BW3 Analisi Comportamentale del Worm MyDoom A

Introduzione

⚜️ **Tag:** #introduzione #malware #worm #sicurezza

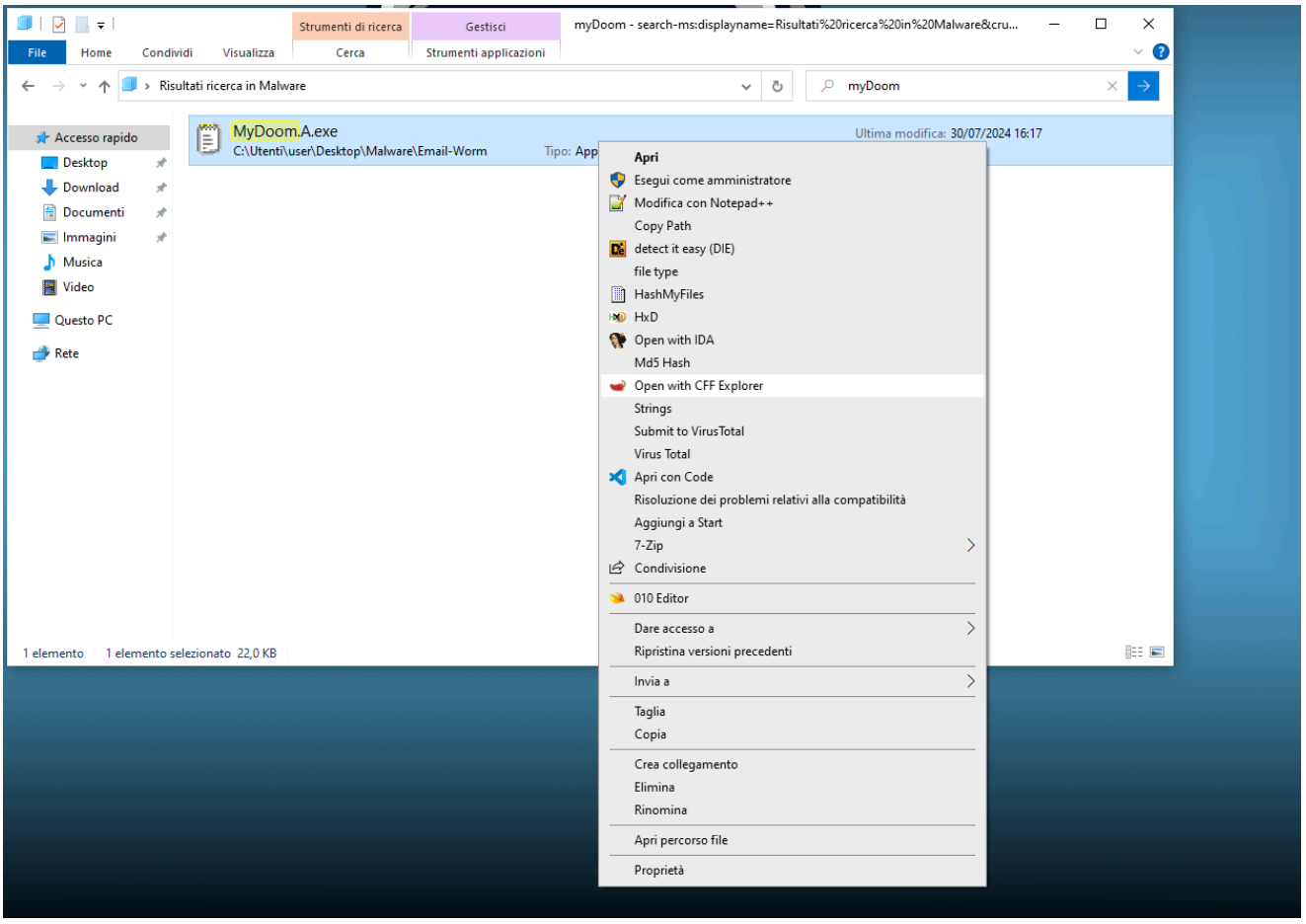
Il worm MYDOOM è noto per la sua pericolosità e diffusione tramite file eseguibili. Questo documento analizza il comportamento del worm attraverso analisi statica e dinamica, offrendo una visione approfondita delle tecniche utilizzate per infettare e persistere nei sistemi compromessi.

