

S9-L2

ANALISI MALWARE



TRACCIA



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



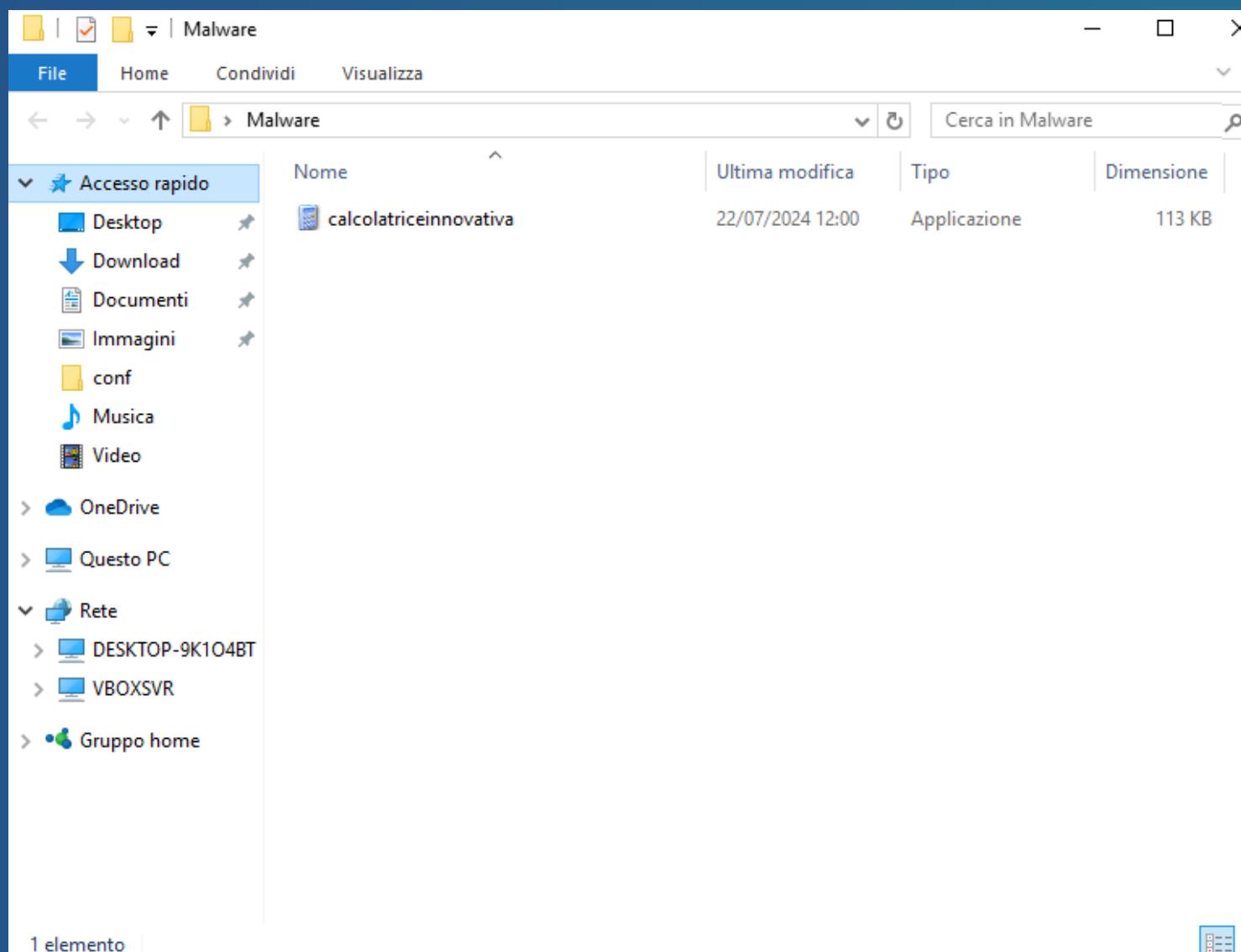
DIFFERENZA TRA ANALISI STATICÀ E DINAMICA

L'analisi del malware si divide in statica e dinamica, due approcci complementari usati per comprenderne il funzionamento.

L'analisi statica studia il malware senza eseguirlo, esaminandone il codice e le strutture interne per individuare funzioni o algoritmi dannosi. È sicura, ma può essere ostacolata da tecniche di offuscamento. L'analisi dinamica, invece, osserva il comportamento del malware in esecuzione in un ambiente controllato, rivelando azioni come modifiche al sistema o connessioni di rete. Questo metodo è più pratico ma rischioso se non ben confinato e vulnerabile a tecniche di evasione.

