ANALISI MALWARE

Analisi malware del file allegato <<Esercizio_Pratico_U3_W2_L1>>.

Dopo un'analisi statica basilare del file allegato presente sulla macchina virtuale Windows 7 professional con il tool CFF,si determineranno per prima cosa le librerie importate,notando in primis che nelle import directory viene specificato un numero inusuale di librerie KERNEL32.DLL(manipolazione file,gestione memoria),dunque spostandoci di seguito nella Section Headers analizzeremo con maggiore precisione le sezioni di cui si compone il malware.
Il malware e' composto da varie richieste di librerie:KERNEL32.dll,ADVAPI32.dll(funzioni per interagire con servizi e registri sistemi operativi),MSVCRT.dll(manipolazione stringhe,allocazione memoria e altro come chiamate input/output come nel linguaggio di programmazione C) ed WININET.dll(funzioni per l'implementazione di alcuni protocolli di rete "HTTP,FTP,NTP"),tra l'altro figurano le funzioni <<LoadLibrary e GetProcAddress>> come figurano anche <<CreateService A,exit,Internet OpenA.
Date le informazioni ottenute con l'analisi effettuata con CFF possiamo dedurre che si tratti di una DLL injection.

Courses

learn.epicode.com/course/79/curricu

Gmail YouTube Word | Microsoft 365 Free Online PDF

Cybersecurity Specialist

Teoria S10/L1

EPICODE

Esempio pratico: Una volta che siamo nella stessa cartella del file eseguibile, possiamo lanciare il comando.
La sintassi per usare md5deep è:

md5deep «percorso del file per il quale vogliamo l'hash»

A titolo di esempio (l'esempio è su XP ma su Windows 7 è i
desktop chiamato **testmd5deep.txt**.
Per calcolare l'hash del file eseguiremo il comando md5dee
questo caso è sul Desktop.

Il risultato del comando, come vedete, è una stringa alfanun
quale è stato calcolato l'hash.

Windows 7 - malware analysis [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

C:\Windows\system32\cmd.exe

```
17/01/2024  12:12    <DIR>          .
17/01/2024  12:12    <DIR>          ..
17/01/2024  12:12            17.715 CHANGES.txt
17/01/2024  12:12            19.422 COPYING.txt
17/01/2024  12:12             2.261 FILEFORMAT.txt
17/01/2024  12:12           800.256 hashdeep.exe
17/01/2024  12:12            12.291 HASHDEEP.txt
17/01/2024  12:12           988.160 hashdeep64.exe
17/01/2024  12:12           800.256 md5deep.exe
17/01/2024  12:12            14.717 MD5DEEP.txt
17/01/2024  12:12           988.160 md5deep64.exe
17/01/2024  12:12           800.256 sha1deep.exe
17/01/2024  12:12           988.160 sha1deep64.exe
17/01/2024  12:12           800.256 sha256deep.exe
17/01/2024  12:12           988.160 sha256deep64.exe
17/01/2024  12:12           800.256 tigerdeep.exe
17/01/2024  12:12           988.160 tigerdeep64.exe
17/01/2024  12:12           800.256 whirlpooldeep.exe
17/01/2024  12:12           988.160 whirlpooldeep64.exe
              17 File     10.796.902 byte
               2 Directory  22.705.106.944 byte disponibili

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\hashdeep64
.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
C:\Users\user\Desktop\Software: No such file or directory
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\Malware:
 No such file or directory
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\analysis
\md5deep-4.3\md5deep-4.3\hashdeep64.exe: No such file or directory

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
sha256deep.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
2303ea535203c79305490d6c20be8454  C:\Users\user\Desktop\Software Malware analysi
s\md5deep-4.3\md5deep-4.3\sha256deep.exe

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>
```

Cerca md5...

