

S10/L1 Esercizio 27/11/2023

Nell'esercizio odierno ci viene richiesto di analizzare il contenuto del file Esercizio Pratico U3 W2 L1:

- Indicare le librerie importate e fornirne la descrizione
- Indicare le sezioni di cui si compone il malware e fornirne la descrizione
- Aggiungere una descrizione sul malware in base alle informazioni raccolte

Le **librerie** importate sono le seguenti:

- **KERNEL32.dll**

È una libreria presente nei sistemi operativi Windows, fa parte del kernel (il nucleo del sistema operativo) di Windows. Questa libreria fornisce molte funzioni di base essenziali per il funzionamento del sistema operativo e delle applicazioni, ad esempio manipolazione dei file e gestione della memoria

- **ADVAPI32.dll**

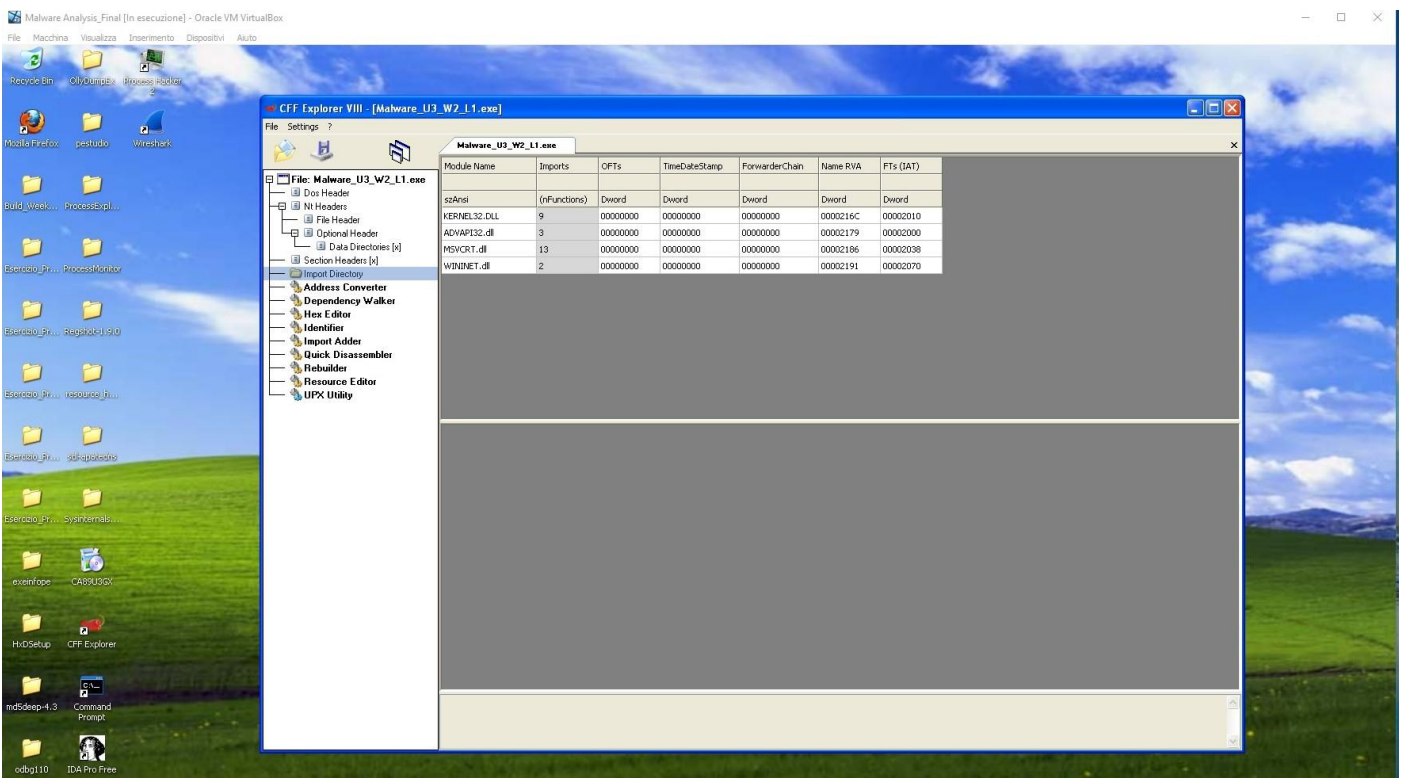
Anche questa è una libreria presente nei sistemi operativi Windows e fornisce funzioni relative alla sicurezza, alla gestione dei servizi e ad altre operazioni di sistema. Contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

- **MSVCRT.dll**

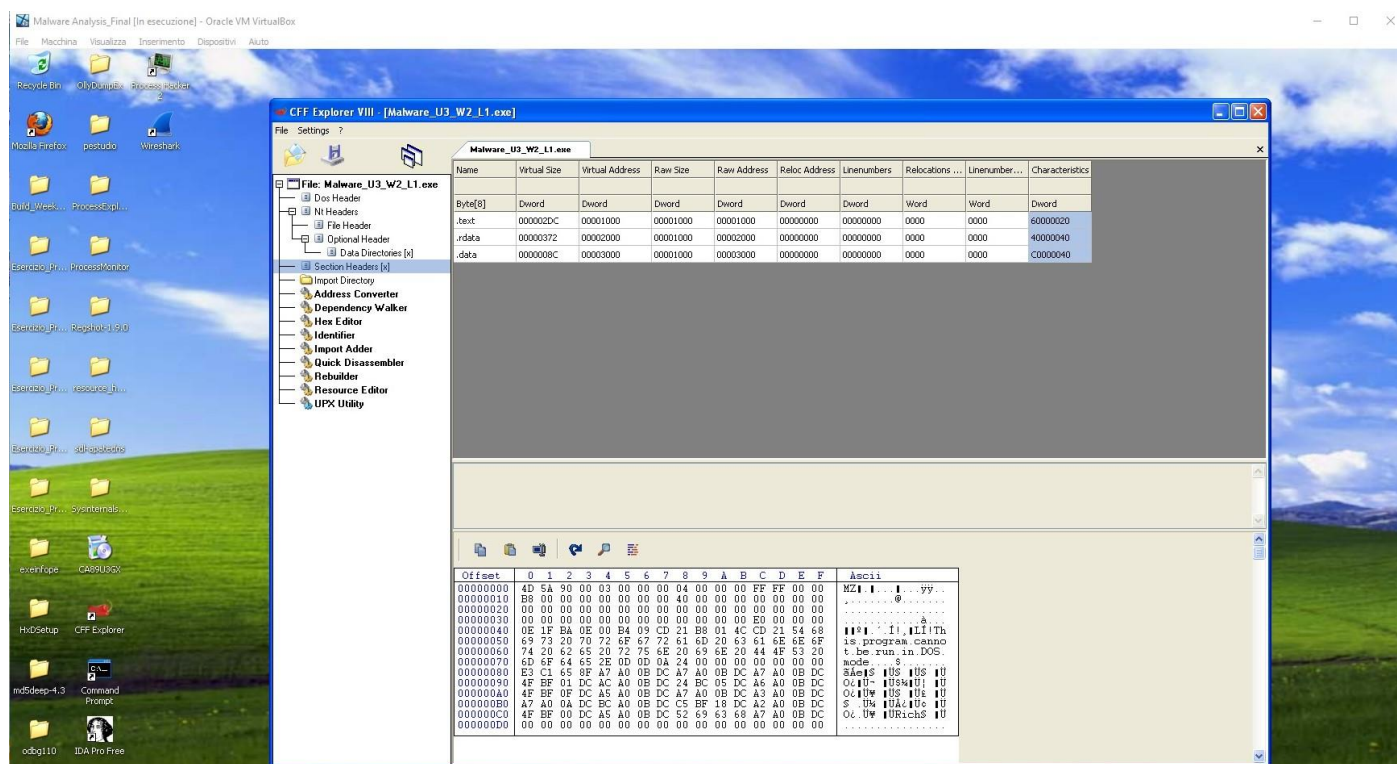
E' una libreria fornita da Microsoft per Windows fornisce implementazioni di funzioni standard del linguaggio C e supporta operazioni di input/output, gestione della memoria e altre funzionalità di base del linguaggio e viene spesso utilizzata quando si sviluppano programmi in C o C++ ad esempio contiene funzioni per la manipolazione stringhe e allocazione memoria

