

Analisi Statica Basica

Obiettivo: Eseguire un'analisi statica basica di un Malware su macchina Windows XP 32 bit.

1) Avvio CMD e Analisi Superficiale Virus

```
CA Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop\md5deep-4.3

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>dir
Volume in drive C has no label.
Volume Serial Number is D8BA-8021

Directory of C:\Documents and Settings\Administrator\Desktop\md5deep-4.3

08/16/2022 03:37 PM <DIR> .
08/16/2022 03:37 PM <DIR> ..
10/24/2012 02:33 AM          17,715 CHANGES.txt
10/24/2012 02:33 AM          19,422 COPYING.txt
10/24/2012 02:33 AM           2,261 FILEFORMAT.txt
10/24/2012 02:33 AM         800,256 hashdeep.exe
10/24/2012 02:33 AM         12,291 HASHDEEP.txt
10/24/2012 02:33 AM         988,160 hashdeep64.exe
10/24/2012 02:33 AM         800,256 md5deep.exe
10/24/2012 02:33 AM         14,717 MD5DEEP.txt
10/24/2012 02:33 AM         988,160 md5deep64.exe
10/24/2012 02:33 AM         800,256 sha1deep.exe
10/24/2012 02:33 AM         988,160 sha1deep64.exe
10/24/2012 02:33 AM         800,256 sha256deep.exe
10/24/2012 02:33 AM         988,160 sha256deep64.exe
10/24/2012 02:33 AM         800,256 tigerdeep.exe
10/24/2012 02:33 AM         988,160 tigerdeep64.exe
10/24/2012 02:33 AM         800,256 whirlpooldeep.exe
10/24/2012 02:33 AM         988,160 whirlpooldeep64.exe
               17 File(s)      10,796,902 bytes
                2 Dir(s)      56,932,188,160 bytes free

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

Per cominciare ho avviato il **Command Prompt** su **Windows 7** per iniziare ad analizzare il **Malware** richiesto. Ho analizzato per prima cosa l'hash con **md5deep**.

```
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "c:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
8363436878404da0ae3e46991e355b83  c:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

Per ottenere ulteriori informazioni ho caricato l'hash sul sito **VirusTotal**

55 security vendors and 1 sandbox flagged this file as malicious

c876a332d7d08da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a4864a6
Lab01-02.exe

Size: 3.00 KB | Last Analysis Date: 4 days ago

peexe checks-disk-space via-tor detect-debug-environment idle long-sleeps upx checks-use-input

Community Score: 55/70

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.ulise/trojanclicker | Threat categories: trojan downloader | Family labels: ulise trojanclicker r902c0b020

