Attività di Analisi del Malware

Oggetto:

Sarà condiviso un malware relativamente innocuo da:
`https://github.com/Akir4d/The-MALWARE-Repo/blob/master/Spyware/butterflyondesktop.exe.zip`

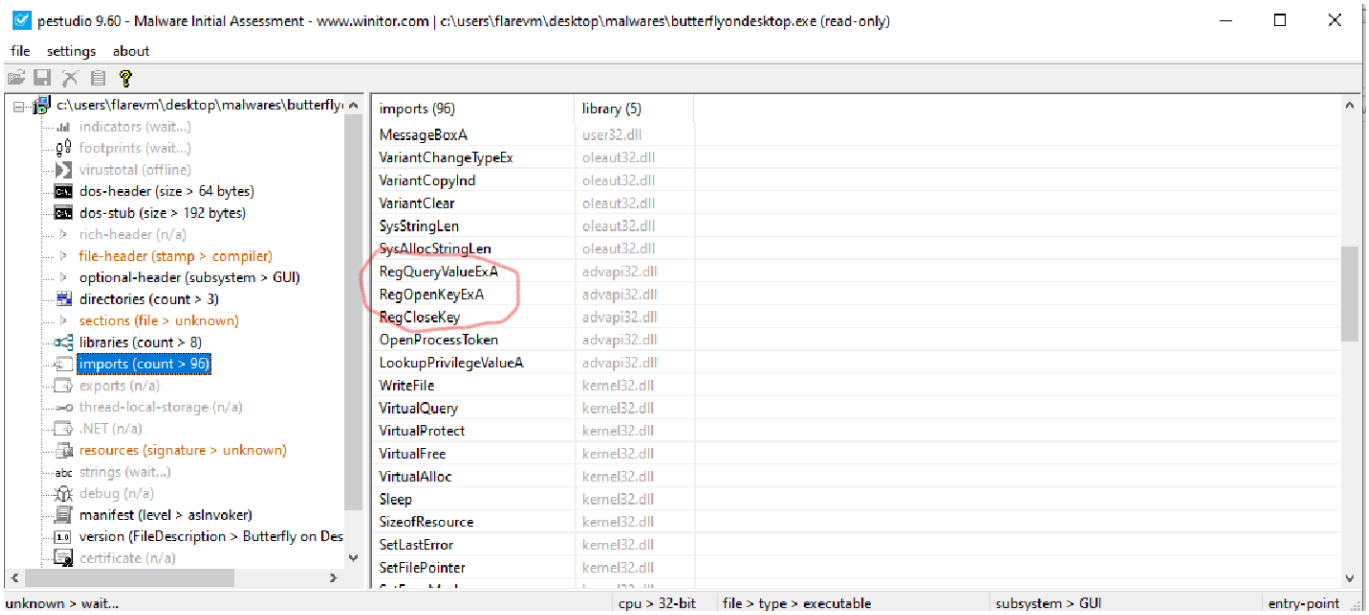
Compiti:

1. **Analisi Statica**: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
2. **Analisi Dinamica:** Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Analisi del malware

