

Analisi ButterflyonDesktop

Analisi Statica

L'analisi statica è stata eseguita esaminando il codice e le proprietà del file "butterflyondesktop.exe" senza eseguirlo. Questo approccio consente di raccogliere informazioni preliminari sul malware, come la sua struttura, eventuali firme note, e le funzionalità che potrebbero essere implementate

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Property Value

File Name	C:\Users\FlareVM\Desktop\Malware\Spyware\butterflyondesktop.exe
File Type	Portable Executable 32
File Info	Borland Delphi 4.0
File Size	2.85 MB (2986944 bytes)
PE Size	53.00 KB (54272 bytes)
Created	Tuesday 25 March 2025, 10.44.14
Modified	Tuesday 25 March 2025, 10.44.14
Accessed	Tuesday 25 March 2025, 14.15.47
MD5	1535AA21451192109B86BE9BCC7C4345
SHA-1	1AF211C686C4D4BF0239ED6620358A19691CF88C

Property Value

Comments	This installation was built with Inno Setup.
CompanyName	Drive Software Company
FileDescription	Butterfly on Desktop Setup
FileVersion	
LegalCopyright	
ProductName	Butterfly on Desktop

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Member	Offset	Size	Value	Mea ^
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	CO
BaseOfCode	0000012C	Dword	00001000	
BaseOfData	00000130	Dword	0000B000	
ImageBase	00000134	Dword	00400000	
SectionAlignment	00000138	Dword	00001000	
FileAlignment	0000013C	Dword	00000200	
MajorOperatingSystemVers...	00000140	Word	0001	
MinorOperatingSystemVers...	00000142	Word	0000	
MajorImageVersion	00000144	Word	0006	
MinorImageVersion	00000146	Word	0000	
MajorSubsystemVersion	00000148	Word	0004	

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
CODE	00009364	00001000	00009400	00000400	00000000	00000000	0000	0000	60000020
DATA	0000024C	0000B000	00000400	00009800	00000000	00000000	0000	0000	C0000040
BSS	00000E4C	0000C000	00000000	00009C00	00000000	00000000	0000	0000	C0000000
.idata	00000950	0000D000	00000A00	00009C00	00000000	00000000	0000	0000	C0000040
.tls	00000008	0000E000	00000000	0000A600	00000000	00000000	0000	0000	C0000000
.idata	00000018	0000F000	00000200	0000A600	00000000	00000000	0000	0000	50000040
.reloc	000008B4	00010000	00000000	00000000	00000000	00000000	0000	0000	50000040
.src	00002C00	00011000	00002C00	0000A800	00000000	00000000	0000	0000	50000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	MZF...0.yy..
00000010	B8	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00
00000040	8A	10	00	0E	1F	B4	09	CD	21	B6	01	4C	CD	21	90	90	80 0 . i j . i i i
00000050	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	This program mus
00000060	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	t be run under W
00000070	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	in32..8?.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
00009E54	N/A	00009C00	00009C04	00009C08	00009C0C	00009C10
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	0000D628	0000D210
comctl32.dll	1	00000000	00000000	00000000	0000D906	0000D244
kernel32.dll	1	00000000	00000000	00000000	0000D93A	0000D24C

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	0000D2E4	0000	LocalFree
N/A	0000D2F0	0000	LocalAlloc
N/A	0000D2FE	0000	WideCharToMultiByte
N/A	0000D314	0000	TlsSetValue
N/A	0000D322	0000	TlsGetValue
N/A	0000D330	0000	MultiByteToWideChar
N/A	0000D346	0000	GetModuleHandleA
N/A	0000D35A	0000	GetLastError

Il file non sembra essere firmato digitalmente, il che aumenta il livello di sospetto.

Le stringhe estratte suggeriscono che il malware potrebbe cercare di:

- Creare una voce nel registro di sistema per garantire la persistenza.
- Modificare file temporanei o creare nuovi file nel sistema.
- Leggere e modificare alcune impostazioni di sicurezza di Internet Explorer.

Analisi Dinamica

L'analisi dinamica è stata condotta eseguendo il malware in un ambiente controllato, come prima cosa avviamo fakenet per simulare una rete, avviamo procmon e procediamo con l'installazione del malware.

Tramite procmon possiamo visualizzare tutto quello che è successo durante e dopo l'installazione del file butterflyondesktop.exe, applicando dei filtri possiamo visualizzare molte operazioni che sembrano malevole.

