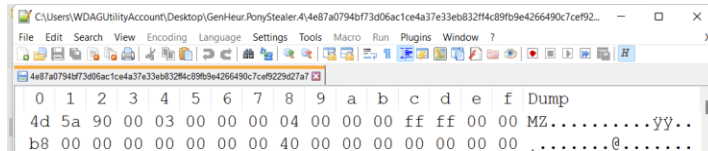


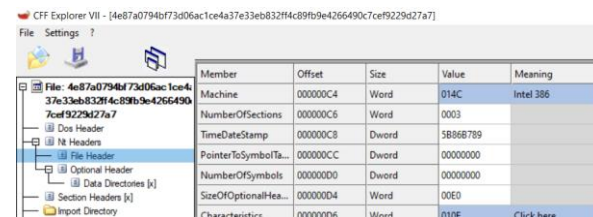
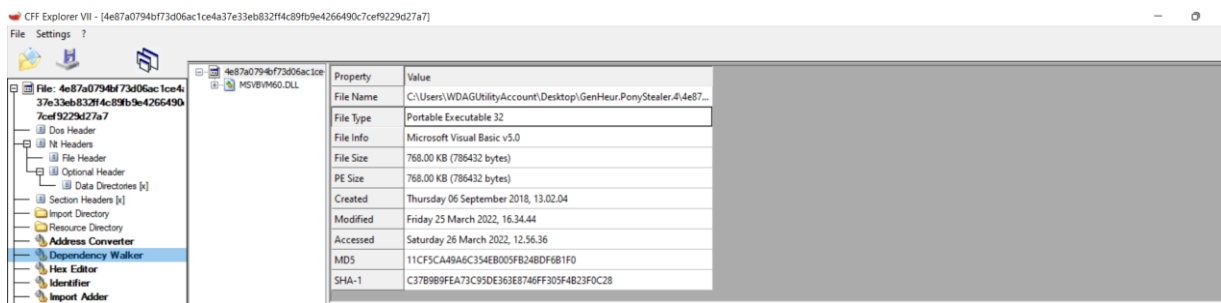
Static Malware Analysis Report

1. Gen:Heur.PonyStealer.4

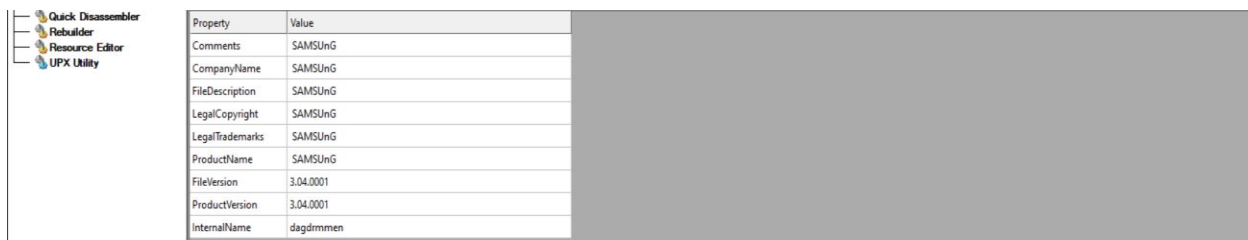
Magic Byte and File Signature: (4d 5a) (MZ) => exe



Machine Information and Exe-Type: 32-bit Micro-processor.

**File-Type:** Portable Executable32

Extra Information: Original File Information



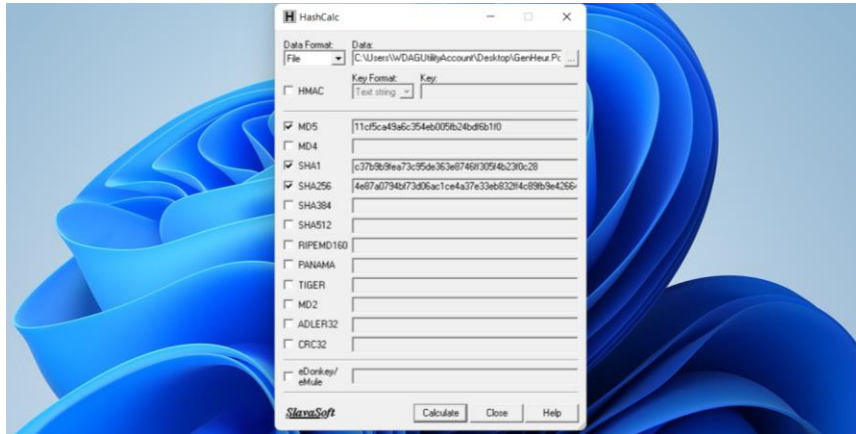
Finger Printing Information:

MD5: 11cf5ca49a6c354eb005fb24bdf6b1f0

SHA1: c37b9b9fea73c95de363e8746ff305f4b23f0c28

SHA256:

4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7



Malicious String:

