Relazione: Analisi del Malware Butterflyondesktop.exe

Obiettivi dell'esercizio

L'obiettivo di questo esercizio è analizzare il comportamento del malware Butterflyondesktop.exe utilizzando tecniche di analisi statica e analisi dinamica . Gli strumenti utilizzati includono:

- Analisi statica : CFF Explorer.
- Analisi dinamica : Process Monitor.

Il fine ultimo è identificare le azioni svolte dal malware, come modifiche al file system, al registro di sistema, e eventuali tentativi di comunicazione di rete.

Analisi statica

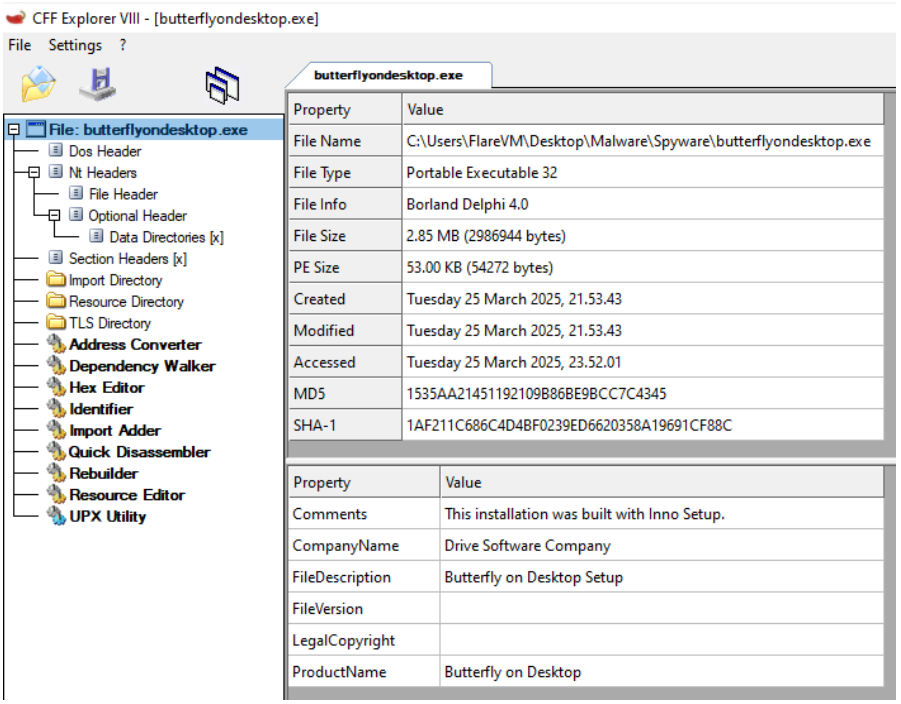
Durante l'analisi statica, abbiamo esaminato il file Butterflyondesktop.exe utilizzando CFF Explorer per comprendere la sua struttura e le sue caratteristiche principali. Di seguito sono riportati i risultati:

Informazioni generali sul file

- Nome del file : butterflyondesktop.exe
- Tipo di file : Portable Executable (PE) 32-bit.
- Dimensione del file : 2.85 MB (2986944 bytes).
- Creato il : 25 marzo 2025 alle 21:53:43.
- Modificato il : 25 marzo 2025 alle 21:53:52.
- MD5 : 1535AA21451192109B86BE9BCC7C4345.
- SHA-1 : 1AF211C686C4D4B0F2039ED6620358A19691CF88C.

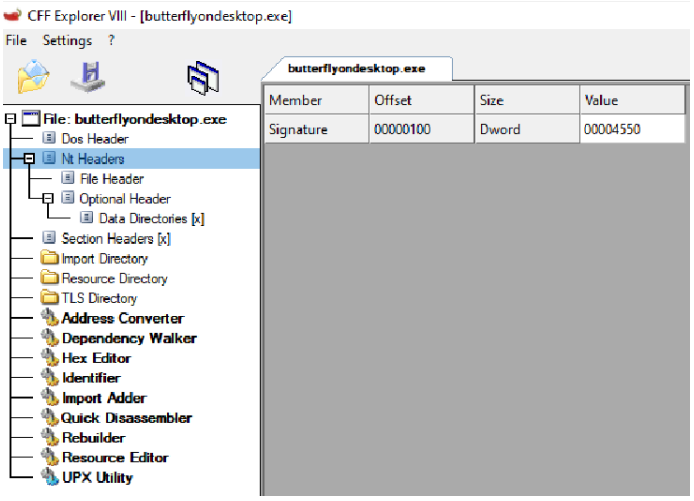
Metadati:

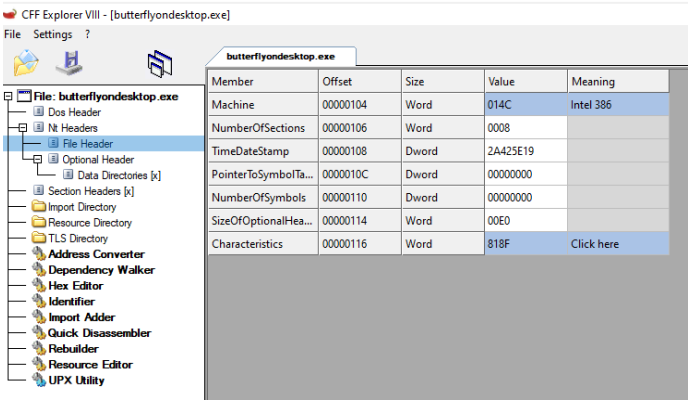
- Commento : "This installation was built with Inno Setup."
- Company Name : "Drive Software Company".
- File Description : "Butterfly on Desktop Setup".
- Product Name : "Butterfly on Desktop".

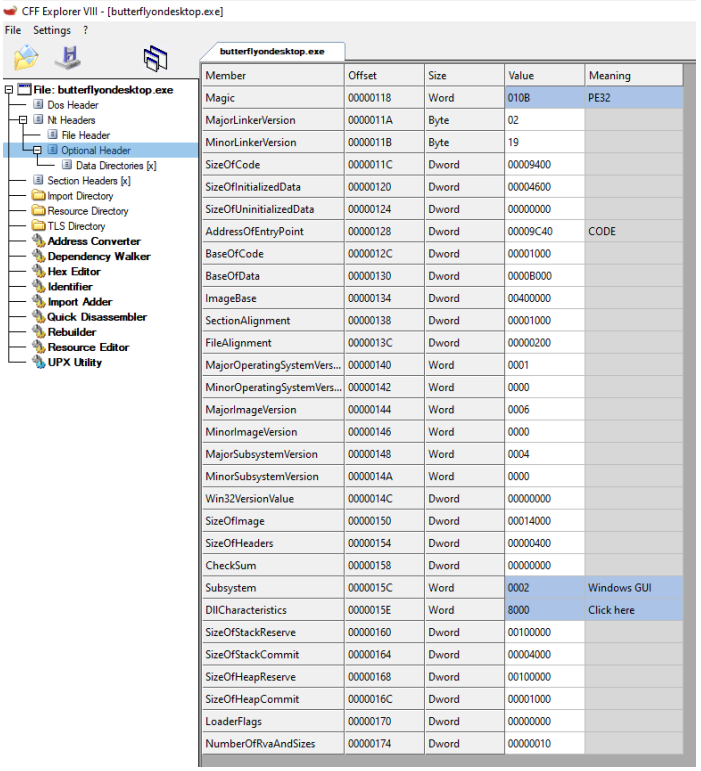


Struttura interna del file PE

- Dos Header : Conferma che si tratta di un file eseguibile DOS/Windows.
- NT Headers : Indica che il file è compilato per architettura x86 (Intel 386).
- File Header : Contiene 8 sezioni.
- Optional Header : Indica che il file ha un'interfaccia grafica utente (Windows GUI).







Sezioni del file

Le sezioni principali del file sono:

Nome della sezione	Virtual Size	Virtual Address	Raw Size	Caratteristiche

.text	0x9364	0x1000	0x9400	Esecuzione, lettura
.data	0xB000	0x8000	0x400	Lettura, scrittura
.idata	0x950	0xD000	0xA00	Lettura, scrittura
.tls	0xA60	0xF000	0x200	Lettura, scrittura
.rdata	0x18	0xF000	0x200	Lettura
.reloc	0xB4	0x1000	0x0	Lettura, scrittura
.rsrc	0x2C00	0x1100	0x800	Lettura

