

Relazione S10L1

L'obiettivo dell'esercizio di oggi è quello di effettuare un'analisi statica basica su un malware presente sulla macchina virtuale installata appositamente.

Come prima cosa sono andato a prendermi l'hash del file e l'ho inserito su virus total per un primo riscontro:



57
/ 72

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe

Size
3.00 KB

Last Analysis Date
20 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/startpage

Threat categories trojan downloader

Family labels ulise startpage trojanclicker

Security vendors' analysis

Do you want to automate checks?

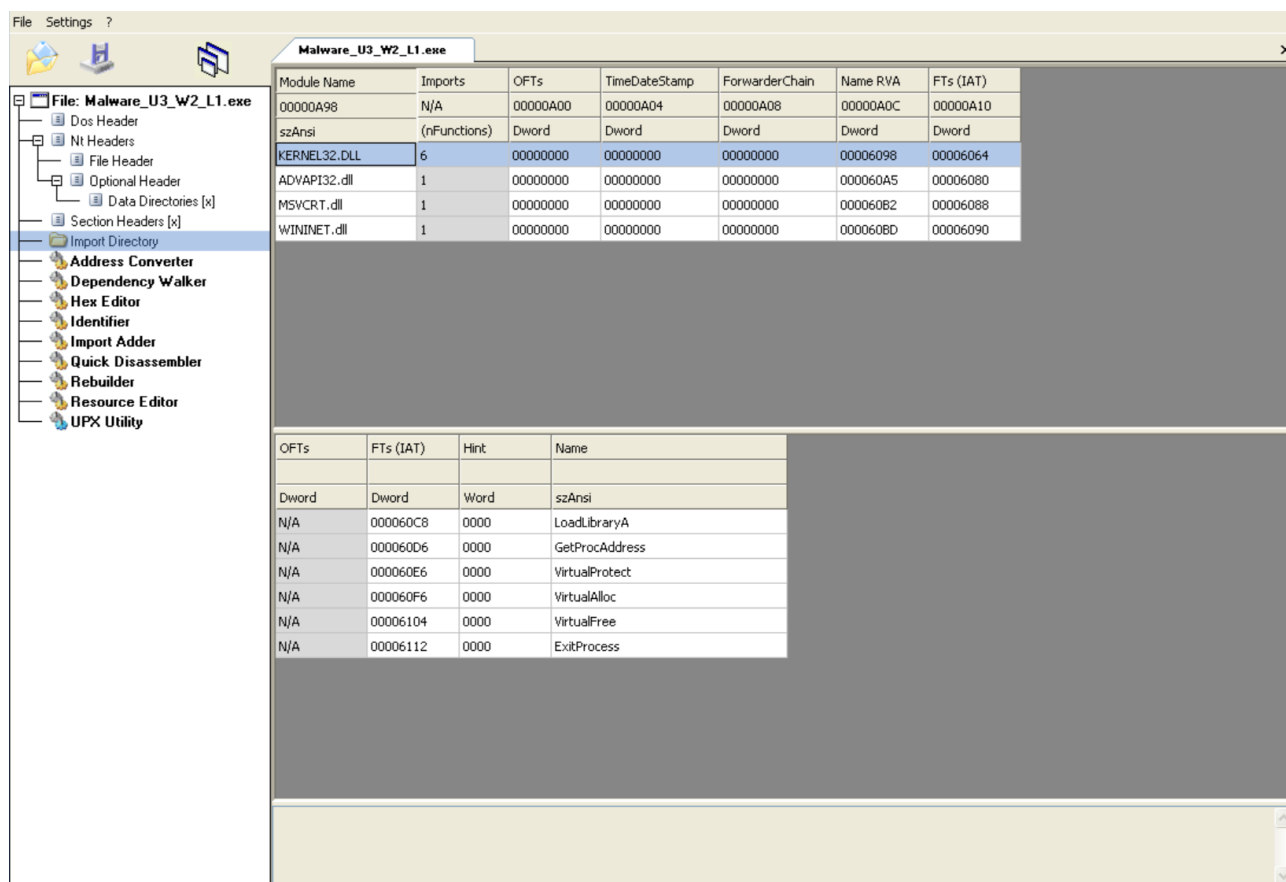
AhnLab-V3	Trojan.Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Generic.47e7b5e4
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan.Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Downloader.Gen
Baidu	Win32:Trojan-Clicker.Agent.ad	BitDefender	Gen:Variant.Ser.Ulise.216
BitDefenderTheta	Gen:NN.ZexaF.36792.amGfaWf867f	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Malware.Agent-6350563-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.cbcb77	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Click3.12740	Elastic	Malicious (moderate Confidence)
Emsisoft	Gen:Variant.Ser.Ulise.216 (B)	eScan	Gen:Variant.Ser.Ulise.216
ESET-NOD32	Win32/TrojanClicker.Agent.NVM	F-Secure	Trojan.TR/Downloader.Gen
Fortinet	W32/Agent.NVMltr	GData	Gen:Variant.Ser.Ulise.216
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Downloader.sdlis2
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.fxq
Kingsoft	Win32:troj.undef.a	Lionic	Trojan.Win32.Zbot.IsXA
Malwarebytes	Trojan.Agent.UPX	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Generic.ait

Possiamo vedere le librerie importate già su VirusTotal:

Imports

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

Tuttavia per avere una certezza maggiore le possiamo controllare sull'apposito programma presente sulla macchina virtuale:



Abbiamo quindi una conferma che le librerie importate sono quelle quattro presenti nella prima foto.

