

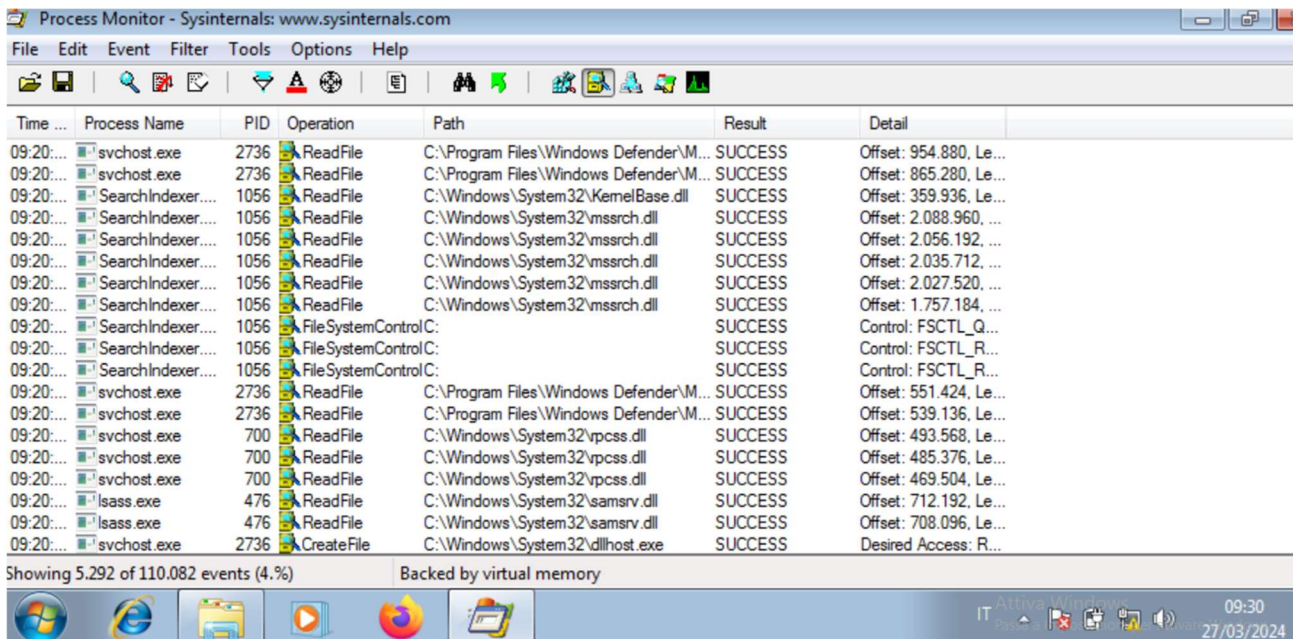
Traccia:

Nella lezione teorica, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica. Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon);
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor;
- Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (le differenze).

Suggerimento:

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione Create File su path noti (ad esempio il path dove è presente l'eseguibile del malware). Creare istantanea da Virtualbox della macchina Windows XP prima di iniziare per poter ripristinare in caso di problemi (o al limite fare il clone).



Time ...	Process Name	PID	Operation	Path	Result	Detail
09:20:...	svchost.exe	2736	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 954.880, Le...
09:20:...	svchost.exe	2736	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 865.280, Le...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 359.936, Le...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2.088.960, ...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2.056.192, ...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2.035.712, ...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 2.027.520, ...
09:20:...	SearchIndexer....	1056	ReadFile	C:\Windows\System32\msrch.dll	SUCCESS	Offset: 1.757.184, ...
09:20:...	SearchIndexer....	1056	FileSystemControl C:		SUCCESS	Control: FSCTL_Q...
09:20:...	SearchIndexer....	1056	FileSystemControl C:		SUCCESS	Control: FSCTL_R...
09:20:...	SearchIndexer....	1056	FileSystemControl C:		SUCCESS	Control: FSCTL_R...
09:20:...	svchost.exe	2736	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 551.424, Le...
09:20:...	svchost.exe	2736	ReadFile	C:\Program Files\Windows Defender\M...	SUCCESS	Offset: 539.136, Le...
09:20:...	svchost.exe	700	ReadFile	C:\Windows\System32\vpss.dll	SUCCESS	Offset: 493.568, Le...
09:20:...	svchost.exe	700	ReadFile	C:\Windows\System32\vpss.dll	SUCCESS	Offset: 485.376, Le...
09:20:...	svchost.exe	700	ReadFile	C:\Windows\System32\vpss.dll	SUCCESS	Offset: 469.504, Le...
09:20:...	lsass.exe	476	ReadFile	C:\Windows\System32\samsrv.dll	SUCCESS	Offset: 712.192, Le...
09:20:...	lsass.exe	476	ReadFile	C:\Windows\System32\samsrv.dll	SUCCESS	Offset: 708.096, Le...
09:20:...	svchost.exe	2736	CreateFile	C:\Windows\System32\dlhost.exe	SUCCESS	Desired Access: R...

