

Attività di Analisi del Malware

Oggetto: Sarà condiviso un malware relativamente innocuo.

Compiti:

1. **Analisi Statica:** Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
2. **Analisi Dinamica:** Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

ANALISI STATICA

Da alcune ricerche su internet troviamo queste informazioni.

Windows bulletin tutorial <https://windowsbulletin.com/files/exe/drive-software-company/butterfly-on-desktop-1-0/butterflyondesktop-exe>

Cos'è ButterflyOnDesktop.exe? È un processo sicuro o un virus/malware? Come correggere, rimuovere e gestire l'avvio

23 dicembre 2023 | Aggiornato maggio 2025

Autore: Phil Hart

Indice dei contenuti

1. Cos'è ButterflyOnDesktop.exe?
2. ButterflyOnDesktop.exe è sicuro o un virus/malware?
3. Posso rimuovere o eliminare ButterflyOnDesktop.exe?
4. Messaggi di errore comuni relativi a ButterflyOnDesktop.exe
5. Come correggere ButterflyOnDesktop.exe
6. Aggiornamento Maggio 2025
7. Scaricare o reinstallare ButterflyOnDesktop.exe

Cos'è ButterflyOnDesktop.exe?

ButterflyOnDesktop.exe è un file eseguibile dell'applicazione **Butterfly on Desktop 1.0** sviluppata da **Drive Software Company**, con una dimensione tipica di circa **3.7 MB**.

Anche se l'estensione .exe indica un file eseguibile, è importante determinare se questo file specifico è una parte sicura del sistema Windows, un'applicazione legittima o un virus/trojan dannoso.

ButterflyOnDesktop.exe è un virus o malware?

Per verificare se ButterflyOnDesktop.exe è legittimo o pericoloso:

- **Controlla il percorso del file:** deve trovarsi in

C:\Program Files\Butterfly on Desktop\

- **Usa Task Manager:** aggiungi la colonna "Percorso immagine" per vedere dove si trova il file.
- **Usa Process Explorer di Microsoft:** controlla lo stato "Verified Signer". Se indica "Impossibile verificare", potrebbero essere necessari controlli aggiuntivi.

Fatti importanti su ButterflyOnDesktop.exe:

- Posizione: C:\Program Files\Butterfly on Desktop\
- Publisher: **Drive Software Company**
- Sito web: www.drive-software.com
- URL editore: www.freedesktopsoft.com

- Disinstallatore: "C:\Program Files\Butterfly on Desktop\unins000.exe"
- Percentuale di utenti che lo rimuove: **53%**
- Valutazione degli utenti: **Buona**

Se sospetti che sia un virus, usa un software come **Malwarebytes** per analizzarlo e rimuoverlo.

Posso rimuovere o eliminare ButterflyOnDesktop.exe?

Questo file appare innocuo.

Non eliminare file eseguibili sicuri, poiché potresti compromettere il corretto funzionamento dell'applicazione associata.

Per rimuoverlo in modo sicuro:

1. Vai su **Pannello di controllo → Programmi**.
2. Trova **Butterfly on Desktop 1.0**.
3. Clicca su **Disinstalla** o **Rimuovi**, quindi segui le istruzioni.

Oppure esegui direttamente il file di disinstallazione:

C:\Program Files\Butterfly on Desktop\unins000.exe

Messaggi di errore comuni di ButterflyOnDesktop.exe

Ecco alcuni errori che potresti vedere:

- "ButterflyOnDesktop.exe Errore Applicazione."
- "ButterflyOnDesktop.exe non valido."
- "ButterflyOnDesktop.exe non trovato."
- "Errore nell'avvio del programma: ButterflyOnDesktop.exe."
- "Percorso applicazione con errore: ButterflyOnDesktop.exe."

Gli errori possono comparire durante l'installazione, l'avvio o l'uso del programma, o anche durante l'avvio/spengimento di Windows.

Come correggere ButterflyOnDesktop.exe

Per evitare ulteriori problemi:

- Esegui regolarmente **scansioni antivirus**.
- Pulisci il disco con strumenti come **Pulizia Disco (cleanmgr)** e **System File Checker (sfc /scannow)**.
- Disinstalla i programmi inutili.
- Gestisci i programmi di avvio con **Task Manager**.
- Abilita gli **aggiornamenti automatici di sistema**.
- Effettua **backup periodici** o crea punti di ripristino.

Per problemi gravi, usa strumenti come **DISM**, **Task Manager** e **Monitor Risorse** per diagnosticare e riparare senza reinstallare il sistema.

Aggiornamento Maggio 2025

Ti consigliamo di provare questo nuovo software che corregge errori, protegge il PC da malware e ne ottimizza le prestazioni.

