

510-L2

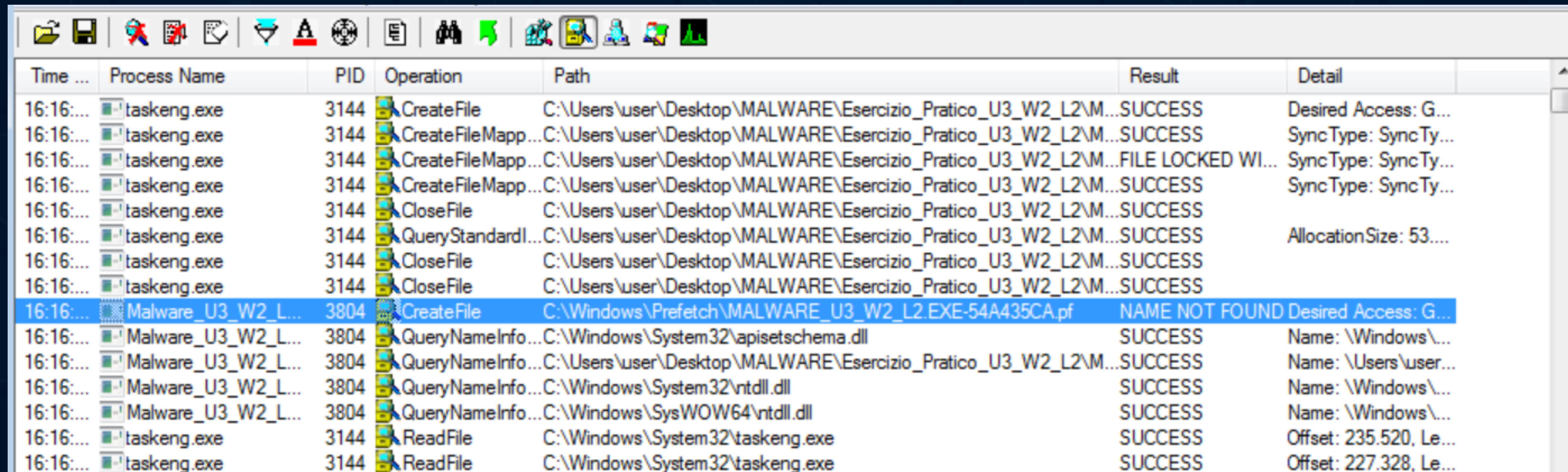


TRACCIA:

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 PROCESS MONITOR (PROC MON):
- 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

Attraverso il software Process Monitor (procmon) possiamo analizzare svariate situazioni, tra cui processi attivi, threads, attività di rete e l'accesso ai file. Come possiamo notare a seguito dell'avvio del malware esso andrà a creare file e chiamerà la dll ntdll, la dll injection è una tecnica di lancio malware che utilizza i processi windows per camuffarsi.



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:16:...	taskeng.exe	3144	CreateFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	Desired Access: G...
16:16:...	taskeng.exe	3144	CreateFileMapp...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	SyncType: SyncTy...
16:16:...	taskeng.exe	3144	CreateFileMapp...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	FILE LOCKED WI...	SyncType: SyncTy...
16:16:...	taskeng.exe	3144	CreateFileMapp...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	SyncType: SyncTy...
16:16:...	taskeng.exe	3144	CloseFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	
16:16:...	taskeng.exe	3144	QueryStandardI...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	AllocationSize: 53...
16:16:...	taskeng.exe	3144	CloseFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	
16:16:...	taskeng.exe	3144	CloseFile	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	
16:16:...	Malware_U3_W2_L...	3804	CreateFile	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: G...
16:16:...	Malware_U3_W2_L...	3804	QueryNameInfo...	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\...
16:16:...	Malware_U3_W2_L...	3804	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	Name: \Users\user...
16:16:...	Malware_U3_W2_L...	3804	QueryNameInfo...	C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\...
16:16:...	Malware_U3_W2_L...	3804	QueryNameInfo...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Name: \Windows\...
16:16:...	taskeng.exe	3144	ReadFile	C:\Windows\System32\taskeng.exe	SUCCESS	Offset: 235.520, Le...
16:16:...	taskeng.exe	3144	ReadFile	C:\Windows\System32\taskeng.exe	SUCCESS	Offset: 227.328, Le...

Analizzando i processi e i threads presenti possiamo ipotizzare che il malware stia utilizzando il processo “consent.exe” per fare una scalata dei privilegi, andando a eseguire operazioni senza la necessità della nostra autorizzazione.

16:16:...	Malware_U3_W2_L...	3804	Process Start	
16:16:...	Malware_U3_W2_L...	3804	Thread Create	
16:16:...	taskeng.exe	3144	Load Image	C:\Windows\System32\apphelp.dll
16:16:...	Malware_U3_W2_L...	3804	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M.
16:16:...	Malware_U3_W2_L...	3804	Load Image	C:\Windows\System32\ntdll.dll
16:16:...	Malware_U3_W2_L...	3804	Load Image	C:\Windows\SysWOW64\ntdll.dll
16:16:...	Malware_U3_W2_L...	3804	Thread Exit	
16:16:...	Malware_U3_W2_L...	3804	Process Exit	
16:16:...	taskeng.exe	3144	Load Image	C:\Windows\System32\mpr.dll
16:16:...	svchost.exe	852	Process Create	C:\Windows\system32\consent.exe
16:16:...	consent.exe	2232	Process Start	
16:16:...	consent.exe	2232	Thread Create	
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\consent.exe
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\ntdll.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\kernel32.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\KernelBase.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\advapi32.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\msvcrt.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\sechost.dll
16:16:...	consent.exe	2232	Load Image	C:\Windows\System32\rpcrt4.dll

Grazie al software regshot possiamo andare a creare un'istanza prima di avviare un malware e una a seguito di ciò, andando così ad analizzare le differenze e quindi le modifiche apportate nel registro dal malware, in quanto il programam ci restituirà un log contenente le differenze tra le due istanze.

Keys added: 17


```

HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hivu
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\windows\CurrentVersion\Explorer\FileExts\.hivu
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\windows\CurrentVersion\Explorer\FileExts\.hivu\openwithList
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\windows\CurrentVersion\Explorer\RecentDocs\.hivu
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\windows\NT\CurrentVersion\AppCompatFlags\Layers
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\18\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\18\ComDlg\{5C4F28B5-F869-4
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg\{FBB3477
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg\{FBB3477
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\18\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\18\ComDlg\{5C4F28B5-F869-4E84-8E60-
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B

```

values added: 47

[illegible]



A seguito di questa analisi dinamica basica, posso ipotizzare che il malware in questione sia un Rootkit Trojan, il quale si camuffa tra i processi standard di windows, andando a eseguire una scalata dei privilegi utilizzando consent.exe e eseguendo azioni dannose sul sistema.