VB5!6&*

C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

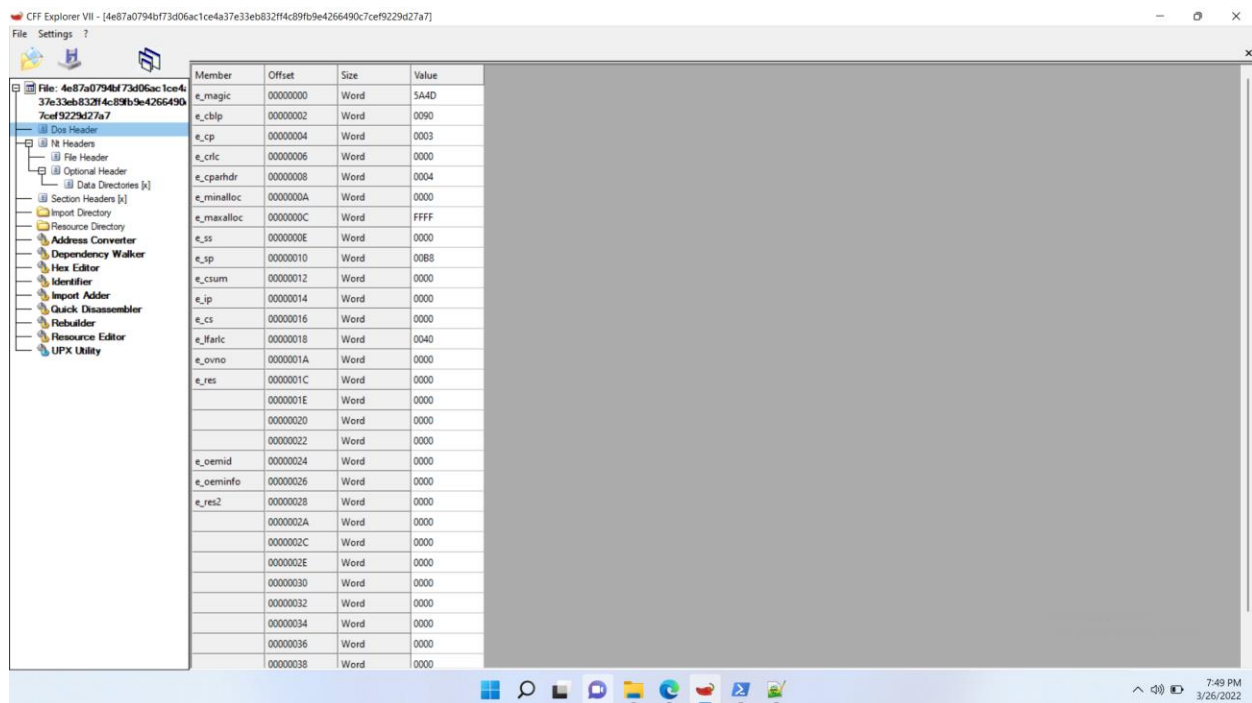
Fjortendagsbladenes

Krankenes5

Badevandsbekendtgrelser

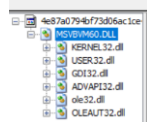
Musikhandlere

Number, Offset, Value:



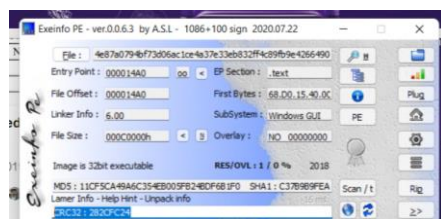
DLL: MSVBVM60.dll

c:\ce4a37e33eb832ff4c89fb9e42\



Packer Information:

CRC32 : 282CFC24



2. Dropped:Trojan.Dropper.Agent.VOE

Magic Byte and File Signature: (4d 5a) (MZ) =>exe

SHA1: 9ee0404b76fe5bda2692f049bb9fc78e17240708

SHA256:
91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

Malicious String:

ADVAPI32.dll

KERNEL32.dll

NTDLL.DLL

GDI32.dll

USER32.dll

COMCTL32.dll

VERSION.dll

VERCHECK

INSTANCECHECK

EXTRACTOPT

TITLE

POSTRUNPROGRAM

RUNPROGRAM

USRQCMD

ADMQCMD

SHOWWINDOW

REBOOT

DecryptFileA

Control Panel\Desktop\ResourceLocale

Number, Offset, Value:

CFF Explorer VII - [91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac]

File Settings ?

Member Offset Size Value

e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000
	00000032	Word	0000
	00000034	Word	0000
	00000036	Word	0000
	00000038	Word	0000

11:56 PM 3/26/2022

DLL: AdvApi32.dll, Kernel32.dll, Gdi32.dll, User32.dll, Comctl32.dll, Version.dll

CFF Explorer VII - [91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac]

File Settings ?

File: 91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

Import Table:

- ADVAPI32.dll
- KERNEL32.dll
- GDI32.dll
- USER32.dll
- COMCTL32.dll
- VERSION.dll

Packer Information:

[1* CAB Archive] , Win32 Cabinet Self-Extractor - try : internal MS .Cab Ripper

Exeinfo PE - ver.0.0.6.3 by A.S.L. - 1086+100 sign 2020.07.22

File: 91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

Entry Point: 0000645C EP Section: .text

File Offset: 0000585C First Bytes: EB 0A 00 00 05

Linker Info: 7.10 Subsystem: Windows GUI PE

File Size: 0006900B Overlay: NO 00000000

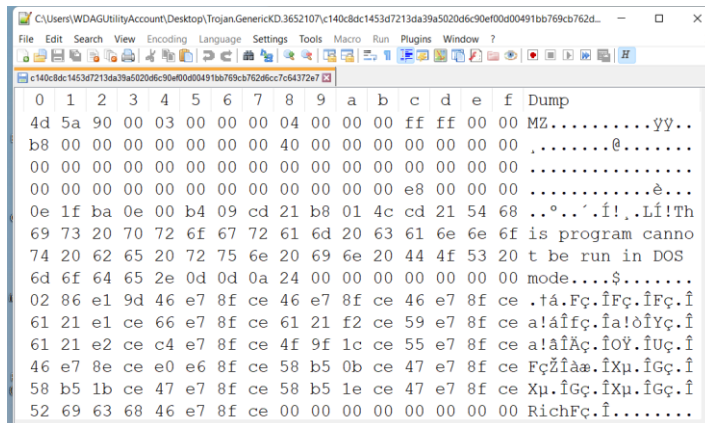
Image is 32bit executable RES/OVL: 90 / 0 % 2004

Scan / t

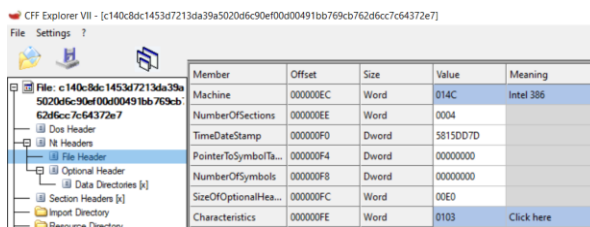
Win32 Cabinet Self-Extractor - try : internal MS .Cab Ripper

3. Trojan.GenericKD.3652107

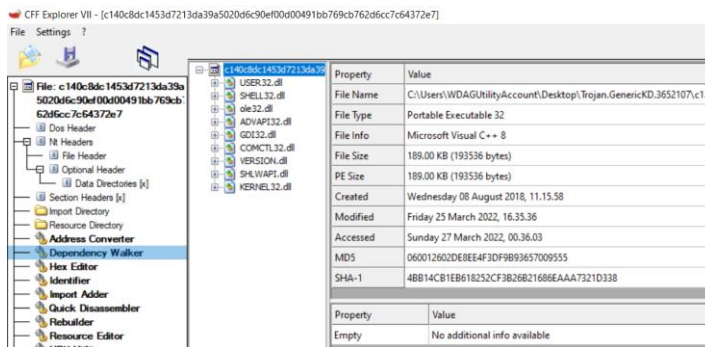
Magic Byte and File Signature: (4d 5a) (MZ) => exe



