W21D2-3

MALWARE ANALYSIS

La 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**)

La traccia

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

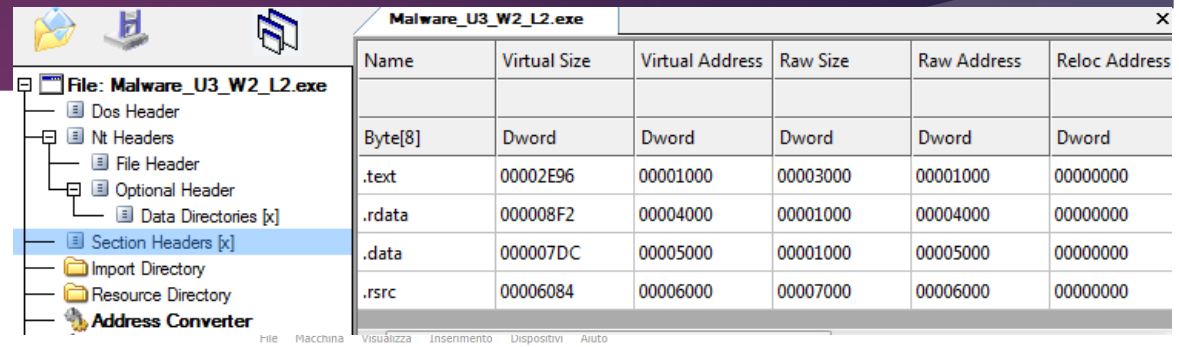
Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

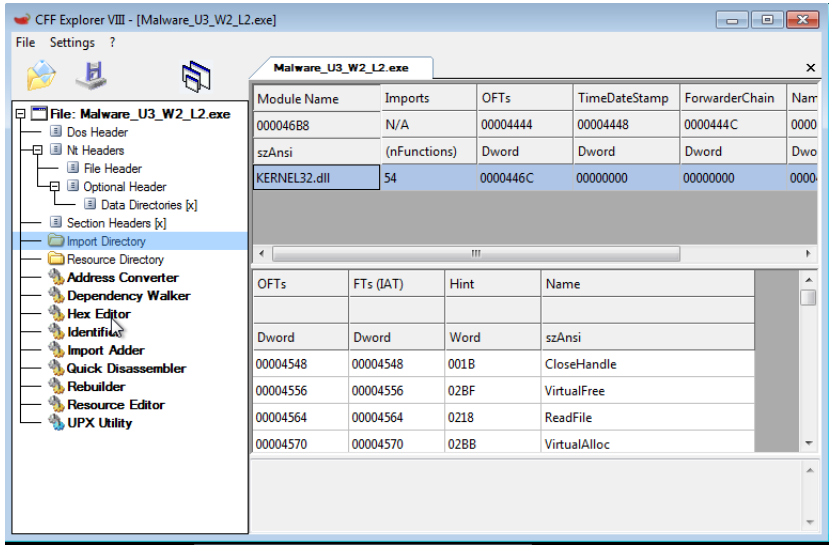
- Identificare eventuali azioni del malware sul **file system** utilizzando **multimon** **https://www.resplendence.com/multimon**
- Identificare eventuali altre azioni del malware

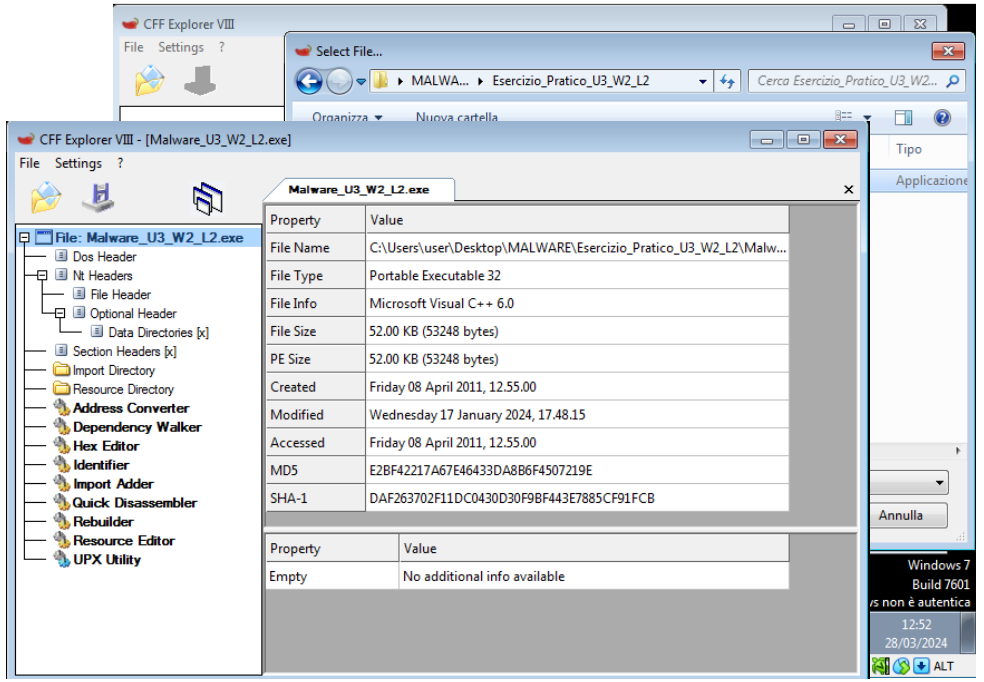
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Analisi statica del Malware