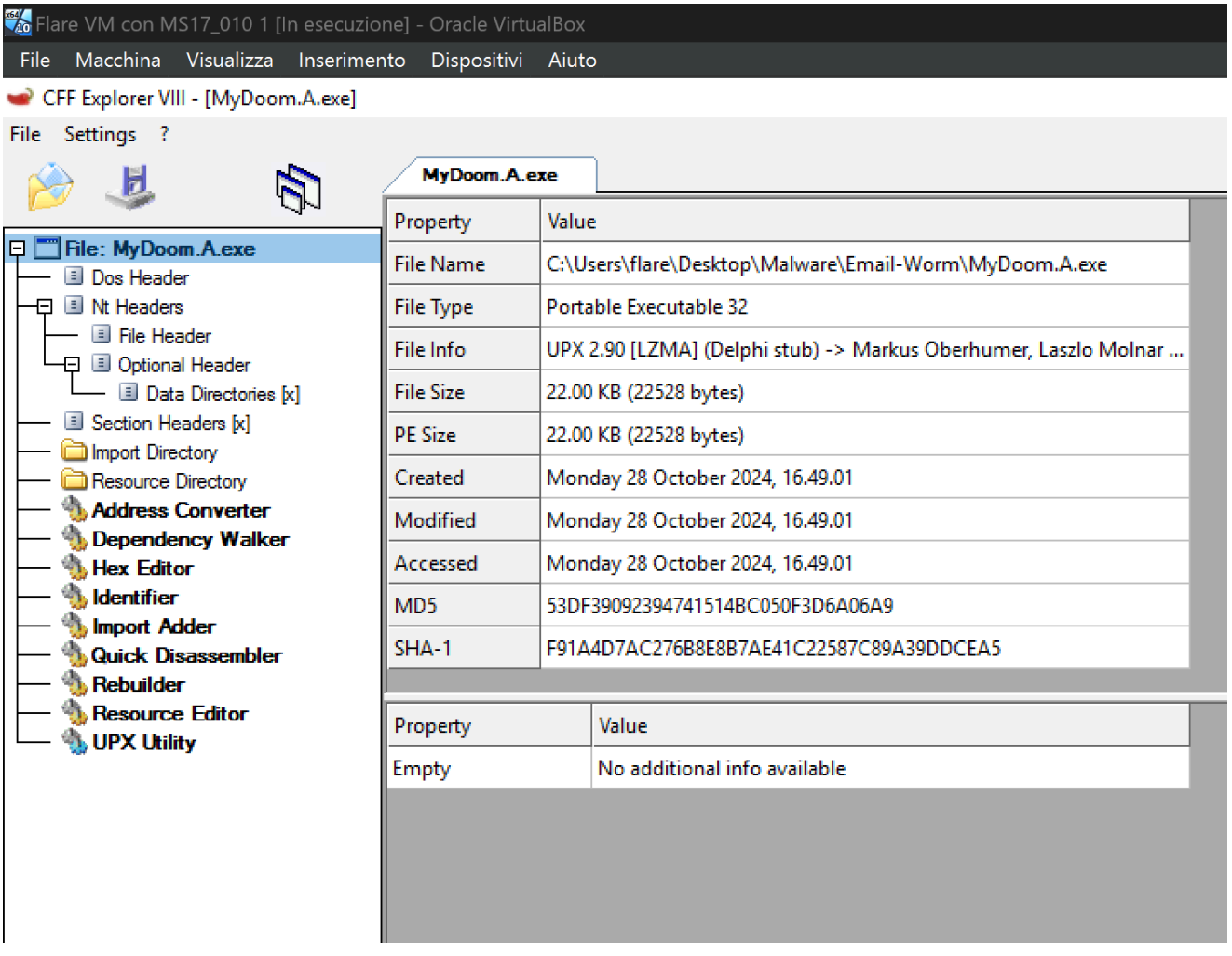
Analisi Statica del Worm MYDOOM

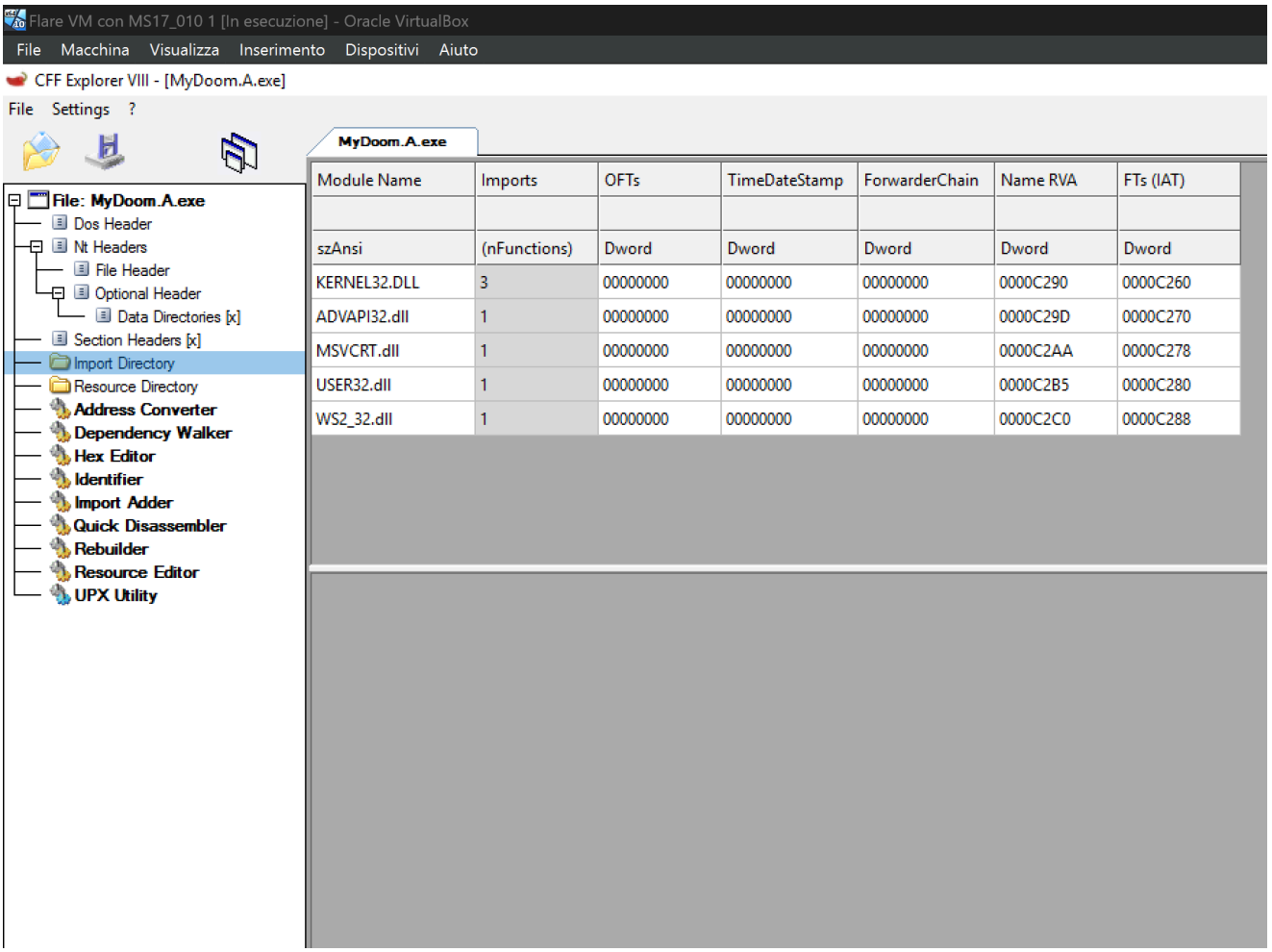
⚜️ **Tag:** #analisi_statica #malware #CFFExplorer #VirusTotal

Per la fase di analisi statica, sono stati utilizzati i seguenti strumenti:

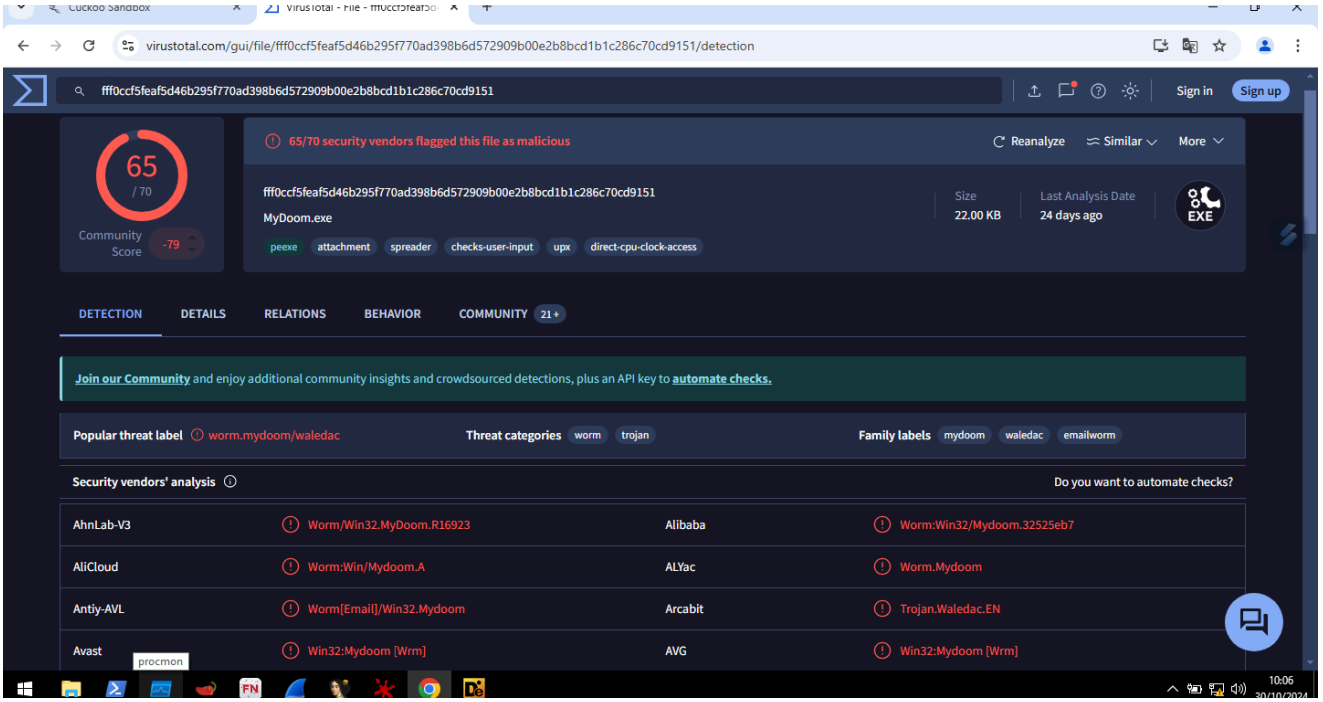
1. **CFF Explorer**: Usato per ottenere dettagli del malware come hash e metodi di esecuzione.
    - Il worm attacca il sistema attraverso il `KERNEL32`, puntando al kernel. Questo permette al worm di ripresentarsi anche dopo la formattazione del sistema.

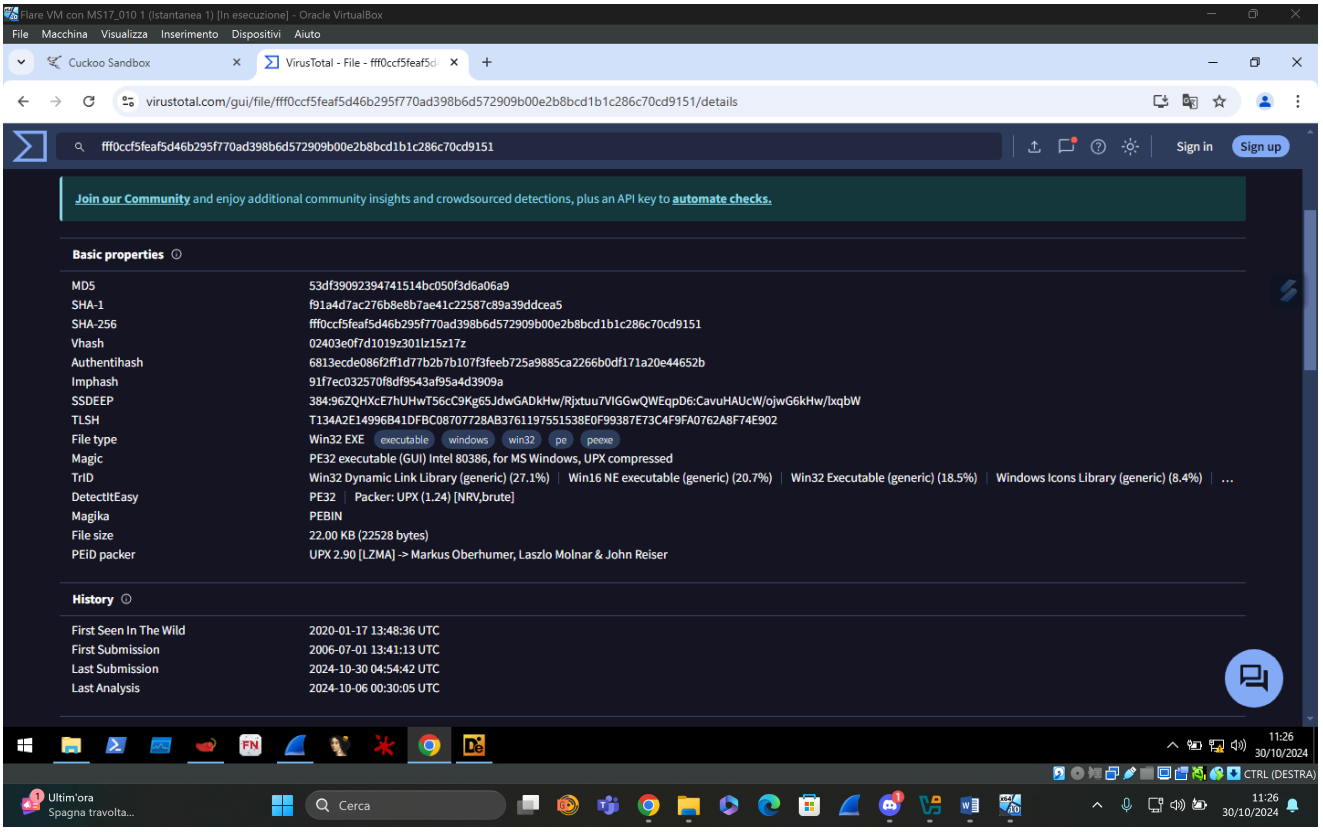

Strumenti di ricerca
Gestisci
myDoom - search-ms:displayname=Risultati%20ricerca%20in%20Malware&cru...
File
Home
Condividi
Visualizza
Cerca
Strumenti applicazioni
Risultati ricerca in Malware
myDoom
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
Video
Questo PC
Rete
MyDoom.A.exe
C:\Utenti\user\Desktop\Malware\Email-Worm
Tipo: App
Ultima modifica: 30/07/2024 16:17
Apri
Esegui come amministratore
Modifica con Notepad++
Copy Path
detect it easy (DIE)
file type
HashMyFiles
HxD
Open with IDA
Md5 Hash
Open with CFF Explorer
Strings
Submit to VirusTotal
Virus Total
Apri con Code
Risoluzione dei problemi relativi alla compatibilità
Aggiungi a Start
7-Zip
Condivisione
010 Editor
Dare accesso a
Ripristina versioni precedenti
Invia a
Taglia
Copia
Crea collegamento
Elimina
Rinomina
Apri percorso file
Proprietà
1 elemento
1 elemento selezionato 22,0 KB


