

Report Esercizio

W21-D2



Redatto da Andrea Sciattella

18/07/2024

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**)

SVOLGIMENTO ESERCIZIO

Primo step, scarichiamo la cartella contenente i malware forniti ed andiamo a selezionare il file chiamato "Esercizio_Pratico_U3_W2_L2".

Secondo step, apriamo Process Monitor fornito dalla suite di Sysinternals, un tool utilizzato per monitorare e visualizzare in tempo reale tutte le attività del file system su un sistema operativo simile a Microsoft Windows o Unix. Ora lanciamo il file:

16.36...	Malware_U3_...	1080	QueryNameInfo...	C:\Documents and Settings\Epicode_u...	SUCCESS	Name: \Document...
16.36...	Malware_U3_...	1080	QueryNameInfo...	C:\Documents and Settings\Epicode_u...	SUCCESS	Name: \Document...
16.36...	winlogon.exe	644	NotifyChangeDi...	C:\WINDOWS	SUCCESS	Filter: FILE_NOTIF...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	Desired Access: G...
16.36...	Malware_U3_...	1080	QueryStandard...	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	AllocationSize: 8.1...
16.36...	Malware_U3_...	1080	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	Offset: 0, Length: 4...
16.36...	Malware_U3_...	1080	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	
16.36...	Malware_U3_...	1080	CreateFile	C:	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	QueryInformatio...	C:	SUCCESS	VolumeCreationTim...
16.36...	Malware_U3_...	1080	FileSystemControl	C:	SUCCESS	Control: FSCTL_FI...
16.36...	Malware_U3_...	1080	CreateFile	C:\	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\	SUCCESS	0: AUTOEXEC.BA...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\	NO MORE FILES	
16.36...	Malware_U3_...	1080	CloseFile	C:\	SUCCESS	

- Da procmon possiamo confermare che il file sia partito immediatamente, ed abbia già iniziato a richiedere accesso e informazioni sul sistema.

16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: .. 1: ... 2: \$winnt...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: emptyregdb.dat, ...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: mqdscli.dll, 1: m...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: rasman.dll, 1: ras...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: wininet.dll, 1: wi...
16.36...	Malware_U3_...	1080	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	
16.36...	Malware_U3_...	1080	CloseFile	C:\WINDOWS\system32	SUCCESS	

- Ora notiamo che il file richiede stranamente l'accesso a tutte le librerie dinamiche del sistema (.DLL).

16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	AllocationSize: 729...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	AllocationSize: 1.0...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\unicode.nls	SUCCESS	AllocationSize: 90...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\locale.nls	SUCCESS	AllocationSize: 266...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	AllocationSize: 24...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\ctype.nls	SUCCESS	AllocationSize: 12...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	AllocationSize: 266...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize: 126...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1.2...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: R...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	QueryStandardl...	C:\WINDOWS\system32\version.dll	SUCCESS	AllocationSize: 20...
16.36...	Malware_U3_...	1080	CreateFileMap...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
16.36...	Malware_U3_...	1080	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: R...

- Possiamo vedere infatti librerie critiche come “kernel32.dll” o “sysmain.sdb” e come ultima azione un richiamo al processo ed eseguibile svchost.exe, un processo “generico” di windows e componente centrale del sistema operativo, dato che ha un ruolo fondamentale e di primo piano nella gestione di vari aspetti legati al funzionamento del sistema stesso. Questo processo è spesso e volentieri usato per mascherare altri processi da parte di molti autori di malware.

16.36...	Malware_U3_...	1080	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
16.36...	svchost.exe	1064	QueryNameInfo...	C:\WINDOWS\system32\svchost.exe	SUCCESS	Name: \WINDOW...
16.36...	svchost.exe	1064	QueryNameInfo...	C:\WINDOWS\system32\svchost.exe	SUCCESS	Name: \WINDOW...
16.36...	svchost.exe	1064	CreateFile	C:\WINDOWS\Prefetch\SVCHOST.EX...	SUCCESS	Desired Access: G...
16.36...	svchost.exe	1064	QueryStandardl...	C:\WINDOWS\Prefetch\SVCHOST.EX...	SUCCESS	AllocationSize: 20...
16.36...	svchost.exe	1064	ReadFile	C:\WINDOWS\Prefetch\SVCHOST.EX...	SUCCESS	Offset: 0, Length: 1...
16.36...	svchost.exe	1064	CloseFile	C:\WINDOWS\Prefetch\SVCHOST.EX...	SUCCESS	

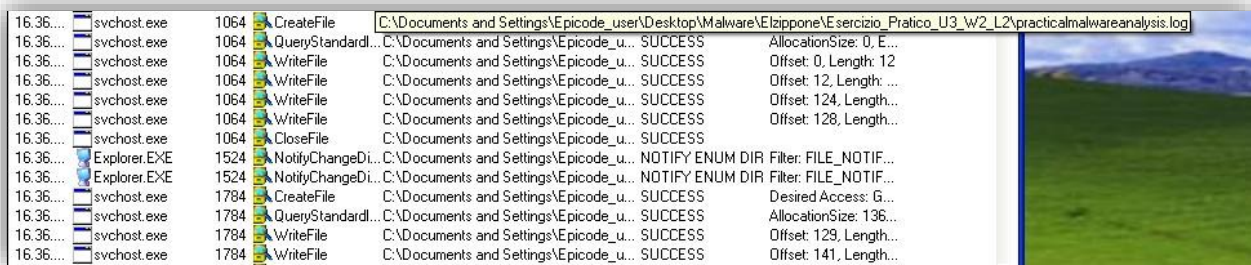
- Possiamo notare come l'ultima azione del file "Malware_U3_W2_L2" sia la chiamata e chiusura dell'eseguibili di svchost.exe e successivamente l'entrata in funzione dell'omonimo processo.