Passaggi:

1. Scarica il **PC Repair & Optimizer Tool** (compatibile con Windows 7/8/8.1/10/11).
2. Clicca su **Start Scan** per trovare problemi nel registro.
3. Clicca su **Repair All** per correggere tutti gli errori.

(Offerta opzionale per Fortect)

Scaricare o reinstallare ButterflyOnDesktop.exe

Non è consigliabile scaricare file .exe da siti terzi: potrebbero contenere malware.

Se necessario, reinstalla l'applicazione **Butterfly on Desktop 1.0** per ottenere nuovamente il file originale.

Compatibilità

Gli errori relativi a ButterflyOnDesktop.exe possono verificarsi in uno qualsiasi dei seguenti sistemi operativi Windows:

- Windows Vista
- Windows 7
- Windows 8 / 8.1
- Windows 10
- Windows 11

Altra ritrovamento la facciamo al seguente link

[Malware analysis butterflyondesktop.exe Malicious activity | ANY.RUN - Malware Sandbox Online](#)

ANYRUN

INTERACTIVE MALWARE ANALYSIS

General

Behavior

MalConf

Static information

Video

Screenshots

System events

Network

General Info

Add for printing

File name:

butterflyondesktop.exe

Full analysis:

[https://app.any.run/tasks/92b3dfd2-b3c5-459e-aba8-05e121d3a0ef](#)

Verdict:

Malicious activity

Threats:

Loader

A loader is malicious software that infiltrates devices to deliver malicious payloads. This malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans or stealers. Criminals usually deliver loaders through phishing emails and links by relying on social engineering to trick users into downloading and running their executables. Loaders employ advanced evasion and persistence tactics to avoid detection.

Analysis date:

February 13, 2024 at 03:52:10

OS:

Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Tags:

loader

Indicators:

MIME:

application/x-dosexec

File info:

PE32 executable (GUI) Intel 80386, for MS Windows

MD5:

1535AA21451192109B86BE9BC7C4345

SHA1:

1AF211C686C4D4BF0239ED6620358A19691CF88C

SHA256:

4641AF6A0071E11E13AD3B1CD950E01300542C2B9EFB6AE92FFECDEDD974A4A6

SSDEEP:

49152:5aa7f7tVmdqK23H2bpHl4Qs5ABV9WRHZRgl82icHGAAkLinXBgJ+VMkX224QsWBq5SfARGrgJ

Malware Trends Tracker

>>>

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

Drops the executable file immediately after the start

- butterflyondesktop.exe (PID: 3668)
- butterflyondesktop.exe (PID: 1776)
- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.exe (PID: 2192)
- livecamwallpaper.exe (PID: 2328)
- livecamwallpaper.tmp (PID: 3428)
- freeclock.tmp (PID: 3760)
- freeclock.exe (PID: 1040)
- freeclock.exe (PID: 764)
- ataclock.exe (PID: 2736)
- ataclock.tmp (PID: 1168)
- ataclock.exe (PID: 3732)
- ataclock.exe (PID: 2940)
- ataclock.exe (PID: 1056)
- ataclock.tmp (PID: 2532)

Changes the autorun value in the registry

- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.tmp (PID: 3428)
- LivecamWallpaper.exe (PID: 1196)
- FreeDesktopClock.exe (PID: 3968)

Starts NET.EXE for service management

- freeclock.tmp (PID: 3760)
- .net.exe (PID: 3196)
- .net.exe (PID: 4020)
- .net.exe (PID: 2028)
- ataclock.tmp (PID: 1168)
- ataclock.tmp (PID: 2532)
- .net.exe (PID: 2136)

SUSPICIOUS

Executable content was dropped or overwritten

- butterflyondesktop.exe (PID: 3668)
- butterflyondesktop.tmp (PID: 2964)
- butterflyondesktop.exe (PID: 1776)
- livecamwallpaper.exe (PID: 2192)
- livecamwallpaper.exe (PID: 2328)
- freeclock.exe (PID: 764)
- livecamwallpaper.tmp (PID: 3428)
- freeclock.exe (PID: 1040)
- freeclock.tmp (PID: 3760)
- ataclock.exe (PID: 2736)
- ataclock.exe (PID: 2940)
- ataclock.tmp (PID: 1168)
- ataclock.exe (PID: 3732)
- ataclock.tmp (PID: 2532)
- ataclock.exe (PID: 1056)

Reads the Windows owner or organization settings

- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.tmp (PID: 3428)
- freeclock.tmp (PID: 3760)
- ataclock.tmp (PID: 1168)
- ataclock.tmp (PID: 2532)

Reads the Internet Settings

- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.tmp (PID: 3428)
- FreeDesktopClock.exe (PID: 2740)
- freeclock.tmp (PID: 2384)

