

CONSEGNA SETTIMANA 10 LEZIONE 2

Analisi dinamica basica

L'analisi dinamica di base si svolge durante l'attacco di un determinato malware. Nel nostro caso abbiamo infettato un sistema windows 7 in un ambiente isolato.

Ci è stato richiesto di completare le seguenti tasks:

- Identificare eventuali azioni del malware sul **file system** utilizzando ProcessMonitor
- Identificare eventuali azioni del malware su **processi e thread** utilizzando ProcessMonitor
- Identificare eventuali modifiche del **registro di sistema** dopo il malware

Prima di poter procedere occorre impostare la macchina virtuale in modo tale che il software dannoso non sia in grado di propagarsi sulla macchina madre.

Per fare questo abbiamo:

- Impostato una rete interna (a differenza della precedente bridge)
- Disattivato i controlli delle porte USB
- Salvato uno snapshot della macchina prima che venisse infettata

A questo punto possiamo procedere con l'avvio di due software che ci serviranno per monitorare il comportamento del malware: **Regshot** e **Process monitor**.

Salviamo una prima cattura tramite regshot e avviamo il malware. Una volta avviato salviamo una seconda cattura per poi compararla alla prima effettuata.

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 14:36:50 , 2024/2/13 14:37:17
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 1
-----
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
-----
Values added: 2
-----
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFE5CD-ACE2-4F4E-9178-9926E41749EA}\Count\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\user\Desktop\MALWARE\Esercizio_P
-----
Values modified: 5
-----
```

Possiamo notare che sono stati aggiunti dei valori al registro di sistema proprio dal file infetto.

Spostiamoci ora sul software Process monitor, che abbiamo avviato prima dell'esecuzione del malware. Tra le varie attività in esecuzione compariranno proprio quelle effettuate dal malware.

15:38:21.6114567	Malware_U3...	1196	Load Image	C:\Windows\SysWOW64\psapi.dll	SUCCESS	Image Base: 0x74f50000, Image Size: 0x5000
15:38:21.6115389	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09
15:38:21.6115487	Malware_U3...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6115541	Malware_U3...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6115788	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Nc
15:38:21.6115867	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6115905	Malware_U3...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6115984	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09
15:38:21.6116123	Malware_U3...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Nc
15:38:21.6116473	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6116520	Malware_U3...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6116551	Malware_U3...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09
15:38:21.6116737	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Nc
15:38:21.6116786	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6116814	Malware_U3...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6116870	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09
15:38:21.6117045	Malware_U3...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Nc
15:38:21.6117399	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6117442	Malware_U3...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6117474	Malware_U3...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09
15:38:21.6117690	Malware_U3...	1196	CreateFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Synchronous IO Nc
15:38:21.6117740	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: AllocationSize: 532,480, EndOfFile: 530,432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21.6117766	Malware_U3...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21.6117821	Malware_U3...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Share CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/2010 04:24:09

