

ANALISI DINAMICA BASICA

Indice

- **Traccia**
- **Configurazione VM**
- **Analisi dinamica e Process Monitor**
- **Analisi**
- **Azioni rilevate su file system del malware**
- **Azioni rilevate su processi e thread del malware**
- **Conclusioni**

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 (PROCMON)**
- **IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SU PROCESSI E THREAD UTILIZZANDO PROCESS MONITOR**
- **MODIFICHE DEL REGISTRO DOPO IL MALWARE(LE DIFFERENZE)**
- **PROVARE A PROFILARE IL MALWARE IN BASE ALLA CORRELAZIONE TRA «OPERATION» E PATH**

Configurazione VM

Tra le buone pratiche da adottare per configurare un ambiente sicuro troviamo:

CONFIGURAZIONE SCHEDA DI RETE

L'ambiente di test non deve avere accesso diretto ad internet, né alle altre macchine sulla rete.

Dunque la configurazione ideale è:

- Eliminare le interfacce di rete durante l'analisi statica;
- abilitare un'interfaccia di rete interna

DISPOSITIVI USB

Quando un dispositivo USB viene collegato alla macchina fisica, esso può essere riconosciuto anche dall'ambiente di test. Al fine di evitare questo comportamento, è buona pratica non abilitare o disabilitare il controller USB.

CARTELLE CONDIVISE

Potrebbero essere utilizzate dal malware per propagarsi al di fuori del laboratorio causando danni alla vostra macchina e alle macchine sulla vostra rete domestica. Di conseguenza, è consigliato non condividere cartelle tra host e guest.

CREARE ISTANTANEE

Analizzando i malware spesso capita di arrecare danno all'ambiente di test; una buona pratica è creare delle **istantanee** della macchina virtuale nel suo stato iniziale, così da ripristinarlo qualora ce ne fosse bisogno.

Analisi dinamica e Process Monitor

L'**analisi dinamica** comprende tutte quelle attività di analisi che presuppongono l'esecuzione del malware in un ambiente dedicato.

L'analisi dinamica basica è generalmente effettuata dopo l'analisi statica basica, per sopperire ai limiti dell'analisi statica ed avere una maggiore visibilità sulle attività e il comportamento del malware in esame.

L'analisi dinamica permette di osservare e studiare le vere funzionalità di un malware in esecuzione su un sistema

ProcessMonitor, o «procmon», è un tool avanzato per Windows che permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo.

Analisi

Per avviare l'analisi delle azioni del malware usiamo procmoc. Dunque, dopo aver avviato Process Monitor eseguiamo il file “Esercizio_Pratico_U3_W2_L2”, ed effettuiamo una cattura mettendo come filtro proprio il nome del nostro file, così da visualizzare solo i processi di nostro interesse.

11:57:...	Malware_U3_W2_L2.exe	2100	Process Start	SUCCESS	Parent PID: 900, C...
11:57:...	Malware_U3_W2_L2.exe	2100	Thread Create	SUCCESS	Thread ID: 1156
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS Image Base: 0x400...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS Image Base: 0x770...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS Image Base: 0x772...
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\Prefetch\MALWARE_U3_...	NAME NOT FOUND Desired Access: G...
11:57:...	Malware_U3_W2_L2.exe	2100	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS Desired Access: Q...
11:57:...	Malware_U3_W2_L2.exe	2100	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WIN...	NAME NOT FOUND Length: 1.024
11:57:...	Malware_U3_W2_L2.exe	2100	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 1.024
11:57:...	Malware_U3_W2_L2.exe	2100	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows	SUCCESS Desired Access: E...
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS CreationTime: 21/1...
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI... SyncType: SyncTy...
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS SyncType: SyncTy...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image	C:\Windows\System32\wow64.dll	SUCCESS Image Base: 0x73f...
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS CreationTime: 21/1...
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...

