Pratica S11L1

Malware analysis

Traccia:

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

1. Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite.
2. Identificare il client software utilizzato dal malware per la connessione ad Internet.
3. 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.

**Soluzione:**

**1)** Il software malevolo assicura la propria permanenza nel sistema inserendo un valore aggiuntivo nella chiave di registro denominata: Software\Microsoft\Windows\CurrentVersion\Run.

Quest'ultima contiene l'elenco dei programmi che si attivano automaticamente quando il sistema operativo si avvia. Le operazioni tecniche impiegate includono l'uso di RegOpenKey, una funzione che consente di accedere alla chiave di registro specificata. Questa operazione avviene passando i parametri tramite le istruzioni "push" eseguite prima della chiamata a RegSetValueEx, una funzione che permette al malware di aggiungere un valore nuovo nella chiave di registro che è stata appena aperta.

**2)** Il client utilizzato dal malware per connettersi ad internet è Internet Explorer, più precisamente la versione 8.A computer screen shot of a computer code

Description automatically generated

**3**) Il software malevolo tenta di stabilire una connessione con l'indirizzo URL [www.malware12.com](http://www.malware12.com/) utilizzando la funzione "InternetOpenURL". Questa specifica chiamata di funzione facilita la connessione del malware a un URL, passando l'indirizzo come parametro alla funzione attraverso l'uso dell'istruzione "push" sullo stack.

**A screenshot of a computer program

Description automatically generated**

**Top of Form**