Flare VM con MS17_010 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CFF Explorer VIII - [MyDoom.A.exe]
File Settings ?
MyDoom.A.exe
File: MyDoom.A.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Property
Value
File Name
C:\Users\flare\Desktop\Malware\Email-Worm\MyDoom.A.exe
File Type
Portable Executable 32
File Info
UPX 2.90 [LZMA] (Delphi stub) -> Markus Oberhumer, Laszlo Molnar ...
File Size
22.00 KB (22528 bytes)
PE Size
22.00 KB (22528 bytes)
Created
Monday 28 October 2024, 16.49.01
Modified
Monday 28 October 2024, 16.49.01
Accessed
Monday 28 October 2024, 16.49.01
MD5
53DF39092394741514BC050F3D6A06A9
SHA-1
F91A4D7AC276B8E8B7AE41C22587C89A39DDCEA5
Property
Value
Empty
No additional info available



2. **VirusTotal**: Utilizzato per ulteriori informazioni sul livello di pericolosità del malware.
    - Risultato: Score di pericolosità elevato, indicando un malware altamente dannoso.
    - Il worm viene inviato principalmente in formato `.exe` e utilizza UPX, un algoritmo per la decompressione rapida del codice eseguibile.



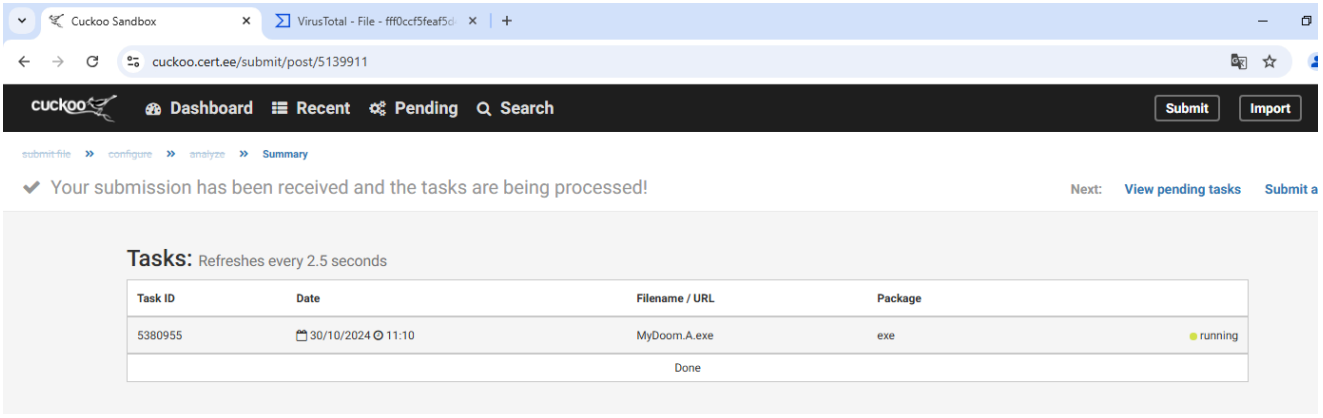


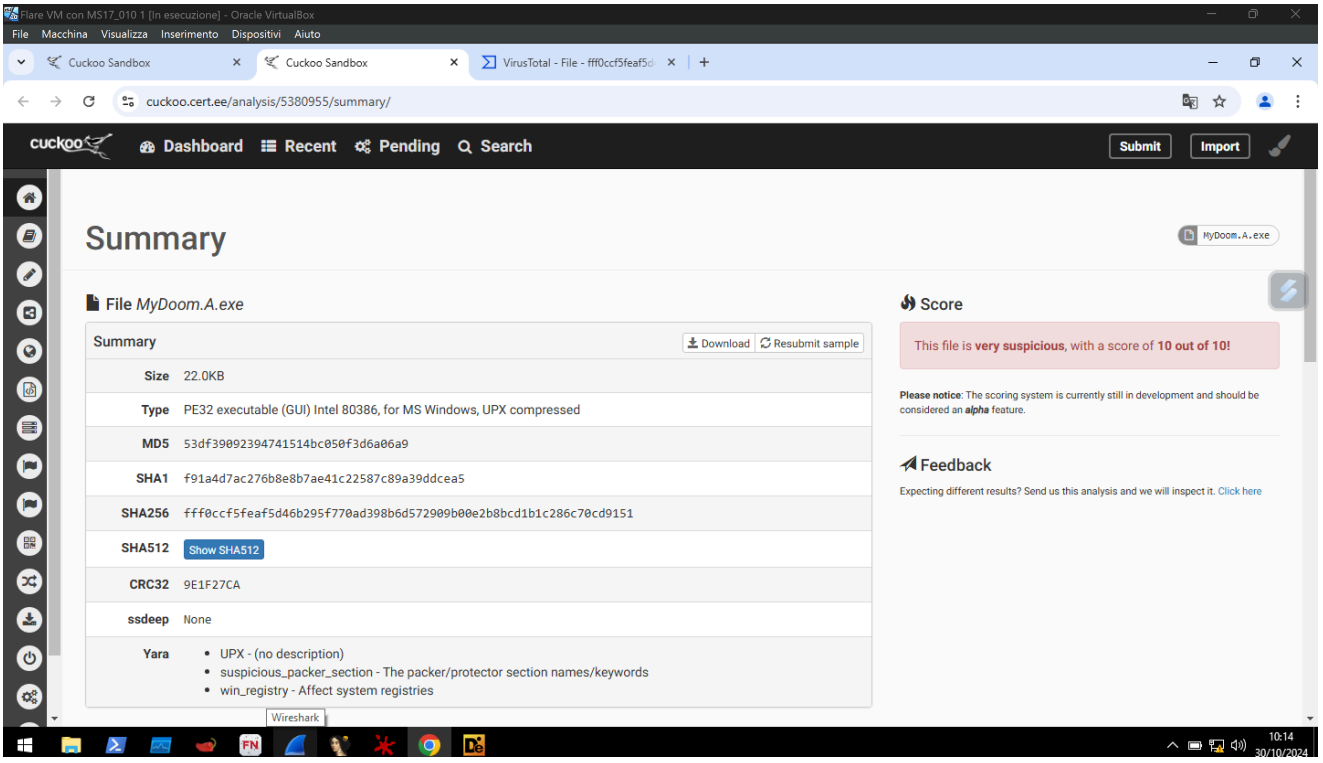
Analisi Dinamica del Worm MYDOOM

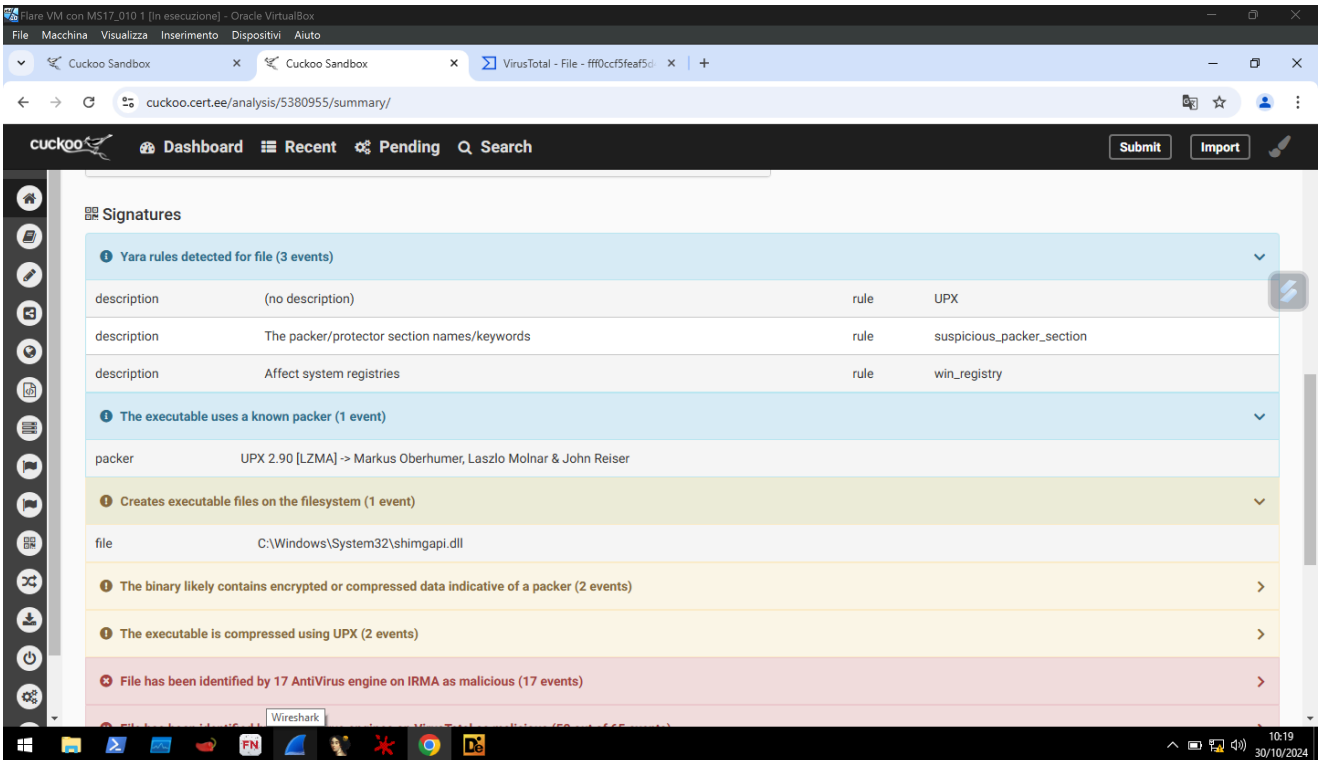
⚜️ **Tag:** #analisi_dinamica #cuckoo #malware