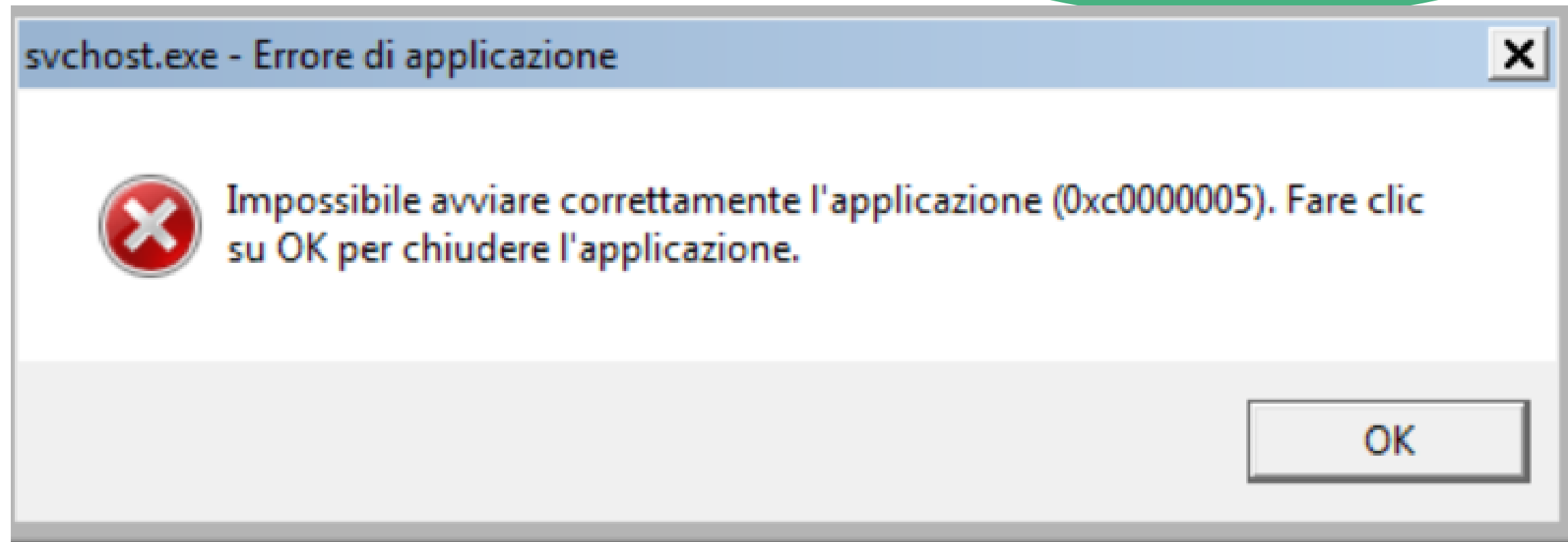
Azioni rilevate su file system del malware

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: winnsi.dll, 1: winr...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: wlanmsm.dll, 1: ...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: wmsgapi.dll, 1: ...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: wshcon.dll, 1: w...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	SUCCESS	0: xcopy.exe, 1: XI...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryDirectory	C:\Windows\SysWOW64	NO MORE FILES	
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\SysWOW64	SUCCESS	
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Desired Access: G...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryStandardI...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	AllocationSize: 24....
11:57:...	Malware_U3_W2_L2.exe	2100	QueryStandardI...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	AllocationSize: 24....
11:57:...	Malware_U3_W2_L2.exe	2100	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 19.968, Len...
11:57:...	Malware_U3_W2_L2.exe	2100	ReadFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Offset: 16.384, Len...
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	
11:57:...	Malware_U3_W2_L2.exe	2100	CreateFile	C:\Windows\SysWOW64\ui\SwDRM.dll	PATH NOT FOUND	Desired Access: R...
11:57:...	Malware_U3_W2_L2.exe	2100	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Owner...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryBasicInfor...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	CreationTime: 14/0...
11:57:...	Malware_U3_W2_L2.exe	2100	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Owner...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryBasicInfor...	C:\Windows\SysWOW64\svchost.exe	SUCCESS	CreationTime: 14/0...
11:57:...	Malware_U3_W2_L2.exe	2100	CloseFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	
11:57:...	Malware_U3_W2_L2.exe	2100	QuerySecurityFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Information: Owner...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryNameInfo...	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Name: \Users\user...
11:57:...	Malware_U3_W2_L2.exe	2100	QueryNameInfo...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Name: \Windows\...

