

Report di Analisi Malware

File analizzato: **butterflyondesktop.exe**

Introduzione

L'obiettivo di questo esercizio è analizzare un malware relativamente innocuo tramite due approcci fondamentali: **analisi statica** e **analisi dinamica**.

Per l'analisi dinamica è stato utilizzato **Cuckoo Sandbox**, mentre per la statica è stato impiegato PeStudio

Dati del file

Campo	Valore
Nome file	butterflyondesktop.exe
Tipo	PE32 executable (GUI, 32 bit)
Dimensione	~2.8 MB
Entropia	7.997 (alta – possibile offuscamento)
SHA256	4641AF6A0071E11E13AD3B1CD950E1300542C89EFB6AE92FFECDE9744A4
Data compilazione	19 giugno 1992 (alterata – sospetta)
Firma digitale	Nessuna

pestudio 9.60 - Malware Initial Assessment - www.winitor.com | c:\users\flarevm\Desktop\new folder\butteflyondesktop.exe (read-only)

file settings about

c:\users\flarevm\Desktop\new folder\butteflyondesktop.exe

property	value
file > sha256	4641AF6A0071E11E13AD3B1CD950E1300542C89EFB6AE92FFECDE9744A4
file > first 32 bytes (hex)	4D 5A 50 00 02 00 00 00 04 00 0F 00 FF 00 00 B8 00 00 00 00 00 00 40 00 1A 00 00 00 00 00
file > first 32 bytes (text)	MZP.....@.....
file > info	size: 2986944 bytes, entropy: 7.997
file > type	executable, 32-bit, GUI
file > version	n/a
file > description	Butterfly on Desktop Setup
entry-point > first 32 bytes (hex)	55 8B EC 83 C4 53 56 57 33 C0 89 45 F0 89 45 DC E8 86 94 FF FF E8 8D A6 FF FF E8 1C A9 FF FF
entry-point > location	0x00009C40 (section:.idata)
file > signature	Microsoft Linker 2.25
stamps	
stamp > compiler	Fri Jun 19 22:22:17 1992 (UTC)
stamp > debug	n/a
stamp > resource	n/a
stamp > import	n/a
stamp > export	n/a

Importazioni di funzioni di sistema (API)

L'analisi della sezione Imports del file ha rivelato **l'utilizzo di funzioni critiche**, tipiche di malware con capacità operative su file, memoria e sistema.

Il file butterflyondesktop.exe importa diverse API critiche di Windows, tra cui CreateFileA, WriteFile e VirtualAlloc.

Queste funzioni sono comunemente utilizzate dai malware per creare file, scrivere su disco e iniettare codice in memoria.

È presente anche l'API RaiseException, a volte usata per tecniche anti-debugging.

L'uso combinato di queste API suggerisce che il file potrebbe contenere comportamenti malevoli.

The screenshot shows the pestudio 9.60 interface. On the left is a sidebar with icons for Recycle Bin, available_p, config.xml, PS_Transcri, Visual Studio Code, and malwareR. The main window has a toolbar with file, settings, and about buttons. The title bar says "pestudio 9.60 - Malware Initial Assessment - www.winitor.com | c:\users\flarevm\Desktop\new folder\butteflyondesktop.exe (read-only)". The left pane shows the file structure of the executable file:

- c:\users\flarevm\Desktop\new folder\butteflyondesktop.exe
 - indicators (wait...)
 - footprints (wait...)
 - virusotal (offline)
 - dos-header (size > 64 bytes)
 - dos-stub (size > 192 bytes)
 - rich-header (n/a)
 - file-header (stamp > compiler)
 - optional-header (subsystem > GUI)
 - directories (count > 3)
 - sections (file > unknown)
 - libraries (count > 8)
 - imports (count > 96)
 - exports (n/a)
 - thread-local-storage (n/a)
 - .NET (n/a)
 - resources (signature > unknown)
 - abc strings (wait...)
 - debug (n/a)
 - manifest (level > asInvoker)
 - version (FileDescription > Butterfly on Desktop Setup)
 - certificate (n/a)
 - overlay (signature > InnoSetup)