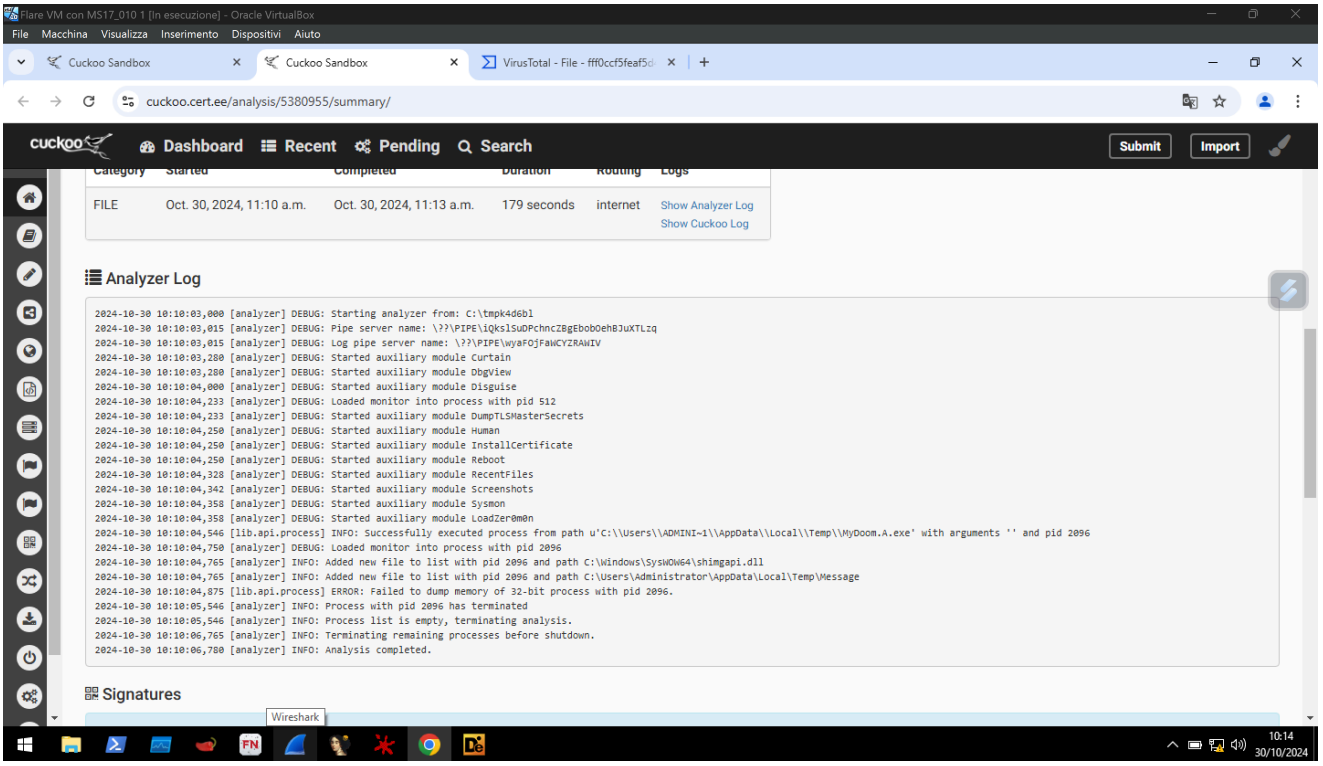
L'analisi dinamica è stata eseguita utilizzando **Cuckoo Sandbox**:

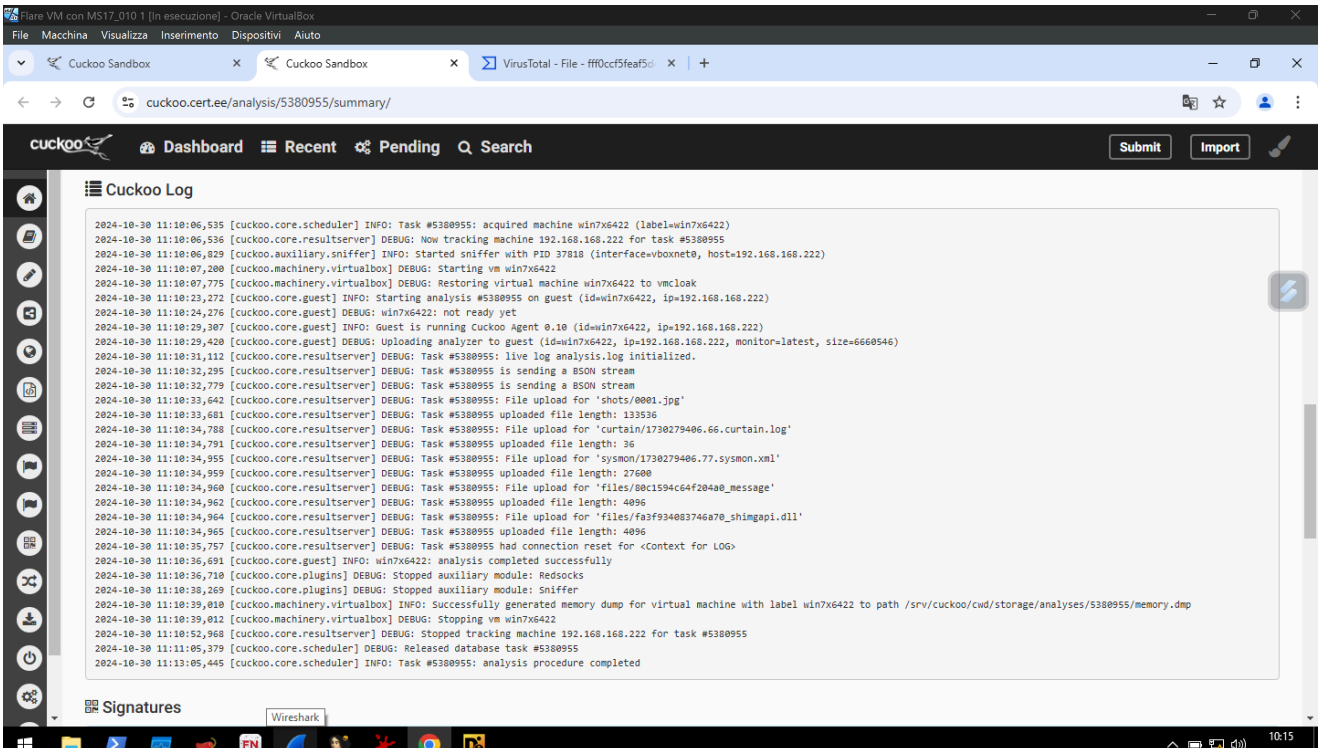
1. **Caricamento e Esecuzione in Cuckoo**: Cuckoo esegue il worm e fornisce dettagli sulla sua attività, inclusi gli algoritmi utilizzati come UPX e l'analisi dei log generati.
    - Dai log è possibile osservare i processi avviati dal worm, con l'obiettivo di creare sessioni di controllo remoto e raccogliere dati.






Flare VM con MS17_010 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cuckoo Sandbox
Cuckoo Sandbox
VirusTotal - File - fff0ccf5feaf5d
cuckoo.cert.ee/analysis/5380955/summary/
cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Signatures
Yara rules detected for file (3 events)
description (no description) rule UPX
description The packer/protector section names/keywords rule suspicious_packer_section
description Affect system registries rule win_registry
The executable uses a known packer (1 event)
packer UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser
Creates executable files on the filesystem (1 event)
file C:\Windows\System32\shimgapi.dll
The binary likely contains encrypted or compressed data indicative of a packer (2 events)
The executable is compressed using UPX (2 events)
File has been identified by 17 AntiVirus engine on IRMA as malicious (17 events)
Wireshark
10:19
30/10/2024


Flare VM con MS17_010 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cuckoo Sandbox
Cuckoo Sandbox
VirusTotal - File - fff0ccf5feaf5d
cuckoo.cert.ee/analysis/5380955/summary/
cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Category Started Completed Duration Routing Logs
FILE Oct. 30, 2024, 11:10 a.m. Oct. 30, 2024, 11:13 a.m. 179 seconds internet Show Analyzer Log Show Cuckoo Log
Analyzer Log
2024-10-30 10:10:03,000 [analyzer] DEBUG: Starting analyzer from: C:\tmpk4d6bl
2024-10-30 10:10:03,015 [analyzer] DEBUG: Pipe server name: \??\PIPE\iQkslSuDPchncZBgEbobOehBJuXTLzq
2024-10-30 10:10:03,015 [analyzer] DEBUG: Log pipe server name: \??\PIPE\wyaFOjFaWCYZRAWIV
2024-10-30 10:10:03,280 [analyzer] DEBUG: Started auxiliary module Curtain
2024-10-30 10:10:03,280 [analyzer] DEBUG: Started auxiliary module DbgView
2024-10-30 10:10:04,000 [analyzer] DEBUG: Started auxiliary module Disguise
2024-10-30 10:10:04,233 [analyzer] DEBUG: Loaded monitor into process with pid 512
2024-10-30 10:10:04,233 [analyzer] DEBUG: Started auxiliary module DumpTLSMasterSecrets
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module Human
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module InstallCertificate
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module Reboot
2024-10-30 10:10:04,328 [analyzer] DEBUG: Started auxiliary module RecentFiles
2024-10-30 10:10:04,342 [analyzer] DEBUG: Started auxiliary module Screenshots
2024-10-30 10:10:04,358 [analyzer] DEBUG: Started auxiliary module Sysmon
2024-10-30 10:10:04,358 [analyzer] DEBUG: Started auxiliary module LoadZer0m0n
2024-10-30 10:10:04,546 [lib.api.process] INFO: Successfully executed process from path u'C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\MyDoom.A.exe' with arguments '' and pid 2096
2024-10-30 10:10:04,750 [analyzer] DEBUG: Loaded monitor into process with pid 2096
2024-10-30 10:10:04,765 [analyzer] INFO: Added new file to list with pid 2096 and path C:\Windows\SysWOW64\shimgapi.dll
2024-10-30 10:10:04,765 [analyzer] INFO: Added new file to list with pid 2096 and path C:\Users\Administrator\AppData\Local\Temp\Message
2024-10-30 10:10:04,875 [lib.api.process] ERROR: Failed to dump memory of 32-bit process with pid 2096.
2024-10-30 10:10:05,546 [analyzer] INFO: Process with pid 2096 has terminated
2024-10-30 10:10:05,546 [analyzer] INFO: Process list is empty, terminating analysis.
2024-10-30 10:10:06,765 [analyzer] INFO: Terminating remaining processes before shutdown.
2024-10-30 10:10:06,780 [analyzer] INFO: Analysis completed.
Signatures
Wireshark
10:14
30/10/2024

