

RAPPORTO

Static Analysis

Per prima cosa ho generato diversi hash del malware e poi ho cercato SHA256 in Virus Total. Mi ha mostrato una possibilità di Trojan:

The image shows a Windows PowerShell terminal window with the following commands and output:

```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti sono riservati.

Il caricamento dei profili personali e di sistema ha richiesto 556 ms.
FLARE-VM 01/18/2025 21:07:58
PS C:\Users\flarevm> Get-FileHash -Path "C:\Users\flarevm\Desktop\butterflyondesktop.exe" -Algorithm SHA256

Algorithm      Hash                                     Path
-----
SHA256         4641AF6A0071E11E13AD3B1CD950E01300542C2B9EFB6AE92FFECEDDE974A4A6  C:\Users\flarevm\Desktop\butt...

FLARE-VM 01/18/2025 21:08:19
PS C:\Users\flarevm> Get-FileHash -Path "C:\Users\flarevm\Desktop\butterflyondesktop.exe" -Algorithm SHA1

Algorithm      Hash                                     Path
-----
SHA1          1AF211C686C4D48F0239ED6620358A19691CF88C  C:\Users\flarevm\Desktop\butterflyondesktop.exe

FLARE-VM 01/18/2025 21:10:18
PS C:\Users\flarevm> Get-FileHash -Path "C:\Users\flarevm\Desktop\butterflyondesktop.exe" -Algorithm MD5

Algorithm      Hash                                     Path
-----
MD5           1535AA21451192109B868E98CC7C4345  C:\Users\flarevm\Desktop\butterflyondesktop.exe
```

Below the terminal, the VirusTotal analysis results for the file `butterflyondesktop.exe` are shown. The file is flagged as malicious by 2/72 security vendors. The analysis details include:

- File name: `butterflyondesktop.exe`
- Size: 2.85 MB
- Last Analysis Date: 5 days ago
- SHA256: `4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6`
- Community Score: -12
- Tags: `peexe`, `direct-cpu-clock-access`, `runtime-modules`, `detect-debug-environment`, `overlay`, `long-sleeps`, `checks-user-input`, `persistence`

The detection results show the following security vendors' analysis:

Security vendors' analysis
Bkav Pro
W32.AIDetectMalware
Gridinsoft (no cloud)
Trojan.Win32.Gen.tr

Poi ho estratto le stringhe leggibili in un file di testo. Ho usato il file per filtrare le API call, gli URL e le chiavi di registro:

```
FLARE-VM 01/18/2025 21:18:29
PS C:\Users\flarevm\Desktop> strings C:\Users\flarevm\Desktop\butterflyondesktop.exe > strings_output.txt
FLARE-VM 01/18/2025 21:19:54
PS C:\Users\flarevm\Desktop>
>> Select-String -Path .\strings_output.txt -Pattern "http", ".com", ".net", ".org" | Out-File urls_output.txt
FLARE-VM 01/18/2025 21:28:22
PS C:\Users\flarevm\Desktop>
>> Select-String -Path .\strings_output.txt -Pattern "HKEY_" | Out-File registry_keys_output.txt
FLARE-VM 01/18/2025 21:29:10
PS C:\Users\flarevm\Desktop>
>> Select-String -Path .\strings_output.txt -Pattern "CreateProcess", "InternetOpen", "VirtualAlloc", "LoadLibrary" | Out-File api_calls_output.txt
```

```
urls_output.txt - Blocco note
File Modifica Formato Visualizza ?

strings_output.txt:4:Sysinternals - www.sysinternals.com
strings_output.txt:556:ECompressError
strings_output.txt:558:ECompressDataError
strings_output.txt:560:ECompressInternalError
strings_output.txt:564:TCompressDecompressor
strings_output.txt:567:TCompressedBlockReader
strings_output.txt:593:TLZMA1SmallDecompressorS
strings_output.txt:595:lzmdecsmall: Compressed data is corrupted (%d)
strings_output.txt:597:lzmdecsmall: %s
strings_output.txt:790:GetCommandLineA
strings_output.txt:852:GetCommandLineA
strings_output.txt:876:InitCommonControls
strings_output.txt:983:Application Error!Format '%s' invalid or incompatible with argument
strings_output.txt:1039:Drive Software Company
strings_output.txt:1053:<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
strings_output.txt:1064:         name="Microsoft.Windows.Common-Controls"
strings_output.txt:1072:<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
strings_output.txt:1079:<application xmlns="urn:schemas-microsoft-com:asm.v3">
strings_output.txt:1081:         <dpiAware xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">true</dpiAware>
strings_output.txt:1084:<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
strings_output.txt:1089:</compatibility>
strings_output.txt:72441:5NqORG
strings_output.txt:85207:oZ3oRGs

api_calls_output.txt - Blocco note
File Modifica Formato Visualizza ?

strings_output.txt:781:VirtualAlloc
strings_output.txt:823:VirtualAlloc
strings_output.txt:834:LoadLibraryA
strings_output.txt:858:CreateProcessA
```

Risultati principali dall'output di stringhe:

1. API call

- VirtualAlloc (righe 781, 823): comunemente utilizzato nei malware per allocare memoria durante l'esecuzione.
- LoadLibraryA (riga 834): suggerisce che il malware carica dinamicamente le librerie (possibilmente DLL).
- CreateProcessA (riga 858): indica la creazione di processi, potenzialmente per l'avvio di altri processi dannosi.
- GetCommandLineA (righe 790, 852): utilizzato per recuperare argomenti della riga di comando; il malware potrebbe basarsi su argomenti specifici per l'esecuzione.

