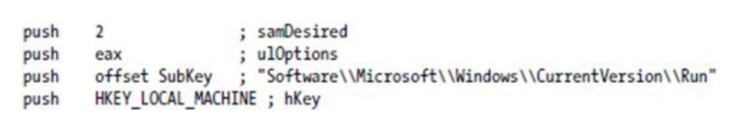
**RISOLUZIONE ESERCIZIO**

Il malware sfrutta le funzioni “RegOpenKeyExW” e “RegSetValueExW” della libreria “ADVAPI32.dll”, che serve per interagire con le chiavi del registro di sistema, al fine di essere avviato durante il boot del sistema operativo.

* Passa i parametri alla funzione attraverso “push



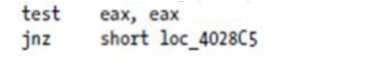
* chiama la funzione “RegOpenKeyExW” e apre la sottochiave

“Software\\Microsoft\\Windows\\CurrentVersion\\Run” all’interno della chiave

“HKEY\_LOCAL\_MACHINE”.



* a questo punto esegue un “ciclo if” attraverso un test: in caso di errore fa un salto alla locazione “4028C5”, che probabilmente conterrà le casistiche per i vari errori plausibili, altrimenti procede in ordine logico.



Proseguendo si arriva alla locazione 402882

**BONUS**

il comando “lea”, Load Effective Memory, carica l’indirizzo di memoria di un operando in un registro.

* “lea ecx, [esp+424h+Data]”, in questo caso “lea” carica l’indirizzo di memoria della

variabile “Data”, che nel programma si trova ad un offset di 424h (esadecimale) -> 1060

(byte) dal registro esp, nel registro ecx;

* Saltiamo alla parte finale del codice dove viene chiamata la funzione “RegSetValueExW”:



alla quale vengono passati i parametri sempre attraverso “push”:

