile
ascii	13	section:.rdata	x	import	execution	T1106 | Execution through API	CreateProcess
ascii	10	section:.rdata	x	import	file	T1105 | Remote File Copy	MoveFileEx
ascii	17	section:.rdata	x	import	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	24	section:.rdata	x	import	execution	T1057 | Process Discovery	CreateToolhelp32Snapshot
ascii	14	section:.rdata	x	import	execution	T1057 | Process Discovery	Process32First
ascii	13	section:.rdata	x	import	execution	T1057 | Process Discovery	Process32Next
ascii	12	section:.rdata	x	import	memory	T1055 | Process Injection	VirtualAlloc
ascii	14	section:.rdata	x	import	memory	T1055 | Process Injection	VirtualProtect
ascii	14	section:.rdata	x	import	execution	T1055 | Process Injection	ZwResumeThread
ascii	19	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptAcquireContext
ascii	19	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptReleaseContext
ascii	11	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptGenKey
ascii	15	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptDestroyKey
ascii	14	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptExportKey
ascii	14	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptImportKey
ascii	12	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptEncrypt
ascii	12	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptDecrypt
ascii	17	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	SystemFunction036
ascii	19	section:.rdata	x	import	cryptography	T1027 | Obfuscated Files or Info...	CryptStringToBinary
ascii	16	section:.rdata	x	import	windowing	-	GetDesktopWindow
ascii	15	section:.rdata	x	import	network	-	GetAdaptersInfo
ascii	12	section:.rdata	x	import	network	-	InternetOpen
ascii	19	section:.rdata	x	import	network	-	InternetCloseHandle
ascii	15	section:.rdata	x	import	network	-	InternetConnect
ascii	16	section:.rdata	x	import	network	-	InternetReadFile
ascii	15	section:.rdata	x	import	network	-	HttpOpenRequest
ascii	21	section:.rdata	x	import	network	-	HttpAddRequestHeaders
ascii	15	section:.rdata	x	import	network	-	HttpSendRequest
ascii	13	section:.rdata	x	import	network	-	HttpQueryInfo
ascii	21	section:.rdata	x	import	network	-	ObtainUserAgentString
ascii	23	section:.rdata	x	import	memory	-	ZwAllocateVirtualMemory
ascii	20	section:.rdata	x	import	memory	-	ZwWriteVirtualMemory
ascii	9	section:.rdata	x	import	file	-	WriteFile
ascii	17	section:.rdata	x	import	file	-	SetFileAttributes
ascii	18	section:.rdata	x	import	execution	-	ZwSetContextThread
ascii	5	section:.rdata	-	-	execution	T1497 | Sandbox Evasion	Sleep
ascii	11	section:.rdata	-	import	dynamic-library	T1106 | Execution through API	LoadLibrary
ascii	8	section:.rdata	-	import	file	T1105 | Remote File Copy	CopyFile
ascii	18	section:.rdata	-	import	reconnaissance	T1083 | File and Directory Disco...	GetSystemDirectory
ascii	15	section:.rdata	-	import	reconnaissance	T1082 | System Information Dis...	GetComputerName
ascii	17	section:.rdata	-	import	reconnaissance	T1082 | System Information Dis...	GetComputerNameEx
ascii	11	section:.rdata	-	import	reconnaissance	T1033 | System Owner/User Dis...	GetUserName
ascii	12	section:.rdata	-	import	synchronization	-	ReleaseMutex
ascii	11	section:.rdata	-	import	synchronization	-	CreateMutex
ascii	13	section:.rdata	-	import	reconnaissance	-	GetSystemInfo
ascii	12	section:.rdata	-	import	reconnaissance	-	GetVersionEx
ascii	12	section:.rdata	-	file	network	-	IPHLPAPI.DLL
ascii	11	section:.rdata	-	file	network	-	WININET.dll
ascii	10	section:.rdata	-	file	network	-	urlmon.dll
ascii	10	section:.rdata	-	import	memory	-	LocalAlloc
ascii	9	section:.rdata	-	import	memory	-	LocalSize
ascii	9	section:.rdata	-	import	memory	-	LocalFree
ascii	10	section:.rdata	-	import	file	-	CreateFile
ascii	11	section:.rdata	-	import	file	-	GetTempPath

encoding ...	size ...	location	flag (36)	label (96)	group (10)	technique (10)	value
ascii	11	section:.rdata	-	import	file	-	GetTempPath
ascii	15	section:.rdata	-	import	file	-	GetTempFileName
ascii	15	section:.rdata	-	import	file	-	SHGetFolderPath
ascii	10	section:.rdata	-	import	file	-	PathAppend
ascii	12	section:.rdata	-	import	execution	-	CreateThread
ascii	11	section:.rdata	-	import	execution	-	ExitProcess
ascii	14	section:.rdata	-	import	execution	-	IsWow64Process
ascii	15	section:.rdata	-	import	dynamic-library	-	GetModuleHandle
ascii	14	section:.rdata	-	import	dynamic-library	-	GetProcAddress
ascii	17	section:.rdata	-	import	dynamic-library	-	GetModuleFileName
ascii	12	section:.rdata	-	import	diagnostic	-	GetLastError
ascii	11	section:.rdata	-	file	cryptography	-	CRYPT32.dll
ascii	11	section:.rdata	-	import	-	-	CloseHandle
ascii	8	section:.rdata	-	import	-	-	wsprintf
ascii	11	section:.rdata	-	import	-	-	GetWindowDC
ascii	9	section:.rdata	-	import	-	-	ReleaseDC
ascii	13	section:.rdata	-	import	-	-	GetWindowRect
ascii	22	section:.rdata	-	import	-	-	CreateCompatibleBitmap
ascii	18	section:.rdata	-	import	-	-	CreateCompatibleDC
ascii	8	section:.rdata	-	import	-	-	DeleteDC
ascii	12	section:.rdata	-	import	-	-	DeleteObject
ascii	12	section:.rdata	-	import	-	-	SelectObject
ascii	21	section:.rdata	-	import	-	-	CreateStreamOnHGlobal
ascii	10	section:.rdata	-	import	-	-	StrToIntEx
ascii	14	section:.rdata	-	import	-	-	GdiplusStartup
ascii	15	section:.rdata	-	import	-	-	GdiplusShutdown
ascii	16	section:.rdata	-	import	-	-	GdipDisposeImage
ascii	21	section:.rdata	-	import	-	-	GdipSaveImageToStream
ascii	27	section:.rdata	-	import	-	-	GdipCreateBitmapFromHBITMAP

Sections:

The provided footprints here enable each section to be researched using the SHA256 value.

property	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]
name	.text	.rdata	.data	.rsrc	.reloc
footprint > sha256	8B700495F6F1CAD69F16BD5...	42805D0F03AA57584026D96...	D4294B046657EF6F80C2A6C...	79E650FC0D108F0B5CB9099...	541CABBBA3BD01F1E
entropy	6.224	5.106	0.913	4.696	2.389
file-ratio (93.10%)	55.17 %	20.69 %	3.45 %	3.45 %	10.34 %
raw-address (begin)	0x00000400	0x00002400	0x00003000	0x00003200	0x00003400
raw-address (end)	0x00002400	0x00003000	0x00003200	0x00003400	0x00003A00
raw-size (13824 bytes)	0x00002000 (8192 bytes)	0x00000C00 (3072 bytes)	0x00000200 (512 bytes)	0x00000200 (512 bytes)	0x00000600 (1536 byte
virtual-address	0x00001000	0x00003000	0x00004000	0x00005000	0x00006000
virtual-size (13138 bytes)	0x00001EBA (7866 bytes)	0x00000B5C (2908 bytes)	0x000002DC (732 bytes)	0x000001E0 (480 bytes)	0x00000480 (1152 byte
characteristics	0x60000020	0x40000040	0xC0000040	0x40000040	0x42000040
write	-	-	x	-	-
execute	x	-	-	-	-
share	-	-	-	-	-
self-modifying	-	-	-	-	-
virtual	-	-	-	-	-
items					
directory > import	-	0x00003234	-	-	-
directory > resource	-	-	-	0x00005000	-
directory > relocation	-	-	-	-	0x00006000
directory > import-address	-	0x00003000	-	-	-
manifest	-	-	-	0x00003260	-
base-of-code	0x00001000	-	-	-	-
base-of-data	-	0x00003000	-	-	-
entry-point	0x000028D8	-	-	-	-

Imports:

Those imports that are flagged in red below are critical to understanding this virus. It clearly indicates that the file performs copies, and includes: obfuscation, cryptography key manipulation, file executions, discovery of processes and process injections, data destruction, attempts to retrieve system file data and connect to the network for exfiltration, attempts at evasion, and attempts to gain persistent access.