2. Metadati incorporati

- Righe 1039: "Drive Software Company": potrebbe essere il nome originale o contraffatto dello sviluppatore.
- Righe 1053–1089: i metadati XML incorporati fanno riferimento a:
 - o Microsoft.Windows.Common-Controls (riga 1064): indica la dipendenza dai controlli Windows comuni.
 - o tag dpiAware (riga 1081): suggerisce un adattamento per display ad alta risoluzione, indicando forse un tentativo di apparire legittimo.

3. Messaggi di errore

- Righe 556–597: messaggi di errore come ECompressError e lzmadecompsmall: i dati compressi sono danneggiati (%d) puntano a routine di compressione/decompressione. Ciò potrebbe significare che il malware utilizza payload o dati compressi.

4. Stringhe sospette

- Righe 72441, 85207: stringhe dall'aspetto offuscato come 5NqORG e oZ3oRG. Potrebbero essere dati codificati (ad esempio, Base64 o codifica personalizzata).

5. URL

- <http://schemas.microsoft.com/SMI/2005/WindowsSettings> (riga 1081): sembra benigno ma richiede una convalida per confermare che non sia stato abusato.

Poi ho analizzato le strutture dei file utilizzando CFF Explorer:

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000A12A	N/A	00009C50	00009C54	00009C58	00009C5C	00009C60
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
kernel32.dll	28	00000000	00000000	00000000	0000D754	0000D084

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	0000D538	0000	WriteFile
N/A	0000D544	0000	VirtualQuery
N/A	0000D554	0000	VirtualProtect
N/A	0000D566	0000	VirtualFree
N/A	0000D574	0000	VirtualAlloc
N/A	0000D584	0000	Sleep
N/A	0000D58C	0000	SizeofResource
N/A	0000D59E	0000	SetLastError
N/A	0000D5AE	0000	SetFilePointer
N/A	0000D5C0	0000	SetErrorMode
N/A	0000D5D0	0000	SetEndOfFile
N/A	0000D5E0	0000	RemoveDirectoryA
N/A	0000D5F4	0000	ReadFile

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000A0BE	N/A	00009C3C	00009C40	00009C44	00009C48	00009C4C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
kernel32.dll	28	00000000	00000000	00000000	0000D254	0000D084
user32.dll	1	00000000	00000000	00000000	0000D43A	0000D128
oleaut32.dll	5	00000000	00000000	00000000	0000D454	0000D130
advapi32.dll	5	00000000	00000000	00000000	0000D48E	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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	0000D4CC	0000	RegQueryValueExA
N/A	0000D4E0	0000	RegOpenKeyExA
N/A	0000D4F0	0000	RegCloseKey
N/A	0000D4FE	0000	OpenProcessToken
N/A	0000D512	0000	LookupPrivilegeValueA

Principali risultati di CFF Explorer:

1. Funzioni correlate alla gestione della memoria:

- **VirtualAlloc, VirtualFree, VirtualProtect:** queste sono funzioni comuni utilizzate per l'allocazione e la protezione dinamica della memoria, spesso utilizzate dal malware per allocare memoria per shellcode o altri payload. Se il malware utilizza queste funzioni, potrebbe allocare ed eseguire codice in memoria.
- **VirtualQuery:** può essere utilizzata per interrogare le informazioni sulla memoria. Ciò potrebbe indicare un tentativo di raccogliere informazioni sulla memoria o evitare il rilevamento.

2. Funzioni correlate alle operazioni sui file:

- **WriteFile, ReadFile, SetFilePointer, SetEndOfFile:** queste sono funzioni standard per interagire con i file. Il malware potrebbe utilizzarle per scrivere payload su disco, leggere file o modificare i puntatori dei file per nascondere le proprie tracce.
- **RemoveDirectoryA:** questa funzione elimina le directory. Se utilizzata dal malware, potrebbe eliminare prove o file dannosi.
- **SizeofResource, LoadResource, LockResource, LoadLibraryA:** queste funzioni sono correlate alla gestione delle risorse e potrebbero indicare che il malware sta caricando risorse (probabilmente il suo payload) dall'interno dell'eseguibile o di altre risorse.

3. Funzioni correlate all'interfaccia utente di Windows e alla gestione dei messaggi:

- **MessageBoxA, MessageBoxW:** queste funzioni mostrano le caselle dei messaggi, che potrebbero essere utilizzate dal malware per l'interazione con l'utente o per visualizzare avvisi o messaggi falsi all'utente.
- **CreateWindowExA, DestroyWindow, SetWindowLongA, DispatchMessageA:** queste sono funzioni per creare, gestire e gestire le finestre. Il malware potrebbe utilizzarle per creare finestre nascoste o false per scopi dannosi.