The right pane displays the imports table:

imports (96)	library (5)
DeleteCriticalSection	kernel32.dll
LeaveCriticalSection	kernel32.dll
EnterCriticalSection	kernel32.dll
InitializeCriticalSection	kernel32.dll
VirtualFree	kernel32.dll
VirtualAlloc	kernel32.dll
LocalFree	kernel32.dll
LocalAlloc	kernel32.dll
WideCharToMultiByte	kernel32.dll
TlsSetValue	kernel32.dll
TlsGetValue	kernel32.dll
MultiByteToWideChar	kernel32.dll
GetModuleHandleA	kernel32.dll
GetLastError	kernel32.dll
GetCommandLineA	kernel32.dll
WriteFile	kernel32.dll
SetFilePointer	kernel32.dll
SetEndOfFile	kernel32.dll
RtlUnwind	kernel32.dll
ReadFile	kernel32.dll
RaiseException	kernel32.dll
GetStdHandle	kernel32.dll
GetFileSize	kernel32.dll
GetSystemTime	kernel32.dll
GetFileType	kernel32.dll
ExitProcess	kernel32.dll
CreateFileA	kernel32.dll

Ambiente di analisi

L'analisi dinamica è stata condotta utilizzando la piattaforma **Cuckoo Sandbox** tramite il portale <https://cuckoo.cert.ee>.

Il file butterflyondesktop.exe è stato caricato ed eseguito in un ambiente isolato per monitorarne il comportamento.

- **Durata dell'esecuzione:** 59 secondi
- **Routing:** internet
- **Log generati:** disponibili su piattaforma Cuckoo

█ File butterflyondesktop.exe

Summary	
Size	2.8MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	1535aa21451192109b86be9bcc7c4345
SHA1	1af211c686c4d4bf0239ed6620358a19691cf88c
SHA256	4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6
SHA512	Show SHA512
CRC32	6EF36069
ssdeep	None
Yara	<ul style="list-style-type: none">• disable_dep - Bypass DEP• escalate_priv - Escalade privileges• win_registry - Affect system registries• win_token - Affect system token• win_files_operation - Affect private profile

Comportamento osservato

Sono state attivate 5 regole YARA indicative di comportamenti critici:

- disable_dep – Tentativo di bypass DEP (Data Execution Prevention)
- escalate_priv – Escalation dei privilegi utente
- win_registry – Interazione con il registro di sistema
- win_token – Gestione dei token di sistema
- win_files_operation – Accesso a file privati di sistema

Rilevamento antivirus

- Rilevato da 1 antivirus su VirusTotal come **malware potenziale**

Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	May 27, 2025, 4:43 p.m.	May 27, 2025, 4:44 p.m.	59 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

- Yara rules detected for file (5 events)
- Allocates read-write-execute memory (usually to unpack itself) (4 events)
- Checks if process is being debugged by a debugger (1 event)
- The executable contains unknown PE section names indicative of a packer (could be a false positive) (3 events)
- Queries for potentially installed applications (2 events)
- File has been identified by one AntiVirus engine on VirusTotal as malicious (1 event)

Comportamento visivo

Durante l'esecuzione il file ha mostrato una finestra pop-up visibile sul desktop.

- Non è stata eseguita alcuna interazione da parte dell'utente
- Il sistema ha catturato 2 schermate:
 - Finestra attiva con messaggio
 - Desktop con wallpaper "Doge"

Screenshots



Name	Response	Post-Analysis Lookup
		No hosts contacted.

Conclusione dell'analisi dinamica

Il comportamento osservato è **coerente con un malware classificabile come dropper o spyware**. Presenta funzionalità sospette come:

- Bypass di protezioni (DEP)
- Escalation di privilegi
- Accesso al registro e gestione dei token
- Anti-debugging
- Rilevamento di software installati

Tuttavia, **non sono state rilevate comunicazioni verso l'esterno**, né alterazioni evidenti del sistema in questa esecuzione limitata nel tempo.

Raccomandazioni finali

- Il file va trattato come **malware sospetto**
- Evitare l'apertura su sistemi non isolati
- Procedere con monitoraggio continuo e blocco hash a livello endpoint