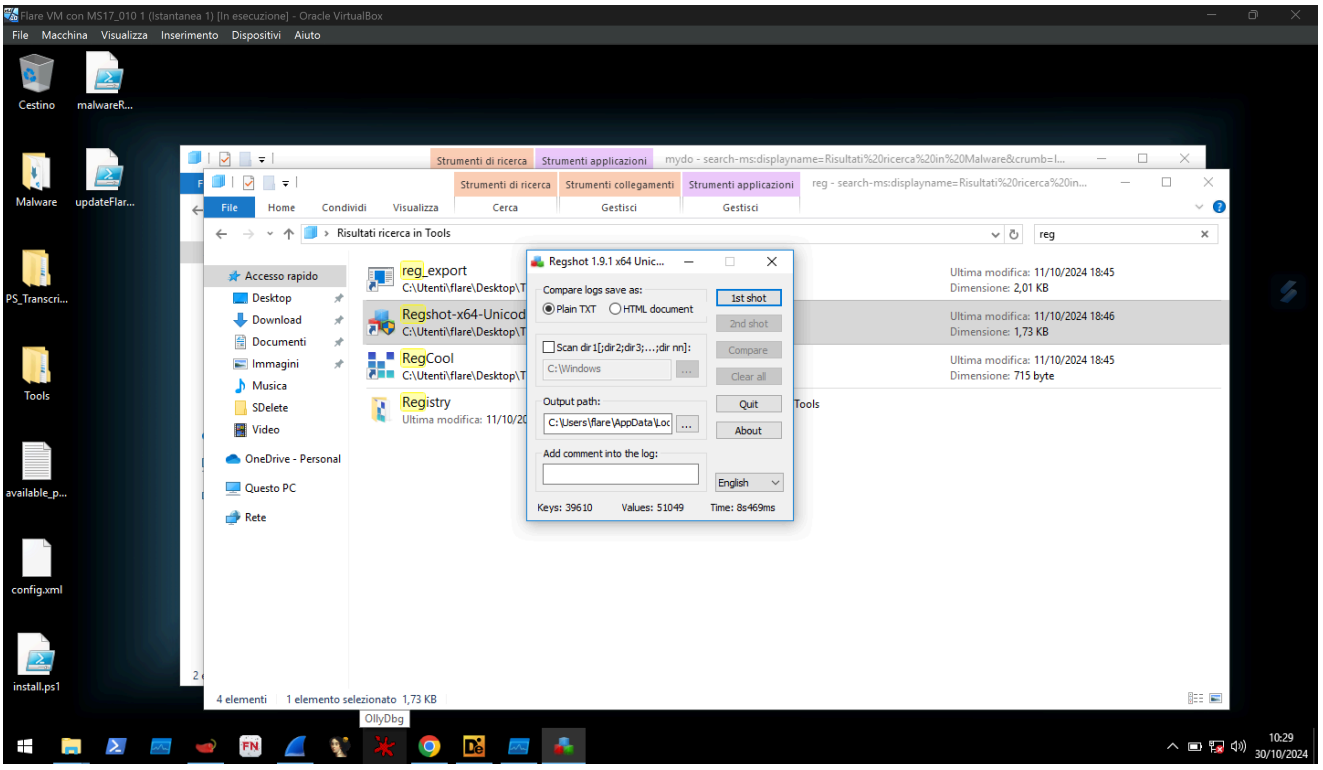


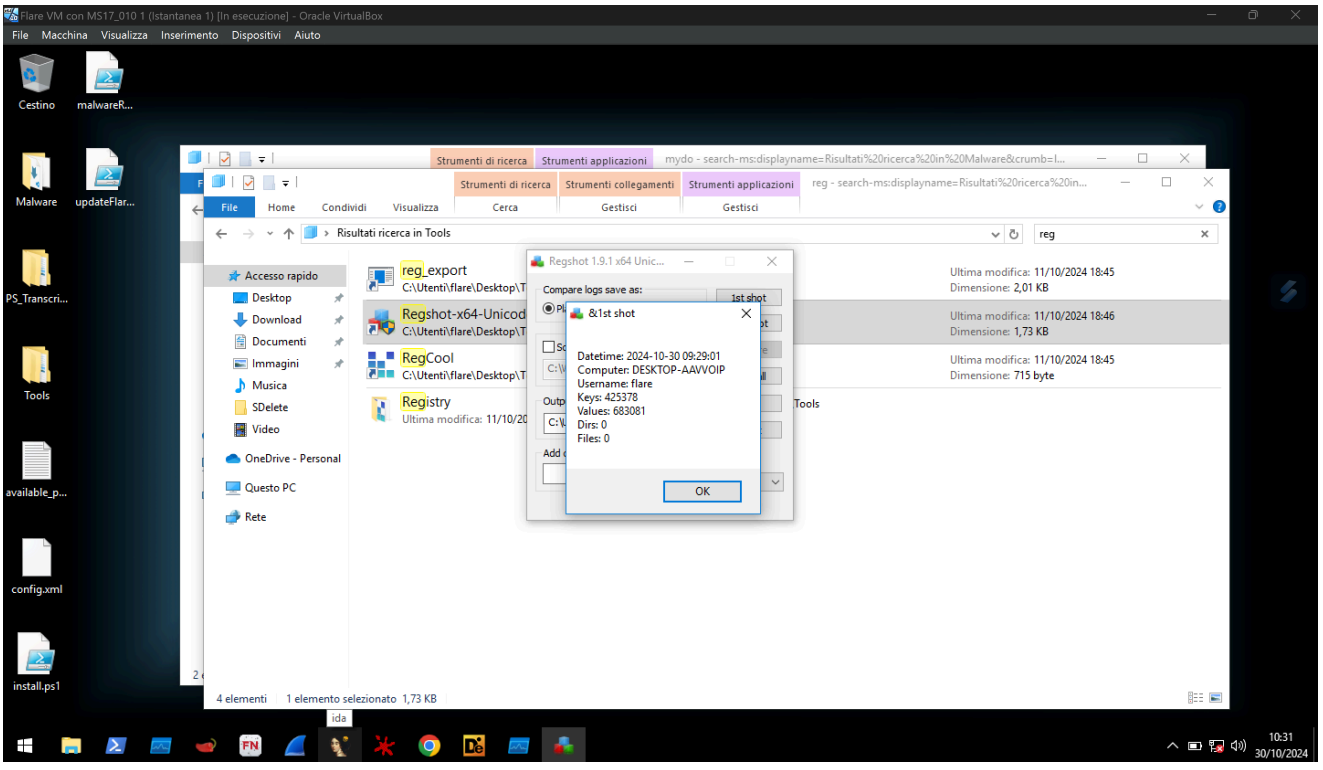
Comportamento del Worm

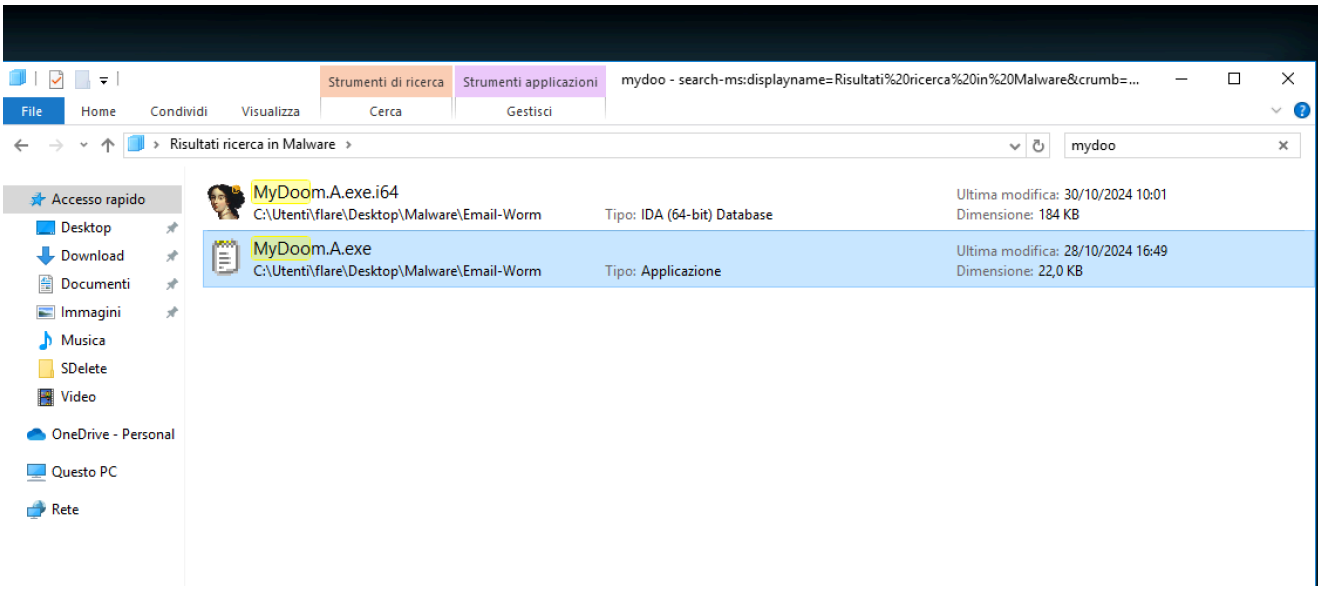
⚜️ **Tag:** #comportamento_malware #REGSHOT #PROCMON #kernel32

