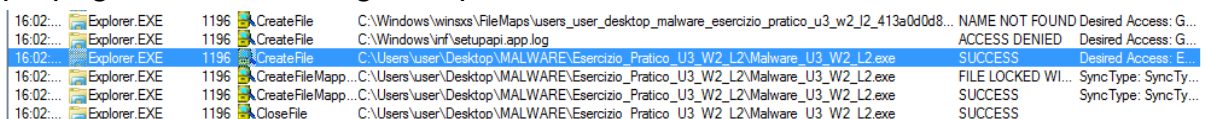


Nell'esercizio di oggi eseguiremo l'analisi dinamica di un malware. Nell'analisi dinamica un malware viene eseguito in un ambiente virtuale protetto per evitare danni e poter osservare il suo comportamento. Per monitorare il malware useremo Process Monitor e regshot.

Process monitor è un software per windows usato per monitorare le attività del sistema operativo.

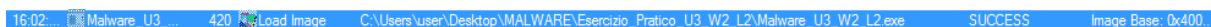
Regshot è un software che permette di scattare due istantanee delle chiavi di registro in momenti diversi e paragonarle. Alcuni malware riescono a cambiare la configurazione di un sistema operativo apportando modifiche alle chiavi di registro. In questo modo possono far sì di essere avviati automaticamente all'avvio del sistema. Per questo è molto importante sapere se e come sono state modificate le chiavi di registro, così da capire il comportamento di un malware.

Dopo aver messo in sicurezza la macchina per evitare che il malware possa propagarsi, avviamo regshot, process monitor e il malware.



16:02:...	Explorer.EXE	1196	CreateFile	C:\Windows\winsxs\FileMaps\users_user_desktop_malware_esercizio_pratico_u3_w2_l2_413a0d0d8...	NAME NOT FOUND	Desired Access: G...
16:02:...	Explorer.EXE	1196	CreateFile	C:\Windows\inf\setupapi.app.log	ACCESS DENIED	Desired Access: G...
16:02:...	Explorer.EXE	1196	CreateFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: E...
16:02:...	Explorer.EXE	1196	CreateFileMapping...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	FILE LOCKED WI...	Sync Type: SyncTy...
16:02:...	Explorer.EXE	1196	CreateFileMapping...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	SyncType: SyncTy...
16:02:...	Explorer.EXE	1196	CloseFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	

Come possiamo vedere dall'immagine sopra il malware sta creando un file tramite la funzione "Create File", probabilmente sta cercando di replicarsi. Questi sono eventi del file system con i quali il malware può controllare le interazioni con il sistema.



16:02:...	Malware_U3...	420	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400...
-----------	---------------	-----	------------	---	---------	----------------------

Invece nell'immagine sopra possiamo notare che sta cercando di caricare un eseguibile o una libreria tramite la funzione "Load Image".

Regshot non ha registrato variazioni nelle chiavi di registro come possiamo vedere dalla figura sotto.

Regshot 1.9.0 x64 Unicode  
Comments:  
Datetime: 2024/2/13 15:27:11 , 2024/2/13 15:28:02  
Computer: USER-PC , USER-PC  
Username: user , user

```
Keys added: 3
```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain {366E06F2-80BB-40A2-A138-F5D07D1E2BA3}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks {366E06F2-80BB-40A2-A138-F5D07D1E2BA3}
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree {5B3DC498-E8F8-4D96-BFE5-825C383BCE0B}
```

```
values added: 7
```

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{366E06F2-80BB-40A2-A138-F5D07D1E2BA3}\Path: {583DE498-E8F8-4D96-BFE5-825C8BCEB0C}\Id: {366E06F2-80BB-40A2-A138-F5D07D1E2BA3}\Hash: E4 E8 8C DD 35 OF 75 FE
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{366E06F2-80BB-40A2-A138-F5D07D1E2BA3}\Triggers: 15 00 00 00 00 00 00
00 00 00 05 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{366E06F2-80BB-40A2-A138-F5D07D1E2BA3}\DynamicInfo: 03 00 00 00 CF 16
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{583DE498-E8F8-4D96-BFE5-825C8BCEB0C}\Id: {366E06F2-80BB-40A2-A138-F5D07D1E2BA3}\Index: 0000000000
HKU\S-1-5-21-3771313050-58705377-3452663001-1001\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\user\Desktop\MALWARE
```

```
values modified: 10
```

[illegible]

Dalle informazioni raccolte possiamo ipotizzare che il malware sia un virus o un trojan.