Dimensione

782 KB
965 KB
782 KB
965 KB
782 KB
965 KB

Windows 7
Build 7601
ndows non è autentica

IT 15:51 25/03/2024

Right Ctrl

18°C Mostly cloudy

Search

ENG GA 15:51 25/03/2024

Courses

learn.epicode.com/course/79/curricu

Gmail YouTube Word | Microsoft 365 Free Online PDF

Cybersecurity Specialist

Teoria S10/L1

EPICODE

Esempio pratico: Una volta che siamo nella stessa cartella del file eseguibile, possiamo lanciare il comando.
La sintassi per usare md5deep è:

md5deep «percorso del file per il quale vogliamo l'hash»

A titolo di esempio (l'esempio è su XP ma su Windows 7 è i
desktop chiamato **testmd5deep.txt**.
Per calcolare l'hash del file eseguiremo il comando md5dee
questo caso è sul Desktop.

Il risultato del comando, come vedete, è una stringa alfanun
quale è stato calcolato l'hash.

Windows 7 - malware analysis [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

C:\Windows\system32\cmd.exe

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\hashdeep64
.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
C:\Users\user\Desktop\Software: No such file or directory
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\Malware:
 No such file or directory
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\analysis
\md5deep-4.3\md5deep-4.3\hashdeep64.exe: No such file or directory

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
sha256deep.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
2303ea535203c79305490d6c20be8454  C:\Users\user\Desktop\Software Malware analysi
s\md5deep-4.3\md5deep-4.3\sha256deep.exe

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
hashdeep64.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
665ccc57a84e5639c4e5151686cc0432  C:\Users\user\Desktop\Software Malware analysi
s\md5deep-4.3\md5deep-4.3\hashdeep64.exe

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
sha1deep.exe
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
2303ea535203c79305490d6c20be8454  C:\Users\user\Desktop\Software Malware analysi
s\md5deep-4.3\md5deep-4.3\sha1deep.exe

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep
MD5DEEP.text
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3\MD5DEEP.
text: No such file or directory

C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>_
```

Cerca md5...

Dimensione

782 KB
965 KB
782 KB
965 KB
782 KB
965 KB

Windows 7
Build 7601
ndows non è autentica

IT 15:54 25/03/2024

Right Ctrl

18°C Mostly cloudy

Search

ENG GA 15:54 25/03/2024

Courses

learn.epicode.com/course/79/curriculum/32046

Gmail YouTube Word | Microsoft 365 Free Online PDF Cre... All Bookmarks

Cybersecurity Specialist

Teoria S10/L1

EPICODE

Cyber Security & Ethical Hacking

Analisi statica basica

Strings

Gli eseguibili contengono molto spesso delle stringhe al loro interno, ad esempio utilizzate per scrivere a schermo un messaggio di benvenuto, o dettagliare l'utilizzo di un software o per connettersi ad un dato URL online.

Nel caso di software dannosi, si potrebbero recuperare importanti informazioni dalle stringhe contenute all'interno degli eseguibili. A tal proposito, l'utility da riga di comando **«strings»** permette di trovare tutte le stringhe utilizzate all'interno di un file eseguibile.

N.B. : «strings» è all'interno della cartella «Sysinternals Suite» sul Desktop della macchina virtuale. Essendo uno strumento da riga di comando, valgono le regole viste in precedenza.

La sintassi di string è: **strings «file_eseguibile»**

Link dell'intera suite: https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

21

Windows 7 - malware analysis [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Computer

C:\Windows\system32\cmd.exe