imports (84)	flag (36)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (10)	technique (10)	t	library (0)
CryptAcquireContextA	x	0x00003806	0x00003806	176 (0x00B0)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptDecrypt	x	0x00003888	0x00003888	180 (0x00B4)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptDestroyKey	x	0x00003842	0x00003842	183 (0x00B7)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptEncrypt	x	0x00003878	0x00003878	186 (0x00BA)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptExportKey	x	0x00003854	0x00003854	191 (0x00BF)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptGenKey	x	0x00003834	0x00003834	192 (0x00C0)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptImportKey	x	0x00003866	0x00003866	202 (0x00CA)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptReleaseContext	x	0x0000381E	0x0000381E	203 (0x00CB)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
SystemFunction036	x	0x00003898	0x00003898	753 (0x02F1)	cryptography	T1027 | Obfuscated Files or Information	i.	ADVAPI32.dll
CryptStringToBinaryA	x	0x00003A8A	0x00003A8A	216 (0x00D8)	cryptography	T1027 | Obfuscated Files or Information	i.	CRYPT32.dll
CreateProcessA	x	0x00003586	0x00003586	164 (0x00A4)	execution	T1106 | Execution through API	i.	KERNEL32.dll
CreateToolhelp32Snapshot	x	0x000036D2	0x000036D2	190 (0x00BE)	execution	T1057 | Process Discovery	i.	KERNEL32.dll
GetCurrentProcess	x	0x00003598	0x00003598	448 (0x01C0)	execution	T1057 | Process Discovery	i.	KERNEL32.dll
Process32First	x	0x000036EE	0x000036EE	917 (0x0395)	execution	T1057 | Process Discovery	i.	KERNEL32.dll
Process32Next	x	0x00003700	0x00003700	919 (0x0397)	execution	T1057 | Process Discovery	i.	KERNEL32.dll
ZwResumeThread	x	0x00003966	0x00003966	1591 (0x0637)	execution	T1055 | Process Injection	i.	ntdll.dll
ZwSetContextThread	x	0x00003978	0x00003978	1602 (0x0642)	execution	-	i.	ntdll.dll
DeleteFileA	x	0x0000365E	0x0000365E	211 (0x00D3)	file	T1485 | Data Destruction	i.	KERNEL32.dll
MoveFileExA	x	0x00003678	0x00003678	863 (0x035F)	file	T1105 | Remote File Copy	i.	KERNEL32.dll
SetFileAttributesA	x	0x00003648	0x00003648	1118 (0x045E)	file	-	i.	KERNEL32.dll
WriteFile	x	0x000035E2	0x000035E2	1317 (0x0525)	file	-	i.	KERNEL32.dll
VirtualAlloc	x	0x00003710	0x00003710	1257 (0x04E9)	memory	T1055 | Process Injection	i.	KERNEL32.dll
VirtualProtect	x	0x00003720	0x00003720	1263 (0x04EF)	memory	T1055 | Process Injection	i.	KERNEL32.dll
ZwAllocateVirtualMemory	x	0x00003934	0x00003934	1312 (0x0520)	memory	-	i.	ntdll.dll
ZwWriteVirtualMemory	x	0x0000394E	0x0000394E	1682 (0x0692)	memory	-	i.	ntdll.dll
GetAdaptersInfo	x	0x00003998	0x00003998	63 (0x003F)	network	-	i.	IPHLPAPI.DLL
HttpAddRequestHeadersA	x	0x00003A1A	0x00003A1A	82 (0x0052)	network	-	i.	WININET.dll
HttpOpenRequestA	x	0x00003A06	0x00003A06	87 (0x0057)	network	-	i.	WININET.dll
HttpQueryInfoA	x	0x00003A48	0x00003A48	89 (0x0059)	network	-	i.	WININET.dll
HttpSendRequestA	x	0x00003A34	0x00003A34	91 (0x005B)	network	-	i.	WININET.dll
InternetCloseHandle	x	0x000039C8	0x000039C8	107 (0x006B)	network	-	i.	WININET.dll
InternetConnectA	x	0x000039DE	0x000039DE	113 (0x0071)	network	-	i.	WININET.dll
InternetOpenA	x	0x000039B8	0x000039B8	151 (0x0097)	network	-	i.	WININET.dll
InternetReadFile	x	0x000039F2	0x000039F2	159 (0x009F)	network	-	i.	WININET.dll
ObtainUserAgentString	x	0x00003A66	0x00003A66	84 (0x0054)	network	-	i.	urlmon.dll
GetDesktopWindow	x	0x00003776	0x00003776	291 (0x0123)	windowing	-	i.	USER32.dll
BitBlt	-	0x00003796	0x00003796	19 (0x0013)	-	-	i.	GDI32.dll
CreateCompatibleBitmap	-	0x000037A0	0x000037A0	47 (0x002F)	-	-	i.	GDI32.dll
CreateCompatibleDC	-	0x000037BA	0x000037BA	48 (0x0030)	-	-	i.	GDI32.dll
DeleteDC	-	0x000037D0	0x000037D0	227 (0x00E3)	-	-	i.	GDI32.dll
DeleteObject	-	0x000037DC	0x000037DC	230 (0x00E6)	-	-	i.	GDI32.dll
SelectObject	-	0x000037EC	0x000037EC	631 (0x0277)	-	-	i.	GDI32.dll
CloseHandle	-	0x000034D0	0x000034D0	82 (0x0052)	-	-	i.	KERNEL32.dll
lstrcpyA	-	0x0000355E	0x0000355E	1351 (0x0547)	-	-	i.	KERNEL32.dll
lstrlenA	-	0x0000356A	0x0000356A	1357 (0x054D)	-	-	i.	KERNEL32.dll
StrToIntExA	-	0x0000391A	0x0000391A	332 (0x014C)	-	-	i.	SHLWAPI.dll
GetWindowDC	-	0x0000374C	0x0000374C	402 (0x0192)	-	-	i.	USER32.dll
GetWindowRect	-	0x00003766	0x00003766	412 (0x019C)	-	-	i.	USER32.dll
ReleaseDC	-	0x0000375A	0x0000375A	613 (0x0265)	-	-	i.	USER32.dll
wsprintfA	-	0x00003740	0x00003740	818 (0x0332)	-	-	i.	USER32.dll
GdipCreateBitmapFromHBIT...	-	0x00003AFE	0x00003AFE	77 (0x004D)	-	-	i.	gdiplus.dll
GdipDisposeImage	-	0x00003AD2	0x00003AD2	152 (0x0098)	-	-	i.	gdiplus.dll
GdipGetImageEncoders	-	0x00003B38	0x00003B38	286 (0x011E)	-	-	i.	gdiplus.dll
GdipGetImageEncodersSize	-	0x00003B1C	0x00003B1C	287 (0x011F)	-	-	i.	gdiplus.dll
GdipSaveImageToStream	-	0x00003AE6	0x00003AE6	497 (0x01F1)	-	-	i.	gdiplus.dll
GdiplusShutdown	-	0x00003AC0	0x00003AC0	628 (0x0274)	-	-	i.	gdiplus.dll
GdiplusStartup	-	0x00003AAE	0x00003AAE	629 (0x0275)	-	-	i.	gdiplus.dll
CreateStreamOnHGlobal	-	0x000038EA	0x000038EA	134 (0x0086)	-	-	i.	ole32.dll
GetLastError	-	0x000035BA	0x000035BA	514 (0x0202)	diagnostic	-	i.	KERNEL32.dll
GetModuleFileNameA	-	0x0000360E	0x0000360E	531 (0x0213)	dynamic-li...	-	i.	KERNEL32.dll
GetModuleHandleA	-	0x000034DE	0x000034DE	533 (0x0215)	dynamic-li...	-	i.	KERNEL32.dll
GetProcAddress	-	0x00003516	0x00003516	581 (0x0245)	dynamic-li...	-	i.	KERNEL32.dll
LoadLibraryA	-	0x00003576	0x00003576	828 (0x033C)	dynamic-li...	T1106 | Execution through API	i.	KERNEL32.dll
CreateThread	-	0x0000354E	0x0000354E	181 (0x00B5)	execution	-	i.	KERNEL32.dll
ExitProcess	-	0x000035AC	0x000035AC	281 (0x0119)	execution	-	i.	KERNEL32.dll
IsWow64Process	-	0x000036C0	0x000036C0	782 (0x030E)	execution	-	i.	KERNEL32.dll
Sleep	-	0x000035DA	0x000035DA	1202 (0x04B2)	execution	T1497 | Sandbox Evasion	i.	KERNEL32.dll
CopyFileA	-	0x0000366C	0x0000366C	112 (0x0070)	file	T1105 | Remote File Copy	i.	KERNEL32.dll
CreateFileA	-	0x00003508	0x00003508	136 (0x0088)	file	-	i.	KERNEL32.dll
GetTempFileNameA	-	0x00003634	0x00003634	642 (0x0282)	file	-	i.	KERNEL32.dll
GetTempPathA	-	0x00003624	0x00003624	644 (0x0284)	file	-	i.	KERNEL32.dll
SHGetFolderPathA	-	0x000038CA	0x000038CA	191 (0x00BF)	file	-	i.	SHELL32.dll
PathAppendA	-	0x0000390C	0x0000390C	51 (0x0033)	file	-	i.	SHLWAPI.dll
LocalAlloc	-	0x00003528	0x00003528	836 (0x0344)	memory	-	i.	KERNEL32.dll
LocalFree	-	0x00003542	0x00003542	840 (0x0348)	memory	-	i.	KERNEL32.dll
LocalSize	-	0x00003536	0x00003536	845 (0x034D)	memory	-	i.	KERNEL32.dll
GetUserNameA	-	0x000038AC	0x000038AC	356 (0x0164)	reconnaissa...	T1033 | System Owner/User Discovery	i.	ADVAPI32.dll
GetComputerNameA	-	0x00003686	0x00003686	396 (0x018C)	reconnaissa...	T1082 | System Information Discovery	i.	KERNEL32.dll
GetComputerNameExA	-	0x0000369A	0x0000369A	397 (0x018D)	reconnaissa...	T1082 | System Information Discovery	i.	KERNEL32.dll
GetSystemDirectoryA	-	0x000034F2	0x000034F2	623 (0x026F)	reconnaissa...	T1083 | File and Directory Discovery	i.	KERNEL32.dll
GetSystemInfo	-	0x000035EE	0x000035EE	627 (0x0273)	reconnaissa...	-	i.	KERNEL32.dll
GetVersionExA	-	0x000036B0	0x000036B0	675 (0x02A3)	reconnaissa...	-	i.	KERNEL32.dll
CreateMutexA	-	0x000035FE	0x000035FE	155 (0x009B)	synchroniz...	-	i.	KERNEL32.dll
ReleaseMutex	-	0x000035CA	0x000035CA	1018 (0x03FA)	synchroniz...	-	i.	KERNEL32.dll

Import Directory:

library (13)	du...	flag (4)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (84)	group	description
KERNEL32.dll	-	-	0x000033A4	0x00003058	implicit	37	-	Windows NT BASE API Client
USER32.dll	-	-	0x00003450	0x00003104	implicit	5	-	Multi-User Windows USER API Client Library
GDI32.dll	-	-	0x00003380	0x00003034	implicit	6	-	GDI Client Library
ADVAPI32.dll	-	-	0x0000334C	0x00003000	implicit	10	-	Advanced Windows 32 Base API
SHELL32.dll	-	-	0x0000343C	0x000030F0	implicit	1	-	Windows Shell Library
ole32.dll	-	-	0x000034C0	0x00003174	implicit	1	-	Microsoft OLE for Windows
SHLWAPI.dll	-	-	0x00003444	0x000030F8	implicit	2	-	Shell Light-weight Utility Library
ntdll.dll	-	-	0x000034AC	0x00003160	implicit	4	-	NT Layer
IPHLPAPI.DLL	-	x	0x0000339C	0x00003050	implicit	1	network	IP Helper API
WININET.dll	-	x	0x00003468	0x0000311C	implicit	8	network	Internet Extensions for Win32 Library
urlmon.dll	-	x	0x000034C8	0x0000317C	implicit	1	network	OLE32 Extensions for Win32
CRYPT32.dll	-	x	0x00003378	0x0000302C	implicit	1	cryptography	Windows Crypto Library
gdiplus.dll	-	-	0x0000348C	0x00003140	implicit	7	-	Microsoft GDI+ Library

