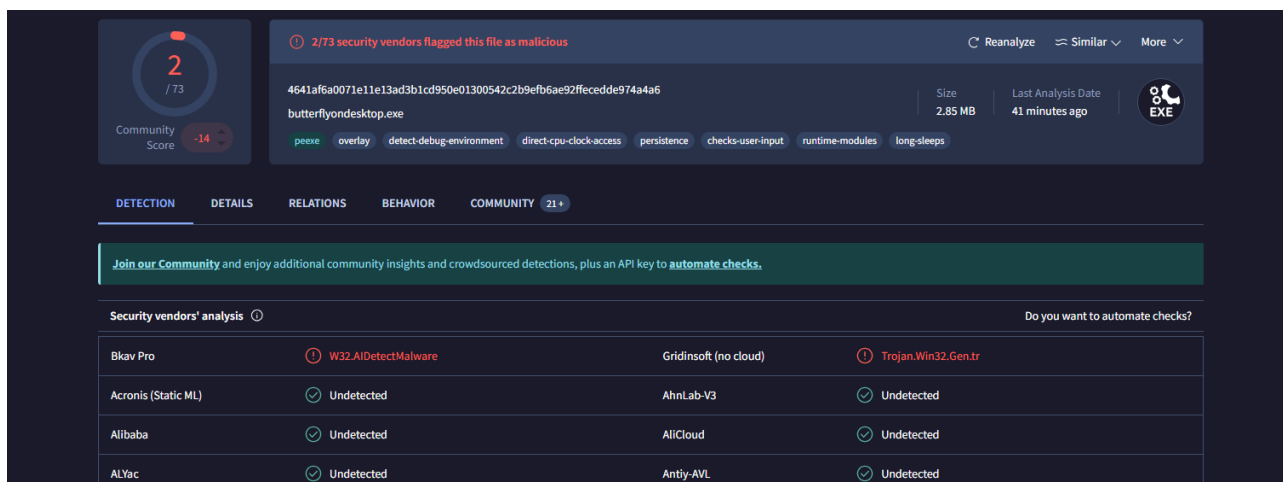


ANALISI DEL MALWARE butterflyondestop.exe

ANALISI STATICA

Partiamo con il caricamento del file sul sito virustotal.com

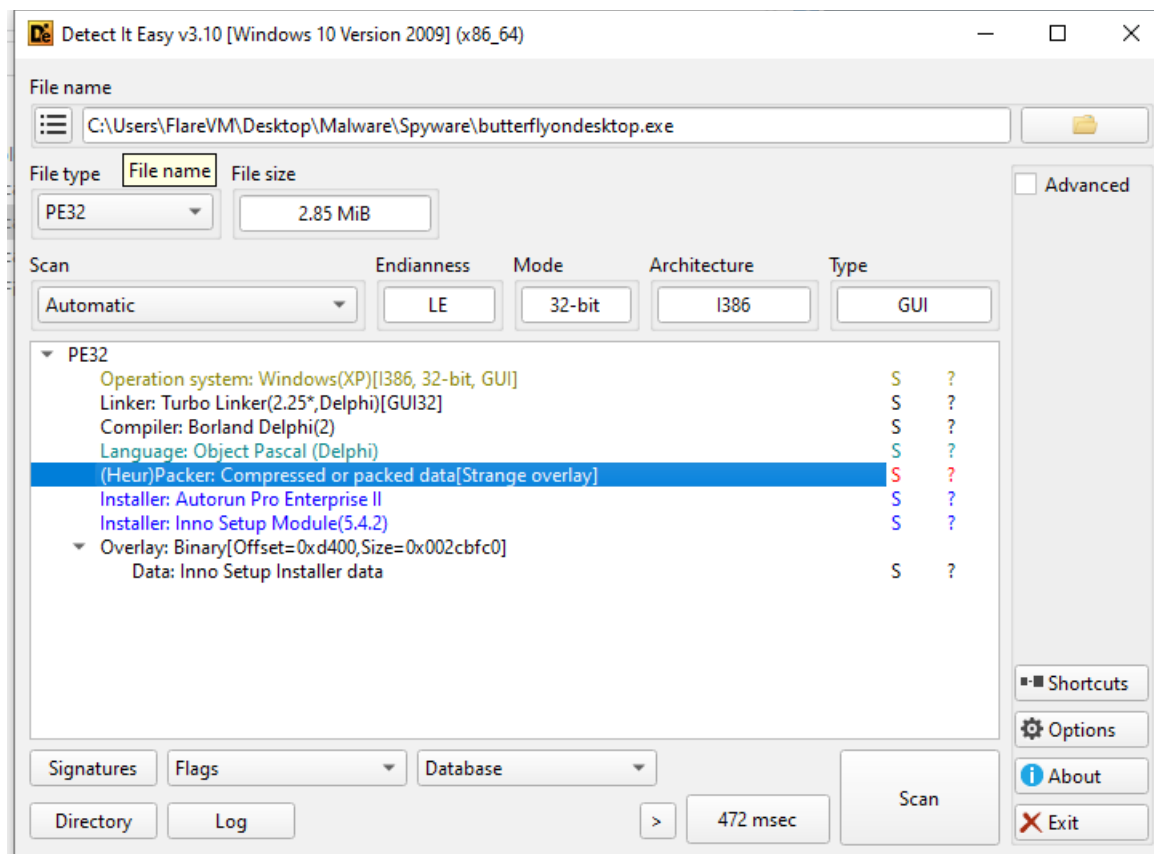


The screenshot shows the VirusTotal interface for the file butterflyondestop.exe. The file is identified by hash 4641af6a0071e11e13ad3b1cd950e01300542c2b9efb6ae92fcedde974a46. It is 2.85 MB and was last analyzed 41 minutes ago. The file is flagged as malicious by 2/73 security vendors. The community score is 2/73, with a -14 change. The file is categorized as a Trojan.Win32.Gen.tr. The analysis shows that the file is detected by two commercial antivirus engines: Bkav Pro and Gridinsoft (no cloud). The file is not detected by Acronis (Static ML), Alibaba, ALYac, AhnLab-V3, AliCloud, and Antiy-AVL. The file is also detected by the community as a Trojan.Win32.Gen.tr.

Security vendors' analysis	Do you want to automate checks?		
Bkav Pro	W32.AIDetectMalware	Gridinsoft (no cloud)	Trojan.Win32.Gen.tr
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Qui vediamo che il file viene rilevato come malevolo da due antivirus in commercio. Nella sezione community sembra ci sia discordanza tra gli utenti, tra chi lo considera sicuro e chi lo definisce dannoso, in quanto può portare ad una diminuzione delle prestazioni del PC.