Process drops legitimate windows executable

- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.tmp (PID: 3428)
- freeclock.tmp (PID: 3760)
- ataclock.tmp (PID: 1168)
- ataclock.tmp (PID: 2532)

Reads security settings of Internet Explorer

- FreeDesktopClock.exe (PID: 2740)

INFO

Reads the computer name

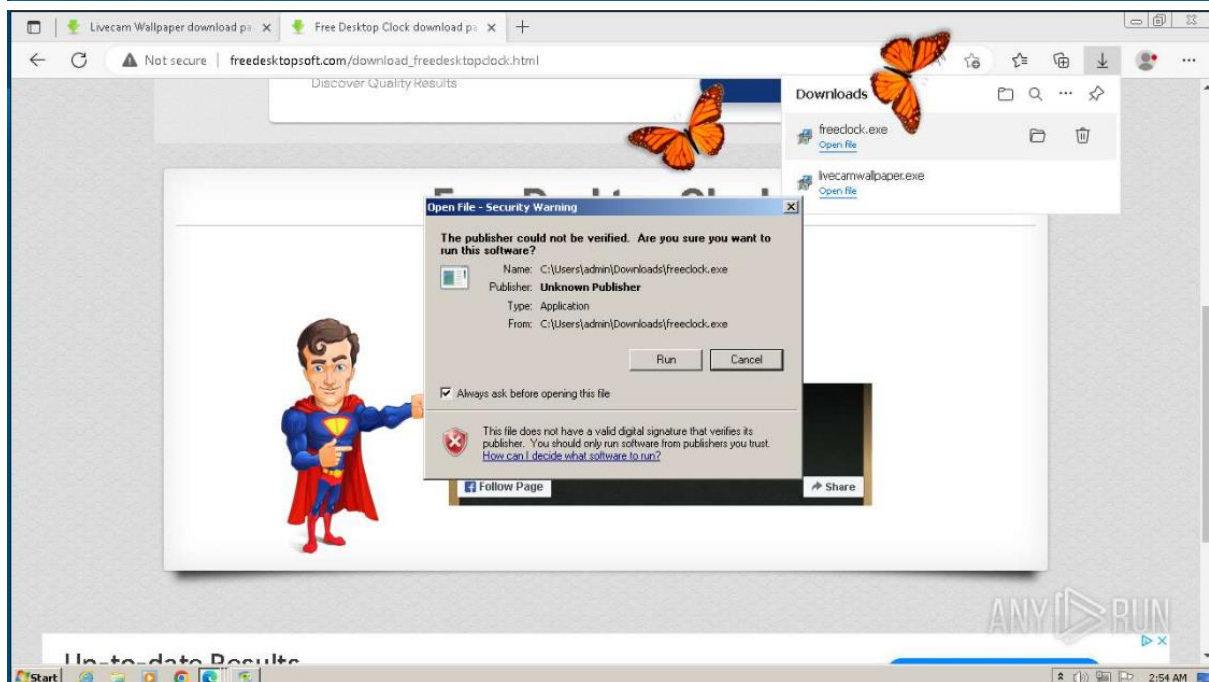
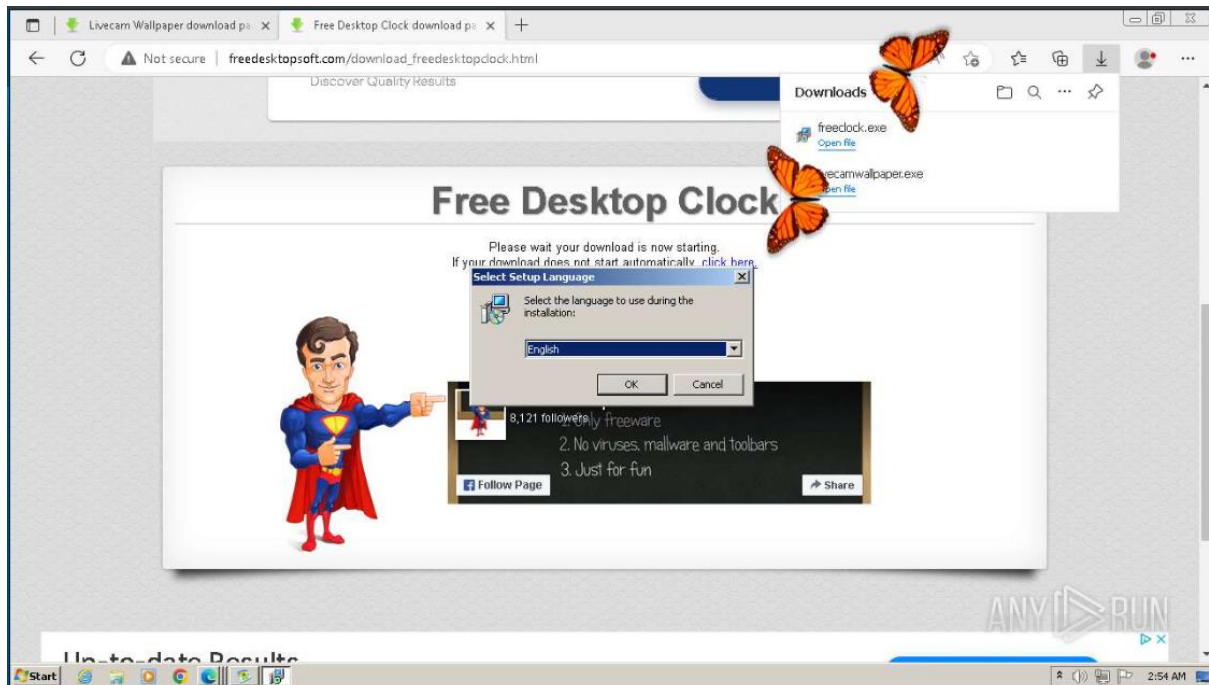
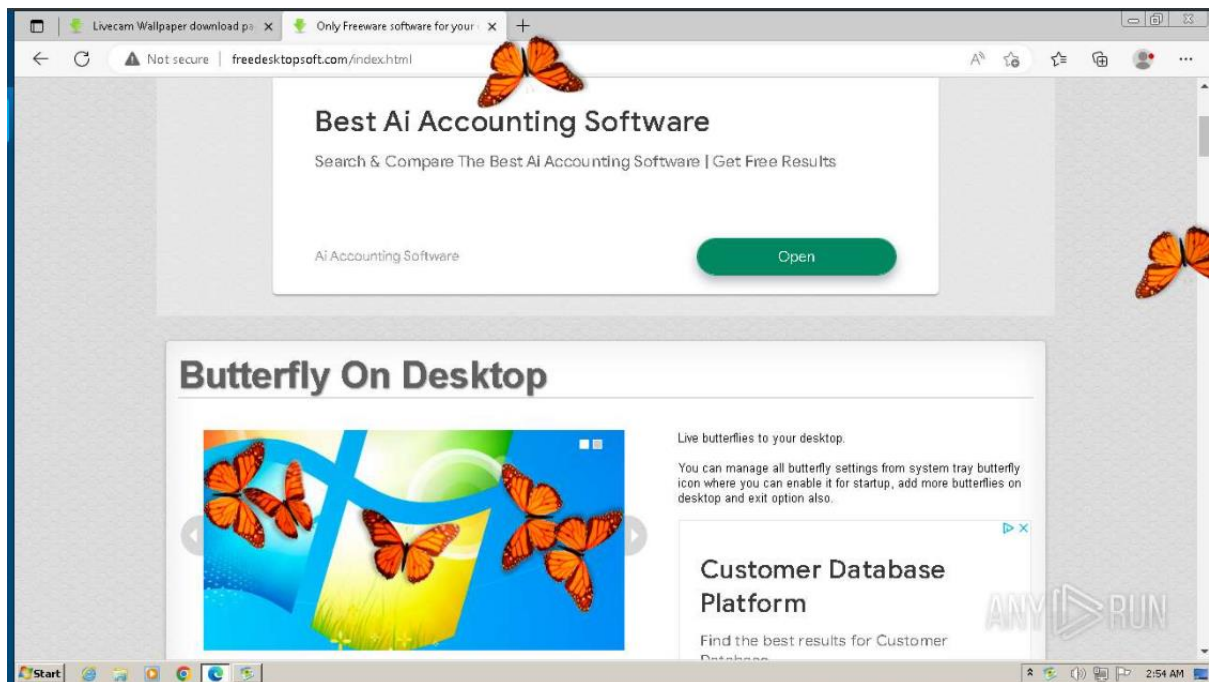
- butterflyondesktop.tmp (PID: 3864)
- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.tmp (PID: 2756)
- livecamwallpaper.tmp (PID: 3428)
- freeclock.tmp (PID: 2384)
- freeclock.tmp (PID: 3760)
- timeserv.exe (PID: 1344)
- FreeDesktopClock.exe (PID: 2740)
- FreeDesktopClock.exe (PID: 3968)
- timeserv.exe (PID: 1380)
- ataclock.tmp (PID: 948)
- ataclock.tmp (PID: 3964)
- LivecamWallpaper.exe (PID: 1196)
- ataclock.tmp (PID: 1168)
- ataclock.tmp (PID: 2532)

