

Malware Analysis

La malware analysis è il processo di esaminare e comprendere il comportamento, le funzionalità e gli obiettivi di un malware. Questo processo può essere suddiviso in due fasi principali:

- Analisi statica: esamina il malware senza eseguirlo, analizzando il codice sorgente per identificare firme, istruzioni o modelli di comportamento.
- Analisi dinamica: osserva il comportamento del malware in un ambiente controllato, come una sandbox.

Per la prima fase, cioè quella statica, per l' esercizio da svolgere, sono stati utilizzati:

- [virustotal.com](https://www.virustotal.com)
- [malware baazar](https://www.malwarebazaar.com)
- [cfx explorer](https://cfxplorer.net)

Virus total

Dopo aver caricato il file malevolo sul sito, già dalla prima analisi rilasciata si può evincere:

- il suo punteggio evidenziato in rosso, che sta a significare che la maggior parte delle aziende che si occupano di sicurezza informatica, lo hanno riconosciuto come un trojan, nello specifico installa una backdoor sulla macchina della vittima.

Malware analysis report for file b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a (CALC.EXE).

Community Score: 59 / 71

59/71 security vendors flagged this file as malicious.

Size: 112.50 KB, Last Analysis Date: 1 hour ago.

Popular threat label: trojan.swort/cryptz. Threat categories: trojan. Family labels: swort, cryptz, marte.

Security vendors' analysis		Do you want to automate checks?	
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
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.cryptz	Cylance	Unsafe

Malware Baazar

VirusTotal rilascia l'hashing del malware, cioè la sua impronta digitale, questo vuol dire che è stato fatto un report su di esso. In questo modo si può verificare se un file corrisponde al malware analizzato confrontandolo con l'hash. Inoltre Gli hash possono essere usati per aggiornare database di antimalware o strumenti di sicurezza per rilevare il malware.

Si inserisce l'hashing sul sito Malware Baazar per avere altre informazioni e ulteriore conferma.

