





# S10/L2 Epicode Cybersecurity

Analisi dinamica basica






Nell'esercizio di oggi ci viene richiesto di effettuare un'analisi dinamica basica su un malware che ci è stato fornito ed identificare il tipo e le azioni che compie sul file system e sui processi.







Time ...	Process Name	PID	Operation	Path	Result	Detail
15:51:...	Malware_U3_...	2976	Process Start		SUCCESS	Parent PID: 1908, Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_...
15:51:...	Malware_U3_...	2976	Thread Create		SUCCESS	Thread ID: 2980
15:51:...	Malware_U3_...	2976	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x76eb0000, Image Size: 0x19f000
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77070000, Image Size: 0x180000
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/...
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronou...
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S...
15:51:...	Malware_U3_...	2976	QueryBasicInformationFile	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 06/02/2024 15:18:20, LastAccessTime: 06/02/2024 15:18:20, LastWriteTime: 21/02/...
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Optio...
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTypeOther
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74a60000, Image Size: 0x3f000
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S...
15:51:...	Malware_U3_...	2976	QueryBasicInformationFile	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 06/02/2024 15:18:12, LastAccessTime: 06/02/2024 15:18:12, LastWriteTime: 21/02/...
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Optio...
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTypeOther
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x74a00000, Image Size: 0x5c000
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S...
15:51:...	Malware_U3_...	2976	QueryBasicInformationFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 06/02/2024 15:18:20, LastAccessTime: 06/02/2024 15:18:20, LastWriteTime: 21/02/...
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Optio...
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection:
15:51:...	Malware_U3_...	2976	CreateFileMapping	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTypeOther
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x749f0000, Image Size: 0x8000
15:51:...	Malware_U3_...	2976	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
15:51:...	Malware_U3_...	2976	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, S...
15:51:...	Malware_U3_...	2976	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76c90000, Image Size: 0x11f000



Possiamo vedere come, avviando il malware, esso crei delle librerie '.dll', le legga e poi le chiuda.

Purtroppo, a differenza dell'esecuzione indicata nell'esercizio, questo è stato svolto su Windows 7 e il file che dovrebbe essere creato nella cartella non è presente.





Come possiamo vedere, il file  
utilizza 'svchost.exe',  
un'applicazione di Windows  
spesso usata per iniettare virus.