Andiamo ad analizzarlo in ambiente sicuro. Cominciamo analizzandolo con Detect It Easy e notiamo che viene rilevato (Heur) Packer, cioè viene rilevato un packer/compressore con un overlay sospetto ("Strange overlay"). Questo è un indizio importante, poiché molti malware utilizzano packer per offuscare il codice e rendere più difficile l'analisi.



The screenshot shows the Detect It Easy v3.10 interface. The file name is C:\Users\FlareVM\Desktop\Malware\Spyware\butterflyondestop.exe. The file type is PE32 and the file size is 2.85 MiB. The scan is set to Automatic. The analysis results show the following details:

Scan	Endianness	Mode	Architecture	Type
Automatic	LE	32-bit	I386	GUI

PE32

- Operation system: Windows(XP)[I386, 32-bit, GUI] S ?
- Linker: Turbo Linker(2.25*,Delphi)[GUI32] S ?
- Compiler: Borland Delphi(2) S ?
- Language: Object Pascal (Delphi) S ?
- (Heur)Packer: Compressed or packed data[Strange overlay] S ?
- Installer: Autorun Pro Enterprise II S ?
- Installer: Inno Setup Module(5.4.2) S ?
- Overlay: Binary[Offset=0xd400,Size=0x002cbfc0] S ?
 - Data: Inno Setup Installer data

