

Malware Analysis

Nel progetto odierno è stata richiesta una **Malware Analysis** di un Malware relativamente pericoloso. Il nome di questo Malware è `calcolatriceinnovativa.exe` (**CALC.EXE**), software malevolo presente sulla VM Windows 10 pro.

Al fine di analizzarlo, sono state adottate entrambe le tecniche che prevedono una corretta analisi del Malware: **Static Analysis and Dynamic Analysis**

Analisi Statica

L'analisi statica di un Malware prevede uno studio, un'analisi del software malevolo, mediante l'uso di tool come CFF, Procmon, o mediante open source come VirusTotal o MalwareBazaar.

Questo ci consentirà di avere un'idea più o meno accurata di come esso potrebbe comportarsi una volta eseguito, e ciò è possibile attraverso un'accurata analisi della sua struttura, e delle informazioni recuperate mediante gli strumenti precedentemente citati.

Virus Total

VirusTotal è un prodotto **Alphabet** che analizza **file, URL, domini e indirizzi IP** sospetti per rilevare malware e altri tipi di minacce e li condivide automaticamente con la community per la sicurezza informatica.

Esso confronta le informazioni da noi fornite con i database di **70+** antivirus differenti in modo da fornire informazioni accurate nel momento in cui all'interno di essi il file caricato risulti essere effettivamente un malware

Analisi Statica

Il primo approccio nell'effettuare l'analisi statica del Malware fornito, è stato quello di utilizzare VirusTotal. Una volta diretto sul sito Web, è stato effettuato l'upload del Malware ed ho atteso l'esito della scansione.

Come si può evincere dall'immagine il file caricato risulta avere riscontri positivi come software malevolo all'interno di 59 **database's antivirus** diversi, mostrando anche diversi riscontri inerenti alla sua natura.

Nello specifico all'interno di alcuni database esso risulta essere una tipologia di Malware differente.

*Per fare alcuni esempi abbiamo un riscontro come **Trojan/CobaltStrike, Wini32:SwPatch (worm)**, o ancora come **Backdoor** con payload meterpreter.*

Proseguendo con l'analisi si può notare che esso invia traffico mediante l'uso del protocollo **TCP** ad **IP pubblici** sconosciuti, rispettivamente sulle porte **443 (https)** e **80 (http)**, e la presenza di un Memory Pattern ad un **indirizzo privato, 192.168.1.80** sulla porta **4444**, il che potrebbe suggerire che tenti di stabilire una connessione tramite **reverse tcp** su quella determinata porta, facendo evincere che molto probabilmente si possa trattare di una backdoor.

59
/ 71

Community Score -13

59/71 security vendors flagged this file as malicious

Reanalyze Similar More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

Size 112.50 KB

Last Analysis Date 55 minutes ago

EXE

peexe idle checks-user-input

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 9

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.swrort/cryptz

Threat categories trojan

Family labels swrort 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

Activity Summary

Download Artifacts Full Reports Help

2 Detections
2 MALWARE 1 TROJAN

Mitre Signatures
7 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
26 OTHER

Network comms
3 IP

Behavior Tags

checks-user-input idle

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE TROJAN

The sandbox C2AE flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

Defense Evasion TA0005

Credential Access TA0006

Discovery TA0007

Collection TA0009

Network Communication

IP Traffic

TCP 20.99.133.109:443

TCP 192.229.211.108:80

TCP 20.99.184.37:443

Memory Pattern Urls

tcp://192.168.1.80:4444

Volendo estrapolare ancora più informazioni dal sito in questione, l'analisi è proseguita mediante zapping all'interno delle varie sezioni riuscendo ad identificare altri dettagli molto utili.

