

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

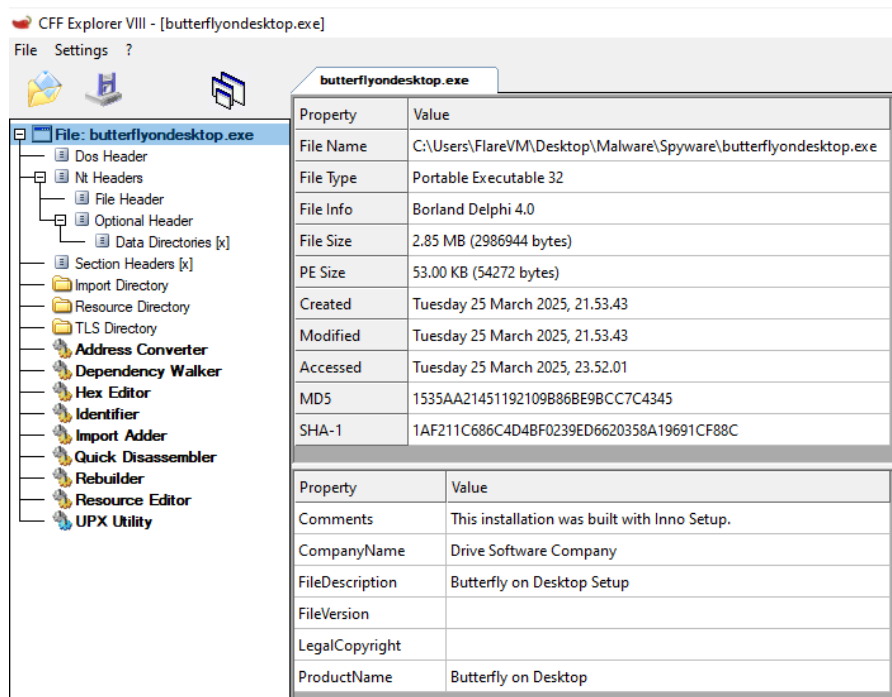
Durante l'analisi statica, abbiamo esaminato il file Butterflyondesktop.exe utilizzando CFF Explorer per comprendere la sua struttura e le sue caratteristiche principali. Di seguito sono riportati i risultati:

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.

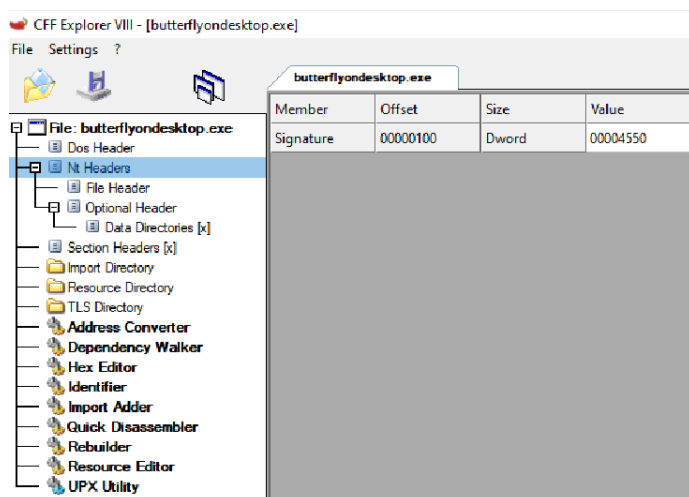
Metadati:

- 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).



CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Member	Offset	Size	Value	Meaning
Machine	00000104	Word	014C	Intel 386
NumberOfSections	00000106	Word	0008	
TimeDateStamp	00000108	Dword	2A425E19	
PointerToSymbolTable	0000010C	Dword	00000000	
NumberOfSymbols	00000110	Dword	00000000	
SizeOfOptionalHeader	00000114	Word	00E0	
Characteristics	00000116	Word	818F	Click here