```
;cO$
n5'
u[H
c~J,
hna
9iCY
0y1
US1
Washington1
Redmond1
Microsoft Corporation1#0!
Microsoft Timestamping PCA
110222222116Z0#
kT6P
Fm3
&Pztc
=`ib
R1 u<
_zv
zrN
dn[
<W$
;6"
```

Mozilla Firefox

Windows 7
Build 7601
Questa copia di Windows non è autentica

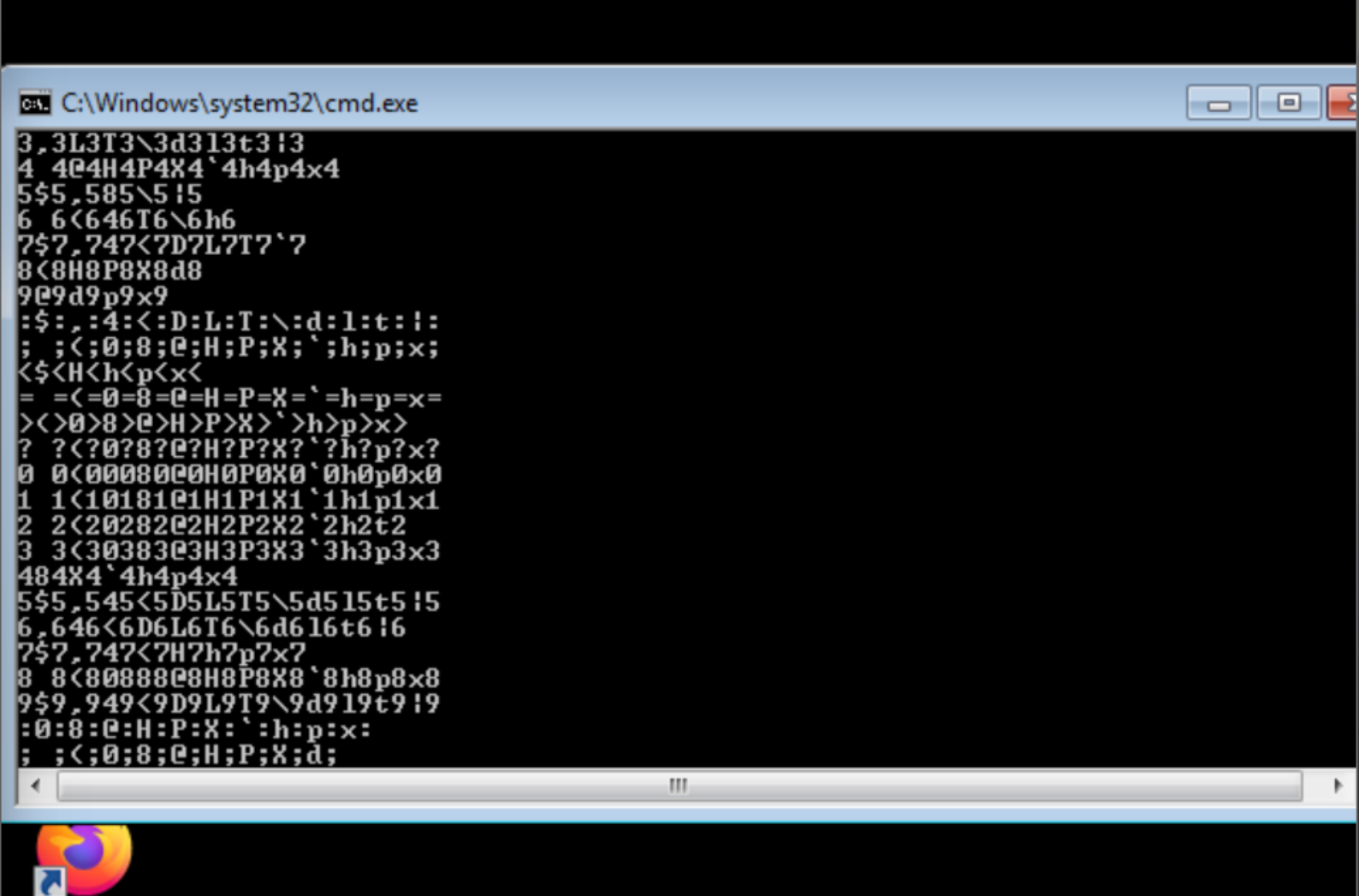
IT 16:07 25/03/2024

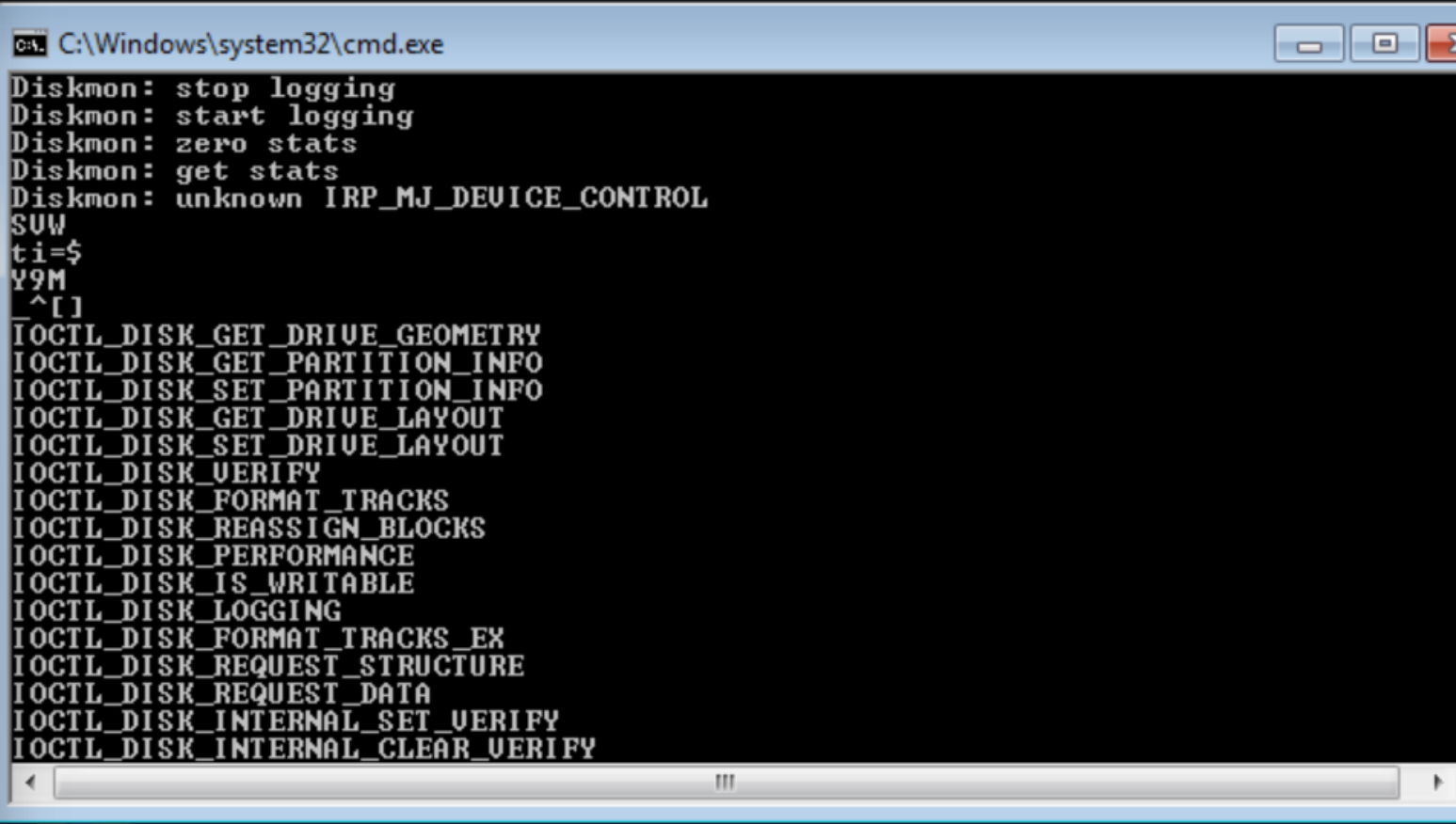
Right Ctrl

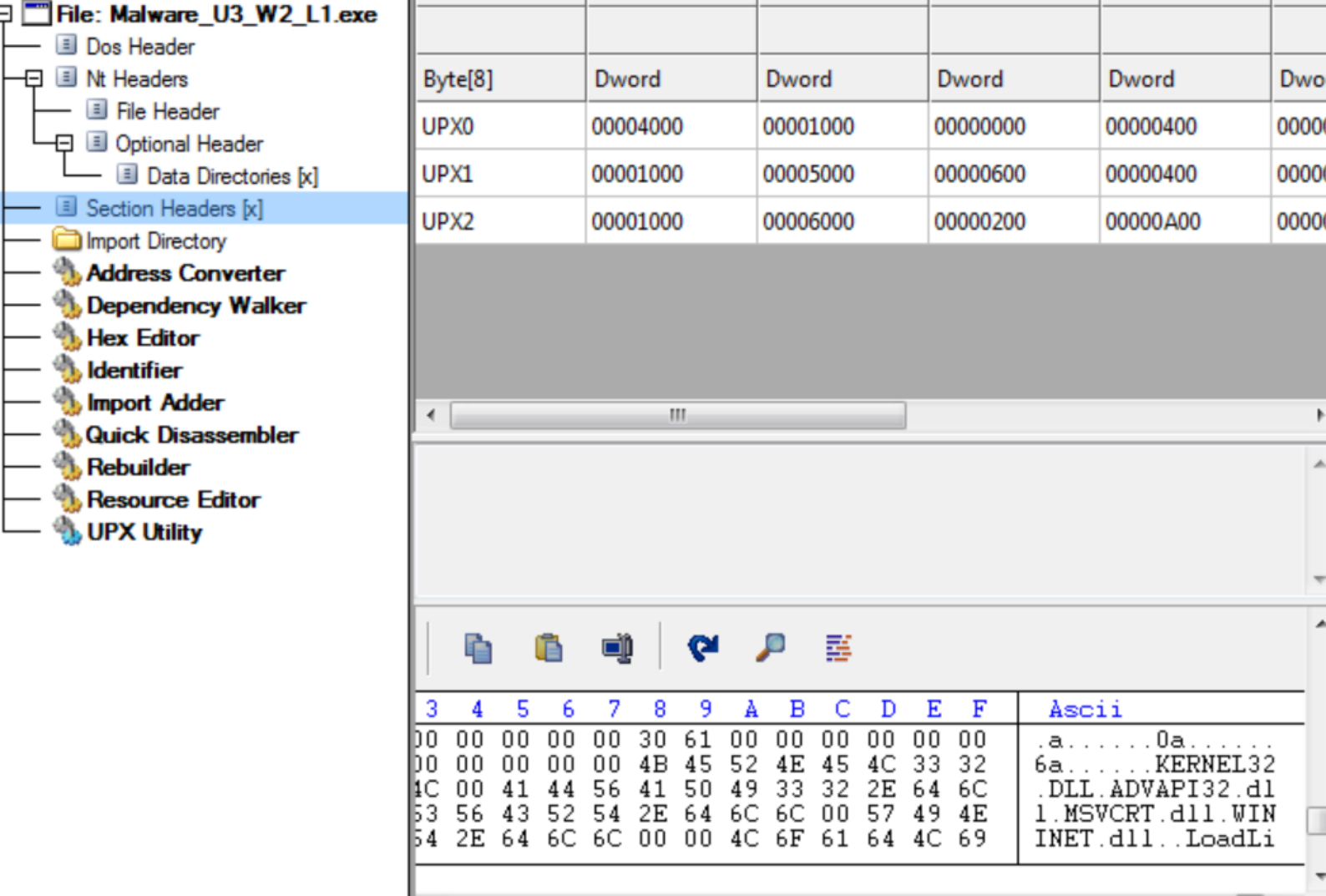
17°C Mostly cloudy

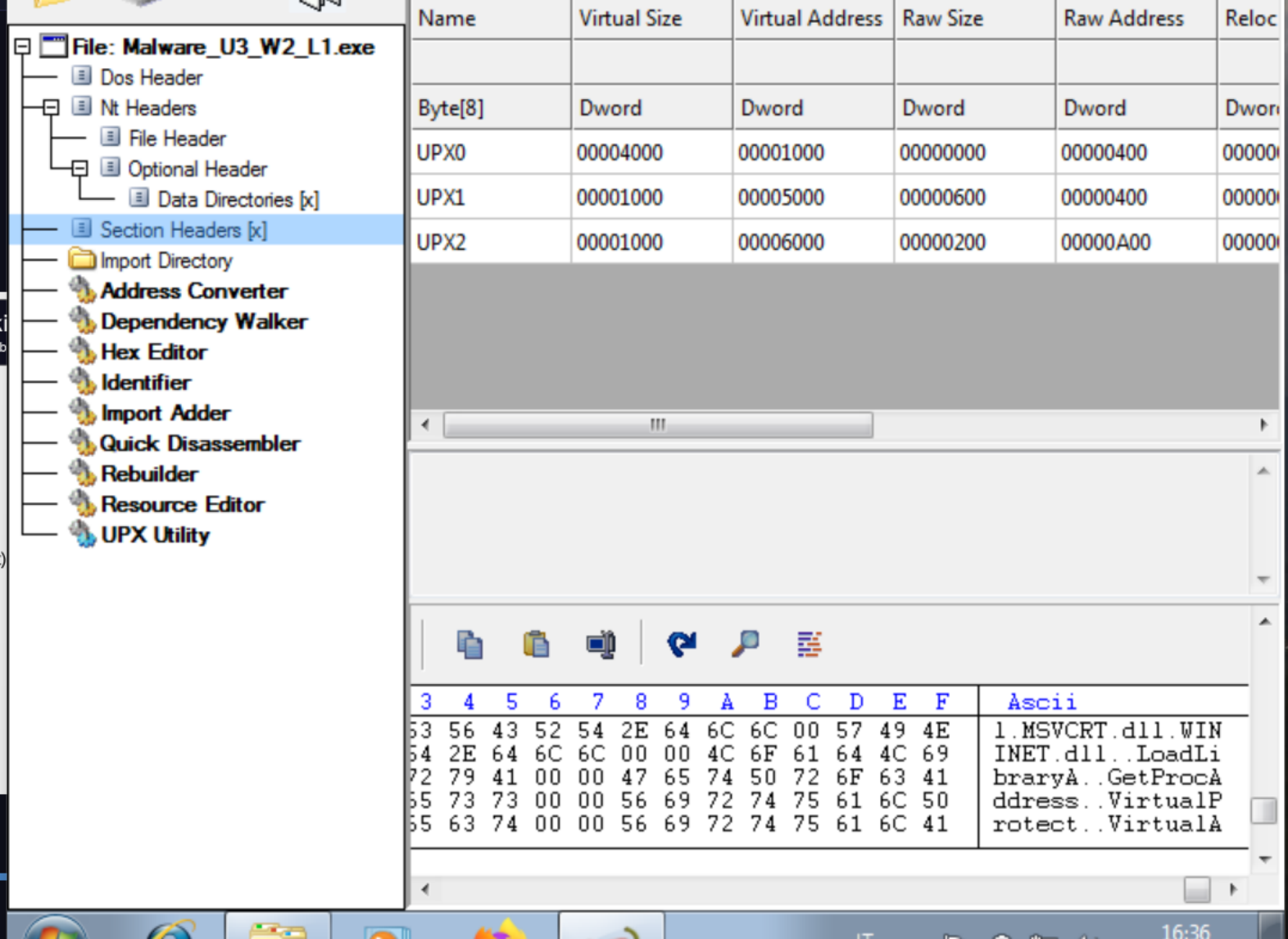
Search

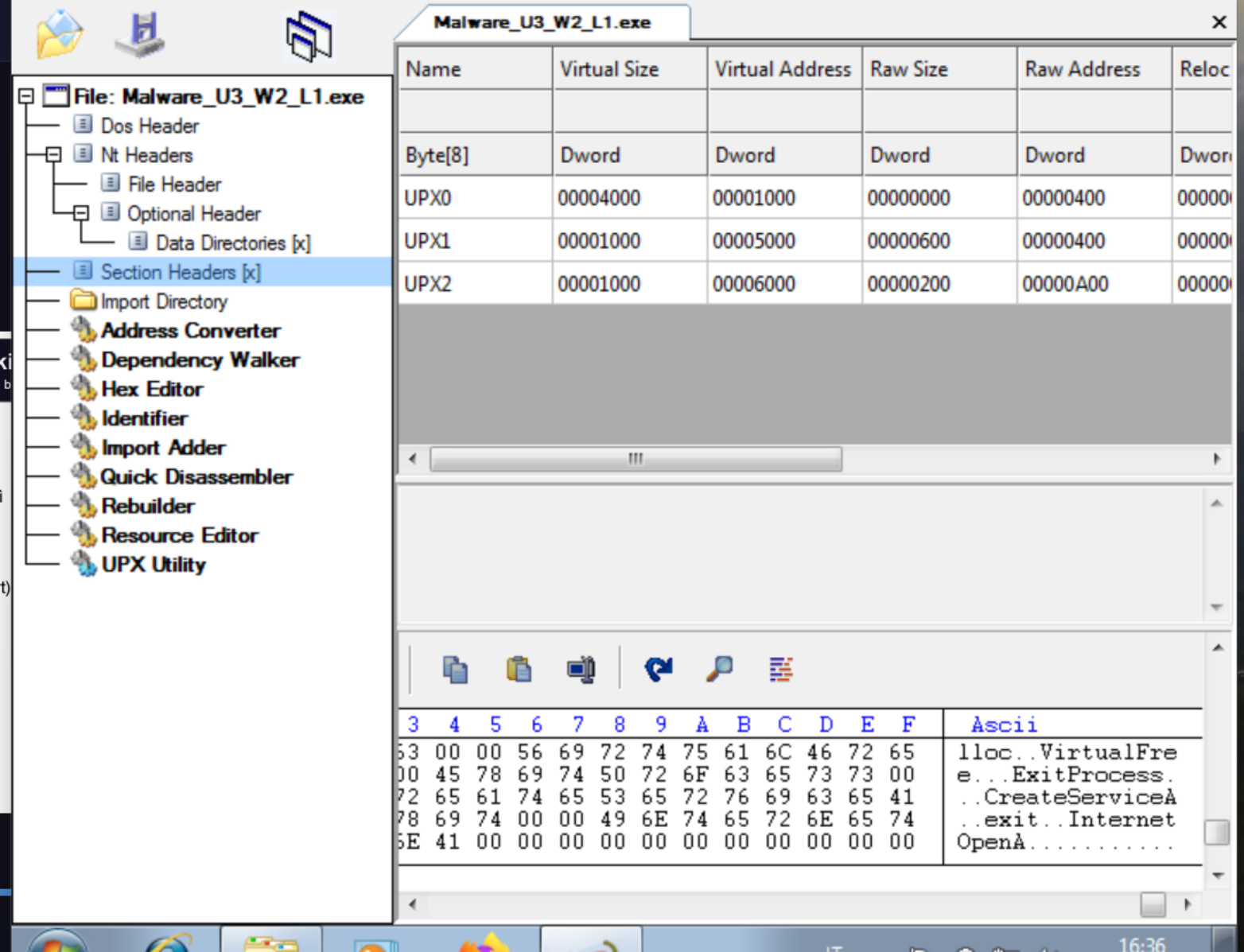
ENG GA 16:07 25/03/2024


C:\Windows\system32\cmd.exe
3,3L3T3\3d3l3t3!3
4 4@4H4P4X4`4h4p4x4