15:38:21.6154926	conhost.exe	Thread Exit	SUCCESS	Thread ID: 1760, User Time: 0.0000000, Kernel Time: 0.0156250
15:38:21.6158390	conhost.exe	QueryNameInfo...C:\Windows\System32\user32.dll	SUCCESS	Name: \Windows\System32\user32.dll
15:38:21.6158539	conhost.exe	QueryNameInfo...C:\Windows\System32\kernel32.dll	SUCCESS	Name: \Windows\System32\kernel32.dll
15:38:21.6158609	conhost.exe	QueryNameInfo...C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\System32\ntdll.dll
15:38:21.6158669	conhost.exe	QueryNameInfo...C:\Windows\System32\conhost.exe	SUCCESS	Name: \Windows\System32\conhost.exe
15:38:21.6158737	conhost.exe	QueryNameInfo...C:\Windows\System32\advapi.dll	SUCCESS	Name: \Windows\System32\advapi.dll
15:38:21.6158806	conhost.exe	QueryNameInfo...C:\Windows\System32\user32.dll	SUCCESS	Name: \Windows\System32\user32.dll
15:38:21.6158874	conhost.exe	QueryNameInfo...C:\Windows\System32\ole32.dll	SUCCESS	Name: \Windows\System32\ole32.dll
15:38:21.6158944	conhost.exe	QueryNameInfo...C:\Windows\System32\kernelbase.dll	SUCCESS	Name: \Windows\System32\kernelbase.dll
15:38:21.6159012	conhost.exe	QueryNameInfo...C:\Windows\System32\vpct4.dll	SUCCESS	Name: \Windows\System32\vpct4.dll
15:38:21.6159083	conhost.exe	QueryNameInfo...C:\Windows\System32\msctf.dll	SUCCESS	Name: \Windows\System32\msctf.dll
15:38:21.6159151	conhost.exe	QueryNameInfo...C:\Windows\System32\lpk.dll	SUCCESS	Name: \Windows\System32\lpk.dll
15:38:21.6159211	conhost.exe	QueryNameInfo...C:\Windows\System32\advapi32.dll	SUCCESS	Name: \Windows\System32\advapi32.dll
15:38:21.6159297	conhost.exe	QueryNameInfo...C:\Windows\System32\msvcrt.dll	SUCCESS	Name: \Windows\System32\msvcrt.dll
15:38:21.6159360	conhost.exe	QueryNameInfo...C:\Windows\System32\oleaut32.dll	SUCCESS	Name: \Windows\System32\oleaut32.dll
15:38:21.6159422	conhost.exe	QueryNameInfo...C:\Windows\System32\imm32.dll	SUCCESS	Name: \Windows\System32\imm32.dll
15:38:21.6159483	conhost.exe	QueryNameInfo...C:\Windows\System32\usp10.dll	SUCCESS	Name: \Windows\System32\usp10.dll
15:38:21.6159547	conhost.exe	QueryNameInfo...C:\Windows\System32\shlwapi.dll	SUCCESS	Name: \Windows\System32\shlwapi.dll
15:38:21.6159618	conhost.exe	QueryNameInfo...C:\Windows\System32\ole32.dll	SUCCESS	Name: \Windows\System32\ole32.dll
15:38:21.6159689	conhost.exe	QueryNameInfo...C:\Windows\System32\gdi32.dll	SUCCESS	Name: \Windows\System32\gdi32.dll
15:38:21.6159751	conhost.exe	QueryNameInfo...C:\Windows\System32\sechost.dll	SUCCESS	Name: \Windows\System32\sechost.dll
15:38:21.6159814	conhost.exe	QueryNameInfo...C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\System32\apisetschema.dll
15:38:21.6159919	conhost.exe	Process Exit	SUCCESS	Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1.220.60
15:38:21.6159971	conhost.exe	RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\...	SUCCESS	
15:38:21.6160007	conhost.exe	CloseFile C:\Windows\System32	SUCCESS	
15:38:21.6160291	conhost.exe	RegCloseKey HKLM	SUCCESS	
15:38:21.6160317	conhost.exe	RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	
15:38:21.6160342	conhost.exe	RegCloseKey HKLM\System\CurrentControlSet\Control\SESSION MANAG...	SUCCESS	
15:38:21.6160455	conhost.exe	RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\Locale	SUCCESS	
15:38:21.6160479	conhost.exe	RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\Locale\Alternat...	SUCCESS	
15:38:21.6160503	conhost.exe	RegCloseKey HKLM\System\CurrentControlSet\Control\Nls\Language Grou...	SUCCESS	
15:38:21.61642729	Malware_U3_...	RegOpenKey HKLM\Software\Microsoft\SQMClient\Windows\DisabledPro...	SUCCESS	Desired Access: Read
15:38:21.61642850	Malware_U3_...	RegSetInfoKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
15:38:21.61642890	Malware_U3_...	RegQueryValue HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	NAME NOT FOUND	Length: 24
15:38:21.61642936	Malware_U3_...	RegCloseKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	
15:38:21.61642988	Malware_U3_...	RegOpenKey HKLM\Software\Microsoft\SQMClient\Windows\DisabledSes...	SUCCESS	Desired Access: Read
15:38:21.61643036	Malware_U3_...	RegSetInfoKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
15:38:21.61643071	Malware_U3_...	RegQueryValue HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	NAME NOT FOUND	Length: 24
15:38:21.61643108	Malware_U3_...	RegCloseKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	
15:38:21.61643144	Malware_U3_...	RegOpenKey HKLM\Software\Microsoft\SQMClient\Windows\DisabledSes...	SUCCESS	Desired Access: Read
15:38:21.61643177	Malware_U3_...	RegSetInfoKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
15:38:21.61643204	Malware_U3_...	RegQueryValue HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	NAME NOT FOUND	Length: 24
15:38:21.61643234	Malware_U3_...	RegCloseKey HKLM\SOFTWARE\Microsoft\SQMClient\Windows\Disabled...	SUCCESS	
15:38:21.61644571	Malware_U3_...	CreateFile C:\Windows\system	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch...
15:38:21.61644651	Malware_U3_...	QueryDirectory C:\Windows\system\wing.dll	NO SUCH FILE	Filter: wing.dll
15:38:21.61644709	Malware_U3_...	CloseFile C:\Windows\system	SUCCESS	
15:38:21.61644921	Malware_U3_...	CreateFile C:\Windows\SysWOW64	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch...
15:38:21.61644974	Malware_U3_...	QueryDirectory C:\Windows\SysWOW64\wing.dll	NO SUCH FILE	Filter: wing.dll
15:38:21.61645034	Malware_U3_...	CloseFile C:\Windows\SysWOW64	SUCCESS	
15:38:21.61645223	Malware_U3_...	CreateFile C:\Windows\system	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch...
15:38:21.61645267	Malware_U3_...	QueryDirectory C:\Windows\system\wing32.dll	NO SUCH FILE	Filter: wing32.dll
15:38:21.61645305	Malware_U3_...	CloseFile C:\Windows\system	SUCCESS	
15:38:21.61645486	Malware_U3_...	CreateFile C:\Windows\SysWOW64	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch...
15:38:21.61645527	Malware_U3_...	QueryDirectory C:\Windows\SysWOW64\wing32.dll	NO SUCH FILE	Filter: wing32.dll
15:38:21.61645571	Malware_U3_...	CloseFile C:\Windows\SysWOW64	SUCCESS	
15:38:21.61646060	Malware_U3_...	RegOpenKey HKLM\Software\Wow6432Node\Microsoft\Windows NT\Cur...	SUCCESS	Desired Access: Read
15:38:21.61646124	Malware_U3_...	RegSetInfoKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
15:38:21.61646154	Malware_U3_...	RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\...	NAME NOT FOUND	Length: 20
15:38:21.61646197	Malware_U3_...	RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\...	SUCCESS	
15:38:21.61646435	Malware_U3_...	Thread Exit	SUCCESS	Thread ID: 1564, User Time: 0.0156250, Kernel Time: 0.0156250
15:38:21.61647542	Malware_U3_...	QueryNameInfo...C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\System32\apisetschema.dll
15:38:21.61647637	Malware_U3_...	QueryNameInfo...C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe

Nome del file .exe	PID	Azione eseguita	PATH
--------------------	-----	-----------------	------

Da queste catture possiamo notare il comportamento del malware e le azioni che ha compiuto, in particolar modo notiamo che sono stati creati dei file all'interno del path **C:\Windows\...** e che il malware ha avuto accesso al registro di sistema, modificando una moltitudine di valori.

Possiamo notare infine un processo nominato **conhost.exe** che, da una breve ricerca, potrebbe essere legato al malware data la sua posizione anomala del path.

Questo processo in particolar modo ha avuto accesso a molteplici librerie di sistema, come **kernel32.dll**, **advapi32.dll**, **user32.dll** e **sechost.dll**

Ci viene infine richiesto di determinare la tipologia di malware.

Data la sua possibile natura e la presenza del processo conhost.exe, in questo caso ritenuto malevolo, ritengo che il malware sia un particolare tipo chiamato **Trojan**.

Un trojan ha la capacità di mascherarsi e immedesimarsi agli occhi di un utente, come un normale processo, spesso rendendo difficile il trovarlo.