Azioni rilevate su processi e thread del malware

11:57:...	Malware_U3_W2_L2.exe	2100	Process Start	SUCCESS	Parent PID: 900, C...
11:57:...	Malware_U3_W2_L2.exe	2100	Thread Create	SUCCESS	Thread ID: 1156
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Ma...	SUCCESS	Image Base: 0x400...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x770...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x772...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73f...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x73f...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73ff...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76c...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76f...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x76e...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76c...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x762...
11:57:...	Malware_U3_W2_L2.exe	2100	Process Create C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2136, Comma...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73b...
11:57:...	Malware_U3_W2_L2.exe	2100	Load Image C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x600...
11:57:...	Malware_U3_W2_L2.exe	2100	Thread Exit	SUCCESS	Thread ID: 1156, ...
11:57:...	Malware_U3_W2_L2.exe	2100	Process Exit	SUCCESS	Exit Status: 0, User...

Errore di applicazione

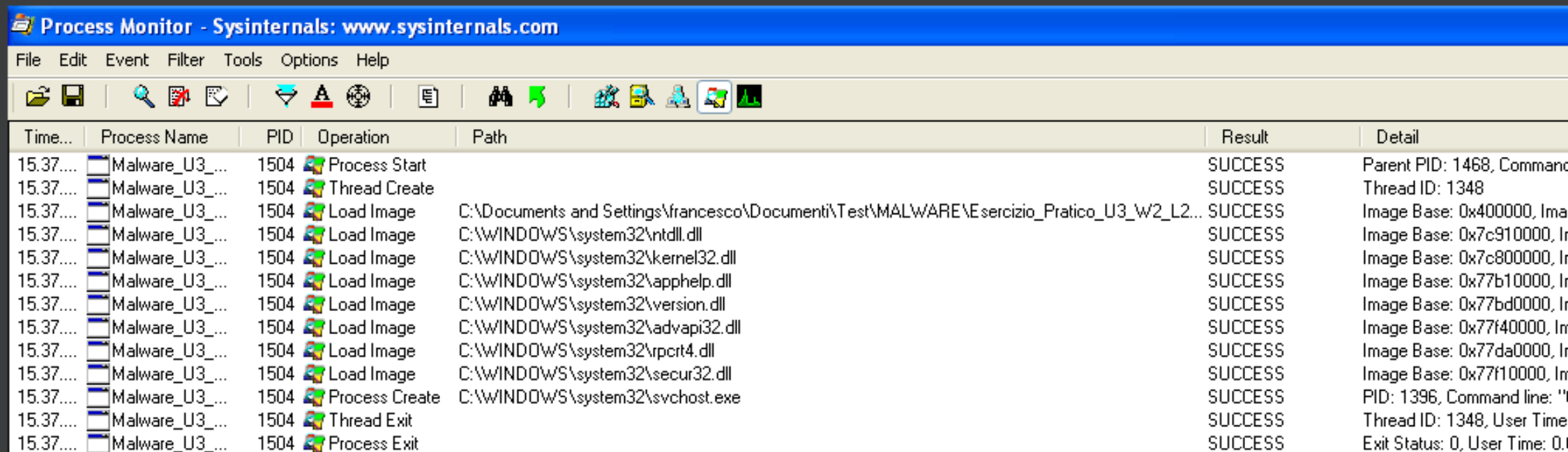


Come è possibile vedere dall'immagine, il .exe avvia dei processi che sono visibili con la cattura di Process Monitor, ma non porta a termine la sua esecuzione portando quest'errore.