Signatures: Flags: Database: Scan: 472 msec

Fatto ciò, andiamo ad analizzare il file con CFF Explorer
Sezione Dos Header

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

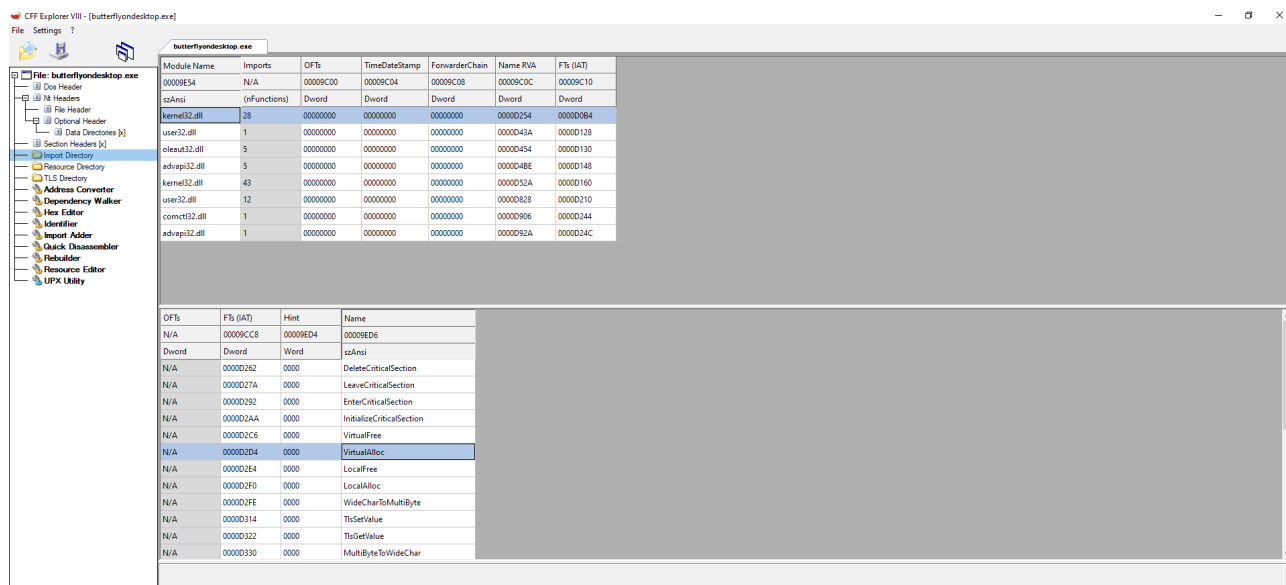
File: butterflyondesktop.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- TLS Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0050
e_cp	00000004	Word	0002
e_crlc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	000F
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarlc	00000018	Word	0040
e_ovno	0000001A	Word	001A
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000
	00000032	Word	0000
	00000034	Word	0000
	00000036	Word	0000
	00000038	Word	0000
	0000003A	Word	0000
e_ifanew	0000003C	Dword	00000100

e_magic: 5A4D - Questo è il campo di firma del DOS Header. Il valore 5A4D corrisponde alle lettere "MZ" in ASCII, che è la firma standard per un file eseguibile DOS e indica che il file è un eseguibile valido.

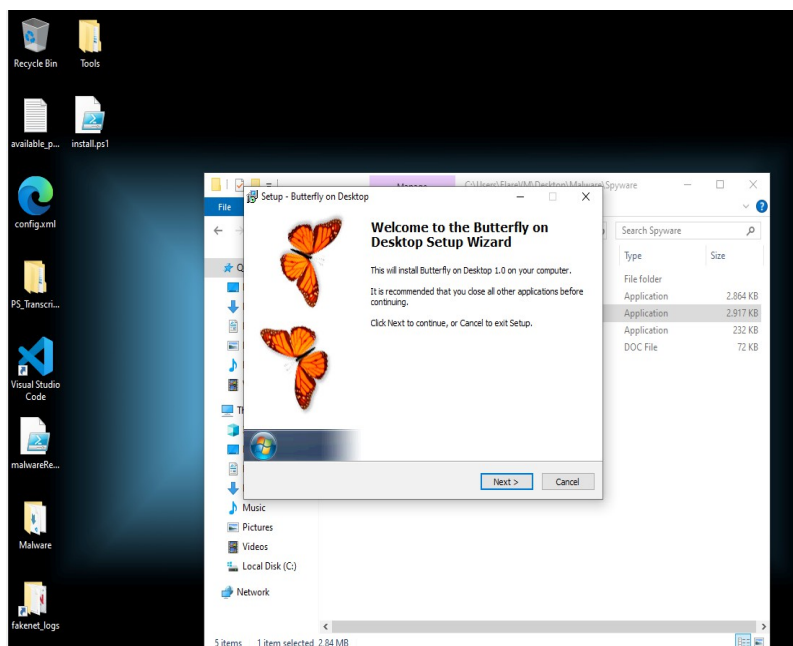
Analisi statica con CFF Explorer – Sezione Import Directory

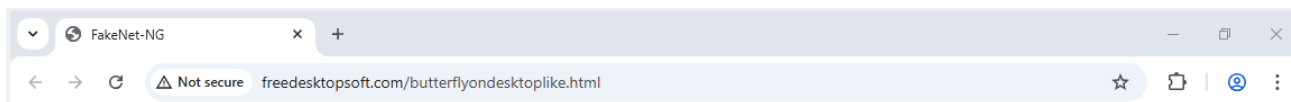


Qui notiamo che il malware andrà a caricare le .dll kernel32, user32, advapi32, oleaut32, comctl32. Le prime 3 ci mettono già in allarme perchè sono quelle più critiche per il sistema Windows, poichè sono quelle che vanno a gestire numerosi aspetti e funzionalità del Sistema operativo. La oleaut32 oleaut32.dll è un componente di sistema critico in Windows, responsabile della gestione di varie funzioni di automazione e scripting. La comctl32.dll è un componente di sistema cruciale in Windows, responsabile della visualizzazione e della gestione dei controlli comuni dell'interfaccia utente.