Process Monitor - Systematic.com | systematic.com

FileEditEventFilterToolsOptionsHelp

Time	Process Name	PID	Operation	Path	Result	Detail
15:00	ButterflyFondest	4532	RegCreateKey	C:\Windows\SysWow64\csrss\api	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegCreateKey	HKLM\System\CurrentControlSet\Control	REFUSAL	Desired Access: All Access; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegCreateKey	HKLM\System\CurrentControlSet\Control	REFUSAL	Desired Access: All Access; Disposition: REG_OPENED_EXISTING_KEY
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	NAME NOT FOUND	Desired Access: Read Attributes; Delete; Disposition: Open; Options: Non-Directory File, Open Reparse Point, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	NAME NOT FOUND	Desired Access: Read Attributes; Delete; Disposition: Open; Options: Non-Directory File, Open Reparse Point, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Synchronize; Disposition: Open; Options: Directory, Synchronous IO Non-Alert, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\ProgramData\Microsoft\Windows\U...	SUCCESS	Desired Access: Generic Read; Write; Disposition: Overwrite; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: 0; Open/Result: Created
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Query Value; Set Value; Disposition: REG_OPENED_EXISTING_KEY
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 20; Data: 542190
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Set Value; Disposition: REG_CREATED_NEW_KEY
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 20; Data: 542190
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 88; Data: C:\Program Files (x86)\Butterfly on Desk...
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 90; Data: C:\Program Files (x86)\Butterfly on Desk...
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 42; Data: Data on Desktop
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 16; Data: RawMem
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 2; Data:
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 38; Data: butterflyfondest
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 8; Data: eng
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 50; Data: Butterfly on Desktop 1
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 118; Data: Program Files (x86)\Butterfly on Desktop\unim00.exe
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 134; Data: C:\Program Files (x86)\Butterfly on Desktop\unim00.exe\"/SILENT
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 46; Data: Drive Software Company
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 52; Data: http://www.freedomsoft.com
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 60; Data: http://www.drive-software.com
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_DWORD, Length: 4; Data:
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_DWORD, Length: 4; Data: 1
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_SZ, Length: 18; Data: 20250325
15:00	ButterflyFondest	4532	RegSetValue	HKCU\Software\Microsoft\Windows\Co...	SUCCESS	Type: REG_DWORD, Length: 4; Data: 685
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Generic Read; Write; Disposition: Overwrite; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: None; AllocationSize: 0; Open/Result: Overwritten
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\SysWow64\agchapi.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\WinSxS\x-wwi\all	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\WinSxS\x-wwi\all	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\SysWow64\kernel32.dll	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\SysWow64\kernel32.dll	SUCCESS	Desired Access: Read Control; Disposition: Open; Options: Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Program Files (x86)\Butterfly on Desk...	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\appcache\eyman.sdb	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Write, AllocationSize: n/a; Open/Result: Opened
15:00	ButterflyFondest	4532	RegSetValue	C:\Windows\SysWow64\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Attributes n/a, ShareMode: Read, Delete, AllocationSize: n/a; Open/Result: Opened

Showing 47 of 373,562 events (0.0%)Backed by virtual memory

[illegible]

Tramite ricerca online risaliamo a delle analisi pronte, in questo caso ho utilizzato quelle di CyberFortress e ANY.RUN

Back

Analysis Report of butterflyondesktop.exe

Visit Website

Print

General Information

Operating System	Windows 10 x64
Network Traffic Mode	VPN
Analysis Type	Full Triage
Score	99.9 %
Indicators	<div>4</div> <div>3</div> <div>1</div>
Classification	<div>EDrigger</div> <div>RTedp8</div> <div>Obelisk</div>
Verdict	<div>malicious</div>
APT Detection	False

File Information

Target	butterflyondesktop.exe
Size (Bytes)	2986944
MD5	1535ae21451192109b86e9bcc7c4345
SHA1	1af211c686c4d4bf0239ed6620358a19691cf88c
SHA256	4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6
SSDEEP	49152:5aA7f7iVmdqK23H2bpHI4Qs5ABv9WRHZRsgl82icHGAaKLinXBgjQ+VMkX224QsWBq5SfARGRqJ

Signature List

Severity	3 11364
Description	System or Hidden File Creation
<div>Details</div>	
Severity	3 11364
Description	Network Activity from Unlogged API Calls
<div>Details</div>	

File name: butterflyondesktop.exe

Full analysis: <https://app.any.run/tasks/3a448a27-86c0-479c-ab0b-d78c44d5fd77>

Verdict:

Malicious activity

Analysis date: March 05, 2025 at 21:50:03

OS: Windows 10 Professional (build: 19045, 64 bit)

Tags:

auto

generic

inno

installer

delphi

Indicators:

MIME: application/vnd.microsoft.portable-executable

File info: PE32 executable (GUI) Intel 80386, for MS Windows, 8 sections

MD5: 1535AA21451192109B86E9BCC7C4345

SHA1: 1AF211C686C4D4BF0239ED6620358A19691CF88C

SHA256: 4641AF6A0071E11E13AD3B1CD950E01300542C2B9EFB6AE92FFECEDDE974A4A6

SSDEEP: 49152:5aA7f7iVmdqK23H2bpHI4Qs5ABv9WRHZRsgl82icHGAaKLinXBgjQ+VMkX224QsWBq5SfARGRqJ

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. **ANY.RUN** does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

☒ Add for printing

MALICIOUS

GENERIC has been found (auto)

- butterflyondesktop.exe (PID: 2392)

Changes the autorun value in the registry

- butterflyondesktop.tmp (PID: 1228)

SUSPICIOUS

Reads security settings of Internet Explorer

- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.tmp (PID: 1228)

Executable content was dropped or overwritten

- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)

Process drops legitimate windows executable

- butterflyondesktop.tmp (PID: 1228)

Reads the Windows owner or organization settings

- butterflyondesktop.tmp (PID: 1228)

There is functionality for taking screenshot (YARA)

- ButterflyOnDesktop.exe (PID: 5680)

INFO

Checks supported languages

- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)
- identity_helper.exe (PID: 7844)
- ButterflyOnDesktop.exe (PID: 5680)

Create files in a temporary directory

- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)

Reads the computer name

- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.tmp (PID: 1228)
- identity_helper.exe (PID: 7844)
- ButterflyOnDesktop.exe (PID: 5680)

Process checks computer location settings

- butterflyondesktop.tmp (PID: 5544)

Compiled with Borland Delphi (YARA)

- butterflyondesktop.tmp (PID: 5544)
- silui.exe (PID: 1348)
- butterflyondesktop.tmp (PID: 1228)
- ButterflyOnDesktop.exe (PID: 5680)

Detects InnoSetup installer (YARA)

- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.tmp (PID: 1228)

Comportamento del malware

Raccolta di Informazioni dal PC

- Il malware legge diverse impostazioni e informazioni dal sistema, tra cui:
- Impostazioni di sicurezza di Internet Explorer : Potrebbe cercare di identificare le politiche di sicurezza configurate per aggirarle.
- Nome del computer : Raccoglie informazioni sul dispositivo infetto.
- Proprietario o organizzazione del sistema : Questo potrebbe essere utile per identificare l'utente o l'azienda di appartenenza.
- Lingue supportate : Verifica quali lingue sono installate sul sistema.

Tentativo di Esfiltrazione dei Dati

Durante l'esecuzione, il malware stabilisce una connessione con un server remoto (indirizzo IP non specificato nel report). Questo suggerisce che:

- Sta tentando di inviare i dati raccolti a un attaccante remoto.
- Potrebbe anche scaricare ulteriori payload malevoli per estendere le sue funzionalità.

Modifica delle Policy del Sistema

Il malware modifica alcune impostazioni del sistema per garantire la sua persistenza e facilitare le sue attività malevole:

- Crea una voce nel registro di sistema : Questo garantisce che il malware venga eseguito automaticamente ogni volta che il sistema si avvia.
- Modifica le policy di sicurezza : Potrebbe abbassare le protezioni del sistema per evitare di essere bloccato.

Creazione e Modifica di File

Il malware crea file temporanei e modifica il file system:

- File creati/modificati : Potrebbero contenere dati raccolti o configurazioni necessarie per il funzionamento del malware.
- Voce di disinstallazione : Crea una voce nel pannello di controllo per fingere di essere un'applicazione legittima.

Funzionalità Aggiuntive

- Screenshot : Il malware ha la capacità di catturare screenshot, il che aumenta il rischio di furto di informazioni sensibili.
- Persistenza : Modifica il registro di sistema per garantire che rimanga attivo anche dopo il riavvio del sistema.

Conclusione

L'analisi combinata di "butterflyondesktop.exe" ha rivelato che il malware è in grado di:

1. Creare persistenza nel sistema tramite modifiche al registro di sistema.
2. Stabilire una comunicazione con un server remoto, probabilmente per scopi malevoli.
3. Modificare il file system e avviare processi secondari.

Sebbene il malware sia stato descritto come "relativamente innocuo", il suo comportamento evidenzia potenziali rischi per la sicurezza del sistema. È fondamentale rimuovere immediatamente qualsiasi istanza di questo malware da un sistema infetto e monitorare eventuali attività sospette successive.