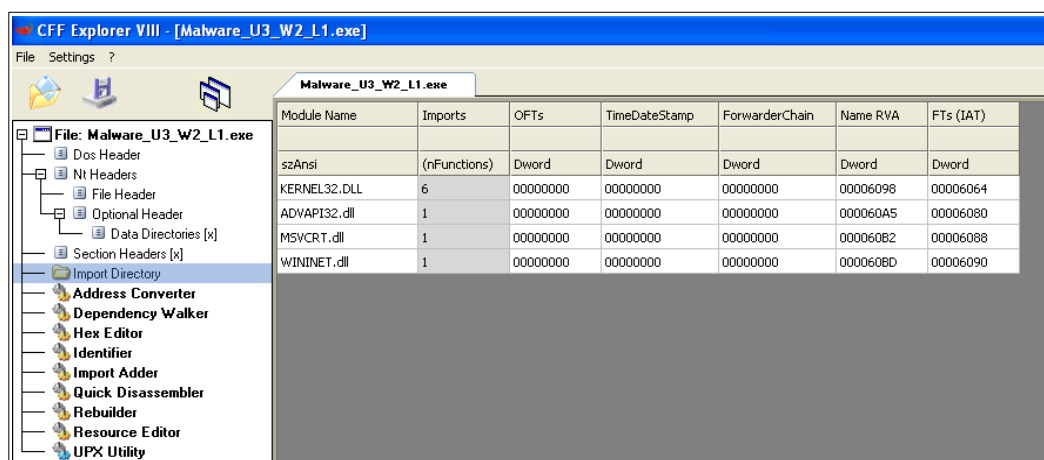
Security vendors' analysis

| Security vendor | Detection | Security vendor | Detection |
|------------------|-------------------------------|--------------------|--------------------------------------|
| AhnLab-V3 | Trojan/Win32.StartPage.C26214 | Alibaba | TrojanClicker.Win32/Generic.1ba1980f |
| ALYac | Trojan.Startpage.3072 | Antiy-AVL | Trojan/Win32.SGeneric |
| Arcabit | Trojan.Ser.Ulisse.216 | Avast | Win32/Malware-gen |
| AVG | Win32/Malware-gen | Avira (no cloud) | TR/Downloader.Gen |
| Baidu | Win32.Trojan-Clicker.Agent.ad | BitDefender | Gen.Variant.Ser.Ulisse.216 |
| BitDefenderTheta | Gen.NN.Zexaf.36270.amGtaW067f | Bkav Pro | W32.AIDetect/Malware |
| ClamAV | Win/Malware.Agent-6350563-0 | CrowdStrike Falcon | Win/malicious_confidence_100% (W) |
| Cybereason | Malicious.878404 | Cylance | Unsafe |

dove 55/70 Antivirus lo segnalano come Malevolo, principalmente come **trojan**.

2) CFF Explore

Utilizzando questo tool possiamo controllare le funzioni esportate ed importate dal Malware. Aprendo semplicemente il file e andando nella sezione *Import Directory* vengono mostrate le *Funzioni Importate*.



Le **Librerie** trovate con rispettive funzioni richieste sono:

- **KERNEL32**: una libreria comune che contiene le funzioni principali per interagire con il sistema operativo.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|----------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000219E | 0000 | SystemTimeToFileTime |
| N/A | 000021B4 | 0000 | GetModuleFileNameA |
| N/A | 000021C8 | 0000 | CreateWaitableTimerA |
| N/A | 000021DE | 0000 | ExitProcess |
| N/A | 000021EC | 0000 | OpenMutexA |
| N/A | 000021F8 | 0000 | SetWaitableTimer |
| N/A | 0000220A | 0000 | WaitForSingleObject |
| N/A | 00002220 | 0000 | CreateMutexA |
| N/A | 0000222E | 0000 | CreateThread |

- **ADVAPI32**: libreria per interagire con i servizi ed i registri del sistema operativo Microsoft.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|-----------------------------|
| Dword | Dword | Word | szAnsi |
| N/A | 0000223C | 0000 | CreateServiceA |
| N/A | 0000224C | 0000 | StartServiceCtrlDispatcherA |
| N/A | 0000226A | 0000 | OpenSCManagerA |

- **MSVCRT**: libreria che contiene le funzioni per la manipolazione di stringhe, l'allocazione di memoria e chiamate per input/output.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|------------------|
| | | | |
| Dword | Dword | Word | szAnsi |
| N/A | 0000227A | 0000 | _exit |
| N/A | 00002282 | 0000 | _XcptFilter |
| N/A | 00002290 | 0000 | exit |
| N/A | 00002296 | 0000 | __p__initenv |
| N/A | 000022A6 | 0000 | __getmainargs |
| N/A | 000022B6 | 0000 | _initterm |
| N/A | 000022C2 | 0000 | __setusermatherr |
| N/A | 000022D4 | 0000 | _adjust_fdiv |
| N/A | 000022E2 | 0000 | __p__commode |
| N/A | 000022F0 | 0000 | __p__fmode |
| N/A | 000022FC | 0000 | __set_app_type |
| N/A | 0000230C | 0000 | _except_handler3 |
| N/A | 0000231E | 0000 | _controlfp |

- **WININET**: questa libreria contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP ed NTP.

| OFTs | FTs (IAT) | Hint | Name |
|-------|-----------|------|------------------|
| | | | |
| Dword | Dword | Word | szAnsi |
| N/A | 0000232A | 0000 | InternetOpenUrlA |
| N/A | 0000233C | 0000 | InternetOpenA |

Alcune funzioni sono risultate visibili solo dopo aver decompresso con **UPX Utility** il codice del **Malware**. Questa procedura di crittografia è utilizzata dai creatori di Malware per renderli meno individuabili agli occhi degli antivirus.