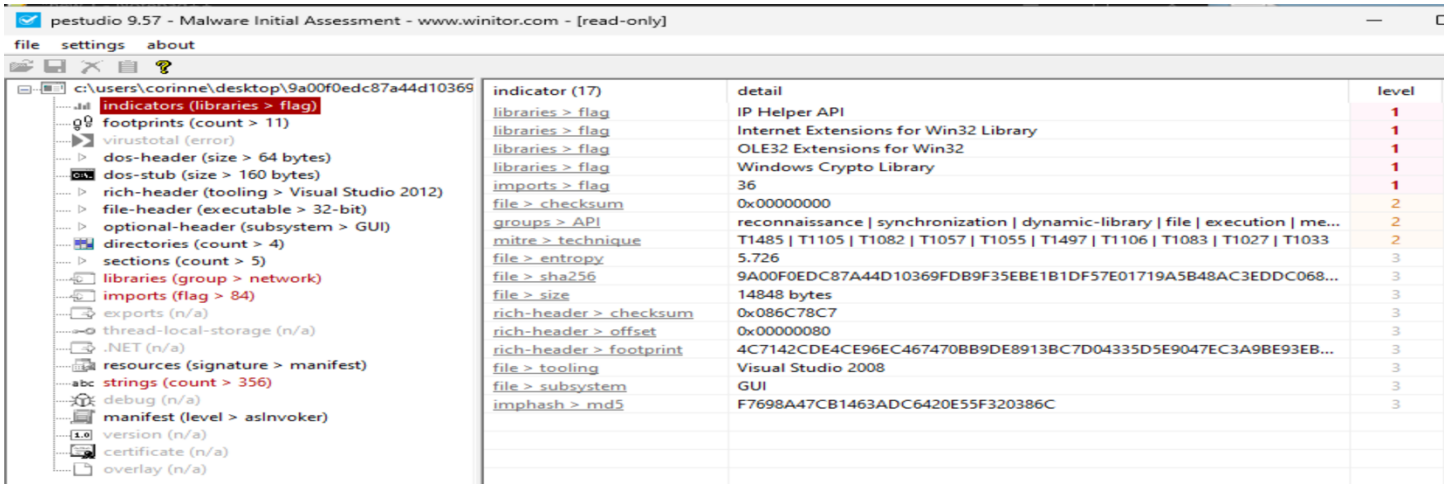
Manifest:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
  <security>
   <requestedPrivileges>
    <requestedExecutionLevel level='asInvoker' uiAccess='false' />
   </requestedPrivileges>
  </security>
 </trustInfo>
</assembly>
```

Malware Initial Assessment:

You can see from this screenshot that there are a number of flags in red. These indicate:

- Libraries related to networking, system information, and cryptography are being used for network communication, information gathering, and encryption tasks
- The Libraries “IP Helper API”, “Internet Extensions for Win32 Library”, “OLE32 Extensions for Win32”, and “Windows Crypto Library” imply that the executable has the capability to interact with network configurations, perform internet operations, and utilize cryptographic functions
- The MITRE ATT&CK Techniques listed for such things as reconnaissance, synchronization, dynamic-library, file, execution, and memory indicate that this file may have known malicious behavior
- You’ll notice that most of the information related to the red flags were seen in the list of Unicode Strings output
- The manifest “asInvoker” means the file does not require elevated privileges to run, which is an attempt by the attacker to avoid suspicion during execution



Appendix B – Advanced Static Analysis

IDAPro– Screenshot Results

The results from IDAPro are very detailed and show that the C code used in this program contained intentional hiding of malicious functions (called obfuscation). Following sub-functions

Functions List:

# IDAPRO FUNCTIONS LIST						
Function name	Segment	Start	Length	Locals	Arguments	R
CreateToolhelp32Snapshot	.text	00402E6C	6	0	8	R
GdipCreateBitmapFromHBITMAP	.text	00402EA8	6	0	0000000C	R
GdipDisposeImage	.text	00402E9C	6	0	4	R
GdipGetImageEncoders	.text	00402EB4	6	0	0000000C	R
GdipGetImageEncodersSize	.text	00402EAE	6	0	8	R
GdipSaveImageToStream	.text	00402EA2	6	0	10	R
GdiplusShutdown	.text	4.02E+98	6	0	4	R
GdiplusStartup	.text	4.02E+92	6	0	0000000C	R
GetAdaptersInfo	.text	4.02E+86	6	0	8	R
ObtainUserAgentString	.text	00402E8A	6	0	0000000C	R
Process32First	.text	4.02E+74	6	0	8	R
Process32Next	.text	4.02E+80	6	0	8	R
StartAddress	.text	004028AE	0000002A	8	4	R
SystemFunction036	.text	00402E7E	6	0	8	R
start	.text	004028D8	43	4		.
sub_401000	.text	401000	0000021E	250	18	R
sub_40121E	.text	0040121E	17	4	4	R
sub_401235	.text	401235	160	000003EC	4	R
sub_401395	.text	401395	79	4	10	R
sub_40140E	.text	0040140E	16	4	4	R
sub_401424	.text	401424	16	4	4	R
sub_40143A	.text	0040143A	000000B4	10	4	R
sub_4014EE	.text	004014EE	000000CB	64	14	R
sub_4015B9	.text	004015B9	33	4	4	R
sub_4015EC	.text	004015EC	000000DF	68	14	R
sub_4016CB	.text	004016CB	0000006C	10	0000000C	R
sub_401737	.text	401737	0000009F	64	4	R
sub_4017D6	.text	004017D6	30	0		R
sub_401806	.text	401806	24	8	8	R

sub_40182A	.text	0040182A	000000A7	54	8	R
sub_4018D1	.text	004018D1	78	0000005C	10	R
sub_401949	.text	401949	19	4	0000000C	R
sub_401962	.text	401962	26	4	8	R
sub_401988	.text	401988	0E+00	0000000C	0000000C	R
sub_401A70	.text	00401A70	22	4	5	R
sub_401A92	.text	00401A92	29	4	8	R
sub_401ABB	.text	00401ABB	48	8	8	R
sub_401B03	.text	00401B03	0000001C	8	4	R
sub_401B1F	.text	00401B1F	14	4	4	R
sub_401B33	.text	00401B33	10	4	4	R
sub_401B43	.text	00401B43	37	4	0000000C	R
sub_401B7A	.text	00401B7A	0000002C	4	0000000C	R
sub_401BA6	.text	00401BA6	20	4	0000000C	R
sub_401BC6	.text	00401BC6	23	4	8	R
sub_401BE9	.text	00401BE9	18	4	4	R
sub_401C01	.text	00401C01	17	4	4	R
sub_401C18	.text	00401C18	44	0000010C		R
sub_401C5C	.text	00401C5C	0000003C	4		R
sub_401C98	.text	00401C98	000000C2	0000013C		R
sub_401D5A	.text	00401D5A	42	8	8	R
sub_401D9C	.text	00401D9C	0000008C	218	8	R
sub_401E28	.text	4.01E+30	48	10		R
sub_401E70	.text	4.01E+72	99	10	8	R
sub_401F09	.text	00401F09	75	48		R
sub_401F7E	.text	00401F7E	000000BA	40	0000000C	R
sub_402038	.text	402038	0000003C	10	0000000C	R
sub_402074	.text	402074	51	10	8	R
sub_4020C5	.text	004020C5	140	18	14	R
sub_402205	.text	402205	0000004B	0000000C		R
sub_402250	.text	402250	0000012A	10	8	R
sub_40237A	.text	0040237A	29	4		R
sub_4023A3	.text	004023A3	000000D7	64		R
sub_40247A	.text	0040247A	0000010B	150	4	R
sub_402585	.text	402585	61	18		R
sub_4025E6	.text	4.025E+09	0000000E	0		R
sub_4025F4	.text	004025F4	0000005B	0000000C		R
sub_40264F	.text	0040264F	74	34	0000000D	R
sub_4026C3	.text	004026C3	0000004A	10	9	R
sub_40270D	.text	0040270D	000000D6	120		R
sub_4027E3	.text	4.027E+06	000000CB	0	4	R
sub_40291C	.text	0040291C	51	0000000C	8	R

sub_40296D	.text	0040296D	000000F8	10	8	R
sub_402A65	.text	00402A65	000000A0	10	10	R
sub_402B05	.text	00402B05	38	8	0000000C	R
sub_402B3D	.text	00402B3D	14	4	4	R
sub_402B51	.text	00402B51	000000F3	84	0000000C	R
sub_402C44	.text	00402C44	000000B2	30		R
sub_402CF6	.text	00402CF6	000000FC	30	4	R
sub_402DF2	.text	00402DF2	0000003F	10	4	R
sub_402E31	.text	4.02E+33	25	8	8	R
sub_402E56	.text	4.02E+58	15	4	8	R

Function Call List:

Address	Called function	
.text:004028E6	call	ds:GetModuleFileNameA
.text:004028F2	call	sub_401BC6
.text:004028F7	call	sub_4023A3
.text:004028FC	call	sub_40237A
.text:00402901	call	sub_402585
.text:0040290B	call	sub_401235
.text:00402915	call	ds:ExitProcess

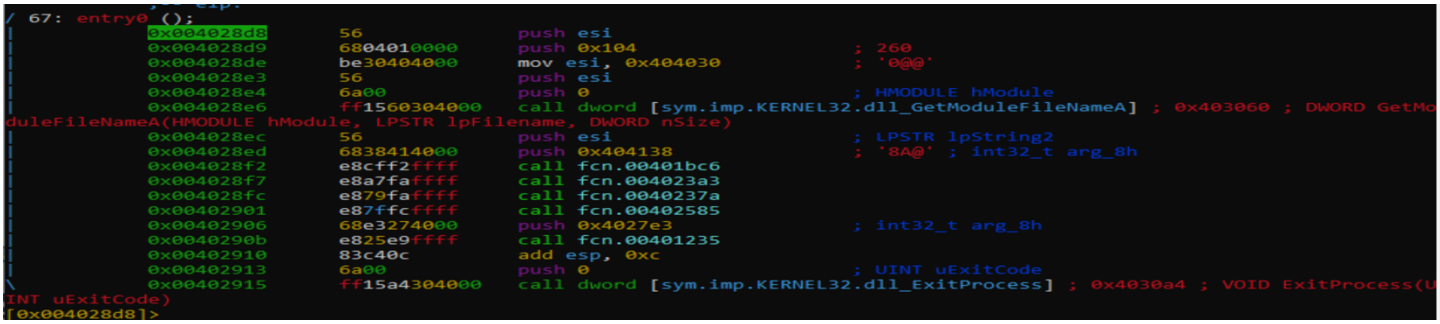
Function Start:

```
; Attributes: noreturn

public start
start proc near
push    esi
push    104h                ; nSize
mov     esi, offset String2
push    esi                 ; lpFilename
push    0                   ; hModule
call    ds:GetModuleFileNameA
push    esi                 ; lpString2
push    offset ExistingFileName ; lpString1
call    sub_401BC6
call    sub_4023A3
call    sub_40237A
call    sub_402585
push    offset sub_4027E3
call    sub_401235
add     esp, 0Ch
push    0                   ; uExitCode
call    ds:ExitProcess
start endp
```

Radare2– Screenshot Results

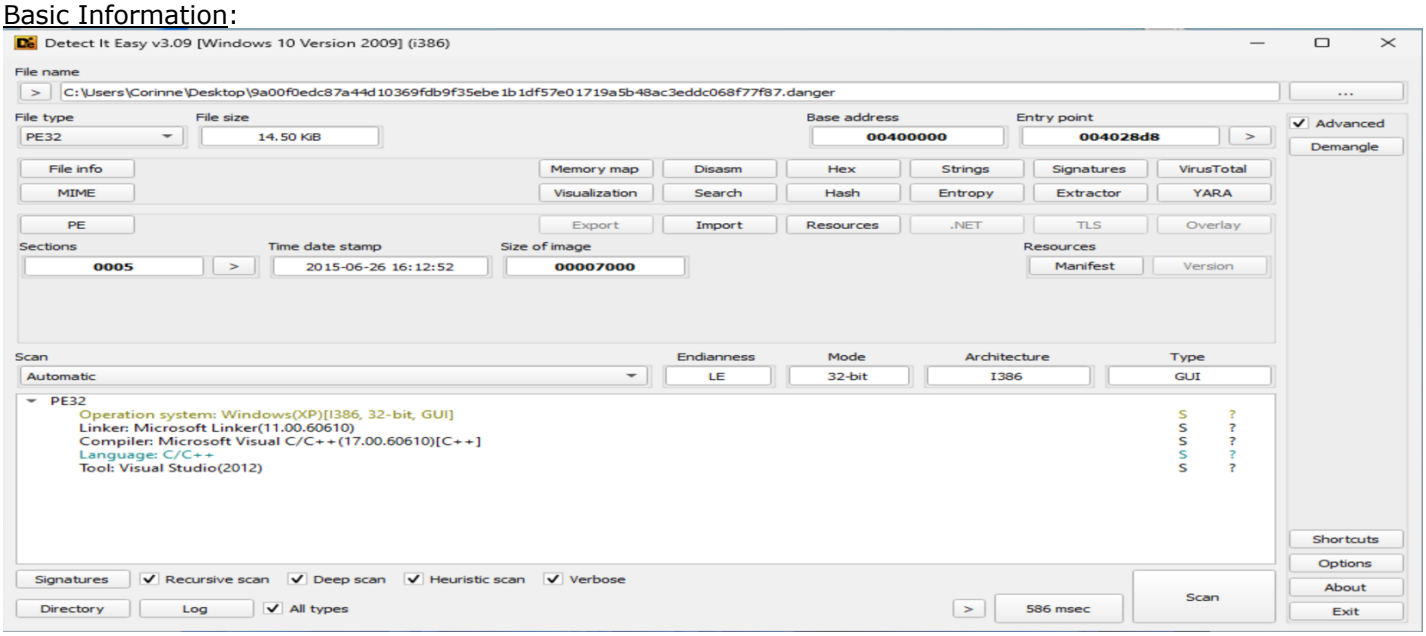
This shows a different view of the disassembled code. The presence of a call to "GetModuleFileNameA" indicates that the program is retrieving its own module's file path. This is common for virus files to attempt to alter the file and possibly self-replicate. The instructions involving "esi" and pushing offsets followed by "call" instructions often indicates that the malware is manipulating strings and/or memory.



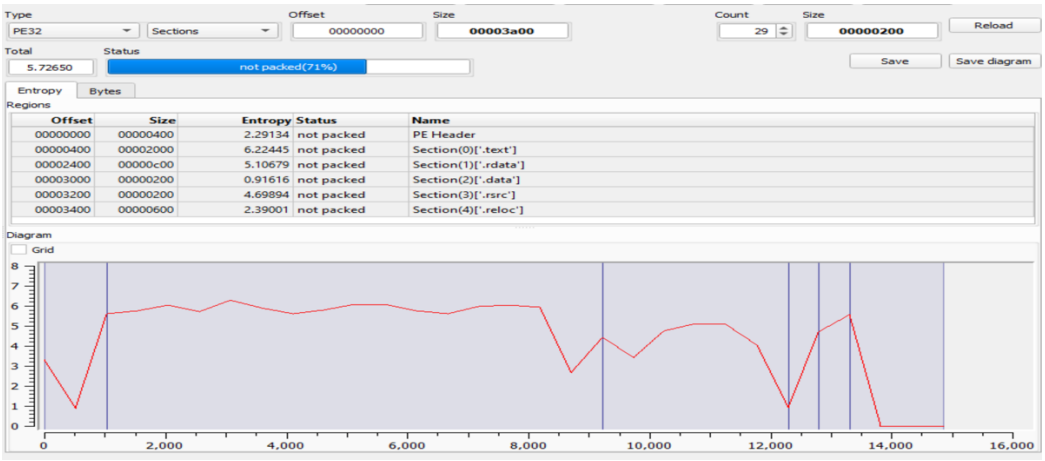
DetectItEasy– Screenshot Results

These screenshots show a more advanced Static snapshot of the file. The Entropy screenshot shows that the

Basic Information:



Entropy:
This entropy graph indicates that the file was not packed. Typically, the entropy value of a section that is 7 or above would indicate that there is a function within that section that is packed.



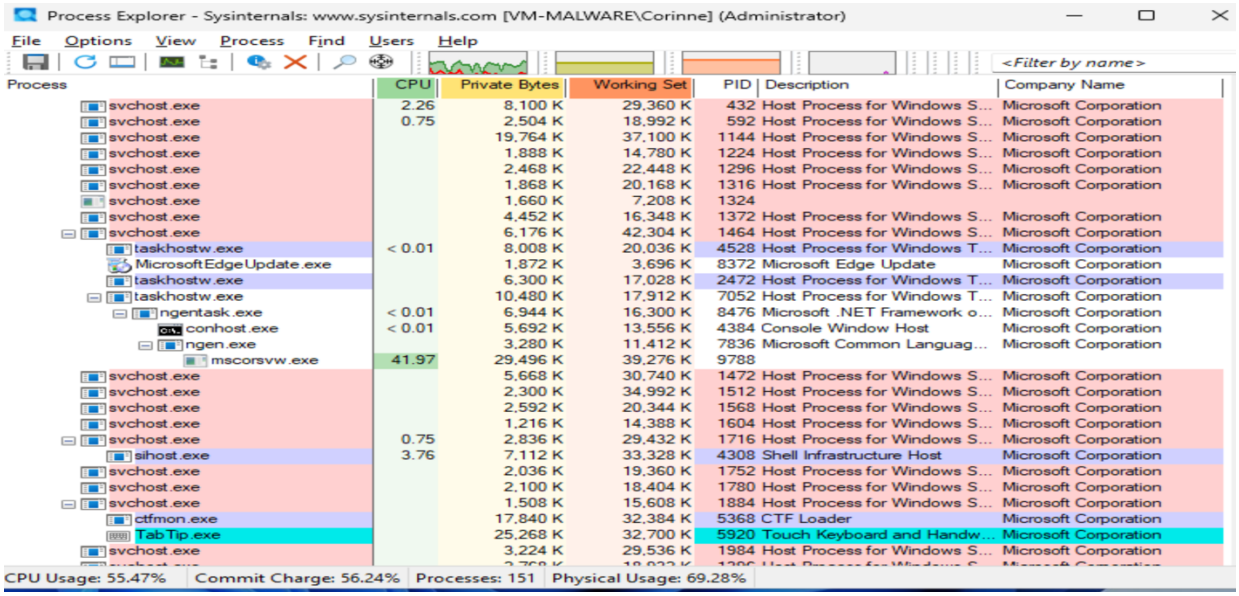
Appendix C – Basic Dynamic Analysis

Regshot Screenshots

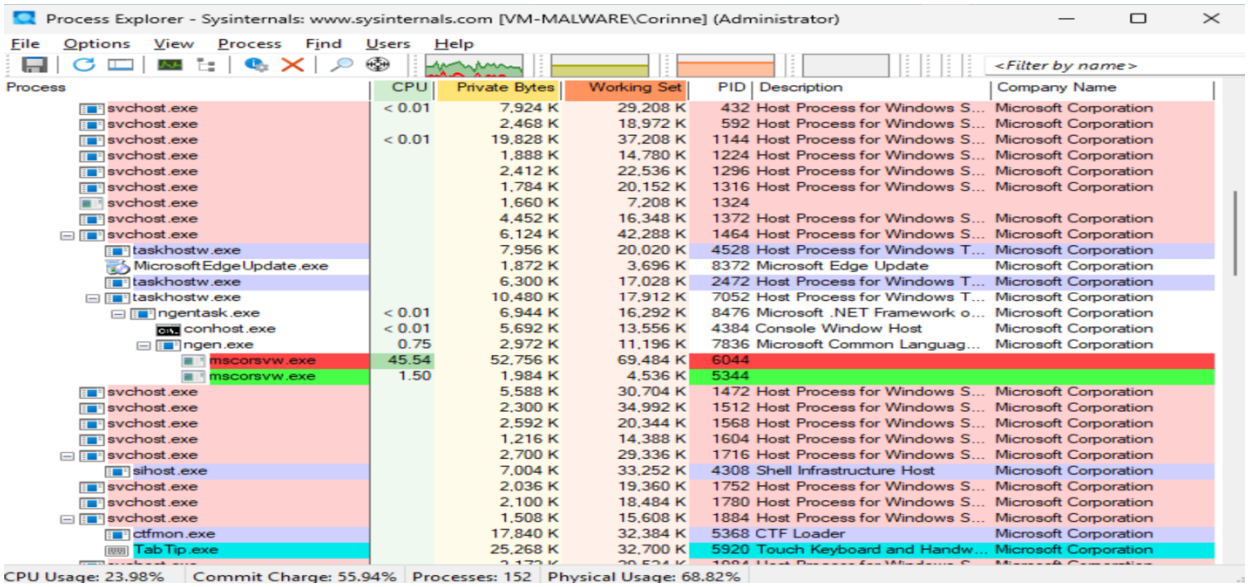
Registry scans are taken before and after running and dynamically analyzing the active processes, file creations/deletions, attempts to connect to the network, etc. Regshot then does a compare of the two scans to provide output on what has changed by running the malicious file. The comparison file is far too large to insert here, but the suspicious changes to the registry were recorded.

Process Explorer Screenshots

Snapshot Before Running the Malicious File:



Snapshot After Running the Malicious File:



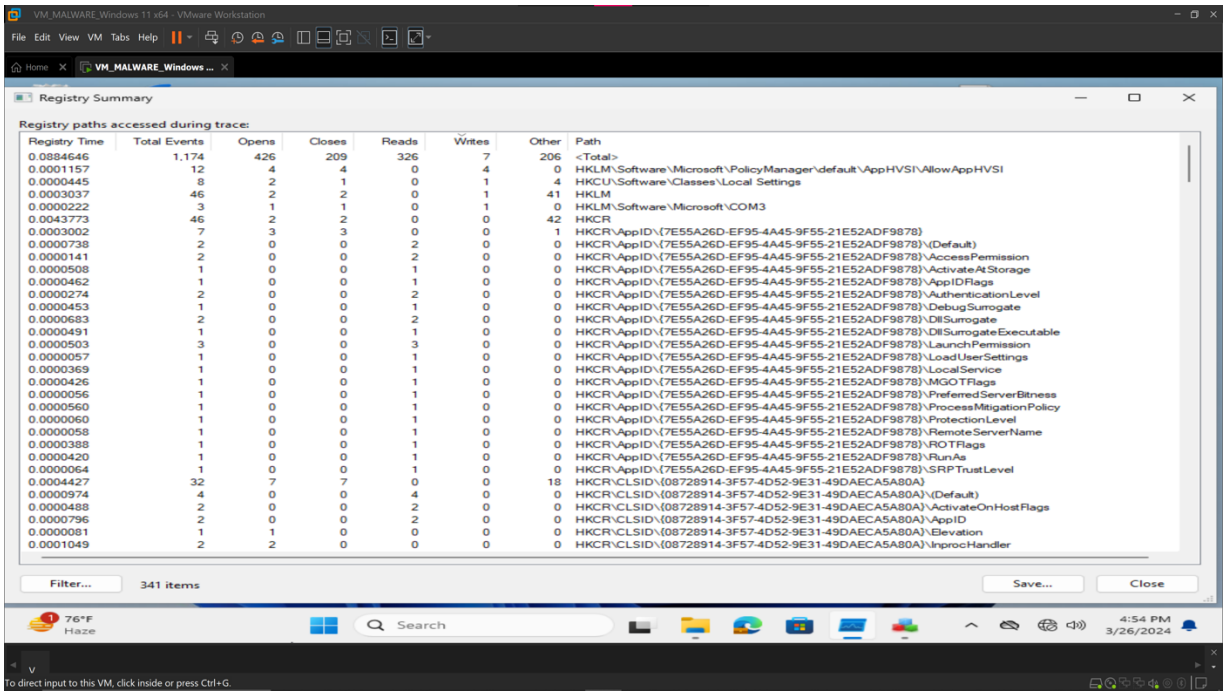
Procman Output Summaries

File Summary:

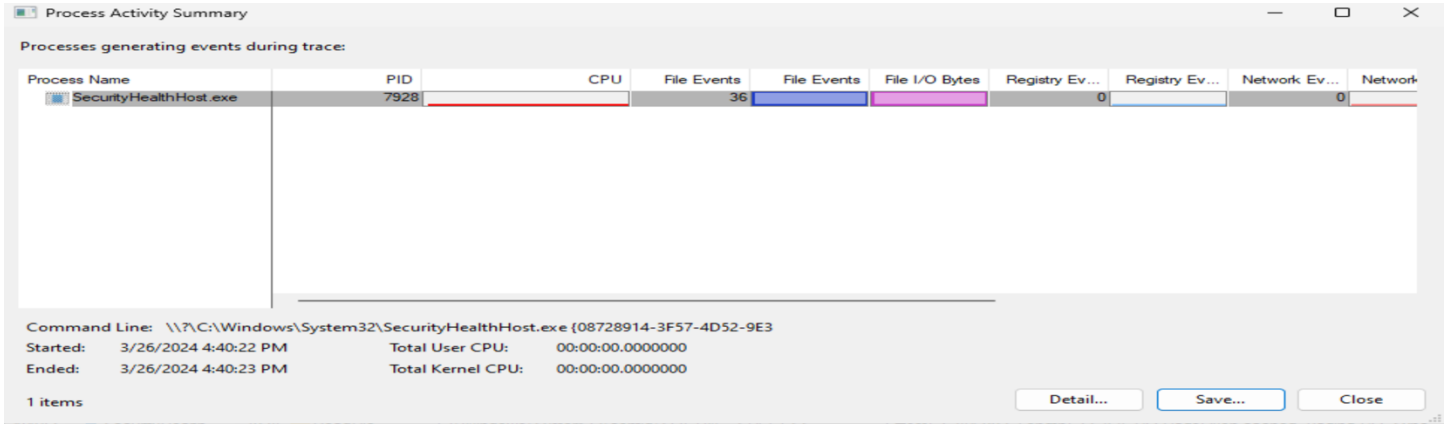
Procmon-FileSummary

File Time	Total Events	Opens	Closes	Reads	Writes	Read Bytes	Write Bytes	Get ACL	Set ACL	Other	Path
0.0280332	244	46	44	36	0	496,416	0	14	0	104	<Total>
0.0067880	23	2	2	13	0	180,224	0	1	0	5	C:\Windows\System32\wpnapps.dll
0.0027401	17	2	2	7	0	102,400	0	1	0	5	C:\Windows\System32\SecurityHealthAgent.dll
0.0038039	15	3	3	2	0	12,288	0	1	0	6	C:\Windows\System32\SecurityHealthUdk.dll
0.0007027	15	2	2	2	0	24,576	0	1	0	8	C:\Windows\System32\wldp.dll
0.0005561	14	4	4	0	0	0	0	0	0	6	C:\Windows\System32\rpcss.dll
0.0022095	11	2	2	1	0	8,192	0	1	0	5	C:\Windows\System32\msxml6.dll
0.0002310	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\OneCoreUAPCommonProxyStub.dll
0.0032228	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\SecurityHealthProxyStub.dll
0.0003772	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\ShellCommonCommonProxyStub.dll
0.0000862	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\WinTypes.dll
0.0001457	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\kernel.appcore.dll