Activity Summary

Download Artifacts ▾Full Reports ▾Help ▾

"%SAMPLEPATH%\calcolatriceinnovativa.exe"

C:\Windows\System32\wuapihost.exe -Embedding

Processes Injected

\\?\C:\Windows\system32\wbem\WMIADAP.EXE

Processes Terminated

%windir%\System32\svchost.exe -k WerSvcGroup

wmiadap.exe /F /T /R

C:\Windows\System32\wuapihost.exe

Processes Tree

2204 - %windir%\System32\svchost.exe -k WerSvcGroup

2820 - wmiadap.exe /F /T /R

2572 - %SAMPLEPATH%

2868 - %windir%\system32\wbem\wmiiprvse.exe

2444 - %WINDIR%\explorer.exe

↳ 3580 - %SAMPLEPATH%\calcolatriceinnovativa.exe

624 - C:\Windows\System32\svchost.exe

↳ 3228 - C:\Windows\System32\wuapihost.exe

7504 - C:\Users\user\Desktop\calcolatriceinnovativa.exe

Highlighted actions ⓘ

Decoded Text

⚙️ {"Type": "Metasploit Connect", "IP": "192.168.1.80", "Port": 4444}

Si può evincere nel sommario delle attività i processi iniettati, quelli terminati, e successivamente l'albero dei processi con relativo **PID**.

Inoltre risalta subito ben in evidenza tra le highlighted actions un decoded text che conferma i nostri sospetti, e ci dice che nel momento in cui esso viene avviato cerca di effettuare una Metasploit connection all'IP privato prima riscontrato.

Activity Summary

Download Artifacts ▾Full Reports ▾Help ▾

⚠️ The sandbox Zenbox flags this file as: MALWARE TROJAN

⚠️ The sandbox C2AE flags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

— Defense Evasion TA0005

⚙️ Obfuscated Files or Information T1027

Binary may include packed or crypted data

⚙️ Software Packing T1027.002

Binary may include packed or crypted data

PE file has an executable .text section which is very likely to contain packed code (zlib compression ratio < 0.3)

— Credential Access TA0006

⚙️ Input Capture T1056

Creates a DirectInput object (often for capturing keystrokes)

— Discovery TA0007

⚙️ System Information Discovery T1082

Reads software policies

⚙️ Software Discovery T1518

⚙️ Security Software Discovery T1518.001

May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

— Collection TA0009

⚙️ Input Capture T1056

















Creates a DirectInput object (often for capturing keystrokes)

Network Communication ⓘ






MalwareBazaar

Dopo avere completato la ricerca di informazioni su **VirusTotal**, è stato adoperato un altro sito web, **MalwareBazaar**, il quale consente di effettuare la ricerca di determinati Malware fornendo come input di ricerca il codice **hash** di un file.

Se il codice hash corrisponde a quello di un Malware, vi è una forte probabilità che esso possa essere presente all'interno del database di MalwareBazaar.

File size:	115'200 bytes
First seen:	2024-11-26 14:00:49 UTC
Last seen:	2024-11-26 14:16:39 UTC
File type:	 exe
MIME type:	application/x-dosexec
imphash 	 08f6a1b121da8cedde2d1089d0906ed8 (1 x ShikataGaNai)
ssdeep 	 3072:DAq2Byr/0He97Ulj7nt5CdLYkOEp0AWLnQoXPBs5ZrR:DAqfB9yBJa7OE0pLnQoo5Zd
TLSH 	 T197B39E01BA94F135C465113448D39FFA93BDBF1705AB16AB33097E4F7E362662A23286
TrID 	43.3% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13) 22.9% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5) 9.1% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2) 7.0% (.EXE) Win16 NE executable (generic) (5038/12/1) 6.2% (.EXE) Win32 Executable (generic) (4504/4/1)
Magika 	pebin
File icon (PE):	
dhash icon 	 0082b4b2cad2ab00 (2 x Kutaki, 1 x <u>ShikataGaNai</u>)
Reporter 	 Pentolino
Tags:	 

Intelligence

File Origin 	
# of uploads 	5
# of downloads 	388
Origin country 	 IT

In questo caso specifico, è stato fornito come input di ricerca il file hash recuperato da VirusTotal, il che ha generato un riscontro positivo all'interno del sito web.