5$5,585\5!5
6 6<646T6\6h6
7$7,747<7D7L7T7`7
8<8H8P8X8d8
9@9d9p9x9
:$:,:4:<:D:L:T:\:d:l:t:!:
; ;<;0;8;@;H;P;X;`;h;p;x;
<$<H<h<p<x<
= =<=0=8=@=H=P=X=`=h=p=x=
><>0>8>@>H>P>X>`>h>p>x>
? ?<?0?8?@?H?P?X?`?h?p?x?
0 0<00080@0H0P0X0`0h0p0x0
1 1<10181@1H1P1X1`1h1p1x1
2 2<20282@2H2P2X2`2h2t2
3 3<30383@3H3P3X3`3h3p3x3
484X4`4h4p4x4
5$5,545<5D5L5T5\5d5l5t5!5
6,646<6D6L6T6\6d6l6t6!6
7$7,747<7H7h7p7x7
8 8<80888@8H8P8X8`8h8p8x8
9$9,949<9D9L9T9\9d9l9t9!9
:0:8:@:H:P:X:`:h:p:x:
; ;<;0;8;@;H;P;X;d;


C:\Windows\system32\cmd.exe
Diskmon: stop logging
Diskmon: start logging
Diskmon: zero stats
Diskmon: get stats
Diskmon: unknown IRP_MJ_DEVICE_CONTROL
