

S10L2.

BENVENUTI LUIGI

### Traccia:

Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito). 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:

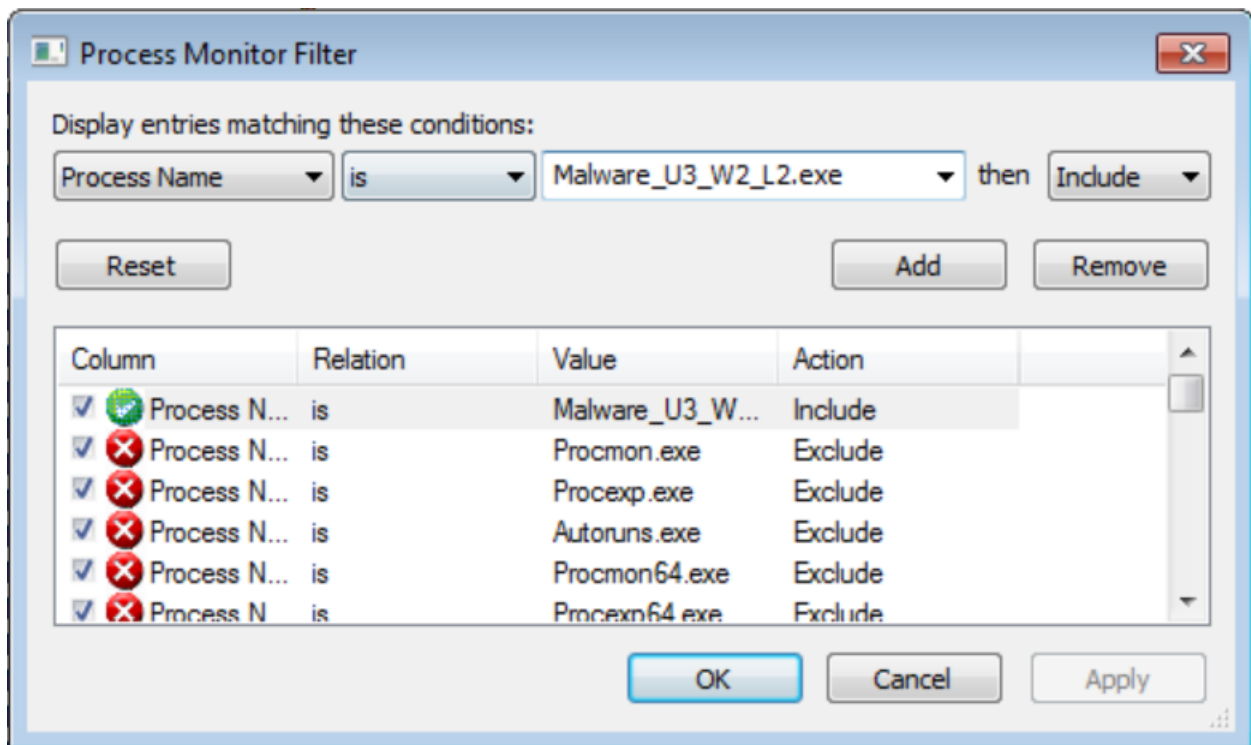
- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon) .
- Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor .
- Modifiche del registro dopo il malware (le differenze).
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

### Procmon:

Time	Process Name	PID	Operation	Path	Result	Detail
15:52...	SearchIndexer.exe	2064	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2 088 960, ...
15:52...	SearchIndexer.exe	2064	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2 056 192, ...
15:52...	SearchIndexer.exe	2064	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2 035 712, ...
15:52...	SearchIndexer.exe	2064	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2 027 520, ...
15:52...	SearchIndexer.exe	2064	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 1 757 184, ...
15:52...	SearchIndexer.exe	2064	File System Control C:		SUCCESS	Control: FSCTL_R...
15:52...	SearchIndexer.exe	2064	File System Control C:		SUCCESS	Control: FSCTL_R...
15:52...	evchost.exe	776	ReadFile	C:\Windows\System32\dhcpcore6.dll	SUCCESS	Offset: 200 704, Le...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: R...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: R...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NAME NOT FOUND	Desired Access: Q...
15:52...	Explorer.EXE	1748	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: Q...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Type: REG_SZ, Le...
15:52...	Explorer.EXE	1748	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NAME NOT FOUND	Length: 144
15:52...	Explorer.EXE	1748	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: R...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: R...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	NAME NOT FOUND	Desired Access: Q...
15:52...	Explorer.EXE	1748	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Query: HandleTag...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Desired Access: Q...
15:52...	Explorer.EXE	1748	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	SUCCESS	Type: REG_SZ, Le...

Showing 18.254 of 97.615 events (18%)      Backed by virtual memory

### Procmon (filter):



Il malware è dunque un **keylogger**, in grado di generare un file di testo e salvare al suo interno i tasti digitati dall'utente.

RegShot:

