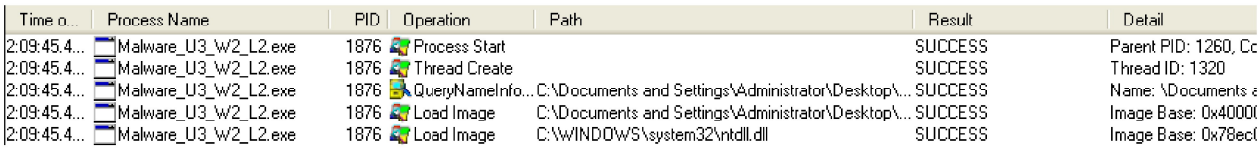
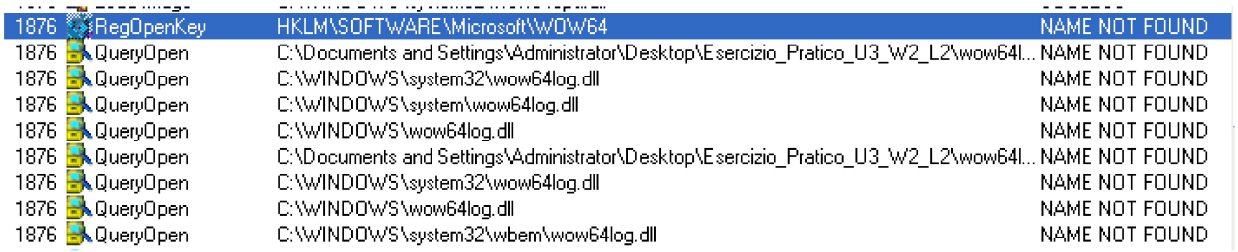
Analisi operazioni del processo

Come possiamo vedere come prima cosa crea un thread



Time o...	Process Name	PID	Operation	Path	Result	Detail
2:09:45.4...	Malware_U3_W2_L2.exe	1876	Process Start		SUCCESS	Parent PID: 1260, Cc
2:09:45.4...	Malware_U3_W2_L2.exe	1876	Thread Create		SUCCESS	Thread ID: 1320
2:09:45.4...	Malware_U3_W2_L2.exe	1876	QueryNameInfo...	C:\Documents and Settings\Administrator\Desktop\...	SUCCESS	Name: \Documents a
2:09:45.4...	Malware_U3_W2_L2.exe	1876	Load Image	C:\Documents and Settings\Administrator\Desktop\...	SUCCESS	Image Base: 0x4000(
2:09:45.4...	Malware_U3_W2_L2.exe	1876	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x78ec(

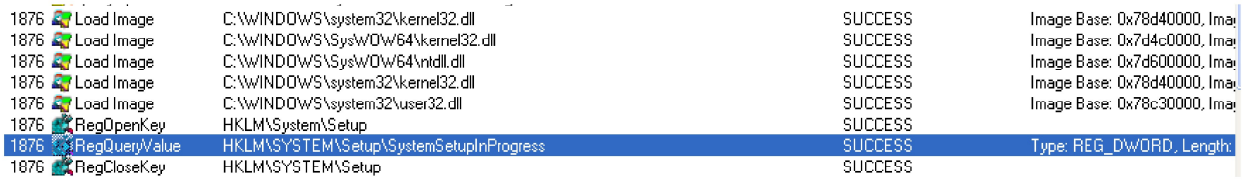
Poi prova a controllare se esistono queste librerie



1876	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND
1876	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\wow64l...	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\system32\wow64log.dll	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\system\wow64log.dll	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\wow64log.dll	NAME NOT FOUND
1876	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\wow64l...	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\system32\wow64log.dll	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\wow64log.dll	NAME NOT FOUND
1876	QueryOpen	C:\WINDOWS\system32\wbem\wow64log.dll	NAME NOT FOUND