Prima di procedere con l'analisi dinamica basica possiamo effettuare una analisi statica col tool **Cff Explorer** , dove caricheremo l'eseguibile del Malware. Qui possiamo osservare le informazioni principali del file, le sezioni e le librerie importate con le relative funzioni.

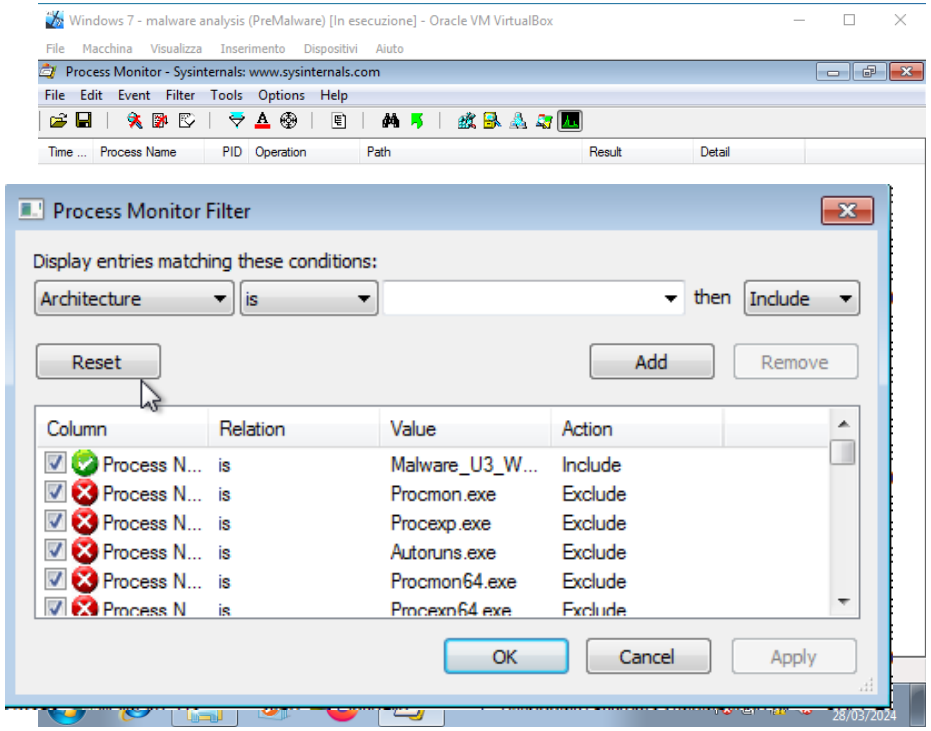


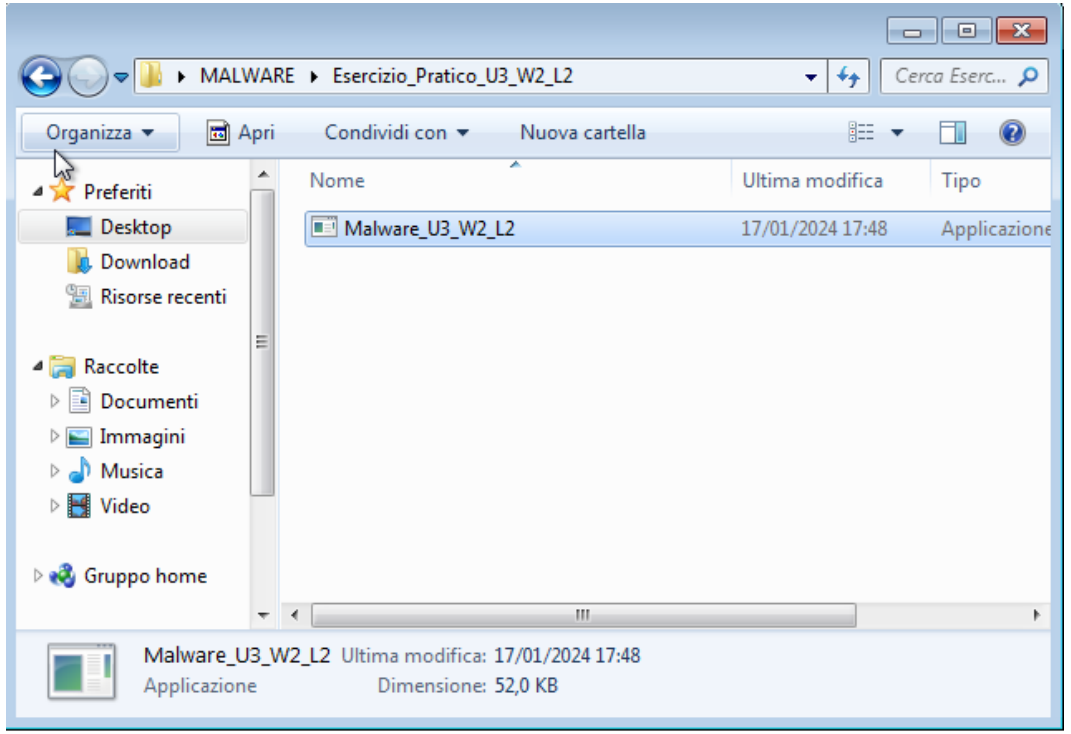




Azioni Malware sul File System

Avviamo il tool ProcMon, per prima cosa visto che il programma monitora tutte le attivitàà del pc isoleremo la sola attività del Malware tramite un filtro per Nome del processo.
Da qui relativamente a tale Malware possiamo isolare gli eventi riguardanti i processi, i thread , le modifiche al File System e l'attività di rete.





Considerazioni in merito agli eventi rilevati

Vedendo gli eventi notiamo che il Malware:

-Crea il suo processo e un thread
-Carica delle librerie(load image)
