MALWARE ANALYSIS

CYBER SECURITY & ETHICAL HACKING

01

Descrivere comeil malware ottiene la persistenza

La persistenza di un malware si riferisce alla capacità del malware di mantenere la sua presenza su un sistema dopo l'infezione iniziale, garantendo così che possa essere eseguito ogni volta che il sistema viene avviato. Esistono varie tecniche attraverso le quali un malware può ottenere la persistenza, e spesso coinvolgono la modifica delle impostazioni di avvio del sistema operativo o l'inserimento di codice malevolo in punti strategici.
Un metodo comune per ottenere la persistenza è attraverso la modifica del Registro di sistema di Windows.

02

Identificare il client software utilizzato dal malware per la connessione ad Internet

L'identificazione del client software utilizzato da un malware per la connessione a Internet può variare a seconda del malware specifico. I malware spesso utilizzano protocolli di rete standard, come HTTP o HTTPS, per comunicare con server remoti controllati dagli attaccanti. Tuttavia, possono mascherare o modificare la loro identità per eludere la rilevazione. Per identificare il client software, è possibile esaminare il traffico di rete generato dal malware. Gli analisti di sicurezza informatica spesso utilizzano strumenti di analisi del traffico di rete, come Wireshark, per catturare e ispezionare i pacchetti inviati e ricevuti dal sistema infetto. Se il malware utilizza un protocollo standard come HTTP, è possibile vedere i dettagli del traffico nel payload del pacchetto, dove potrebbero esserci informazioni sul client utilizzato. Ad esempio, potrebbe essere presente una stringa di User-Agent nel campo delle intestazioni HTTP, che potrebbe rivelare il client software o persino essere manipolata dal malware per sembrare un browser o un'applicazione legittima.

03

Identificare l’URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzioneche permette al malware di connettersi ad un URL

Identificare il client software utilizzato dal malware e l'URL a cui cerca di connettersi richiede l'analisi del codice specifico del malware, che può variare notevolmente a seconda del tipo e della variante del malware. Tuttavia, posso fornire un esempio generico di come un malware potrebbe tentare di connettersi a un URL utilizzando istruzioni di assembly. È importante notare che il codice reale sarà molto più complesso e varierà in base al comportamento specifico del malware.