4. Funzioni del registro:

- **RegOpenKeyExA, RegQueryValueExA, RegCloseKey:** queste funzioni vengono utilizzate per interagire con il registro di Windows. Il malware le utilizza comunemente per verificare determinate chiavi del registro, creare nuove chiavi del registro (per la persistenza) o modificare le impostazioni per mantenere la propria presenza nel sistema.
- ### 5. Funzioni di escalation dei privilegi e di sicurezza:

- **OpenProcessToken, LookupPrivilegeValueA, AdjustTokenPrivileges:** queste funzioni sono correlate alla modifica dei privilegi utente. Il malware può utilizzare queste funzioni per elevare i privilegi e ottenere l'accesso amministrativo.

6. Funzioni di sincronizzazione dei thread:

- **DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSection:** queste sono correlate alla sincronizzazione delle sezioni critiche. Queste funzioni aiutano a gestire i thread e possono essere utilizzate dal malware per controllare o bloccare l'accesso alle risorse condivise in un ambiente multithread.

7. Gestione dei processi e delle esecuzioni:

- **CreateWindowExA, ExitWindowsEx, PeekMessageA, MsgWaitForMultipleObjects:** queste funzioni sono correlate alla gestione di finestre o messaggi nella GUI e possono essere utilizzate dal malware per manipolare la GUI del sistema o mantenersi in esecuzione in background senza interazione dell'utente.

8. Altre importazioni sospette varie:

- **Sleep:** questa funzione mette in pausa l'esecuzione del programma. Il malware potrebbe usarla per ritardare le sue azioni o per evitare il rilevamento da parte di sandbox o software antivirus.

- **IsDBCSLeadByte:** questa funzione è usata per l'elaborazione del set di caratteri e potrebbe essere usata dal malware per manipolare o nascondere stringhe specifiche, il che potrebbe essere parte di tattiche di evasione.

