EPICODE

Esercizio S11 – L1

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  
• BONUS: qual è il significato e il funzionamento del comando assembly "lea"

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Segue

Immagine che contiene testo, schermata, linea, numero

Descrizione generata automaticamente

SOLUZIONE

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

- La maggior parte dei malware necessitano di ottenere la persistenza sui sistemi infettati, il che significa che devono essere in grado di resistere ai riavvii del sistema. In altre parole, se si spegne il sistema e poi lo si riaccende, il malware rimane ancora attivo.  
Per ottenere la persistenza i malware possono:

Scrivere nel Registro di Windows: Uno dei modi più diffusi è la scrittura nelle chiavi di registro di Windows. In particolare, la chiave HKLM “Software\Microsoft\Windows\CurrentVersion\Run” è spesso bersagliata visto che in questa chiave vengono inseriti i processi da avviare durante l’avvio del sistema.

API di modifica del Registro: Per ottenere la persistenza, i malware utilizzano le API di modifica del Registro, come RegSetValueEx. Queste API consentono modificare valori all’interno delle chiavi di registro.

Segue

Nella figura di seguito è possibile notare la chiamata alla funzione RegOpenKeyEx. Grazie a questa funzione il malware accede alla chiave di registro HKLM. Successivamente chiama la funzione RegSetValueEx per modificare il valore del registro in modo tale da ottenere la persistenza all’avvio del sistema operativo.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

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

- Come è possibile notare nell’immagine sottostante il client software utilizzato per la connessione ad Internet è “Internet Explorer 8.0”.

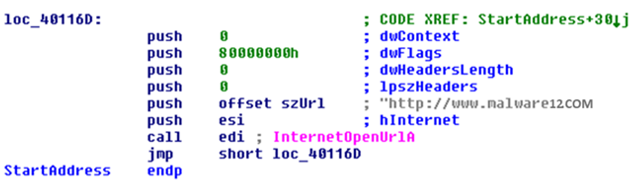
Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Segue

• 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

- Come mostrato nell’immagine sottostante l’URL al quale il malware tenta di connettersi è “http://www.malware12COM”



• BONUS: qual è il significato e il funzionamento del comando assembly "lea"

- lea dice dove si trova un oggetto senza andare a prenderlo. Non tocca l’oggetto stesso, ma ti dice dove trovarlo. È utile per leggere caratteri da una stringa o valori da una tabella. lea calcola l’indirizzo effettivo di un’etichetta (come un nome di variabile) senza accedere alla memoria.

In breve, lea è come una mappa che ti dice dove trovare qualcosa senza doverlo prendere fisicamente.