Ci vengono fornite informazioni come Paese di origine, tipologia del file (in questo caso un eseguibile **.exe**), l'icona del file stesso ed altre informazioni, come quella che cita **Shikata_ga_nai**, un famoso encoder molto forte e conosciuto per la sua efficienza.

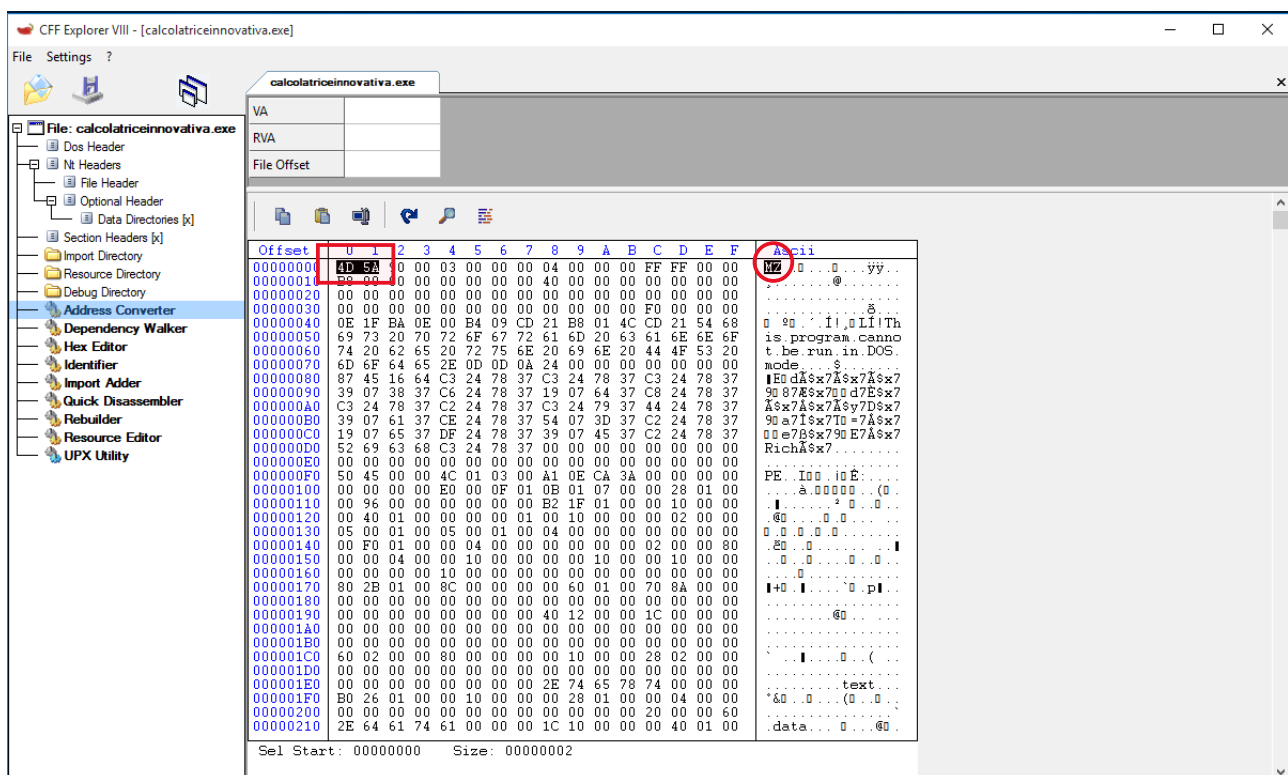
MalwareBazaar è una piattaforma online gestita da Abuse.ch che consente la condivisione e l'analisi di campioni di malware. È progettata per aiutare ricercatori di sicurezza, analisti di malware e professionisti della cybersecurity a raccogliere, analizzare e confrontare campioni di malware in modo collaborativo.

CFF Explorer

Successivamente è stato adoperato un tool molto efficace, CFF Explorer. Esso è uno strumento avanzato per l'analisi e la modifica di file eseguibili, come i file **PE (Portable Executable)** usati su Windows.

