



ANALISI MALWARE

PROTECTING YOUR DIGITAL FUTURE





INTRO



In primis ho importato il malware da analizzare con wget
<https://github.com/Akir4d/The-MALWARE-Repo/raw/master/Spyware/butterflyondesktop.exe.zip>
unzip butterflyondesktop.exe.zip e salvato i relativi hash per i prossimi test

```
(kali㉿kali)-[~]
└─$ wget https://github.com/Akir4d/The-MALWARE-Repo/raw/master/Spyware/butterflyondesktop.exe.zip
unzip butterflyondesktop.exe.zip
--2025-05-27 10:29:02--  https://github.com/Akir4d/The-MALWARE-Repo/raw/master/Spyware/butterflyondesktop.exe.zip
Resolving github.com (github.com) ... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://raw.githubusercontent.com/Akir4d/The-MALWARE-Repo/master/Spyware/butterflyondesktop.exe.zip [following]
--2025-05-27 10:29:02--  https://raw.githubusercontent.com/Akir4d/The-MALWARE-Repo/master/Spyware/butterflyondesktop.exe.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.111.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2963532 (2.8M) [application/zip]
Saving to: 'butterflyondesktop.exe.zip.1'

butterflyondesktop.exe.zip.1          100%[=====]  2.83M  4.27MB/s  in
2025-05-27 10:29:03 (4.27 MB/s) - 'butterflyondesktop.exe.zip.1' saved [2963532/2963532]

Archive: butterflyondesktop.exe.zip
[butterflyondesktop.exe.zip] butterflyondesktop.exe password:
  inflating: butterflyondesktop.exe  successg... 56L2.png  S7L3c.png  barbero_sa...  S7L5(3)ses...  outputql.png  S7L5(12)set...  S7L5(5)file...  BW2.png

(kali㉿kali)-[~]
└─$ sha256sum butterflyondesktop.exe
md5sum butterflyondesktop.exe
4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6  butterflyondesktop.exe
1535aa21451192109b86be9bcc7c4345  butterflyondesktop.exe
```

VIRUSTOTAL

dopo aver provato ad analizzare il file .exe su virustotal questo è ciò che ho notato

1. Hash del File:

4641af6a0071e11e13ad3b1cd950e01300542c2b9efb
6ae92ffecedde974a4a8 (Identificatore unico del
file basato sul suo contenuto)

2. Risultati della Scansione:

- 1 su 72 vendor di sicurezza ha classificato il file come malware
- La maggior parte degli scanner (inclusi Acronis, AinLab-V3 e Alibaba) non ha rilevato minacce
- Solo "Blow Pro" lo ha identificato come "W32-AlDeleteNahware"

3. Comportamento Sospetto:

- Il file mostra caratteristiche preoccupanti come:
 - Persistenza nel sistema
 - Interazione con l'ambiente utente
 - Possibile overlay (tecnica usata per nascondere attività malevole)

Valutazione del Rischio

- Basso tasso di rilevamento: Solo 1 scanner su 72 lo segnala come malevolo
- Possibile falso positivo: Potrebbe essere un file legittimo erroneamente contrassegnato
- Comportamenti sospetti: Le caratteristiche evidenziate meritano ulteriore analisi



The screenshot shows the VirusTotal analysis interface for the file 4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a8. The main summary indicates that 1 out of 72 security vendors flagged the file as malicious. The file is named butterflyondesktop.exe, has a size of 2.85 MB, and was last analyzed 17 minutes ago. Below the summary, tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY are visible. The BEHAVIOR section highlights suspicious behaviors like persistence, long sleeps, and runtime modules. The SECURITY VENDORS' ANALYSIS section shows results from Bkav Pro (W32.AIDetectMalware), AhnLab-V3 (Undetected), Acronis (Static ML) (Undetected), and Alibaba (Undetected).

Vendor	Detection	Notes
Bkav Pro	W32.AIDetectMalware	Detected
AhnLab-V3	Undetected	Undetected
Acronis (Static ML)	Undetected	Undetected
Alibaba	Undetected	Undetected

