Task 14/01/25: Attività di Analisi del Malware

Traccia

Obiettivo dell'Esercizio:

Sarà condiviso un malware relativamente innocuo.

Passaggi da Seguire:

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

Task 14/01/25: Attività di Analisi del Malware

Report

Introduzione:

Il seguente report documenta l'analisi statica e preliminare del malware "butterflyondesktop.exe", utilizzando strumenti come VirusTotal, Detect It Easy (DIE) e Strings. L'obiettivo è comprendere il comportamento del malware e identificare eventuali indicatori di compromissione (IOC).

1. Analisi con VirusTotal

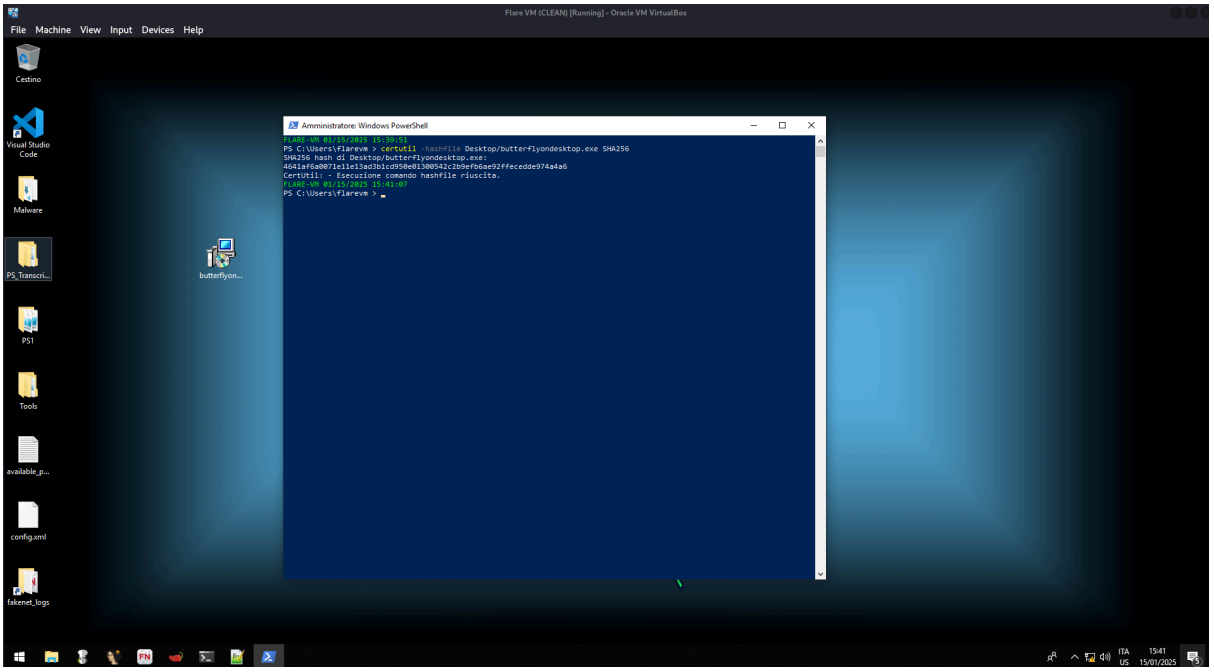
Hash del file SHA256
4641afa60071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6