MALWARE bazaar

Database Entry

ShikataGaNai

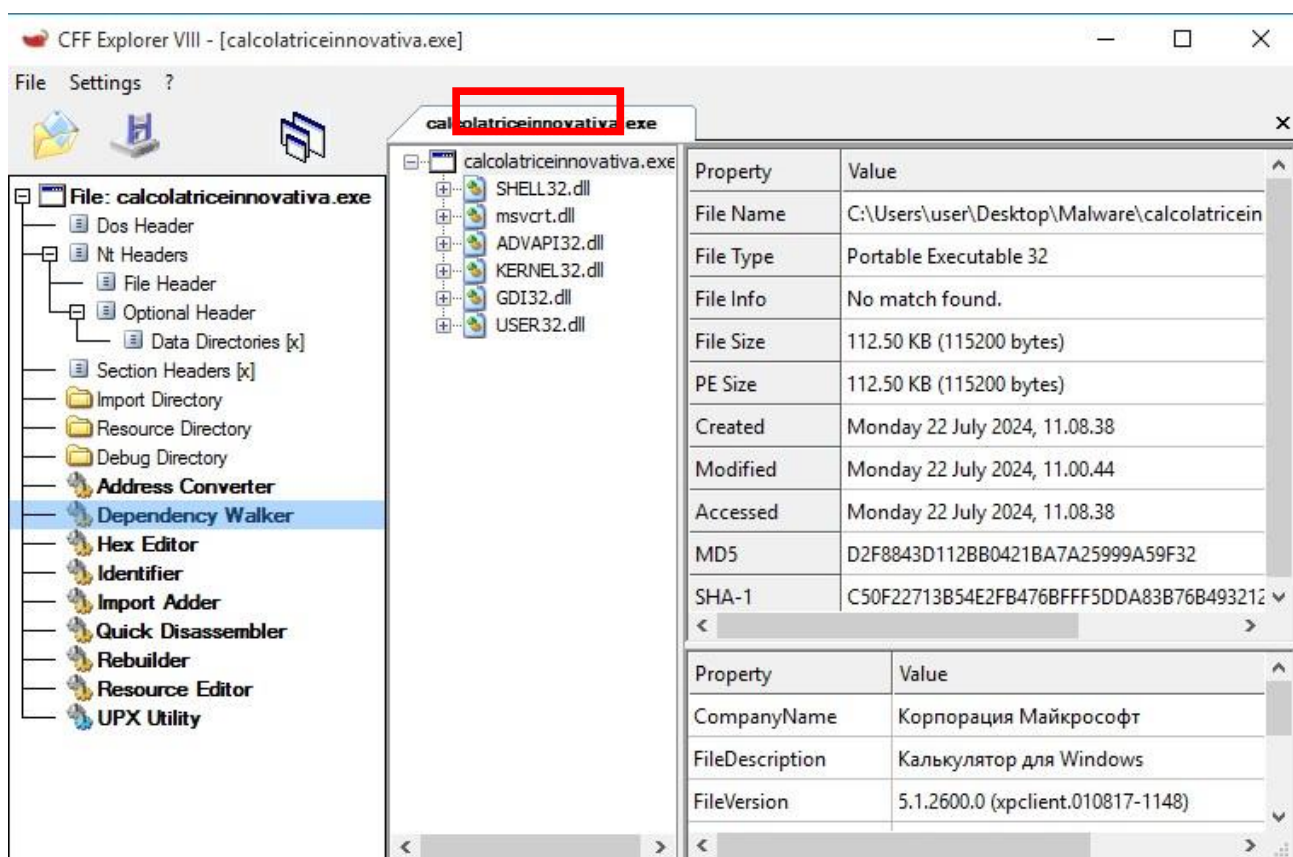
Vendor detections: 11

Intelligence 11	IOCs	YARA 1	File information	Comments	Actions
SHA256 hash:	b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a				
SHA3-384 hash:	b211f60b618a49136d23af49bbfa5cb15d2ceb47b5714e58ec81f0a503eb3c8e5bbb1aefd756d1538f4d922a5944415				
SHA1 hash:	c50f22713b54e2fb476bfff5dda83b76b493212c				
MD5 hash:	d2f8843d112bb0421ba7a25999a59f32				
humanhash:	oranges-freddie-wisconsin-undress				
File name:	calcolatriceinnovativa.exe				
Download:	download sample				
Signature	ShikataGaNai Alert				
File size:	115'200 bytes				
First seen:	2024-11-26 14:00:49 UTC				
Last seen:	2024-11-26 14:16:39 UTC				

Come si può notare dall' immagine, viene segnalato l' utilizzo nel codice, dell' encoder *shigata ga nai*. Viene utilizzato per offuscare il codice così da non essere riconosciuto dagli antimalware, in base al numero di iterazioni applicate.

CFF Explorer

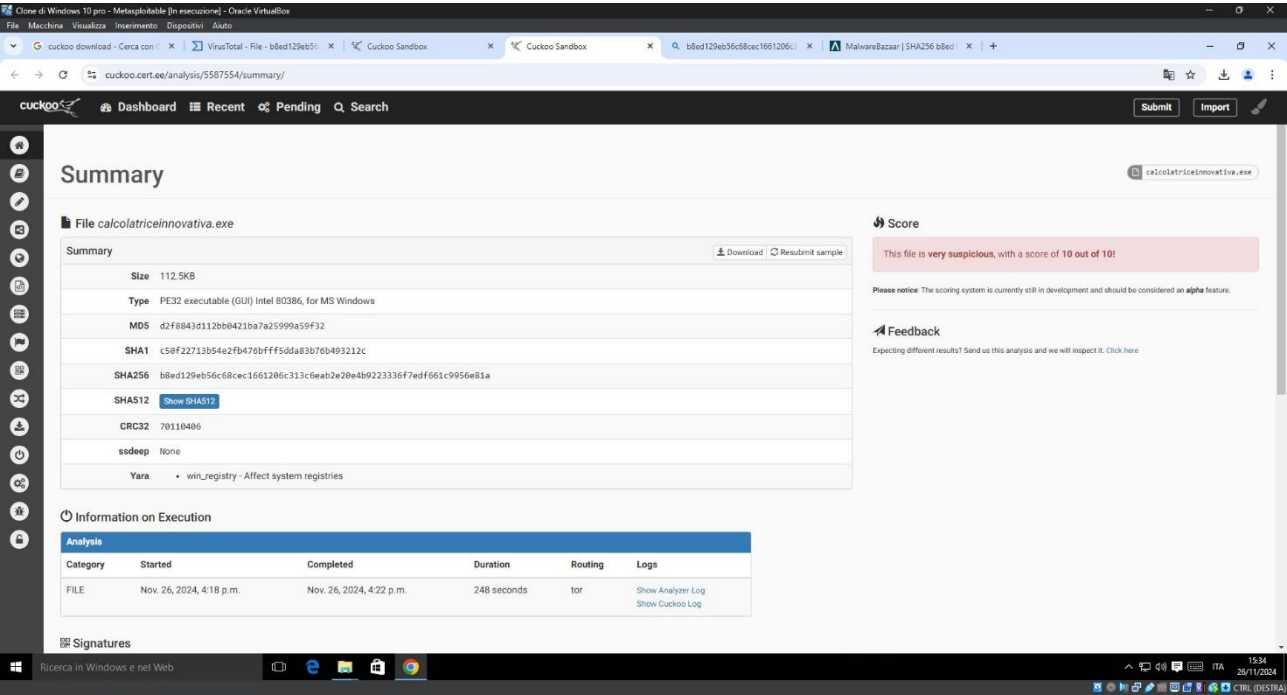
Con questo terzo tool, andiamo a verificare la voce "*dependency walker*". Questa sezione elenca tutte le librerie dalle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente. Come rappresentato nell' immagine, il malware ha bisogno della libreria shell32.dll. Questo ci conferma quanto riscontrato da virustotal che lo segnala come backdoor. Perché tramite questa libreria, può creare una shell, cioè un collegamento tra l' attaccante e la vittima, con la quale può dare istruzione e muoversi liberamente nella macchina.



Per la seconda fase, cioè l' analisi dinamica, si utilizza il tool cuckoo.

Cuckoo

Esso consente di esaminare file sospetti e osservare il loro comportamento in un ambiente virtuale o isolato (sandbox).



Anche con questo tool, si ha la conferma che è un malware, dato che lo classifica con un punteggio di 10/10. Ma essendo un' analisi dinamica, si può capire anche come agisce. Infatti nella sezione behavioral analysis, si può notare, come cerchi di connettersi ed inviare dati ad una macchina esterna.