File: butterflyondesktop.exe

- Dos Header
- NT Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- TLS Directory
- Address Converter
- Dependency Walker
- Hax Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Member	Offset	Size	Value	Meaning
Magic	00000118	Word	010B	PE32
MajorLinkerVersion	0000011A	Byte	02	
MinorLinkerVersion	0000011B	Byte	19	
SizeOfCode	0000011C	Dword	00009400	
SizeOfInitializedData	00000120	Dword	00004600	
SizeOfUninitializedData	00000124	Dword	00000000	
AddressOfEntryPoint	00000128	Dword	00009C40	CODE
BaseOfCode	0000012C	Dword	00001000	
BaseOfData	00000130	Dword	0000B000	
ImageBase	00000134	Dword	00400000	
SectionAlignment	00000138	Dword	00001000	
FileAlignment	0000013C	Dword	00000200	
MajorOperatingSystemVersion	00000140	Word	0001	
MinorOperatingSystemVersion	00000142	Word	0000	
MajorImageVersion	00000144	Word	0006	
MinorImageVersion	00000146	Word	0000	
MajorSubsystemVersion	00000148	Word	0004	
MinorSubsystemVersion	0000014A	Word	0000	
Win32VersionValue	0000014C	Dword	00000000	
SizeOfImage	00000150	Dword	00014000	
SizeOfHeaders	00000154	Dword	00000400	
Checksum	00000158	Dword	00000000	
Subsystem	0000015C	Word	0002	Windows GUI
DllCharacteristics	0000015E	Word	8000	Click here
SizeOfStackReserve	00000160	Dword	00100000	
SizeOfStackCommit	00000164	Dword	00004000	
SizeOfHeapReserve	00000168	Dword	00100000	
SizeOfHeapCommit	0000016C	Dword	00001000	
LoaderFlags	00000170	Dword	00000000	
NumberOfRvaAndSizes	00000174	Dword	00000010	

File: butterflyondesktop.exe

- Dos Header
- NT Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- TLS Directory
- Address Converter
- Dependency Walker
- Hax Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

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

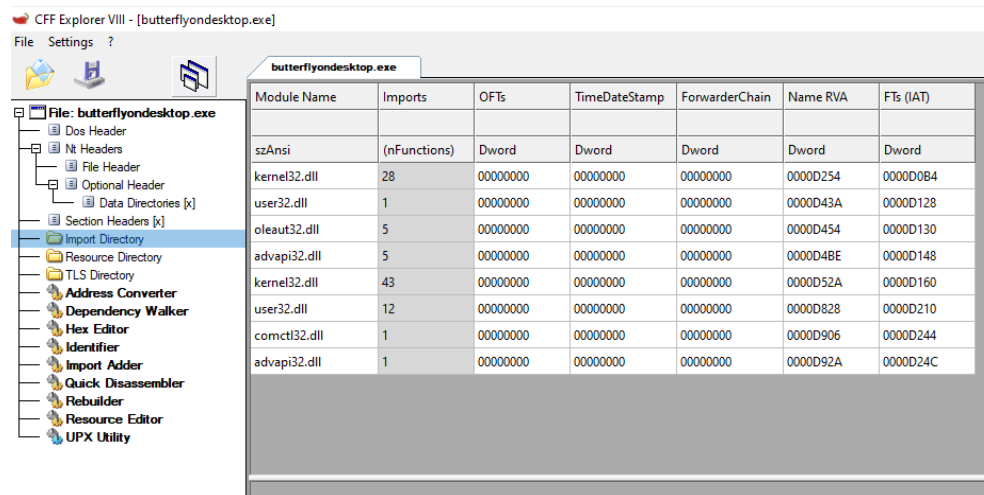
Import Directory

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:

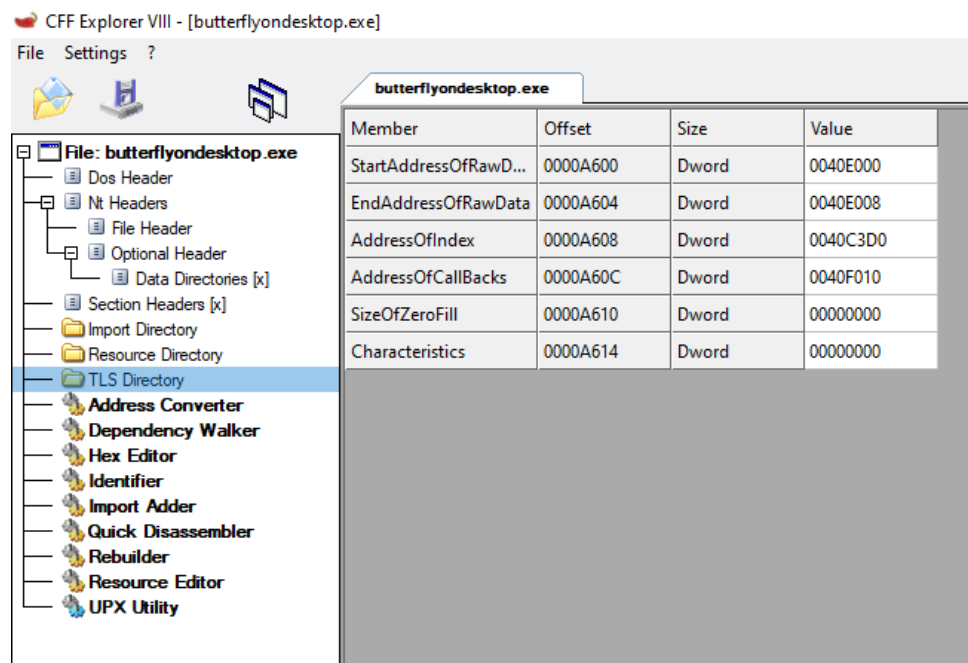
- kernel32.dll : Modifica file, gestione processi, memoria.
- user32.dll : Interfaccia utente.
- advapi32.dll : Registro di sistema.



TLS Directory

La TLS directory mostra:

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



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:

Process Monitor - Sysinternals www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
23:41:52.950293	Butterflyondesktop.exe	4056	Process Start		SUCCESS	Process PID: 3258, Command line: "C:\Users\FilareVM\Desktop\Malware\Spyware\Butterflyondesktop.exe" - Current dir...
23:41:52.960617	Butterflyondesktop.exe	4056	Thread Create		SUCCESS	Thread ID: 3872
23:41:52.964900	Butterflyondesktop.exe	4056	Load Image	C:\Users\FilareVM\Desktop\Malware\Spyware\Butterflyondesktop.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x14000
23:41:52.995195	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x781000000, Image Size: 0x95000
23:41:52.995204	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x771c0000, Image Size: 0x1a400
23:41:52.995507	Butterflyondesktop.exe	4056	CreateFile	C:\Windows\Prefetch\BUTTERFLYONDDESKTOP_EXE_0758FFC1.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Non...
23:41:52.995606	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
23:41:52.996700	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
23:41:52.995716	Butterflyondesktop.exe	4056	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\PhaseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 0
23:41:52.995714	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
23:41:52.995756	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
23:41:52.995744	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Query Value
23:41:52.995760	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
23:41:52.995728	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
23:41:52.995778	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
23:41:52.995745	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
23:41:52.995932	Butterflyondesktop.exe	4056	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, S...
23:41:52.996143	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x780000000, Image Size: 0x95000
23:41:52.996450	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\wow64api.dll	SUCCESS	Image Base: 0x780000000, Image Size: 0x95000
23:41:52.996717	Butterflyondesktop.exe	4056	CreateFile	C:\Windows	NAME NOT FOUND	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, S...
23:41:52.997884	Butterflyondesktop.exe	4056	CreateFile	C:\Windows	SUCCESS	Desired Access: Read
23:41:52.998020	Butterflyondesktop.exe	4056	CreateFile	C:\Windows	SUCCESS	Desired Access: Read
23:41:52.998028	Butterflyondesktop.exe	4056	CreateFile	C:\Windows	SUCCESS	Desired Access: Read
23:41:52.9980473	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\Software\Microsoft\Wow64\OS	NAME NOT FOUND	Length: 120
23:41:52.998056	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Wow64\OS\Butterflyondesktop.exe	NAME NOT FOUND	Length: 120
23:41:52.9980724	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Wow64\OS (Default)	SUCCESS	Type: REG_SZ, Length: 26, Data: wow64api.dll
23:41:52.998007	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SOFTWARE\Microsoft\Wow64\OS	SUCCESS	Image Base: 0x77b00000, Image Size: 0xa000
23:41:52.998034	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\wow64api.dll	SUCCESS	Desired Access: Query Value
23:41:52.998103	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
23:41:52.998352	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
23:41:52.998304	Butterflyondesktop.exe	4056	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: KeySetHandleTagInformation, Length: 0
23:41:52.998642	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\PhaseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 0
23:41:52.9957945	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
23:41:52.9977179	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
23:41:52.997721	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Query Value
23:41:52.997739	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
23:41:52.997850	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
23:41:52.997777	Butterflyondesktop.exe	4056	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: KeySetHandleTagInformation, Length: 0
23:41:52.997879	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
23:41:52.997854	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
23:41:53.000530	Butterflyondesktop.exe	4056	CreateFile	C:\Users\FilareVM\Desktop\Malware\Spyware	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, S...
23:41:53.0008113	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77070000, Image Size: 0x95000
23:41:53.0010983	Butterflyondesktop.exe	4056	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77070000, Image Size: 0x95000
23:41:53.0023172	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	REPARSE	Desired Access: Read
23:41:53.0023366	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	NAME NOT FOUND	Desired Access: Read
23:41:53.0024036	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	REPARSE	Desired Access: Query Value, Set Value
23:41:53.0024030	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	REPARSE	Desired Access: Query Value, Set Value
23:41:53.0025037	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	REPARSE	Desired Access: Read
23:41:53.0025100	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectorMap\Keys	NAME NOT FOUND	Desired Access: Read
23:41:53.0025238	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE	Desired Access: Query Value
23:41:53.0025206	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
23:41:53.0025476	Butterflyondesktop.exe	4056	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	KeySetInformationClass: KeySetHandleTagInformation, Length: 0
23:41:53.0025570	Butterflyondesktop.exe	4056	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	NAME NOT FOUND	Length: 0

Avvio del processo :

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