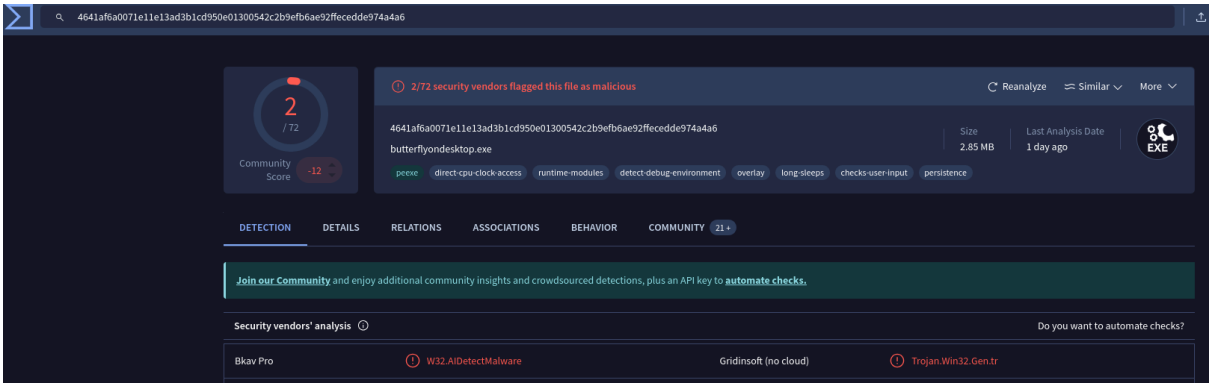
Risultati:
Numero di motori antivirus che identificano il file come malevolo 2/72

Rilevazioni

- Bkav Pro: W32.AIDetectMalware
- Gridinsoft (No Cloud): Trojan.Win32.Gen.tr

Indicatori di compromissione
Tecniche sospette identificate: utilizzo di accesso al clock della CPU, rilevazione di ambienti di debug, comportamenti persistenti e controlli sull'input dell'utente.





2. Analisi Statica con Detect It Easy (DIE)

Formato
PE32 (32-bit, GUI)

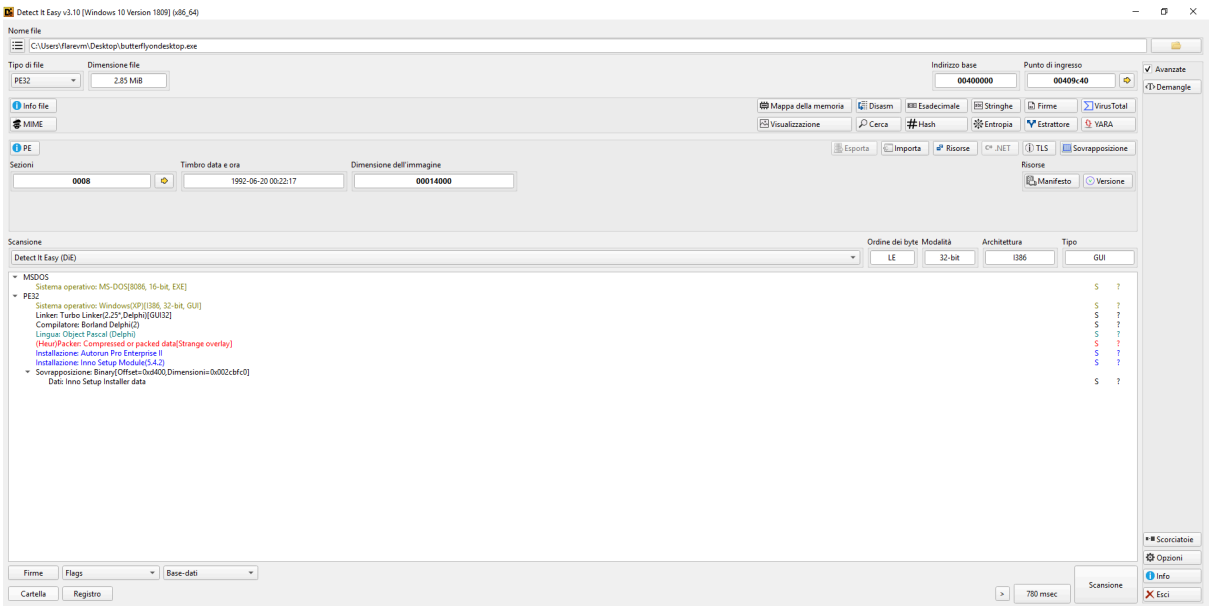
Compilatore
Borland Delphi (linguaggio Object Pascal)

Packer
Rilevato uso di compressione o sovrapposizione (Heur/packer).

Installazione rilevata
Inno Setup Module v5.4.2

Tecniche sospette:

- Overlay rilevato (Strange overlay)
- Potenziale uso di tecniche anti-debugging.



