**INTRODUZIONE ALL'ANALISI DEI MALWARE**

**Cos'è un malware**

Il termine "malware" è una combinazione delle parole "malicious" (malizioso) e "software", e si riferisce a qualsiasi tipo di software progettato per danneggiare o prendere il controllo di un sistema informatico. Ci sono diversi tipi di malware, tra cui virus, worm, trojan, adware, spyware, dialer, keylogger, backdoor, rootkit, bootkit, botnet e ransomware. Ognuno di questi tipi di malware ha un obiettivo diverso, ma tutti possono causare danni finanziari o operativi ai sistemi informatici.

**I registri di Windows**

I registri di Windows sono una parte fondamentale del sistema operativo Microsoft Windows e contengono informazioni importanti sulle impostazioni e le attività del sistema. I malware possono sfruttare i registri di Windows per ottenere informazioni sensibili, modificare le impostazioni del sistema o persino eseguire codice dannoso. Ad esempio, un malware può inserire una chiave di registro per avviarsi automaticamente all'avvio del sistema, rendendo difficile la sua rimozione.

**MsfVenom**

MsfVenom è uno strumento di hacking incluso nel framework Metasploit, utilizzato principalmente per creare malware personalizzati. Con MsfVenom, gli hacker possono generare payload (carichi utili) che possono essere utilizzati per sfruttare vulnerabilità nei sistemi informatici e ottenere l'accesso non autorizzato. Questo strumento è spesso utilizzato per creare trojan e backdoor, che possono essere utilizzati per infiltrarsi nei sistemi e rubare informazioni sensibili. Tuttavia, MsfVenom può anche essere utilizzato per scopi legittimi, come testare la sicurezza dei sistemi informatici e sviluppare contromisure per proteggerli dai malware.

**Virus**

I virus sono uno dei tipi di malware più conosciuti e diffusi. Si diffondono attraverso file eseguibili e richiedono l'attivazione umana per propagarsi. Ciò significa che un utente deve eseguire il file infetto per permettere al virus di replicarsi e diffondersi ad altri sistemi. Una volta attivato, il virus può causare danni al sistema, come la cancellazione di file o la corruzione dei dati.

**Worm**

I worm sono un altro tipo di malware che si diffonde rapidamente attraverso le reti informatiche. A differenza dei virus, i worm sono autonomi e non richiedono l'attivazione umana per replicarsi. Sfruttano le vulnerabilità dei sistemi per diffondersi e possono causare danni significativi, come il rallentamento delle prestazioni del sistema o la saturazione della rete.

**Adware**

Gli adware sono programmi progettati per mostrare annunci pubblicitari sul computer dell'utente. Possono essere integrati in altre applicazioni o installati separatamente e spesso monitorano le attività di navigazione dell'utente per mostrare pubblicità mirate. Sebbene non siano sempre dannosi, possono compromettere la privacy dell'utente e rallentare le prestazioni del sistema.

**Spyware**

Gli spyware sono programmi maligni che raccolgono informazioni sulle attività degli utenti senza il loro consenso. Possono raccogliere una vasta gamma di dati, come siti web visitati, password, informazioni finanziarie e altre informazioni personali e sensibili. Queste informazioni vengono poi utilizzate per scopi malevoli, come il furto d'identità o le frodi finanziarie.

**Trojan Horse**

I Trojan Horse sono un tipo di malware che si presenta come un software legittimo o utile per indurre gli utenti a installarlo ed eseguirlo. Una volta installato, il Trojan può eseguire una serie di azioni dannose senza il consenso dell'utente, come il furto di informazioni, la creazione di backdoor per il controllo remoto del sistema o l'installazione di altri tipi di malware. Possono anche essere utilizzati come "zombie" per eseguire attacchi distribuiti di negazione del servizio (DDoS).

**Dialer**

I dialer sono programmi che utilizzano il modem del computer per chiamare numeri telefonici a pagamento senza il consenso dell'utente. Anche se meno comuni oggi a causa dell'uso diffuso delle connessioni internet a banda larga, possono ancora rappresentare una minaccia per chi utilizza connessioni telefoniche. Possono generare costi elevati per l'utente e causare problemi finanziari.

