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

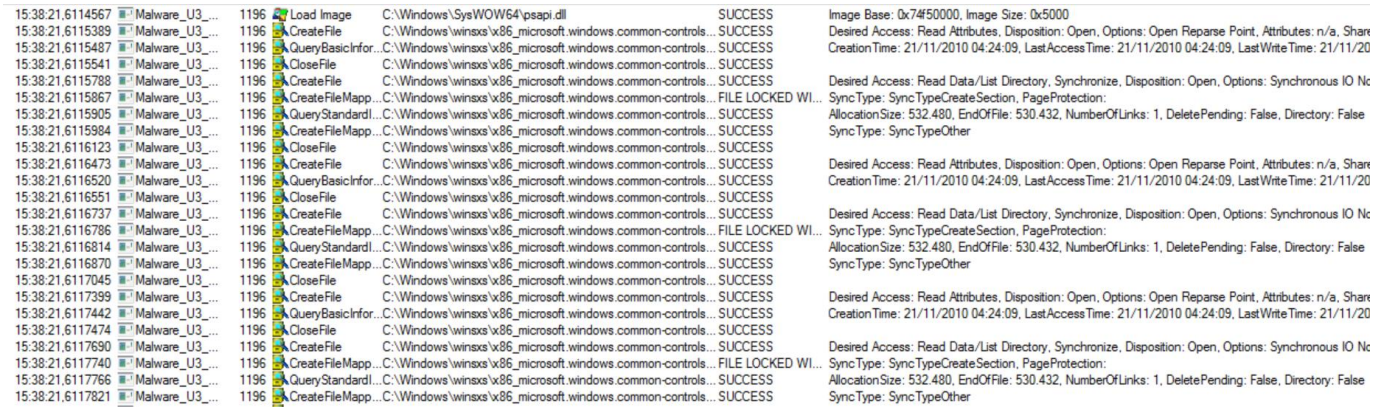
A questo punto possiamo procedere con l'avvio di due software che ci serviranno per monitorare il comportamento del malware: ***Regshot*** e ***Process monitor***.

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

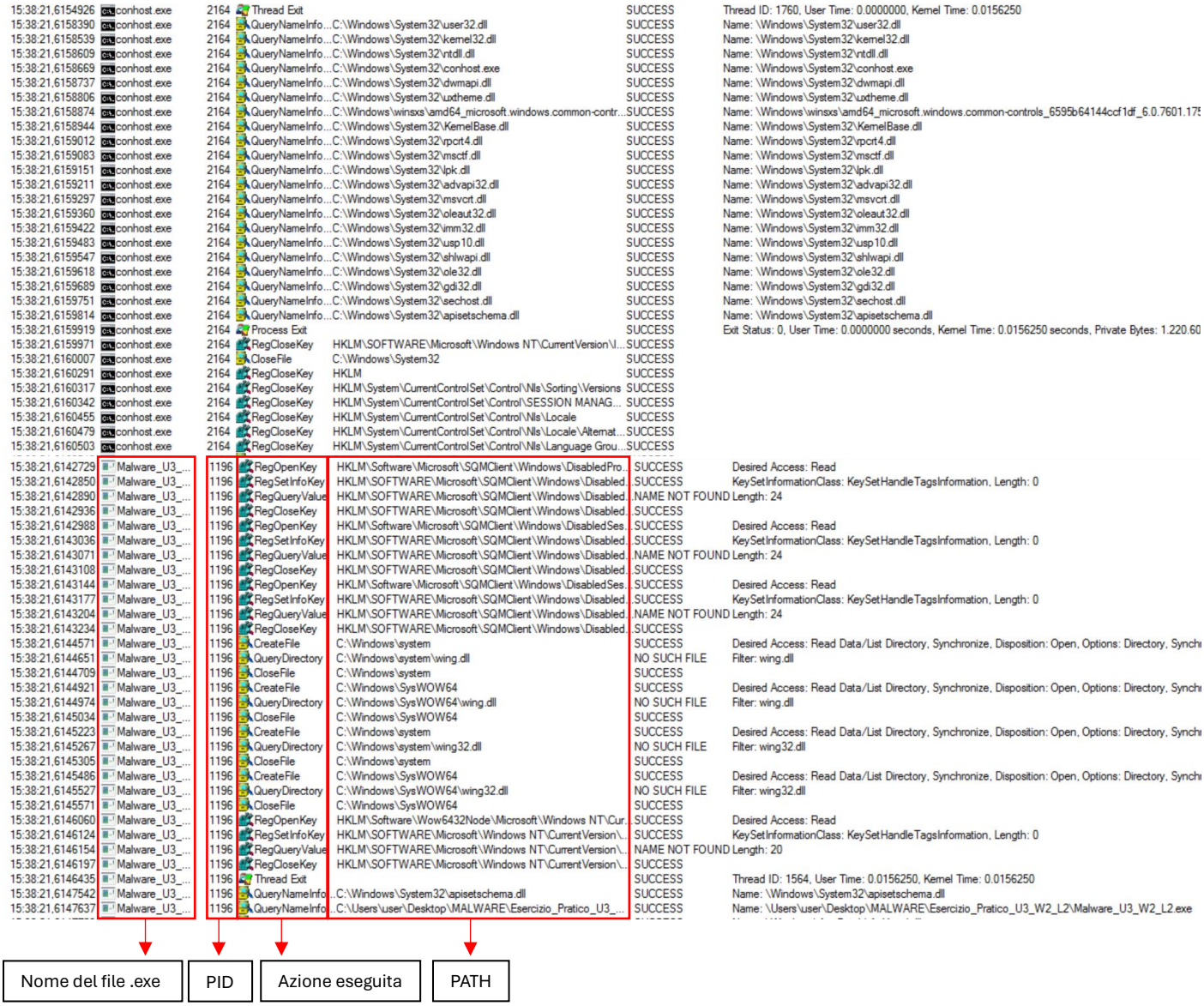
```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 14:36:50   ,  2024/2/13 14:37:17
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
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\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\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
15:38:21,6115487	Malware_U3_...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/20
15:38:21,6115541	Malware_U3_...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	
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 No
15:38:21,6115867	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:38:21,6115905	Malware_U3_...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	AllocationSize: 532.480, EndOfFile: 530.432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21,6115984	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21,6116123	Malware_U3_...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	
15:38:21,6116473	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
15:38:21,6116520	Malware_U3_...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/20
15:38:21,6116551	Malware_U3_...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	
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 No
15:38:21,6116786	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:38:21,6116814	Malware_U3_...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	AllocationSize: 532.480, EndOfFile: 530.432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21,6116870	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther
15:38:21,6117045	Malware_U3_...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	
15:38:21,6117399	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
15:38:21,6117442	Malware_U3_...	1196	QueryBasicInfor...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	CreationTime: 21/11/2010 04:24:09, LastAccessTime: 21/11/2010 04:24:09, LastWriteTime: 21/11/20
15:38:21,6117474	Malware_U3_...	1196	CloseFile	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	
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 No
15:38:21,6117740	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:38:21,6117766	Malware_U3_...	1196	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	AllocationSize: 532.480, EndOfFile: 530.432, NumberOfLinks: 1, DeletePending: False, Directory: False
15:38:21,6117821	Malware_U3_...	1196	CreateFileMapp...	C:\Windows\winsxs\x86_microsoft.windows.common-controls...	SUCCESS	SyncType: SyncTypeOther



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.