Esso ci permette di esaminare la struttura interna dei **PE**, e ci mostra dettagli su intestazioni, sessioni, tabelle e molto altro. Viene utilizzato principalmente per **Sviluppo, sicurezza e Reverse Engineering**.

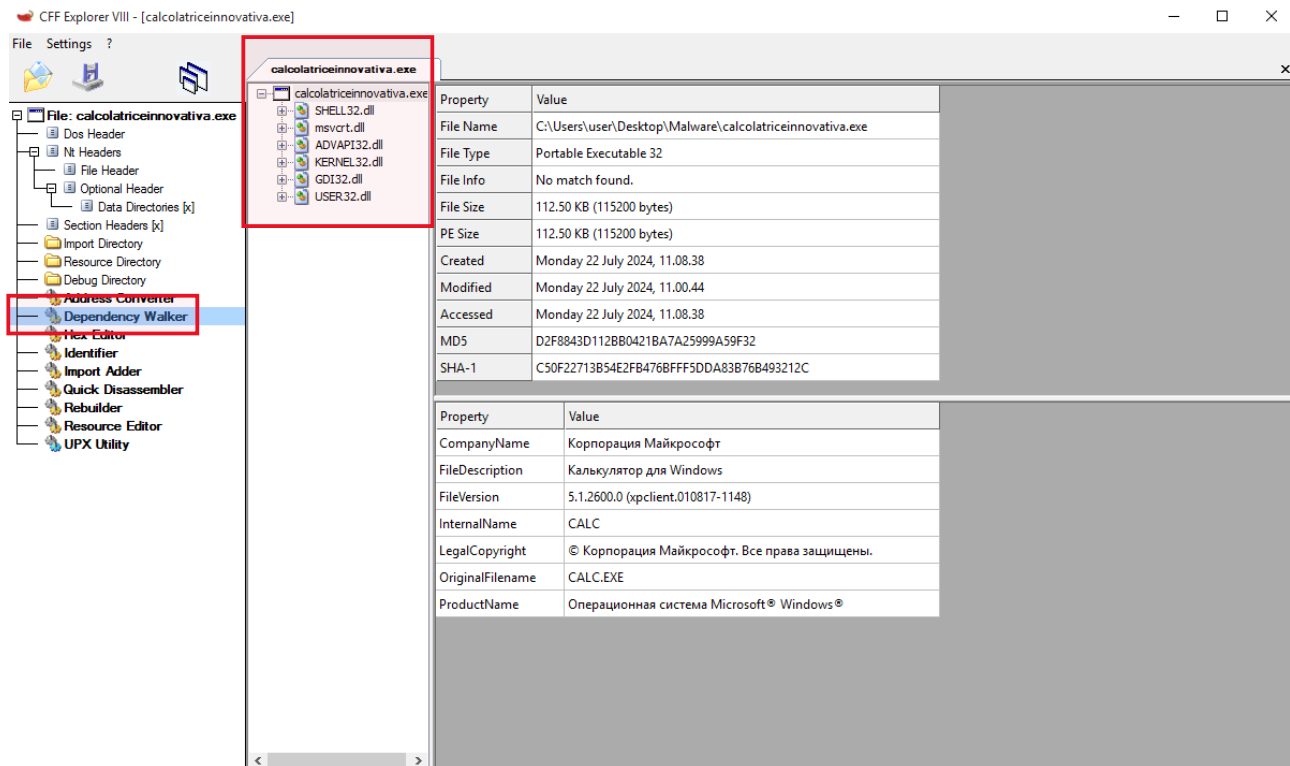
Una volta avviato è stato inserito il file a analizzare e mediante l'interfaccia grafica (GUI) del tool, è stata eseguita un'analisi del malware mediante un controllo delle directory e dei file presenti all'interno di esse.



Una delle prime cose che salta all'occhio è la presenza della firma **MZ**, la quale ci garantisce che stiamo parlando di un file eseguibile. Esso è presente nella colonna centrale sotto forma decimale (**Hex Dump**), e si può riconoscere grazie alla traduzione parziale effettuata mediante **l'ASCII** nella colonna di destra.