-In create file fa delle operazioni di lettura(success o failed), alcuni file non li trova o non riesce a scrivere
-Createfilemapping: la mappatura di file in memoria è un'operazione che consente ai processi di accedere direttamente ai dati presenti nei file, senza doverli leggere o scriverli esplicitamente su disco.
-Query directory come ls in linux per avere tutti i file presenti in una directory

Considerazioni in merito agli eventi rilevati

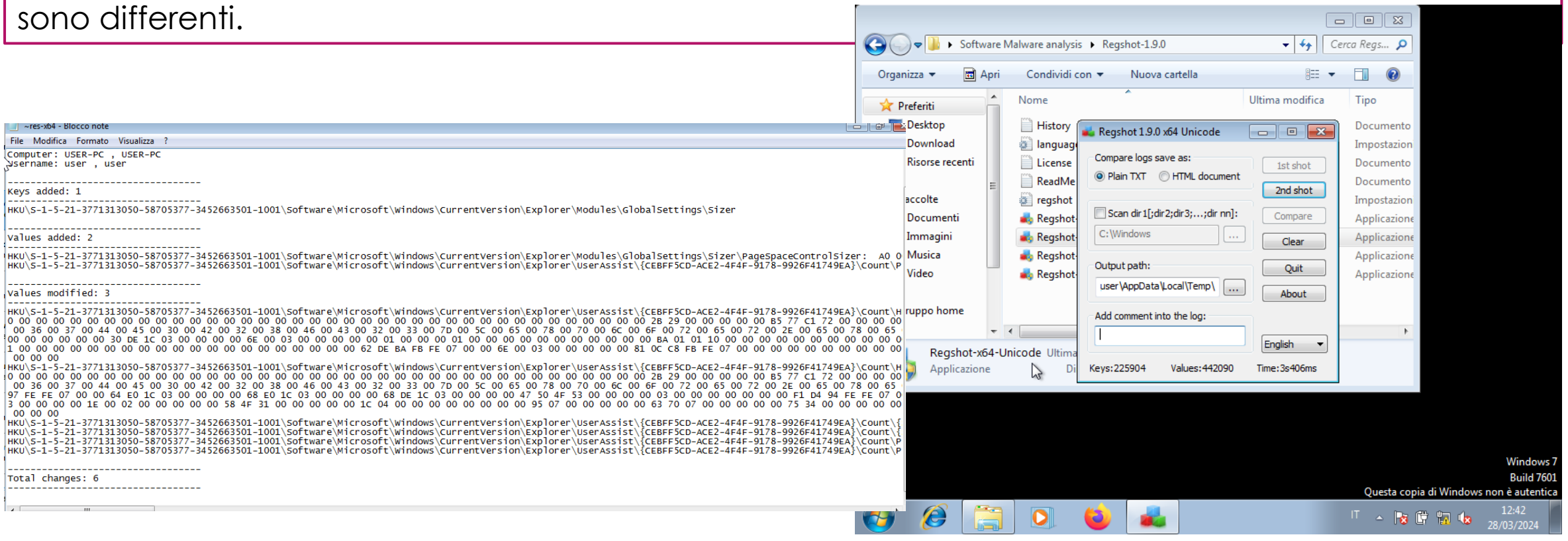
-Cerca di copiare svchost , lo crea con un pid=> se è tra i processi in corso lo trovo
-Quando apro stack di un processo vedo le funzioni invocate per dare vita a quel processo K=kernel u=usermode.
-Check chiavi di registro: può essere utile per esempio inserire sul web chiave di registro modificata per vedere se qualcuno che ha fatto un analisi dove viene menzionata si può capire a cosa porta tale modifica, questo potrebbe configurarsi come un IOC.