SUW
ti=$
Y9M
_^[]
IOCTL_DISK_GET_DRIVE_GEOMETRY
IOCTL_DISK_GET_PARTITION_INFO
IOCTL_DISK_SET_PARTITION_INFO
IOCTL_DISK_GET_DRIVE_LAYOUT
IOCTL_DISK_SET_DRIVE_LAYOUT
IOCTL_DISK_VERIFY
IOCTL_DISK_FORMAT_TRACKS
IOCTL_DISK_REASSIGN_BLOCKS
IOCTL_DISK_PERFORMANCE
IOCTL_DISK_IS_WRITABLE
IOCTL_DISK_LOGGING
IOCTL_DISK_FORMAT_TRACKS_EX
IOCTL_DISK_REQUEST_STRUCTURE
IOCTL_DISK_REQUEST_DATA
IOCTL_DISK_INTERNAL_SET_VERIFY
IOCTL_DISK_INTERNAL_CLEAR_VERIFY


File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Byte[8] Dword Dword Dword Dword Dwo
UPX0 00004000 00001000 00000000 00000400 0000
UPX1 00001000 00005000 00000600 00000400 0000
UPX2 00001000 00006000 00000200 00000A00 0000
3 4 5 6 7 8 9 A B C D E F Ascii
00 00 00 00 00 30 61 00 00 00 00 00 00 .a.....0a.....
00 00 00 00 00 4B 45 52 4E 45 4C 33 32 6a.....KERNEL32
4C 00 41 44 56 41 50 49 33 32 2E 64 6C .DLL.ADVAPI32.dl
53 56 43 52 54 2E 64 6C 6C 00 57 49 4E l.MSVCRT.dll.WIN
54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69 INET.dll..LoadLi


File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Name
Virtual Size
Virtual Address
Raw Size
Raw Address
Reloc
Byte[8]
Dword
Dword
Dword
Dword
Dwor
UPX0
00004000
00001000
00000000
00000400
00000
UPX1
00001000
00005000
00000600