La combinazione dei due approcci è essenziale: l'analisi statica svela l'intenzione nascosta del malware, mentre quella dinamica ne evidenzia gli effetti reali. Questo equilibrio è fondamentale per proteggersi dalle minacce informatiche e sviluppare sistemi di rilevamento più efficaci.

MALWARE



Malware fornito per l'analisi

VIRUS TOTAL

Abbiamo iniziato con un'analisi statica analizzando il file.exe senza eseguirlo utilizzando virus total. Già qua potremo facilmente fermarci e dire che è a tutti gli effetti un malware, tuttavia continueremo le nostre analisi.

The screenshot shows the VirusTotal analysis interface for a file named 'CALC.EXE'. The main summary card displays a 'Community Score' of 60/72, indicating that 60 out of 72 security vendors flagged the file as malicious. Below the score, the file's SHA256 hash is listed as 'b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f...', and its size is '112.50 KB'. The 'Last Analysis Date' is '10 minutes ago'. A small icon of a calculator with the letters 'EXE' next to it is shown. The interface includes tabs for DETECTION, DETAILS, RELATIONS, ASSOCIATIONS, BEHAVIOR, and COMMUNITY (with 9 items). A call-to-action button says 'Join our Community'. Below the main card, there are sections for 'Popular threat label' (trojan.swort/cryptz), 'Threat categories' (trojan), and 'Family labels' (swort, cryptz, marte). The 'Security vendors' analysis' section lists various vendor detections, such as Alibaba (Trojan:Win32/CobaltStrike.5c89), AliCloud (Backdoor:Win/meterpreter.A), ALYac (Trojan.CryptZ.Marte.1.Gen), Antiy-AVL (Trojan/Win32.Rozena), Arcabit (Trojan.CryptZ.Marte.1.Gen), Avast (Win32:SwPatch [Wrm]), AVG (Win32:SwPatch [Wrm]), Avira (no cloud) (TR/Patched.Gen2), BitDefender (Trojan.CryptZ.Marte.1.Gen), Bkav Pro (W32.AIDetectMalware), and Cloudmark (Trojan/Win32.Rozena). A 'Do you want to automate checks?' button is also present.

MALWARE BAZAAR

Abbiamo effettuato un'ulteriore controllo con MalwareBazaar per controllare all'interno del database se fosse potenzialmente un malware fornendo il codice hash per accedere alla pagina dello stesso.