MALWARE BAZAAR

```
ho provato a consultare  
Malwarebazaar utilizzando il  
comando curl -X POST https://mb-  
api.abuse.ch/api/v1/ \  
-d 'query=get_info' \  
-d  
'hash=4641af6a0071e11e13ad3b1cd95  
0e01300542c2b9efb6ae92ffecedde9  
74g4a6'
```



```
$ curl -X POST https://mb-api.abuse.ch/api/v1/directory
-d 'query=get_info'
-d 'hash=4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6'
{ $ curl https://github.com/Akir4d/The-MALWARE-Repo/raw/master/Spyware/butterflyondesktop.exe
  "query_status": "ok", "exe.zip"
  "data": [
    {
      "sha256_hash": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
      "sha3_384_hash": "2e83a12c4e8374c7df2902a2c3f40fe8d13d2811cea298df2bb8adf4",
      "sha1_hash": "1af211c686c4d4bf0239ed6620358a19691cf88c",
      "md5_hash": "1535aa21451192109b86be9bcc7c4345",
      "first_seen": "2025-01-24 03:58:51",
      "last_seen": "2025-05-07 11:19:38",
      "file_name": "Butterfly On Desktop.exe",
      "Length": 2963,
      "file_size": 2986944,
      "file_type_mime": "application/x-dosexec",
      "file_type": "exe",
      "reporter": "BastianHein_",
      "origin_country": "CL",
      "anonymous": 0,
      "signature": null,
      "imphash": "884310b1928934402ea6fec1dbd3cf5e",
      "tlsh": "T1CAD533476FCD0474E318EF38AE79C1DC586FBAA93539244937CC869423E23E9",
      "infesting_file": "butterflyondesktop.exe",
      "telfhash": null,
      "gimphash": null,
      "ssdeep": "49152:5aA7f7tlVmdqK23H2bpHI4Qs5ABV9WRHZRsgI82lcHGAaKLInXBgJ:Q+V",
      "magika": "pebin",
      "md5sum_butterflyondesktop.exe": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
      "dhash_icon": "b298acbab2ca7a72",
      "trid": [
        {
          "hash": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
          "name": "76.2% (.EXE) Inno Setup Installer (107240\\4\\30)",
          "confidence": 76.2
        },
        {
          "hash": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
          "name": "10.0% (.EXE) Win32 Executable Delphi generic (14182\\79\\4)",
          "confidence": 10.0
        },
        {
          "hash": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
          "name": "4.6% (.DLL) Win32 Dynamic Link Library (generic) (6578\\25\\2)",
          "confidence": 4.6
        },
        {
          "hash": "4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6",
          "name": "3.2% (.EXE) Win32 Executable (generic) (4504\\4\\1)",
          "confidence": 3.2
        }
      ]
    }
  ],
  "verdict": "Malicious activity",
  "file_name": "3733dd006aac034c22ce60b0262d33b24f11575c4197165348de4ca1427bac37.exe",
  "date": "2024-05-19 18:29:08",
  "analysis_url": "https://app.any.run/tasks/5ae9cb4d-e104-41ff-ad2b-2527c4c29a0a",
  "tags": [
    "malware",
    "malwarefamily"
  ]
}

```



DURANTE L'ANALISI STATICÀ CON STRINGS, ABBIAMO TROVATO NUMEROSE STRINGHE CHE INDICANO CHE L'ESEGUIBILE BUTTERFLYONDESKTOP.EXE È UN'APPLICAZIONE SCRITTA IN DELPHI, COME MOSTRANO RIFERIMENTI A TOBJECT, INITINSTANCE, E DISPATCH. È STRUTTURATO SECONDO IL FORMATO PE DI WINDOWS E CONTIENE STRINGHE OFFUScate CHE SUGGERISCONO COMPORTAMENTI SOSPETTI, PROBABILMENTE CARICATI DINAMICAMENTE IN FASE DI ESECUZIONE PER EVITARE IL RILEVAMENTO. LA PRESENZA DELLA STRINGA "THIS PROGRAM MUST BE RUN UNDER WIN32" CONFERMA CHE IL FILE È DESTINATO A SISTEMI OPERATIVI WINDOWS.

UTILIZZANDO EXIFTOOL, È STATO ANALIZZATO IL FILE BUTTERFLYONDESKTOP.EXE. DAI METADATI EMERGE CHE SI TRATTA DI UN ESEGUIBILE PE32 A 32 BIT CON INTERFACCIA GRAFICA (WINDOWS GUI). LA DESCRIZIONE INDICA UN'APPLICAZIONE APPARENTEMENTE INNOCUA, "BUTTERFLY ON DESKTOP", E IL FILE È STATO IMPACCHETTATO CON INNO SETUP, UNO STRUMENTO COMUNE PER CREARE INSTALLAZIONI WINDOWS. QUESTO SUGGERISCE CHE IL MALWARE POTREBBE ESSERE OFFUSCATO ALL'INTERNO DI UN INSTALLER, TIPICO COMPORTAMENTO PER NASCONDERE SPYWARE. L'USO DI DATA FASULLE (TIMESTAMP DEL 1992) PUÒ INDICARE UN TENTATIVO DI ELUDERE I SISTEMI DI SICUREZZA AUTOMATICA O I FILTRI CRONOLOGICI DEI SISTEMI ANTIVIRUS. INOLTRE, LA PRESENZA DI UNA VERSIONE MANCANTE O STRINGHE VUOTE NEI CAMPI FILE/PRODUCT VERSION È UN ALTRO INDIZIO CHE IL FILE POTREBBE ESSERE STATO ALTERATO.

