

Pratica W21D1(1-2)

Traccia:



Esercizio
Analisi dinamica

Traccia:

Nella lezione teorica, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- ❑ Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor (procmon)
- ❑ Identificare eventuali azioni del malware su **processi e thread** utilizzando Process Monitor
- ❑ Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (**le differenze**)



Esercizio
Analisi dinamica

Traccia:

Nella lezione teorica, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- ❑ Identificare eventuali azioni del malware sul **file system** utilizzando **multimon**
<https://www.resplendence.com/multimon>
- ❑ Identificare eventuali altre azioni del malware
- ❑ Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Soluzione:

Utilizziamo innanzitutto CFF Explorer, questo è uno strumento software utilizzato principalmente per

analizzare, modificare e estrarre informazioni da file eseguibili Windows, come file EXE, DLL, SYS e altri formati correlati. Il nome "CFF" sta per "Code Freaks File Explorer".

Le funzionalità principali di CFF Explorer includono:

1. **Analisi dei file eseguibili:** CFF Explorer fornisce dettagliate informazioni sui file eseguibili, come l'header del file, le sezioni, le tabelle di esportazione e di importazione, nonché altre informazioni pertinenti.
2. **Modifica dei file:** Permette agli utenti di modificare alcuni aspetti dei file eseguibili, come cambiare le intestazioni dei file, manipolare le tabelle di esportazione e di importazione, e altro ancora.
3. **Estrazione di risorse:** Consente di estrarre risorse come immagini, icone, stringhe e altri dati incorporati nei file eseguibili.
4. **Analisi dei file in esecuzione:** Può essere utilizzato per esaminare i processi in esecuzione nel sistema, fornendo informazioni dettagliate sui processi, i moduli caricati e altro ancora.
5. **Patch e reverse engineering:** È utilizzato anche per l'applicazione di patch ai file eseguibili e per il reverse engineering, consentendo agli utenti di analizzare il codice dei programmi e apportare modifiche.

Sezioni:

- **File Header (Intestazione del file):** Questa sezione fornisce informazioni di base sul file, come il tipo di file (ad esempio, PE32 o PE32+), la versione del linker, la data e l'ora di compilazione, le dimensioni del codice e dei dati, l'indirizzo dell'entry point, e altro ancora.
- **Optional Header (Intestazione opzionale):** Contiene informazioni aggiuntive sul file, come l'architettura del processore di destinazione, la versione del sistema operativo richiesta, le caratteristiche del file (ad esempio, se è eseguibile, DLL, ecc.), le dimensioni delle sezioni, l'allineamento della memoria, e così via.
- **Sections (Sezioni):** Questa sezione elenca tutte le sezioni presenti nel file eseguibile, come il codice eseguibile, i dati inizializzati, i dati non inizializzati, le risorse, le informazioni di debug, ecc. Fornisce informazioni dettagliate su ciascuna sezione, come l'indirizzo di inizio, la dimensione, gli attributi di protezione, e altro ancora.
- **Imports (Importazioni):** Mostra le librerie esterne che il file eseguibile importa durante l'esecuzione, insieme alle funzioni specifiche importate da ciascuna libreria. Questa sezione è utile per comprendere le dipendenze di un file eseguibile e le funzioni che utilizza da altre librerie.
- **Exports (Esportazioni):** Elenco delle funzioni esportate dal file eseguibile. Le funzioni esportate sono accessibili ad altri programmi o librerie. Questa sezione è importante quando si utilizzano le librerie DLL, in quanto fornisce informazioni sulle funzioni che possono essere utilizzate esternamente.

- **Resources (Risorse)**: Contiene una lista di tutte le risorse incorporate nel file eseguibile, come immagini, icone, stringhe, manifesti, e altro ancora. Questa sezione consente di estrarre o visualizzare le risorse integrate nel file.
- **Manifest (Manifesto)**: Sezione che mostra il manifest del file eseguibile. Il manifest contiene informazioni sulle dipendenze del sistema operativo, i privilegi richiesti, la versione di Windows supportata e altre informazioni relative alla compatibilità.
- **TLS (Thread Local Storage)**: Mostra le informazioni relative allo storage locale del thread (TLS), che sono dati accessibili solo al thread che li ha allocati. Questa sezione è utile per programmi multithreading.
- **Debug (Debug)**: Fornisce informazioni di debug, come i simboli di debug e altre informazioni utili per il debug del programma.

CFF Explorer VIII - [Malware_U3_W2_L2.exe]

File Settings ?

Malware_U3_W2_L2.exe

Property Value

File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malw...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	52.00 KB (53248 bytes)
PE Size	52.00 KB (53248 bytes)
Created	Friday 08 April 2011, 12:55:00
Modified	Wednesday 17 January 2024, 17:48:15
Accessed	Friday 08 April 2011, 12:55:00
MD5	E2BF42217A67E46433DA8B6F4507219E
SHA-1	DAF263702F11DC0430D30F9BF443E7885CF91FCB

Property Value

Empty	No additional info available
-------	------------------------------

CFF Explorer VIII - [Malware_U3_W2_L2.exe]

File Settings ?

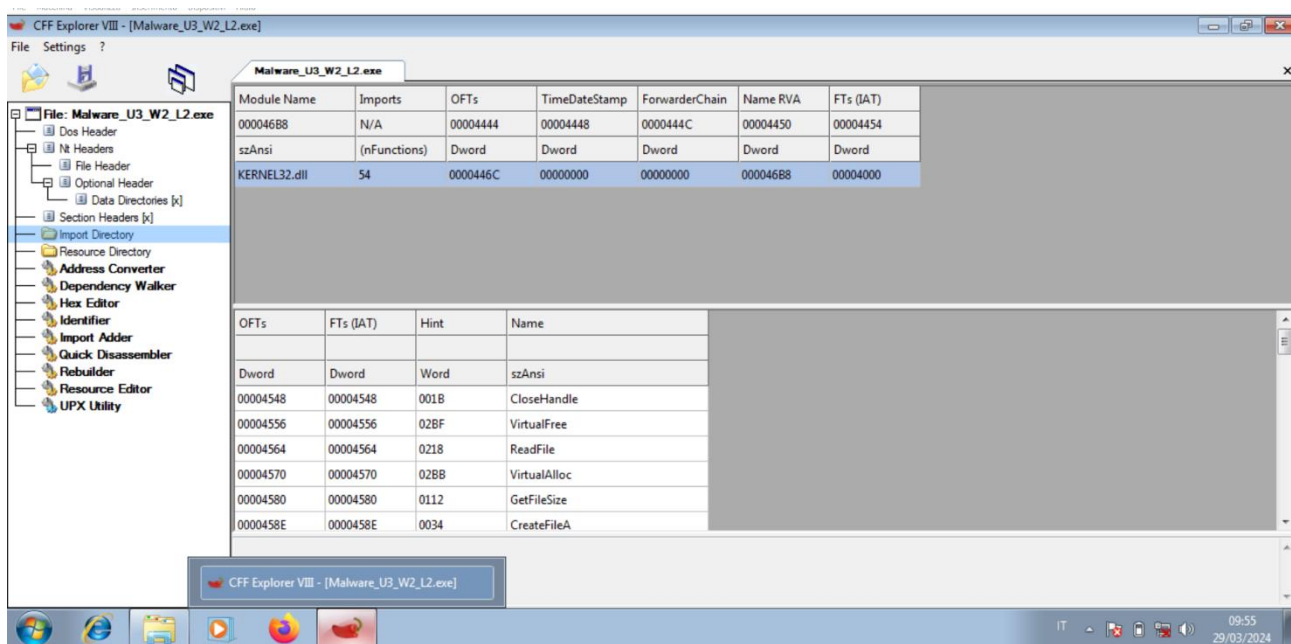
Malware_U3_W2_L2.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00002E96	00001000	00003000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000008F2	00004000	00001000	00004000	00000000	00000000	0000	0000	40000040
.data	000007DC	00005000	00001000	00005000	00000000	00000000	0000	0000	C0000040
.rsrc	00006084	00006000	00007000	00006000	00000000	00000000	0000	0000	40000040

This section contains:

Code Entry Point: 00001ADB

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	55	8B	EC	51	C7	45	FC	00	00	00	00	EB	09	8B	45	FC	U!QcEu...e!Eu
00000010	83	C0	01	89	45	FC	8B	4D	FC	3B	4D	0C	73	15	8B	55	!A!Eu!Hu;M!e+!U
00000020	08	03	55	FC	8A	02	32	45	10	8B	4D	08	03	4D	FC	88	!U!i!-2E+!M!c!Hu!
00000030	01	EB	DA	8B	E5	5D	C3	55	8B	EC	83	EC	10	C7	45	F8	eU!a!AU!i!i+!C!e
00000040	00	00	00	00	6A	00	68	80	00	00	00	6A	03	6A	00	6A	...j.h!...j!-j!j



-Ora utilizziamo **Regshot**, questo è un'applicazione software utilizzata per confrontare lo stato del registro di sistema di Windows prima e dopo l'installazione di un'applicazione o di modifiche al sistema. È spesso utilizzato dagli utenti e dagli amministratori di sistema per identificare esattamente quali modifiche sono state apportate al registro di sistema durante un'installazione o durante l'esecuzione di determinate azioni sul sistema operativo.

Facciamo uno shot prima e dopo l'avvio del malware:

Regshot 1.9.0 x64 Unicode

Compare logs save as:

☒ Plain TXT ☐ HTML document

☐ Scan dir 1[:dir 2;dir 3;...;dir nn]:

C:\Windows

Output path:

C:\Users\user\AppData\Loc

Add comment into the log:

English

1st shot

2nd shot

Compare

Clear

Quit

About

Keys:226440 Values:441315 Time:2s359ms

~res-x64_0000 - Blocco note

File Modifica Formato Visualizza ?

Regshot 1.9.0 x64 Unicode

Comments:

Datetime: 2024/3/30 07:34:57 , 2024/3/30 07:39:55

Computer: USER-PC , USER-PC

Username: user , user

Keys deleted: 2

HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\Schedule\TaskCache\Plain\{7206988A-C46D-4E3A-B05A-704B104EF1F3}

HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7206988A-C46D-4E3A-B05A-704B104EF1F3}

Keys added: 47

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5

HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASAPI32

HKLM\SOFTWARE\Microsoft\Tracing\iexplore_RASMANCS

HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\Schedule\TaskCache\Plain\{C6AFEE2A-8FC7-4FAD-93C2-2053166EB793}

HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C6AFEE2A-8FC7-4FAD-93C2-2053166EB793}

HKLM\SOFTWARE\wow6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_RSPMMFS\0000\Control