- **WININET.dll**

E' una libreria che fornisce funzionalità di networking per le applicazioni di Windows. Viene spesso utilizzata per effettuare operazioni di rete come l'accesso a risorse su internet, download e upload di file e la gestione delle connessioni HTTP, FTP e NTP



- **.text**
contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto
- **.rdata**
include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- **.data**
contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.



https://www.virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

57 / 72

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size 3.00 KB Last Analysis Date 22 hours ago EXE

peexe checks-disk-space checks-user-input detect-debug-environment idle long-sleeps upx via-tor

Community Score

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.ulisse.startpage** Threat categories trojan downloader Family labels ulisse startpage trojandclicker

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.S.Generic
Arcabit	Trojan.Ser.Ulisse.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.Ulisse.216
BitDefenderTheta	Gen:NN.Zexaf.36792.am/GfaW/867f	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)

https://www.virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Cynet	Malicious (score: 100)	DeepInstinct	Malicious
DrWeb	Trojan.Click3.12740	Elastic	Malicious (moderate Confidence)
Emisoft	Gen:Variant.Ser.Ulisse.216 (B)	eScan	Gen:Variant.Ser.Ulisse.216
ESET-NOD32	Win32/TrojanClicker.Agent.NVM	F-Secure	Trojan.TR/Downloader.Gen
Fortinet	W32/Agent.NVMtr	GData	Gen:Variant.Ser.Ulisse.216
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Downloader.sds2
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.fxdq
Kingsoft	Win32.trj.undef.a	Lionic	Trojan.Win32.Zbot.LsXA
Malwarebytes	Trojan.Agent.LUPX	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Generic.ait
NANO-Antivirus	Trojan.Win32.Click3.laupgs	Rising	TrojanClicker-Agent8.13 (TFE:S4DYHMG...
Sangfor Engine Zero	Suspicious.Win32.Save.a	SecureAge	Malicious
Skyhigh (SWG)	Generic.ait	Sophos	Mal/Generic-S
Symantec	Trojan.Horse	Tencent	Malware.Win32.Gencirc.10ba33c6
Trapmine	Malicious.high.ml.score	Trellix (FireEye)	Generic.mg.8363436878404dso
TrendMicro	TROJ_GEN.R002C0DHD20	TrendMicro-HouseCall	TROJ_GEN.R002C0DHD20
Varist	W32/Agent.DJC.gen/Eldorado	VBA32	Trojan.Click
VIPRE	Gen:Variant.Ser.Ulisse.216	VirIT	Trojan.Win32.Generic.CMEY
ViRobot	Trojan.Win32.S.StartPage.3072	Webroot	
Xcitium	Malware@#22epulwibvym	Yandex	Trojan.CL.Agent.SYJ1Ye/ZV4
Zillya	Trojan.Agent.Win32.1288291	Acronis (Static ML)	Undetected

Abbiamo ricavato il codice hash da MD5 e come possiamo rilevare dalla scansione effettuata con virus total si tratta sicuramente di un malware di tipo trojan, un tipo di software dannoso che si presenta come qualcosa di legittimo o affidabile, ma che in realtà contiene codice dannoso. Nello specifico troviamo il trojan downloader che ha lo scopo di scaricare e installare altri malware sul sistema.