Volevo usare GHIDRA per disassemblare il binario per un'ulteriore analisi, sfortunatamente il portatile non è riuscito a procedere e ha mostrato errori fatali. Per prova, i log degli errori sono riportati di seguito:

```
hs_err_pid3880.log - Blocco note
File Modifica Formato Visualizza ?

#
# A fatal error has been detected by the Java Runtime Environment:
#
# EXCEPTION_ACCESS_VIOLATION (0xc0000005) at pc=0x00000000b95ba40, pid=3880, tid=1108
#
# JRE version: OpenJDK Runtime Environment (21.0.1+12) (build 21.0.1+12-29)
# Java VM: OpenJDK 64-Bit Server VM (21.0.1+12-29, mixed mode, tiered, compressed oops, compressed class ptrs, g1 gc, windows-amd64)
# Problematic frame:
# J 6648 c1 sun.security.provider.MD5.GG(IIIIIII)I java.base@21.0.1 (27 bytes) @ 0x00000000b95ba40 [0x00000000b95ba40+0x0000000000000000]
#
# No core dump will be written. Minidumps are not enabled by default on client versions of Windows
#
# If you would like to submit a bug report, please visit:
# https://bugreport.java.com/bugreport/crash.jsp
#

----- S U M M A R Y -----

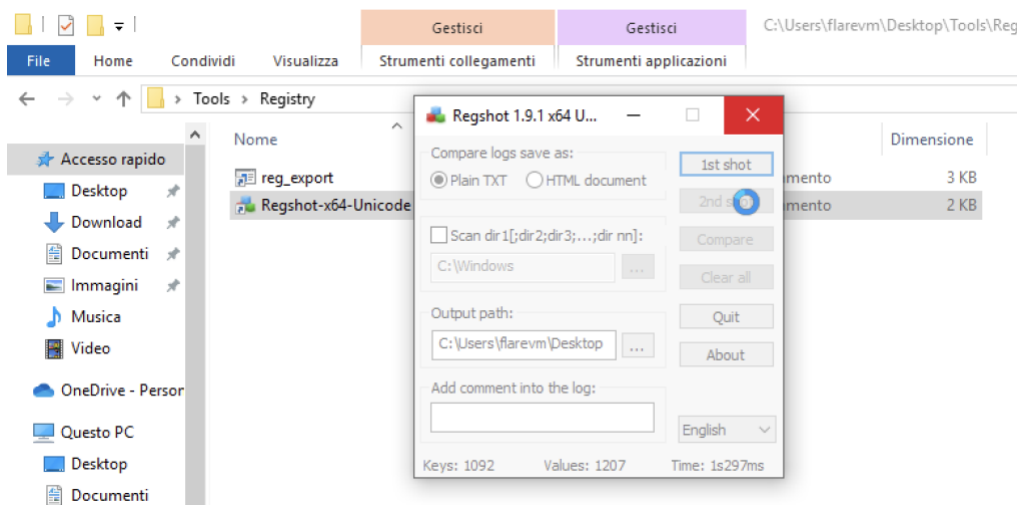
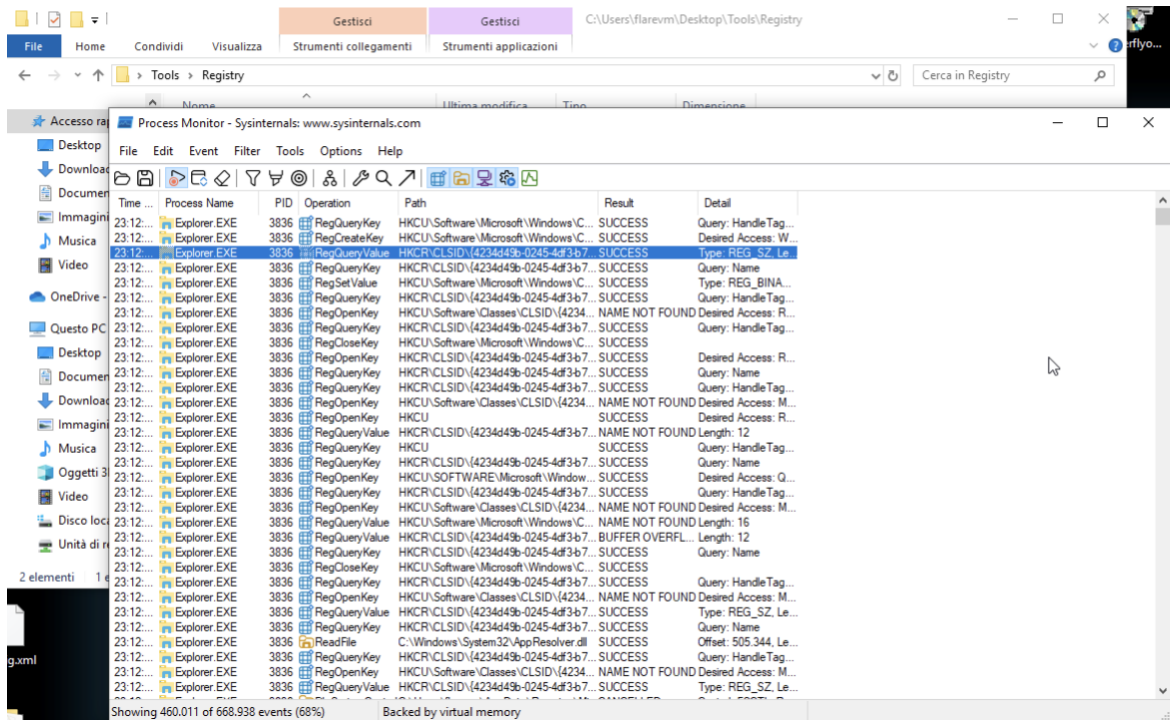
Command Line: -Duser.home=C:\Users\flarevm -Djava.system.class.loader=ghidra.GhidraClassLoader -Dfile.encoding=UTF8 -Duser.country=US -Duser.language=en -Duser.variant=-Dsun.
Host: Intel Core Processor (Skylake), 5 cores, 4G, Windows 10 , 64 bit Build 17763 (10.0.17763.1)
Time: Sat Jan 18 22:33:50 2025 ora solare Europa occidentale elapsed time: 206.952195 seconds (0d 0h 3m 26s)

----- T H R E A D -----

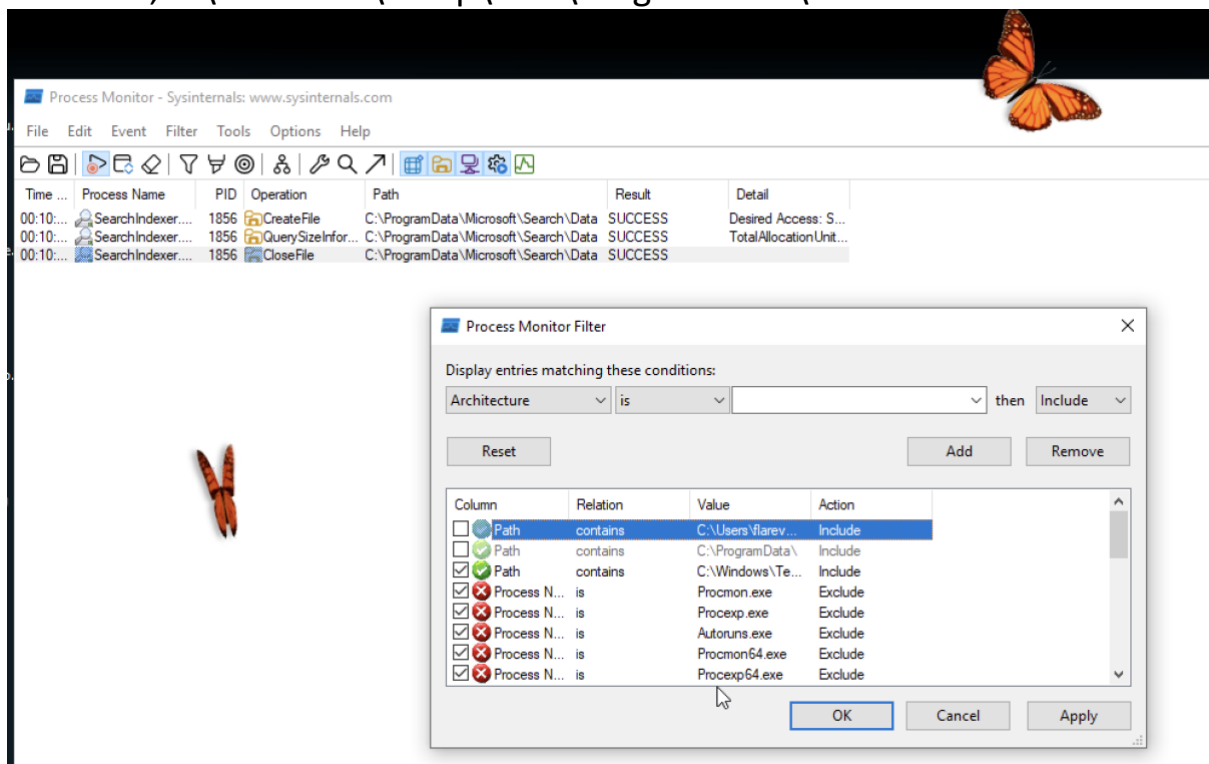
Current thread (0x000000002687eeb0): JavaThread "Task - Import" daemon [_thread_in_Java, id=1108, stack(0x000000002bd10000,0x000000002be10000) (1024K)]

Stack: [0x000000002bd10000,0x000000002be10000], sp=0x000000002be0ead8, free space=1018k
Native frames: (J=compiled Java code, j=interpreted, Vv=VM code, C=native code)
C 0x00000000b95ba40

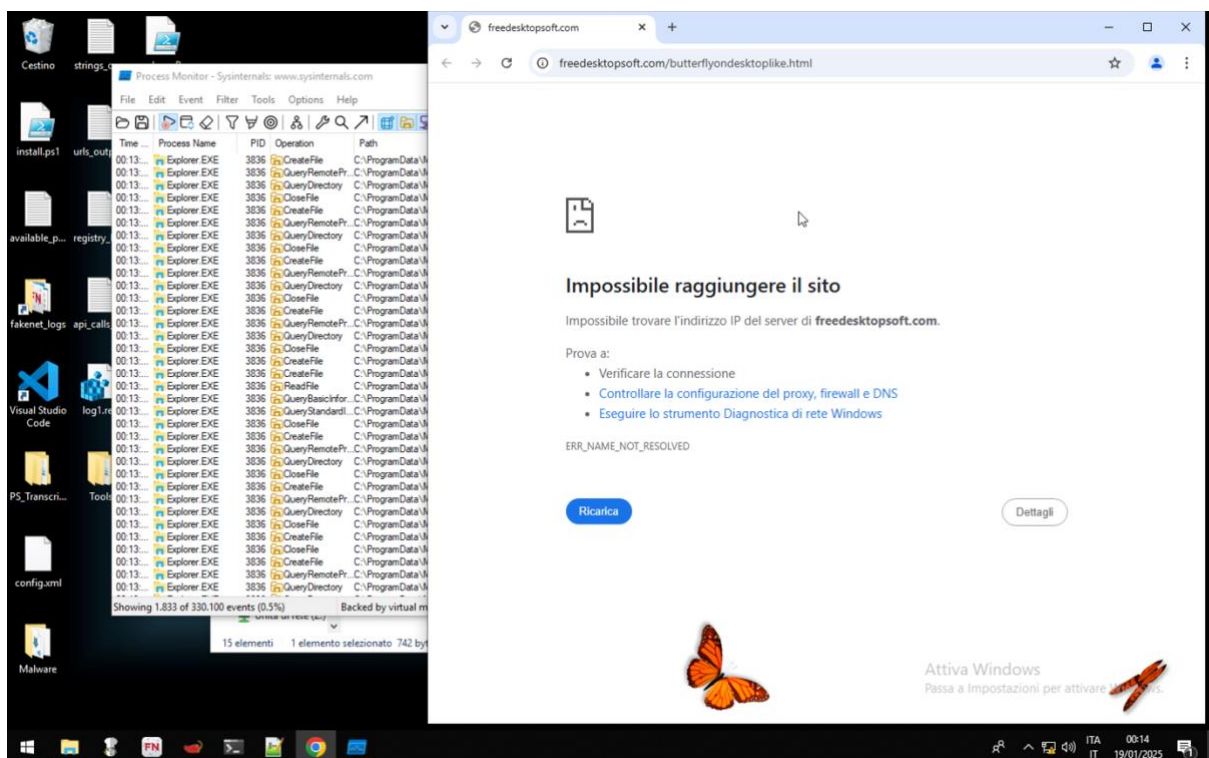
The last pc belongs to nmethod (printed below).
```

