

Esercitazione W21D1 - Pratica 1

Malware Analysis: Analisi dinamica basica

Fabio Benevento - 26/03/2024

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:

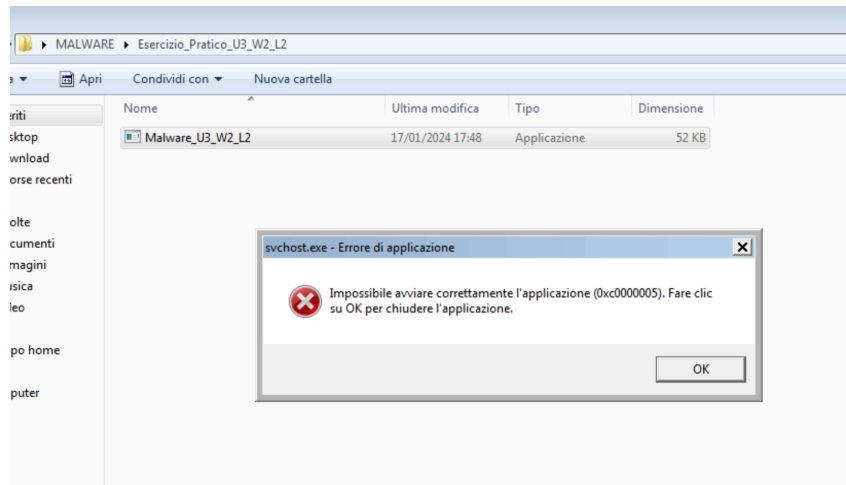
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (le differenze)

Implementazione

Dopo aver avviato Procmon ho lanciato il malware Malware_U3_W2_L2, quindi dopo circa un minuto ho stoppato la cattura.

L'esecuzione del malware termina con un errore come mostrato in figura.

Una volta stoppata l'esecuzione ho filtrato per nome del processo al fine di limitare i risultati della cattura al solo malware.



1. Identificare eventuali azioni del malware sul file system

Filtrando ulteriormente per i soli eventi del file system è possibile individuare numerose operazioni di creazione e lettura/scrittura di file. Alcune di queste vanno a buon fine (SUCCESS) altre invece vengono bloccate dal sistema operativo o comunque non vanno a buon fine (FILE LOCKED, NAME NOT FOUND...)

