

ANALISI STATICA BASICA

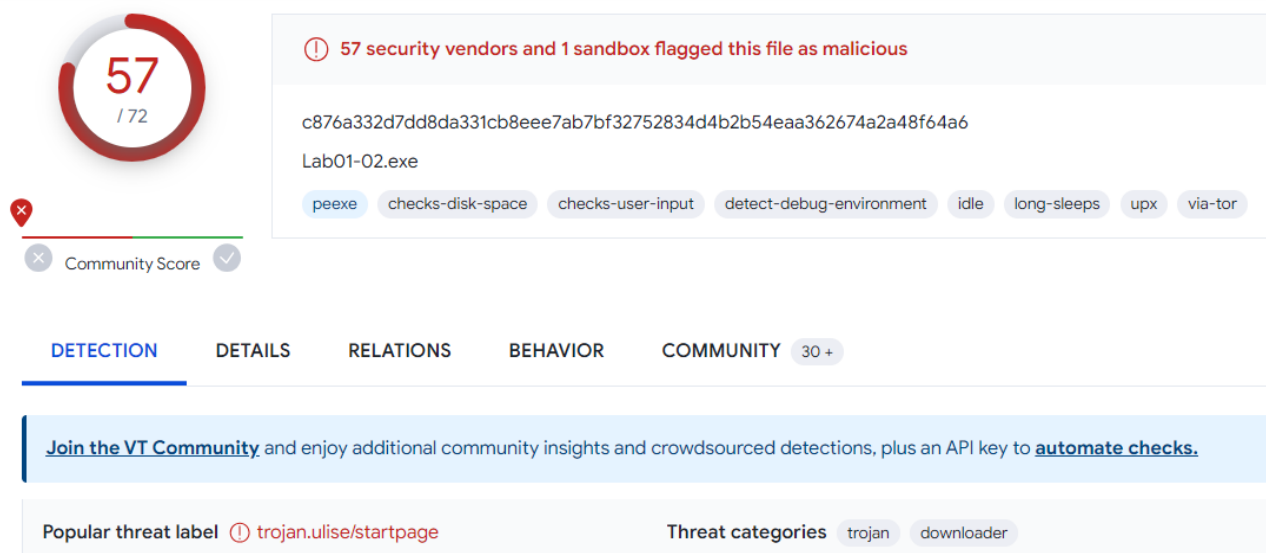
Nell'esercizio di oggi dovevamo analizzare un malware sulla macchina virtuale Windows XP tramite diversi tool per l'analisi statica basica.

Come primo passo sono andato ad usare il tool md5deep per ottenere il codice hash del file.

```
C:\ Command Prompt
27/11/2023 16.21      2.261 FILEFORMAT.txt
27/11/2023 16.21      800.256 hashdeep.exe
27/11/2023 16.21      12.291 HASHDEEP.txt
27/11/2023 16.21      988.160 hashdeep64.exe
27/11/2023 16.21      800.256 md5deep.exe
27/11/2023 16.21      14.717 MD5DEEP.txt
27/11/2023 16.21      988.160 md5deep64.exe
27/11/2023 16.21      800.256 sha1deep.exe
27/11/2023 16.21      988.160 sha1deep64.exe
27/11/2023 16.21      800.256 sha256deep.exe
27/11/2023 16.21      988.160 sha256deep64.exe
27/11/2023 16.21      800.256 tigerdeep.exe
27/11/2023 16.21      988.160 tigerdeep64.exe
27/11/2023 16.21      800.256 whirlpooldeep.exe
27/11/2023 16.21      988.160 whirlpooldeep64.exe
      17 File      10.796.902 byte
      2 Directory 8.056.832.000 byte disponibili

C:\Documents and Settings\Epicode_user\Desktop\Malanalysis\md5deep-4.3>md5deep "
C:\Documents and Settings\Epicode_user\Desktop\Malanalysis\Esercizio_Pratico_U3_
W2_L1\Malware_U3_W2_L1.exe"
8363436878404da0ae3e46991e355b83 C:\Documents and Settings\Epicode_user\Desktop
\Malanalysis\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
C:\Documents and Settings\Epicode_user\Desktop\Malanalysis\md5deep-4.3>
```

Ottenuto il codice, sono andato ad cercarlo sul sito VirusTotal per vedere se c'è un riscontro tra le firme di malware già noti. Il risultato è che si tratta di un trojan di tipo downloader.



57 / 72

57 security vendors and 1 sandbox flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Lab01-02.exe

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

Community Score 30 +

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 ① trojan.ulise/startpage

Threat categories trojan downloader

Come secondo passaggio sono andato ad usare il tool CFF Explorer per vedere di quante e quali sezioni è composto il malware e quali librerie usa.

Dopo aver spaccettato i section headers, possiamo vedere che il file è composto di tre sezioni: .text (che contiene il codice con le istruzioni per la CPU), .rdata (che include informazioni sulle librerie importate ed esportate dal file) e .data (che contiene le variabili globali del programma).

Malware_U3_W2_L1.exe									
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
.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

Con CFF Explorer possiamo anche vedere le librerie importate dal malware. Nel nostro caso sono presenti quattro librerie: KERNEL32.DLL (che contiene le funzioni per interagire con il sistema operativo), ADVAPI32.dll (che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo), MSVCRT.dll (che contiene funzioni per manipolare le stringhe e allocare memoria) e WININET.dll (che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP).

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000216C	N/A	0000208C	00002090	00002094	00002098	0000209C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

Infine ho usato la utility strings per ottenere ulteriori informazioni sul malware: Anche tramite strings ho ottenuto come ritorno l'elenco delle librerie importate, che queste vengono importate tramite il metodo runtime (dato che sono presenti le librerie Load Library e GetProcAddress), nonché conferma del fatto che il file opera su internet.

Posso quindi dire che, secondo le informazioni ottenute con questa analisi, il malware in questione È un downloader progettato per scaricare altri malware da internet su un sistema attaccato.