Machine Information and Exe-Type: 32-bit microprocessor



File-Type: Portable Executable 32



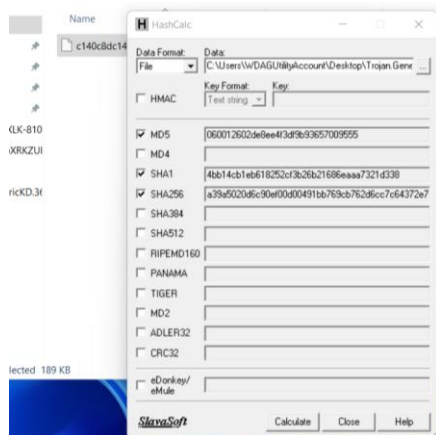
Finger Printing Information:

MD5: 060012602de8ee4f3df9b93657009555

SHA1: 4bb14cb1eb618252cf3b26b21686eaaa7321d338

SHA256:

c140c8dc1453d7213da39a5020d6c90ef00d00491bb769cb762d6cc7c64372e7



Malicious String:

GetWindowsDirectoryA

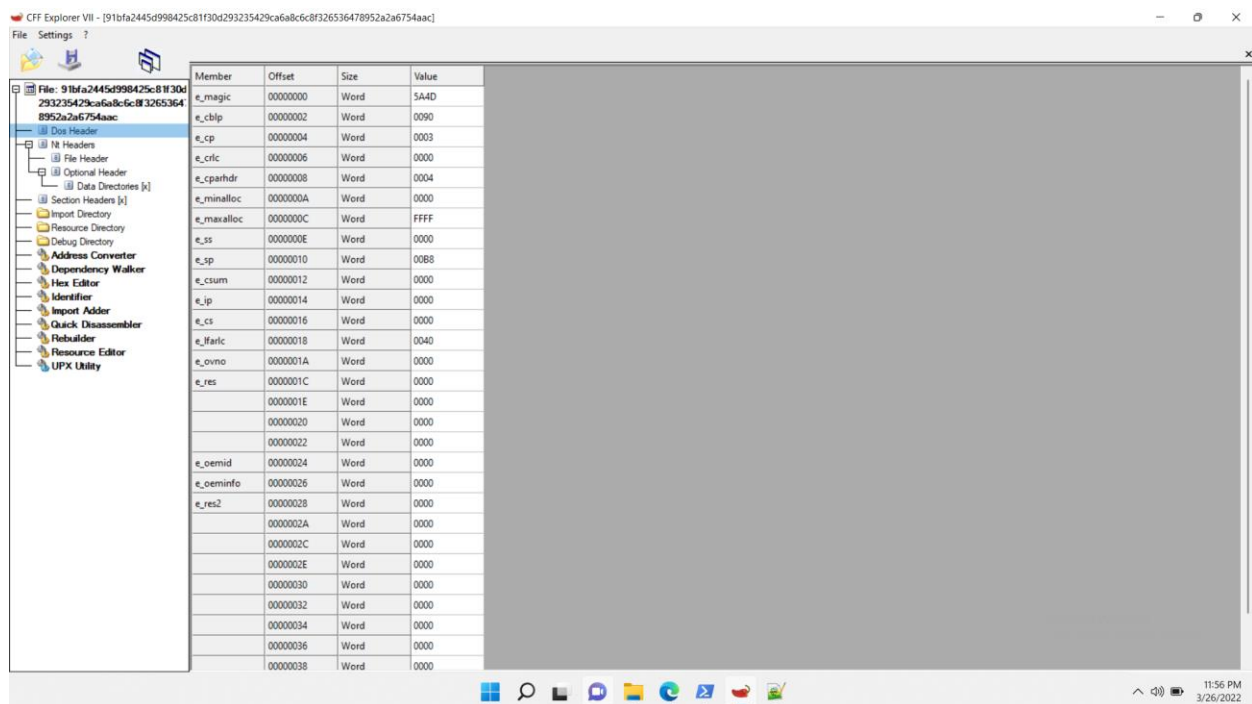
RemoveDirectoryA

CreateFileA

CopyFileA

RegDeleteKeyA

Number, Offset, Value:

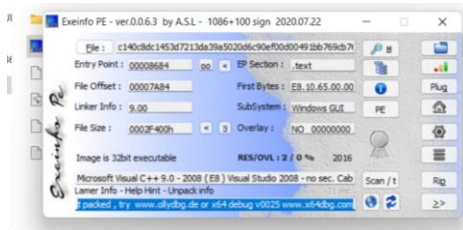


DLL: User32.dll, shell32.dll, ole32.dll, AdvApi32.dll, Gdi32.dll, Comctl32.dll, Version.dll, Shlwapi.dll, Kernel32.dll



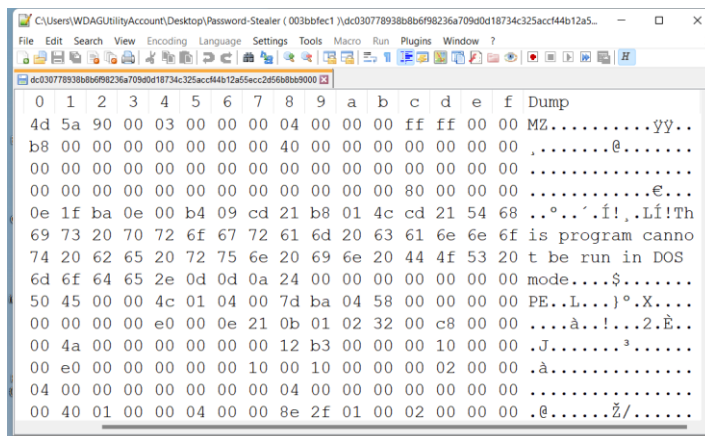
Packer Information:

Not packed

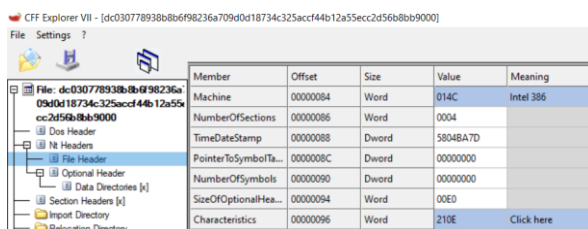


4. Password-Stealer (003bbfec1)

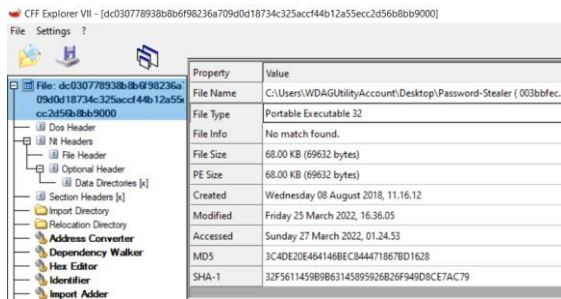
Magic Byte and File Signature: (4d 5a) (MZ) =>exe