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_RSPMON\0000\Control

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control

HKLM\SYSTEM\ControlSet001\services\PROCMON23

HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances

HKLM\SYSTEM\ControlSet001\services\PROCMON23\Instances\Process Monitor 23 Instance

HKLM\SYSTEM\Setup\Setupapi\LogStatus

HKLM\SYSTEM\CurrentControlSet\Control\Class\{3A1380F4-708F-49DE-B2EF-04D25EB009D5}

HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RSPMMFS\0000\Control

HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RSPMON\0000\Control

HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23

HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000

HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control

HKLM\SYSTEM\CurrentControlSet\services\PROCMON23

HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances

HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Instances\Process Monitor 23 Instance

-Ora utilizziamo **Procmon (Process Monitor)** , questo è uno strumento di monitoraggio avanzato per il sistema operativo Windows, sviluppato da Microsoft. Serve principalmente per monitorare e registrare l'attività del sistema in tempo reale, inclusi processi, thread, file di registro, attività di rete, operazioni di registro di sistema e altro ancora. È uno strumento estremamente potente utilizzato per analizzare il comportamento del sistema e risolvere una vasta gamma di problemi, come errori di applicazioni, problemi di prestazioni, vulnerabilità di sicurezza e altro ancora.

Le varie sezioni di Procmon includono:

1. Menu Principale:

- Il menu principale di Procmon fornisce accesso a varie funzionalità, inclusi comandi per avviare/fermare la registrazione, impostazioni di visualizzazione, opzioni di filtro e altro ancora.

2. Barra degli strumenti:

- La barra degli strumenti contiene pulsanti rapidi per le azioni comuni, come avviare/fermare la registrazione, cancellare il log corrente, impostare i filtri e altro ancora.

3. Visualizzazione degli eventi:

- Procmon visualizza gli eventi in tempo reale mentre monitora l'attività del sistema. Questi eventi includono operazioni di file, accesso al registro, attività di rete e altro ancora. Ogni evento è registrato con informazioni dettagliate come il timestamp, il processo che ha eseguito l'azione, il tipo di azione, il percorso del file o della chiave di registro coinvolto e altro ancora.

4. Colonne:

- Procmon mostra varie colonne di informazioni per ogni evento registrato. Queste colonne includono dettagli come il timestamp, il processo che ha generato l'evento, il tipo di evento (ad esempio, "Crea file", "Accesso al registro"), il percorso del file o della chiave di registro coinvolto, il risultato dell'operazione e altro ancora.

5. Filtro:

- Procmon consente di applicare filtri per visualizzare solo gli eventi rilevanti. I filtri possono essere basati su vari attributi, come il processo, il percorso del file, il tipo di operazione e altro ancora. Questo è estremamente utile per concentrarsi solo sugli eventi pertinenti a una particolare attività o problema.

6. Statistiche:

- Procmon offre anche informazioni statistiche, come il numero totale di eventi catturati, il numero di eventi attualmente visualizzati dopo l'applicazione dei filtri, il tempo trascorso dalla registrazione e altro ancora.

Da qui notiamo che c'è un cambio dei registri e la creazione di un file di testo chiamato svcshot.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 548
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
11:09:...	Malware_U3_...	2892	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\Software\Wow6432Node\Polici...	REPARSE	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
11:09:...	Malware_U3_...	2892	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
11:09:...	Malware_U3_...	2892	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...

Showing 140 of 62.585 events (0.2%)

Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:09:...	Malware_U3_...	2892	Process Start		SUCCESS	Parent PID: 1988, ...
11:09:...	Malware_U3_...	2892	Thread Create		SUCCESS	Thread ID: 2280
11:09:...	Malware_U3_...	2892	Load Image	C:\Users\user\Desktop\MALWARE\E...	SUCCESS	Image Base: 0x400...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x771...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x773...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73d...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x73c...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73c...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x756...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x770...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x756...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x76c...
11:09:...	Malware_U3_...	2892	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2300, Comma...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73b...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x220...
11:09:...	Malware_U3_...	2892	Thread Exit		SUCCESS	Thread ID: 2280, ...
11:09:...	Malware_U3_...	2892	Process Exit		SUCCESS	Exit Status: 0, User...

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:09:...	Malware_U3_...	2892	Process Start		SUCCESS	Parent PID: 1988, ...
11:09:...	Malware_U3_...	2892	Thread Create		SUCCESS	Thread ID: 2280
11:09:...	Malware_U3_...	2892	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x771...
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x773...
11:09:...	Malware_U3_...	2892	IRP_MJ_CLOSE	C:	SUCCESS	
11:09:...	Malware_U3_...	2892	IRP_MJ_CREA...	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND	Desired Access: G...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
11:09:...	Malware_U3_...	2892	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:09:...	Malware_U3_...	2892	IRP_MJ_CREA...	C:\Windows	SUCCESS	Desired Access: E...
11:09:...	Malware_U3_...	2892	FASTIO_NET...	C:\Windows\System32\wow64.dll	FAST IO DISALLO...	
11:09:...	Malware_U3_...	2892	IRP_MJ_CREA...	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	FASTIO_QUE...	C:\Windows\System32\wow64.dll	SUCCESS	Type: QueryBasicI...
11:09:...	Malware_U3_...	2892	IRP_MJ_CLE...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	IRP_MJ_CLOSE	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	IRP_MJ_CREA...	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
11:09:...	Malware_U3_...	2892	FASTIO_ACQU...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
11:09:...	Malware_U3_...	2892	FASTIO_ACQU...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	FASTIO_RELE...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	FASTIO_RELE...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	FASTIO_ACQU...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
11:09:...	Malware_U3_...	2892	FASTIO_RELE...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73d...
11:09:...	Malware_U3_...	2892	IRP_MJ_CLE...	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	IRP_MJ_CLOSE	C:\Windows\System32\wow64.dll	SUCCESS	
11:09:...	Malware_U3_...	2892	FASTIO_NET...	C:\Windows\System32\wow64win.dll	FAST IO DISALLO...	
11:09:...	Malware_U3_...	2892	IRP_MJ_CREA...	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...

