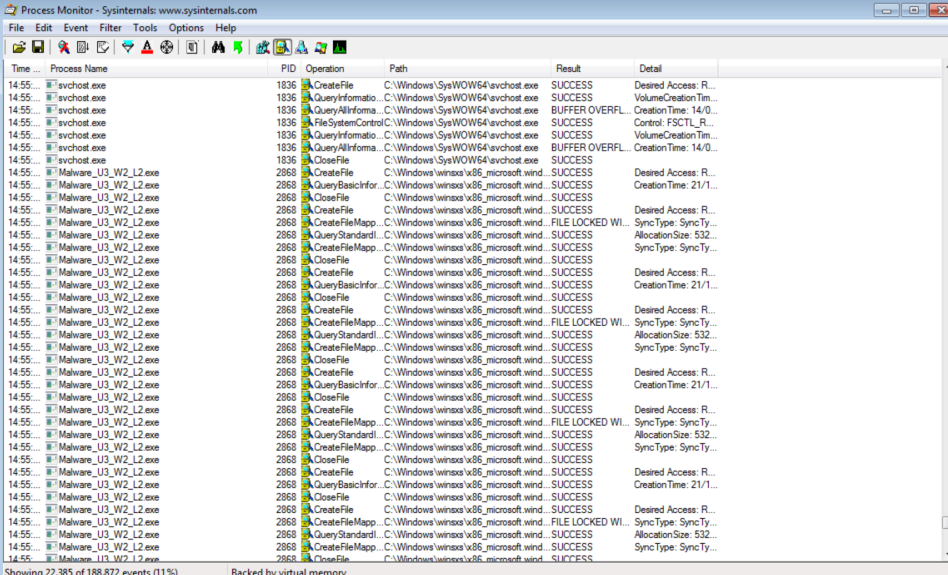


ESERCIZIO 2 SETTIMANA 10

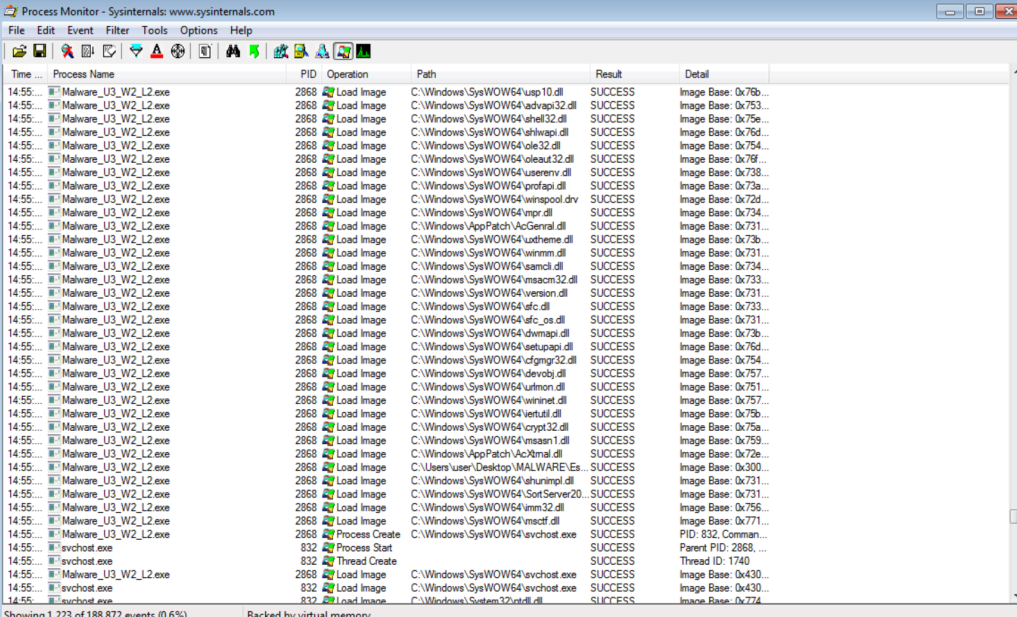
Oggi bisogna monitorare il sistema utilizzando Process Monitor che è uno strumento di monitoraggio del sistema per Windows che consente di visualizzare in tempo reale l'attività del sistema operativo, inclusi i processi in esecuzione, i file system, il Registro di sistema e altro ancora. Ti fornisce dettagli approfonditi su cosa sta accadendo nel sistema, utile per diagnosticare problemi, individuare malware, monitorare le prestazioni e altro ancora.

Qui possiamo notare i file system



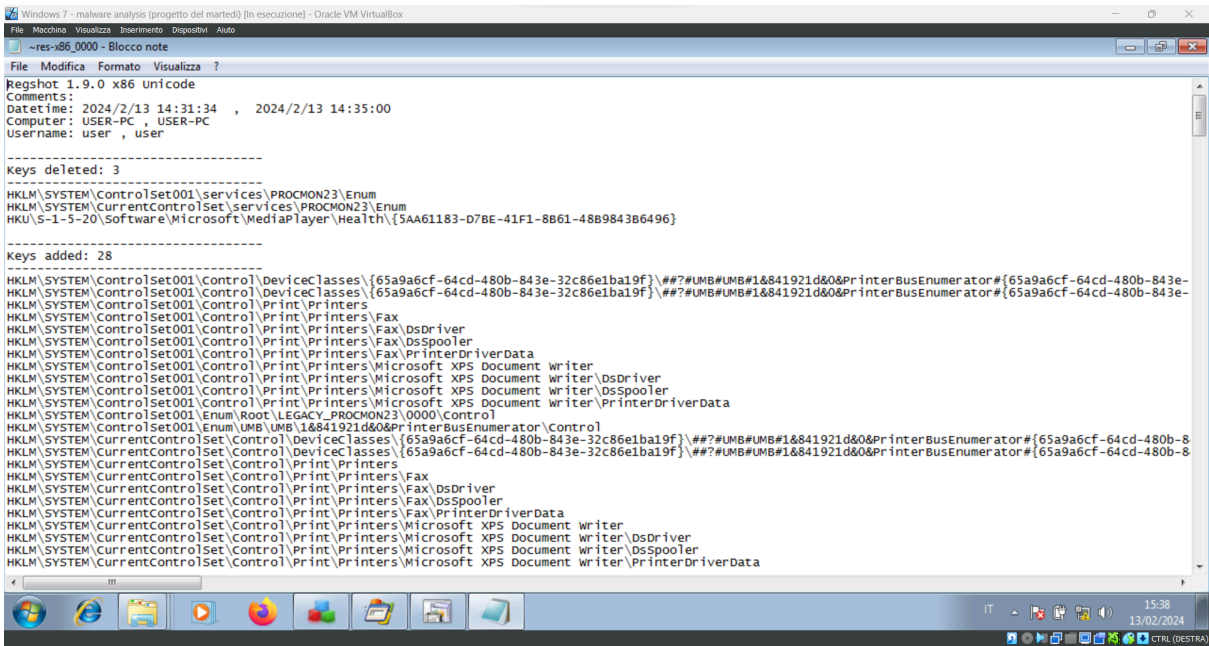
Time	Process Name	PID	Operation	Path	Result	Detail
14:55...	svchost.exe	1836	CreateFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Desired Access: R...
14:55...	svchost.exe	1836	QueryInformation	C:\Windows\SysWOW64\svchost.exe	SUCCESS	VolumeCreationTim...
14:55...	svchost.exe	1836	QueryInformation	C:\Windows\SysWOW64\svchost.exe	SUCCESS	CreationTime: 14/0...
14:55...	svchost.exe	1836	FileSystemControl	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Control: FSCTL_R...
14:55...	svchost.exe	1836	QueryInformation	C:\Windows\SysWOW64\svchost.exe	SUCCESS	VolumeCreationTim...
14:55...	svchost.exe	1836	QueryAllInforma...	C:\Windows\SysWOW64\svchost.exe	BUFFER OVERFL...	CreationTime: 14/0...
14:55...	Malware_U3_W2_L2.exe	1836	CreateFile	C:\Windows\SysWOW64\svchost.exe	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	QueryBasicInfor...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	CreationTime: 21/1...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	FILE LOCKED WI...	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	QueryStandardI...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	AllocationSize: 532...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	QueryBasicInfor...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	CreationTime: 21/1...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	FILE LOCKED WI...	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	QueryStandardI...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	AllocationSize: 532...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	QueryBasicInfor...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	CreationTime: 21/1...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	FILE LOCKED WI...	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	QueryStandardI...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	AllocationSize: 532...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	QueryBasicInfor...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	CreationTime: 21/1...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	
14:55...	Malware_U3_W2_L2.exe	2868	CreateFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	Desired Access: R...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	FILE LOCKED WI...	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	QueryStandardI...	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	AllocationSize: 532...
14:55...	Malware_U3_W2_L2.exe	2868	CreateFileMap	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	SyncType: SyncTy...
14:55...	Malware_U3_W2_L2.exe	2868	CloseFile	C:\Windows\winsx\w86_microsoft.wind...	SUCCESS	

