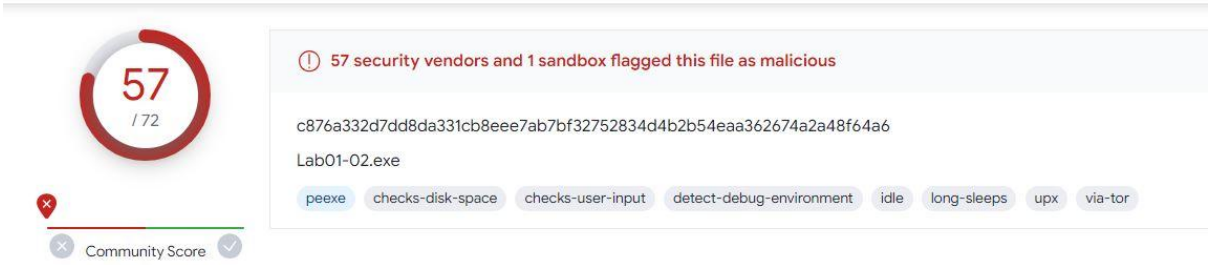
Progetto S10-L1

Studente: Simone Mininni

Task: Malware analysis, Basic Static analysis, trovare le librerie importate dal programma malevolo, le sezioni del programma e intuire il suo comportamento.

Controllo della cifra di hash md5.

Una volta ricavato il codice hash del programma, eseguo un controllo su virus total per capire concretamente se si tratta di un malware ed che tipo.



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.amGfaWi867f	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

Dal report di virus total 57 vendor lo hanno etichettato come malevolo. In particolare sembra trattarsi di un trojan downloader.

Quindi mi aspetto che il programma si connetterà a un sito malevolo per scaricare qualcosa.

Procedendo con l‘analisi, individuo le funzioni di windows che chiama presumibilmente a run time.

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

Imports

— ADVAPI32.dll

CreateServiceA

— KERNEL32.DLL

ExitProcess
GetProcAddress
LoadLibraryA
VirtualAlloc
VirtualFree
VirtualProtect

— MSVCRT.dll

exit

— WININET.dll

InternetOpenA

Ci sono quattro librerie di windows importate.
-Kernel32.dll= funzioni core del sistema per manipolare file, allocare in memoria.
-WININET.dll=Effettua connessioni di rete con protocolli http, ftp, ecc…
-ADVAPI32.dll = contiene le funzioni per interagire con i registri e i servizi di sistema.
-MSVCTR.dll= funzioni per chiamate input, output, manipolazione stringhe.

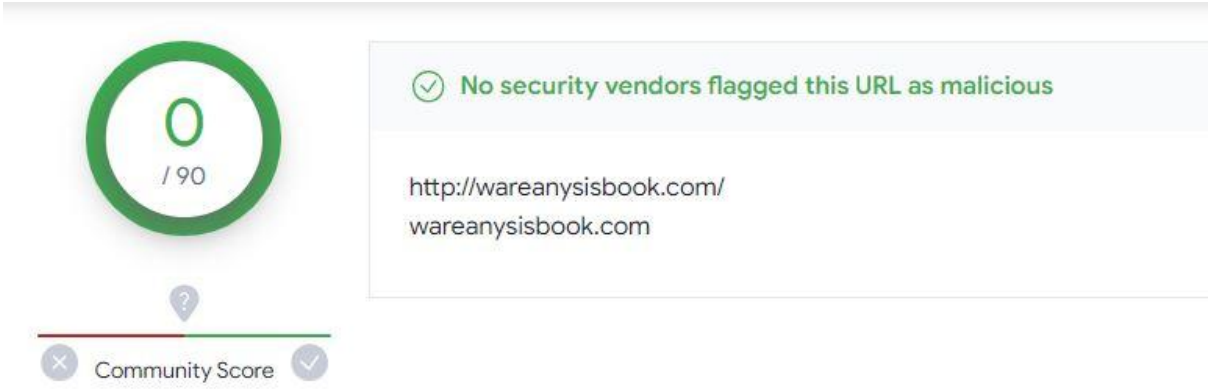
Sezioni del programma, offuscate con upx packer.

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2011-01-19 16:10:41 UTC
Entry Point	21520
Contained Sections	3

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



Con il comando strings, riusciamo a trovare un url che esaminato su virtualtotal , non sembra essere malevolo.

In fine, da questa prima analisi possiamo dedurre che si tratta di un trojan downloader, offuscato con upx, che andrà a effettuare una richiesta http con la funzione di windows “InternetOpenA”.