

Epicode
CS-0124
Pratica S10/L2
Francesco Ficetti

1. Traccia.....	3
2. Svolgimento.....	4
2.1 Esecuzione del malware su Windows 7.....	4
2.2 Esecuzione del malware su Windows XP.....	4
2.2.1 Azioni del malware su file system.....	5
2.2.2 Azioni del malware su processi e threads.....	5
2.2.3 Modifiche sul registro.....	6
3. Conclusioni.....	6

1. Traccia

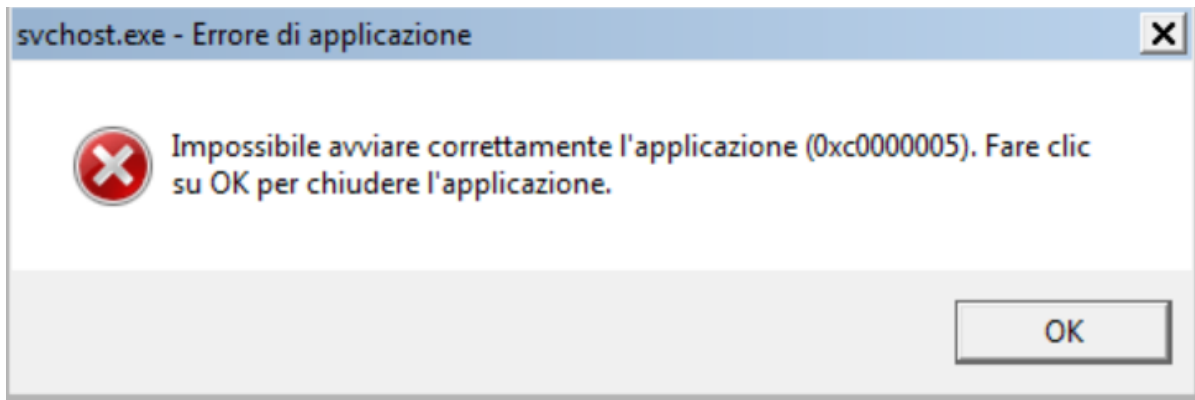
Con riferimento al malware allegato a questo esercizio rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor.
- Identificare eventuali azioni del malware sui processi ed i threads utilizzando ProcessMonitor.
- Modifiche del registro dopo il malware.
- Provare a profilare il malware in base alla correlazione tra Operation e Path.

2. Svolgimento

2.1 Esecuzione del malware su Windows 7

L'esecuzione del malware su Windows 7 restituisce il seguente errore.



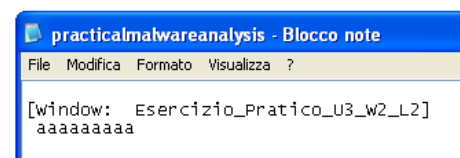
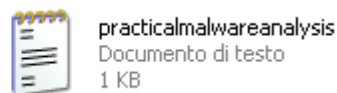
L'esercizio è quindi proseguito su Windows XP.

2.2 Esecuzione del malware su Windows XP

Per prima cosa si deve avviare *procmon*, in modo da iniziare la cattura dei processi. Successivamente è possibile avviare il malware.

Esso non impatta le prestazioni della macchina, se un utente lo dovesse eseguire involontariamente non ne noterebbe la presenza.

Non appena si preme un qualsiasi tasto, viene creato un file, nella stessa cartella del malware, chiamato "praticamalwareanalysis". Al suo interno si trova la "cronologia" di tutti i tasti premuti dall'esecuzione del malware.



Su *procmon* è possibile filtrare la cattura dei processi. In questo caso sono stati applicati due filtri, il primo per vedere solo i processi riguardanti il malware eseguito, il secondo per vedere quelli che eseguivano un'operazione di creazione di un file. Il risultato è il seguente.

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\Documents\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\system.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: Open...

Come si può vedere, ci sono molte chiamate alla funzione `CreateFile`, tra le quali proprio quella che crea il file contenente i tasti premuti.

2.2.2 Azioni del malware su processi e threads

Per quanto riguarda questa parte di analisi, l'unico filtro applicato è quello per vedere solo i processi del malware eseguito.

The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, search, and process management. The main pane displays a list of operations performed by the process Malware_U3_1504. The columns are Time..., Process Name, PID, Operation, Path, Result, and Detail. The operations include Process Start, Thread Create, Load Image, Process Create, Thread Exit, and Process Exit. The Detail column provides additional information such as Parent PID, Command line, Thread ID, Image Base, Image Size, User Time, Kernel Time, and Exit Status.

Time...	Process Name	PID	Operation	Path	Result	Detail
15:37...	Malware_U3_1504	1504	Process Start		SUCCESS	Parent PID: 1468, Command line: "C:\Documents and Settings\francesco\Documents\Test\MALWARE\Esercizio_Pratico_U3_w2_12..."
15:37...	Malware_U3_1504	1504	Thread Create		SUCCESS	Thread ID: 1348
15:37...	Malware_U3_1504	1504	Load Image	C:\Documents and Settings\francesco\Documents\Test\MALWARE\Esercizio_Pratico_U3_w2_12...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c910000, Image Size: 0xb5000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x101000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b10000, Image Size: 0x22000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77bd0000, Image Size: 0x8000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77140000, Image Size: 0xab000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\vpapi4.dll	SUCCESS	Image Base: 0x77da0000, Image Size: 0x32000
15:37...	Malware_U3_1504	1504	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77110000, Image Size: 0x11000
15:37...	Malware_U3_1504	1504	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1396, Command line: "C:\WINDOWS\system32\svchost.exe"
15:37...	Malware_U3_1504	1504	Thread Exit		SUCCESS	Thread ID: 1348, User Time: 0.000000, Kernel Time: 0.000000
15:37...	Malware_U3_1504	1504	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time: 0.000000

Da questa cattura, si può vedere che viene richiamato il processo *svchost.exe*, processo di Windows che in questo caso serve al malware per camuffarsi agli occhi dell' antivirus.

2.2.3 Modifiche sul registro

Con il tool *regshot*, si può eseguire un'istantanea dei registri del sistema operativo prima di avviare il malware, ed una dopo averlo avviato. Successivamente è possibile effettuare una comparazione tra le due. In questo caso, ci sono stati diversi cambiamenti.

3. Conclusioni

Tutti i comportamenti analizzati sono congrui con il comportamento di un keylogger.