Machine Information and Exe-Type: 32-bit microprocessor



File-Type: Portable Executable 32



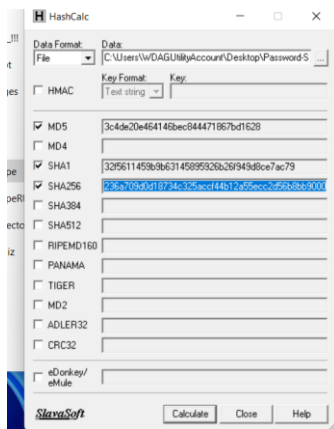
Finger Printing Information:

MD5: 3c4de20e464146bec844471867bd1628

SHA1: 32f5611459b9b63145895926b26f949d8ce7ac79

SHA256:

dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000



Malicious String:

<http://www.ibsensoftware.com/>

<http://reninparwil.com/zapoy/gate.php>

<http://leftthenhispar.ru/zapoy/gate.php>

<http://reptertinrom.ru/zapoy/gate.php>

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Number, Offset, Value:

The screenshot shows the CFF Explorer VII interface. The left pane displays the file structure, including headers, sections, and various utilities. The right pane shows the export table with the following data:

Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000
	00000032	Word	0000
	00000034	Word	0000
	00000036	Word	0000
	00000038	Word	0000

DLL: Wsock32.dll, kernel32.dll, urlmon.dll, Userenv.dll, ole32.dll, User32.dll, advapi32.dll, wininet.dll, shlwapi.dll

The screenshot shows the CFF Explorer VII interface. The left pane displays the file structure. The right pane shows the import table with the following data:

Module Name	Module Path
wsock32.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
kernel32.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
urlmon.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
Userenv.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
ole32.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
User32.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
advapi32.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
wininet.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e
shlwapi.dll	dc030778938b8b6f98236a709d0d18734c325acc44b12a55e

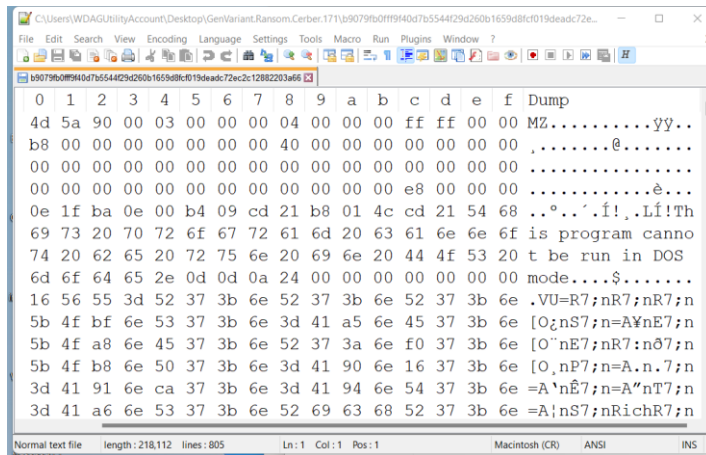
Packer Information:

Not packed

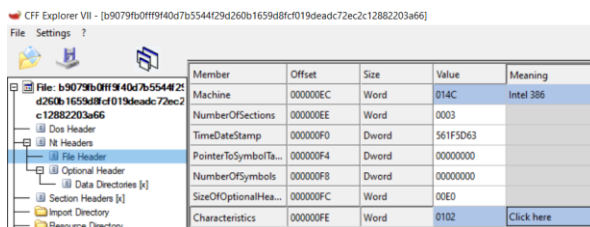
The screenshot shows the Exiftool interface. The file being analyzed is 'dc030778938b8b6f98236a709d0d18734c325acc44b12a55e'. The entry point is 00000312, and the entry section is .text. The file offset is 0000A712, and the first bytes are 55 8B EC 33 D5. The linker info is 2.50, and the subsystem is Windows GUI. The file size is 00011000h, and the overlay is NO_00000000. The DLL is 32-bit, library image, and the RES/OVL is 0/0%. The file is packed with UPX v3.95, and the packer info is 1999-2018. The file is packed with UPX v3.95, and the packer info is 1999-2018.

5. Gen:Variant.Ransom.Cerber.171

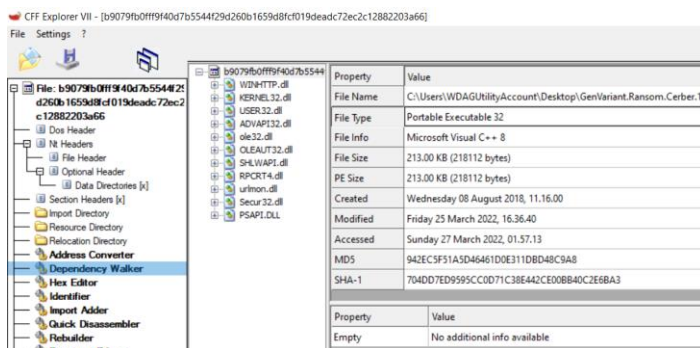
Magic Byte and File Signature: (4d 5a) (MZ) =>exe



Machine Information and Exe-Type: 32-bit microprocessor



File-Type: Portable Executable 32



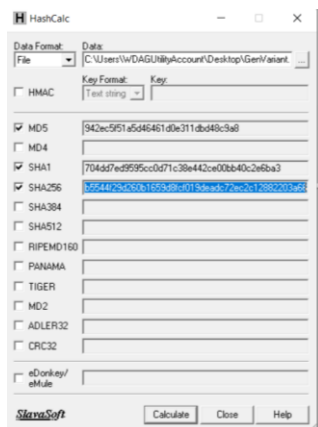
Finger Printing Information:

MD5: 942ec5f51a5d46461d0e311dbd48c9a8

SHA1: 704dd7ed9595cc0d71c38e442ce00bb40c2e6ba3

SHA256:

b9079fb0fff9f40d7b5544f29d260b1659d8fcf019deadc72ec2c12882203a66



Malicious String:

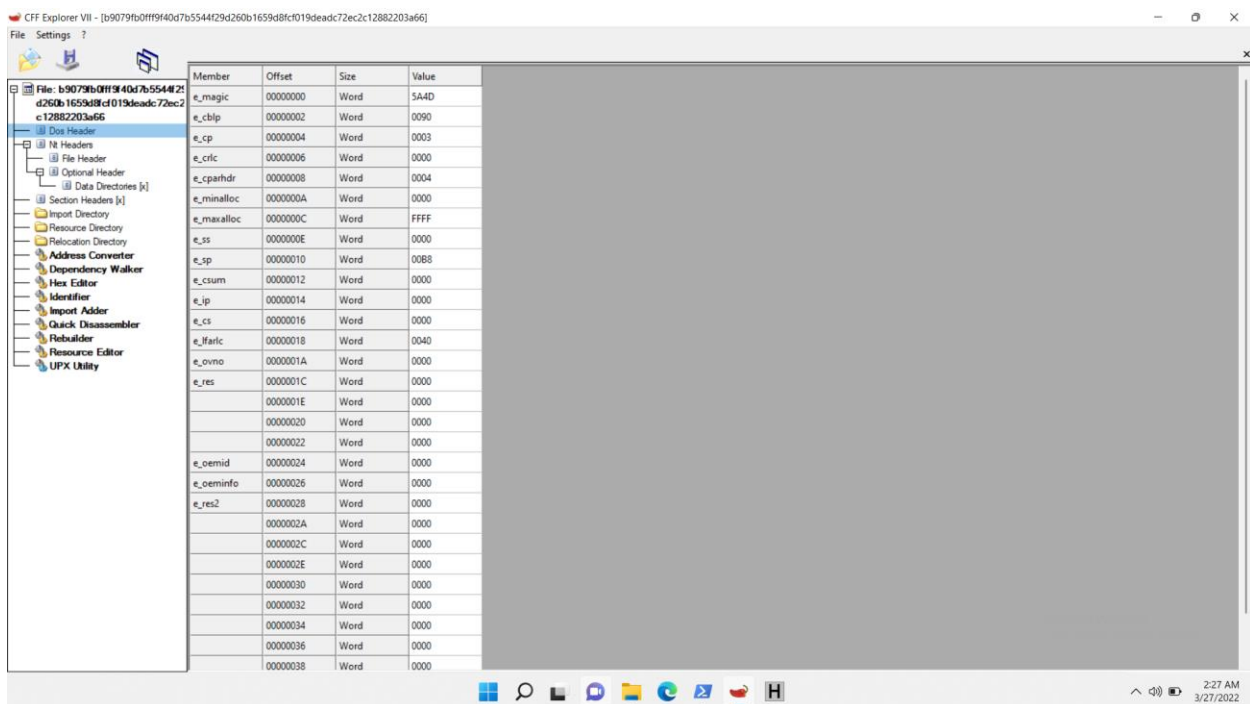
.?AV_Locimp@locale@std@@

.?AVlogic_error@std@@

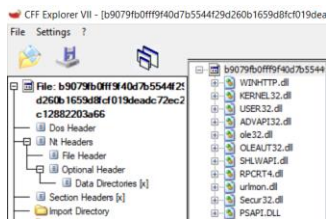
.?AVlength_error@std@@

.?AVout_of_range@std@@

Number, Offset, Value:

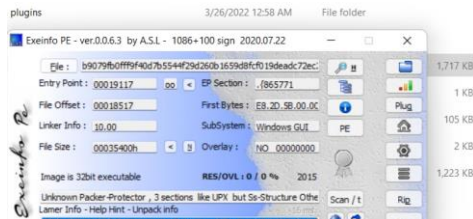


DLL: Winhttp.dll, Kernel32.dll, User32.dll, Advapi32.dll, ole32.dll, Oleaut32.dll, Shlwapi.dll, Rpcrt4.dll, Urlmon.dll, Secur32.dll, Psapi.dll



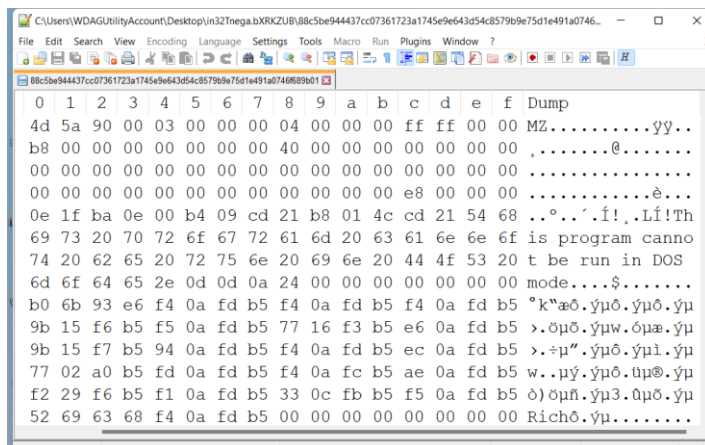
Packer Information:

{ 865771 , Click - [Scan / t] Button or try Detector - DIE v2.x <http://ntinfo.biz>

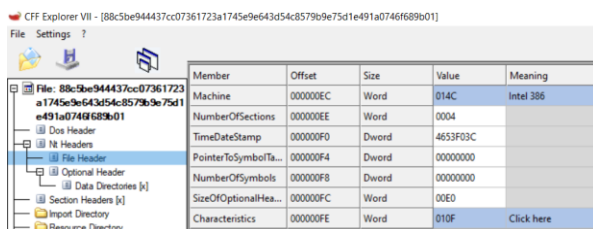


6. in32/Tnega.bXRKZUB

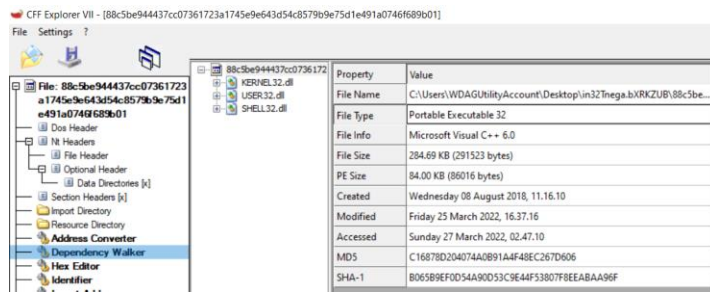
Magic Byte and File Signature: (4d 5a) (MZ) =>exe