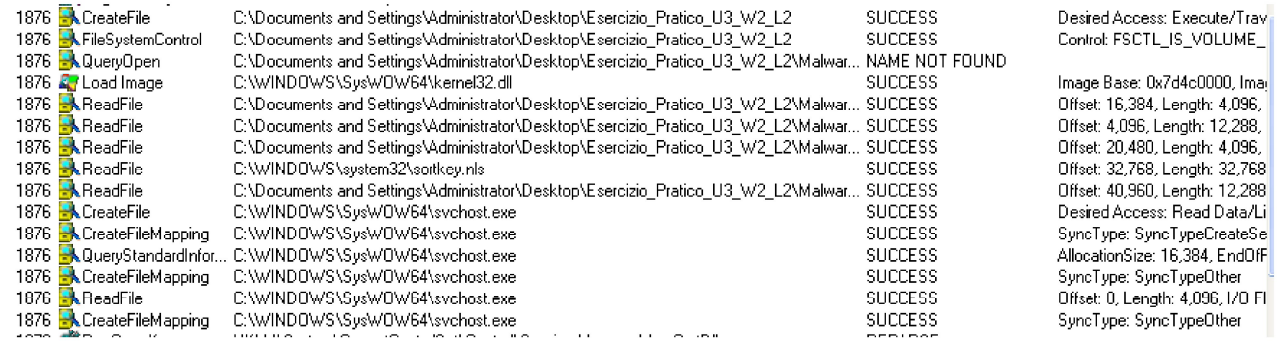
Legge dei dati dalle librerie esistenti, sta caricando dinamicamente le librerie probabilmente, registrando quello che sembra un pointer, probabilemte alla funzione richiamata, poi apre il registro setup, scrive 4 caratteri e chiude il registro.

Una qualche forma di persistenza?



1876	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x78d40000, Ima
1876	Load Image	C:\WINDOWS\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7d4c0000, Ima
1876	Load Image	C:\WINDOWS\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x7d600000, Ima
1876	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x78d40000, Ima
1876	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x78c30000, Ima
1876	RegOpenKey	HKLM\System\Setup	SUCCESS	
1876	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress	SUCCESS	Type: REG_DWORD, Length:
1876	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	

Sembra poi si ricrei e si riavvii, poi crea un file eseguibile chiamato svchost.exe, che è un processo realmente esistente in windows, quindi probabilmente si sta fingendo un servizio esistente



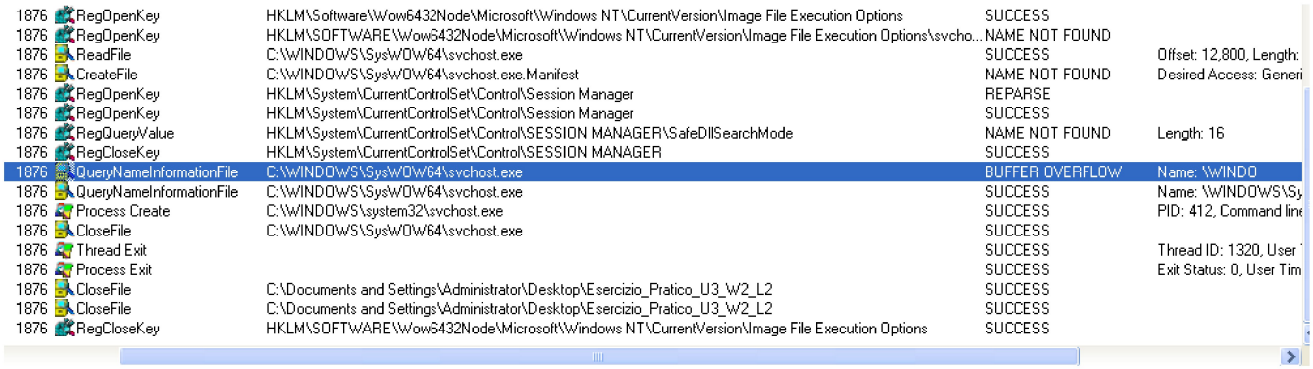
1876	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/Trav
1876	FileSystemControl	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Control: FSCTL_IS_VOLUME_
1876	QueryOpen	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	NAME NOT FOUND	
1876	Load Image	C:\WINDOWS\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7d4c0000, Ima
1876	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS	Offset: 16,384, Length: 4,096,
1876	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS	Offset: 4,096, Length: 12,288,
1876	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS	Offset: 20,480, Length: 4,096,
1876	ReadFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Offset: 32,768, Length: 32,768
1876	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwar...	SUCCESS	Offset: 40,960, Length: 12,288
1876	CreateFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	Desired Access: Read Data/Li
1876	CreateFileMapping	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	SyncType: SyncTypeCreateSe
1876	QueryStandardInfor...	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	AllocationSize: 16,384, EndOfF
1876	CreateFileMapping	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	SyncType: SyncTypeOther
1076	ReadFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	Offset: 0, Length: 4,096, I/O Fl
1876	CreateFileMapping	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	SyncType: SyncTypeOther