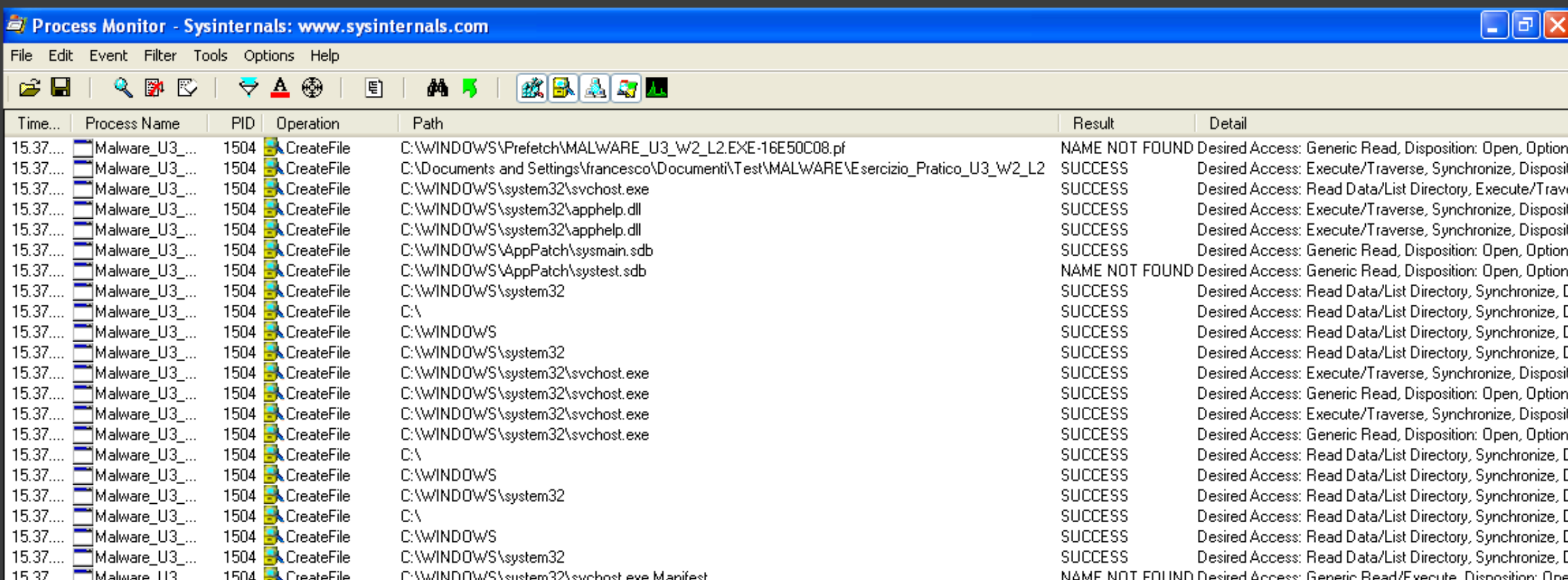
Passando su WinXP

ANALISI

Su macchina WinXP invece vediamo le differenze, il programma va in esecuzione senza dare l'errore visto in precedenza.



Time...	Process Name	PID	Operation	Path	Result	Detail
15.37....	Malware_U3_...	1504	Process Start		SUCCESS	Parent PID: 1468, Command...
15.37....	Malware_U3_...	1504	Thread Create		SUCCESS	Thread ID: 1348
15.37....	Malware_U3_...	1504	Load Image	C:\Documents and Settings\francesco\Documenti\Test\MALWARE\Esercizio_Pratico_U3_W2_L2...	SUCCESS	Image Base: 0x400000, Im...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c910000, In...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, In...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b10000, In...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77bd0000, In...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77f40000, Im...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77da0000, In...
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f10000, Im...
15.37....	Malware_U3_...	1504	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1396, Command line: "h...
15.37....	Malware_U3_...	1504	Thread Exit		SUCCESS	Thread ID: 1348, User Time...
15.37....	Malware_U3_...	1504	Process Exit		SUCCESS	Exit Status: 0, User Time: 0...



Time...	Process Name	PID	Operation	Path	Result	Detail
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-16E50C08.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\Documents and Settings\francesco\Documenti\Test\MALWARE\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Execute/Trave...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\AppPatch\sysrest.sdb	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND	Desired Access: Generic Read/Execute, Disposition: Oper...



Conclusioni

Abbiamo visto che questo malware cerca di mascherarsi creando il processo «svchost.exe», dopo di che fa partire un keylogger che salva i caratteri che vengono digitati in un file di tipo .txt creato nella cartella dove si trova il malware eseguibile



Malware_U3_W2_L2



practicalmalwareanalysis
Documento di testo
1 KB

