

Oggi faremo un'analisi statica basica di un malware presente sulla macchina virtuale xp finalizzata esattamente per l'analisi malware, con i tool appositi già installati.

Una volta installata la macchina, carichiamo il file in questione e ne studiamo le informazioni.

Come possiamo vedere, le librerie importate nell'eseguibile sono 4:

| Module Name  | Imports      | OFTs     | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
|              |              |          |               |                |          |           |
| szAnsi       | (nFunctions) | Dword    | Dword         | Dword          | Dword    | Dword     |
| KERNEL32.DLL | 6            | 00000000 | 00000000      | 00000000       | 00006098 | 00006064  |
| ADVAPI32.dll | 1            | 00000000 | 00000000      | 00000000       | 000060A5 | 00006080  |
| MSVCRT.dll   | 1            | 00000000 | 00000000      | 00000000       | 000060B2 | 00006088  |
| WININET.dll  | 1            | 00000000 | 00000000      | 00000000       | 000060BD | 00006090  |

Sappiamo che la libreria KERNEL32.DLL contiene e carica le funzioni principali per interagire con il sistema operativo, mentre la libreria ADVAPI32.dll contiene le funzioni per interagire con MICROSOFT, la libreria MSVCRT.dll contiene le funzioni per la manipolazione delle stringhe, l'allocazione della memoria, e per le chiamate input/output ed, infine, l'ultima libreria, la wininet.dll contiene le funzioni per l'implementazione di protocolli noti, quali http,ftp,ntp.

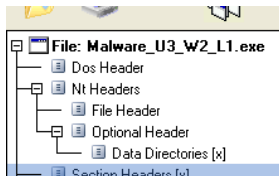
Come possiamo vedere, possiamo notare la lista delle funzioni richieste all'interno della libreria (in questo caso, la kernel32.dll):

| Module Name  | Imports      | OFTs     | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|--------------|--------------|----------|---------------|----------------|----------|-----------|
| 00000A98     | N/A          | 00000A00 | 00000A04      | 00000A08       | 00000A0C | 00000A10  |
| szAnsi       | (nFunctions) | Dword    | Dword         | Dword          | Dword    | Dword     |
| KERNEL32.DLL | 6            | 00000000 | 00000000      | 00000000       | 00006098 | 00006064  |
| ADVAPI32.dll | 1            | 00000000 | 00000000      | 00000000       | 000060A5 | 00006080  |
| MSVCRT.dll   | 1            | 00000000 | 00000000      | 00000000       | 000060B2 | 00006088  |
| WININET.dll  | 1            | 00000000 | 00000000      | 00000000       | 000060BD | 00006090  |

| OFTs  | FTs (IAT) | Hint | Name           |
|-------|-----------|------|----------------|
|       |           |      |                |
| Dword | Dword     | Word | szAnsi         |
| N/A   | 000060C8  | 0000 | LoadLibraryA   |
| N/A   | 000060D6  | 0000 | GetProcAddress |
| N/A   | 000060E6  | 0000 | VirtualProtect |
| N/A   | 000060F6  | 0000 | VirtualAlloc   |
| N/A   | 00006104  | 0000 | VirtualFree    |
| N/A   | 00006112  | 0000 | ExitProcess    |

Sono presenti le due funzioni che possiamo trovare tipicamente nei malware: Loadlibrary e GetProcAddress, che richiamano la libreria solo all'occorrenza (importazione della libreria "runtime").

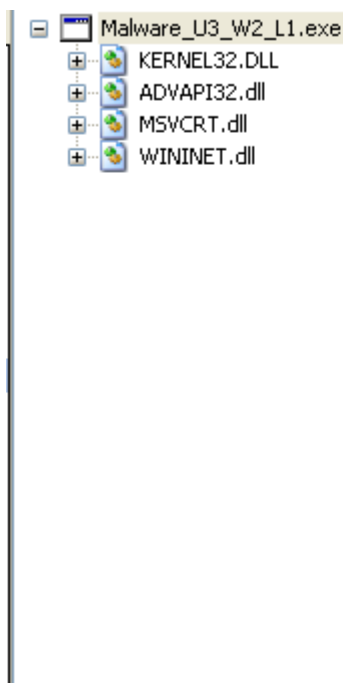
Ora invece andiamo ad analizzare le componenti dell'header del malware (.text,.rdata,data,.rsrc) che ci sono di grande utilita:



| Name     | Virtual Size | Virtual Address | Raw Size | Raw Address | Reloc Address | Linenumbers | Relocations ... | Linenumber... | Characteristics |
|----------|--------------|-----------------|----------|-------------|---------------|-------------|-----------------|---------------|-----------------|
| 000001D8 | 000001E0     | 000001E4        | 000001E8 | 000001EC    | 000001F0      | 000001F4    | 000001F8        | 000001FA      | 000001FC        |
| 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        |

Come possiamo notare, e stato utilizzare un packer noto per i malware: UXP.

UXP funziona comprimendo le sezioni memorizzate all'interno della cartella (.text,data ecc.) nominandole UPX0,UPX1 e cosi via.



| Property  | Value   |
|-----------|---|
| File Name | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W... |
| File Type | Portable Executable 32  |
| File Info | No match found.   |
| File Size | 3.00 KB (3072 bytes)  |
| PE Size   | 3.00 KB (3072 bytes)  |
| Created   | Tuesday 16 August 2022, 14.37.31  |
| Modified  | Wednesday 19 January 2011, 11.10.41                                       |
| Accessed  | Monday 27 March 2023, 13.45.56  |
| MD5       | 8363436878404DA0AE3E46991E355B83  |
| SHA-1     | 5A016FACBCB77E2009A01EA5C67B39AF209C3FCB                                  |

| Property | Value                        |
|----------|------------------------------|
| Empty    | No additional info available |

In questa sezione possiamo vedere la grandezza del malware (o anche delle librerie che l'eseguibile ha chiamato) in questione, il suo hash (sia md5 che SHA-1), il suo path, data di creazione e di modifica e cosi via.

Una volta preso l'hash dell'eseguibile, abbiamo cercato con virus total se fosse un malware noto ed il risultato e stato questo:

51

/ 69

Community Score

51 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

3.00 KB

2023-03-27 07:58:18 UTC

Lab01-02.exe

Size

6 hours ago

EXE

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

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 r002c0dhd20

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

Trojan/Win32.StartPage.C26214

Alibaba

TrojanClicker.Win32/Generic.1baf980f

Come possiamo vedere, e un trojan e possiamo leggere tantissime altre informazioni, essendo un malware gia noto.