

**2024**



**CS0124**

# **REPORT**

**Week 10 Lesson 1**

---

**PREPARED BY : Bruno Falconi**

## Report sull'Analisi del Malware - Esercizio\_Pratico\_U3\_W2\_L1

### Introduzione

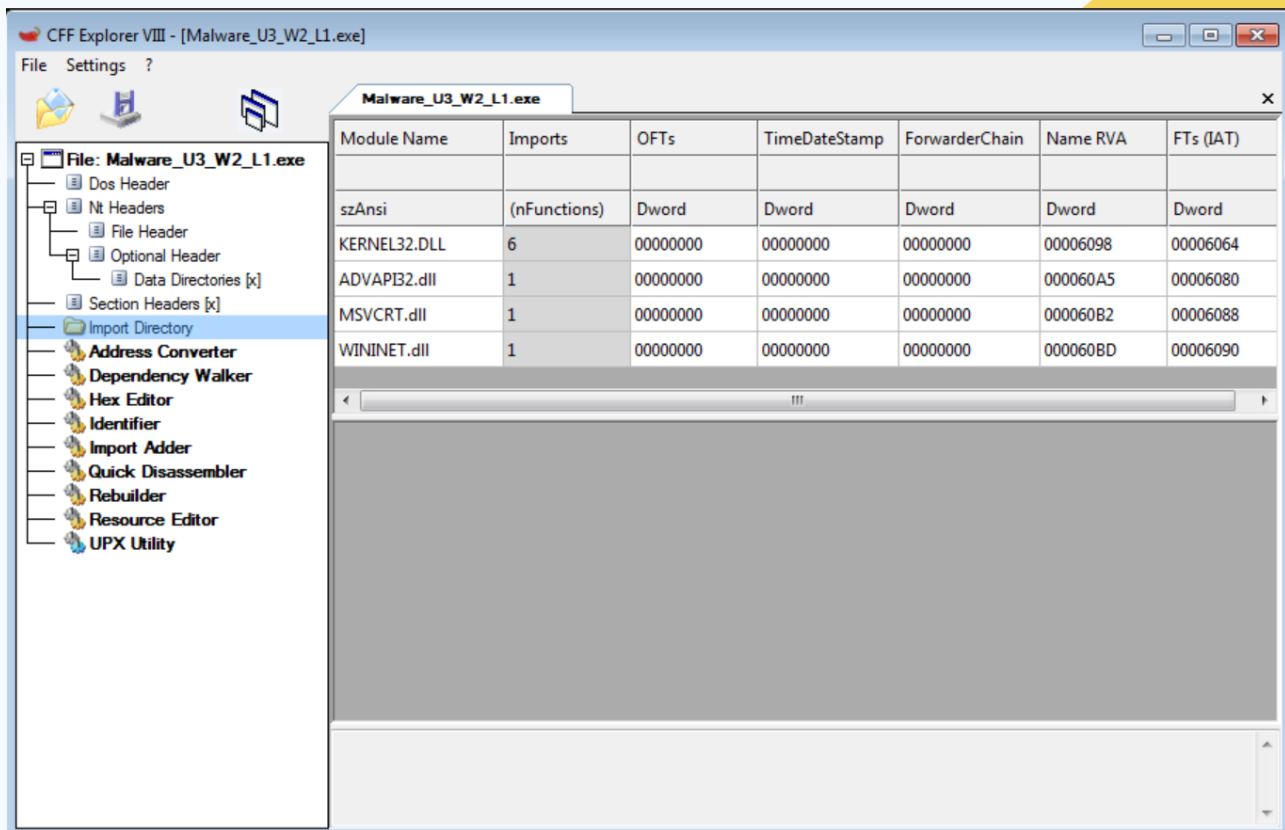
Il presente report descrive l'analisi del file eseguibile "Esercizio\_Pratico\_U3\_W2\_L1" trovato nella cartella omonima sul Desktop della macchina virtuale dedicata all'analisi dei malware. Il file è stato sottoposto a varie analisi utilizzando CFF Explorer VIII, compresa la verifica MD5 tramite Ash, e successivamente è stato caricato su VirusTotal per una scansione antivirus e un'ulteriore analisi. Lo scopo di queste analisi è identificare le librerie importate, le sezioni e le potenziali minacce del malware.