Checks supported languages

- butterflyondesktop.exe (PID: 1776)
- ButterflyOnDesktop.exe (PID: 2340)
- butterflyondesktop.tmp (PID: 2964)
- livecamwallpaper.exe (PID: 2192)
- livecamwallpaper.tmp (PID: 2756)
- livecamwallpaper.exe (PID: 2328)
- livecamwallpaper.tmp (PID: 3428)
- LivecamWallpaper.exe (PID: 1196)
- butterflyondesktop.exe (PID: 3668)
- freeclock.exe (PID: 764)
- freeclock.tmp (PID: 2384)
- freeclock.tmp (PID: 3760)
- butterflyondesktop.tmp (PID: 3864)
- FreeDesktopClock.exe (PID: 2740)
- timeserv.exe (PID: 1344)
- FreeDesktopClock.exe (PID: 3968)
- timeserv.exe (PID: 1380)
- ataclock.exe (PID: 2736)
- ataclock.tmp (PID: 948)

Purtroppo con le precedenti informazioni riguardanti gli hash non riusciamo a trovare informazioni sul sito di Malware bazar

Da altri ritrovamenti capiamo anche cosa si visualizza su desktop



Inoltre passandolo su Virustotal abbiamo questo risultato

0

Community Score

No security vendors flagged this URL as malicious

Reanalyze

Search

More

https://app.any.run/tasks/92b3dfd2-b3c5-459e-aba8-05e121d3a0ef

Status200

Content type
text/html; charset=utf-8

Last Analysis Date
a moment ago

app.any.run

text/html

DETECTION

DETAILS

COMMUNITY

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks**.

Security vendors' analysis

Do you want to automate checks?

URLQuery	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

ANALISI DINAMICA

Prepariamo l'ambiente isolato con rete interna , scompattiamo il malware, avviamo fakenet,

File Home Share View Extract Compressed Folder Tools

C:\Users\Flare\VM\Desktop\Malware\Spyware

Malware > Spyware

Name	Date modified	Type	Size
The Worst Of All!!!!!!	27/05/2025 15:57	File folder	
AgentTesla.exe.zip	27/05/2025 15:57	ZIP File	2.847 KB
butterflyondesktop.exe	21/05/2025 16:46	Application	2.917 KB
butterflyondesktop.exe.zip	27/05/2025 15:57	ZIP File	2.895 KB
HawkEye.exe.zip	27/05/2025 15:57	ZIP File	130 KB
Kakwa.docx.zip	27/05/2025 15:57	ZIP File	37 KB

6 items 1 item selected 2.82 MB

Avviamo anche Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time Process Name PID Operation Result Detail

16:19: butterflyondesk... 604 Process Start SUCCESS Parent PID: 4336...

16:19: butterflyondesk... 604 Thread Create SUCCESS Thread ID: 2564

16:19: butterflyondesk... 604 Load Image SUCCESS Image Base: 0x000...

16:19: butterflyondesk... 604 Load Image SUCCESS Image Base: 0x789...

16:19: butterflyondesk... 604 Load Image SUCCESS Image Base: 0x773...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 CreateFile C:\Windows SUCCESS Desired Access: E...

16:19: butterflyondesk... 604 Load Image C:\Windows\System32\wow64.dll SUCCESS Image Base: 0x789...

16:19: butterflyondesk... 604 Load Image C:\Windows\System32\wow64.dll SUCCESS Image Base: 0x789...

16:19: butterflyondesk... 604 QueryOpen C:\Windows\System32\wow64.dll NAME NOT FOUND Length: 24

16:19: butterflyondesk... 604 CreateFile C:\Windows SUCCESS Desired Access: R...

16:19: butterflyondesk... 604 QueryNameInfo C:\Windows SUCCESS Name: Windows

16:19: butterflyondesk... 604 CloseFile C:\Windows SUCCESS

16:19: butterflyondesk... 604 RegOpenKey HKLM\Software\Microsoft\Wow64x86 SUCCESS Desired Access: R...

16:19: butterflyondesk... 604 RegOpenKey HKLM\SOFTWARE\Microsoft\Wow64... NAME NOT FOUND Length: 520

16:19: butterflyondesk... 604 RegOpenKey HKLM\SOFTWARE\Microsoft\Wow64... SUCCESS Type: REG_SZ, Le...

16:19: butterflyondesk... 604 RegOpenKey HKLM\Software\Microsoft\Wow64... SUCCESS

16:19: butterflyondesk... 604 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x773...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 80

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Con... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 24

16:19: butterflyondesk... 604 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: E...

16:19: butterflyondesk... 604 CreateFile C:\Users\Flare\VM\Desktop\Malware\S... SUCCESS Image Base: 0x75a...