00000400
00000
UPX2
00001000
00006000
00000200
00000A00
00000
3 4 5 6 7 8 9 A B C D E F
Ascii
53 56 43 52 54 2E 64 6C 6C 00 57 49 4E
l.MSVCRT.dll.WIN
54 2E 64 6C 6C 00 00 4C 6F 61 64 4C 69
INET.dll..LoadLi
72 79 41 00 00 47 65 74 50 72 6F 63 41
braryA..GetProcA
65 73 73 00 00 56 69 72 74 75 61 6C 50
ddress..VirtualP
65 63 74 00 00 56 69 72 74 75 61 6C 41
rotect..VirtualA


Malware_U3_W2_L1.exe
File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Name
Virtual Size
Virtual Address
Raw Size
Raw Address
Reloc
Byte[8]
Dword
Dword
Dword
Dword
Dwor
UPX0
00004000
00001000
00000000
00000400
00000
UPX1
00001000
00005000
00000600
00000400
00000
UPX2
00001000
00006000
00000200
00000A00
00000
3 4 5 6 7 8 9 A B C D E F
Ascii
53 00 00 56 69 72 74 75 61 6C 46 72 65
lloc..VirtualFre
00 45 78 69 74 50 72 6F 63 65 73 73 00
e...ExitProcess.
72 65 61 74 65 53 65 72 76 69 63 65 41
..CreateServiceA
78 69 74 00 00 49 6E 74 65 72 6E 65 74
..exit..Internet
6E 41 00 00 00 00 00 00 00 00 00 00 00
OpenA.....
16:36

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChai
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000
ADVAPI32.dll	1	00000000	00000000	00000000
MSVCRT.dll	1	00000000	00000000	00000000
WININET.dll	1	00000000	00000000	00000000