0.0001042	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\msasn1.dll
0.0000881	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\msvcp110_win.dll
0.0001837	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\ntmarta.dll
0.0002191	10	2	2	0	0	0	0	1	0	5	C:\Windows\System32\policymanager.dll
0.0001267	8	2	2	0	0	0	0	0	0	4	C:\Windows\System32\msxml6r.dll
0.0000883	7	2	2	0	0	0	0	0	0	3	C:\Windows\System32\imm32.dll
0.0001004	7	2	2	0	0	0	0	0	0	3	C:\Windows\System32\oleaut32.dll
0.0000917	6	1	1	0	0	0	0	0	0	4	C:\Windows\System32\SecurityHealthHost.exe
0.0004520	6	1	1	1	0	20,480	0	0	0	3	C:\Windows\System32\en-US\SecurityHealthAgent.dll.mui
0.0027159	5	1	1	2	0	16,260	0	0	0	1	C:\Windows\Prefetch\SECURITYHEALTHHOST.EXE-06344EE9.pf
0.0012725	5	0	0	5	0	131,072	0	0	0	0	C:\Windows\System32\config\SOFTWARE
0.0001059	5	1	1	0	0	0	0	0	0	3	C:\Windows\System32\en-US\KernelBase.dll.mui
0.0014779	3	0	0	3	0	924	0	0	0	0	C:\$MapAttributeValue
0.0000407	2	1	1	0	0	0	0	0	0	0	C:\Windows\System32
0.0000450	2	2	0	0	0	0	0	0	0	0	C:\Windows\System32\MsMpLics.dll
0.0000412	1	0	0	0	0	0	0	0	0	1	C:\Windows\System32\SHCore.dll
0.0000097	1	0	0	0	0	0	0	0	0	1	C:\Windows\System32\shell32.dll
0.0000070	1	0	0	0	0	0	0	0	0	1	C:\Windows\System32\shlwapi.dll

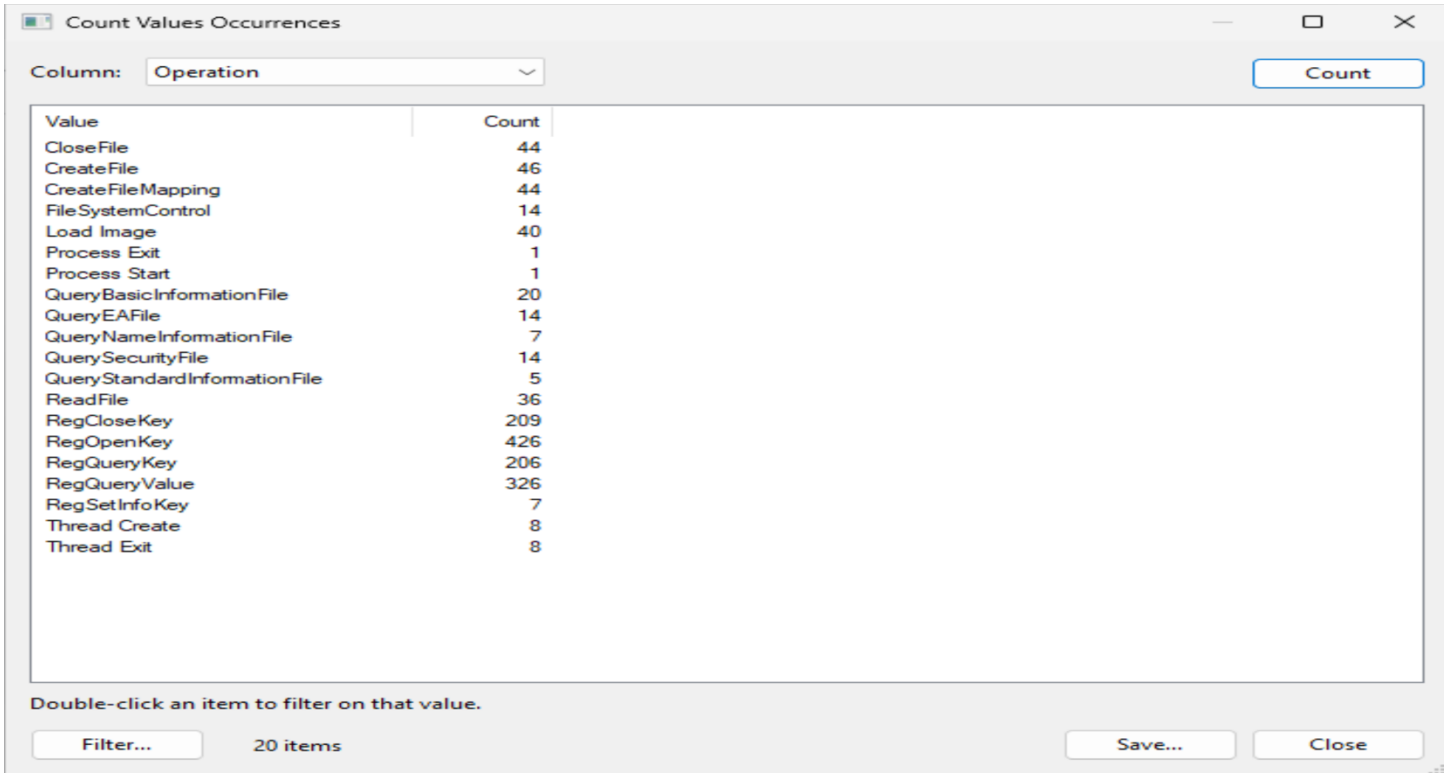
Registry Summary:



Process Activity Summary:



Count Values Occurrences Summary:



Logfile Summary:

Included in Zip File. This logfile was essential to identifying what the malicious software was doing upon execution and trying to do after. It also confirmed that most of the strings that were identified as suspicious early on did turn out to be malicious.

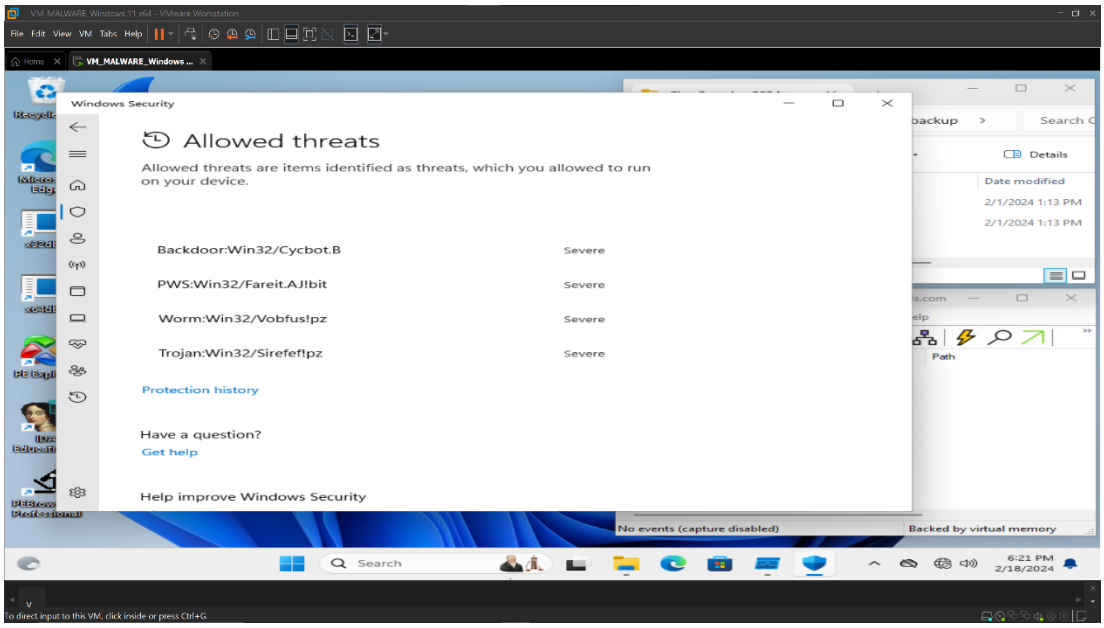
Wireshark Results

The Wireshark output is far too large to include here, but as you can see, the malicious file did make efforts to get out to the network to go to this url (highlighted in black):

… 61.451562	localhost	localhost	TCP	44	0	50721 → ddi-tcp-1(8888) [ACK] Seq=1 Ack=1 Win=262144 Len=0
… 61.465454	localhost	localhost	HTTP	403	359	GET http://adobe-dns-3-adobe.com/wlemf.php?fyuj=4156b7a30441&dfrofe=ASCmxt
… 61.465526	localhost	localhost	TCP	44	0	ddi-tcp-1(8888) → 50721 [ACK] Seq=1 Ack=360 Win=2160896 Len=0

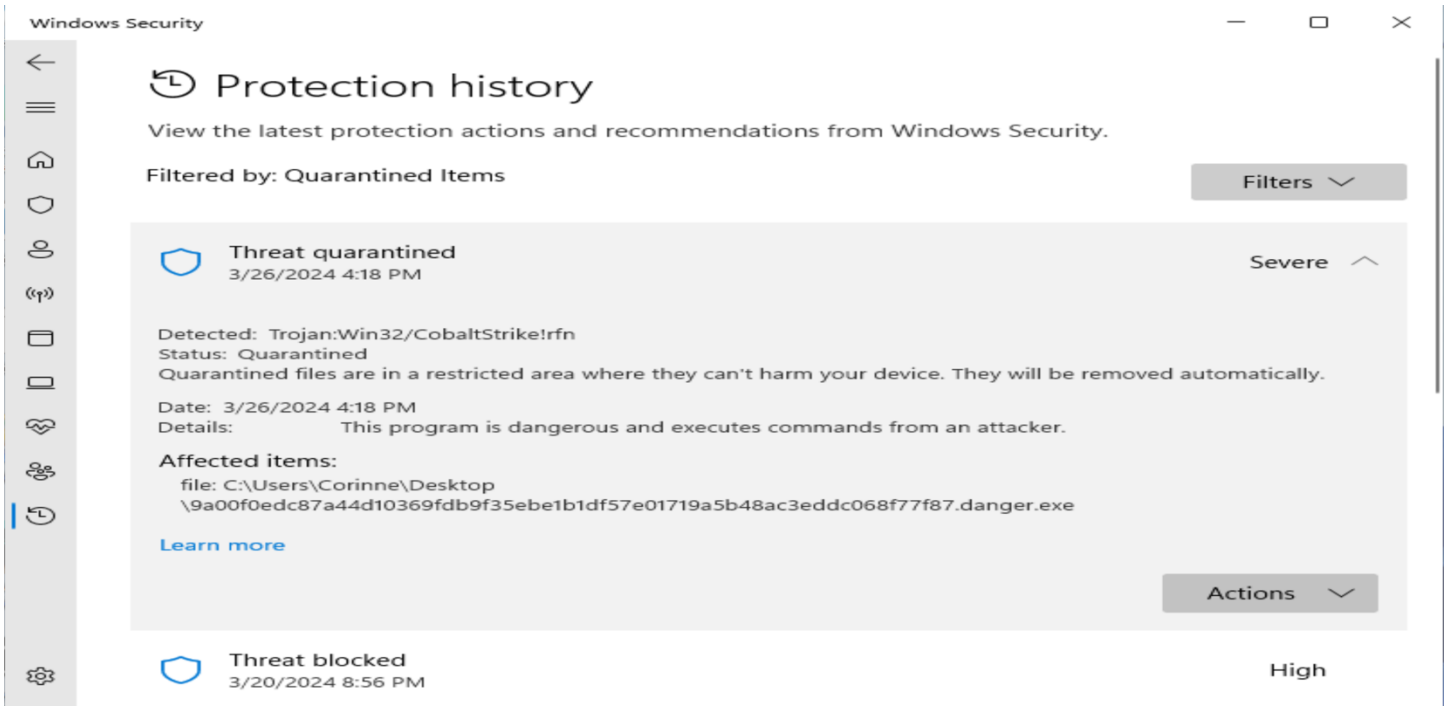
Anitvirus Screenshots

Notifications from Windows Antivirus During Execution of file:



Windows Defender Alert Screenshot

As you can see, Windows Defender did recognize and quarantine this malicious file.


Windows Security
Protection history
View the latest protection actions and recommendations from Windows Security.
Filtered by: Quarantined Items
Filters
Threat quarantined
3/26/2024 4:18 PM
Severe
Detected: Trojan:Win32/CobaltStrike!rfn
Status: Quarantined
Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.
Date: 3/26/2024 4:18 PM
Details: This program is dangerous and executes commands from an attacker.
Affected items:
file: C:\Users\Corinne\Desktop
\9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87.danger.exe
Learn more
Actions
Threat blocked
3/20/2024 8:56 PM
High

Appendix D – Advanced Static Analysis

Capa File Analysis

The Capa utility shows how each of the functions works, what they are trying to do, and how the program flows. This provided the most essential information in discovering the functionality of the code.