Machine Information and Exe-Type: 32-bit microprocessor



File-Type: Portable Executable 32



Finger Printing Information:

MD5: c16878d204074a0b91a4f48ec267d606

SHA1: b065b9ef0d54a90d53c9e44f53807f8eeabaa96f

SHA256:

88c5be944437cc07361723a1745e9e643d54c8579b9e75d1e491a0746f689b01



Malicious String:

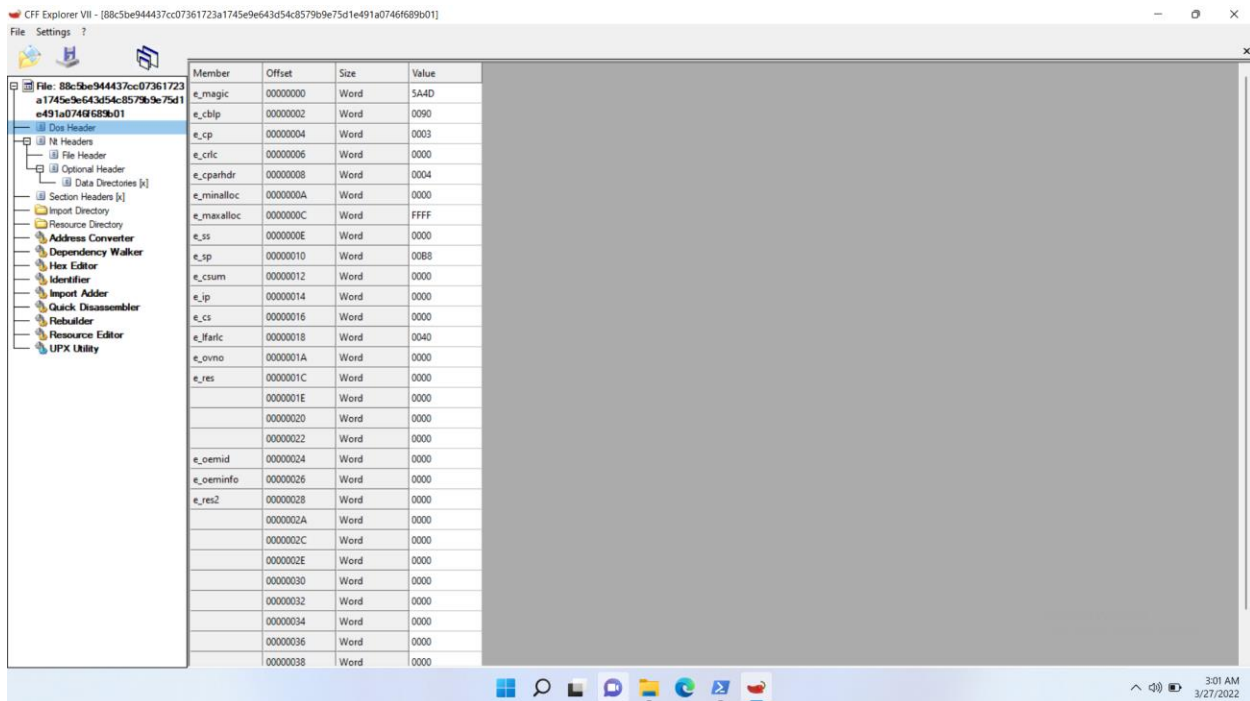
(null)

KERNEL32

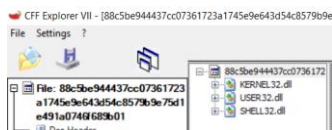
DestroyWindow

SendMessageA

Number, Offset, Value:



DLL: Kernel32.dll, User32.dll, Shell32.dll

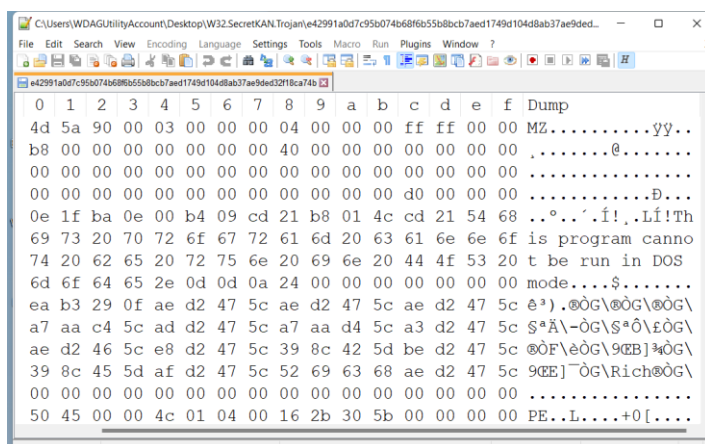


Packer Information:

Not packed

7. W32.SecretKAN.Trojan

Magic Byte and File Signature: (4d 5a) (MZ) =>exe



Machine Information and Exe-Type: 32-bit microprocessor

CFF Explorer VII - [e42991a0d7c95b074b68f6b55b8bcb7aed1749d104d8ab37ae9ded32f18ca74b]

File Settings ?

Member	Offset	Size	Value	Meaning
Machine	000000D4	Word	014C	Intel 386
NumberOfSections	000000D6	Word	0004	
TimeDateStamp	000000D8	Dword	5B302B16	
PointerToSymbolTa...	000000DC	Dword	00000000	
NumberOfSymbols	000000E0	Dword	00000000	
SizeOfOptionalHea...	000000E4	Word	00E0	
Characteristics	000000E6	Word	0102	Click here

File-Type: Portable Executable 32

CFF Explorer VII - [e42991a0d7c95b074b68f6b55b8bcb7aed1749d104d8ab37ae9ded32f18ca74b]

File Settings ?

Property	Value
File Name	C:\Users\WDA\UtilityAccount\Desktop\W32.SecretKAN.Trojan[e42991a0d7c95b074b68f6b55b8bcb7aed1749d104d8ab37ae9ded32f18ca74b]
File Type	Portable Executable 32
File Info	No match found.
File Size	870.00 KB (890880 bytes)
PE Size	870.00 KB (890880 bytes)
Created	Thursday 06 September 2018, 13.04.52
Modified	Friday 25 March 2022, 16.37.43
Accessed	Sunday 27 March 2022, 11.22.03
MD5	7b1596db20ee16d889d5f5b57736e387
SHA-1	E1E63B917D88A6C7D7E0CF97AB00C1B9A2C7417D

Finger Printing Information:

MD5: 7b1596db20ee16d889d5f5b57736e387

SHA1: e1e63b917d88a6c7d7e0cf97ab00c1b9a2c7417d

SHA256:

e42991a0d7c95b074b68f6b55b8bcb7aed1749d104d8ab37ae9ded32f18ca74b



Malicious String:

NtReadFile

NtWriteFile

NtReadVirtualMemory

NtQueryObject

NtQuerySystemInformation

NtQueryInformationFile

NtQueryInformationProcess

NtWow64ReadVirtualMemory64

baf5f61aad6bc18ed886

f23e1993dfdXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

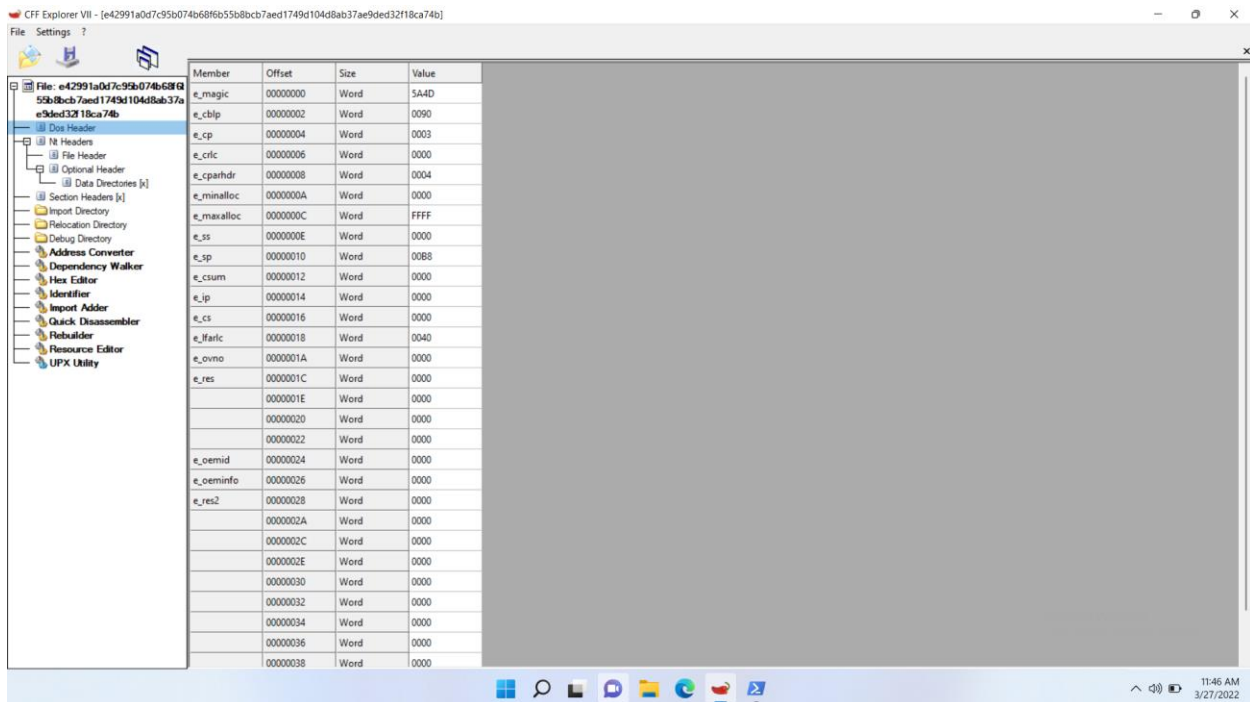
WrdJdgYRmg

XTALXXXXXX

update_url

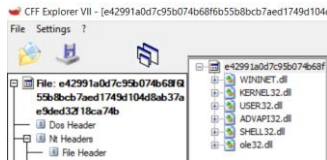
URL="file:///

Number, Offset, Value:



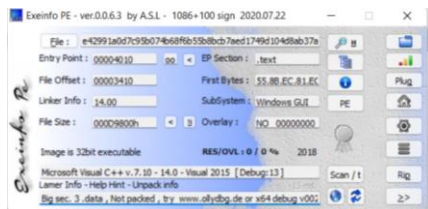
Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	0008
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000
	00000032	Word	0000
	00000034	Word	0000
	00000036	Word	0000
	00000038	Word	0000

DLL: Wininet.dll, Kernel32.dll, User32.dll, Advapi32.dll, Shell32.dll, ole32.dll



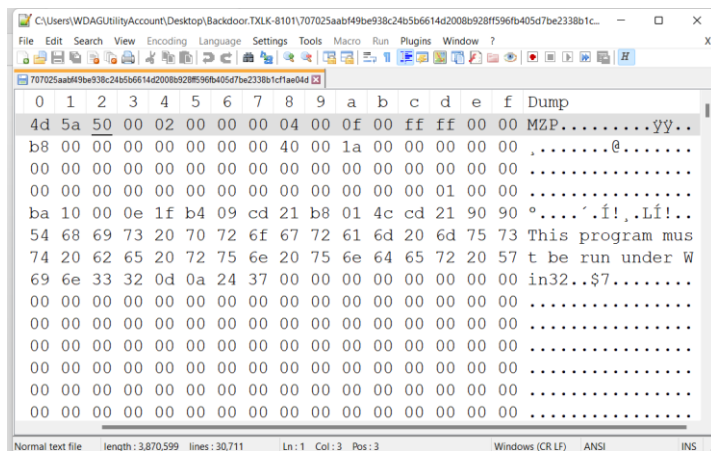
Packer Information:

Not packed

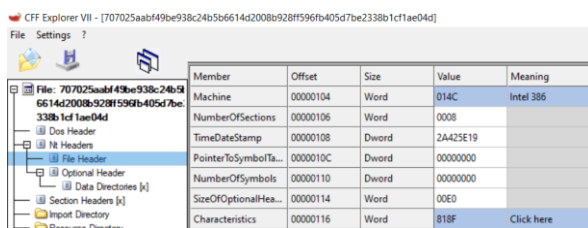


8. Backdoor.TXLK-8101

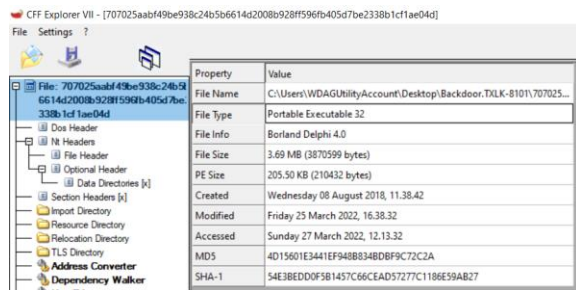
Magic Byte and File Signature: (4d 5a 50) (MZIP) => mountable zip file



