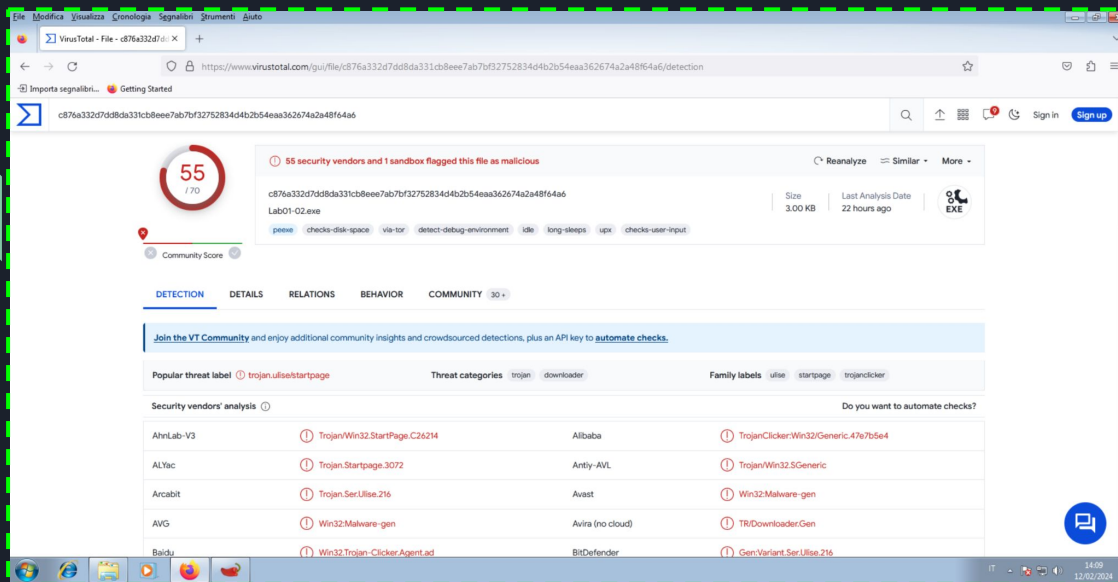




# ANALISI STATICA MALWARE

Kamenica Kristiano



Per prima cosa, abbiamo eseguito il caricamento del file su VirusTotal al fine di ottenere una scansione preliminare e generare un report dettagliato.

VirusTotal è una piattaforma online che consente di analizzare i file attraverso una varietà di motori antivirus e anti-malware.

Questo ci ha permesso di valutare la sicurezza del file confrontando i risultati ottenuti da diversi scanner.

Su VirusTotal, è possibile visualizzare direttamente le librerie importate dal malware.

Tuttavia per avere una visione migliore utilizzeremo il software CFF Explorer.

### Imports

- + ADVAPI32.dll
- + KERNEL32.DLL
- + MSVCRT.dll
- + WININET.dll

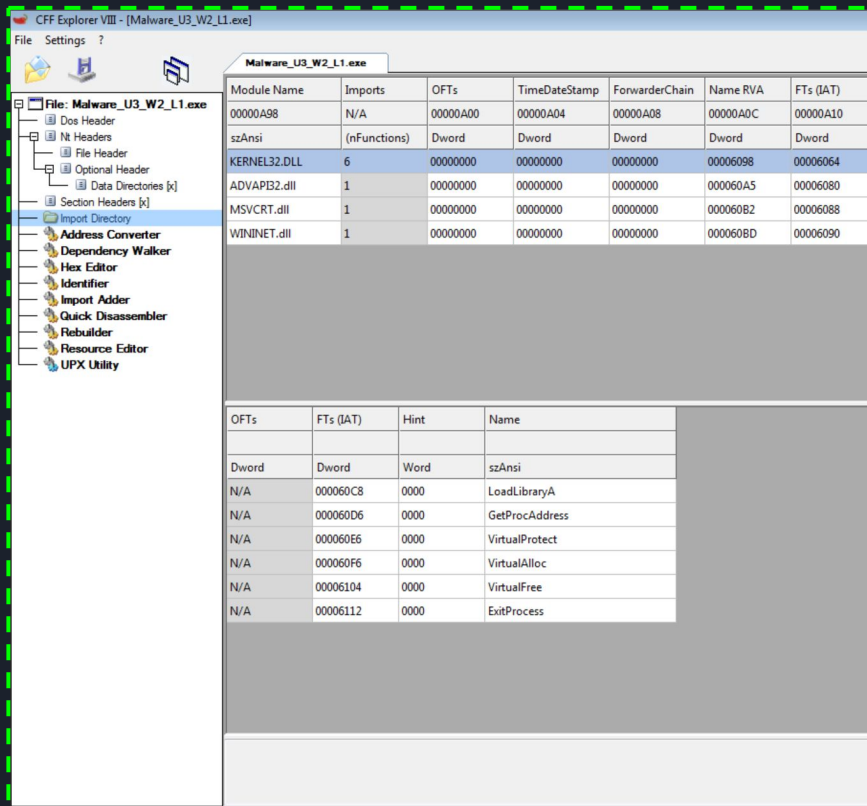
Quindi, abbiamo identificato queste librerie cruciali:

**ADVAPI32.DLL:** Questa libreria aiuta il sistema operativo Windows a gestire cose come i servizi e la sicurezza. È fondamentale per garantire che il sistema funzioni correttamente e sia protetto da minacce esterne.

**KERNEL32.DLL:** Considerata il "cuore" del sistema operativo, questa libreria gestisce molte funzioni di base come la gestione dei file, della memoria e dei processi. È essenziale per il funzionamento stabile del sistema.

**MSVCRT.DLL:** Questa libreria fornisce supporto per molte operazioni di base dei programmi, come l'input/output e la gestione della memoria. È utilizzata da molti programmi per garantire il corretto funzionamento delle loro funzionalità.

**WININET.DLL:** Questa libreria è coinvolta nell'accesso a Internet, consentendo ai programmi di connettersi a siti web e servizi online. È essenziale per le applicazioni che richiedono connettività Internet.



CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

Module Name	Imports	OFTs	TimeStamp	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

Mi e stato inoltre richiesto anche di indicare le sezioni di cui si compone il virus:

Sections						
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	16384	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908	5848.3
UPX2	24576	4096	512	2.8	f998d25f473e69cc89bf43af3102beea	53922

Abbiamo confermato tramite CFF Explorer:

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Word	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

Analizzando attentamente le sezioni, notiamo che sono identificate con il nome "**UPX**".

UPX è un software open source utilizzato per comprimere il codice in un file compresso, al fine di nascondere le informazioni contenute al suo interno.

Dato che le informazioni sono nascoste, abbiamo optato per decomprimere UPX:

```
C:\Users\user\Desktop\upx>upx -d L1.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser      Jan 3rd 2024


  File size      Ratio      Format      Name
-----
  16384 <-      3072      18.75%      win32/pe      L1.exe

Unpacked 1 file.

C:\Users\user\Desktop\upx>
```

Ora abbiamo una visione in chiaro delle sezioni:


L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	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:** Questa sezione contiene le istruzioni, ovvero le righe di codice, che la CPU eseguirà una volta che il software sarà avviato. È la parte del file eseguibile che viene effettivamente eseguita dalla CPU. Tutte le altre sezioni contengono dati o informazioni di supporto.

**.rdata:** Questa sezione include generalmente le informazioni sulle librerie e sulle funzioni importate ed esportate dall'eseguibile. Come abbiamo visto, queste informazioni possono essere ottenute utilizzando CFF Explorer.

**.data:** Questa sezione contiene tipicamente i dati o le variabili globali del programma eseguibile, che devono essere accessibili da qualsiasi parte del programma. Una variabile è considerata globale quando non è definita all'interno del contesto di una funzione, ma è dichiarata globalmente ed è quindi accessibile da qualsiasi funzione all'interno dell'eseguibile.



Dagli indicatori di comportamento che emergono, come:

- ***checks-disk-space*** = verifica dello spazio sul disco
- ***checks-user-input*** = controllo degli input utente
- ***detect-debug-environment*** = rilevamento dell'ambiente debug
- ***idle*** = Inattività
- ***long-sleeps*** = lunghi periodi di inattività

Ipotesizzo che il malware(nel caso specifico un trojan), una volta attivo, fornisca informazioni sull'ambiente di sistema e sui file presenti. Sembra anche in grado di monitorare gli input degli utenti o di stabilire un canale di comunicazione attraverso il quale trasmettere dati alla macchina dell'attaccante.