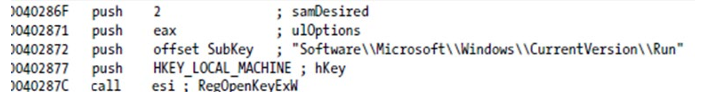


Analizziamo il codice assembly per rispondere alle domande:

Persistenza del malware:

Il malware ottiene la persistenza modificando il registro di sistema, aggiungendo una voce al registro di esecuzione automatica di Windows. Ecco il codice assembly corrispondente:

Qui, il malware chiama la funzione RegOpenKeyExA per aprire la chiave di registro "Software\Microsoft\Windows\CurrentVersion\Run" e quindi aggiungere una voce per il malware per eseguirsi all'avvio.

Client software utilizzato per la connessione ad Internet:

Il malware utilizza la libreria wininet.dll per stabilire la connessione Internet.

URL a cui il malware tenta di connettersi: L'URL a cui il malware tenta di connettersi è "http://uwu.nalwareizcom".



Qui, il malware chiama la funzione InternetOpenUrlA per tentare di aprire una connessione all'URL specificato.

Chiamata di funzione per la connessione all'URL:

La chiamata di funzione per la connessione all'URL è InternetOpenUrlA, che fa parte della libreria wininet.dll.



Bonus: Comando lea in assembly: lea (Load Effective Address) è un'istruzione in assembly x86 utilizzata per calcolare l'indirizzo effettivo di una variabile o di un'area di memoria e memorizzarlo in un registro. A differenza dell'istruzione mov, lea non carica il valore dalla memoria, ma calcola solo l'indirizzo. Ad esempio:

lea ecx; [ebp-8]

In questo caso, lea viene utilizzato per caricare l'indirizzo di memoria di una variabile o un'area di memoria in un registro anziché il valore effettivo memorizzato in quella posizione di memoria.