

Utilizzando il tool Procmon andiamo ad analizzare il comportamento del malware stimando la tipologia a cui appartiene.

Event	Process	Stack
Date:	8/1/2023 4:37:54.4439391 PM	
Thread:	788	
Class:	File System	
Operation:	CreateFile	
Result:	SUCCESS	
Path:	C:\WINDOWS\system32\ctype.nls	
Duration:	0.0000145	
Desired Access:	Read Data/List Directory, Read Attributes	
Disposition:	Open	
Options:	Non-Directory File	
Attributes:	N	
ShareMode:	Read, Write, Delete	
AllocationSize:	n/a	
OpenResult:	Opened	

Analizzando alcune delle proprietà evento vediamo che il malware richiede l'accesso alla lettura e scrittura dei file e alle cartelle del sistema.

Senza scendere nel dettaglio degli stack, leggiamo tra gli eventi un altro processo sospetto

Event	Process	Stack
Date:	8/1/2023 4:37:54.4616196 PM	
Thread:	788	
Class:	File System	
Operation:	CreateFile	
Result:	SUCCESS	
Path:	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	
Duration:	0.0000142	
Desired Access:	Execute/Traverse, Synchronize	
Disposition:	Open	
Options:	Directory, Synchronous IO Non-Alert	
Attributes:	n/a	
ShareMode:	Read, Write	
AllocationSize:	n/a	
OpenResult:	Opened	

Nella stessa cartella il malware ha creato un file di testo che andiamo ad aprire.

```
[window: Process Monitor Filter]
u30 [ENTER]
[window: Find]

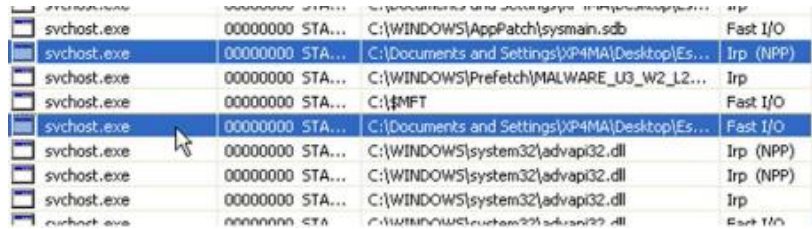
[window: Find]
mmaa11aaBACKSPACE BACKSPACE wwaarree0 [ENTER] 0 [ENTER]
[window: Esercizio_Pratico_U3_W2_L5]

[window: Esercizio_Pratico_U3_W2_L5]

[window: Esercizio_Pratico_U3_W2_L5]
ccc
```

Il contenuto del file di testo dovrebbe far presupporre che si tratti di un logger, ovvero una tipologia di malware che registra tutto ciò che viene scritto dall'utente andando anche a "mappare" dove lo si è scritto, in modo tale da conservare le credenziali o informazioni personali della vittima.

Ulteriori conferme circa il comportamento vengono date dal tool Multimon



The screenshot shows the Multimon tool interface with a list of system events. The events are filtered to show only those involving 'svchost.exe'. The table has four columns: Process Name, PID, Operation, and Path. The operations include 'Fast I/O', 'Irp (NPP)', and 'Irp'. The paths include system files like 'sysmain.sdb', 'advapi32.dll', and user-specific paths like 'C:\Documents and Settings\XP4MA\Desktop\Es...'. A mouse cursor is pointing at the fourth row of the table.

Process Name	PID	Operation	Path
svchost.exe	00000000	STA...	C:\WINDOWS\AppPatch\sysmain.sdb
svchost.exe	00000000	STA...	C:\Documents and Settings\XP4MA\Desktop\Es...
svchost.exe	00000000	STA...	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2...
svchost.exe	00000000	STA...	C:\MFT
svchost.exe	00000000	STA...	C:\Documents and Settings\XP4MA\Desktop\Es...
svchost.exe	00000000	STA...	C:\WINDOWS\system32\advapi32.dll
svchost.exe	00000000	STA...	C:\WINDOWS\system32\advapi32.dll
svchost.exe	00000000	STA...	C:\WINDOWS\system32\advapi32.dll
svchost.exe	00000000	STA...	C:\WINDOWS\system32\advapi32.dll