La libreria **ADVAPI32.dll** fornisce funzioni sia per interagire con i servizi del sistema operativo (farli partire e fermare), sia per operazioni sul registro nonché per gestire la sicurezza come la crittografia e l'autenticazione.

La libreria **KERNEL32.dll** viene utilizzata per creare threads, gestire gli errori e le eccezioni. Questa libreria viene utilizzata anche per gestire la memoria virtuale, i file e i dispositivi I/O.

La libreria **MSVCRT.dll** viene utilizzata per la manipolazione delle stringhe, l'allocazione della memoria, la gestione dei processi e dei file. Anche questa libreria fornisce funzioni per gestire le ec-

cezioni e gli errori.

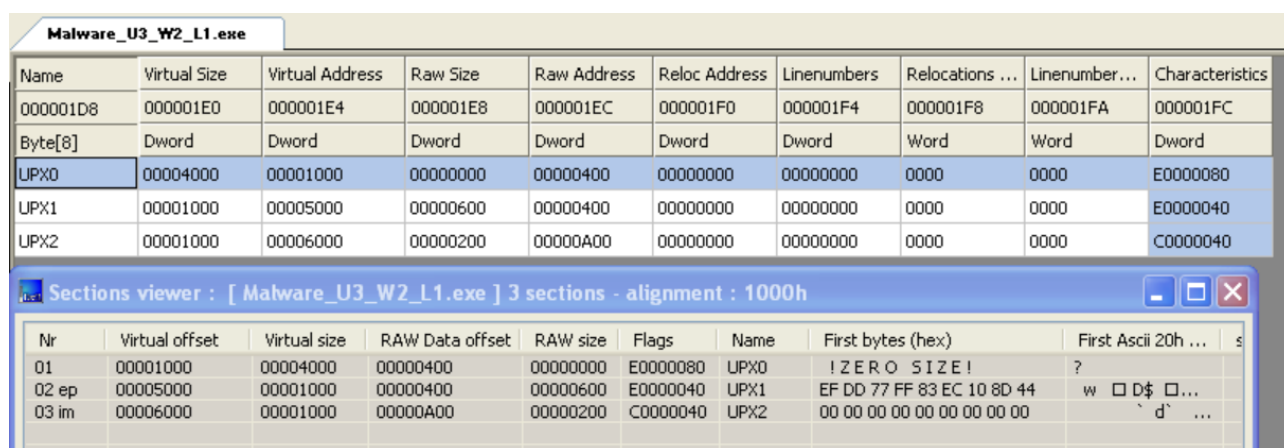
La libreria **WININET.dll** viene utilizzata per fornire un'interfaccia di programmazione per le applicazioni che utilizzano i protocolli come HTTP , FTP e NTP.

Nell'analisi del malware viene richiesto anche di indicare le sezioni di cui si compone. Anch'esse si possono vedere su VirusTotal:

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

Come sempre però per sicurezza sono andato ad utilizzare gli appositi programmi per verificare l'esattezza delle informazioni:



The image shows two screenshots from a malware analysis tool. The top screenshot is a table titled 'Malware_U3_W2_L1.exe' showing sections. The bottom screenshot is a 'Sections viewer' window for the same file, showing 3 sections with alignment 1000h.

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

Nr	Virtual offset	Virtual size	RAW Data offset	RAW size	Flags	Name	First bytes (hex)	First Ascii 20h ...
01	00001000	00004000	00000400	00000000	E0000080	UPX0	! Z E R O S I Z E !	?
02 ep	00005000	00001000	00000400	00000600	E0000040	UPX1	EF DD 77 FF 83 EC 10 8D 44	w □ D\$ □...
03 im	00006000	00001000	00000A00	00000200	C0000040	UPX2	00 00 00 00 00 00 00 00	` d' ...

Anche in questo caso le sezioni trovate confermano quanto visto su VirusTotal.

Osservando bene le sezioni vediamo che vengono identificate con il nome UPX che non è altro che un software open source che comprime il codice in un file compresso così da nascondere le informazioni.

Poiché non è prevista un'analisi approfondita possiamo solo basarci sulle informazioni raccolte fin'ora per determinare lo scopo di questo malware. La fonte di informazioni maggiori per è su VirusTotal in quanto questo file è già stato analizzato numerose volte, guardando i tag di comportamento vediamo:

checks-disk-space

checks-user-input

detect-debug-environment

idle

long-sleeps

Viene quindi da pensare che questo malware una volta entrato in azione possa fornire informazioni all'attaccante sul sistema e i file all'interno di esso. Sembra anche che possa tenere traccia degli input dell'utente e che possa creare un canale di comunicazione grazie al quale invia le informazioni alla macchina attaccante.

Davide Lecci