ESERCIZIO W21D1 PARTE 2

Nella seconda fase di pratica, analizzeremo il malware usando un altro tool: Multimon.

Traccia

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 multimon https://www.resplendence.com/multimon
- Identificare eventuali altre azioni del malware
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Dati raccolti

Errori di applicazione in fase di esecuzione

29/03/2024 15:10:20....	Active Window ...	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	Active Window ...	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	Active Window ...	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Alert	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Alert	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Alert	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	Dialog Start	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	Dialog Start	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	Dialog Start	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Sound	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Sound	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:20....	System Sound	csrss.exe	(772,356)		svchost.exe - Errore di applicazione
29/03/2024 15:10:21	Dialog End	explorer.exe	(814,380)		ShellView

Tasti premuti sulla tastiera

29/03/2024 15:11:31....	0xFF IRP_MJ_...	System	00000000 STATUS_SUCC...	C:\Windows\Media\Windows Ding.wav	MiniFilter	0x00	0x40	0x00000...	4
29/03/2024 15:11:31....	0xFE IRP_MJ_...	System	00000000 STATUS_SUCC...	C:\Windows\Media\Windows Ding.wav	MiniFilter	0x00	0x31	0x00000...	4
29/03/2024 15:11:31....	0x02 IRP_MJ_...	System	00000000 STATUS_SUCC...	C:\Windows\Media\Windows Ding.wav	Irp	0x00	0x00	0x00000...	4