Qui notiamo i processi e i thread

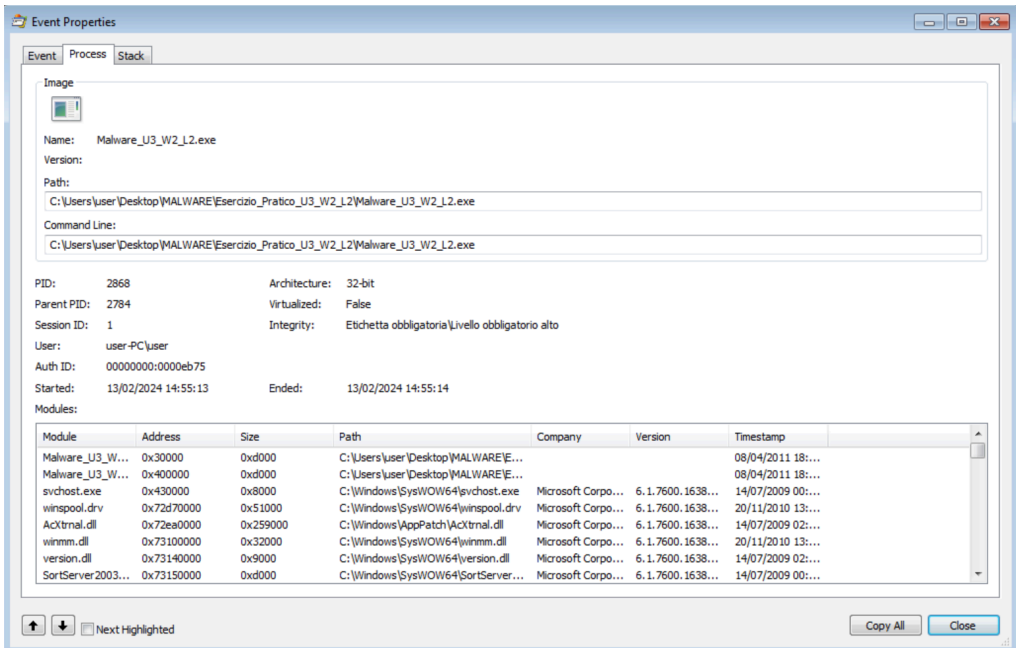
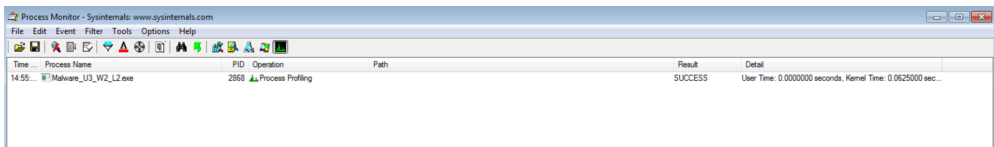


Time	Process Name	PID	Operation	Path	Result	Detail
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Image Base: 0x7b...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x73...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x75...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x76d...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x754...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x7f8...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\userenv.dll	SUCCESS	Image Base: 0x738...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x73a...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ufgnp32.dll	SUCCESS	Image Base: 0x72d...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\mpr.dll	SUCCESS	Image Base: 0x734...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\AppPatch\AcGennal.dll	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\lutheme.dll	SUCCESS	Image Base: 0x73b...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\winmm.dll	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\eamcl.dll	SUCCESS	Image Base: 0x734...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ufgnp32.dll	SUCCESS	Image Base: 0x733...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\version.dll	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ufc.dll	SUCCESS	Image Base: 0x733...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ufc_os.dll	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Image Base: 0x73b...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\setupapi.dll	SUCCESS	Image Base: 0x76d...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ufgnp32.dll	SUCCESS	Image Base: 0x754...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Image Base: 0x757...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\utlntm.dll	SUCCESS	Image Base: 0x751...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x757...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\vertutil.dll	SUCCESS	Image Base: 0x79b...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x75a...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\ntasn1.dll	SUCCESS	Image Base: 0x759...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\AppPatch\AcXrmal.dll	SUCCESS	Image Base: 0x72e...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Users\user\Desktop\MALWARE.Es...	SUCCESS	Image Base: 0x300...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\shunimpl.dll	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\SetServer20...	SUCCESS	Image Base: 0x731...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\mm32.dll	SUCCESS	Image Base: 0x756...
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\mscmt.dll	SUCCESS	Image Base: 0x771...
14:55...	Malware_U3_W2_L2.exe	2868	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 832, Comman...
14:55...	svchost.exe	832	Process Start		SUCCESS	Parent PID: 2868, ...
14:55...	svchost.exe	832	Thread Create		SUCCESS	Thread ID: 1740
14:55...	Malware_U3_W2_L2.exe	2868	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x430...
14:55...	svchost.exe	832	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x430...
14:55...	svchost.exe	832	Load Image	C:\Windows\System32\nt.dll	SUCCESS	Image Base: 0x774...

Qui possiamo notare le modifiche dopo il malware



Provare a profilare il malware in base alla correlazione tra «operation» e Path.



Possiamo notare che la winmm.dll è una libreria di collegamento dinamico (DLL) di Windows che fornisce funzionalità per la gestione dei suoni e della multimedialità.

Essa contiene diverse funzioni per la gestione di file audio e video, controllare i dispositivi multimediali come altoparlanti e microfoni, e per la riproduzione di suoni su un sistema Windows. In pratica, è coinvolta nella gestione di varie operazioni audio e multimediali all'interno del sistema operativo Windows.

Anche la presenza di Winspool.drv, che è una libreria di collegamento dinamico (DLL) di Windows che fornisce funzionalità per la gestione delle stampanti e delle code di stampa nel sistema operativo Windows. Questa libreria contiene diverse funzioni che consentono alle applicazioni di interagire con le stampanti installate, come ad esempio inviare documenti da stampare, monitorare lo stato delle stampanti e gestire le impostazioni di stampa. In sostanza, winspool.drv facilita la comunicazione e il controllo delle operazioni di stampa nel sistema operativo Windows.