Analisi Dinamica Basica

L'analisi dinamica basica si riferisce a un tipo di valutazione e studio di un Malware sul loro comportamento e le varie azioni che intervengono su un sistema.

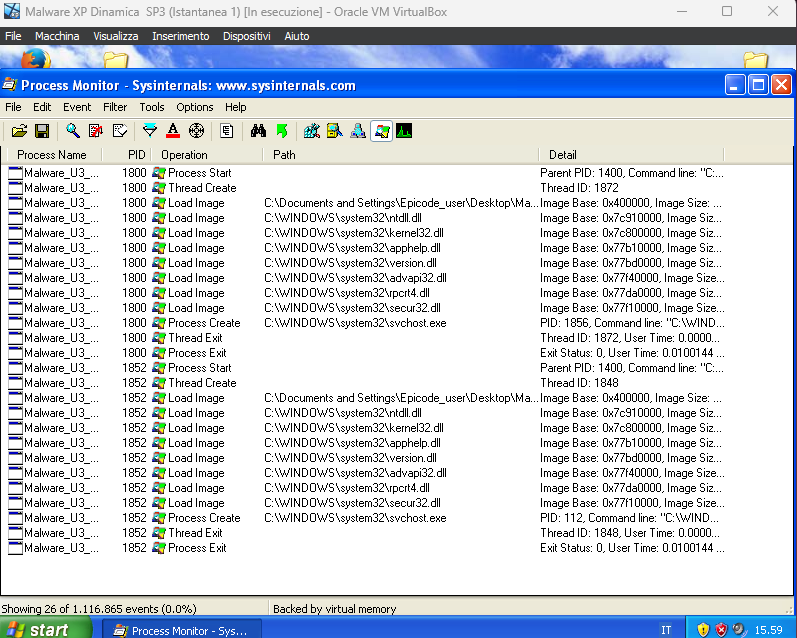
In generale, l'analisi dinamica considera il sistema in movimento, testando l’esecuzione del malware in un laboratorio protetto.

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Con l’utilizzo del tool Process Explorer durante l’avvio del malware si vede l’immediata creazione di questi due processi malevoli ‘‘camuffati’’ come generici processi del sistema operativo con il nome di ‘’svchost.exe’’.

Utilizzando il tool Process Monitor, filtrando i processi che si creano e i trhead, si può vedere come il malware crei dei nuovi processi eseguendoli ed importa innumerevoli moduli e librerie.



Dopo un’attenta analisi di questi processi, utilizzando come filtro i nuovi PID che andava a creare il malware, abbiamo constatato la creazione di un file .txt con l’utilizzo del ‘’Notepad’’.

Seguendo il percorso path della creazione di questo file txt possiamo capire dov’è posto quest’ultimo e scopriamo che questo file non sia altro che un registro che tiene traccia di tutte le nostre azioni.

Questo tipo di malware si chiama keylogger che è un tipo di software dannoso progettato per registrare e memorizzare le informazioni digitate sulla tastiera di un computer o di un dispositivo.

Inoltre, il malware sicuramente cercherà di inviare questi dati al dispositivo dell’attaccante in modo da raccogliere informazioni sensibili, come password, dati finanziari, informazioni personali e altro ancora.

