

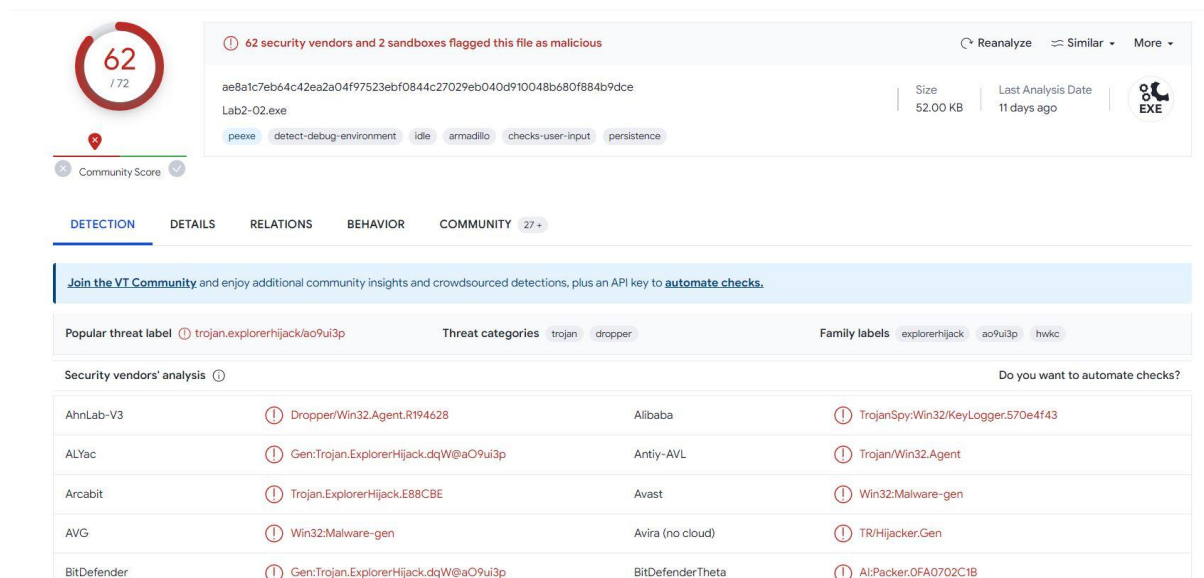
Progetto S10-L2

Studente: Simone Mininni

Task: Malware analysis, Analisi Dinamica basica.

Malware_U3_W2_L2

Analisi statica:



The screenshot shows the VirusTotal analysis interface for the file 'Lab2-02.exe'. At the top, a red circle indicates a community score of 62/72. A warning message states: '62 security vendors and 2 sandboxes flagged this file as malicious'. The file's SHA-256 hash is 'ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce', its size is 52.00 KB, and it was last analyzed 11 days ago. Below this, tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' are visible. The 'DETECTION' tab is active, showing a 'Popular threat label' of 'trojan.explorerhijack/ao9ui3p', 'Threat categories' of 'trojan' and 'dropper', and 'Family labels' of 'explorerhijack', 'ao9ui3p', and 'hwkc'. A table titled 'Security vendors' analysis' lists detections from various vendors:

Security vendors' analysis		Do you want to automate checks?	
AhnLab-V3	ⓘ Dropper/Win32.Agent.R194628	Alibaba	ⓘ TrojanSpy:Win32/KeyLogger.570e4f43
ALYac	ⓘ Gen:Trojan.ExplorerHijack.dqW@aO9ui3p	Antiy-AVL	ⓘ Trojan/Win32.Agent
Arcabit	ⓘ Trojan.ExplorerHijack.E88CBE	Avast	ⓘ Win32:Malware-gen
AVG	ⓘ Win32:Malware-gen	Avira (no cloud)	ⓘ TR/Hijacker.Gen
BitDefender	ⓘ Gen:Trojan.ExplorerHijack.dqW@aO9ui3p	BitDefenderTheta	ⓘ AI:Packers.OFA0702C1B

Confrontando il codice di hash, il programma risulta essere malevolo e sembra essere un trojan dropper.

Analisi dinamica:

Eseguiamo il malware per osservare il suo comportamento, utilizzando alcuni software utili come "process explorer", "procmon", "regshot", "wireshark".

Evidenze Network: Nessuna

Monitorando il traffico con Wireshark non si nota nessun tentativo di connessione alla rete. Quindi il programma andrà ad eseguire operazioni solo sulla macchina host.

The screenshot shows two windows from a Windows operating system. The left window is the Task Manager, displaying a list of running processes. The right window is a File Explorer showing the contents of the C:\WINDOWS\system32 directory.

Process Name	PID	Description	Path
MalwareL2.exe	2308		C:\Documents & Settings\user\My Recent Documents\...
svchost.exe	2316	Generic Host Process for Win32 Services	C:\WINDOWS\system32\svchost.exe
Idle	0	Idle	
System	4	System	
smss.exe	596	Windows NT Session Manager	C:\WINDOWS\system32\smss.exe
csrss.exe	652	Client Server Runtime Process	C:\WINDOWS\system32\csrss.exe
winlogon.exe	676	Windows NT Logon Process	C:\WINDOWS\system32\winlogon.exe
services.exe	720	Windows NT Services	C:\WINDOWS\system32\services.exe
svchost.exe	720	Generic Host Process for Win32 Services	C:\WINDOWS\system32\svchost.exe

The File Explorer window shows the following files and folders in C:\WINDOWS\system32:

- ssstask
- ssstext3d
- stdclient.dll
- stimon
- stobject.dll
- storage.dll
- subrange.uce
- subst
- svchost

2308	Process Start		SUCCESS	Parent PID: 1792, Command line: "C:\Documents and Settings\Administrator\My Recent Documents\malware2.exe"
2308	Thread Create		SUCCESS	Thread ID: 2312
2308	Load Image	C:\Documents and Settings\Administrator\Desktop\malware2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
2308	Load Image	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xa1000
2308	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
2308	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
2308	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
2308	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
2308	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
2308	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
2308	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2316, Command line: "C:\WINDOWS\system32\svchost.exe"
2308	Thread Exit		SUCCESS	Thread ID: 2312, User Time: 0.0000000, Kernel Time: 0.0468750
2308	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0312500 seconds

Infine andando a confrontare i file di registro prima e dopo il lancio del malware notiamo con regshot alcune differenze

[illegible]

Per quanto riguarda le chiavi modificate, praticamente il malware non setta nessun nuovo valore di registro, poichè le modifiche vengono effettuate da explorer.exe e “regshot” stesso.

Mentre svchost.exe, il programma creato dal malware, va a settare un random seed.

A livello di file system, crea un file di testo nella cartella del malware che sovrascrive informazioni, comportandosi come un keylogger.