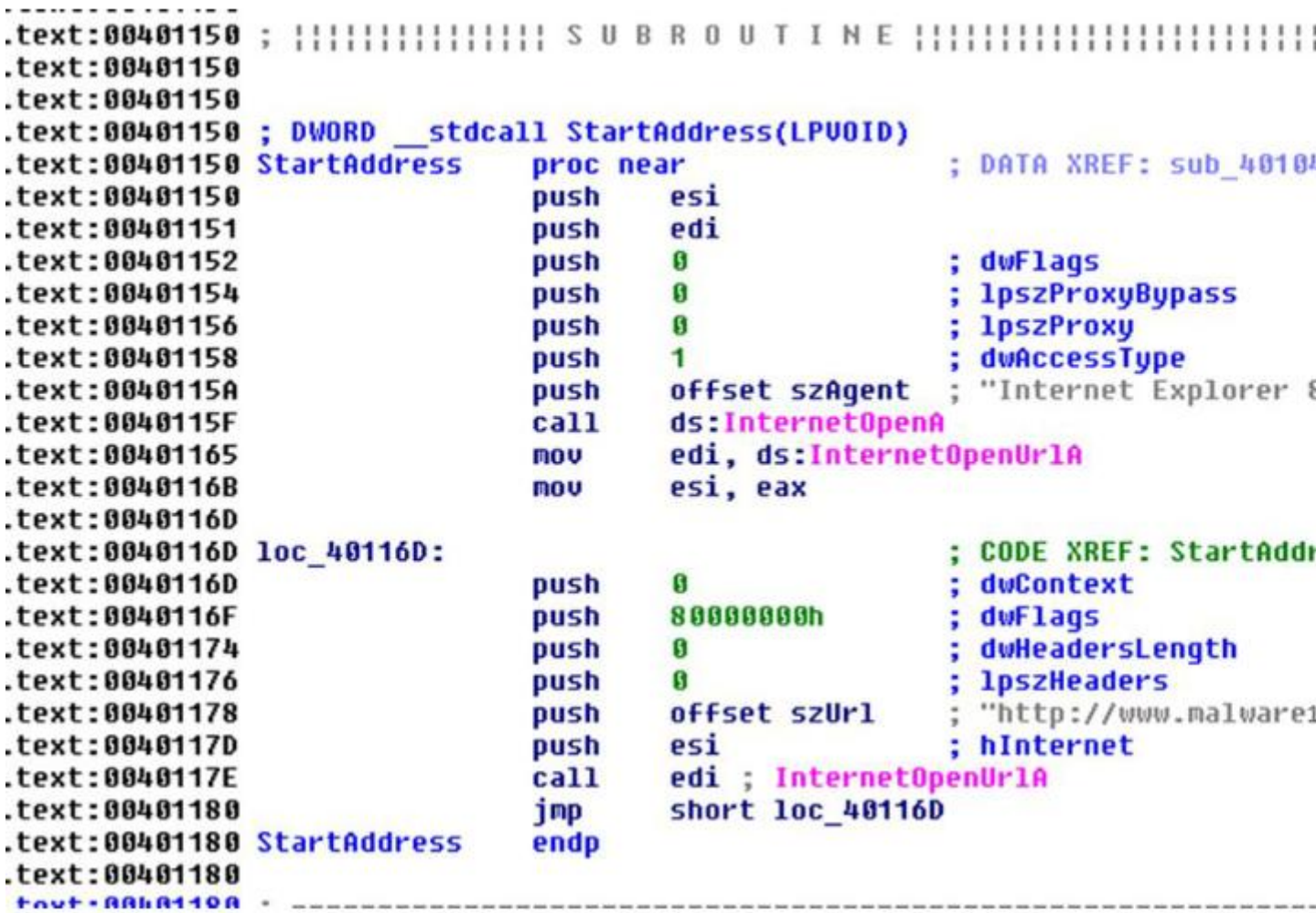
Oggi andremo ad analizzare i due malware scritti in linguaggio assembly, ed andremo a rispondere alle domande poste nell'esercizio.

I due malware in questione sono i seguenti:

```
)040286F   push    2                 ; samDesired
)0402871   push    eax               ; ulOptions
)0402872   push    offset SubKey     ; "Software\\Microsoft\\Windows\\CurrentVersion\
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
)040287E   test    eax, eax
)0402880   jnz     short loc_4028C5
)0402882
)0402882 loc_402882:
)0402882   lea     ecx, [esp+424h+Data]
)0402886   push    ecx               ; lpString
)0402887   mov     bl, 1
)0402889   call    ds:lstrlenW
)040288F   lea     edx, [eax+eax+2]
)0402893   push    edx               ; cbData
)0402894   mov     edx, [esp+428h+hKey]
)0402898   lea     eax, [esp+428h+Data]
)040289C   push    eax               ; lpData
)040289D   push    1                 ; dwType
)040289F   push    0                 ; Reserved
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx               ; lpValueName
)04028A9   push    edx               ; hKey
)04028AA   call    ds:RegSetValueExW
```



Risposta domanda numero 1:

come sappiamo, molti malware usano i registri di windows per far si che essi vengano salvati nelle entry dei programmi che vengono avviati all'accensione del PC, in modo tale da ottenere la "persistenza", ovvero l'avvio automatico di essi ogni qualvolta il device venga avviato.

Vediamo come nel primo malware, esso memorizzi il path della chiave di registro che spesso viene usata dai malware per ottenere la persistenza (windows//currentversion//run), poi vediamo come acceda al registro HKEY_LOCAL_MACHINE (il registro contenente tutte le configurazioni della macchina in questione) con il comando "push" e poi usa la funzione regopenkeyEx con il comando "call". Sappiamo che i malware richiamano questa funzione che permette di accedere e modificare chiavi di registro .

Il continuo del codice del malware sono appunto le "modifiche" che quest'ultimo apporta alla chiave di registro affinchè possa ottenere la persistenza.

Risposta domanda numero 2:

nel secondo malware, esso usa la chiamata stdcall che viene usata specificatamente per le chiamate di funzione win32 a 32 bit (sappiamo che DWORD indica un intero a 32 bit), ed assegna tramite il puntatore un valore (start address) che sara il client software usato per la connessione ad internet. