Traccia:

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- Identificare il client software utilizzato dal malware per la connessione ad Internet
- Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL

Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite

La persistenza del malware è fondamentale per garantire che il malware sopravviva anche dopo riavvii o chiusure del sistema. Uno dei modi comuni attraverso cui il malware ottiene la persistenza è **modificando le chiavi di registro**. Vediamo alcune di queste tecniche utilizzate dai malware:

1. **Chiavi Run/RunOnce**: Queste chiavi di registro sono spesso sfruttate dai malware per ottenere la persistenza. A livello utente, le chiavi coinvolte sono:
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce A livello di sistema, i malware possono infettare queste chiavi:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
2. **Chiave BootExecute**: Questa chiave viene utilizzata dal processo smss.exe per eseguire comandi prima che il sottosistema Windows venga caricato. Se questa chiave contiene valori aggiuntivi oltre a autocheck autochk*, potrebbe indicare che il malware verrà avviato all'avvio del sistema.
3. **Chiavi utilizzate dal processo WinLogon**:
    - La chiave Userinit nel percorso HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon viene utilizzata dal processo WinLogon per avviare script di accesso.
    - Le sottochiavi Notify in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon vengono utilizzate per notificare eventi quando si verifica una sequenza di attenzione sicura (SAS) (ad esempio, Ctrl+Alt+Del). Queste sottochiavi possono essere modificate per avviare DLL quando si verifica un evento SAS.
    - La chiave Shell in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon punta a explorer.exe e dovrebbe contenere solo la stringa "explorer.exe" per garantire che l'interfaccia di Windows venga avviata correttamente.

Dal codice sembra coinvolgere l'apertura di una connessione Internet tramite le funzioni InternetOpenA e InternetOpenUrlA. Questo potrebbe essere parte di un meccanismo di comunicazione del malware con un server di comando e controllo o per scaricare ulteriori carichi dannosi.

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

Il client software utilizzato dal malware per la connessione a Internet è "Internet Explorer 8.0"[1]. Questo particolare software è stato individuato nel codice sorgente dell'immagine e viene utilizzato come user agent per le comunicazioni di rete da parte del malware.

Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL

L'url al quale il malware tenta di connettersi è "http://www.malware12.com"