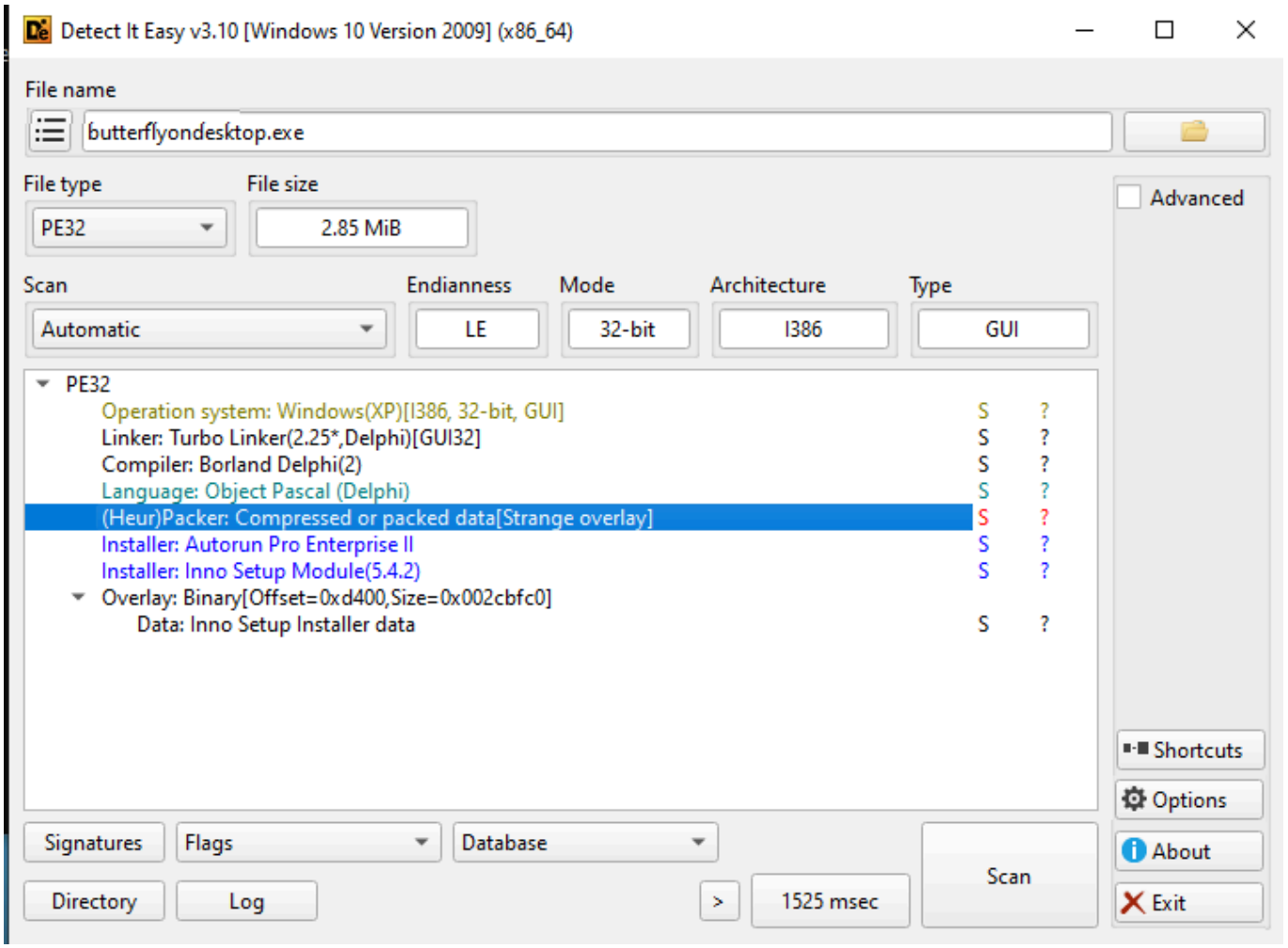
1. Uso di PE Studio

E' stato caricato l'eseguibile sullo strumento PE Studio e la prima cosa saltata all'occhio e' l'alto numero di import, come le API di windows e moduli come virtualAlloc, o moduli per scrittura e lettura di file:



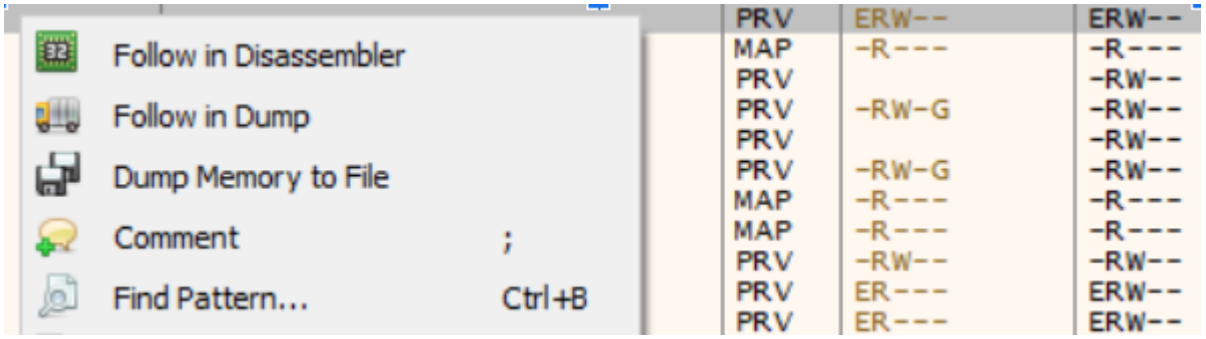
2. Uso di DIE (Detect it easy)

Il software ha rilevato una compressione o un impacchettamento, quindi sarà necessario agire di conseguenza per poi analizzarne il comportamento staticamente.



3. Analisi del Dump

Si fa il dump di una sezione sospetta della memory map usando **x32dbg**, ipotizzando che contenga la parte malevola del file, cliccando su "`dump memory to file`"



Successivamente sono state trovate tramite ghidra alcune stringhe che confermano l'uso di un loader per camuffare il codice malevolo:

402a	NtOpenProcess	"NtOpenProcess"	ds
403a	RtlDosPathNameToNtPat...	"RtlDosPathNameToNtPa...	ds
405a	NtAllocateVirtualMemory	"NtAllocateVirtualMemory"	ds
4074	NtReadVirtualMemory	"NtReadVirtualMemory"	ds

4. Analisi dinamica con regshot

Regshot come dice il nome fa due istantanee dei registri di windows per poi confrontarle. Avviamo il malware a cavallo tra le istantanee e poi le confrontiamo.
Si possono leggere vari riferimenti a browser come google chrome, probabilmente per cercare di recuperare delle password salvate.

```
---------------------------------
Keys added: 10
---------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\3d82dbc9-9681-4562-a43f-ca70bb1a6c9f
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\3d82dbc9-9681-4562-a43f-ca70bb1a6c9f
HKU\S-1-5-21-254094793-3860855394-4186930808-1001\SOFTWARE\Google\Chrome\ThirdParty
HKU\S-1-5-21-254094793-3860855394-4186930808-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManag
HKU\S-1-5-21-254094793-3860855394-4186930808-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManag
HKU\S-1-5-21-254094793-3860855394-4186930808-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManag
HKU\S-1-5-21-254094793-3860855394-4186930808-1001\SOFTWARE\ButterflyOnDesktop

---------------------------------
Values added: 40
---------------------------------
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SRUM\Telemetry\ScreenOnLatestAnalyzedSessionTimestamp: 0x01DBCF0F1EA60E6D
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: Setup Version: "5.4.2 (a)"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: App Path: "C:\Program Files (x86)\Butterfly on Desktop"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\InstallLocation: "C:\Program Files (x86)\Butterfly on Desktop\"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: Icon Group: "Butterfly on Desktop"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: User: "FlareVM"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: Selected Tasks: ""
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: Deselected Tasks: "butterflyondesktop"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Inno Setup: Language: "eng"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\DisplayName: "Butterfly on Desktop 1.0"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\UninstallString: ""C:\Program Files (x86)\Butterfly on Desktop\unins000.exe""
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\QuietUninstallString: ""C:\Program Files (x86)\Butterfly on Desktop\unins000.exe"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\Publisher: "Drive Software Company"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\URLInfoAbout: "http://www.freedesktopsoft.com"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1\HelpLink: "http://www.drive-software.com"
```