**Keylogger**

I keylogger sono un tipo di spyware progettato per registrare ogni tasto premuto sulla tastiera della vittima. Possono catturare testi digitati, credenziali di accesso, messaggi di chat, email e altre informazioni sensibili. Queste informazioni vengono poi inviate a un server controllato dall'attaccante e possono essere utilizzate per scopi malevoli, come il furto d'identità o l'accesso non autorizzato a reti e sistemi.

**Backdoor**

Le backdoor sono programmi che consentono l'accesso non autorizzato a un sistema informatico, spesso bypassando le normali misure di sicurezza. Sono composte da due componenti principali: un server installato sulla macchina della vittima e un client eseguito sulla macchina dell'attaccante. Una volta stabilita la connessione, l'attaccante può eseguire comandi, trasferire file e controllare il sistema a distanza. Le backdoor possono essere utilizzate per scopi malevoli, come il furto di informazioni o l'esecuzione di attacchi informatici.

**Rootkit**

I rootkit sono un tipo di malware avanzato progettato per ottenere e mantenere l'accesso privilegiato a un sistema informatico. Possono modificare il sistema operativo e i suoi componenti per evitare il rilevamento e rimanere nascosti agli utenti e ai software di sicurezza. Le funzionalità tipiche di un rootkit includono la capacità di nascondere processi e file, modificare le impostazioni di sicurezza e creare backdoor per il controllo remoto del sistema. Possono essere utilizzati per scopi malevoli, come il furto di informazioni o l'accesso non autorizzato a reti e sistemi.

**Tipi di malware**

I malware sono programmi malevoli progettati per danneggiare o controllare un sistema informatico senza il consenso dell'utente. Esistono diversi tipi di malware, ognuno con caratteristiche e scopi diversi. Tra i più comuni troviamo i rootkit, i bootkit, le botnet e i ransomware.I rootkit sono un tipo di malware che si insinua nel kernel del sistema operativo per ottenere privilegi elevati e controllo completo del sistema. Possono essere difficili da rilevare e rimuovere poiché agiscono a un livello molto basso del sistema.I bootkit sono una variante dei rootkit che si installano nella fase di avvio del sistema, prima che il sistema operativo venga completamente caricato. Questo li rende particolarmente pericolosi poiché possono aggirare molte delle misure di sicurezza del sistema operativo.Le botnet sono reti di computer compromessi, controllati da un attaccante remoto, che possono essere utilizzate per eseguire attività dannose come attacchi DDOS, invio di spam, furto di informazioni e distribuzione di malware aggiuntivo.I ransomware sono un tipo di malware che cifra i file del sistema e richiede un riscatto per fornire la chiave di decrittazione necessaria per ripristinare l'accesso ai file. Sono spesso distribuiti tramite campagne di phishing o sfruttando vulnerabilità nei sistemi.

**Il Registro di Windows**

Il Registro di Windows è un database gerarchico che contiene le impostazioni e le configurazioni del sistema operativo e delle applicazioni installate. È diviso in diverse sezioni, chiamate "Hive", che contengono informazioni specifiche.Le sezioni dei registri più importanti sono HKEY\_CURRENT\_USER, che contiene le impostazioni dell'utente corrente, HKEY\_LOCAL\_MACHINE, che contiene le impostazioni del sistema, e HKEY\_CLASSES\_ROOT, che contiene le informazioni sulle estensioni dei file e le applicazioni associate.I malware spesso utilizzano i registri di Windows per nascondersi e persistere nel sistema. Possono modificare le chiavi e i valori dei registri per avviarsi automaticamente all'avvio del sistema o per evitare la rilevazione da parte degli strumenti di sicurezza.Le API di Windows (Application Programming Interface) sono un insieme di funzioni e procedure che consentono alle applicazioni di interagire con il sistema operativo. I malware possono utilizzare queste API per eseguire operazioni dannose, come l'installazione di altri malware o la modifica delle impostazioni del sistema.Le funzioni e i tipi di dati dei registri di Windows sono importanti per comprendere come i malware possono manipolare le impostazioni del sistema. Ad esempio, possono utilizzare le funzioni di lettura e scrittura per modificare le chiavi e i valori dei registri, mentre i tipi di dati come le stringhe e i numeri possono essere utilizzati per memorizzare informazioni utili per il funzionamento del malware.Il networking e i processi di Windows sono anche importanti per i malware, poiché possono utilizzare le funzioni di rete per comunicare con server remoti e scaricare ulteriori componenti dannosi. Inoltre, possono creare nuovi processi per eseguire operazioni dannose senza essere rilevati dagli utenti. È quindi fondamentale monitorare attentamente i processi e le attività di rete per individuare eventuali attività sospette.

