ESERCIZIO W21D1

Nell'esercizio andremo ad analizzare un malware contenuto nella macchina virtuale Windows 7. Seguiamo la traccia presentata di seguito:

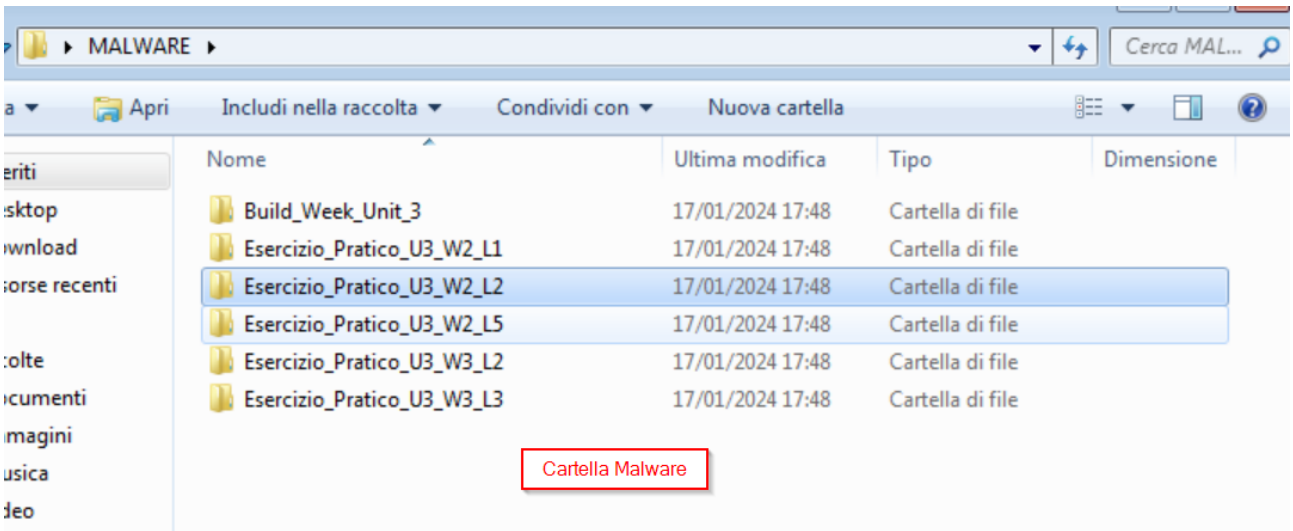
Nella lezione teorica, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

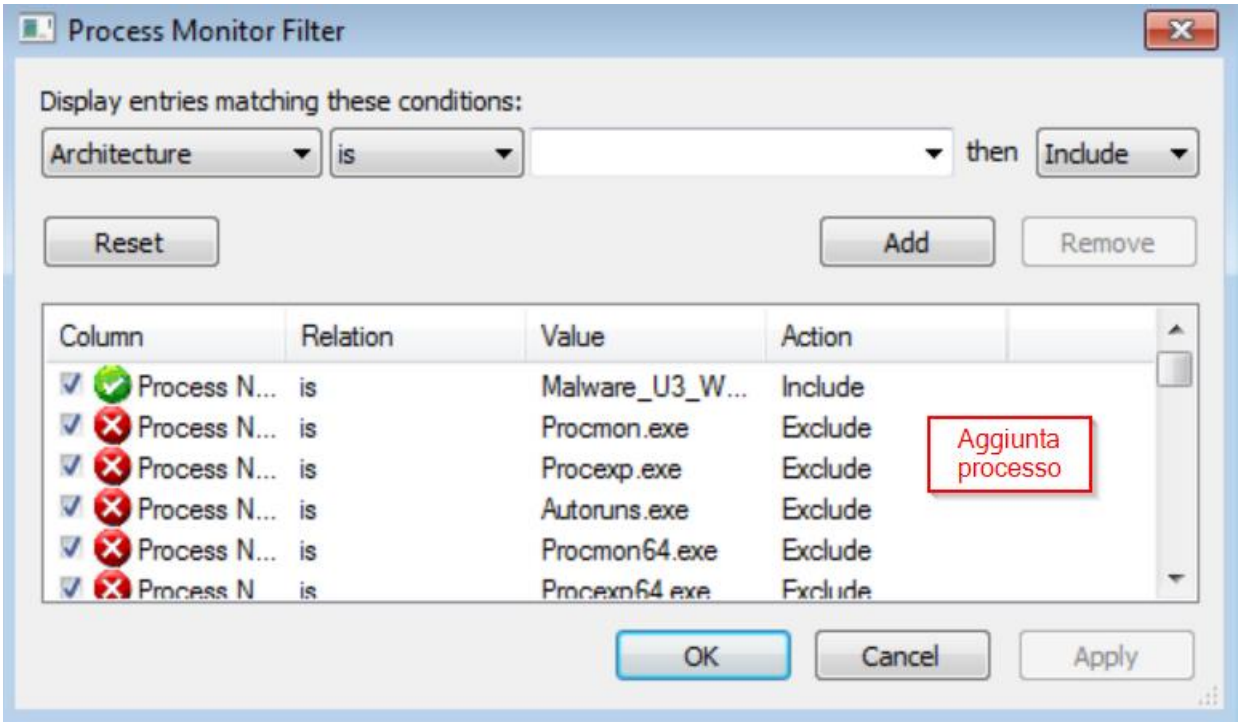
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- 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).

Preparazione Procmon e cartella

Eseguiamo l'eseguibile all'interno della cartella e teniamoci pronti con procmon.

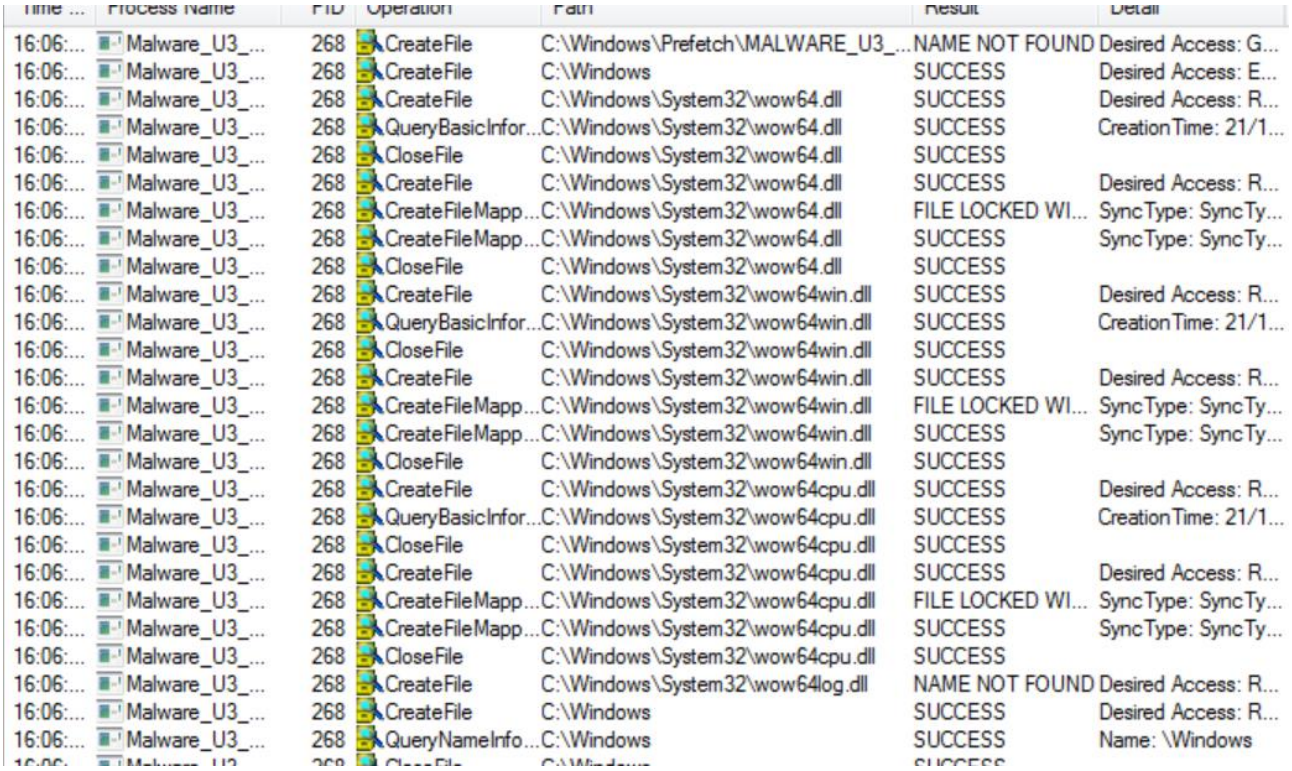




Informazioni raccolte – Registri

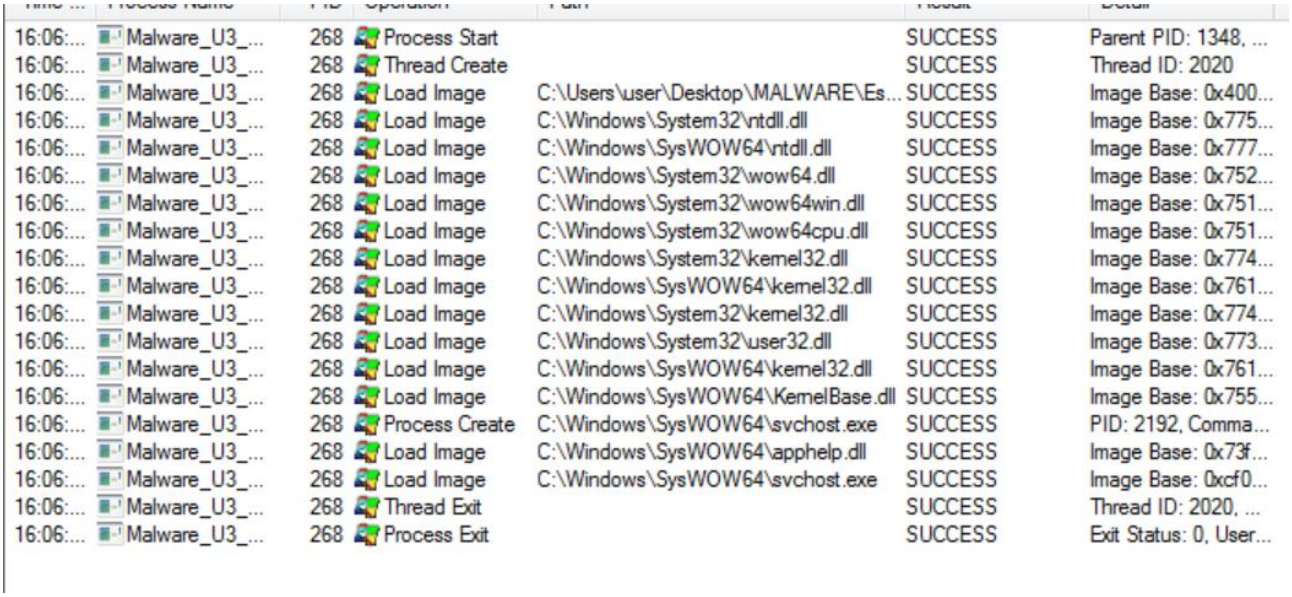
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
16:06:...	Malware_U3_...	268	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
16:06:...	Malware_U3_...	268	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	REPARSE	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
16:06:...	Malware_U3_...	268	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 548
16:06:...	Malware_U3_...	268	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
16:06:...	Malware_U3_...	268	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
16:06:...	Malware_U3_...	268	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...

Informazioni raccolte – File System



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND	Desired Access: G...
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/1...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/1...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/1...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
16:06:...	Malware_U3_...	268	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
16:06:...	Malware_U3_...	268	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
16:06:...	Malware_U3_...	268	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows

Informazioni raccolte – Processi e Threads



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:06:...	Malware_U3_...	268	Process Start		SUCCESS	Parent PID: 1348, ...
16:06:...	Malware_U3_...	268	Thread Create		SUCCESS	Thread ID: 2020
16:06:...	Malware_U3_...	268	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x775...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x777...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x752...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x751...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x751...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x774...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x761...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x774...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x773...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x761...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x755...
16:06:...	Malware_U3_...	268	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2192, Comma...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73f...
16:06:...	Malware_U3_...	268	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0xcf0...
16:06:...	Malware_U3_...	268	Thread Exit		SUCCESS	Thread ID: 2020, ...
16:06:...	Malware_U3_...	268	Process Exit		SUCCESS	Exit Status: 0, User...