S11 L1

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

1)Descrivere comeil 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 funzioneche permette al malware di connettersi ad un URL

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

1) La persistenza viene ottenuta dal malware agendo sulla chiave di registro Software\\Microsoft\\Windows\\CurrentVersion\\Run, aggiungendo un valore nuovo , infatti è una chiave che include tutti quei programmi che partono con l'accensione del sistema operativo.
Le funzioni chiamate sono :
RegOpenKey, che permette di aprire la chiave selezionata. I parametri sono passati sullo stack tramite le istruzioni «push» che precedono la chiamata di funzione
RegSetValueEx, che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta

2) Per connettersi a Internet il malware usa Internet Explorer 8.0

3) l malware cerca di connettersi all'URL www.malware12.com tramite la chiamata di funzione **InternetOpenURL**

4) Il comando **"lea"** in assembly sta per **"Load Effective Address"**. Questo comando non carica i dati dalla memoria, ma carica l'indirizzo effettivo di un'operando (ad esempio una variabile o una posizione di memoria) in un registro. In pratica, il comando "lea" calcola l'indirizzo di un'operando e lo mette in un registro, senza accedere effettivamente alla memoria per recuperare i dati. Questo è utile quando si desidera effettuare operazioni di calcolo sull'indirizzo di una variabile piuttosto che sui suoi dati.