```
md5                     c9b105ec2412ac0e2ace20bfa71e1450
sha1                    3cef1ca36a78cba308fb29a46b20e5ca22d03289
sha256                  9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48ac3eddc068f77f87
path
C:/Users/Corinne/Desktop/Danger2/FinalRE/9a00f0edc87a44d10369fdb9f35ebe1b1df57e01719a5b48
ac3eddc068f77f87.danger
timestamp               2024-03-29 01:24:55.870681
capa version            7.0.1
os                      windows
format                  pe
arch                    i386
analysis                static
extractor               VivisectFeatureExtractor
base address            0x400000
rules                   C:/Users/Corinne/AppData/Local/Temp/_MEI84762/rules
function count          79
library function count  2
total feature count     3086

allocate memory (2 matches, only showing first match of library rule)
author  0x534a@mailbox.org, @mr-tz
scope   basic block
mbc     Memory::Allocate Memory [C0007]
basic block @ 0x4012C9 in function 0x401235
  or:
    api: ZwAllocateVirtualMemory @ 0x4012EC

allocate or change RW memory (library rule)
author  0x534a@mailbox.org, @mr-tz
scope   basic block
mbc     Memory::Allocate Memory [C0007]
basic block @ 0x402B05 in function 0x402B05
  and:
    or:
      match: allocate memory @ 0x402B05
        or:
          api: VirtualAlloc @ 0x402B1C
    or:
      number: 0x4 = PAGE_READWRITE @ 0x402B0C

change memory protection (library rule)
author  @mr-tz
scope   basic block
mbc     Memory::Change Memory Protection [C0008]
basic block @ 0x402A24 in function 0x40296D
  or:
    api: VirtualProtect @ 0x402A32

contain loop (23 matches, only showing first match of library rule)
author  moritz.raabe@mandiant.com
scope   function
function @ 0x401000
  or:
    characteristic: loop @ 0x401000

create or open file (4 matches, only showing first match of library rule)
author  michael.hunhoff@mandiant.com, joakim@intezer.com
scope   basic block
mbc     File System::Create File [C0016]
basic block @ 0x401D9C in function 0x401D9C
  or:
    api: CreateFile @ 0x401DE4
```

```
delay execution (2 matches, only showing first match of library rule)
author      michael.hunhoff@mandiant.com, @ramen0x3f
scope       basic block
mbc         Anti-Behavioral Analysis::Dynamic Analysis Evasion::Delayed Execution
[B0003.003]
references  https://docs.microsoft.com/en-us/windows/win32/sync/wait-functions,
https://github.com/LordNoteworthy/al-khaser/blob/master/al-
khaser/TimingAttacks/timing.cpp
basic block @ 0x402228 in function 0x402205
  or:
    and:
      os: windows
      or:
        api: Sleep @ 0x40222D

get OS version (library rule)
author  @mr-tz
scope   function
function @ 0x40247A
  or:
    api: GetVersionEx @ 0x4024D1

write process memory (library rule)
author  moritz.raabe@mandiant.com
scope   function
att&ck  Defense Evasion::Process Injection [T1055]
function @ 0x401235
  or:
    api: ZwWriteVirtualMemory @ 0x401326

get MAC address on Windows
namespace   collection/network
author      moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com,
echernofsky@google.com
scope       function
att&ck      Discovery::System Information Discovery [T1082]
references  https://github.com/LordNoteworthy/al-khaser/blob/master/al-
khaser/Shared/Utils.cpp#L128,
https://evasions.checkpoint.com/techniques/network.html#check-if-mac-address-is-specific
function @ 0x4023A3
  and:
    os: windows
    or:
      and:
        api: GetAdaptersInfo @ 0x4023B6, 0x4023CB
        or:
          offset: 0x194 = IP_ADAPTER_INFO.Address @ 0x4023F0

capture screenshot
namespace  collection/screenshot
author     moritz.raabe@mandiant.com, @_re_fox, michael.hunhoff@mandiant.com
scope      function
att&ck     Collection::Screen Capture [T1113]
mbc        Collection::Screen Capture::WinAPI [E1113.m01]
function @ 0x402C44
  or:
    and:
      or:
        api: GetWindowDC @ 0x402C58
      or:
        api: BitBlt @ 0x402CC7
      api: CreateCompatibleDC @ 0x402C6A
      api: CreateCompatibleBitmap @ 0x402C9E
      optional:
        or:
          api: GetDesktopWindow = get entire desktop @ 0x402C4E
```