16.36...	svchost.exe	1064	CreateFileMapp...	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTy...
16.36...	svchost.exe	1064	CreateFile	C:\WINDOWS\system32\SHELL32.dll...	NAME NOT FOUND	Desired Access: G...
16.36...	svchost.exe	1064	CreateFile	C:\WINDOWS\system32\SHELL32.dll...	NAME NOT FOUND	Desired Access: G...
16.36...	csrss.exe	620	CreateFile	C:\WINDOWS\WinSxS\Policies\x86_P...	NAME NOT FOUND	Desired Access: R...
16.36...	csrss.exe	620	CreateFile	C:\WINDOWS\Assembly\GAC\Policy.6...	PATH NOT FOUND	Desired Access: R...

- Continuando ad analizzare i processi, notiamo che viene richiamato anche il processo "csrss.exe" altro processo di Windows cioè "Client Server Runtime Subsystem" utilizzato per caricare diverse DLL.

16.36...	svchost.exe	1064	QueryStandardl...	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	AllocationSize: 4.0...
16.36...	svchost.exe	1064	CreateFile	C:\WINDOWS\WindowsShell.Config	NAME NOT FOUND	Desired Access: G...
16.36...	csrss.exe	620	QueryBasicInfor...	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	CreationTime: 15/0...
16.36...	csrss.exe	620	QueryBasicInfor...	C:\WINDOWS\WindowsShell.Manifest	SUCCESS	CreationTime: 15/0...

Altre azioni perpetrate dai due processi sotto controllo del malware sono nel path "C:\Windows\WindowsShell.Manifest", un importante componente per garantire che la shell di Windows e le applicazioni correlate funzionino correttamente e con le giuste dipendenze.



Process	PID	Action	Path	Result	Details
svchost.exe	1064	CreateFile	C:\Documents and Settings\Epicode_user\Desktop\Malware\EIzippone\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log		
svchost.exe	1064	QueryStandard...	C:\Documents and Settings\Epicode_u...	SUCCESS	AllocationSize: 0, E...
svchost.exe	1064	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 0, Length: 12
svchost.exe	1064	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 12, Length: ...
svchost.exe	1064	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 124, Length...
svchost.exe	1064	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 128, Length...
svchost.exe	1064	CloseFile	C:\Documents and Settings\Epicode_u...	SUCCESS	
svchost.exe	1524	NotifyChangeDi...	C:\Documents and Settings\Epicode_u...	NOTIFY ENUM DIR Filter: FILE_NOTIF...	
svchost.exe	1524	NotifyChangeDi...	C:\Documents and Settings\Epicode_u...	NOTIFY ENUM DIR Filter: FILE_NOTIF...	
svchost.exe	1784	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: G...
svchost.exe	1784	QueryStandard...	C:\Documents and Settings\Epicode_u...	SUCCESS	AllocationSize: 136...
svchost.exe	1784	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 129, Length...
svchost.exe	1784	WriteFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Offset: 141, Length...

- Seguendo le azioni del file, arriviamo al path dove è contenuto l'eseguibile del malware, dove viene creato il file "practicalmalwareanalysis.log".



```

[Window: C:\Documents and settings\Epicode_user\desktop\Malware\EIzippone\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe]
a
[Window: C:\Documents and settings\Epicode_user\desktop\Malware\EIzippone\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe]
a
[Window: Esercizio_Pratico_U3_W2_L2]
n
[Window: Esercizio_Pratico_U3_W2_L2]
nddrreeaa ssccllaattttttttttt ssooonnoo 11oo aannddrreeaa

```

- Apriamo il file notepad, e vediamo che il file contiene dei caratteri registrati dalla nostra tastiera e si rivela quindi essere un **KEYLOGGER**.

CONCLUSIONI

Il file eseguibile nella cartella «Esercizio_Pratico_U3_W2_L2» si è rivelato essere un keylogger dopo l'analisi dinamica basica. Un keylogger è un tipo di malware progettato per registrare e monitorare le attività di input dell'utente, come tasti premuti sulla tastiera. Le azioni rilevate tramite Process Monitor includono:

- Azioni sul file system: Il malware ha creato un file di log e archiviato dati raccolti in file temporanei o nascosti nel sistema.
- Azioni su processi e thread: Il malware ha interagito con processi e thread per avviare, monitorare o nascondere la sua attività.