

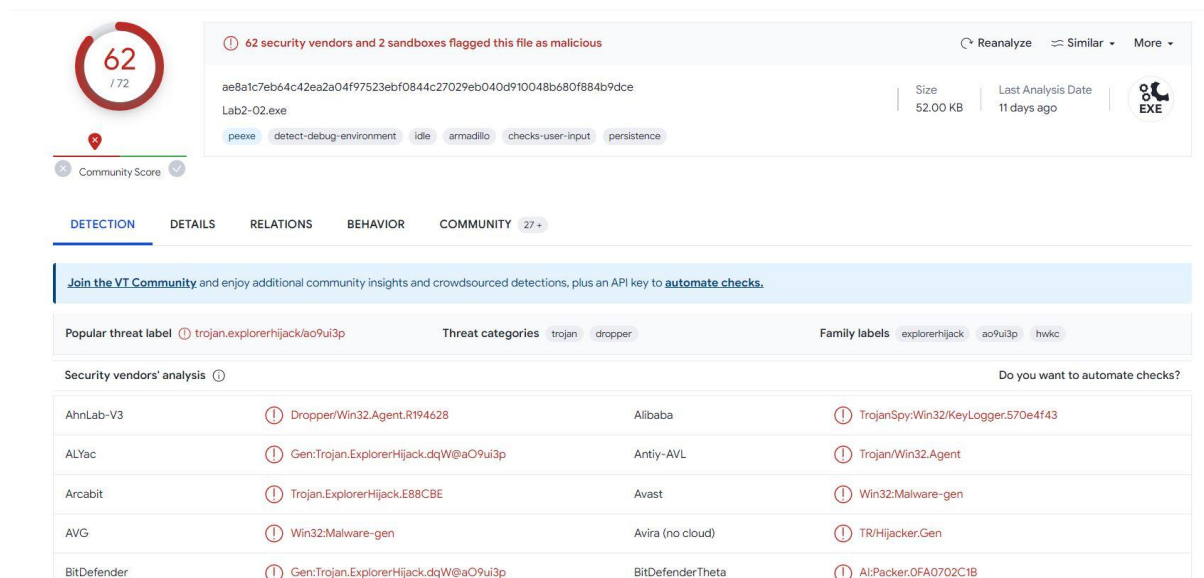
## Progetto S10-L2

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, a row of tags includes 'peexe', 'detect-debug-environment', 'idle', 'armadillo', 'checks-user-input', and 'persistence'. 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:

Vendor	Detection
AhnLab-V3	⚠ Dropper/Win32.Agent.R194628
ALYac	⚠ Gen:Trojan.ExplorerHijack.dqW@aO9ui3p
Arcabit	⚠ Trojan.ExplorerHijack.E88CBE
AVG	⚠ Win32:Malware-gen
BitDefender	⚠ Gen:Trojan.ExplorerHijack.dqW@aO9ui3p
Alibaba	⚠ TrojanSpy:Win32/KeyLogger.570e4f43
Antiy-AVL	⚠ Trojan/Win32.Agent
Avast	⚠ Win32:Malware-gen
Avira (no cloud)	⚠ TR/Hijacker.Gen
BitDefenderTheta	⚠ AI:Packers.OFA0702C1B

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

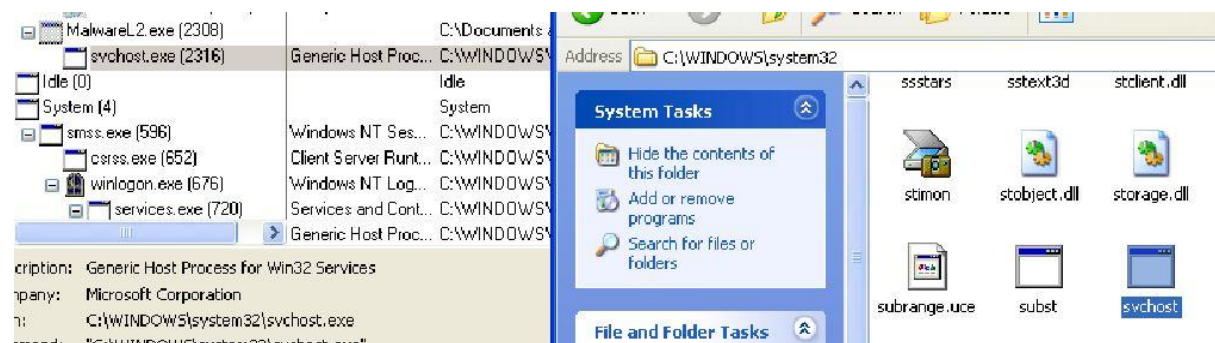
Analisi dinamica:

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.

## Evidenze sulla macchina host:



Dall' albero dei processi possiamo notare che “MalwareL2” crea un processo figlio “svchost.exe”.

MalwareL2.exe	2308	Process Start		SUCCESS	Parent PID: 1792, Command line: "C:\Documents and Settings\Administrator\Desktop\MalwareL2.exe"
MalwareL2.exe	2308	Thread Create		SUCCESS	Thread ID: 2312
MalwareL2.exe	2308	Load Image	C:\Documents and Settings\Administrator\Desktop\MalwareL2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xa1000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x46000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77d00000, Image Size: 0x8000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d00000, Image Size: 0x96000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
MalwareL2.exe	2308	Load Image	C:\WINDOWS\system32\securlib.dll	SUCCESS	Image Base: 0x77e00000, Image Size: 0x11000
MalwareL2.exe	2308	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2316, Command line: "C:\WINDOWS\system32\svchost.exe"
MalwareL2.exe	2308	Thread Exit		SUCCESS	Thread ID: 2312, User Time: 0.0000000, Kernel Time: 0.0468750
MalwareL2.exe	2308	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0312500 seconds

Filtrando per processi e thread, constatiamo che il malware è un dropper, ovvero carica le librerie in memoria a tempo di esecuzione e crea un nuovo processo.

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

Username: Administrator , Administrator					
-----					
Values added: 4					
-----					
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\0 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.01357...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\0 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08759...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\1 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08774...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\2 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08787...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\3 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08804...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\4 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08820...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\5 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08843...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\6 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.41.08941...	winiprv.exe	1212	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\7 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.58006...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\8 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76724...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\9 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76739...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\10 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76752...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\11 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76755...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\12 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76778...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\13 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76791...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\14 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.44.76810...	svchost.exe	1244	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\15 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84345...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\16 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84356...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\17 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84510...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\18 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84523...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\19 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84536...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\20 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84548...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\21 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.53.84575...	Regshot-x86-Unicode.exe	1628	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\ControlSet001\Services\WinMx\Enum\22 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,28.33.88183...	svchost.exe	888	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
HKLM\SYSTEM\CurrentControlSet\Services\WinMx\Enum\23 : 'Sw\{bf6afdc0-a680-11d0-8000-000000000000}	2,30.02.95268...	NOTEPAD.EXE	2052	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed
-----					
Total changes: 11					

Vengono aggiunte delle chiavi, windows tiene traccia nella muicache del programma lanciato.

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.

0  
/ 72

Community Score

✓ File distributed by Microsoft

2910ebc692d833d949bfd56059e8106d324a276d5f165f874f3fb1b6c613cdd5

svchost.exe

peexe detect-debug-environment idle via-tor known-distributor trusted

File Version Information

Copyright

© Microsoft Corporation. All rights reserved.

Product

Microsoft® Windows® Operating System

Description

Generic Host Process for Win32 Services

Original Name

svchost.exe

Internal Name

svchost.exe

File Version

5.1.2600.5512 (xpsp.080413-2111)

Known Source ⓘ

Organization

Microsoft Corporation

File name

svchost.exe

Description

The file belongs to the Win product, it can be found, for example, in SW DVD5 Win English WinXP Mode N OEM.

svchost.exe sembra essere effettivamente il servizio di windows, quindi innocuo.