Poi scrive altro nelle policies di windows, AutenticodeEnabled da documentazione:

What is Windows Authenticode?

Windows Authenticode is a digital signature format that is used to determine the origin and integrity of software binaries. Authenticode uses Public-Key Cryptography Standards (PKCS) #7 signed data and X.509 certificates to bind an Authenticode-signed binary to the identity of a software publisher. The term "Authenticode signature" refers to a digital signature format that is generated and verified using the WinVerifyTrust function.

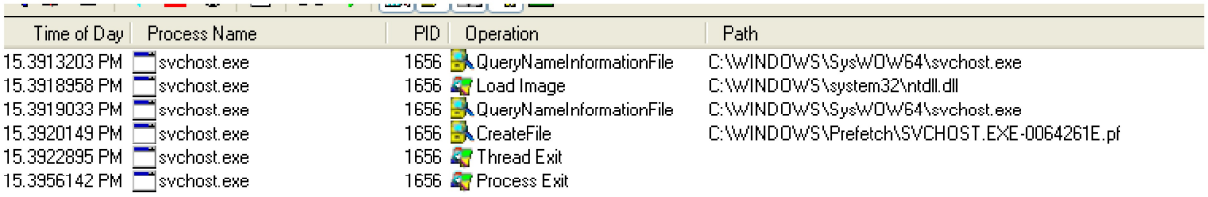
Probabilmente è un controllo di autenticità che viene disattivato



1876	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	
1876	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\svcho...	NAME NOT FOUND	
1876	ReadFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	Offset: 12,800, Length:
1876	CreateFile	C:\WINDOWS\SysWOW64\svchost.exe.Manifest	NAME NOT FOUND	Desired Access: Generi
1876	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	
1876	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
1876	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\SafeDllSearchMode	NAME NOT FOUND	Length: 16
1876	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
1876	QueryNameInformationFile	C:\WINDOWS\SysWOW64\svchost.exe	BUFFER OVERFLOW	Name: \WINDO
1876	QueryNameInformationFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	Name: \WINDOWS\Sy
1876	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 412, Command line
1876	CloseFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS	
1876	Thread Exit		SUCCESS	Thread ID: 1320, User
1876	Process Exit		SUCCESS	Exit Status: 0, User Tim
1876	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
1876	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
1876	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	

Queste sono le ultime operazioni che fa prima di chiudersi: crea un manifest di svchost.exe, poi viene causato un bufferoverflow, in ultimo crea un processo figlio con pid 412 di svchost, e si chiude.

L'istanza di svchost creata dopo poco si chiude senza fare niente.



Time of Day	Process Name	PID	Operation	Path
15.3913203 PM	svchost.exe	1656	QueryNameInformationFile	C:\WINDOWS\SysWOW64\svchost.exe
15.3918958 PM	svchost.exe	1656	Load Image	C:\WINDOWS\system32\ntdll.dll
15.3919033 PM	svchost.exe	1656	QueryNameInformationFile	C:\WINDOWS\SysWOW64\svchost.exe
15.3920149 PM	svchost.exe	1656	CreateFile	C:\WINDOWS\Prefetch\SVCHOST.EXE-0064261E.pf
15.3922895 PM	svchost.exe	1656	Thread Exit	
15.3956142 PM	svchost.exe	1656	Process Exit	

Non sembra faccia altro.