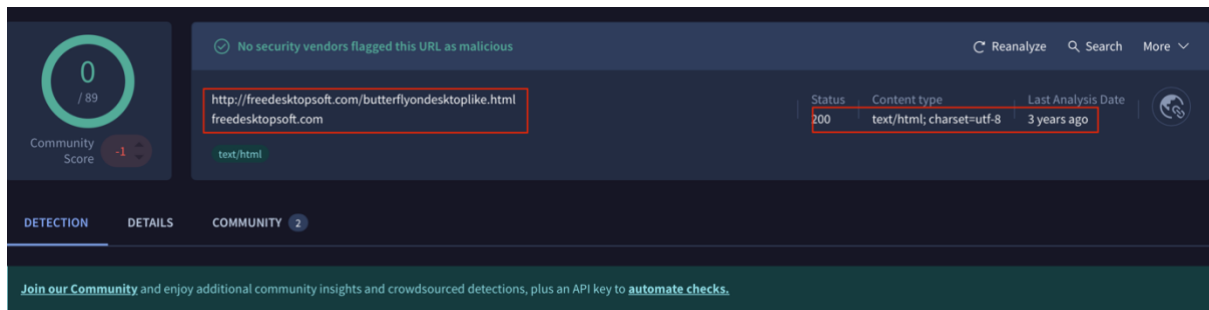
Quindi ho deciso di usare lo strumento che avevo aperto per primo, Process Monitor. L'ho filtrato per gli eventi contenenti i percorsi del malware, C:\Windows\Temp\ e C:\ProgramData\:



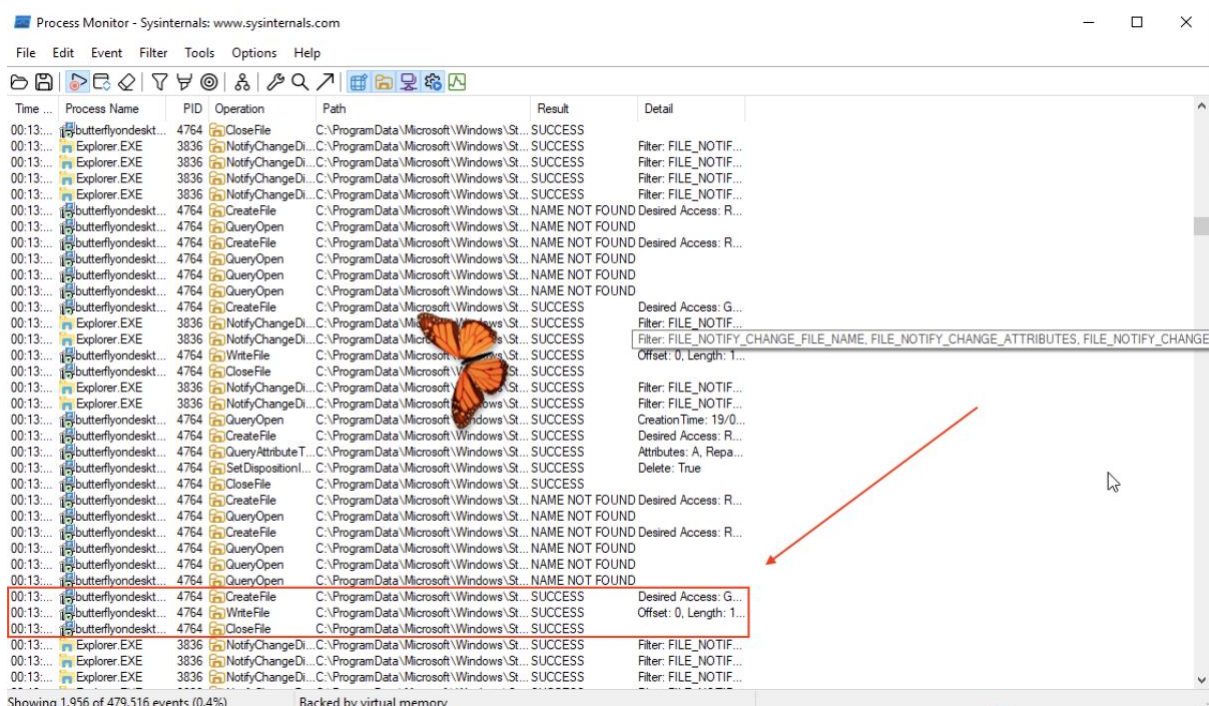
Poi stranamente è stata aperta una pagina web sul browser Chrome:



Quindi ho copiato l'URL e l'ho eseguito su Virus Total per analizzare qualsiasi traccia di malware, tuttavia tutto sembra ok. Era accessibile con il codice di stato 200. Quell'URL è stato scansionato 3 anni fa l'ultima volta...:



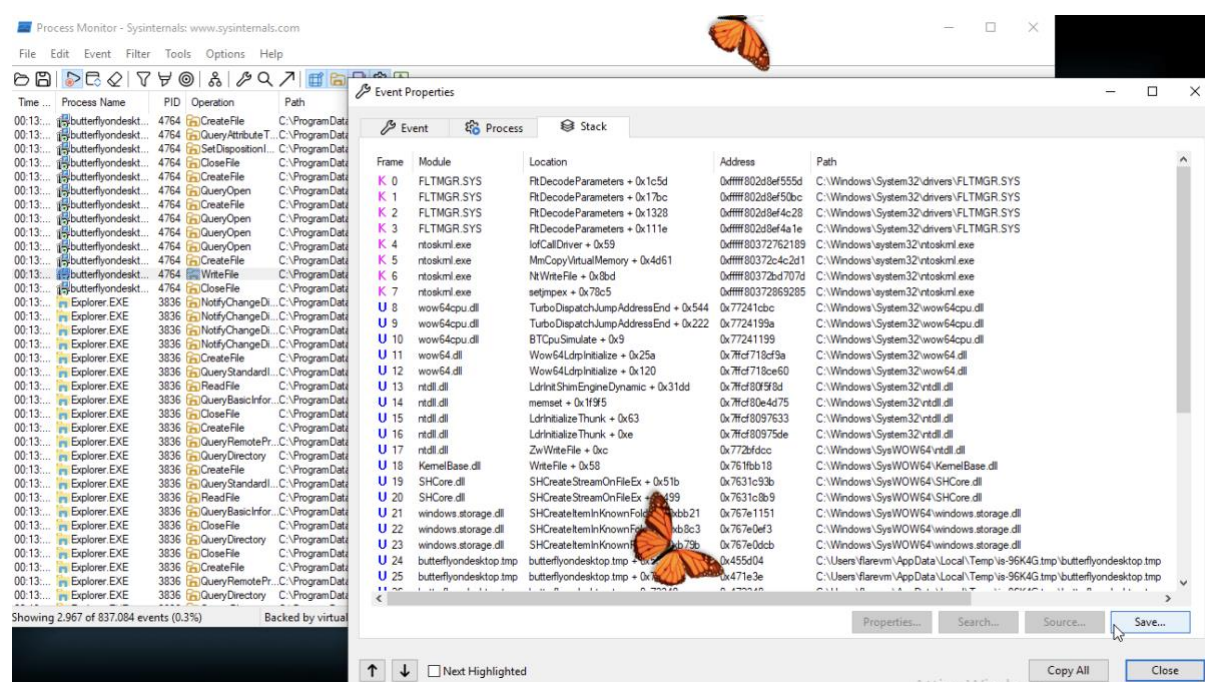
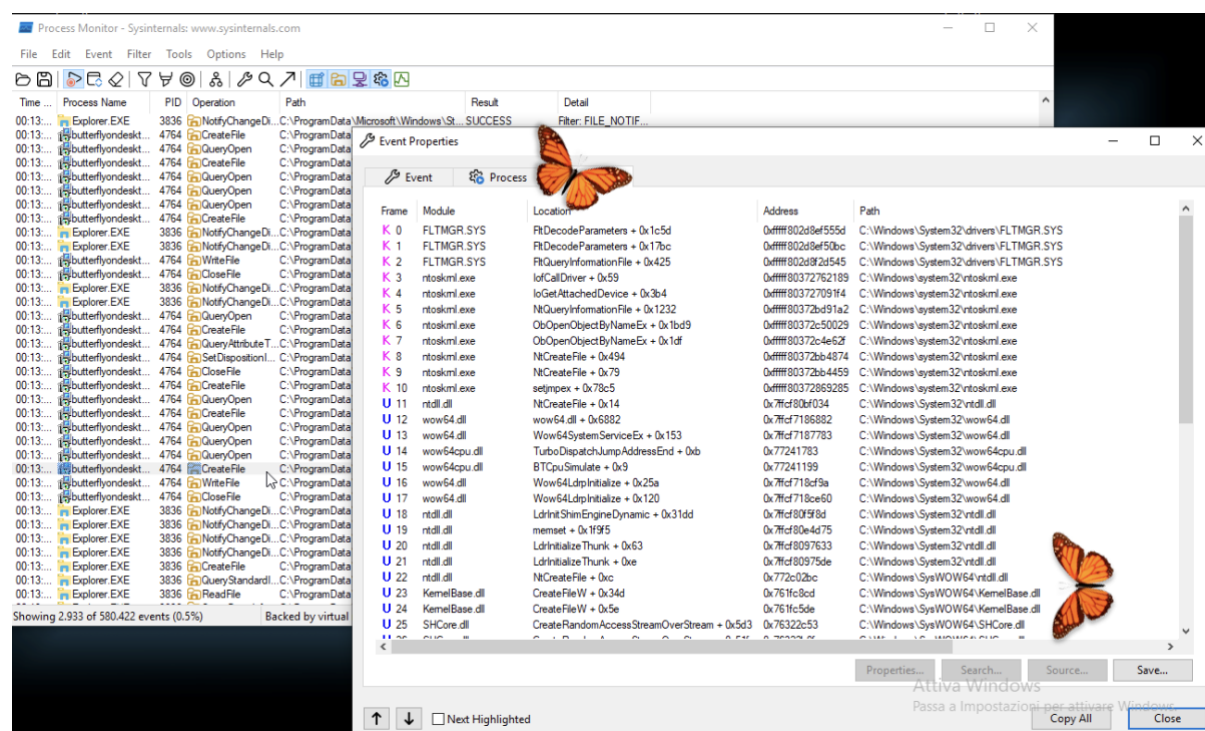
Poi sono tornato a Process Monitor e ho iniziato a cercare qualcosa di particolare e ho trovato:



1. Posizione del collegamento: la cartella

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Butterfly sul Desktop fa parte del sistema del menu Start in Windows. La directory ProgramData è comunemente utilizzata dai programmi per archiviare dati accessibili a tutti gli utenti. Poiché il malware ha creato un collegamento in questa directory, potrebbe potenzialmente essere eseguito all'avvio per tutti gli utenti.