**Struttura dei registri**

I registri di Windows sono un elemento fondamentale del sistema operativo, in quanto contengono tutte le informazioni necessarie per far funzionare il computer e le applicazioni. La loro struttura è organizzata in una forma gerarchica a forma di albero, composta da chiavi e valori. Le chiavi possono essere paragonate alle cartelle del file system, in quanto possono contenere altre chiavi o valori. I valori, invece, sono le informazioni effettive memorizzate all'interno delle chiavi, ognuna con un nome e dei dati associati. Un esempio di struttura dei registri potrebbe essere HKEY\_LOCAL\_MACHINE (HKLM) - Software - Microsoft - Windows - CurrentVersion - Run. In questo caso, la chiave "Run" contiene i valori relativi ai programmi che vengono avviati automaticamente all'avvio del sistema.

**Utilizzo dei registri**

I registri di Windows sono utilizzati per salvare le configurazioni e le impostazioni del sistema operativo e delle applicazioni. Ad esempio, per personalizzare lo sfondo del desktop, Windows salva la nuova impostazione nel registro di Windows. Inoltre, i registri sono suddivisi in diverse chiavi principali, tra cui HKEY\_LOCAL\_MACHINE (HKLM), HKEY\_CURRENT\_USER (HKCU), HKEY\_CLASSES\_ROOT (HKCR), HKEY\_USERS (HKU) e HKEY\_CURRENT\_CONFIG (HKCC). Ogni chiave ha un ruolo specifico e contiene informazioni importanti per il funzionamento del sistema. Alcuni esempi pratici di utilizzo dei registri potrebbero essere la modifica delle preferenze del browser web, come la home page di Internet Explorer, o la configurazione dei servizi di sistema.

**Utilizzo dei registri da parte dei malware**

Purtroppo, i registri di Windows possono essere sfruttati anche da malware per compiere azioni dannose. Uno dei modi in cui i malware utilizzano i registri è attraverso la persistenza, ovvero la capacità di riavviarsi automaticamente all'accensione del computer. Per fare ciò, i malware modificano le chiavi di registro che gestiscono l'avvio automatico dei programmi, come ad esempio HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Inoltre, i malware possono anche cambiare le impostazioni di sistema per disabilitare antivirus o firewall, sfruttando ad esempio la chiave HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services. Un esempio concreto di utilizzo dei registri da parte di un malware potrebbe essere l'aggiunta di una voce nella chiave di registro Run, che permette al malware di essere eseguito automaticamente all'avvio del sistema, senza che l'utente se ne accorga. È quindi importante prestare attenzione ai cambiamenti nei registri e mantenere sempre aggiornato il proprio sistema operativo per evitare l'insorgere di malware.

**API per i Registri**

Le API per i Registri di Windows sono un insieme di funzioni utilizzate esclusivamente per interagire con il registro di Windows. Questo è un componente fondamentale del sistema operativo che contiene informazioni importanti per il funzionamento del computer, come le impostazioni di sistema, le informazioni di configurazione e le preferenze degli utenti.Una delle operazioni più comuni che possono essere eseguite utilizzando le API per i Registri è la creazione di nuove chiavi e valori di registro. Queste chiavi e valori possono essere utilizzati per memorizzare informazioni specifiche, come ad esempio le impostazioni di un programma o le preferenze di un utente.Alcune delle funzioni API comuni in questa categoria includono RegCreateKeyEx, che viene utilizzata per creare o aprire una chiave di registro, e RegSetValueEx, che viene utilizzata per impostare un valore all'interno di una chiave di registro. Altre funzioni utili includono RegOpenKeyEx, RegGetValue, RegDeleteKey e RegDeleteValue, che consentono rispettivamente di aprire una chiave di registro esistente, recuperare i dati associati a una chiave, eliminare una chiave di registro e eliminare un valore da una chiave di registro.Le API per i Registri sono fondamentali per molti programmi legittimi, ma possono anche essere utilizzate da malware per modificare le impostazioni di sistema o per nascondere la propria presenza. Per questo motivo, è importante utilizzare queste funzioni con cautela e solo quando necessario.

**API per il File System e Altri Componenti**

Le API per il File System e Altri Componenti sono un insieme di funzioni utilizzate per interagire con il file system e altri componenti del sistema operativo, come dispositivi di input/output. Queste API consentono di eseguire operazioni comuni come la creazione, la lettura, la scrittura e la cancellazione di file e directory.Una delle funzioni più utilizzate in questa categoria è CreateFile, che viene utilizzata per creare o aprire un file, una pipe, un dispositivo di I/O o una directory. Altre funzioni importanti includono ReadFile e WriteFile, che consentono rispettivamente di leggere dati da un file e di scriverli.Le API per il File System e Altri Componenti sono fondamentali per molti programmi legittimi, ma possono anche essere utilizzate da malware per eseguire operazioni dannose, come la creazione di file dannosi o la modifica di file di sistema. Per questo motivo, è importante utilizzare queste funzioni con cautela e solo quando necessario.

**Cos'è un Virus Polimorfo**

Un virus polimorfo è un tipo di malware che utilizza tecniche di codifica e decodifica per modificare il proprio aspetto e rendere più difficile la sua identificazione da parte dei software di sicurezza. Questo tipo di virus è composto da una routine di decodifica, che può variare ogni volta che il virus si propaga, e una routine di codifica, che applica trasformazioni al corpo del virus per modificarne l'aspetto. Un esempio pratico di come funziona un virus polimorfo è il seguente: quando il virus infetta un file eseguibile, codifica il proprio corpo utilizzando un algoritmo di codifica e inserisce la routine di decodifica e il corpo codificato nel file infetto. Quando il file viene eseguito, la routine di decodifica decodifica il corpo del virus, che esegue la sua funzione dannosa e cerca nuovi file da infettare.

**Utilizzo di msfvenom per creare un Virus Polimorfo**

Msfvenom è uno strumento utilizzato per creare payload polimorfici, ovvero codici malevoli difficili da rilevare per gli antivirus. Per creare un payload polimorfico con msfvenom, è possibile utilizzare diversi encoders e numerose iterazioni per ricodificare il payload grezzo. Ad esempio, si può utilizzare l'encoder shikata\_ga\_nai per 100 iterazioni per creare un payload Meterpreter con una connessione inversa TCP, e successivamente ricodificare il payload utilizzando l'encoder countdown per 200 iterazioni. Infine, si può applicare un'ulteriore ricodifica con shikata\_ga\_nai per 138 iterazioni e salvare il risultato finale come polimorficommm.exe.

**Finalità del Comando**

L'obiettivo principale del comando descritto nel testo iniziale è creare un payload polimorfico che sia difficile da rilevare per gli antivirus. Utilizzando più livelli di codifica con diversi encoders e numerose iterazioni, il payload finale cambia forma molte volte, rendendo più difficile per i software di sicurezza identificarlo come minaccia. Questo tipo di payload è spesso utilizzato da hacker e cyber criminali per diffondere malware e attaccare sistemi informatici. Grazie alla sua capacità di modificare il proprio aspetto, il payload polimorfico può eludere i sistemi di sicurezza e infettare i dispositivi senza essere rilevato. Tuttavia, grazie a strumenti come VirusTotal, è possibile analizzare file e URL sospetti per identificare eventuali minacce e proteggere i sistemi informatici.