Showing 5,292 of 110,082 events (4.%) Backed by virtual memory

IT Attiva Monitoraggio 09:30 27/03/2024

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
09:20:...	svchost.exe	868	Thread Create		SUCCESS	Thread ID: 2108
09:20:...	svchost.exe	868	Thread Create		SUCCESS	Thread ID: 2884
09:20:...	AUDIODG.EXE	2384	Thread Create		SUCCESS	Thread ID: 2936
09:20:...	svchost.exe	868	Thread Create		SUCCESS	Thread ID: 2704
09:20:...	wbmprvse.exe	2876	Load Image	C:\Windows\System32\wbem\wbempro...	SUCCESS	Image Base: 0x7ef...
09:20:...	wbmprvse.exe	2876	Thread Create		SUCCESS	Thread ID: 1564
09:20:...	AUDIODG.EXE	2384	Thread Exit		SUCCESS	Thread ID: 2936, ...
09:20:...	AUDIODG.EXE	2384	Thread Create		SUCCESS	Thread ID: 2456
09:20:...	svchost.exe	780	Load Image	C:\Windows\System32\drivers\fltMgr.sys	SUCCESS	Image Base: 0x138...
09:20:...	AUDIODG.EXE	2384	Thread Exit		SUCCESS	Thread ID: 2456, ...
09:20:...	Explorer.EXE	1260	Thread Create		SUCCESS	Thread ID: 2412
09:20:...	Explorer.EXE	1260	Load Image	C:\Users\user\AppData\Local\Temp\P...	SUCCESS	Image Base: 0x13f...
09:20:...	lsass.exe	476	Thread Create		SUCCESS	Thread ID: 776
09:20:...	Explorer.EXE	1260	Load Image	C:\Program Files\Mozilla Firefox\firefox.e...	SUCCESS	Image Base: 0x13f...
09:20:...	Explorer.EXE	1260	Load Image	C:\Program Files\Mozilla Firefox\firefox.e...	SUCCESS	Image Base: 0x13f...
09:20:...	Explorer.EXE	1260	Thread Create		SUCCESS	Thread ID: 2044
09:20:...	Explorer.EXE	1260	Thread Create		SUCCESS	Thread ID: 2932
09:20:...	Explorer.EXE	1260	Thread Create		SUCCESS	Thread ID: 1436
09:20:...	svchost.exe	1416	Thread Create		SUCCESS	Thread ID: 1992

Showing 606 of 108.383 events (0.5%) Backed by virtual memory

IT Attiva Windows 09:29
Passa a 27/03/2024

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
21:04:...	Explorer.EXE	1260	RegOpenKey	HKCU\Software\Classes\exefile	NAME NOT FOUND	Desired Access: M...
21:04:...	Explorer.EXE	1260	RegQueryValue	HKCR\exefile\AppDataModelID	NAME NOT FOUND	Length: 144
21:04:...	Explorer.EXE	1260	RegCloseKey	HKCR\exefile	SUCCESS	
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
21:04:...	Malware_U3_...	2608	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
21:04:...	Malware_U3_...	2608	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND	Desired Access: Q...
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS	Desired Access: Q...
21:04:...	Malware_U3_...	2608	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
21:04:...	Malware_U3_...	2608	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
21:04:...	Malware_U3_...	2608	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
21:04:...	Malware_U3_...	2608	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
21:04:...	Malware_U3_...	2608	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
21:04:...	csrss.exe	380	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Desired Access: Q...

Showing 14.506 of 62.681 events (23%) Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
21:04:...	Malware_U3_...	2608	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
21:04:...	Malware_U3_...	2608	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/1...
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
21:04:...	Malware_U3_...	2608	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
21:04:...	Malware_U3_...	2608	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/1...
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
21:04:...	Malware_U3_...	2608	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
21:04:...	Malware_U3_...	2608	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	

Showing 1.461 of 62.681 events (2.%) Backed by virtual memory

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
21:04:...	Malware_U3_...	2608	Process Start		SUCCESS	Parent PID: 1260, ...
21:04:...	Malware_U3_...	2608	Thread Create		SUCCESS	Thread ID: 2700
21:04:...	Explorer.EXE	1260	Load Image	C:\Windows\System32\sfcdll.dll	SUCCESS	Image Base: 0x736...
21:04:...	Explorer.EXE	1260	Load Image	C:\Windows\System32\sfcdll.dll	SUCCESS	Image Base: 0x736...
21:04:...	Malware_U3_...	2608	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x76c...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x76e...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x744...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x74a...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76b...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x759...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76b...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x76a...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x759...
21:04:...	Malware_U3_...	2608	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x762...
21:04:...	csrss.exe	380	Process Create	C:\Windows\system32\conhost.exe	SUCCESS	PID: 2824, Comma...
21:04:...	conhost.exe	2824	Process Start		SUCCESS	Parent PID: 380, C...
21:04:...	conhost.exe	2824	Thread Create		SUCCESS	Thread ID: 2520

Showing 169 of 62.681 events (0.2%) Backed by virtual memory

Event Properties

Event	Process	Stack
Date:	27/03/2024 21:04:39	
Thread:	2700	
Class:	File System	
Operation:	CreateFile	
Result:	NAME NOT FOUND	
Path:	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	
Duration:	0.0000367	
Desired Access:	Generic Read	
Disposition:	Open	
Options:	Synchronous IO Non-Alert	
Attributes:	n/a	
ShareMode:	None	
AllocationSize:	n/a	