2. Collegamento di disinstallazione: il file si chiama "Uninstall Butterfly on Desktop.lnk", che in genere indica che potrebbe essere stato progettato per apparire come un legittimo programma di disinstallazione per il malware. Il malware spesso crea questo tipo di file per mascherare la sua vera natura o per dare l'impressione di una "uscita pulita", nel caso in cui l'utente provi a rimuoverlo manualmente.



Il fatto che il malware abbia creato una scorciatoia indica che sta tentando di funzionare automaticamente dopo il riavvio del sistema. Ciò potrebbe anche suggerire che il malware potrebbe avere un meccanismo autoreplicante che posiziona i file in altre directory di sistema o modifica il registro.

Process Tree

☐ Only show processes still running at end of current trace
☒ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
updater.exe (6008)	Google Updater	C:\Program Files (...)		Google LLC	NT AUTHORITY\...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
svchost.exe (5036)	svchost.exe (5036)	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	19/01/2025 00:1...	19/01/2025 00:1...
svchost.exe (4780)	svchost.exe (4780)	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	19/01/2025 00:1...	19/01/2025 00:2...
lsass.exe (672)	lsass.exe (672)	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\sys...	18/01/2025 21:0...	n/a
fontdrvhost.exe (816)	fontdrvhost.exe (816)	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	18/01/2025 21:0...	n/a
cars.exe (508)	cars.exe (508)	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\a...	18/01/2025 21:0...	n/a
winlogon.exe (600)	winlogon.exe (600)	C:\Windows\sys...		Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	18/01/2025 21:0...	n/a
fontdrvhost.exe (820)	fontdrvhost.exe (820)	C:\Windows\sys...		Microsoft Corporat...	Font Driver Host\...	"fontdrvhost.exe"	18/01/2025 21:0...	n/a
dwm.exe (72)	dwm.exe (72)	C:\Windows\sys...		Microsoft Corporat...	Window Manager...	"dwm.exe"	18/01/2025 21:0...	n/a
Explorer.EXE (3836)	Esplora risorse	C:\Windows\Expl...		Microsoft Corporat...	DESKTOP-S6M9...	C:\Windows\Expl...	18/01/2025 21:0...	n/a
ZoomIt64.exe (5644)	Sysinternals Scree...	C:\Tools\sysinter...		Sysinternals - ww...	DESKTOP-S6M9...	"C:\Tools\sysinter...	18/01/2025 21:0...	n/a
Procmon.exe (4496)	Process Monitor	C:\Tools\sysinter...		Sysinternals - ww...	DESKTOP-S6M9...	"C:\Tools\sysinter...	19/01/2025 00:0...	n/a
Procmon64.exe (4276)	Process Monitor	C:\Users\flarevm\...		Sysinternals - ww...	DESKTOP-S6M9...	"C:\Users\flarevm...	19/01/2025 00:0...	n/a
butterflyondesktop.exe (1376)	Butterfly on Desk...	C:\Users\flarevm\...		Drive Software Co...	DESKTOP-S6M9...	"C:\Users\flarevm...	19/01/2025 00:1...	19/01/2025 00:1...
butterflyondesktop.tmp (476)	Setup/Uninstall	C:\Users\flarevm\...		DESKTOP-S6M9...	DESKTOP-S6M9...	"C:\Users\flarevm...	19/01/2025 00:1...	19/01/2025 00:1...
ButterflyOnDesktop.exe	ButterflyOnDesktop.exe	C:\Program Files (...)		DESKTOP-S6M9...	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	n/a
chrome.exe (3156)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (4940)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (4400)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (1616)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (3924)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (1020)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (3740)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (4540)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (3648)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (2492)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
chrome.exe (1460)	Google Chrome	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:1...	19/01/2025 00:1...
ButterflyOnDesktop.exe (3880)	ButterflyOnDesktop.exe	C:\Program Files (...)		Google LLC	DESKTOP-S6M9...	"C:\Program Files (...)	19/01/2025 00:0...	19/01/2025 00:1...

Description: Setup/Uninstall
Company:
Path: C:\Users\flarevm\AppData\Local\Temp\is-96K4G.tmp\butterflyondesktop.tmp
Command: "C:\Users\flarevm\AppData\Local\Temp\is-96K4G.tmp\butterflyondesktop.tmp" /SL5="S1804
User: DESKTOP-S6M9MPE\flarevm
PID: 4764 Started: 19/01/2025 00:13:14
Exited: 19/01/2025 00:13:45
Go To Event Include Process Include Subtree

Attiva Windows
Passa a Impostazioni per att...

Close