S9/L2

🧪 Analisi del Malware con Cuckoo Sandbox

Malware: `butterflyondesktop.exe`
Ambiente: Flare VM + Cuckoo Sandbox
Metodo: Analisi Statica + Dinamica

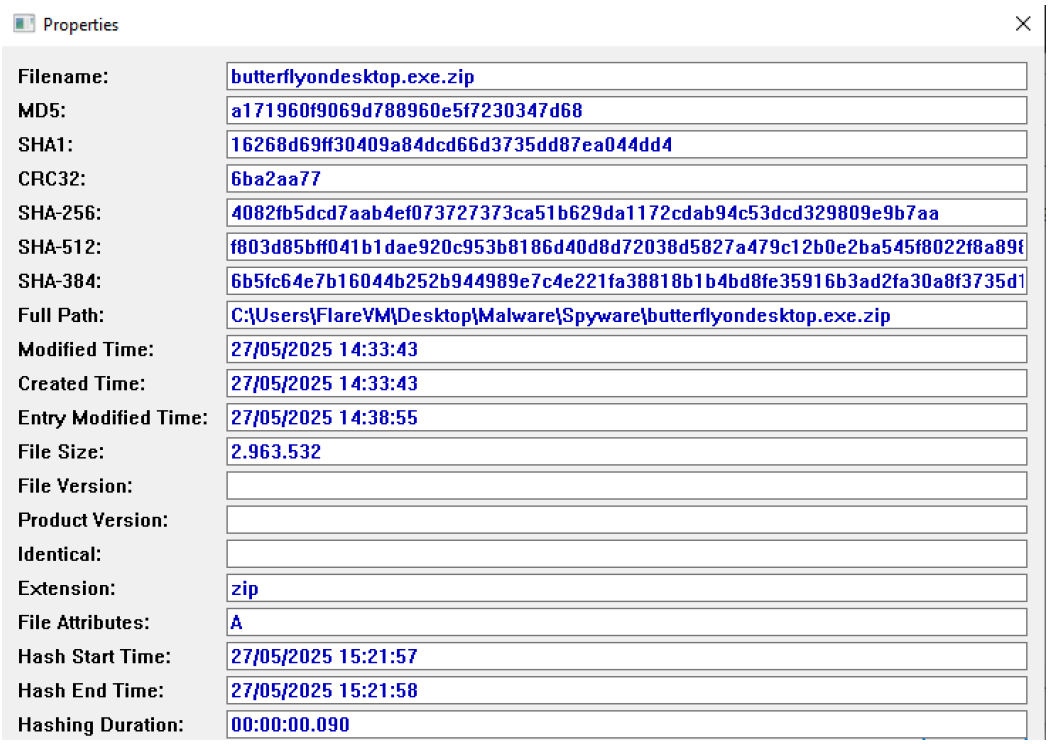
1. Analisi Statica (via Cuckoo + strumenti integrati)

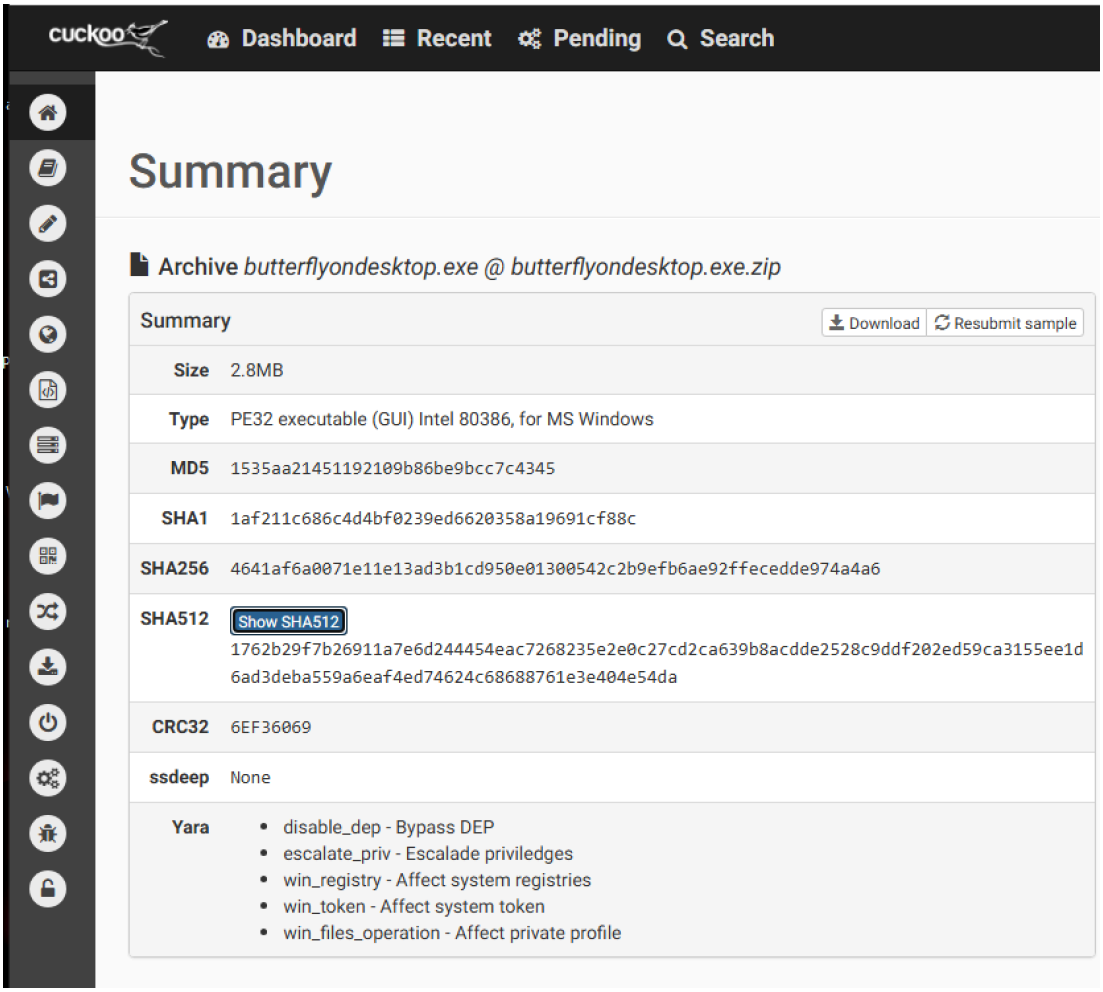
Informazioni Preliminari (Static Info)

Estratte automaticamente da Cuckoo al caricamento del sample:

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

1.1 Analisi statica ed info




cuckoo
Dashboard
Recent
Pending
Search
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 priviledges
win_registry - Affect system registries
win_token - Affect system token
win_files_operation - Affect private profile