### Analisi delle Librerie Importate e Sezioni del Malware:

Dopo un'attenta analisi con CFF Explorer VIII, sono state individuate le seguenti librerie importate e funzioni del malware:

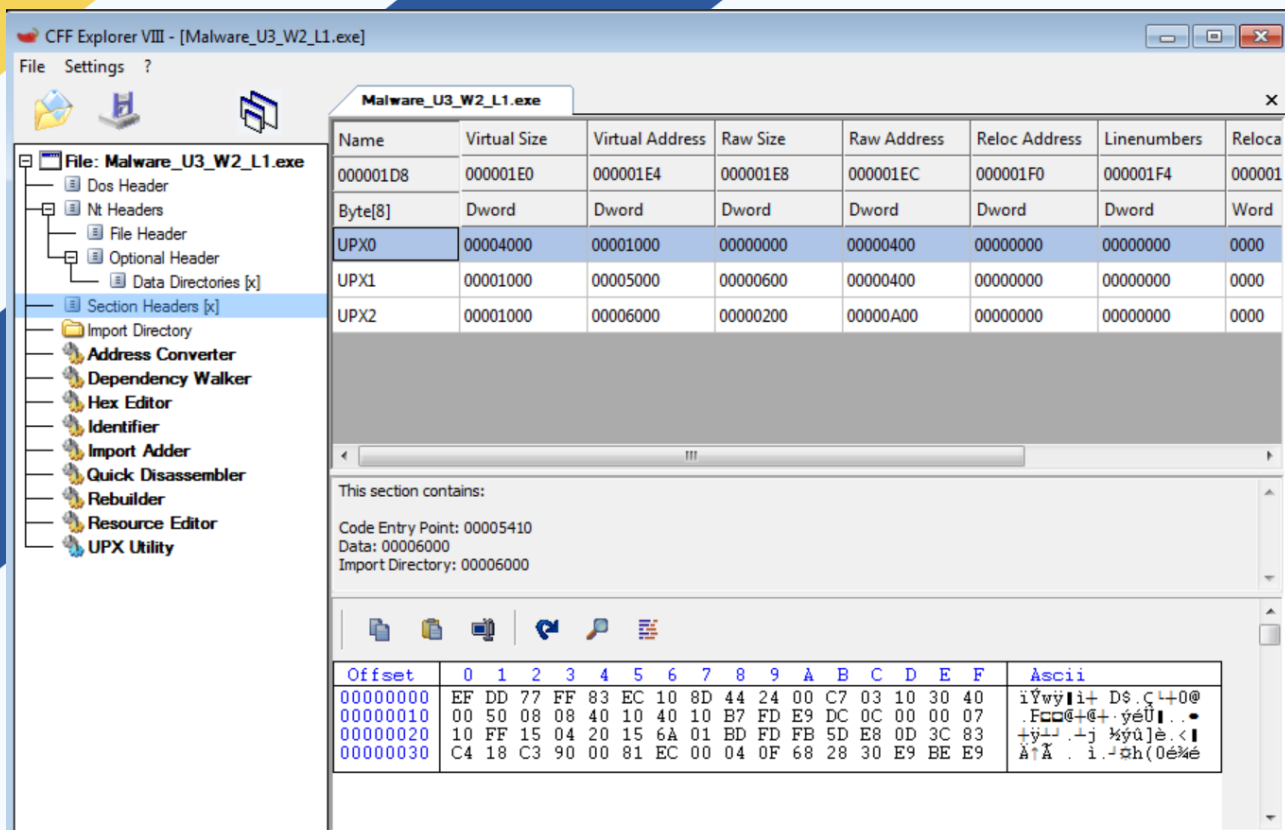
#### 1. Librerie Importate:

- **KERNEL32.dll:**
  - LoadLibraryA
  - GetProcAddress
  - VirtualProtect
  - VirtualAlloc
  - VirtualFree
  - ExitProcess
- **ADVAPI32.dll:**
  - CreateServiceA
- **MSVCRT.dll:**
  - exit
- **WININET.dll:**
  - InternetOpenA