Multimon

-ci permette di vedere anche più eventi , per esempio errore nell'avvio Malware , il suono di sistema , cambio finestra ecc.
-sezione keyboard serve a vedere se alla pressione dei tasti corrispondono degli eventi del malware.
-clipboard serve a veder operazioni dei MW.

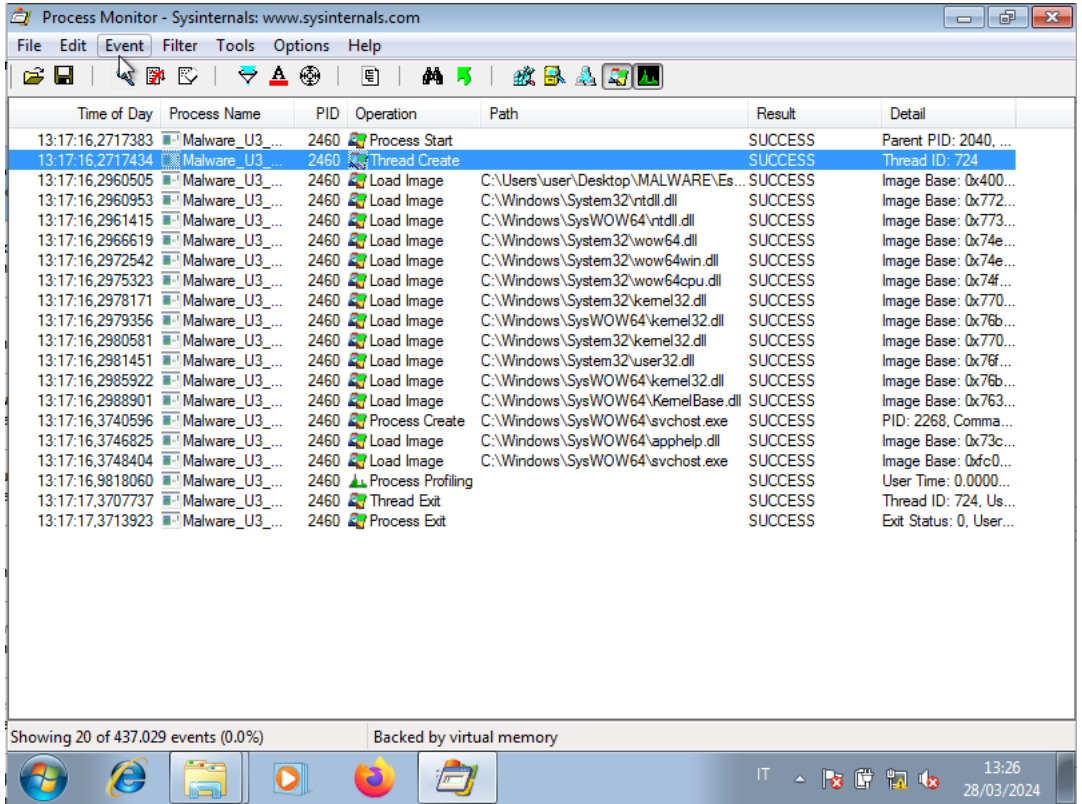
Azioni Malware: modifiche del registro

Per evidenziare le modifiche del registro procederemo con uno «shot» cioè una «fotografia» del registro prima e dopo la sua esecuzione in modo far emergere quali chiavi di registro per esempio sono differenti.



Azioni Malware relative a Processi e Threads.

Qui invece possiamo evidenziare i processi e i threads creati.



