Esercizio S11/L1

Malware analysis

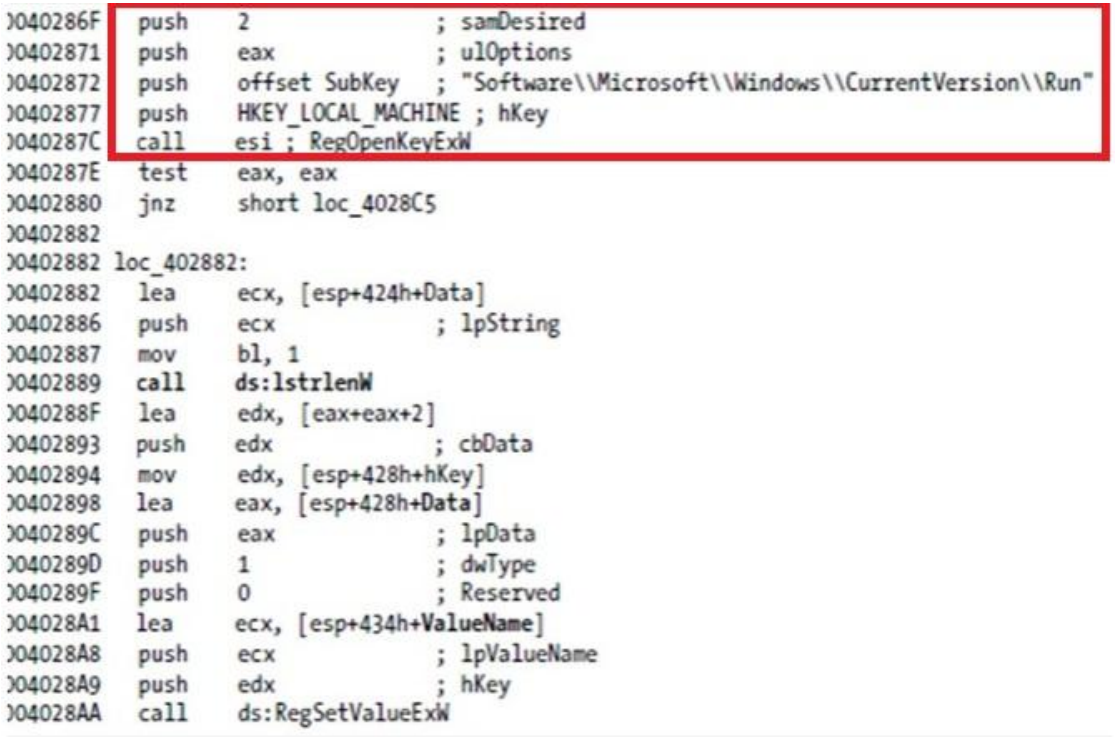
Traccia

Nell’esercizio di oggi eseguiremo l’analisi di un malware. Tra gli obiettivi abbiamo:

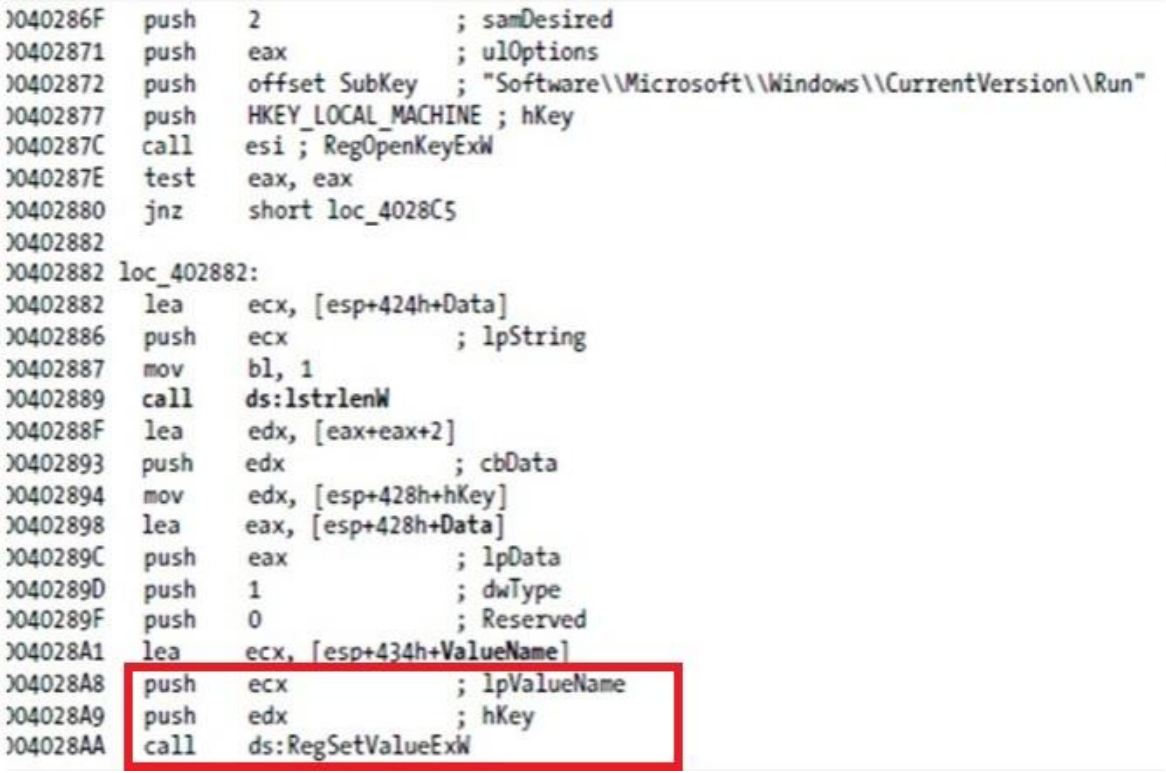
- Individuare la parte di codice con il quale il malware ottiene la persistenza;
- Identificare il client software utilizzato dal malware per la connessione ad internet;
- Identificare la funzione e la rispettiva URL a cui si connette;
- Bonus: spiegare il significato e il funzionamento del comando “lea”.

Per persistenza si intende un qualcosa di non volatile, ovvero qualcosa che persiste anche quando il processo che lo ha generato termina, come per esempio i dati su un hard disk. Nel caso di un malware la si può intendere come una resistenza al reboot. Normalmente un malware ottiene la persistenza cambiando le chiavi di registro in modo tale da essere avviati automaticamente all'avvio del sistema.

Nel riquadro rosso dell'immagine a fianco viene evidenziata la funzione "RegOpenKeyExW" che permette di aprire una chiave di registro per modificarla.



Nella figura accanto viene evidenziata la funzione “RegSetValueExW” che permette di aggiungere un valore al registro. Tramite questa funzione e quella vista in precedenza il malware ottiene la persistenza. Queste modifiche vengono effettuate nella root key HKEY_LOCAL_MACHINE dove sono contenute le configurazioni della macchina.



```
0040286F   push    2               ; samDesired
00402871   push    eax             ; ulOptions
00402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877   push    HKEY_LOCAL_MACHINE ; hKey
0040287C   call    esi ; RegOpenKeyExW
0040287E   test    eax, eax
00402880   jnz     short loc_4028C5
00402882
00402882 loc_402882:
00402882   lea     ecx, [esp+424h+Data]
00402886   push    ecx             ; lpString
00402887   mov     bl, 1
00402889   call    ds:lstrlenW
0040288F   lea     edx, [eax+eax+2]
00402893   push    edx             ; cbData
00402894   mov     edx, [esp+428h+hKey]
00402898   lea     eax, [esp+428h+Data]
0040289C   push    eax             ; lpData
0040289D   push    1               ; dwType
0040289F   push    0               ; Reserved
004028A1   lea     ecx, [esp+434h+ValueName]
004028A8   push    ecx             ; lpValueName
004028A9   push    edx             ; hKey
004028AA   call    ds:RegSetValueExW
```

Nel primo riquadro nella figura a fianco viene evidenziato il browser usato dal malware per connettersi a internet, cioè Internet Explorer 8.0, mentre in quello più in basso la URL a cui si connette tramite la funzione “InternetOpenUrlA”.

L’istruzione “lea” (load effective address) copia l’indirizzo di una certa variabile, passata come sorgente, in un registro, passato come destinazione. A differenza di “mov”, che permette di copiare il valore, “lea” può eseguire più operazioni in linea usando meno istruzioni.