

ANALISI DINAMICA BASICA

S10L2

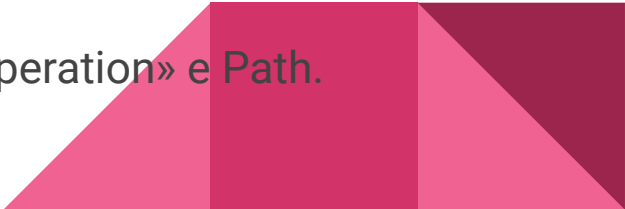
INDICE

- TRACCIA
- AZIONI DEL MALWARE



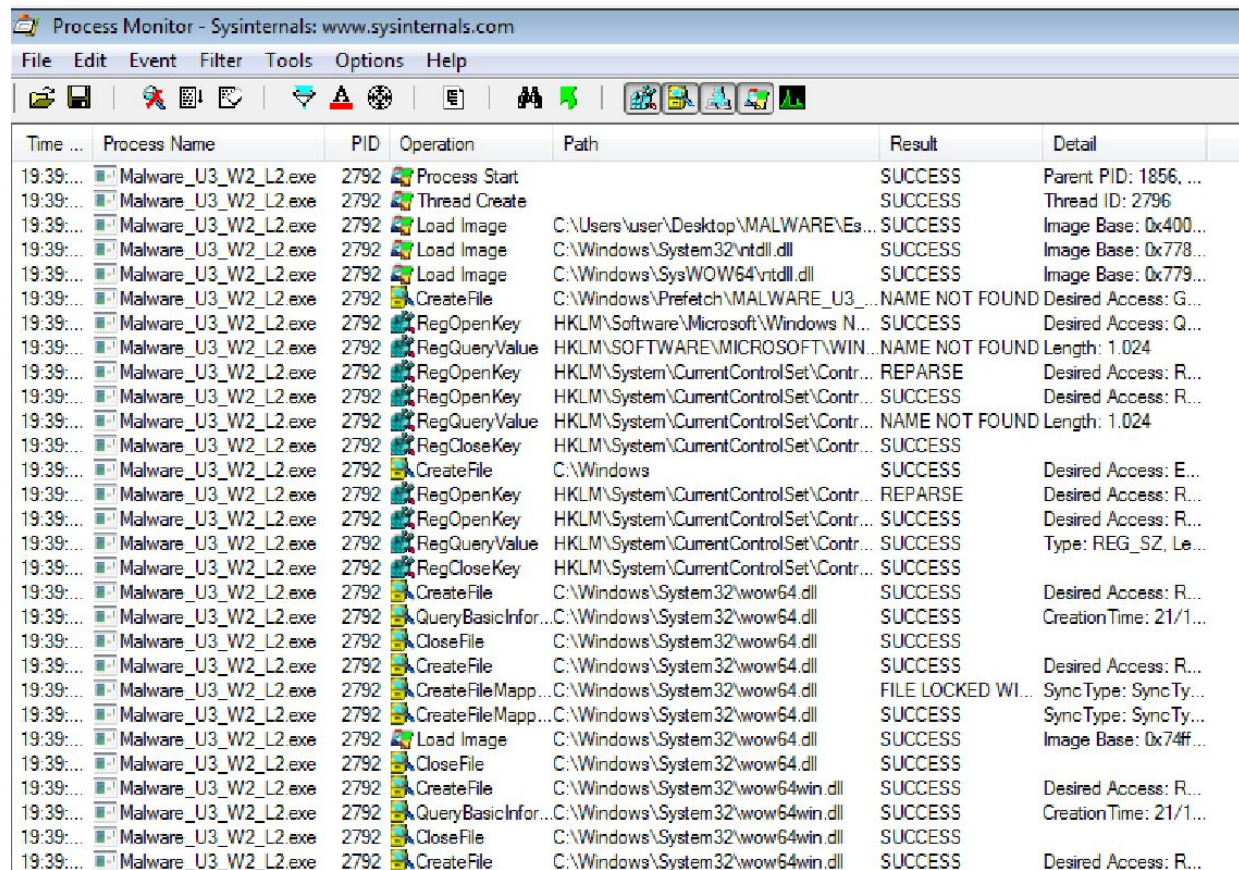
TRACCIA

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 ProcessMonitor (procmon)
 - 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.
- 

Azioni del malware

Come possiamo vedere appena avviamo il malware prova a creare dei file ma senza successo.



Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
19:39:...	Malware_U3_W2_L2.exe	2792	Process Start		SUCCESS	Parent PID: 1856, ...
19:39:...	Malware_U3_W2_L2.exe	2792	Thread Create		SUCCESS	Thread ID: 2796
19:39:...	Malware_U3_W2_L2.exe	2792	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
19:39:...	Malware_U3_W2_L2.exe	2792	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x778...
19:39:...	Malware_U3_W2_L2.exe	2792	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND	Desired Access: G...
19:39:...	Malware_U3_W2_L2.exe	2792	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
19:39:...	Malware_U3_W2_L2.exe	2792	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WIN...	NAME NOT FOUND	Length: 1.024
19:39:...	Malware_U3_W2_L2.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
19:39:...	Malware_U3_W2_L2.exe	2792	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
19:39:...	Malware_U3_W2_L2.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
19:39:...	Malware_U3_W2_L2.exe	2792	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/1...
19:39:...	Malware_U3_W2_L2.exe	2792	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
19:39:...	Malware_U3_W2_L2.exe	2792	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74ff...
19:39:...	Malware_U3_W2_L2.exe	2792	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
19:39:...	Malware_U3_W2_L2.exe	2792	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/1...
19:39:...	Malware_U3_W2_L2.exe	2792	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
19:39:...	Malware_U3_W2_L2.exe	2792	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...



Grazie