3. Strings Analysis

Stringhe significative individuate

Funzioni API:

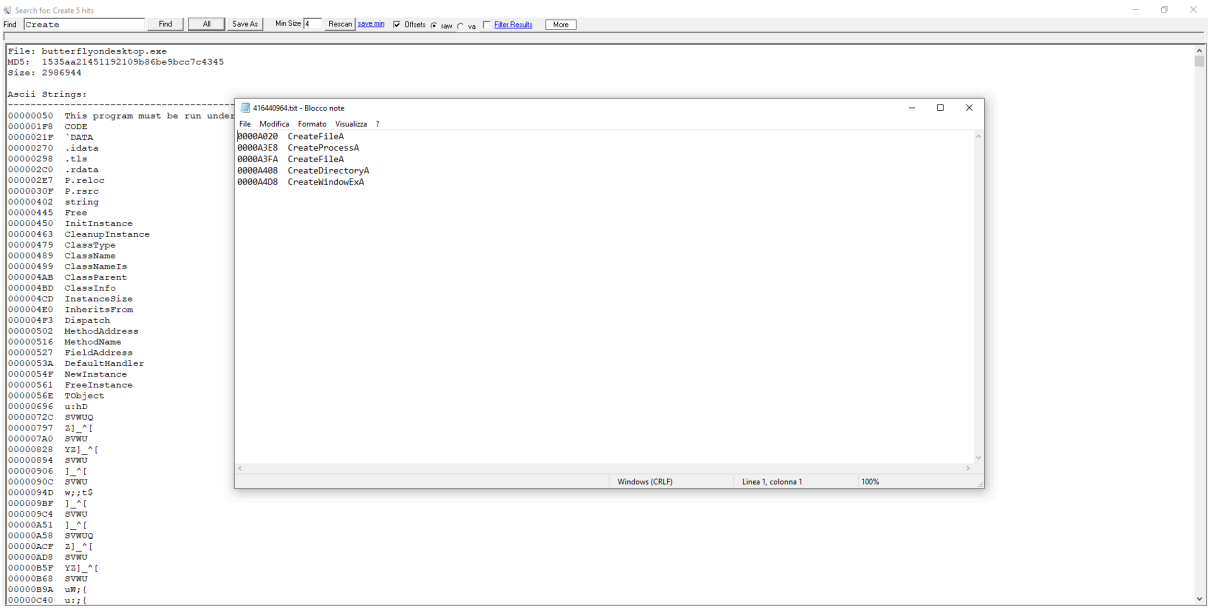
- CreateFileA
- CreateProcessA
- WriteFile
- RegOpenKeyExA
- OpenProcessToken

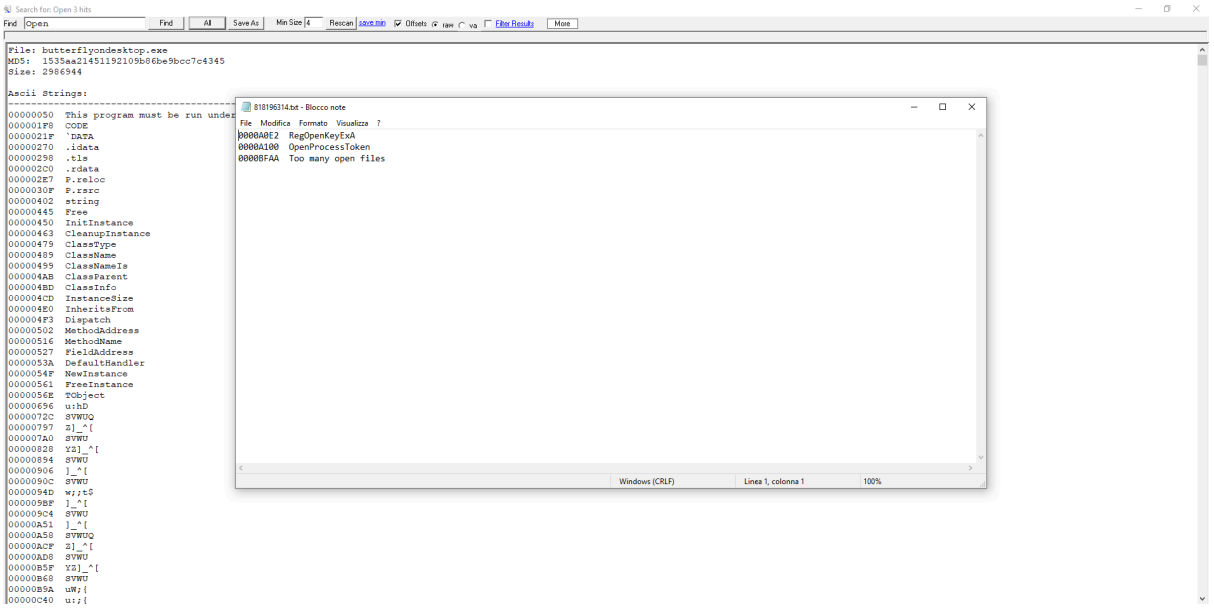
Altre stringhe sospette:

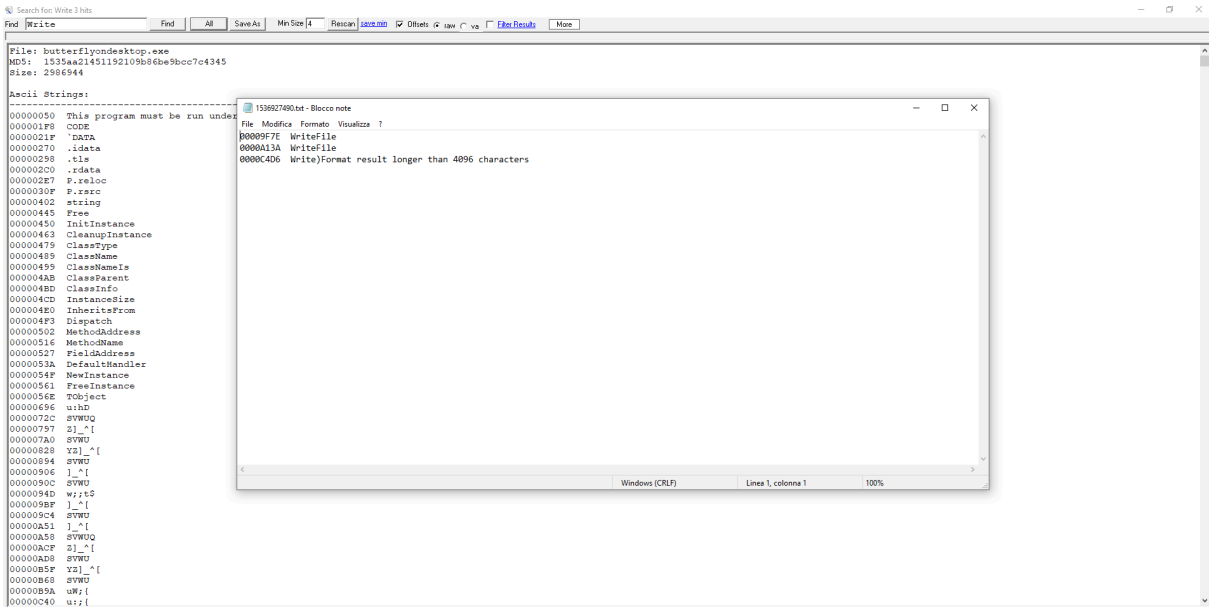
- "This program must be run under Win32"
- Percorsi generici come \DATA.

Queste API suggeriscono possibili operazioni di:

- Accesso a file.
- Creazione di nuovi processi.
- Manipolazione del registro di sistema.







Conclusione

L'analisi preliminare suggerisce che "butterflyondesktop.exe" potrebbe essere un malware dotato di funzionalità di:

- Manipolazione di file e registro di sistema.
- Esecuzione di nuovi processi.
- Anti-debugging per evadere strumenti di analisi.

Raccomandazioni di Sicurezza

- Identificare IOC e bloccare domini/IP collegati.
- Aggiornare regole degli antivirus per rilevare varianti di questo malware.