Analisi Dinamica

Per l'analisi dinamica, avviamo il Process Monitor e dopo di che il file butterflydesktop.exe. Dopo il processo di installazione e l'avvio dell'applicazione installata avremo sullo schermo due vistose farfalle che volano e l'apertura automatica del browser sulla pagina butterflydesktoplike.html. Nell'immagine si noti che è stata “bloccata” dal tool FakeNet già avviato sulla macchina virtuale





FakeNet-NG is a next generation dynamic network analysis tool for malware analysts and penetration testers. It is open source and designed for the latest versions of Windows.

The tool allows you to intercept and redirect all or specific network traffic while simulating legitimate network services. Using FakeNet-NG, malware analysts can quickly identify malware's functionality and capture network signatures. Penetration testers and bug hunters will find FakeNet-NG's configurable interception engine and modular framework highly useful when testing application's specific functionality and prototyping PoCs.

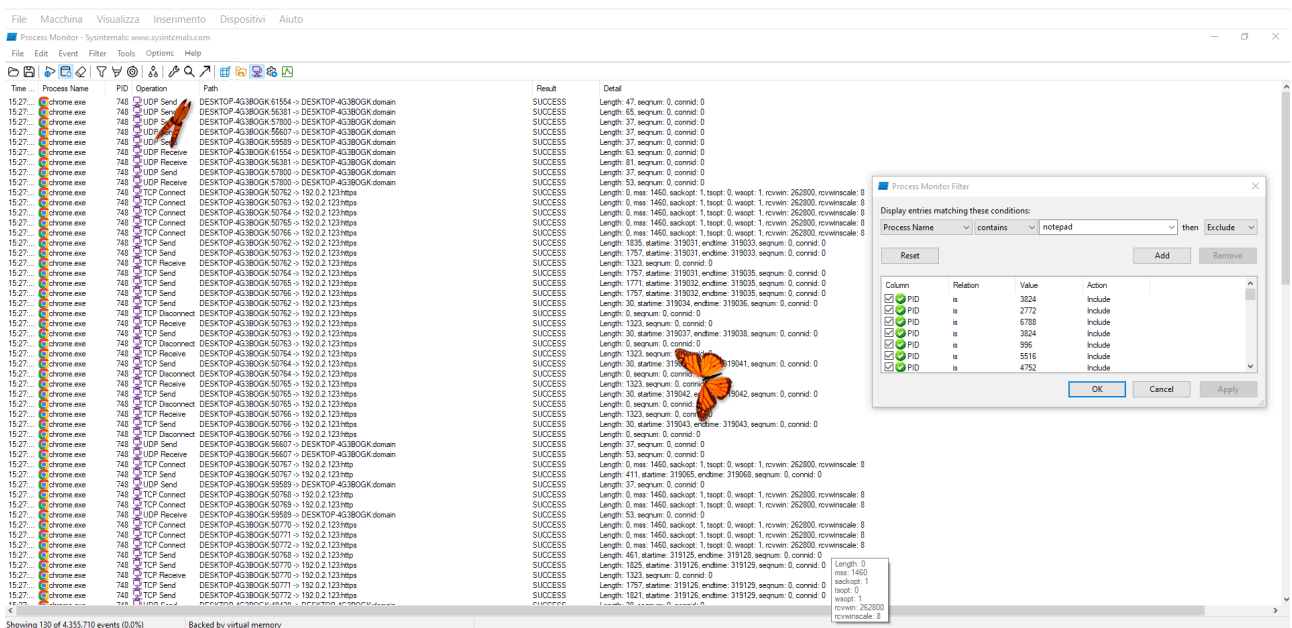
FakeNet-NG is based on the excellent Fakenet tool developed by Andrew Honig and Michael Sikorski.

Contact

For bugs, crashes, or other comments please contact **The FLARE Team** by email FakeNet@mandiant.com.



Su Process Monitor andiamo ad applicare vari filtri per poter analizzare quanto operato solo dall'installer e dall'applicazione da esso installato riferito al malware sotto esame.



Dall'analisi possiamo notare che ci sono state moltissimi processi da parte dell'applicazione atti a modificare o creare nuovi .dll all'interno del sistema.