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry


ShikataGaNai

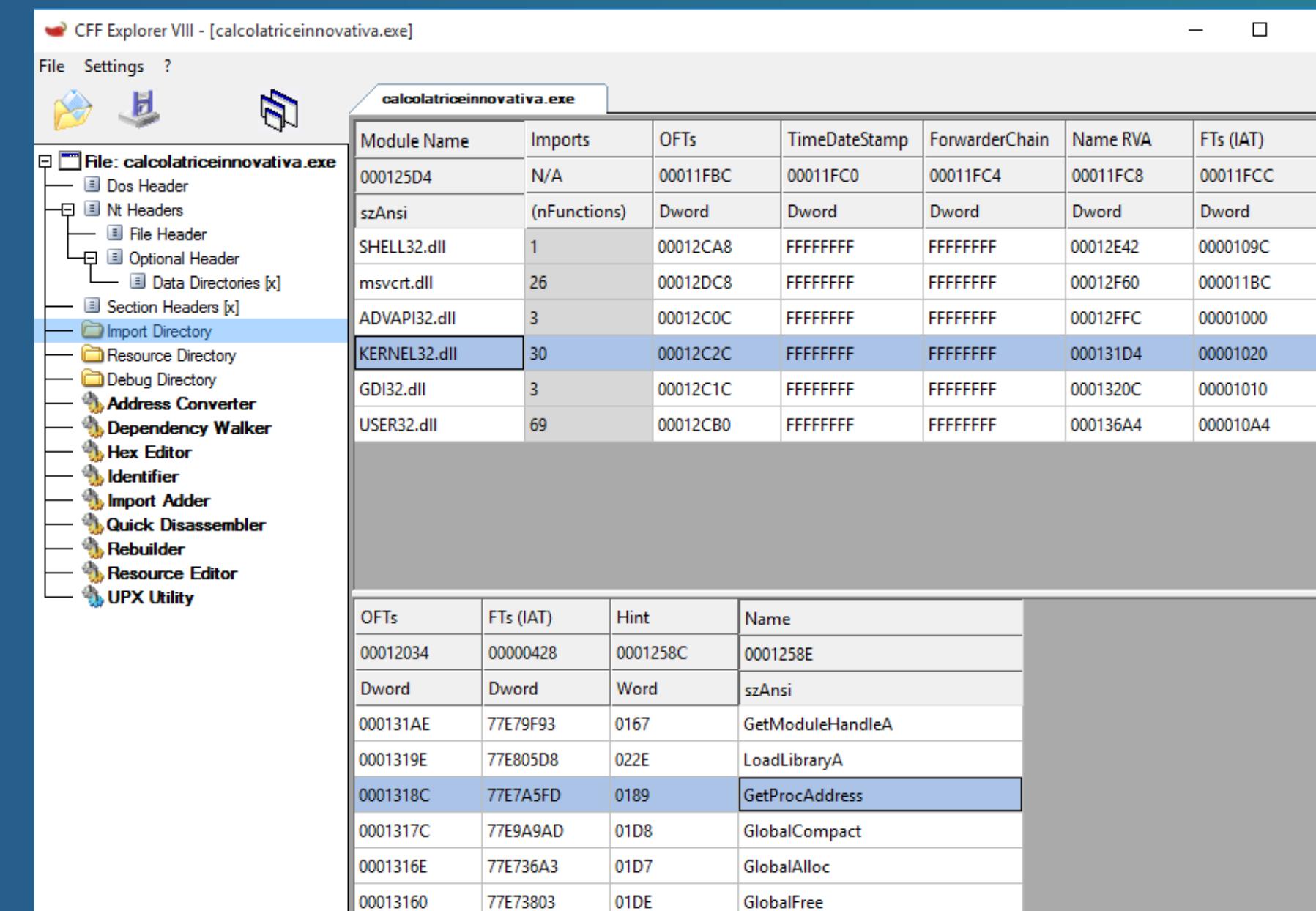

Vendor detections: 13

Intelligence 13	IOCs	YARA 1	File information	Comments	Actions ▾
SHA256 hash:	b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a				
SHA3-384 hash:	b211f60b618a49136d23af49bbfa5cb15d2cebd47b5714e58ec81f0a503eb3c8e5bbb1aefd756d1538f4d922a5944415				
SHA1 hash:	c50f22713b54e2fb476bfff5dda83b76b493212c				
MD5 hash:	d2f8843d112bb0421ba7a25999a59f32				
humanhash:	oranges-freddie-wisconsin-undress				
File name:	calcolatriceinnovativa.exe				
Download:	download sample				
Signature ②	ShikataGaNai Alert ▾				
File size:	115'200 bytes				
First seen:	2024-11-26 14:00:49 UTC				

CFF EXPLORER

il termine GetProcAddress (evidenziato in blu) si riferisce a una funzione dell'API di Windows che consente di ottenere l'indirizzo di una funzione esportata da una libreria dinamica. Questa funzione è comunemente utilizzata dai programmi e, a volte, dai malware per caricare dinamicamente funzioni da DLL durante l'esecuzione.

I malware usano spesso GetProcAddress per caricare funzioni che alterano il sistema, come VirtualAlloc, CreateProcess, o funzioni di rete come send e recv. Essendo una calcolatrice non dovrebbe contenere un file eseguibile



CUKOO

Come ultima analisi procediamo con un'analisi dinamica con un ambiente virtuale su cuckoo per vedere il comportamento del malware e come risponso avremo una critica di 10/10

The screenshot shows the Cuckoo analysis interface. On the left is a sidebar with various icons for file operations. The main area has a header with 'Dashboard', 'Recent', 'Pending', 'Search', 'Submit', 'Import', and a pencil icon. Below the header, the file name 'calcolatriceinnovativa.exe' is shown. The main content is divided into sections: 'Summary' (containing file details like Size, Type, MD5, SHA1, SHA256, SHA512, CRC32, ssdeep, and Yara results), 'Score' (showing a score of 10 out of 10 with a note about it being suspicious), and 'Feedback' (a section for reporting errors). At the bottom, there's an 'Information on Execution' table with columns for Category, Started, Completed, Duration, Routing, and Logs.

Category	Started	Completed	Duration	Routing	Logs
FILE	Nov. 26, 2024, 9:43 p.m.	Nov. 26, 2024, 9:48 p.m.	284 seconds	internet	Show Analyzer Log Show Cuckoo Log



GRAZIE
MATTIA DI DONATO