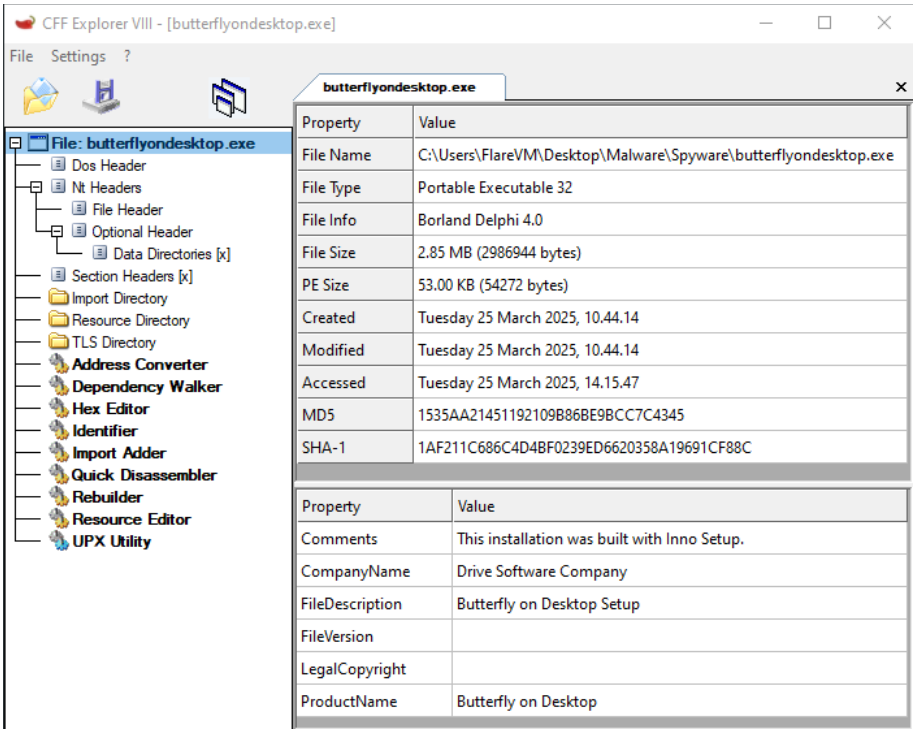
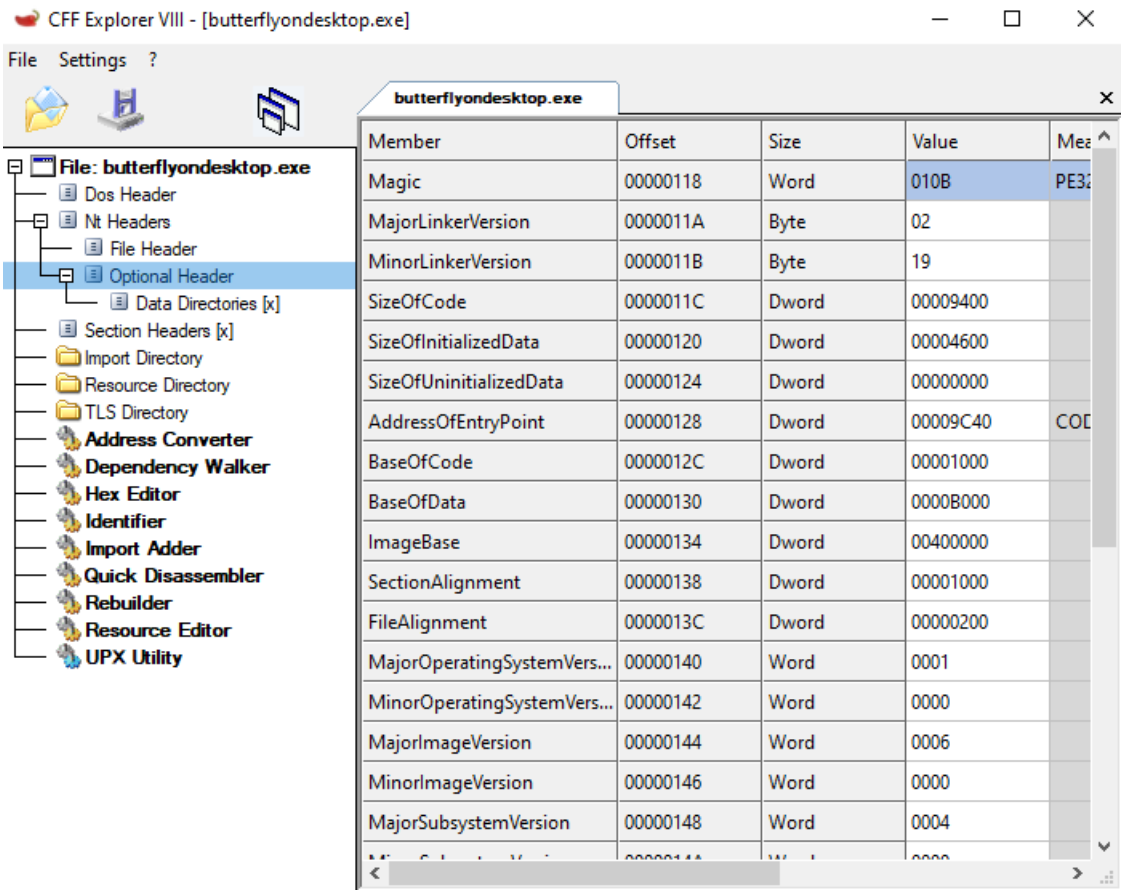