Showing 365 of 62.585 events (0.5%)

Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegCloseKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	IRP_MJ_CREA...	C:\Users\user\D
11:48:...	Malware_U3_...	1820	Load Image	C:\Windows\Sys
11:48:...	Malware_U3_...	1820	Load Image	C:\Windows\Sys
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegCloseKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\Software\
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\SOFTWA
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\SOFTWA
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\SOFTWA
11:48:...	Malware_U3_...	1820	RegCloseKey	HKLM\SOFTWA
11:48:...	Malware_U3_...	1820	RegOpenKey	HKCU\Software\
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegOpenKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegSetInfoKey	HKLM\System\Q
11:48:...	Malware_U3_...	1820	RegQueryValue	HKLM\System\Q
11:48:...	Malware_U3_...	1820	IRP_MJ_CREA...	C:\Windows\Sys

Event Properties

Event Process Stack

Date: 29/03/2024 11:48:52
Thread: 2476
Class: File System
Operation: IRP_MJ_CREATE
Result: SUCCESS
Path: C:\Windows\SysWOW64\svchost.exe
Duration: 0.0000338

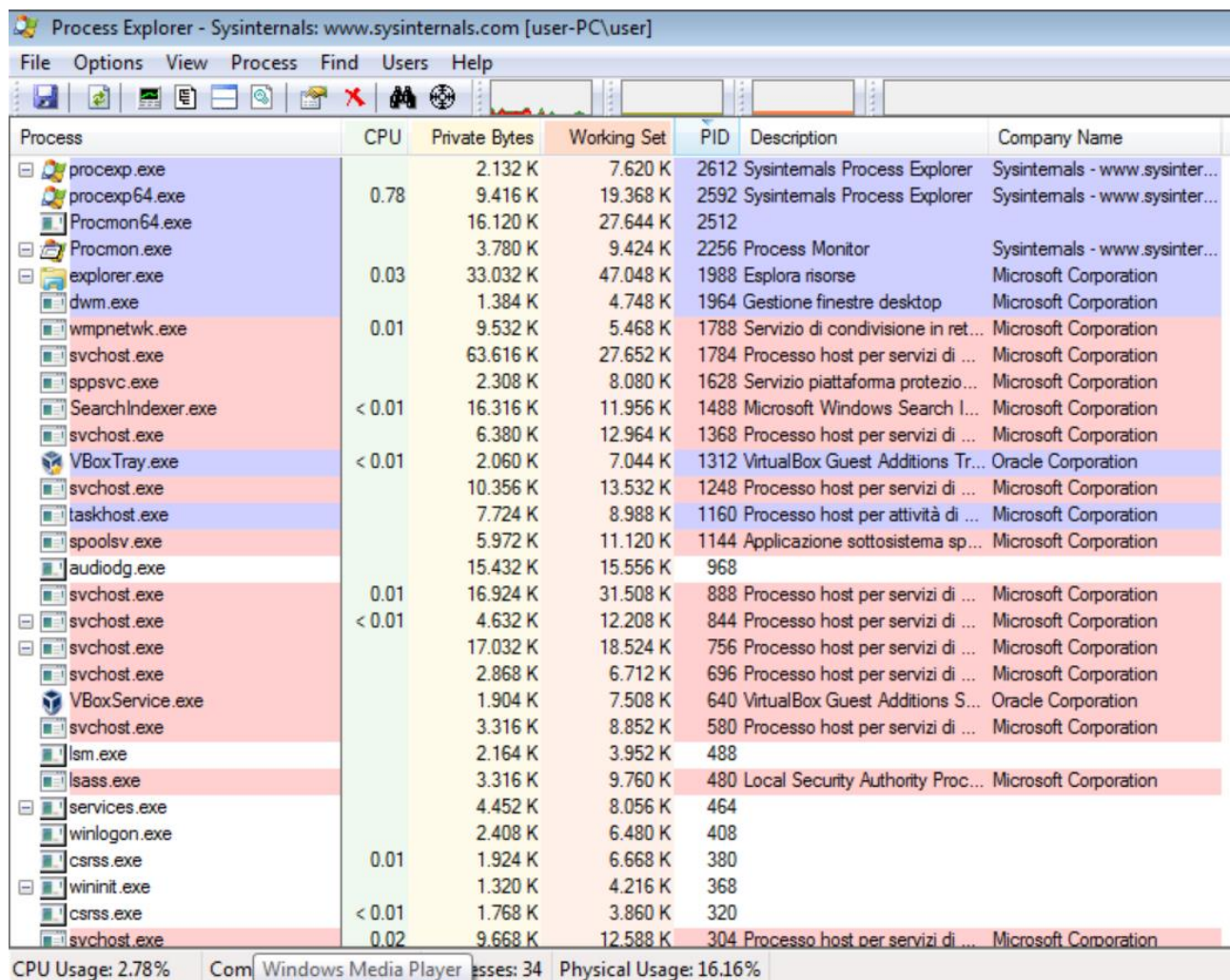
Desired Access: Read Data/List Directory, Execute/Traverse, f
Disposition: Open
Options: Synchronous IO Non-Alert, Non-Directory File
Attributes: n/a
ShareMode: Read, Delete
AllocationSize: n/a
OpenResult: Opened