Successivamente è stato effettuato un controllo all'interno de percorso **Dependency Walker**.

*Il **Dependency Walker** elenca tutte le librerie (DLL) dalle quali il file eseguibile **dipende**, cioè le librerie che deve caricare per funzionare correttamente. Senza le librerie il malware non avrà accesso a determinate funzionalità, quindi il software non funzionerà. Se vi è il dubbio che una determinata libreria sia presente o meno è possibile importarla, oppure scaricarla da internet.*



All'interno possiamo notare che essa presenta 7 le librerie dll di Windows:

- **SHELL32** Comprende funzioni per interagire con le shell Windows
- **Msvcrt.dll** Fornisce le funzioni della libreria runtime standard del C su Windows, essenziale per l'esecuzione di molti programmi sviluppati in C/C++.
- **ADVAPI.dll** Comprende funzioni per manipolare sicurezza, funzioni ed eventi di Windows.
- **KERNEL32.dll** Fornisce le funzioni base per il funzionamento del sistema operativo
- **GDI32.dll** Comprende le funzioni basiche peer le funzioni grafiche
- **USER32.dll** Comprende funzioni come gestione finestre, controllo della tastiera o messaggi di sistema. In generale, informazioni relative a come l'utente utilizza il sistema operativo

Esse non presenteranno tutte le funzioni della libreria ma soltanto alcune. Esse sono state controllate per verificare che il Malware non potesse effettuare operazioni critiche come creare, modificare o cancellare registri Windows, o ancora, se avesse la possibilità di connettersi ad internet.

Dopo aver eseguito l'analisi statica si è successivamente passati all'analisi dinamica del file malevolo, mediante **Cuckoo**.

Cuckoo



Cuckoo è un sandbox per l'analisi di **malware** open-source. Permette di eseguire file sospetti in un ambiente isolato (**sandbox**) per osservarne il comportamento e raccogliere informazioni dettagliate senza rischiare di compromettere il sistema principale.

Mi sono quindi diretto su **Cuckoo.ee**, in modo da poter uploadare il file e testarne il comportamento. Dopo aver completato l'analisi ci sono state quindi fornite le informazioni.

The screenshot displays the Cuckoo Sandbox web interface. At the top, there's a navigation bar with 'Dashboard', 'Recent', 'Pending', and 'Search' options. Below this, a table lists analysis results for a specific file. The table includes columns for SHA1, SHA256, SHA512, CRC32, ssdeep, and Yara. The Yara column shows a rule 'win_registry' that affects system registries. Below the table, there's a section titled 'Information on Execution' which includes a table with columns for Category, Started, Completed, Duration, Routing, and Logs. The 'FILE' category shows a duration of 409 seconds and routing to the internet. To the right of the table, there's a 'Feedback' section with a link to 'Click here'. Below the execution information, there's a 'Signatures' section listing various detection events, such as 'Yara rule detected for file (1 event)', 'Allocates read-write-execute memory (usually to unpack itself) (1 event)', 'The binary likely contains encrypted or compressed data indicative of a packer (2 events)', 'File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)', and 'File has been identified by 59 AntiVirus engines on VirusTotal as malicious (50 out of 59 events)'.

SHA1	SHA256	SHA512	CRC32	ssdeep	Yara
c50f22713b54e2fb476bfff5dda83b76b493212c	b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a		70110406	None	win_registry - Affect system registries

Category	Started	Completed	Duration	Routing	Logs
FILE	Nov. 26, 2024, 4:12 p.m.	Nov. 26, 2024, 4:18 p.m.	409 seconds	internet	Show Analyzer Log Show Cuckoo Log

Signatures

- Yara rule detected for file (1 event)
- Allocates read-write-execute memory (usually to unpack itself) (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- File has been identified by 16 AntiVirus engine on IRMA as malicious (16 events)
- File has been identified by 59 AntiVirus engines on VirusTotal as malicious (50 out of 59 events)

Grazie all'analisi dinamica si è evinto che l'idea che ci si era fatta del Malware durante l'analisi statica **coincideva** con il funzionamento effettivo del Malware stesso.