```
receive data
namespace    communication
author       william.ballenthin@mandiant.com
scope        function
mbc          Command and Control::C2 Communication::Receive Data [B0030.002]
description  all known techniques for receiving data from a potential C2 server
function @ 0x401000
  or:
    match: read data from Internet @ 0x401000
      and:
        optional:
          or:
            match: connect to HTTP server @ 0x401000
              and:
                api: InternetConnect @ 0x401059
                optional:
                  match: create HTTP request @ 0x401000
                    and:
                      optional:
                        api: InternetCloseHandle @ 0x4011FC, 0x401205, 0x401211
                      or:
                        api: InternetOpen @ 0x40102C
        or:
          api: InternetReadFile @ 0x401182

send data
namespace    communication
author       william.ballenthin@mandiant.com, joakim@intezer.com
scope        function
mbc          Command and Control::C2 Communication::Send Data [B0030.001]
description  all known techniques for sending data to a potential C2 server
function @ 0x401000
  or:
    and:
      os: windows
      or:
        match: send HTTP request @ 0x401000
          or:
            and:
              or:
                api: HttpOpenRequest @ 0x40109D
                api: InternetConnect @ 0x401059
              or:
                api: HttpSendRequest @ 0x40115F

reference HTTP User-Agent string
namespace   communication/http
author      @mr-tz
scope       function
mbc         Communication::HTTP Communication [C0002]
references  https://www.useragents.me/, https://www.whatismybrowser.com/guides/the-
latest-user-agent/
function @ 0x401000
  or:
    api: ObtainUserAgentString @ 0x40101C

connect to HTTP server
namespace  communication/http/client
author     michael.hunhoff@mandiant.com
scope      function
mbc        Communication::HTTP Communication::Connect to Server [C0002.009]
function @ 0x401000
  and:
    api: InternetConnect @ 0x401059
    optional:
      match: create HTTP request @ 0x401000
```

```
        and:
          optional:
            api: InternetCloseHandle @ 0x4011FC, 0x401205, 0x401211
          or:
            api: InternetOpen @ 0x40102C

create HTTP request
namespace  communication/http/client
author     michael.hunhoff@mandiant.com, anushka.virgaonkar@mandiant.com
scope      function
mbc        Communication::HTTP Communication::Create Request [C0002.012]
function @ 0x401000
  and:
    optional:
      api: InternetCloseHandle @ 0x4011FC, 0x401205, 0x401211
    or:
      api: InternetOpen @ 0x40102C

read data from Internet
namespace  communication/http/client
author     michael.hunhoff@mandiant.com, anushka.virgaonkar@mandiant.com
scope      function
mbc        Communication::HTTP Communication::Get Response [C0002.017]
function @ 0x401000
  and:
    optional:
      or:
        match: connect to HTTP server @ 0x401000
          and:
            api: InternetConnect @ 0x401059
            optional:
              match: create HTTP request @ 0x401000
                and:
                  optional:
                    api: InternetCloseHandle @ 0x4011FC, 0x401205, 0x401211
                  or:
                    api: InternetOpen @ 0x40102C
    or:
      api: InternetReadFile @ 0x401182

send HTTP request
namespace  communication/http/client
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
mbc        Communication::HTTP Communication::Send Request [C0002.003]
function @ 0x401000
  or:
    and:
      or:
        api: HttpOpenRequest @ 0x40109D
        api: InternetConnect @ 0x401059
      or:
        api: HttpSendRequest @ 0x40115F

decode data using Base64 via WinAPI (2 matches)
namespace  data-manipulation/encoding/base64
author     michael.hunhoff@mandiant.com
scope      basic block
att&ck     Defense Evasion::Deobfuscate/Decode Files or Information [T1140]
basic block @ 0x4016EA in function 0x4016CB
  and:
    api: CryptStringToBinary @ 0x4016F7
    or:
      number: 0x1 = dwFlags=CRYPT_STRING_BASE64 @ 0x4016F1
basic block @ 0x401705 in function 0x4016CB
  and:
    api: CryptStringToBinary @ 0x401721
```

```
    or:
      number: 0x1 = dwFlags=CRYPT_STRING_BASE64 @ 0x40171B

encode data using XOR (2 matches)
namespace  data-manipulation/encoding/xor
author     moritz.raabe@mandiant.com
scope      basic block
att&ck     Defense Evasion::Obfuscated Files or Information [T1027]
mbc        Defense Evasion::Obfuscated Files or Information::Encoding-Standard Algorithm
[E1027.m02], Data::Encode Data::XOR [C0026.002]
basic block @ 0x402430 in function 0x4023A3
  and:
    characteristic: tight loop @ 0x402430
    characteristic: nzxor @ 0x402434
    not: = filter for potential false positives
      or:
        or: = unsigned bitwise negation operation (~i)
          number: 0xFFFFFFFF = bitwise negation for unsigned 32 bits
          number: 0xFFFFFFFFFFFFFFFF = bitwise negation for unsigned 64 bits
        or: = signed bitwise negation operation (~i)
          number: 0xFFFFFFF = bitwise negation for signed 32 bits
          number: 0xFFFFFFFFFFFFFFF = bitwise negation for signed 64 bits
        or: = Magic constants used in the implementation of strings functions.
          number: 0x7EFEFEFF = optimized string constant for 32 bits
          number: 0x81010101 = -0x81010101 = 0x7EFEFEFF
          number: 0x81010100 = 0x81010100 = ~0x7EFEFEFF
          number: 0x7EFEFEFEFEFEFEFF = optimized string constant for 64 bits
          number: 0x8101010101010101 = -0x8101010101010101 = 0x7EFEFEFEFEFEFEFF
          number: 0x8101010101010100 = 0x8101010101010100 = ~0x7EFEFEFEFEFEFEFF
basic block @ 0x402E18 in function 0x402DF2
  and:
    characteristic: tight loop @ 0x402E18
    characteristic: nzxor @ 0x402E1C
    not: = filter for potential false positives
      or:
        or: = unsigned bitwise negation operation (~i)
          number: 0xFFFFFFFF = bitwise negation for unsigned 32 bits
          number: 0xFFFFFFFFFFFFFFFF = bitwise negation for unsigned 64 bits
        or: = signed bitwise negation operation (~i)
          number: 0xFFFFFFF = bitwise negation for signed 32 bits
          number: 0xFFFFFFFFFFFFFFF = bitwise negation for signed 64 bits
        or: = Magic constants used in the implementation of strings functions.
          number: 0x7EFEFEFF = optimized string constant for 32 bits
          number: 0x81010101 = -0x81010101 = 0x7EFEFEFF
          number: 0x81010100 = 0x81010100 = ~0x7EFEFEFF
          number: 0x7EFEFEFEFEFEFEFF = optimized string constant for 64 bits
          number: 0x8101010101010101 = -0x8101010101010101 = 0x7EFEFEFEFEFEFEFF
          number: 0x8101010101010100 = 0x8101010101010100 = ~0x7EFEFEFEFEFEFEFF

create new key via CryptAcquireContext (3 matches)
namespace   data-manipulation/encryption
author      chuong.dong@mandiant.com
scope       function
att&ck      Defense Evasion::Obfuscated Files or Information [T1027]
mbc         Cryptography::Encryption Key [C0028]
references  https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-
cryptacquirecontexta
function @ 0x4014EE
  and:
    api: CryptAcquireContext @ 0x40150D
    or:
      number: 0x18 = CRYPT_NEWKEYSET | CRYPT_DELETEKEYSET @ 0x401504
function @ 0x4015EC
  and:
    api: CryptAcquireContext @ 0x40160B
    or:
      number: 0x18 = CRYPT_NEWKEYSET | CRYPT_DELETEKEYSET @ 0x401602
```

```
function @ 0x401737
  and:
    api: CryptAcquireContext @ 0x401756
    or:
      number: 0x8 = CRYPT_NEWKEYSET @ 0x40177E, 0x401799
      number: 0x18 = CRYPT_NEWKEYSET | CRYPT_DELETEKEYSET @ 0x40174D

encrypt or decrypt via WinCrypt (2 matches)
namespace  data-manipulation/encryption
author     moritz.raabe@mandiant.com
scope      function
att&ck     Defense Evasion::Obfuscated Files or Information [T1027]
mbc        Cryptography::Decrypt Data [C0031], Cryptography::Encrypt Data [C0027]
function @ 0x4014EE
  and:
    or:
      api: CryptDecrypt @ 0x401583
    optional:
      or:
        api: CryptAcquireContext @ 0x40150D
        api: CryptImportKey @ 0x40154D
function @ 0x4015EC
  and:
    or:
      api: CryptEncrypt @ 0x40166A, 0x4016A2
    optional:
      or:
        api: CryptAcquireContext @ 0x40160B
        api: CryptImportKey @ 0x40164B

encrypt data using AES via WinAPI (3 matches)
namespace  data-manipulation/encryption/aes
author     moritz.raabe@mandiant.com
scope      function
att&ck     Defense Evasion::Obfuscated Files or Information [T1027]
mbc        Defense Evasion::Obfuscated Files or Information::Encryption-Standard
Algorithm [E1027.m05], Cryptography::Encrypt Data::AES [C0027.001]
function @ 0x4014EE
  and:
    or:
      api: CryptImportKey @ 0x40154D
    or:
      number: 0x6610 = CALG_AES_256 @ 0x401529
    optional:
      or:
        number: 0x1 = PROV_RSA_FULL @ 0x40157D
        api: CryptAcquireContext @ 0x40150D
        api: CryptDecrypt @ 0x401583
function @ 0x4015EC
  and:
    or:
      api: CryptImportKey @ 0x40164B
    or:
      number: 0x6610 = CALG_AES_256 @ 0x401627
    optional:
      or:
        number: 0x1 = PROV_RSA_FULL @ 0x401661, 0x40169C
        api: CryptAcquireContext @ 0x40160B
        api: CryptEncrypt @ 0x40166A, 0x4016A2
function @ 0x401737
  and:
    or:
      api: CryptGenKey @ 0x40176E
    or:
      number: 0x6610 = CALG_AES_256 @ 0x401766
    optional:
      or:
```

```
        number: 0x1 = PROV_RSA_FULL @ 0x401764
        api: CryptAcquireContext @ 0x401756

generate random numbers via RtlGenRandom (2 matches)
namespace   data-manipulation/prng
author      william.ballenthin@mandiant.com, richard.weiss@mandiant.com
scope       function
mbc         Cryptography::Generate Pseudo-random Sequence::Use API [C0021.003]
references  https://doxygen.reactos.org/df/d13/sysfunc_8c_source.html,
https://blog.gentilkiwi.com/tag/systemfunction036
function @ 0x401806
  or:
    api: SystemFunction036 @ 0x401810
function @ 0x40182A
  or:
    api: SystemFunction036 @ 0x401855

get common file path (3 matches)
namespace  host-interaction/file-system
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com,
anushka.virgaonkar@mandiant.com
scope      function
att&ck     Discovery::File and Directory Discovery [T1083]
mbc        Discovery::File and Directory Discovery [E1083]
function @ 0x401235
  or:
    api: GetSystemDirectory @ 0x40124A
function @ 0x401D9C
  or:
    api: GetTempPath @ 0x401DB3
    api: GetTempFileName @ 0x401DCB
function @ 0x40270D
  or:
    api: SHGetFolderPath @ 0x402727

copy file
namespace  host-interaction/file-system/copy
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
mbc        File System::Copy File [C0045]
function @ 0x40270D
  or:
    api: CopyFile @ 0x4027B0

delete file
namespace  host-interaction/file-system/delete
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
mbc        File System::Delete File [C0047]
function @ 0x401C5C
  or:
    api: DeleteFile @ 0x401C7B

set file attributes (4 matches)
namespace  host-interaction/file-system/meta
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com,
anushka.virgaonkar@mandiant.com
scope      basic block
att&ck     Defense Evasion::File and Directory Permissions Modification [T1222]
mbc        File System::Set File Attributes [C0050]
basic block @ 0x401C5C in function 0x401C5C
  or:
    api: SetFileAttributes @ 0x401C74
basic block @ 0x401E70 in function 0x401E70
  or:
    api: SetFileAttributes @ 0x401E8D
basic block @ 0x401EF8 in function 0x401E70
```