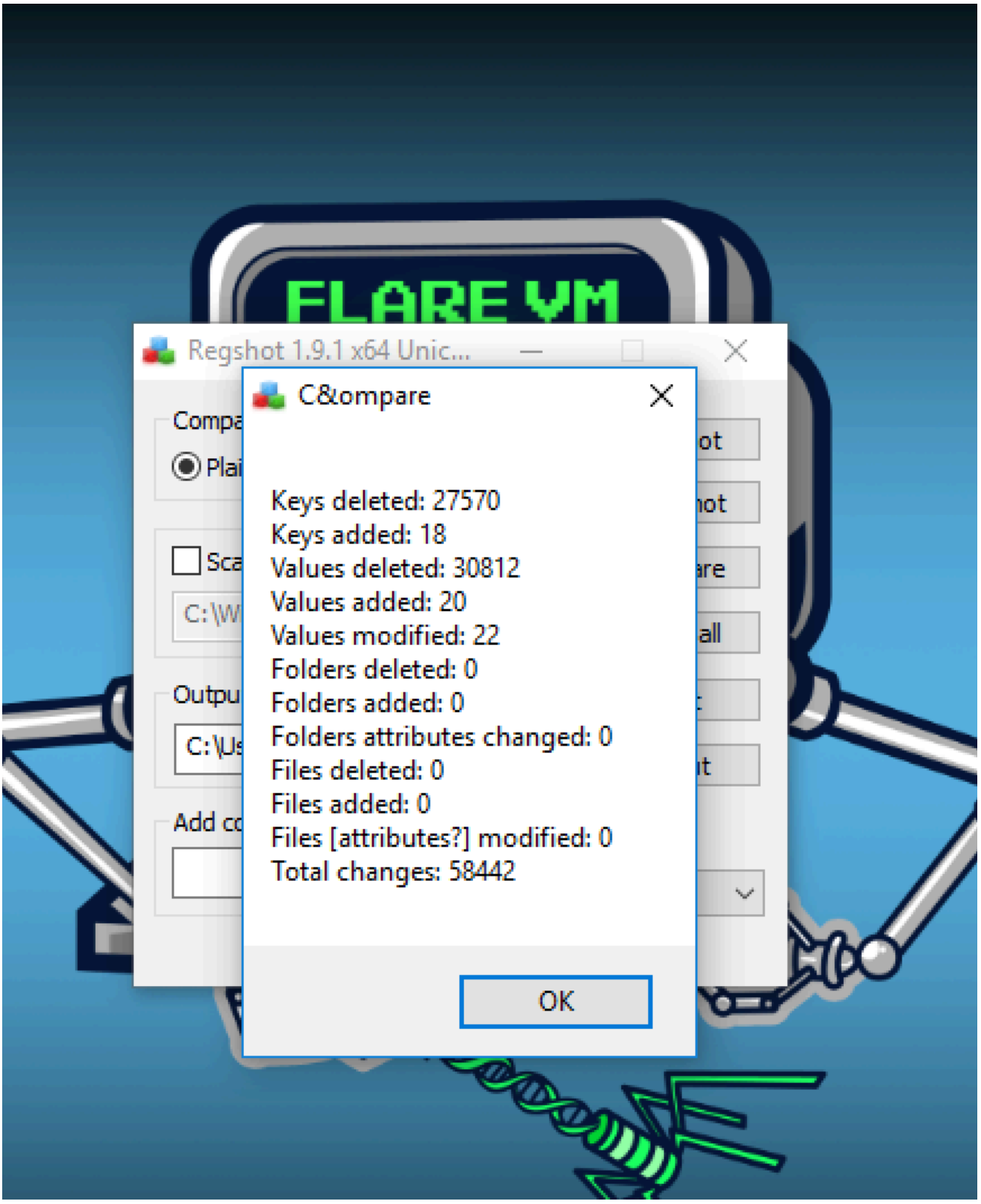
L’analisi comportamentale del worm è stata svolta con vari tool per verificare l’impatto del worm sul sistema:

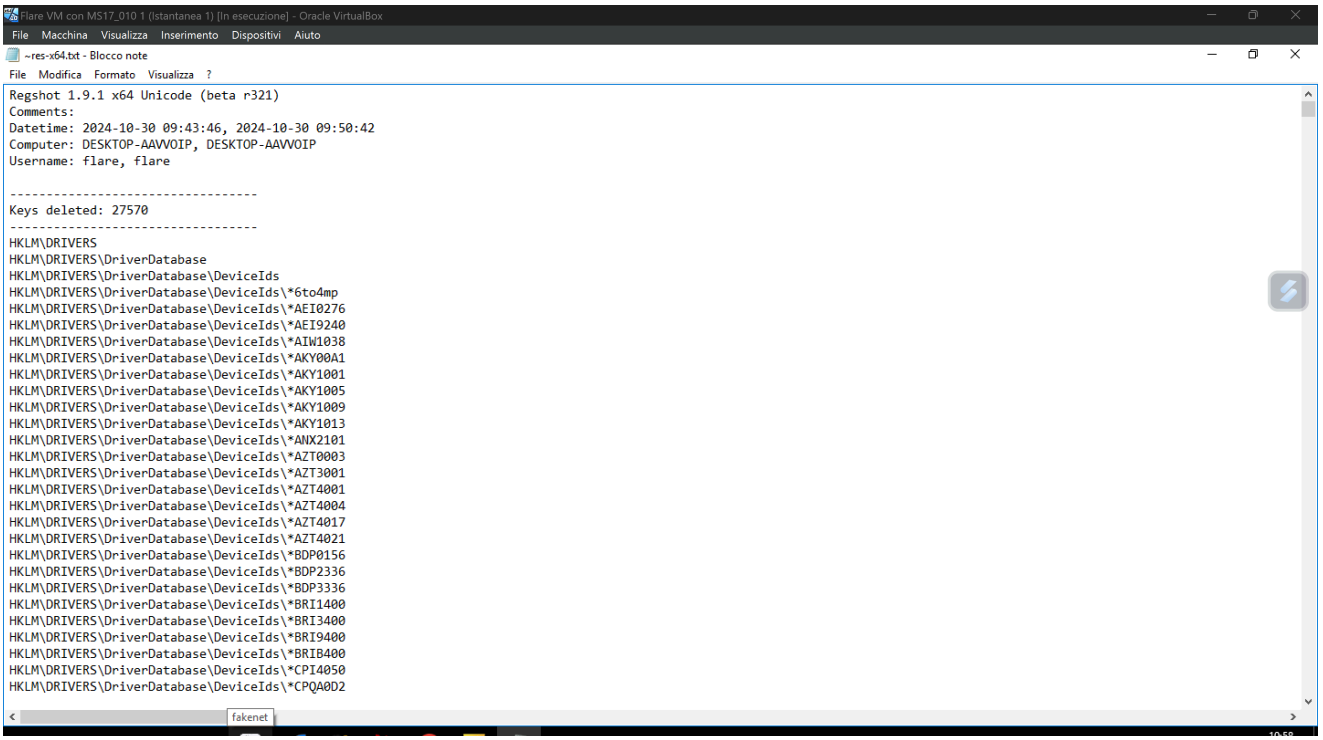
1. **REGSHOT**: Verifica delle chiavi di registro prima e dopo l'esecuzione del worm.
    - Numero di chiavi prima: 425378.
    - Dopo l’avvio: Eliminazione di oltre 27.000 chiavi e modifica di 20 valori.


Flare VM con MS17_010 1 (istantanea 1) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malwareR...
Malware
updateFlar...
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Regshot 1.9.1 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear all
Quit
About
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\flare\AppData\Loc
Add comment into the log:
English
Keys: 39610
Values: 51049
Time: 8s469ms
reg_export
Regshot-x64-Unicod
RegCool
Registry
Ultima modifica: 11/10/2024 18:45
Dimensione: 2,01 KB
Ultima modifica: 11/10/2024 18:46
Dimensione: 1,73 KB
Ultima modifica: 11/10/2024 18:45
Dimensione: 715 byte
4 elementi
1 elemento selezionato 1,73 KB
OllyDbg
10:29
30/10/2024