Multimon

-Cerca di copiare svchost , lo crea con un pid=> se è tra i processi in corso lo trovo
-Quando apro stack di un processo vedo le funzioni invocate per dare vita a quel processo K=kernel u=usermode.
-Check chiavi di registro: può essere utile per esempio inserire sul web chiave di registro modificata per vedere se qualcuno che ha fatto un analisi dove viene menzionata si può capire a cosa porta tale modifica, questo potrebbe configurarsi come un IOC.

Multimon

-ci permette di vedere anche più eventi , per esempio errore nell'avvio Malware , il suono di sistema , cambio finestra ecc.
-sezione keyboard serve a vedere se alla pressione dei tasti corrispondono degli eventi del malware.
-clipboard serve a veder operazioni dei MW.

Multimon

Da qui per esempio possiamo vedere come il malware crei un secondo processo con un nome di un altro processo legittimo.

19.19.53,9774067	Malware_U3_W2_L2.exe	228	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/04/2008 13.00
19.19.53,9775436	Malware_U3_W2_L2.exe	228	CreateFile	C:\	SUCCESS	Desired Access: Read Data/Li
19.19.53,9776478	Malware_U3_W2_L2.exe	228	QueryDirectory	C:\WINDOWS	SUCCESS	Filter: WINDOWS, 1: WINDOWS
19.19.53,9776484	Malware_U3_W2_L2.exe	228	CloseFile	C:\	SUCCESS	
19.19.53,9782875	Malware_U3_W2_L2.exe	228	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/Li
19.19.53,9785493	Malware_U3_W2_L2.exe	228	QueryDirectory	C:\WINDOWS\system32	SUCCESS	Filter: system32, 1: system32
19.19.53,9786689	Malware_U3_W2_L2.exe	228	CloseFile	C:\WINDOWS	SUCCESS	
19.19.53,9811533	Malware_U3_W2_L2.exe	228	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/Li
19.19.53,9813033	Malware_U3_W2_L2.exe	228	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost.exe, 1: svchost.e
19.19.53,9814600	Malware_U3_W2_L2.exe	228	CloseFile	C:\WINDOWS\system32	SUCCESS	
19.19.53,9816310	Malware_U3_W2_L2.exe	228	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16.384, EndOfFi
19.19.53,9818028	Malware_U3_W2_L2.exe	228	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeCreateSe
19.19.53,9818341	Malware_U3_W2_L2.exe	228	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16.384, EndOfFi
19.19.53,9818944	Malware_U3_W2_L2.exe	228	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
19.19.53,9820500	Malware_U3_W2_L2.exe	228	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
19.19.53,9821302	Malware_U3_W2_L2.exe	228	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	Desired Access: Read
19.19.53,9822802	Malware_U3_W2_L2.exe	228	RegCloseKey	HKCU	SUCCESS	
19.19.53,9823249	Malware_U3_W2_L2.exe	228	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	BUFFER OVERFL...	Length: 144
19.19.53,9824073	Malware_U3_W2_L2.exe	228	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	SUCCESS	Type: REG_SZ, Length: 142, De
19.19.53,9825311	Malware_U3_W2_L2.exe	228	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	SUCCESS	
19.19.53,9825705	Malware_U3_W2_L2.exe	228	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
19.19.53,9826507	Malware_U3_W2_L2.exe	228	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\LogFileName	NAME NOT FOUND	Length: 536
19.19.53,9827479	Malware_U3_W2_L2.exe	228	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
19.19.53,9827674	Malware_U3_W2_L2.exe	228	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value,
19.19.53,9828985	Malware_U3_W2_L2.exe	228	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svchost.exe	NAME NOT FOUND	Desired Access: Read
19.19.53,9831250	Malware_U3_W2_L2.exe	228	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND	Desired Access: Generic Reac
19.19.53,9833150	Malware_U3_W2_L2.exe	228	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 240, Command line: "C:\WI
19.19.53,9852208	Malware_U3_W2_L2.exe	228	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
19.19.54,9831949	Malware_U3_W2_L2.exe	228	Thread Exit			
19.19.54,9834265	Malware_U3_W2_L2.exe	228	Process Exit			
19.19.54,9836338	Malware_U3_W2_L2.exe	228	CloseFile	C:\Documents and Settings\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2	SUCCESS	

PID: 240
Command line: "C:\WINDOWS\system32\svchost.exe"

Multimon

Qui invece evidenziamo un comportamento del Malware, cioè il fatto di avviarsi per un tempo brevissimo, il tempo di generare un secondo processo con un nome legit che avrà pid diverso al fine di «nascondersi». Di fianco l'immagine del filtro per pid per visualizzare l'attività relativa.