4. MALWARE

Un malware (**ma**licious soft**ware**) è una sequenza di codice (o programma) nocivo che viene progettato per provocare intenzionalmente danni o alterare il normale comportamento di un sistema informatico e i dati in esso contenuti. Viene eseguito all'insaputa dell'utente. I danni provocati potrebbero essere irreversibili di conseguenza possono essere molto gravi.

Spesso vengono utilizzati meccanismi di offuscamento o di packing per rendere i malware difficili da rilevare ed analizzare: con i meccanismi di **offuscamento** si cerca di occultare l'esecuzione di un malware, con i meccanismi di **packing** si comprime (impacchetta) il programma malevolo. Entrambe le tecniche limitano significativamente la probabilità che il malware venga rilevato mediante alcune tipologie di analisi, ad esempio analisi statistica.

Un aspetto importante è che in generale i programmi legittimi (non malevole) includono generalmente molte stringhe che possono essere estratte in fase di analisi:

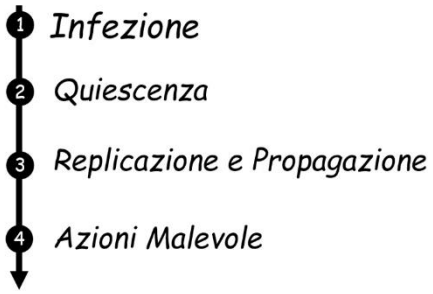
- Un malware compresso (meccanismo di packing) o offuscato contiene **pochissime** stringhe.
- Se in seguito dell'analisi di un programma vengono individuate poche stringhe, probabilmente il è compresso o offuscato (e **potrebbe** essere malevolo).

Un malware può avere vari obiettivi. Possiamo delineare delle macro categorie di obiettivi: rubare le credenziali della vittima (**maggiori dettagli al corso di Penetration and Hacking Test**), effettuare il dump delle informazioni archiviate nel S.O., registrare alcuni comportamenti della vittima (battiture di tasti, screenshot del S.O. , etc..).

In che modo viene eseguito un malware in un pc che possiede barriere protettive contro di essi? L'esecuzione del codice malevolo contenuto in un malware è possibile grazie a vari fattori: utenti inesperti, infrastrutture di rete deboli, falle nel sistema informatico, etc….. bisogna insomma cercare di avere un sistema operativo aggiornato, un buon antivirus aggiornato e comportarsi in maniera responsabile.

Dopo aver dato una panoramica sui malware, analizziamone il ciclo di vita (quali sono le fasi che caratterizzano la vita di un malware).

Le fasi sono 4: **Infezione, Quiescenza, Replicazione e Propagazione, Azioni malevole**.



Nella fase di **Infezione**, il malware penetra nel sistema superando eventuali difese quali antivirus, sistema operativo. I canali principali attraverso i quali avviene l'infezione sono: Web (e-mail…), dispositivi esterni (penne USB, HDD, SD card…) etc… maggiori dettagli ed esempi di Infezione al corso di Penetration and Hacking Test.

Nella fase di **Quiescenza,** il codice malevolo è memorizzato all'interno del sistema ma non è attivo. Per attivarsi attende che si verifichi una determinata condizione. Durante questa fase il malware è vulnerabile ad eventuali controlli anti-malware (tuttavia sono programmati per essere difficilmente individuabili).

Nella fase di **Replicazione e Propagazione**, il malware, al verificarsi di determinati eventi o condizioni, si replica e seleziona i bersagli su cui replicarsi (altri sistemi, etc…). Questa fase è tipica della maggior parte dei software malevoli.

La fase di **Azione Malevole** è caratterizzata dalla combinazione di numerose problematiche (furto di dati, file etc…) che tengono a generarsi a cascata. Vengono eseguite al verificarsi di determinati eventi o condizioni.

Vediamo le caratteristiche e le peculiarità dell'analisi dei Malware. Ci concentreremo sull'analisi statica e sull'analisi dinamica.