16:19: butterflyondesk... 604 Load Image C:\Windows\System32\kernel32.dll SUCCESS Image Base: 0x751...

16:19: butterflyondesk... 604 Load Image C:\Windows\System32\kernel32.dll SUCCESS Image Base: 0x751...

Process Tree

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Description	Image Path	Life Time	Compan
svchost.exe (3000)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (1292)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (5352)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (5552)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (1904)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (4852)	Host Process for ...	C:\Windows\layt...		Microsoft
elevation_service.exe (1452)	Google Chrome	C:\Program Files\...		Google L
svchost.exe (5140)	Host Process for ...	C:\Windows\layt...		Microsoft
svchost.exe (1956)	Host Process for ...	C:\Windows\layt...		Microsoft
update.exe (2564)	Google Updater	C:\Program Files (...)		Google L
update.exe (3816)	Google Updater	C:\Program Files (...)		Google L
lsass.exe (608)	Local Security Aut...	C:\Windows\layt...		Microsoft
fontdrvhost.exe (828)	Usermode Font Dr...	C:\Windows\layt...		Microsoft
csrss.exe (524)	Client Server Run...	C:\Windows\layt...		Microsoft
winlogon.exe (58)	Windows Logon A...	C:\Windows\layt...		Microsoft
fontdrvhost.exe (820)	Usermode Font Dr...	C:\Windows\layt...		Microsoft
lsass.exe (1020)	Local Security Aut...	C:\Windows\layt...		Microsoft
Explorer.EXE (4336)	Windows Explorer	C:\Windows\Expl...		Microsoft
VBox Tray.exe (5528)				

Descriptions: Butterfly on Desktop Setup

Company: Drive Software Company

Path: C:\Users\Flare\VM\Desktop\Malware\Spyware\butterflyondesktop.exe

Commands: "C:\Users\Flare\VM\Desktop\Malware\Spyware\butterflyondesktop.exe"

