S11L1

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

Il malware ottiene la persistenza attraverso:

```
push offsetSubkey;"Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push HKEY_LOCAL_MACHINE ;hKey
call esi ; RegOpenKeyExW
```

Il malware in questione va a posizionarsi nel registro di sistema di windows,il quale contiene i programmi che si avviano in modo automatico all'avvio del pc.

Traccia: Identificare il client software utilizzato dal malware per la connessione ad Internet.
Il **client software** che il malware utilizza è internet explorer versione 8.0

Traccia: 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.

```
push offset szUrl ; "http://www.malware12.com"
push esi ;hinternet
call edi ; InternetOpenUrlA
```

FUNZIONE: InternetOpenUrlA
URL:http://www.malware12.com

Bonus:qual è il significato e il funzionamento del comando assembly"lea"
Il comando “lea”,viene utilizzato per caricare l'indirizzo di memoria di una variabile o di un oggetto in un registro,è simile al comando mov.
Sintassi: lea destinazione, sorgente