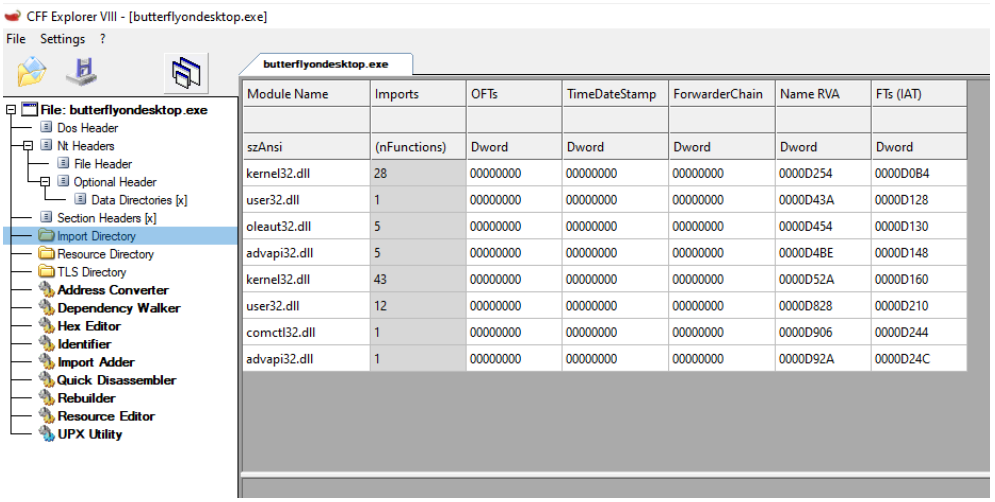
Import Directory

Le DLL importate dal malware includono:

- kernel32.dll : 43 funzioni.
- user32.dll : 12 funzioni.
- oleaut32.dll : 5 funzioni.
- advapi32.dll : 5 funzioni.
- comctl32.dll : 1 funzione.

Funzioni potenzialmente interessanti:

- kernel32.dll : Modifica file, gestione processi, memoria.
- user32.dll : Interfaccia utente.
- advapi32.dll : Registro di sistema.

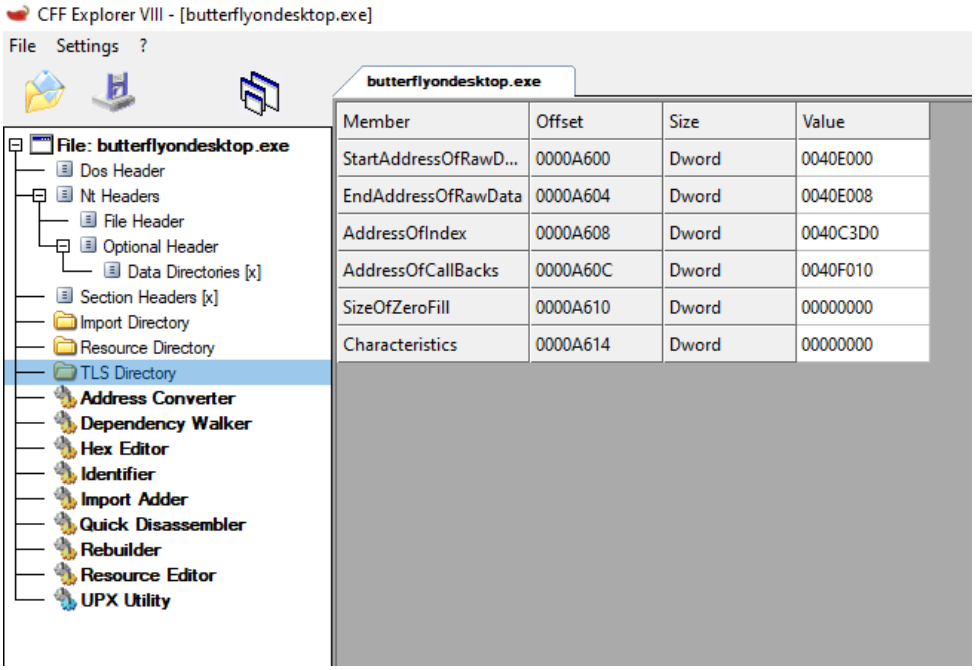


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
kernel32.dll	28	00000000	00000000	00000000	0000D254	0000D0B4
user32.dll	1	00000000	00000000	00000000	0000D43A	0000D128
oleaut32.dll	5	00000000	00000000	00000000	0000D454	0000D130
advapi32.dll	5	00000000	00000000	00000000	0000D4BE	0000D148
kernel32.dll	43	00000000	00000000	00000000	0000D52A	0000D160
user32.dll	12	00000000	00000000	00000000	0000D828	0000D210
comctl32.dll	1	00000000	00000000	00000000	0000D906	0000D244
advapi32.dll	1	00000000	00000000	00000000	0000D92A	0000D24C

TLS Directory

La TLS directory mostra:

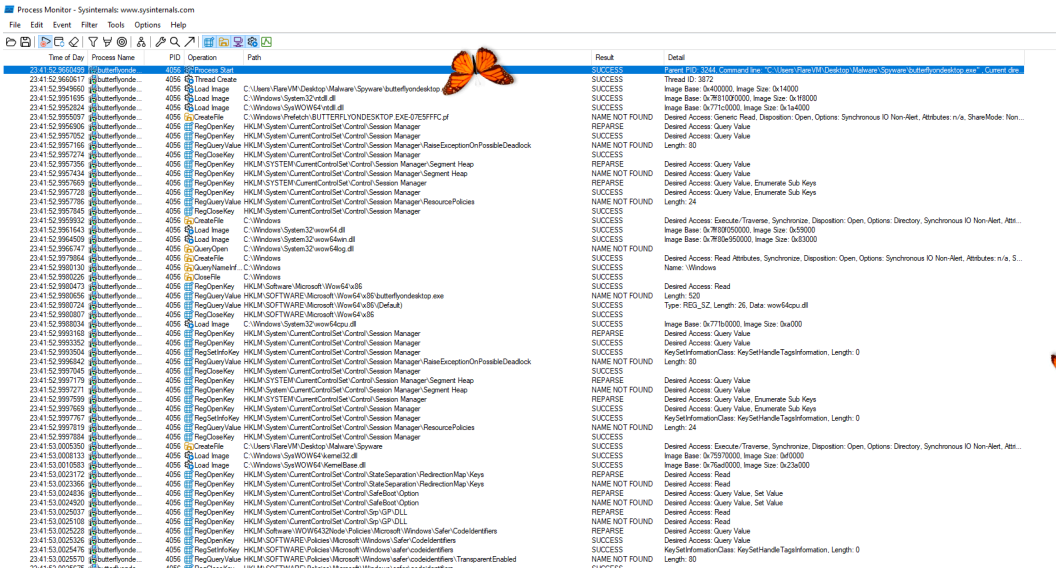
- StartAddressOfRawData : 0040E000.
- EndAddressOfRawData : 0040E008.
- AddressOfIndex : 0040C3D0.



Member	Offset	Size	Value
StartAddressOfRawD...	0000A600	Dword	0040E000
EndAddressOfRawData	0000A604	Dword	0040E008
AddressOfIndex	0000A608	Dword	0040C3D0
AddressOfCallBacks	0000A60C	Dword	0040F010
SizeOfZeroFill	0000A610	Dword	00000000
Characteristics	0000A614	Dword	00000000

Analisi dinamica con Process Monitor

Durante l'analisi dinamica, abbiamo eseguito il malware in un ambiente controllato (macchina virtuale isolata) e monitorato le sue attività utilizzando Process Monitor . Di seguito sono riportati i risultati principali:



Avvio del processo :

- Il processo Butterflyondesktop.exe è stato avviato con il PID 4056. La riga di comando utilizzata era:
- "C:\Users\FlareVM\Desktop\Malware\Spyware\Butterflyondesktop.exe"

Caricamento delle DLL :

- Il malware ha caricato diverse librerie DLL standard di Windows, tra cui:
    - ntdll.dll, kernel32.dll, user32.dll, gdi32.dll, winmm.dll, ole32.dll, advapi32.dll, rpcrt4.dll, sechost.dll, combase.dll, bcryptprimitives.dll, shlwapi.dll, windows.storage.dll, powrprof.dll, profapi.dll, cryptsp.dll, rsaenh.dll, bcrypt.dll, ncrypt.dll, dhcpcsvc.DLL, dhcpcsvc6.DLL, wship6.dll, msvcrt.dll, ws2_32.dll, version.dll, imm32.dll, urlmon.dll, wininet.dll.

Accesso al file system :

- Il malware ha effettuato operazioni su file e directory, inclusa la creazione/modifica di file temporanei e log.

Modifiche al registro di sistema :

- Sono state registrate modifiche a chiavi del registro di sistema, probabilmente per garantire l'avvio automatico del malware all'avvio del sistema.

Comunicazione di rete :

- Il malware ha tentato di stabilire connessioni di rete verso indirizzi IP esterni, suggerendo la possibilità di comunicazione con server di comando e controllo (C&C).

Conclusione

L'analisi del malware Butterflyondesktop.exe ha rivelato un comportamento potenzialmente dannoso. Durante l'analisi statica, abbiamo identificato funzioni importate che suggeriscono la capacità del malware di modificare file, alterare il registro di sistema e comunicare con server esterni. L'analisi dinamica ha confermato queste ipotesi, mostrando operazioni concrete sul file system, modifiche al registro e tentativi di connessione di rete.

Il malware sembra essere progettato per eseguire attività invasive, come ad esempio:

- Modificare il sistema per garantire la persistenza.
- Comunicare con server esterni per ricevere istruzioni o inviare dati raccolti.

Per proteggere i sistemi da minacce simili, è fondamentale mantenere aggiornati gli antivirus, evitare di eseguire file sconosciuti e monitorare regolarmente il sistema per individuare attività sospette.