ANALISI DINAMICA

identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon) oppure se ci sono problemi multimonhttps://www.resplendence.com/multimon https://multimon.it.uptodown.com/windows/download/23982versione 2.5 per XP

• Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor

• Modifiche del registro dopo il malware (le differenze)

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

Le azioni che possiamo notare effettuate dal malware sono la creazione di un file di testo.

Grazie al **Process Monitor** abbiamo settato nel filtro il nome del malware e ci ha riportato il percorso con la rispettiva creazione del file come vediamo nell’immagine seguente

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedcome vediamo il malware ha creato un file di testo che legge tutto quello che scriviamo da tastiera,

**il Malware un questione è un keylogger**.

Che cos’è il nome del processo SVChost.exe

Microsoft definisce SVCHost.exe un processo di sistema generico di Windows, che può ospitare uno o più servizi del sistema operativo, molto spesso essenziali al funzionamento del computer.

In passato, SVCHost.exe è stato un nome spesso sfruttato da autori di malware per realizzare dei file malevoli in grado di “nascondersi” all’interno dei numerosi servizi di Windows per agire più o meno indisturbati.

Le azioni del malware sono molteplici una come evidenziata in precedenza è proprio la creazione del file

A screenshot of a computer

Description automatically generated

La foto precedentemente riportata è uno screen fatto da regshot, è il compare fatto da screenshot 1 (prima dell’avvio del malware) e screenshot 2 (fatto appena dopo l’avvio del malware).

Per verificare la correlazione come visto in precedenza basta seguire il percorso del file, aprirlo e notare come come qualsiasi cosa scritta da tasiera venga riportata

A screenshot of a computer

Description automatically generated