3) Sezioni del Malware

Con **CFF Explorer** è possibile analizzare anche le *Sezioni* che compongono il Malware analizzato, più precisamente in **Section Headers**. Se controlliamo questa parte prima di decomprimere con **UPX Utility** non verranno mostrati i nomi delle sezioni ma la dicitura **UPX**.

| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations ... | Linenumber... | Characteristics |
|---------|--------------|-----------------|----------|-------------|---------------|-------------|-----------------|---------------|-----------------|
| | | | | | | | | | |
| Byte[8] | Dword | Dword | Dword | Dword | Dword | Dword | Word | Word | Dword |
| UPX0 | 00004000 | 00001000 | 00000000 | 00000400 | 00000000 | 00000000 | 0000 | 0000 | E0000080 |
| UPX1 | 00001000 | 00005000 | 00000600 | 00000400 | 00000000 | 00000000 | 0000 | 0000 | E0000040 |
| UPX2 | 00001000 | 00006000 | 00000200 | 00000A00 | 00000000 | 00000000 | 0000 | 0000 | C0000040 |

Perciò utilizziamo l'Utility del nostro programma

| Name | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations ... | Linenumber... | Characteristics |
|----------|--------------|-----------------|----------|-------------|---------------|-------------|-----------------|---------------|-----------------|
| 00000228 | 00000230 | 00000234 | 00000238 | 0000023C | 00000240 | 00000244 | 00000248 | 0000024A | 0000024C |
| Byte[8] | Dword | Dword | Dword | Dword | Dword | Dword | Word | Word | Dword |
| .text | 000002DC | 00001000 | 00001000 | 00001000 | 00000000 | 00000000 | 0000 | 0000 | 60000020 |
| .rdata | 00000372 | 00002000 | 00001000 | 00002000 | 00000000 | 00000000 | 0000 | 0000 | 40000040 |
| .data | 0000008C | 00003000 | 00001000 | 00003000 | 00000000 | 00000000 | 0000 | 0000 | C0000040 |

- **text**: contiene istruzioni che la CPU eseguirà una volta che il software sarà avviato.
- **rdata**: include informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.
- **data**: questa sezione contiene i dati e variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

La traccia dell'esercizio chiede di ipotizzare cosa questo **Malware** faccia. Analizzando le sezioni **rdata** e **data** ho notato che nella prima alcune stringhe dove accenna ad un **mutex**, un processo di sincronizzazione che impedisce che task paralleli accedano contemporaneamente ai dati di memoria.

| |
|---------------------|
| Ascii |
| WaitableTimerA... |
| ExitProcess...Op |
| ntMutexA...SetWai |
| tableTimer...Wait |
| ForSingleObject... |
| CreateMutexA... |
| CreateThread...Cr |
| createServiceA...St |
| artServiceCtrlDi |
| spatcherA...Open |
| SCManagerA...exi |
| t..._XcptFilter... |
| ..._exit..._p...in |
| itenv..._getmai |
| nargs..._initter |
| m..._setusermat |
| herr..._adjust_fd |
| iv..._p...commode |
| ..._p...fmode... |

```

Ascii
eateServiceA...St
artServiceCtrlDi
spatcherA...Open
SCManagerA...exi
t...XcptFilter.
...exit..._p_in
itenv...__getmai
nargs..._initter
m...__setusermat
herr...__adjust_fd
iv..._p_commode
..._p_fmode...
set_app_type..._e
xcent_handler3
_controlfp...Inte
rnetOpenUrlA...In
ternetOpenA.....
.....

```

In secondo luogo ho anche notato la presenza di un **Internet Open URL** che collegato con il link trovato nella sezione data (figura in basso) mi fa pensare che probabilmente questo Malware porti ad creare una connessione verso la pagina e a mantenere attiva la sessione.

```

Ascii
MalService..Mals
ervice..HGL345..
http://www.malwa
reanalysisbook.c
om..Internet Exp
lorer.8.0...!...

```