User: DESKTOP-4G3BQDG\Flare\VM

PID: 604

Started: 27/05/2025 16:19:28

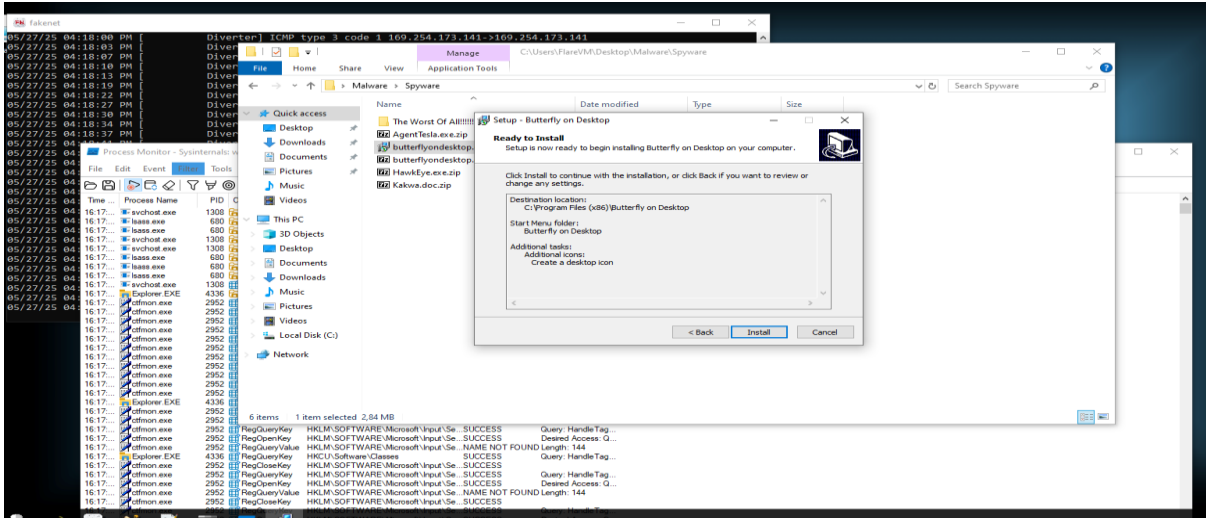
Exited: 27/05/2025 16:19:48

Go To Event

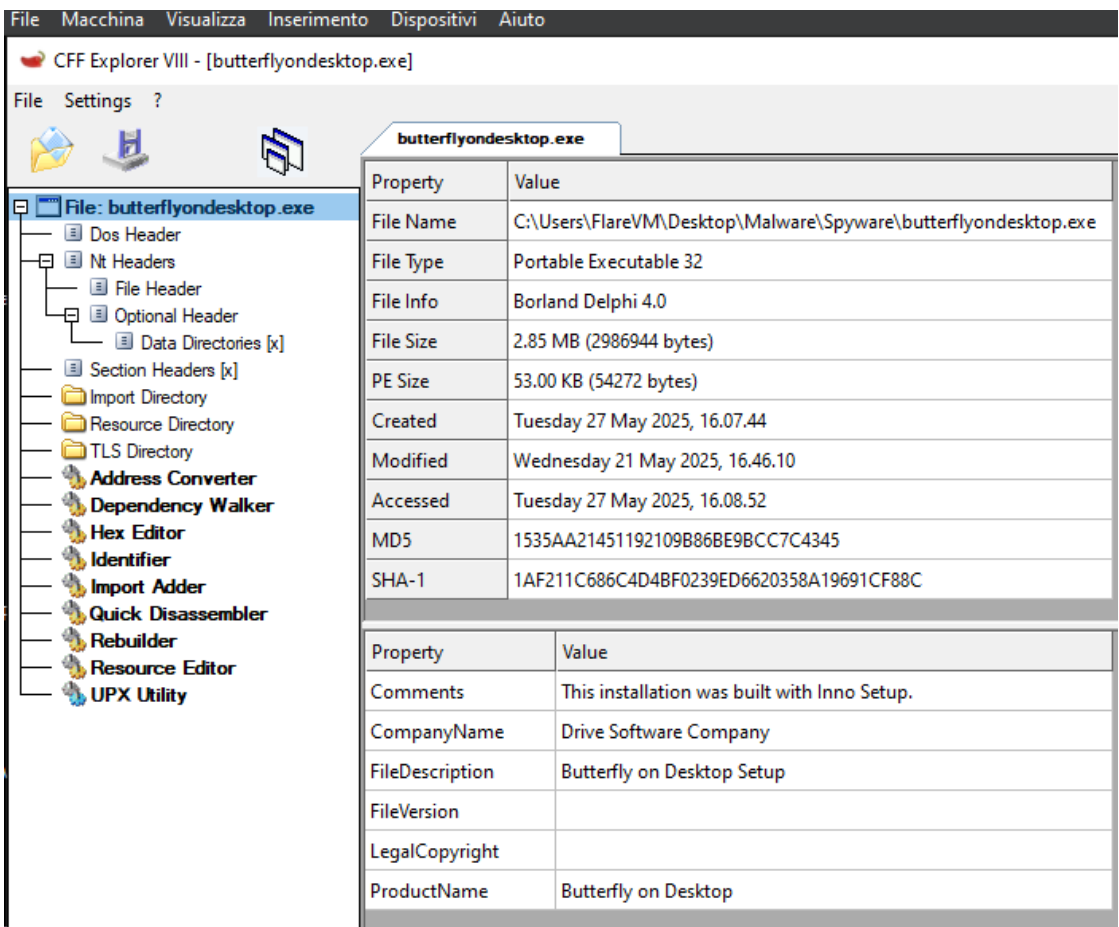
Include Process

Include Subtree

Avviamo il file butterfly.exe

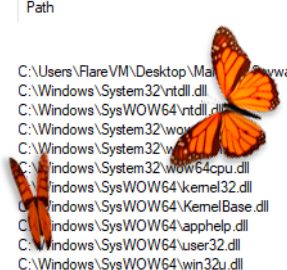


Avviamo CFF explorer



Process Monitor - Sysinternals: www.sysinternals.com

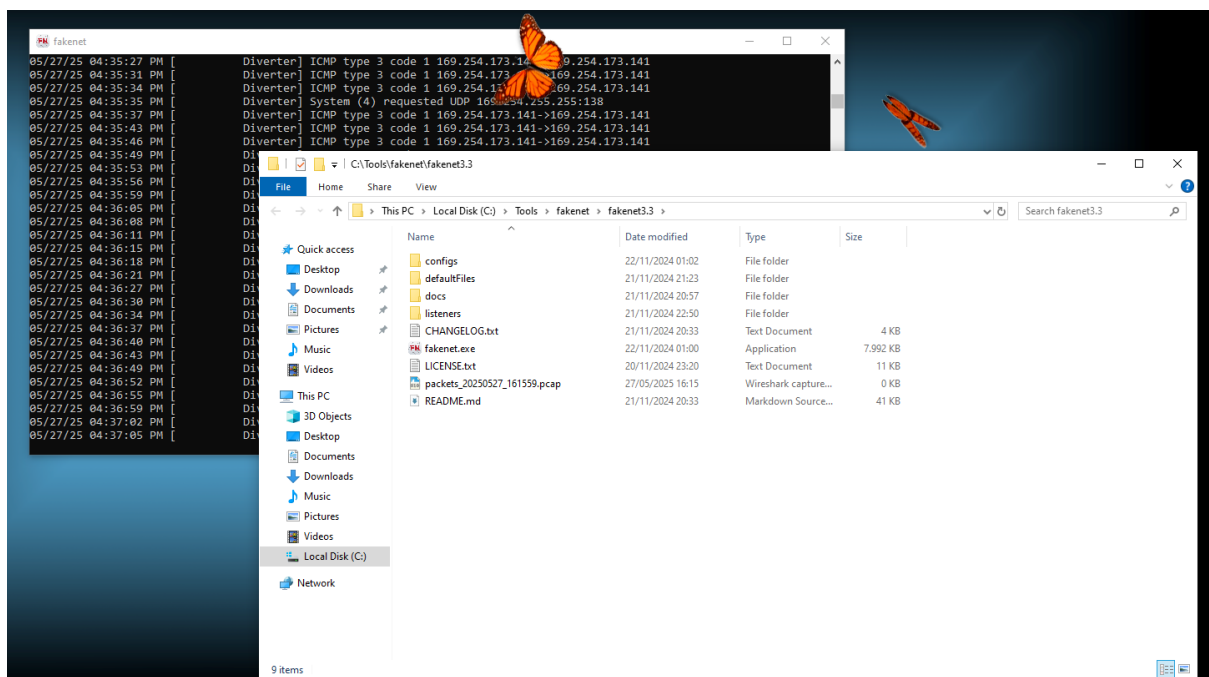
File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:19:...	butterflyondesk...	604	Process Start		SUCCESS	Parent PID: ...
16:19:...	butterflyondesk...	604	Thread Create		SUCCESS	Thread ID: 2
16:19:...	butterflyondesk...	604	Load Image	C:\Users\FlareVM\Desktop\Ma...ware\butterflyondesk.exe	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Thread Create		SUCCESS	Thread ID: 4
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\msvcp_win.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\ucrtbase.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Thread Create		SUCCESS	Thread ID: 5
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Thread Create		SUCCESS	Thread ID: 5
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\vpport.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.363...	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	604	Process Create	C:\Users\FlareVM\AppData\Local\Temp\is-CECQN.tmp\butterflyondesk.tmp	SUCCESS	PID: 3032, C...
16:19:...	butterflyondesk...	3032	Process Start		SUCCESS	Parent PID: ...
16:19:...	butterflyondesk...	3032	Thread Create		SUCCESS	Thread ID: 1
16:19:...	butterflyondesk...	3032	Load Image	C:\Users\FlareVM\AppData\Local\Temp\is-CECQN.tmp\butterflyondesk.tmp	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: ...
16:19:...	butterflyondesk...	3032	Load Image	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Image Base: ...

Showing 7,883 of 1,296,455 events (0.6%) Backed by virtual memory