Next Highlighted
Copy All Close

Showing 365 of 81.200 events (0.4%)

Backed by virtual memory

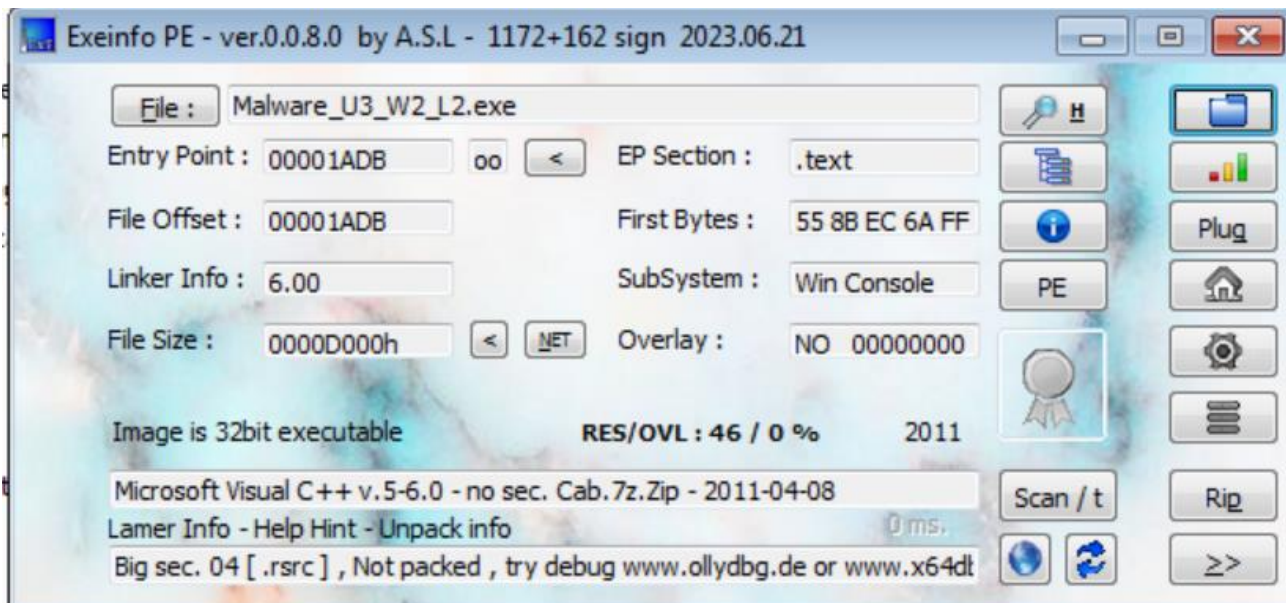
-Ora utilizziamo Process Explorer per visualizzare i servizi attivi e ricerchiamo il PID trovato frequentemente su Procmon per valutare se ancora presente l'esecuzione del malware sul nostro S.O.



