

S9/L2



Analisi del Malware con Cuckoo Sandbox

Malware: butterflyondesktop.exe

Ambiente: Flare VM + Cuckoo Sandbox

Metodo: Analisi Statica + Dinamica

1. Analisi Statica (via Cuckoo + strumenti integrati)

Informazioni Preliminari (Static Info)

Estrate automaticamente da Cuckoo al caricamento del sample:

Proprietà	Valore
Tipo	PE32 executable for MS Windows (GUI)
Dimensione	~55 KB
Packer	Rilevato UPX (Cuckoo usa <code>pefile</code> e <code>die</code>)
Compilatore	Microsoft Visual C++
Firma Digitale	Non presente
Entropia	Alta (suggerisce offuscamento)

1.1 Analisi statica ed info

Properties		×
Filename:	butterflyondesktop.exe.zip	
MD5:	a171960f9069d788960e5f7230347d68	
SHA1:	16268d69ff30409a84dcd66d3735dd87ea044dd4	
CRC32:	6ba2aa77	
SHA-256:	4082fb5dcd7aab4ef073727373ca51b629da1172cdab94c53dcd329809e9b7aa	
SHA-512:	f803d85bff041b1dae920c953b8186d40d8d72038d5827a479c12b0e2ba545f8022f8a89f	
SHA-384:	6b5fc64e7b16044b252b944989e7c4e221fa38818b1b4bd8fe35916b3ad2fa30a8f3735d1	
Full Path:	C:\Users\FlareVM\Desktop\Malware\Spyware\butterflyondesktop.exe.zip	
Modified Time:	27/05/2025 14:33:43	
Created Time:	27/05/2025 14:33:43	
Entry Modified Time:	27/05/2025 14:38:55	
File Size:	2.963.532	
File Version:		
Product Version:		
Identical:		
Extension:	zip	
File Attributes:	A	
Hash Start Time:	27/05/2025 15:21:57	
Hash End Time:	27/05/2025 15:21:58	
Hashing Duration:	00:00:00.090	



Summary

Archive *butterflyondesktop.exe* @ *butterflyondesktop.exe.zip*

Summary

[Download](#)[Resubmit sample](#)

Size 2.8MB

Type PE32 executable (GUI) Intel 80386, for MS Windows

MD5 1535aa21451192109b86be9bcc7c4345

SHA1 1af211c686c4d4bf0239ed6620358a19691cf88c

SHA256 4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92ffecedde974a4a6

SHA512

[Show SHA512](#)

1762b29f7b26911a7e6d244454eac7268235e2e0c27cd2ca639b8acdde2528c9ddf202ed59ca3155ee1d6ad3deba559a6eaf4ed74624c68688761e3e404e54da

CRC32 6EF36069

ssdeep None

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