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

1. Persistenza: L'istruzione `Push` viene comunemente utilizzata per inserire valori nello stack prima di chiamare una funzione. Potrebbe essere possibile che il malware stia preparando dei dati da passare ad una funzione di sistema o a una funzione personalizzata per ottenere la persistenza nel sistema.

2. Client software per la connessione ad Internet: Spesso, i malware utilizzano API di sistema come `WinINet` o `Winsock` per effettuare connessioni Internet. Il codice utilizza l'API di sistema Windows per effettuare la connessione ad Internet. Questo è indicato dalla chiamata alla funzione Call edi, che potrebbe essere un riferimento a una funzione all'interno della libreria di sistema di Windows per la gestione delle connessioni Internet.

3. URL a cui il malware tenta di connettersi: L'istruzione `Call` seguita da `Lea` e `Push` potrebbe essere utilizzata per preparare l'URL prima di effettuare una chiamata a una funzione di connessione Internet.