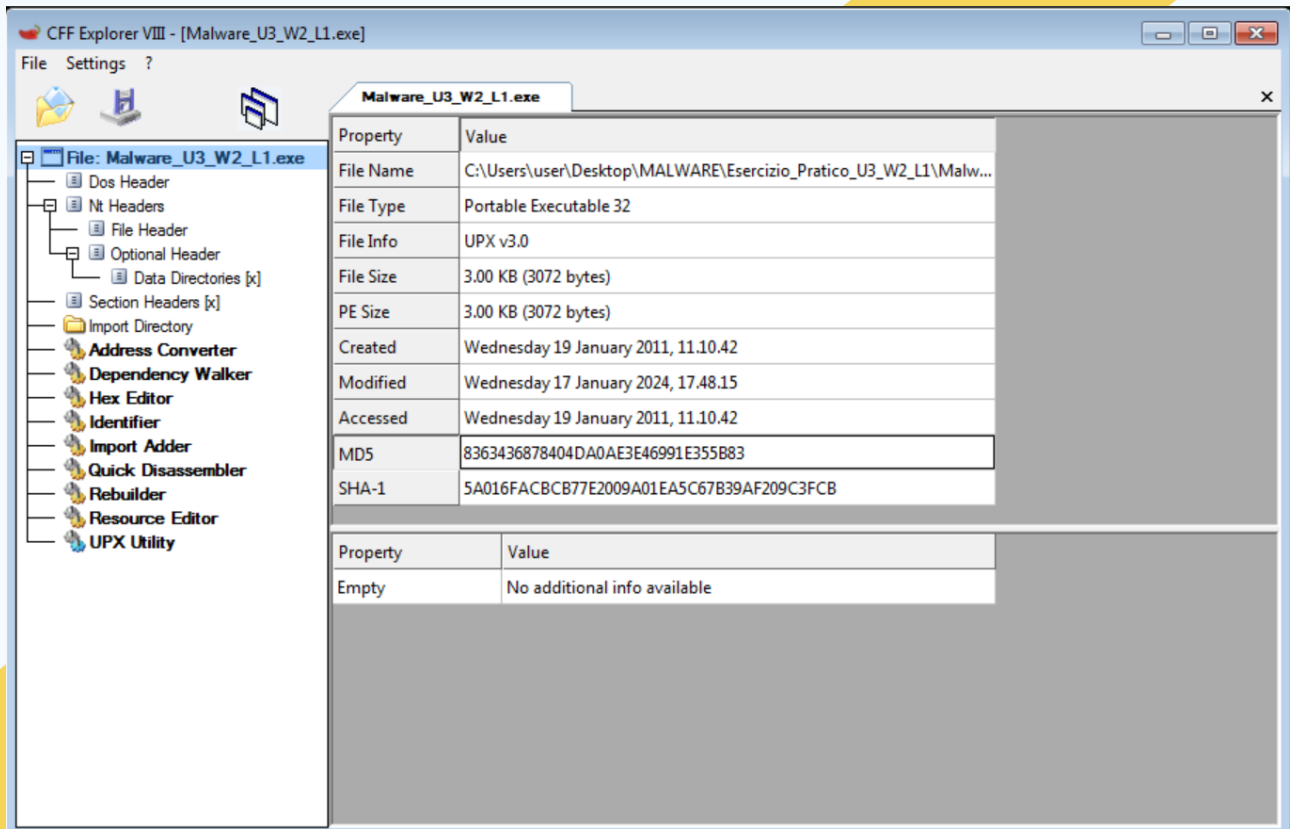
## 2. Sezioni del Malware:

- Sezioni Codificate: All'interno del malware sono presenti tre sezioni il cui contenuto è codificato e non immediatamente leggibile. Queste sezioni potrebbero contenere dati crittografati o codificati utilizzati per scopi non rivelati.



## Analisi con VirusTotal:

Dopo aver ottenuto il checksum MD5 del file tramite Ash, lo abbiamo caricato su VirusTotal per eseguire una scansione antivirus e un'ulteriore analisi. Abbiamo confrontato le informazioni fornite da VirusTotal con quelle ottenute da CFF Explorer per identificare eventuali discrepanze.



## Risultati dell'Analisi:

- Le informazioni sulle librerie importate segnalate da CFF Explorer corrispondono a quelle segnalate da VirusTotal, confermando la coerenza delle informazioni fornite da entrambi gli strumenti.

- Non sono state identificate discrepanze tra le librerie segnalate da CFF Explorer e quelle segnalate da VirusTotal.

Security vendors' analysis

AhnLab-V3	Trojan.Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Generic.47e7b5e4
AliCloud	Backdoor	ALYac	Trojan.Startpage.3072
Antiy-AVL	Trojan.Win32.SGeneric	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.36802.amGfaWi867f
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Malware.Agent-6350563-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.878404
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInSight	MALICIOUS	DrWeb	Trojan.Click3.12740
Elastic	Malicious (moderate Confidence)	Emsisoft	Gen:Variant.Ser.Ulisse.216 (B)
eScan	Gen:Variant.Ser.Ulisse.216	ESET-NOD32	Win32/TrojanClicker.Agent.NVM
Fortinet	W32/Agent.NVMtr	GData	Gen:Variant.Ser.Ulisse.216
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Downloader.sdlis2
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.fslq
Kingsoft	Win32.troj.undef.a	Lionic	Trojan.Win32.Zbot.LsXA
Malwarebytes	Trojan.Agent.UPIX	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Generic.alt

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	Ch2
UPX0	4096	16384	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	20480	4096	1536	7.07	ad0f236c2b34f1031486c8cc4803a908	5848.3
UPX2	24576	4096	512	2.8	f998d25f473e69cc89b43af3102beea	53922

Imports

- KERNEL32.DLL
  - ExitProcess
  - GetProcAddress
  - LoadLibraryA
  - VirtualAlloc
  - VirtualFree
  - VirtualProtect
- ADVAPI32.dll
  - CreateServiceA
- MSVCRT.dll
  - exit
- WININET.dll
  - InternetOpenA

## Ipotesi di Funzionamento del Malware:

Basandoci sulle informazioni fornite dalle analisi, possiamo ipotizzare il seguente funzionamento del malware:

- Caricamento Dinamico di Librerie:** Il malware potrebbe caricare dinamicamente altre librerie utilizzando le funzioni di caricamento come **LoadLibraryA** e **GetProcAddress**. Questo potrebbe consentire al malware di estendere le sue funzionalità o di caricare moduli aggiuntivi per eseguire operazioni specifiche.
- Manipolazione della Memoria:** Le funzioni come **VirtualProtect**, **VirtualAlloc**, e **VirtualFree** potrebbero consentire al malware di manipolare la memoria del processo

corrente. Questo potrebbe essere utilizzato per eseguire tecniche di evasione delle protezioni o per nascondere parti del malware dalla rilevazione.

3. **Comunicazione su Internet:** La presenza della funzione **InternetOpenA** indica che il malware è in grado di inizializzare una sessione di comunicazione su Internet. Questo potrebbe consentire al malware di inviare o ricevere dati da server remoti, potenzialmente per scopi dannosi come il furto di informazioni o l'esecuzione di comandi remoti.
4. **Creazione di Servizi di Sistema:** La funzione **CreateServiceA** potrebbe consentire al malware di creare un nuovo servizio di sistema o aprire un servizio esistente. Questo potrebbe essere utilizzato per persistere nel sistema, eseguendo il malware automaticamente all'avvio del sistema o con privilegi elevati.
5. **Terminazione del Processo:** La funzione **ExitProcess** potrebbe consentire al malware di terminare il processo corrente e tutti i suoi thread in esecuzione. Questo potrebbe essere utilizzato per interrompere l'esecuzione di processi critici o per nascondere le tracce del malware dopo aver completato le sue attività.

#### **Considerazioni Finali:**

L'analisi del malware ha rivelato l'utilizzo di librerie importate comuni per operazioni di sistema, comunicazione su Internet e altro ancora. La presenza di sezioni codificate indica la presenza di dati o istruzioni non immediatamente leggibili, che richiedono ulteriori analisi per comprenderne appieno il contenuto e le potenziali minacce. Nonostante le informazioni fornite da CFF Explorer e VirusTotal siano