Intanto Fakenet ha stilato un file.pcap che volendo si potrebbe zippare assieme alle varie ricerche che si fanno su Process Monitor, anche queste salvabili tramite la creazione di un file.



Diamo il file . Exe del presunto malware in pasto a cuckoo e vediamo cosa trova.

FileMachineVisualizatorIntelligenceLogisticsAudio

Cuckoo SandboxCuckoo Sandbox

cuckoo.cert.tee/submit/post/5326017

SubmitImport

DashboardRecentPendingSearch

submitfileconfiguresandboxSummary

✓ Your submission has been received and the tasks are being processed!

Next:View pending tasksSubmit again

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package
6514971	27/05/2025 17:42	butterflyondesktop.exe	exe
Done			

DashboardRecentPendingSearch

Summary

File butterflyondesktop.exe

SummaryDownloadResubmit sample

Size2.8MB

TypePE32 executable (GUI) Intel 80386, for MS Windows

MD51535aa21451192109b86be9bcc7c4345

SHA11af211c686c4d4bf0239ed6620358a19691cf88c

SHA2564641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6

SHA512Show SHA512

CRC326EF36069

ssdeepNone

Yara

- disable_dep - Bypass DEP
- escalate_priv - Escalade privileges
- win_registry - Affect system registries
- win_token - Affect system token
- win_files_operation - Affect private profile

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	May 27, 2025, 5:42 p.m.	May 27, 2025, 5:43 p.m.	59 seconds	internet	Show Analyzer Log

Signatures

Yara rules detected for file (5 events)

Allocates read-write-execute memory (usually to unpack itself) (4 events)

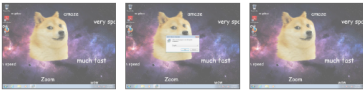
Checks if process is being debugged by a debugger (1 event)

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)

Screenshots



Name	Response	Post-Analysis Lookup	IP Address	Status	Action	VT	Location
------	----------	----------------------	------------	--------	--------	----	----------