```
  or:
    api: SetFileAttributes @ 0x401EFF
basic block @ 0x4027BA in function 0x40270D
  or:
    api: SetFileAttributes @ 0x4027C3

move file (2 matches)
namespace  host-interaction/file-system/move
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
mbc        File System::Move File [C0063]
function @ 0x401C5C
  or:
    api: MoveFileEx @ 0x401C89
function @ 0x402205
  or:
    api: MoveFileEx @ 0x402246

write file on Windows (2 matches)
namespace  host-interaction/file-system/write
author     william.ballenthin@mandiant.com, anushka.virgaonkar@mandiant.com
scope      function
mbc        File System::Writes File [C0052]
function @ 0x401D9C
  or:
    and:
      os: windows
      optional:
        basic block:
          or:
            number: 0x40000000 = GENERIC_WRITE @ 0x401DD8
            number: 0x2 = FILE_WRITE_DATA @ 0x401DD4
            match: create or open file @ 0x401D9C
              or:
                api: CreateFile @ 0x401DE4
      or:
        api: WriteFile @ 0x401DFE
function @ 0x401E70
  or:
    and:
      os: windows
      optional:
        basic block:
          or:
            number: 0x40000000 = GENERIC_WRITE @ 0x401E9C
            number: 0x2 = FILE_WRITE_DATA @ 0x401E98
            match: create or open file @ 0x401E70
              or:
                api: CreateFile @ 0x401EA2
      or:
        api: WriteFile @ 0x401EBB

check mutex and exit
namespace  host-interaction/mutex
author     @_re_fox, moritz.raabe@mandiant.com
scope      function
mbc        Process::Check Mutex [C0043], Process::Terminate Process [C0018]
function @ 0x401F09
  and:
    match: create mutex @ 0x401F09
      or:
        api: CreateMutex @ 0x401F41
    or:
      or:
        and:
          api: GetLastError @ 0x401F50
          or:
```

```
            number: 0xB7 = ERROR_ALREADY_EXISTS @ 0x401F56

create mutex
namespace  host-interaction/mutex
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
mbc        Process::Create Mutex [C0042]
function @ 0x401F09
  or:
    api: CreateMutex @ 0x401F41

get hostname (2 matches)
namespace  host-interaction/os/hostname
author     moritz.raabe@mandiant.com, joakim@intezer.com, anushka.virgaonkar@mandiant.com
scope      function
att&ck     Discovery::System Information Discovery [T1082]
mbc        Discovery::System Information Discovery [E1082]
function @ 0x4023A3
  or:
    api: GetComputerName @ 0x402428
function @ 0x40247A
  or:
    api: GetComputerNameEx @ 0x40251C

get system information on Windows
namespace  host-interaction/os/info
author     moritz.raabe@mandiant.com, joakim@intezer.com
scope      function
att&ck     Discovery::System Information Discovery [T1082]
function @ 0x40247A
  and:
    os: windows
    or:
      api: GetSystemInfo @ 0x40248F

create process on Windows
namespace  host-interaction/process/create
author     moritz.raabe@mandiant.com
scope      basic block
mbc        Process::Create Process [C0017]
basic block @ 0x4018D1 in function 0x4018D1
  or:
    api: CreateProcess @ 0x401909

allocate or change RWX memory
namespace  host-interaction/process/inject
author     @mr-tz
scope      basic block
mbc        Memory::Allocate Memory [C0007]
basic block @ 0x4012C9 in function 0x401235
  and:
    or:
      match: allocate memory @ 0x4012C9
        or:
          api: ZwAllocateVirtualMemory @ 0x4012EC
    or:
      number: 0x40 = PAGE_EXECUTE_READWRITE @ 0x4012D7

enumerate processes
namespace  host-interaction/process/list
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
att&ck     Discovery::Process Discovery [T1057], Discovery::Software Discovery [T1518]
function @ 0x401C98
  or:
    and:
      api: Process32First @ 0x401CC2
```

```
      api: Process32Next @ 0x401D1A
      optional:
        basic block:
          and:
            api: CreateToolhelp32Snapshot @ 0x401CA9
            or:
              number: 0x2 = TH32CS_SNAPPROCESS @ 0x401CA7

terminate process (2 matches)
namespace  host-interaction/process/terminate
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com,
anushka.virgaonkar@mandiant.com
scope      function
mbc        Process::Terminate Process [C0018]
function @ 0x4027E3
  or:
    and:
      or:
        api: ExitProcess @ 0x40289E
function @ 0x4028D8
  or:
    and:
      or:
        api: ExitProcess @ 0x402915

get session user name
namespace  host-interaction/session
author     moritz.raabe@mandiant.com, anushka.virgaonkar@mandiant.com
scope      function
att&ck     Discovery::System Owner/User Discovery [T1033], Discovery::Account Discovery
[T1087]
function @ 0x40247A
  or:
    api: GetUserName @ 0x402558

create thread
namespace  host-interaction/thread/create
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com, joakim@intezer.com,
anushka.virgaonkar@mandiant.com
scope      basic block
mbc        Process::Create Thread [C0038]
basic block @ 0x401949 in function 0x401949
  or:
    and:
      os: windows
      or:
        api: CreateThread @ 0x40195A

resume thread
namespace  host-interaction/thread/resume
author     0x534a@mailbox.org, anushka.virgaonkar@mandiant.com
scope      basic block
mbc        Process::Resume Thread [C0054]
basic block @ 0x401345 in function 0x401235
  or:
    api: ZwResumeThread @ 0x401376

link function at runtime on Windows
namespace  linking/runtime-linking
author     moritz.raabe@mandiant.com, michael.hunhoff@mandiant.com
scope      function
att&ck     Execution::Shared Modules [T1129]
function @ 0x40143A
  and:
    os: windows
    or:
      api: GetProcAddress @ 0x4014B9
```

```
    optional:
      api: LoadLibrary @ 0x401478

inspect section memory permissions
namespace    load-code/pe
author       @Ana06
scope        function
mbc          Discovery::Code Discovery::Inspect Section Memory Permissions [B0046.002]
description  translate section memory permissions (specified in the 'Characteristics'
field of the image section header) into page protection constants
function @ 0x40296D
  and:
    os: windows
    3 or more:
      and:
        number: 0x40000000 = IMAGE_SCN_MEM_READ @ 0x4029B6
        number: 0x2 = PAGE_READONLY @ 0x4029FD
      and:
        number: 0x20000000 = IMAGE_SCN_MEM_EXECUTE @ 0x4029AE
        number: 0x10 = PAGE_EXECUTE @ 0x402A01
      and:
        or:
          number: 0x60000000 = IMAGE_SCN_MEM_READ | IMAGE_SCN_MEM_EXECUTE @ 0x4029BE
          and:
            number: 0x40000000 = IMAGE_SCN_MEM_READ @ 0x4029B6
            number: 0x20000000 = IMAGE_SCN_MEM_EXECUTE @ 0x4029AE
        number: 0x20 = PAGE_EXECUTE_READ @ 0x4029F9
      and:
        or:
          number: 0xC0000000 = IMAGE_SCN_MEM_READ | IMAGE_SCN_MEM_WRITE @ 0x4029D6
          and:
            number: 0x40000000 = IMAGE_SCN_MEM_READ @ 0x4029B6
            number: 0x80000000 = IMAGE_SCN_MEM_WRITE @ 0x4029C6
        number: 0x4 = PAGE_READWRITE @ 0x4029EA
      and:
        or:
          number: 0xE0000000 = IMAGE_SCN_MEM_READ | IMAGE_SCN_MEM_WRITE |
IMAGE_SCN_MEM_EXECUTE @ 0x4029A7, 0x4029DE
          and:
            number: 0x40000000 = IMAGE_SCN_MEM_READ @ 0x4029B6
            number: 0x80000000 = IMAGE_SCN_MEM_WRITE @ 0x4029C6
            number: 0x20000000 = IMAGE_SCN_MEM_EXECUTE @ 0x4029AE
        number: 0x40 = PAGE_EXECUTE_READWRITE @ 0x4029E6, 0x402A15

parse PE header
namespace  load-code/pe
author     moritz.raabe@mandiant.com
scope      function
att&ck     Execution::Shared Modules [T1129]
function @ 0x4017D6
  and:
    os: windows
    and:
      mnemonic: cmp @ 0x4017E5, 0x4017ED, 0x4017F5
      or:
        number: 0x4550 = IMAGE_NT_SIGNATURE (PE) @ 0x4017F5
      or:
        number: 0x5A4D = IMAGE_DOS_SIGNATURE (MZ) @ 0x4017E0

execute shellcode via indirect call
namespace  load-code/shellcode
author     ronnie.salomonsen@mandiant.com
scope      function
mbc        Memory::Allocate Memory [C0007]
function @ 0x401235
  and:
    match: allocate or change RWX memory @ 0x4012C9
```

```
      and:
        or:
          match: allocate memory @ 0x4012C9
            or:
              api: ZwAllocateVirtualMemory @ 0x4012EC
        or:
          number: 0x40 = PAGE_EXECUTE_READWRITE @ 0x4012D7
    or:
      characteristic: indirect call @ 0x401387, 0x40138C

get startup folder
namespace  persistence/startup-folder
author     matthew.williams@mandiant.com
scope      basic block
att&ck     Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup
Folder [T1547.001]
basic block @ 0x40270D in function 0x40270D
  and:
    or:
      number: 0x7 = CSIDL_STARTUP @ 0x402724
    or:
      api: SHGetFolderPath @ 0x402727

write file to startup folder
namespace  persistence/startup-folder
author     matthew.williams@mandiant.com
scope      function
att&ck     Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup
Folder [T1547.001]
function @ 0x40270D
  and:
    match: get startup folder @ 0x40270D
      and:
        or:
          number: 0x7 = CSIDL_STARTUP @ 0x402724
        or:
          api: SHGetFolderPath @ 0x402727
    or:
      match: copy file @ 0x40270D
        or:
          api: CopyFile @ 0x4027B0
```

Appendix E – Conclusion

All IDAPro database saves, logs, raw data files, screenshots, etc. are in the zipped file entitled "Associated Materials." I have also included the Outline that I created after researching each part of what was asked for in the Challenge.