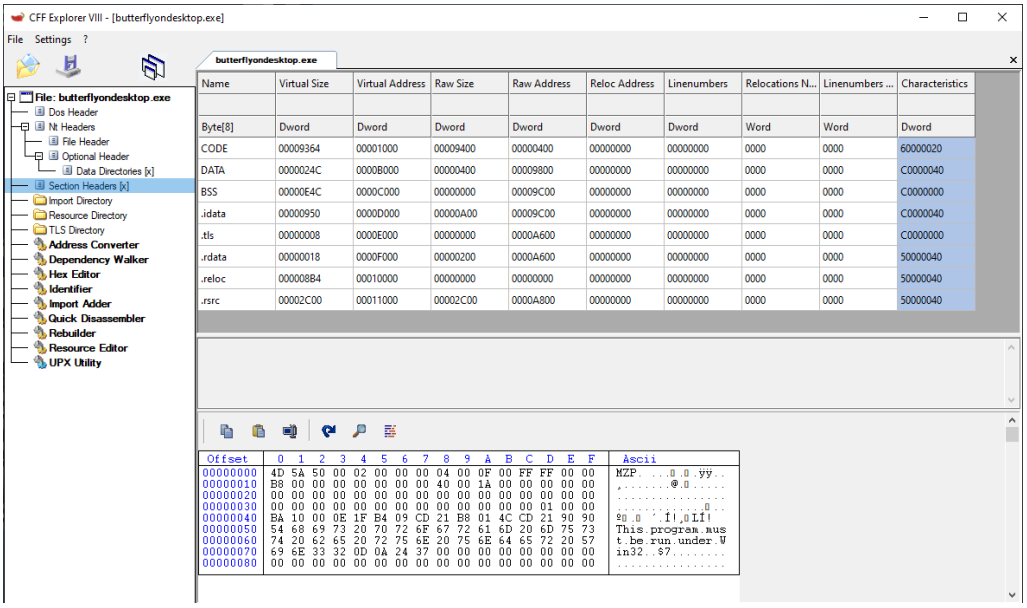
Analisi ButterflyonDesktop