Esso è quindi risultato malevolo in molteplici antivirus database, è stato fornito il codice hash del file, e grosso modo un'ottima parte delle informazioni precedentemente riscontrate mediante la Static Analysis. Tra questi riscontri anche la possibilità che si trattasse di una backdoor.

Time & API	Arguments	Status	Return	Repeated
	base_address: 0x00740000			
NtFreeVirtualMemory Nov. 26, 2024, 4:11 p.m.	free_type: 32768 process_handle: 0xffffffff process_identifier: 2084 base_address: 0x00740000 size: 393216	1	0	0
NtAllocateVirtualMemory Nov. 26, 2024, 4:11 p.m.	process_identifier: 2084 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 4 (PAGE_READWRITE) process_handle: 0xffffffff allocation_type: 4096 (MEM_COMMIT) base_address: 0x007a0000	1	0	0
LdrLoadDll Nov. 26, 2024, 4:11 p.m.	module_name: ws2_32 base_name: ws2_32 module_address: 0x76ae0000 flags: 0 stack_pivoted: 0	1	0	0
WSAStartup Nov. 26, 2024, 4:11 p.m.	wVersionRequested: 400	1	0	0
WSASocketA Nov. 26, 2024, 4:11 p.m.	type: 1 flags: 0 socket: 152 protocol: 0	1	152	0
connect Nov. 26, 2024, 4:12 p.m.	ip_address: 192.168.1.80 socket: 152 port: 4444		4294967295	0

Anche qui di fatto, ci viene detto che effettua una connessione in rete LAN sulla porta 4444.

Avendo a disposizione una VM di Windows 10 pro, è stato quindi deciso di effettuare un test ancora più pratico relativo al suo funzionamento.

Analisi Dinamica Avanzata

Dopo aver appurato che non può causare gravi danni, e dopo aver sanitizzato la nostra zona di test, è stato avviato sulla VM.

Ho deciso di fare ciò poiché avendo a disposizione una VM i rischi erano veramente pochi, ma per accortezza, è stato rimosso qualunque collegamento bidirezionale con qualunque altra VM su dispositivo, compresa la nostra stessa macchina, ed è stata eliminata la connessione ad internet.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:50:...	Explorer.EXE	3792	Thread Create		SUCCESS	Thread ID: 2720
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x230...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x779...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x75d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x777...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4036
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Image Base: 0x759...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\vpct4.dll	SUCCESS	Image Base: 0x756...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\bcryptprimitiv...	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4552
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x77b...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x74d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x758...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x757...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x775...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\nsi.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x73d...

Mediante l'ausilio del tool **Procmon** sono stati visualizzati e controllati tutti i processi sulla nostra macchina, e tra di essi è comparso proprio il nostro Malware, più volte. Un filtro ha aiutato ad "isolare" i processi che si venivano a creare quando esso veniva avviato. È stato inoltre verificato che come da aspettativa tentava la connessione agli indirizzi precedentemente individuati, nonché il tentativo di connessione **alla porta 4444 con indirizzo IP 192.168.1.80**.

È stato quindi riattivato l'accesso ad Internet, passando quindi ad un esame **dinamico avanzato**, e mediante la nostra macchina Kali Linux, tramite l'ausilio del tool Metasploit, è stato possibile mettere la nostra macchina in ascolto sulla porta 4444, stabilendo successivamente la connessione con la VM windows 10.

*Da qui è tutto in discesa, poiché un possibile attaccante che riesca a sfruttare la backdoor creata da questo Malware, è in grado di utilizzare il comando migrate per migrare da servizio in servizio, potrebbe utilizzare **Mimikatz** e tutte le sue funzioni, **aprire shell** direttamente sulla macchina, o ancora, eseguire una **privilege escalation** in modo da ottenere accesso ai dati riservati ed avere il controllo totale a livello admin della macchina.*