

2024



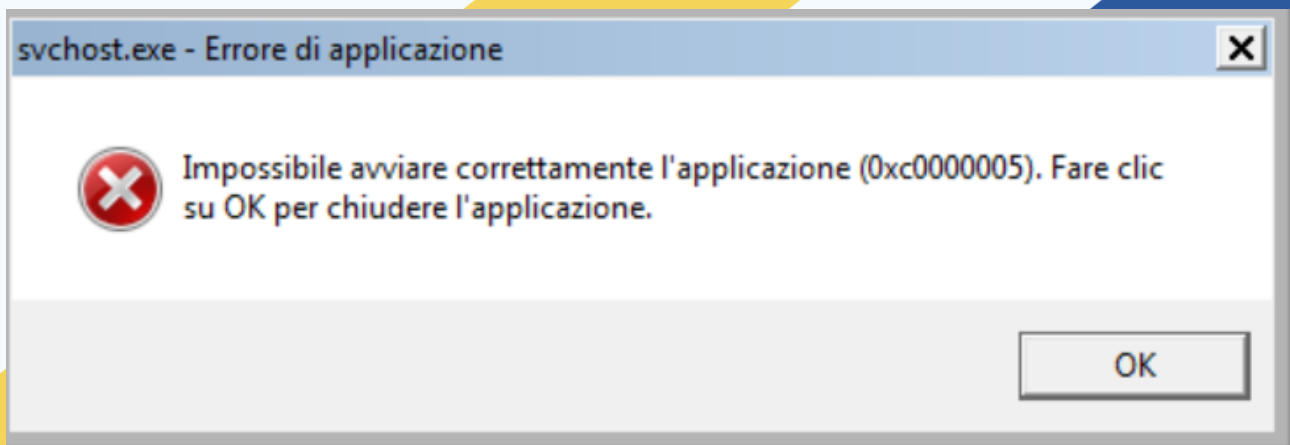
CS0124

REPORT

Week 10 Lesson 2

PREPARED BY : Bruno Falconi

Dopo Aver configurato la macchina virtuale ed aver avviato tutti gli strumenti necessari all'individuazione dei processi del malware ed aver effettivamente avviato l'exe malevolo è risultato impossibile avviare correttamente l'applicazione in quanto supportata da Windows Xp e non da Windows 7. Dopo aver provato varie volte a lanciare l'exe concedendogli permessi di amministratore ed usando lo strumento per la compatibilità come si può constatare il malware non viene lanciato con successo in quanto non riesce a portare a termine la sua esecuzione Tuttavia facendo una analisi statica del malware tramite CFF Explorer e virustotal possiamo dedurre che si tratti di un keylogger che proverà ad inviare i comandi eseguiti dall'utente.



Process Monitor - Sysinternals: www.sysinternals.com

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\sysmain.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:\WINDOWS\system32	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	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:\WINDOWS\system32\svchost.exe	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	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	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...

Process Monitor - Sysinternals: www.sysinternals.com

Time...	Process Name	PID	Operation	Path	Result	Detail
15.37....	Malware_U3_...	1504	Process Start		SUCCESS	Parent PID: 1468, Command line: "C:\Documents and Set...
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, Image Size: 0x0000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c910000, Image Size: 0xb5000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x101000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b10000, Image Size: 0x22000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77bd0000, Image Size: 0x8000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0xab000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77da0000, Image Size: 0x32000
15.37....	Malware_U3_...	1504	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77f10000, Image Size: 0x11000
15.37....	Malware_U3_...	1504	Process Create		SUCCESS	PID: 1396, Command line: "C:\WINDOWS\system32\svch...
15.37....	Malware_U3_...	1504	Thread Exit		SUCCESS	Thread ID: 1348, User Time: 0.000000, Kernel Time: 0.05...
15.37....	Malware_U3_...	1504	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time...