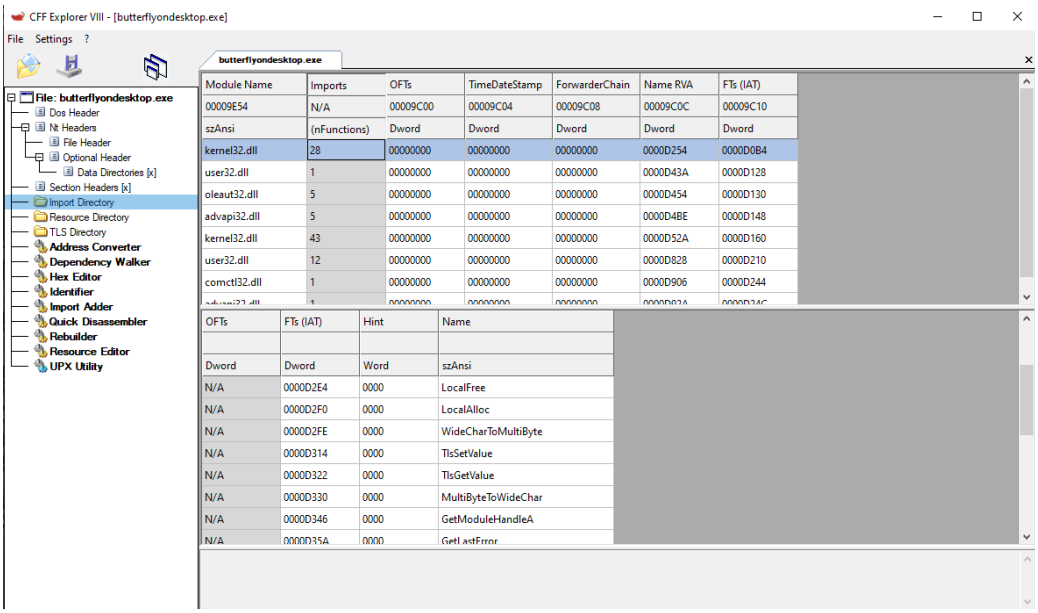
Analisi Statica

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









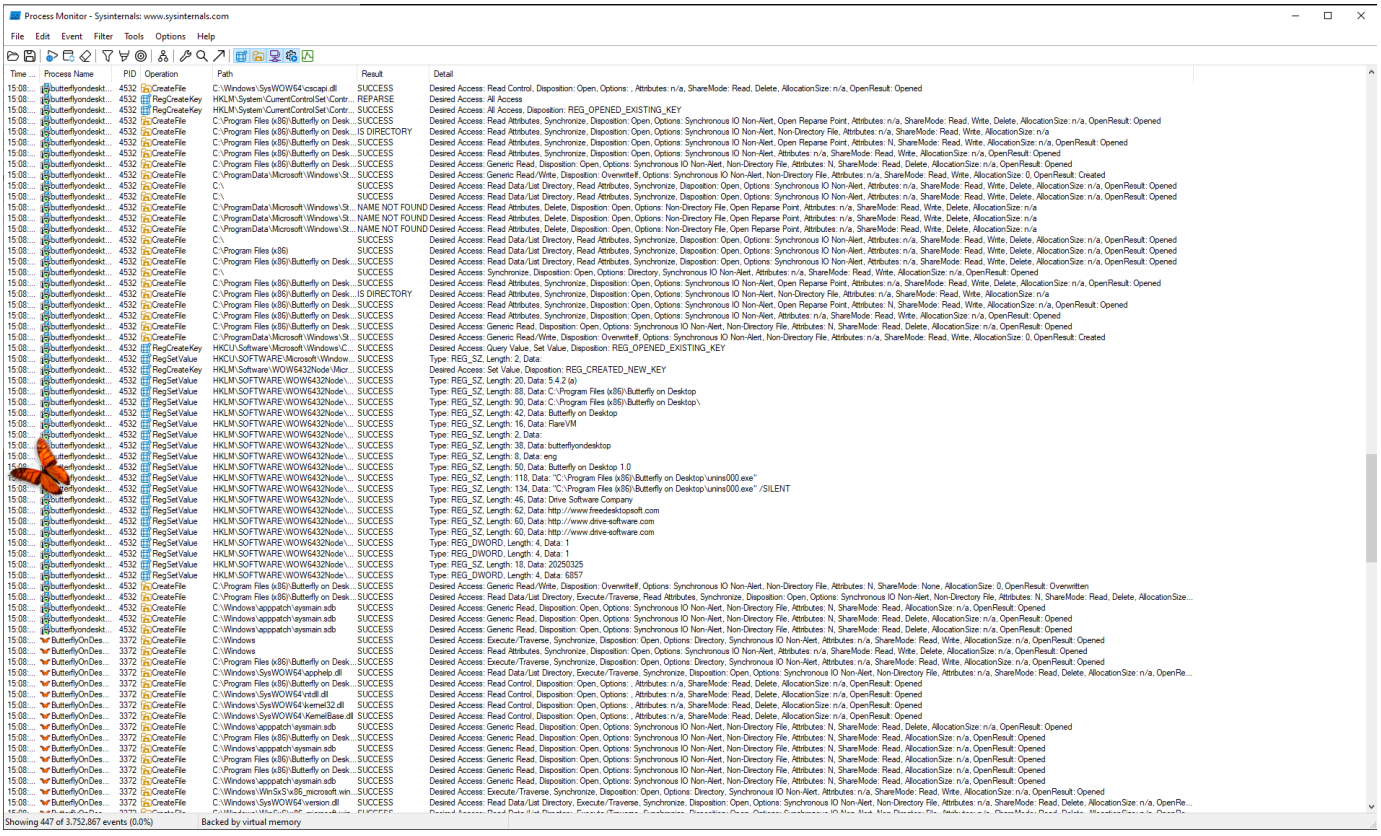
Il file non sembra essere firmato digitalmente, il che aumenta il livello di sospetto.
Le stringhe estratte suggeriscono che il malware potrebbe cercare di:

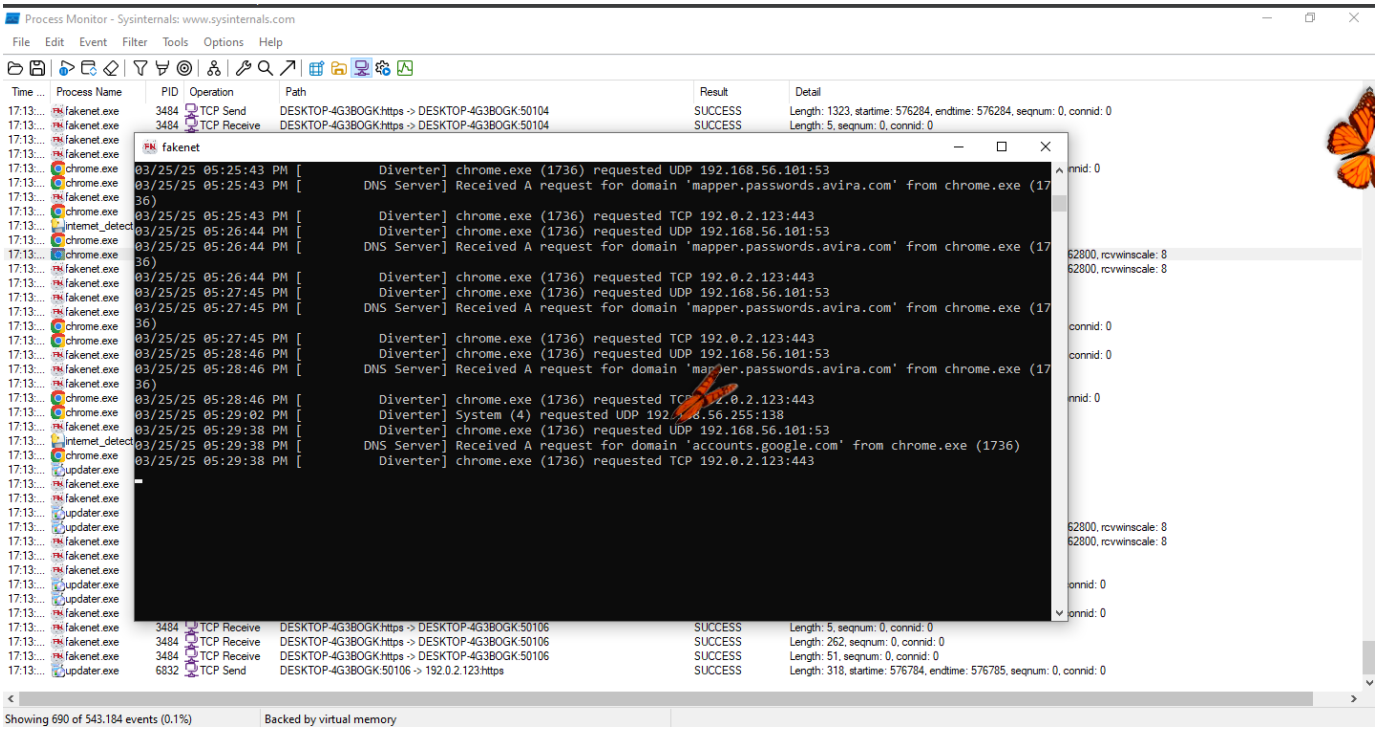
- Creare una voce nel registro di sistema per garantire la persistenza.
- Modificare file temporanei o creare nuovi file nel sistema.
- Leggere e modificare alcune impostazioni di sicurezza di Internet Explorer.