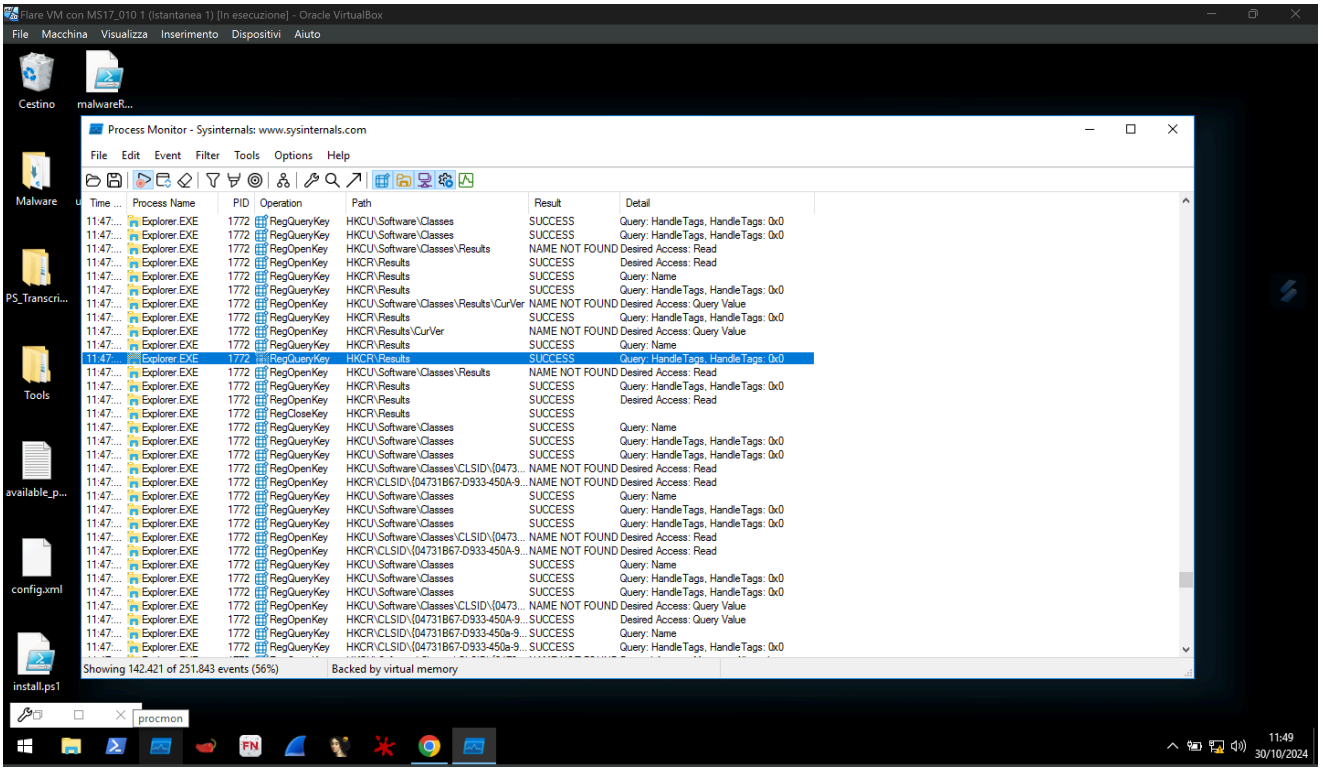

Flare VM con MS17_010 1 (istantanea 1) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malwareR...
Malware
updateFlar...
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
&1st shot
Datetime: 2024-10-30 09:29:01
Computer: DESKTOP-AAVVOIP
Username: flare
Keys: 425378
Values: 683081
Dirs: 0
Files: 0
OK
reg_export
Regshot-x64-Unicod
RegCool
Registry
Ultima modifica: 11/10/2024 18:45
Dimensione: 2,01 KB
Ultima modifica: 11/10/2024 18:46
Dimensione: 1,73 KB
Ultima modifica: 11/10/2024 18:45
Dimensione: 715 byte
4 elementi
1 elemento selezionato 1,73 KB
ida
10:31
30/10/2024

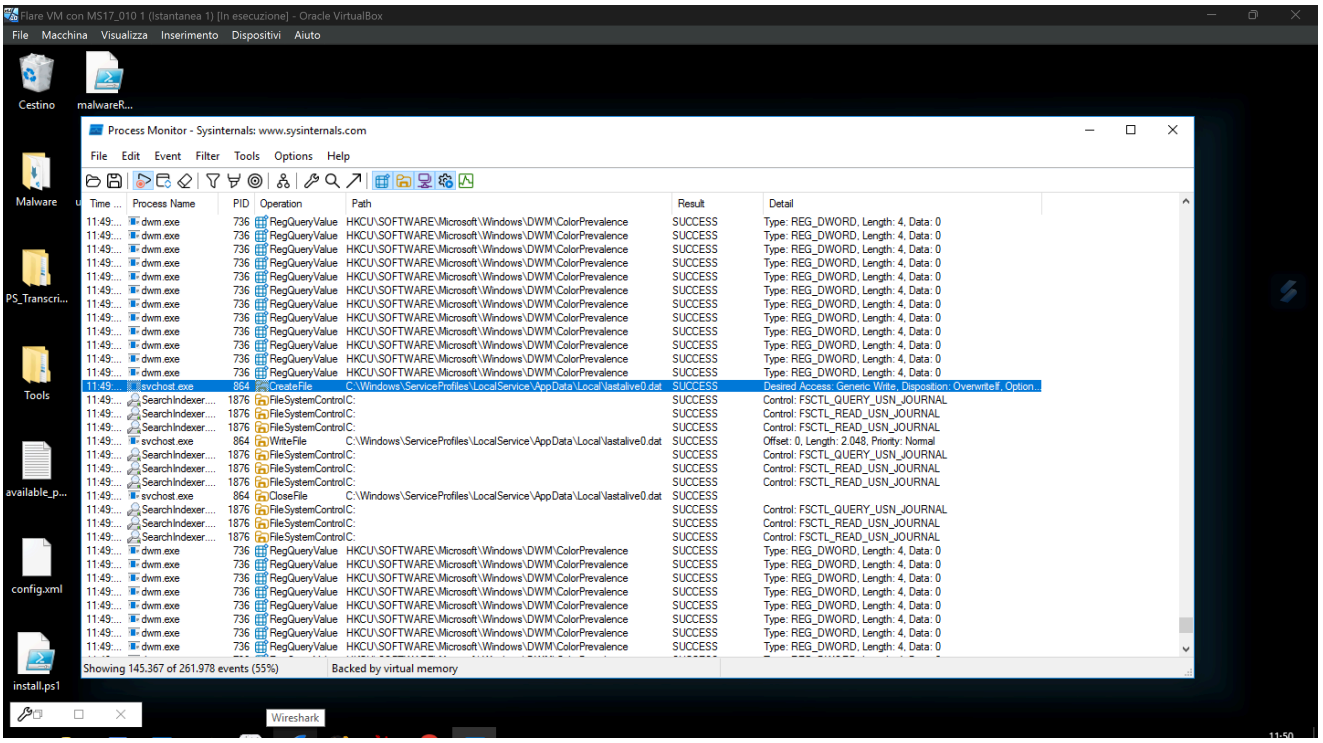

Strumenti di ricerca
Strumenti applicazioni
mydoo - search-ms:displayname=Risultati%20ricerca%20in%20Malware&crumb=...
File
Home
Condividi
Visualizza
Cerca
Gestisci
Risultati ricerca in Malware
mydoo
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
SDelete
Video
OneDrive - Personal
Questo PC
Rete
MyDoom.A.exe.i64
C:\Utenti\flare\Desktop\Malware\Email-Worm
Tipo: IDA (64-bit) Database
Ultima modifica: 30/10/2024 10:01
Dimensione: 184 KB
MyDoom.A.exe
C:\Utenti\flare\Desktop\Malware\Email-Worm
Tipo: Applicazione
Ultima modifica: 28/10/2024 16:49
Dimensione: 22,0 KB

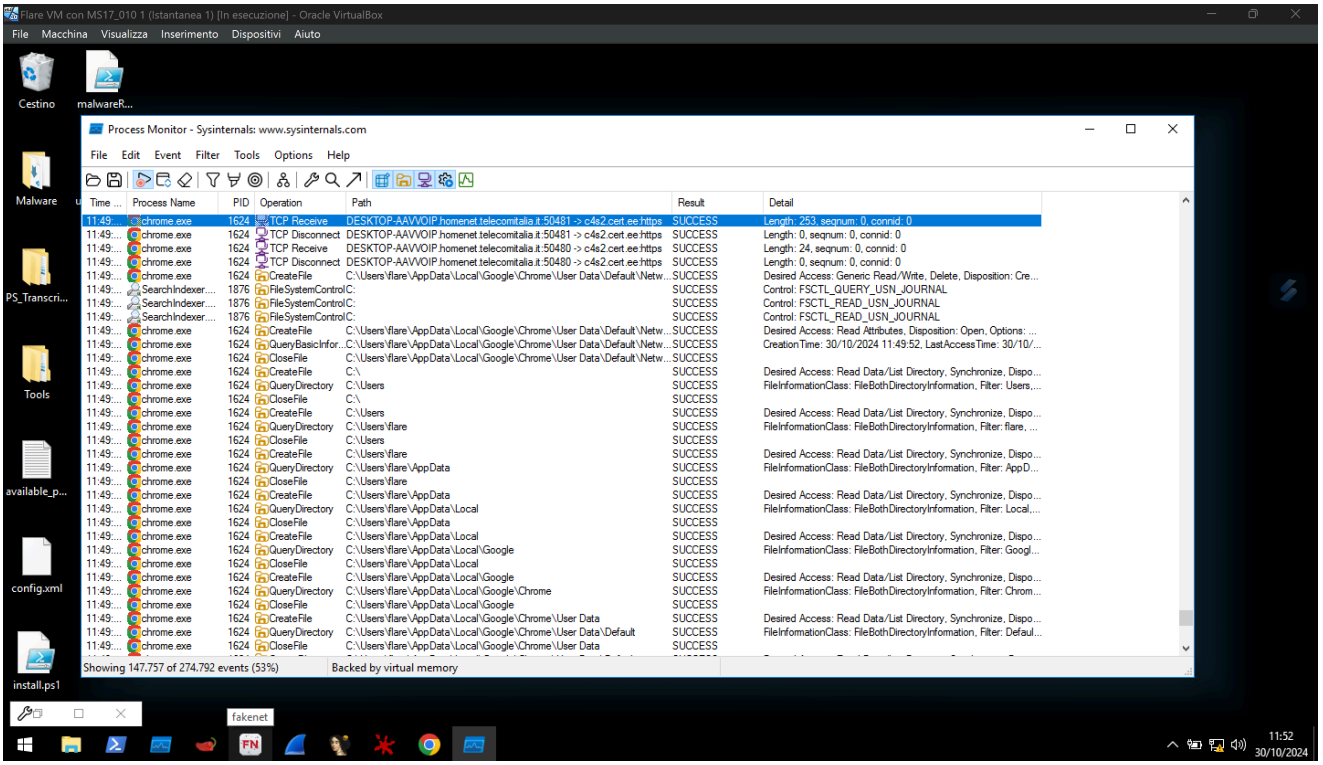

FLARE VM
Regshot 1.9.1 x64 Unic...
C&ompare
Keys deleted: 27570
Keys added: 18
Values deleted: 30812
Values added: 20
Values modified: 22
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 58442
OK