CUCKOO



DURANTE L'ANALISI DINAMICA DEL FILE BUTTERFLYONDESKTOP.EXE UTILIZZANDO CUCKOO SANDBOX, ABBIAMO OSSERVATO DIVERSI ELEMENTI INTERESSANTI. IL FILE, UN ESEGUIBILE WINDOWS A 32 BIT DI CIRCA 2.8 MB, SI PRESENTA UFFICIALMENTE COME UN PRODOTTO DELLA "DRIVE SOFTWARE COMPANY" CON IL NOME "BUTTERFLY ON DESKTOP". TUTTAVIA, NONOSTANTE QUESTA APPARENTE LEGITTIMITÀ, L'ANALISI HA RIVELATO COMPORTAMENTI SOSPESSI CHE SUGGERISCONO UNA POSSIBILE NATURA DANNOSA.

CUCKOO HA ASSEGNATO AL FILE UN PUNTEGGIO DI RISCHIO PARI A 3.7 SU 10, INDICANDO LA PRESENZA DI AZIONI ANOMALE MA NON ESTREMAMENTE PERICOLOSE. TRA QUESTE, SONO EMERSI TENTATIVI DI DISABILITARE PROTEZIONI DI MEMORIA COME IL DEP, OPERAZIONI VOLTE A OTTENERE PRIVILEGI ELEVATI E MODIFICHE AL REGISTRO DI SISTEMA, TUTTE TIPICHE DI MALWARE CHE CERCANO DI COMPROMETTERE LA SICUREZZA DEL SISTEMA. INOLTRE, IL MALWARE SEMBRA MANIPOLARE TOKEN DI AUTENTICAZIONE E AGIRE SU FILE E CONFIGURAZIONI DELL'UTENTE, AZIONI CHE POSSONO FACILITARE UN'INTRUSIONE SILENTE. UN ULTERIORE SEGNALE SOSPETTO RIGUARDA L'ALLOCAZIONE DI MEMORIA ESEGUIBILE TRAMITE FUNZIONI COME NTPROTECTVIRTUALMEMORY E NTALLOCATEVIRTUALMEMORY. QUESTO COMPORTAMENTO È TIPICO DI MALWARE CHE UTILIZZANO TECNICHE DI UNPACKING O DI CODICE AUTO-MODIFICANTE PER NASCONDERE IL PROPRIO FUNZIONAMENTO. INOLTRE, È STATO RILEVATO L'USO DELLA FUNZIONE ISDEBUGGERPRESENT, IMPIEGATA PER EVITARE L'ANALISI TRAMITE DEBUGGER, UNA TECNICA ANTI-ANALISI PIUTTOSTO COMUNE TRA I PROGRAMMI DANNOSI.

IL FILE SEMBRA INOLTRE ESSERE STATO CONFEZIONATO CON UN PACKER, COME INDICATO DALLA PRESENZA DI SEZIONI PE NON STANDARD, PROBABILMENTE PER OFFUSCARE IL CODICE E RENDERNE PIÙ DIFFICILE IL RILEVAMENTO. IL MALWARE HA ANCHE INTERAGITO CON CHIAVI DI REGISTRO TIPICHE DI PROGRAMMI INSTALLATI, PROBABILMENTE PER CAMUFFARSI DA SOFTWARE LEGITTIMO.

DURANTE L'ESECUZIONE, NON È STATO RILEVATO ALCUN TRAFFICO DI RETE, SUGGERENDO CHE IL MALWARE POTESSE ESSERE IN FASE DI INSTALLAZIONE O IN ATTESA DI UNA CONDIZIONE SPECIFICA PER ATTIVARSI. DAL PUNTO DI VISTA DEL RILEVAMENTO ANTIVIRUS, SOLO UNO DEI MOTORI SU VIRUSTOTAL HA RICONOSCIUTO IL FILE COME POTENZIALMENTE DANNOSO, IL CHE INDICA CHE POTREBBE TRATTARSI DI UN MALWARE POCO CONOSCIUTO O PERSONALIZZATO.

IN CONCLUSIONE, NONOSTANTE L'ASpetto APPARENTEMENTE INNOCUO DI QUESTA APPLICAZIONE, I COMPORTAMENTI EVIDENZIATI FANNO PENSARE A UN SOFTWARE POTENZIALMENTE PERICOLOSO, CON CARATTERISTICHE TIPICHE DI MALWARE UTILIZZATI PER SPIONAGGIO O INTRUSIONE. PER QUESTO MOTIVO, SI CONSIGLIA DI ISOLARE IL FILE E DI EVITARNE L'ESECUZIONE SU SISTEMI REALI.

<https://cuckoo.cert.ee/analysis/6514992/summary>