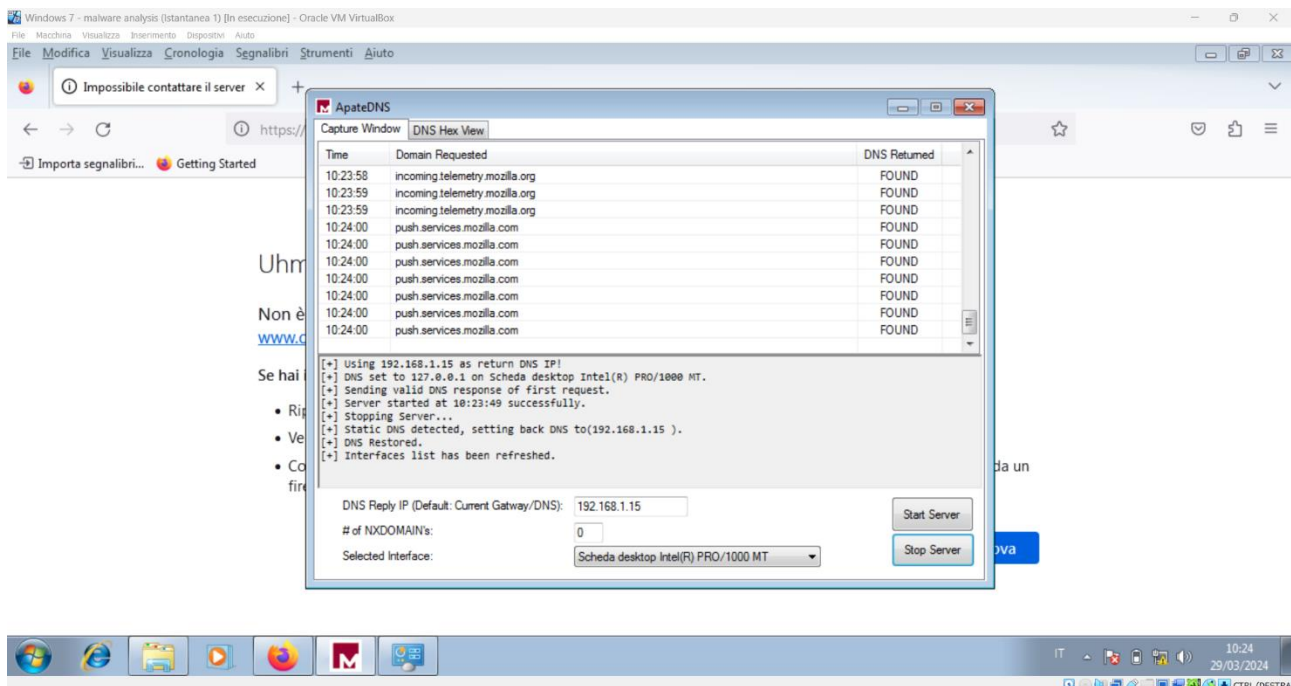
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
procexp.exe		2.132 K	7.620 K	2612	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.78	9.416 K	19.368 K	2592	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon64.exe		16.120 K	27.644 K	2512		
Procmon.exe		3.780 K	9.424 K	2256	Process Monitor	Sysinternals - www.sysinter...
explorer.exe	0.03	33.032 K	47.048 K	1988	Esplora risorse	Microsoft Corporation
dwm.exe		1.384 K	4.748 K	1964	Gestione finestre desktop	Microsoft Corporation
wmpnetwk.exe	0.01	9.532 K	5.468 K	1788	Servizio di condivisione in ret...	Microsoft Corporation
svchost.exe		63.616 K	27.652 K	1784	Processo host per servizi di ...	Microsoft Corporation
spsvc.exe		2.308 K	8.080 K	1628	Servizio piattaforma protezio...	Microsoft Corporation
SearchIndexer.exe	< 0.01	16.316 K	11.956 K	1488	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		6.380 K	12.964 K	1368	Processo host per servizi di ...	Microsoft Corporation
VBoxTray.exe	< 0.01	2.060 K	7.044 K	1312	VirtualBox Guest Additions Tr...	Oracle Corporation
svchost.exe		10.356 K	13.532 K	1248	Processo host per servizi di ...	Microsoft Corporation
taskhost.exe		7.724 K	8.988 K	1160	Processo host per attività di ...	Microsoft Corporation
spoolsv.exe		5.972 K	11.120 K	1144	Applicazione sottosistema sp...	Microsoft Corporation
audiodg.exe		15.432 K	15.556 K	968		
svchost.exe	0.01	16.924 K	31.508 K	888	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	4.632 K	12.208 K	844	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		17.032 K	18.524 K	756	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.868 K	6.712 K	696	Processo host per servizi di ...	Microsoft Corporation
VBox.Service.exe		1.904 K	7.508 K	640	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		3.316 K	8.852 K	580	Processo host per servizi di ...	Microsoft Corporation
lsim.exe		2.164 K	3.952 K	488		
lsass.exe		3.316 K	9.760 K	480	Local Security Authority Proc...	Microsoft Corporation
services.exe		4.452 K	8.056 K	464		
winlogon.exe		2.408 K	6.480 K	408		
csrss.exe	0.01	1.924 K	6.668 K	380		
wininit.exe		1.320 K	4.216 K	368		
csrss.exe	< 0.01	1.768 K	3.860 K	320		
svchost.exe	0.02	9.668 K	12.588 K	304	Processo host per servizi di ...	Microsoft Corporation

CPU Usage: 2.78% Com Windows Media Player Processes: 34 Physical Usage: 16.16%

-Ora utilizziamo **Exeinfo** che è un tool molto simile a CFF explorer:



-Ora utilizziamo **ApateDNS** , è uno strumento software progettato per simulare e testare attacchi DNS (Domain Name System) all'interno di un ambiente controllato. Questo strumento è particolarmente utile per valutare la resistenza di un'infrastruttura di rete agli attacchi che sfruttano il protocollo DNS, come ad esempio gli attacchi di spoofing DNS, il phishing basato su DNS e altri tipi di manipolazione del traffico DNS.



-Ora utilizziamo **Pestudio** , questo è uno strumento di analisi statica che viene utilizzato principalmente nell'ambito della sicurezza informatica. Ecco alcuni dettagli su di esso:

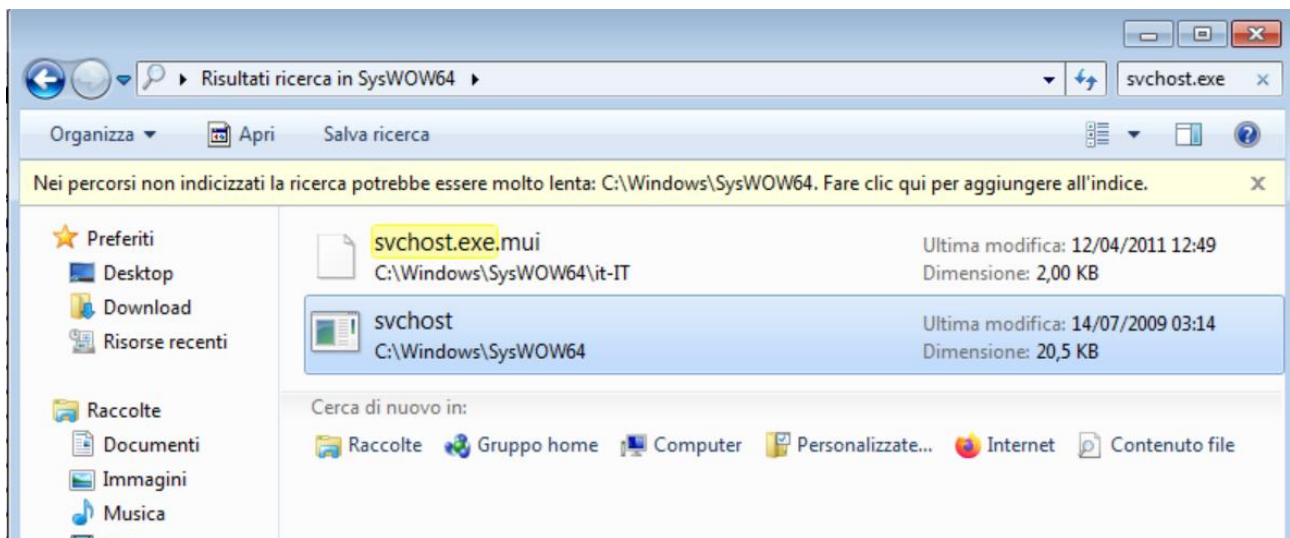
1. **Analisi Statica:** PEStudio è progettato per eseguire analisi statiche su file eseguibili Windows (formato PE, Portable Executable) senza eseguirli. Ciò significa che analizza il contenuto dei file senza eseguirli sul sistema operativo. Questo aiuta a rilevare potenziali minacce o comportamenti sospetti senza rischiare la sicurezza del sistema.
2. **Funzionalità di Analisi:** Il software fornisce una serie di funzionalità di analisi che possono aiutare gli esperti di sicurezza informatica e gli sviluppatori a identificare comportamenti dannosi o indesiderati nei file eseguibili. Queste funzionalità includono la verifica delle firme digitali, l'analisi della struttura del file, la visualizzazione delle stringhe all'interno del file, l'identificazione delle dipendenze delle librerie dinamiche e altro ancora.
3. **Rilevamento di Malware:** PEStudio è spesso utilizzato come strumento di supporto nella ricerca di malware. Le sue funzionalità di analisi possono aiutare a identificare indicatori di compromissione (IOC) nei file eseguibili, aiutando gli analisti a rilevare e rispondere alle minacce alla sicurezza informatica.

The screenshot displays the PEStudio 9.07 interface. The top window shows the 'property' tab with various file metadata. The bottom window shows the 'indicators' tab with a list of 22 indicators and their details.

property	value
md5	E28F42217A67E46433DA8B6F4507219E
sha1	DAF263702F11DC0430D30F9BF443E7885CF91FCB
sha256	AE8A1C7EB64C42EA2A04F97523EBF0844C27029EB040D910048B680F884B9DCE
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z @
file-size	53248 (bytes)
size-without-overlay	n/a
entropy	4.965
imphash	E0017B10CD72D6D03248C4D8D7943A88
signature	Microsoft Visual C++ v6.0
entry-point	55 8B EC 6A FF 68 E0 40 00 68 A0 25 40 00 64 A1 00 00 00 50 64 89 25 00 00 00 00 83 EC 10 53
file-version	n/a
description	n/a
file-type	executable
cpu	32-bit
subsystem	console
compiler-stamp	0x4D9F4BCF (Fri Apr 08 19:54:23 2011 - UTC)
debugger-stamp	n/a
resources-stamp	empty
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

xml-id	indicator (22)	detail	level
1430	The file references string(s) tagged as blacklist	count: 13	1
1525	The file contains another file	signature: unknown, location: .rsrc, offset: 0x00006084	1
1485	The count of libraries is suspicious	count: 1	1
1266	The file imports symbol(s) tagged as blacklist	count: 10	1
1267	The file references a string with a suspicious size	size: 3504 bytes	2
1267	The file references a string with a suspicious size	size: 1928 bytes	2
1267	The file references a string with a suspicious size	size: 3263 bytes	2
1251	The file references an unknown resource	resource: UNICODE:LOCALIZATION	2
1261	The file imports deprecated function(s)	count: 7	3
1036	The file checksum is invalid	checksum: 0x00000000	3
1633	The file references string(s) tagged as hint	type: file	3
1633	The file references string(s) tagged as hint	type: size	3
1268	The file references whitelist string(s)	count: 20	4
1484	The file score is not available	msg: Impossibile risolvere il nome o l'indirizzo del ...	4
1050	The file uses Control Flow Guard (CFG) as software security defense	status: no	4
1100	The file opts for Data Execution Prevention (DEP) as software security defense	status: no	4
1102	The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: no	4
1106	The file opts for Stack Buffer Overrun Detection (GS) as software security defense	status: no	4
1040	The file contains a digital Certificate	status: no	4
1109	The file opts for Code Integrity (CI) as software security defense	status: no	4

Adesso verifichiamo l'esistenza di un file chiamato svchost che sembra essere presente nella cartella SysWOW64 all'interno della cartella Windows:



-Infine installiamo **Multimon**, questo è un tool simile a Procmon (Process Monitor) che consente di monitorare e analizzare l'attività di sistema su Windows; a differenza di Procmon qui possiamo avere anche la sezione Keyword.