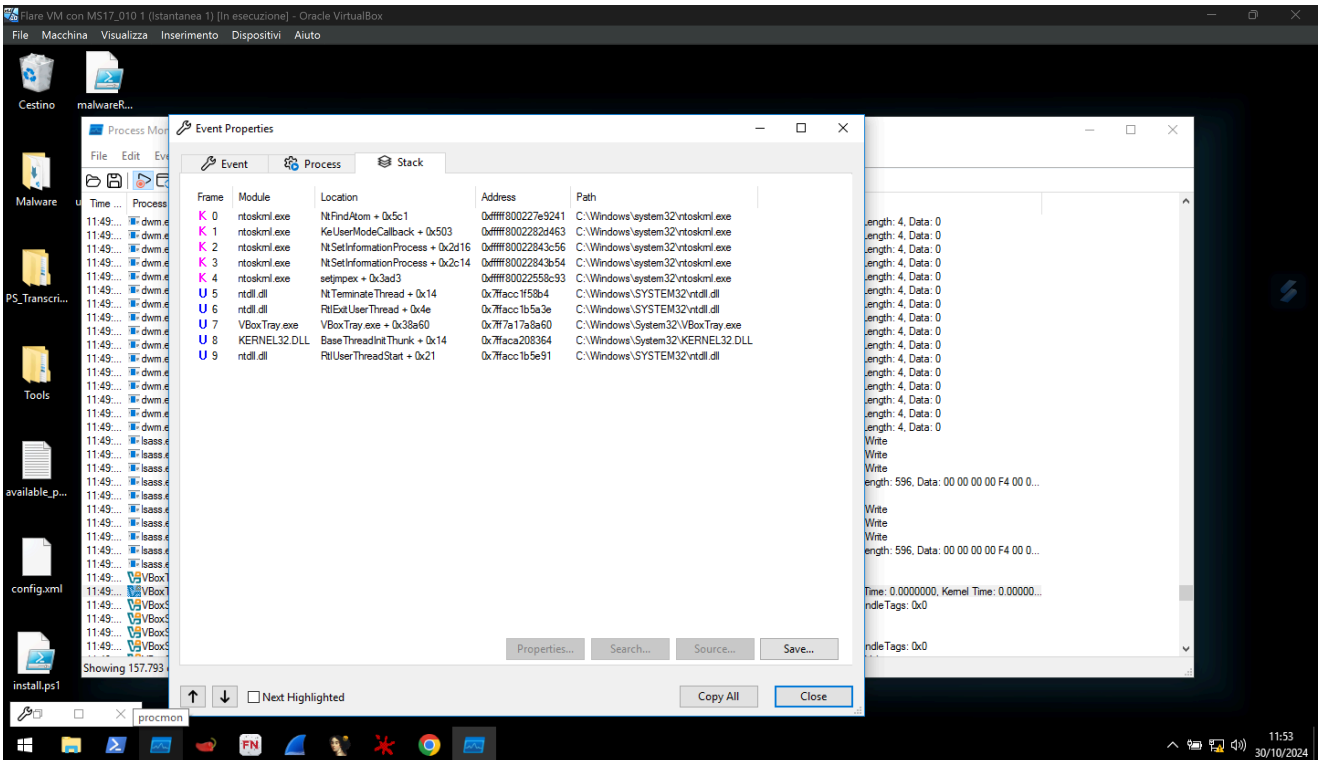


2. **PROCMON**: Monitoraggio dei processi in tempo reale.
    - Il worm modifica o elimina chiavi di registro e crea cartelle di sistema per l'installazione di backdoor, ottenendo così il controllo remoto delle macchine compromesse.
    - Utilizza il `KERNEL32.DLL` per ripresentarsi a ogni formattazione, rendendo il sistema vulnerabile.

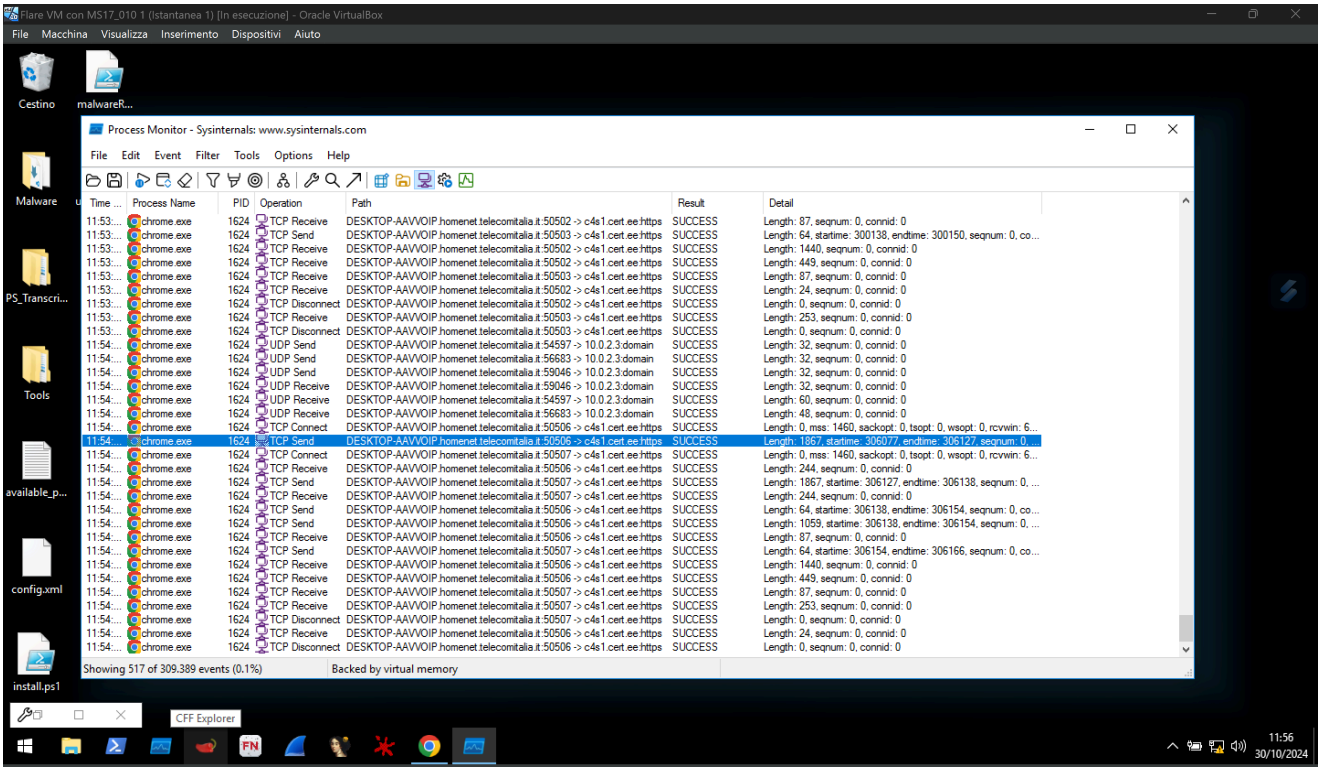



Flare VM con MS17_010 1 (istantanea 1) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malwareR...
Malware
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 145.367 of 261.978 events (55%)
Backed by virtual memory
Wireshark


Flare VM con MS17_010 1 (istantanea 1) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
malwareR...
Malware
PS_Transcri...
Tools
available_p...
config.xml
install.ps1
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Showing 147.757 of 274.792 events (53%)
Backed by virtual memory
fakenet
11:52
30/10/2024



3. **Attacchi DOS**: Oltre alle modifiche descritte, MYDOOM esegue attacchi DOS per rendere inaccessibili i sistemi infetti, saturando i processi TCP come mostrato dai log.



Raccomandazioni

⚜️ **Tag:** #raccomandazioni #sicurezza_informatica #prevenzione

1. **Aggiornamenti Regolari**: Mantenere sistemi e software aggiornati.
2. **Soluzioni di Sicurezza**: Utilizzo di firewall e antimalware aggiornati per prevenire infezioni.
3. **Educazione degli Utenti**: Formare gli utenti sui rischi legati al malware e sulle pratiche sicure di utilizzo del sistema.
4. **Analisi Proattiva**: Monitoraggio costante del traffico di rete e dei log per identificare attività sospette.
5. **Collaborazione**: Cooperare con agenzie di sicurezza per un blocco tempestivo delle minacce.

🔑 **Chiavi:**
[MYDOOM, malware, analisi statica, analisi dinamica, sicurezza informatica, worm, KERNEL32, attacchi DOS, firewall, UPX]

Suggerimenti per Approfondimenti

- **Analisi di altri worm**: Valutare e confrontare il comportamento di altri worm come Sasser e Blaster.
- **Tecniche di Persistence**: Esplorare in dettaglio le tecniche di persistenza dei malware.
- **Strumenti di analisi avanzata**: Approfondire l'uso di strumenti come Yara per l'identificazione di pattern specifici nel codice malevolo.