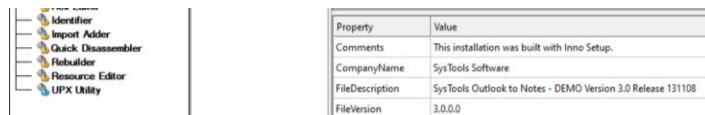
Machine Information and Exe-Type: 32-bit microprocessor



File-Type: Portable Executable 32



Extra Information: Original File Information



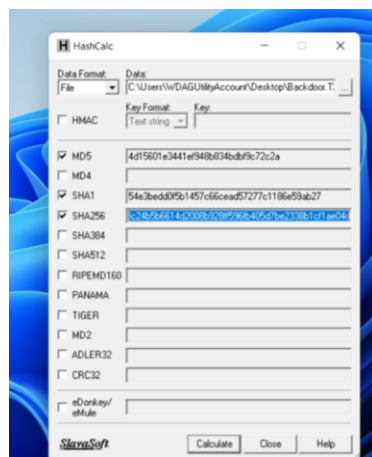
Finger Printing Information:

MD5: 4d15601e3441ef948b834bdf9c72c2a

SHA1: 54e3bedd0f5b1457c66cead57277c1186e59ab27

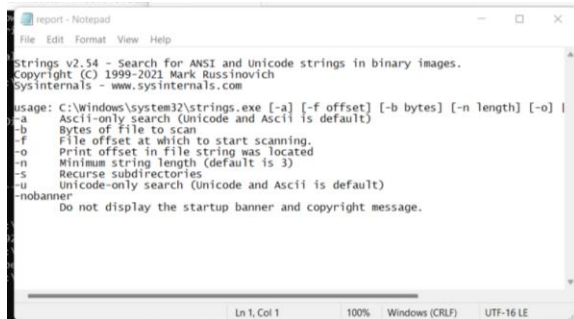
SHA256:

707025aabf49be938c24b5b6614d2008b928ff596fb405d7be2338b1cf1ae04d

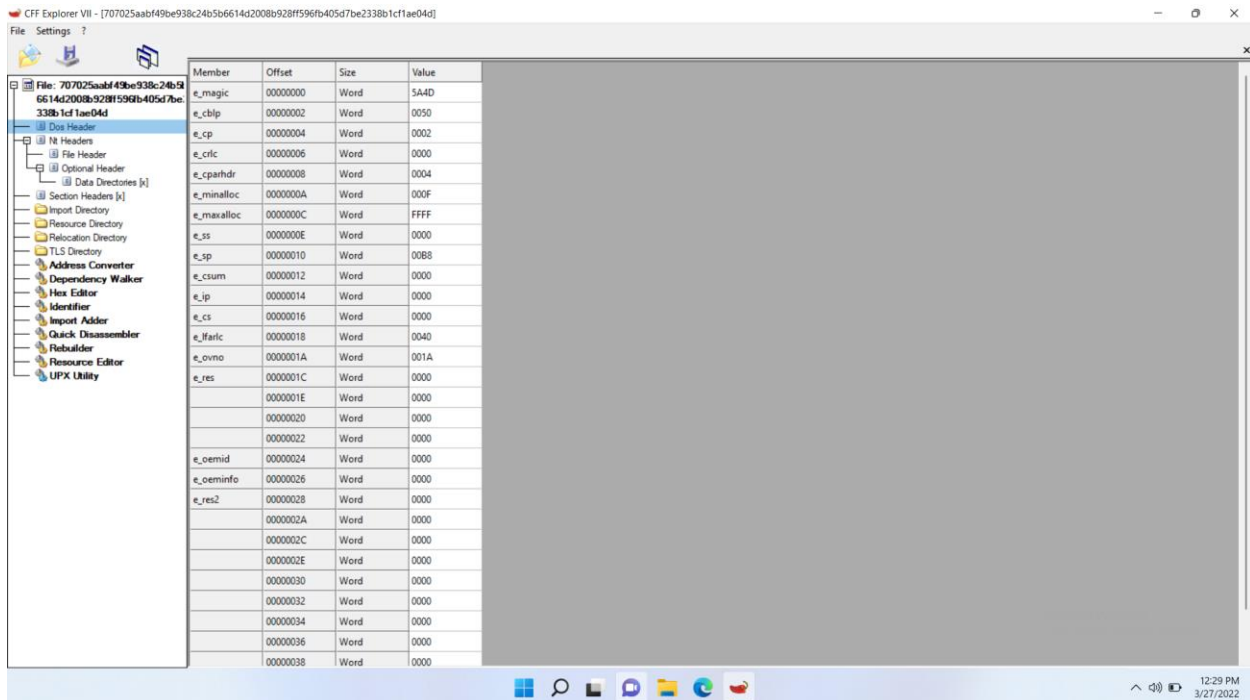


Malicious String:

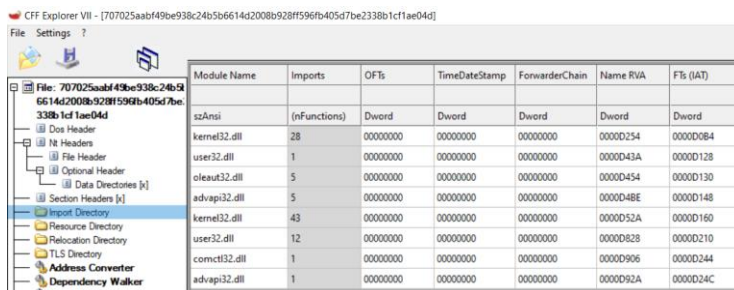
Nothing is display due to zip of file.



Number, Offset, Value:



DLL: kernel32.dll, user32.dll, oleaut32.dll, Advapi32.dll, comctl32.dll



Packer Information:

[WARN : Base Relock > 0000] - try InnoExtractor v5.3 GUI (2018) -
www.havyssoft.cl - or - Inno Setup Unpacker v0.49 ->

<http://innounp.sourceforge.net> or Total Commander + plugin - InstallExplorer Ver.0.9.1 or try Universal extractor - www.legroom.net/software/uniextract

Tools Used:

- CFF Explorer
- Notepad++
- Process Hacker
- Yara
- ExeInfo PE
- Hash Calc
- TriadNet