MultiMon 3.01 Home Edition - <http://www.resplendence.com>

File Edit View Help

Activate monitors

- ☒ File System
- ☒ System
- ☒ Registry
- ☒ Keyboard
- ☒ User
- ☒ Clipboard

Drives to monitor

Results

Time running: 0:02:0

System: 679

File System: 10409

Registry: 13129

Keyboard: 5

Processes to monitor

Date/time	Major Function	Process	Status	File	Type	Minor Fu...	Operato...	IRP Flags	PID
29/03/2024 12:46:54...	0x12 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Irp	0x00	0x46	0x00000...	2720
29/03/2024 12:46:54...	0x02 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Irp	0x00	0xA0	0x00000...	2720
29/03/2024 12:46:54...	0x00 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Irp (NPP)	0x00	0x50	0x00000...	2720
29/03/2024 12:46:54...	0xFF IRP_MJ_...	MultiMon.exe	0000012A Unk...	C:\Windows\SysWOW64\image...	MiniFilter	0x00	0x04	0x00000...	2720
29/03/2024 12:46:54...	0x05 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Fast I/O	0x00	0x56	0x00000...	2720
29/03/2024 12:46:54...	0xFE IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	MiniFilter	0x00	0xC8	0x00000...	2720
29/03/2024 12:46:54...	0x12 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Irp	0x00	0x48	0x00000...	2720
29/03/2024 12:46:54...	0x02 IRP_MJ_...	MultiMon.exe	00000000 STA...	C:\Windows\SysWOW64\image...	Irp	0x00	0x80	0x00000...	2720
29/03/2024 12:46:54...	0x00 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Critical Stop.wav	Irp (NPP)	0x00	0x5C (S...	0x00000...	1244
29/03/2024 12:46:54...	0x05 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Critical Stop.wav	Fast I/O	0x00	0x17	0x00000...	1244
29/03/2024 12:46:54...	0x05 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Critical Stop.wav	Fast I/O	0x00	0x46	0x00000...	1244
29/03/2024 12:46:54...	0x12 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Critical Stop.wav	Irp	0x00	0x00	0x00000...	1244
29/03/2024 12:46:54...	0x02 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Critical Stop.wav	Irp	0x00	0x00	0x00000...	1244
29/03/2024 12:46:54...	0x00 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Irp (NPP)	0x00	0x56 (S...	0x00000...	1244
29/03/2024 12:46:54...	0x05 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Fast I/O	0x00	0x17	0x00000...	1244
29/03/2024 12:46:54...	0x03 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Irp	IRP_MN_...	0x56 (S...	0x00060...	1244
29/03/2024 12:46:54...	0x03 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Irp	IRP_MN_...	0x17 (S...	0x00060...	1244
29/03/2024 12:46:54...	0x05 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Fast I/O	0x00	0x56	0x00000...	1244
29/03/2024 12:46:54...	0x12 IRP_MJ_...	taskhost.exe	00000000 STA...	C:\Windows\Media\Windows Ding.wav	Irp	0x00	0x17	0x00000...	1244
29/03/2024 12:46:57...	0xFF IRP_MJ_...	System	00000000 STA...	C:\Windows\Media\Windows Ding.wav	MiniFilter	0x00	0xC0	0x00000...	4
29/03/2024 12:46:57...	0xFE IRP_MJ_...	System	00000000 STA...	C:\Windows\Media\Windows Ding.wav	MiniFilter	0x00	0x48	0x00000...	4

Include Filter:

Exclude Filter:

MultiMon 3.01 Home Edition - <http://www.resplendence.com>

File Edit View Help

Activate monitors

- ☒ File System
- ☒ System
- ☒ Registry
- ☒ Keyboard
- ☒ User
- ☒ Clipboard

Drives to monitor

Results

Time running: 0:02:0

System: 679

File System: 10409

Registry: 13129

Keyboard: 5

Processes to monitor

Details

Date/time: 29/03/2024 12:45:07.4510208

Action: Active Window Change

Process: C:\Users\user\Desktop\MALWARE\Esercizio_U3_W2_I2\Malware_U3_W2_I2.exe

Position: (677,317)

Test code:

Window Title: C:\Users\user\Desktop\MALWARE\Esercizio_U3_W2_I2\Malware_U3_W2_I2.exe

Alternative Title:


Handle: 328350

PID: 2588

ThreadID: 1428

Copy to clipboard

Close

Details

Action

Date/time

29/03/2024 12:45:09.5351326

Action

Active Window Change

Process

csrss.exe

Position

(921,292)

Test code

Window Title

svchost.exe - Errore di applicazione

Alternative Title

Handle











262828

PID

380

ThreadID

416

Date/time	Action	Process	Key	Keycode	Window Title	Alternativ
 29/03/2024 12:46:52....	KeyPress	 C:\Program...	m	77	MultiMon 3.01 Home Edition - http://www.res...	
 29/03/2024 12:46:52....	KeyPress	 C:\Program...	a	65	MultiMon 3.01 Home Edition - http://www.res...	
 29/03/2024 12:46:53....	KeyPress	 C:\Program...	l	76	MultiMon 3.01 Home Edition - http://www.res...	
 29/03/2024 12:46:54....	KeyPress	 C:\Program...	ENTER	13	MultiMon 3.01 Home Edition - http://www.res...	
 29/03/2024 12:46:56....	KeyPress	 C:\Program...	BACKSP	8	MultiMon 3.01 Home Edition - http://www.res...	