Time	Process Name	PID	Operation	Path	Result	Detail
09:53...	Malware_U3...	3040	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes; Disposition: Open; Options: Open Reparse Point; Attributes: n/a; ShareMode: Read, Write, Delete; AllocationSize: n/a; Op...
09:53...	Malware_U3...	3040	QueryBasicInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Creation Time: 21/11/2010 05:24:32; LastAccessTime: 21/11/2010 05:24:32; LastWriteTime: 21/11/2010 05:24:32; ChangeTime: 17/01/2024 12:14:47; F...
09:53...	Malware_U3...	3040	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Directory File, Abbi...
09:53...	Malware_U3...	3040	CreateFileMap	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection; PageProtection: SyncType: SyncTypeOther
09:53...	Malware_U3...	3040	CreateFileMap	C:\Windows\System32\wow64cpu.dll	SUCCESS	
09:53...	Malware_U3...	3040	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	NAME NOT FOUND	Desired Access: Read Attributes; Disposition: Open; Options: Open Reparse Point; Attributes: n/a; ShareMode: Read, Write, Delete; AllocationSize: n/a
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes; Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert; Attributes: n/a; ShareMode: Read, Write, Delete; Allo...
09:53...	Malware_U3...	3040	QueryNameInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Name: 'Windows'
09:53...	Malware_U3...	3040	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
09:53...	Malware_U3...	3040	CreateFile	C:\Users\user\Desktop\MALWARE-Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/Traverse, Synchronize; Disposition: Open; Options: Directory, Synchronous IO Non-Alert; Attributes: n/a; ShareMode: Read, Write...
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 338,944; Length: 15,360; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 330,752; Length: 8,192; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 62,464; Length: 32,768; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Users\user\Desktop\MALWARE-Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 40,960; Length: 12,288; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 259,072; Length: 32,768; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 439,296; Length: 32,768; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize; Disposition: Open; Options: Synchronous IO Non-Alert, Non-Dir...
09:53...	Malware_U3...	3040	CreateFileMap	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTypeCreateSection; PageProtection: SyncType: SyncTypeOther
09:53...	Malware_U3...	3040	QueryStandardInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	AllocationSize: 24,576; EndOfFile: 20,992; NumberOfLinks: 2; DeletePending: False; Directory: False
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 0; Length: 4,096; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 19,968; Length: 1,024; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	CreateFileMap	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTypeOther
09:53...	Malware_U3...	3040	QuerySecurityInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Information: Label
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 1,024; Length: 14,848; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	ReadFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Offset: 17,408; Length: 2,560; I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
09:53...	Malware_U3...	3040	QueryNameInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Name: 'Windows\SysWOW64\svchost.exe'
09:53...	Malware_U3...	3040	QuerySecurityInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Information: Owner, Group, DACL, SACL, Label
09:53...	Malware_U3...	3040	QueryBasicInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Creation Time: 14/07/2009 01:19:28; LastAccessTime: 14/07/2009 01:19:28; LastWriteTime: 14/07/2009 03:14:41; ChangeTime: 17/01/2024 12:14:16; F...
09:53...	Malware_U3...	3040	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes; Disposition: Open; Options: Open Reparse Point; Attributes: n/a; ShareMode: Read, Write, Delete; AllocationSize: n/a; Op...
09:53...	Malware_U3...	3040	QueryBasicInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Creation Time: 21/11/2010 05:24:14; LastAccessTime: 21/11/2010 05:24:14; LastWriteTime: 21/11/2010 05:24:14; ChangeTime: 17/01/2024 12:14:02; F...

2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

Analizzando le operazioni svolte dal malware su processi e thread, è possibile notare che una volta partito il malware crea un nuovo thread, dopo di che effettua diverse operazioni di caricamento di librerie (Load Image).

Nel mezzo di queste operazioni ciò che salta all'occhio è un tentativo da parte del malware di creare un sottoprocesso con nome svchost.exe. Svchost.exe è un processo

normalmente presente nei sistemi operativi Windows. Molto probabilmente il malware tenta di avviare delle operazioni “nascondendosi” dietro il processo lecito svchost.exe. L'operazione va a buon fine e viene creato un nuovo processo con PID 2804

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time	Process Name	PID	Operation	Path	Result Detail
09:53	Malware_U3	3040	Process Start		SUCCESS Parent PID: 1844. Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe". Current directory: C:\Us...
09:53	Malware_U3	3040	Thread Create		SUCCESS Thread ID: 1912
09:53	Malware_U3	3040	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS Image Base: 0x400000. Image Size: 0xd000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\ntldr.dll	SUCCESS Image Base: 0x7b60000. Image Size: 0x1a9000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\wow64.dll	SUCCESS Image Base: 0x7b60000. Image Size: 0x180000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\wow64.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x3000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x5c00
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x110000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x110000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\user32.dll	SUCCESS Image Base: 0x7660000. Image Size: 0xf4000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\user32.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x110000
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\user32.dll	SUCCESS Image Base: 0x7260000. Image Size: 0x4000
09:53	Malware_U3	3040	Process Create	C:\Windows\System32\svchost.exe	SUCCESS PID: 2804. Command line: "C:\Windows\system32\svchost.exe"
09:53	Malware_U3	3040	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS Image Base: 0x7460000. Image Size: 0x4c00
09:53	Malware_U3	3040	Thread Exit	C:\Windows\System32\svchost.exe	SUCCESS Image Base: 0x380000. Image Size: 0xd000
09:53	Malware_U3	3040	Process Exit		SUCCESS Thread ID: 1912. User Time: 0.0000000 seconds. Kernel Time: 0.0468750 seconds. Private Bytes: 643,072. Peak Private Bytes: 675,840. Working Set: 2,314...

3. Identificare le eventuali modifiche del registro dopo l'esecuzione del malware

Filtrando all'interno di Procmon per le sole operazioni relative al registro di sistema, è possibile identificare numerose operazioni di lettura/scrittura di chiavi del registro.

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time	Process Name	PID	Operation	Path	Result Detail
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompat	NAME NOT FOUND Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE Desired Access: Query Value, Set Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND Desired Access: Query Value, Set Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
09:53	Malware_U3	3040	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	NAME NOT FOUND Length: 80
09:53	Malware_U3	3040	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS Type: REG_DWORD, Length: 4, Data: 0
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompat	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompat	NAME NOT FOUND Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegSetInfoKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
09:53	Malware_U3	3040	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache	SUCCESS Type: REG_SZ, Length: 142, Data: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	REPARSE Desired Access: Query Value
09:53	Malware_U3	3040	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale	NAME NOT FOUND Length: 120
09:53	Malware_U3	3040	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale	NAME NOT FOUND Length: 120
09:53	Malware_U3	3040	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Language	SUCCESS Desired Access: Read
09:53	Malware_U3	3040	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Nls\Language	SUCCESS KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
09:53	Malware_U3	3040	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Language\InstallLanguageFallback	NAME NOT FOUND Length: 16
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	SUCCESS Desired Access: Read
09:53	Malware_U3	3040	RegEnumKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	SUCCESS Index: 0, Name: 8-IT
09:53	Malware_U3	3040	RegQueryValue	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	SUCCESS Query Handle Tags, Handle Tags: 0x400
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\8-IT	SUCCESS Desired Access: Read
09:53	Malware_U3	3040	RegQueryValue	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\8-IT\AlternateCodePage	SUCCESS Type: REG_DWORD, Length: 4, Data: 145
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\8-IT	NAME NOT FOUND Length: 12
09:53	Malware_U3	3040	RegEnumKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages	SUCCESS NO MORE ENTRI... Index: 1, Length: 512
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	SUCCESS Desired Access: Maximum Allowed, Granted Access: All Access
09:53	Malware_U3	3040	RegOpenKey	HKCU\Control Panel\Desktop\MuiCachedMachineLanguageConfiguration	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration	SUCCESS Desired Access: Read
09:53	Malware_U3	3040	RegEnumKey	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration	SUCCESS KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
09:53	Malware_U3	3040	RegEnumKey	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration	SUCCESS NO MORE ENTRI... Index: 0, Length: 512
09:53	Malware_U3	3040	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	REPARSE Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Software\Wow6432Node\Policies\Microsoft\MUI\Settings	SUCCESS Desired Access: Maximum Allowed, Granted Access: All Access
09:53	Malware_U3	3040	RegOpenKey	HKCU\Control Panel\Desktop\MuiCachedMachineLanguageConfiguration	NAME NOT FOUND Desired Access: Read
09:53	Malware_U3	3040	RegOpenKey	HKCU\Control Panel\Desktop\MuiCachedMachineLanguageConfiguration	SUCCESS Query Handle Tags, Handle Tags: 0x0

Prendendo in esame tra le tante la riga selezionata, ad esempio, esso riguarda la modifica (RegSetHotKey) di una chiave sotto il path (HKLM\System\CurrentControlSet\Control\MUI\UILanguages) che fa quindi supporre la modifica di chiavi inerenti la lingua di sistema. Cliccando sull'evento per maggiori dettagli è possibile vedere che la chiave nello specifico è la chiave KeySetHandleTagInformation e l'operazione va a buon fine (SUCCESS.)

