



Esercizio S10-L2



Traccia:

Nella lezione teorica del mattino, 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.

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






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

Svolgimento

Per lo svolgimento di questo esercizio ci serviremo della macchina virtuale fornita e degli strumenti in essa contenuti.

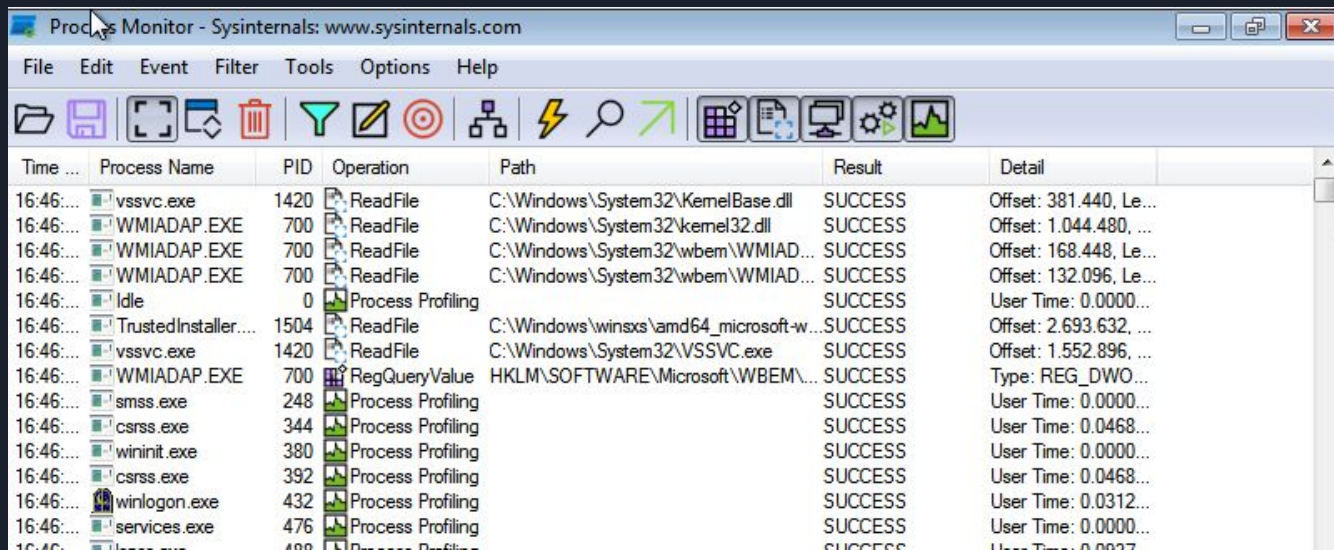
Per prima cosa avviamo la macchina e spostiamoci nella cartella Procmon, questa cartella contiene il programma Process Monitor, che useremo per tracciare i processi attivi quando avvieremo il malware.

Facciamo dunque partire il programma Procmon64.

 Eula	06/02/2024 11:50	Documento di testo	8 KB
 procmon	06/02/2024 11:50	File della Guida H...	63 KB
 Procmon	06/02/2024 11:50	Applicazione	4.716 KB
 Procmon64	06/02/2024 11:50	Applicazione	2.444 KB
 Procmon64a	06/02/2024 11:50	Applicazione	2.488 KB

Svolgimento

Procmon comincerà a catturare i processi non appena si apre. Dopo aver aperto Procmon avviamo anche il malware U3_W2_L2 e aspettiamo un minuto così che procmon catturi tutti i processi del malware, passato un minuto possiamo interrompere la cattura premendo sul pulsante a forma di cornice in alto a sinistra.

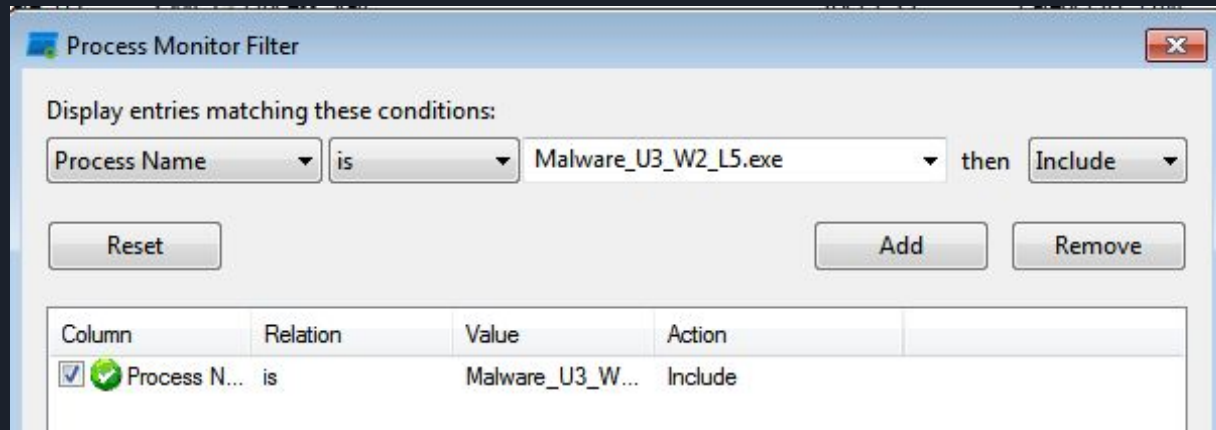


Time ...	Process Name	PID	Operation	Path	Result	Detail
16:46:...	vssvc.exe	1420	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 381.440, Le...
16:46:...	WMIADAP.EXE	700	ReadFile	C:\Windows\System32\kernel32.dll	SUCCESS	Offset: 1.044.480, ...
16:46:...	WMIADAP.EXE	700	ReadFile	C:\Windows\System32\wbem\WMIAD...	SUCCESS	Offset: 168.448, Le...
16:46:...	WMIADAP.EXE	700	ReadFile	C:\Windows\System32\wbem\WMIAD...	SUCCESS	Offset: 132.096, Le...
16:46:...	Idle	0	Process Profiling		SUCCESS	User Time: 0.0000...
16:46:...	TrustedInstaller...	1504	ReadFile	C:\Windows\winsxs\amd64_microsoft-w...	SUCCESS	Offset: 2.693.632, ...
16:46:...	vssvc.exe	1420	ReadFile	C:\Windows\System32\VSSVC.exe	SUCCESS	Offset: 1.552.896, ...
16:46:...	WMIADAP.EXE	700	RegQueryValue	HKLM\SOFTWARE\Microsoft\WBEM\...	SUCCESS	Type: REG_DWO...
16:46:...	smss.exe	248	Process Profiling		SUCCESS	User Time: 0.0000...
16:46:...	csrss.exe	344	Process Profiling		SUCCESS	User Time: 0.0468...
16:46:...	wininit.exe	380	Process Profiling		SUCCESS	User Time: 0.0000...
16:46:...	csrss.exe	392	Process Profiling		SUCCESS	User Time: 0.0468...
16:46:...	winlogon.exe	432	Process Profiling		SUCCESS	User Time: 0.0312...
16:46:...	services.exe	476	Process Profiling		SUCCESS	User Time: 0.0000...
16:46:...	...	488	Process Profiling		SUCCESS	User Time: 0.0037...

Svolgimento:

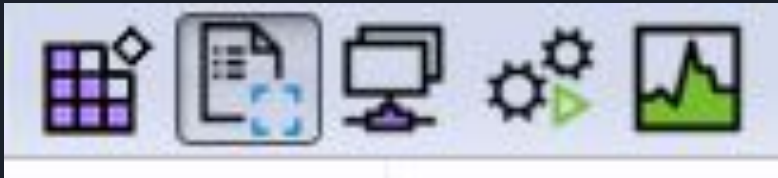
Dopo aver interrotto la cattura andiamo nella sezione Filter e modifichiamola per mostrare solo i processi del malware, per fare ciò eliminiamo tutti i filtri presenti e ne aggiungiamo uno come mostrato in figura.

Questo filtro dice al programma di mostrare solamente i processi avviati dal malware e di non mostrare tutti gli altri processi.



Svolgimento:





















Ci viene richiesto di analizzare in particolare i processi che il malware crea e che vanno ad interagire col file system, per fare questo aggiungiamo ulteriori filtri al programma deselezionando i 5 riquadri in alto a destra e mantenendo selezionato il secondo, che appunto mostra i processi che coinvolgono il file system.



Come possiamo osservare questi processi mostrano come il malware è andato ad aprire, leggere, modificare diversi file contenuti all'interno della macchina.

16:59:...	Malware_U3_...	2904	QueryOpen	C:\Users\Windows\AppData\Local\Mic...FAST IO DISALLO...	
16:59:...	Malware_U3_...	2904	CreateFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	Desired Access: R...
16:59:...	Malware_U3_...	2904	QueryBasicInfor...	C:\Users\Windows\AppData\Local\Mic...SUCCESS	CreationTime: 05/0...
16:59:...	Malware_U3_...	2904	CloseFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	
16:59:...	Malware_U3_...	2904	IRP_MJ_CLOSE	C:\Users\Windows\AppData\Local\Mic...SUCCESS	
16:59:...	Malware_U3_...	2904	QueryOpen	C:\Users\Windows\AppData\Local\Mic...FAST IO DISALLO...	
16:59:...	Malware_U3_...	2904	CreateFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	Desired Access: R...
16:59:...	Malware_U3_...	2904	QueryBasicInfor...	C:\Users\Windows\AppData\Local\Mic...SUCCESS	CreationTime: 05/0...
16:59:...	Malware_U3_...	2904	CloseFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	
16:59:...	Malware_U3_...	2904	IRP_MJ_CLOSE	C:\Users\Windows\AppData\Local\Mic...SUCCESS	
16:59:...	Malware_U3_...	2904	QueryOpen	C:\Users\Windows\AppData\Local\Mic...FAST IO DISALLO...	
16:59:...	Malware_U3_...	2904	CreateFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	Desired Access: R...
16:59:...	Malware_U3_...	2904	QueryBasicInfor...	C:\Users\Windows\AppData\Local\Mic...SUCCESS	CreationTime: 05/0...
16:59:...	Malware_U3_...	2904	CloseFile	C:\Users\Windows\AppData\Local\Mic...SUCCESS	

Selezionando il quarto pulsante in alto a destra verranno messi in risalto le azioni relative ai processi ed ai thread, in questa schermata possiamo vedere come il malware abbia tentato con successo di caricare varie librerie che hanno garantito il funzionamento del malware e lo svolgimento delle operazioni che era programmato a svolgere.

16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\System32\wow64win.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\System32\kernel32.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\System32\kernel32.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\System32\user32.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS
16:59:...		Malware_U3_...	2904		Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS



Considerazioni finali

Possiamo ipotizzare quindi che il nostro malware quando viene eseguito cerca prima di camuffarsi creando un nuovo processo chiamato «svchost.exe», poi lancia la sua principale funzionalità ovvero un keylogger che salva i caratteri digitati dall'utente nel file «practicalmalwareanalysis» creato appositamente nella cartella dove si trova l'eseguibile.