Analisi Dinamica

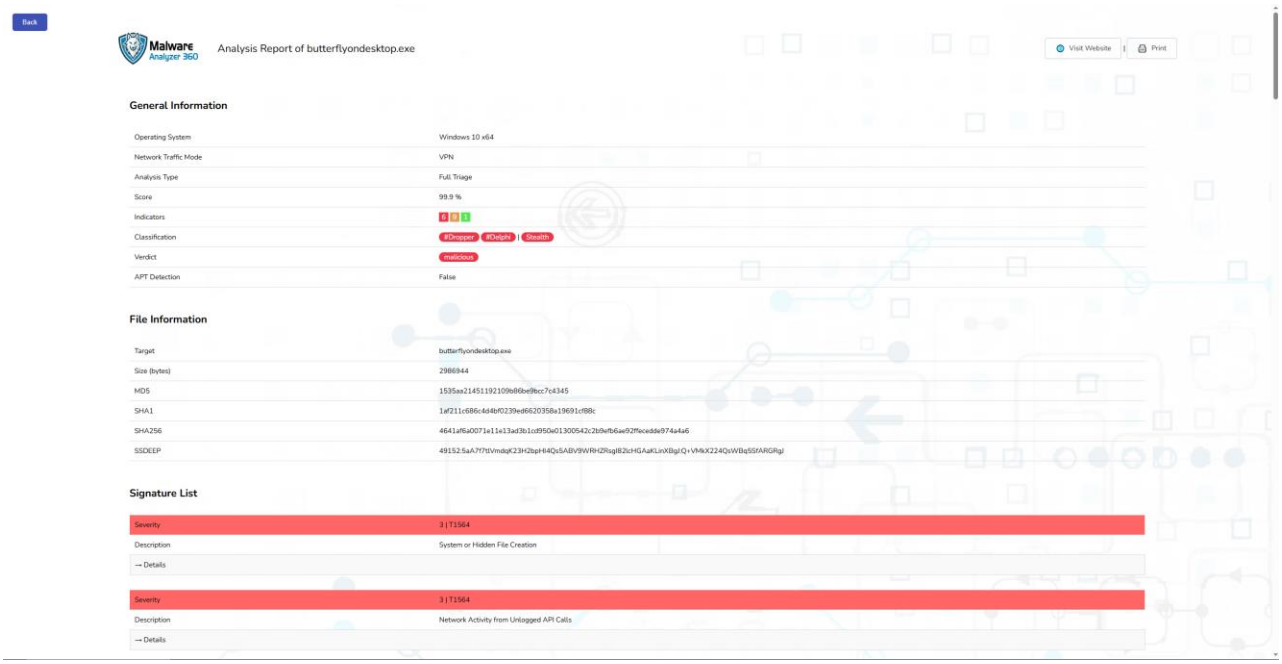
L'analisi dinamica è stata condotta eseguendo il malware in un ambiente controllato, come prima cosa avviamo fakenet per simulare una rete, avviamo procmon e procediamo con l'installazione del malware.

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.





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



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: 1535AA21451192109B86BE9BCC7C4345
SHA1: 1AF211C686C4D4BF0239ED6620358A19691CF88C
SHA256: 4641AF6A0071E11E13AD3B1CD950E01300542C2B9EFB6AE92FFECEDDE974A4A6
SSDEEP: 49152:5aA7f7tlVmdqK23H2bpHI4Qs5ABV9WRHZRsgI82lcHGAaKLinXBgJ:Q+VMkX224QsWBq5SfARGRgJ

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)
- slui.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.