Analizzare un malware significa cercare di comprenderne il comportamento, al fine di:

- **Identificare** il malware.
- **Difendersi** dal malware.
- **Eliminare** il malware.
- **Sviluppare adeguate contromisure** verso il malware

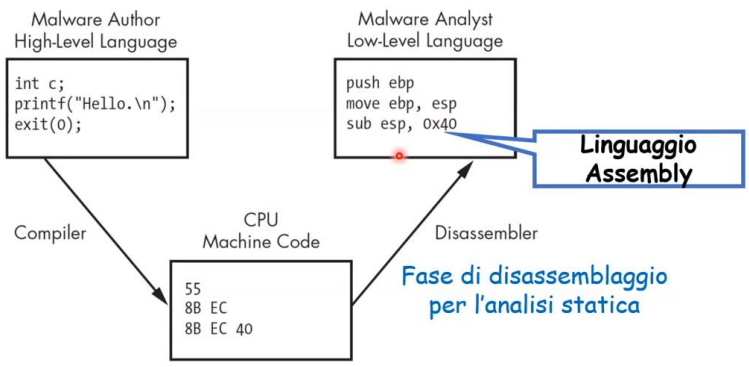
Durante l'analisi di un malware è necessario tener ben presente che si sta analizzando software dannoso e di conseguenza sono necessarie opportune precauzioni. In alcuni contesti è possibile effettuare un'infezione "controllata" al fine di reperire informazioni utili sul malware.

Esistono diverse metodologie per l'analisi di software malevolo: analisi **statica** e analisi **dinamica** che rappresentano due approcci diversi ma complementari, di solito infatti devono essere usati entrambi per un'analisi approfondita di un malware.

L'analisi **statica** definisce le metodologie per l'analisi del codice e della struttura di un malware, in pratico, osservo il codice e ne deduco mediante ragionamento logico, il comportamento in fase di esecuzione. Questo viene fatto per determinarne il suo funzionamento. Durante l'analisi statica il malware non viene eseguito. Da questa analisi si possono ottenere varie informazioni importanti. Queste informazioni possono essere ottenute mediante antivirus-anti-malware, utilizzando funzioni Hash etc…

I malware sono generalmente programmati mediante linguaggi di alto livello (il codice eseguito dalla CPU è generato dal compilatore). L'analisi dei malware viene di solito eseguita su linguaggi di bassi livello. Mediante **disassemblatori** è possibile generare codice assembly, tale codice può essere analizzato e compreso durante l'analisi statica.

Un esempio di disassemblatore è il seguente:



Veniamo ora all'analisi dinamica, di solito effettuata dopo quella statica. A differenza dell'analisi statica in cui il malware non viene eseguito, in questo caso è richiesta la sua esecuzione in particolare osservandone il comportamento in maniera analoga a quella che risulterebbe all'utente (infetto quindi un sistema in modo controllato). Mediante l'analisi dinamica è possibile ottenere informazioni riguardanti il funzionamento del malware in esame. Ad esempio analizzando un malware appartenente alla categoria dei KeyLogger è possibile individuare in quale file ed in che modo vengono memorizzate e trasmesse le informazioni. Naturalmente quando si effettua l'analisi dinamica è necessario procedere con attenzione. Una precauzione potrebbe essere quello di utilizzare un computer dedicato solo all'esecuzione del malware (quindi senza avere responsabilità su un'eventuale formattazione), oppure utilizzando una macchina virtuale.

Durante l'analisi dinamica si utilizzano strumenti di debugging, per analizzare step by step il comportamento del malware e la sua influenza nel sistema.

Esistono due approcci per l'analisi dinamica di un malware: **Black Box** e **White Box:**

L'approccio **Black** box si focalizza sull'analisi degli effetti derivanti dall'esecuzione del malware, senza soffermarsi sulla comprensione del comportamento e sui meccanismi che innescano effettivamente le attività malevole. Questo è un approccio "superficiale". Non vengono ottenute informazioni dettagliate ma ha il vantaggio di avere informazioni in tempi brevi ed è un'analisi poco dispendiosa.

A differenza dell'approccio Black Box, l'approccio **White** Box è più profondo. È necessario conoscere dettagli sulle caratteristiche e sul codice del malware in esame. Durante l'analisi White Box vengono analizzati tutti gli aspetti relativi all'esecuzione del malware. Vengono analizzati tutti quegli aspetti che conducono: dallo stato del sistema prima dell'infezione del malware, allo stato del sistema dopo l'esecuzione del malware stesso.

Per l'approccio White Box è necessario conoscere e comprendere il codice di esecuzione del malware, osservare il malware per un certo lasso di tempo. Possono essere usati strumenti quali debugger, editor, etc…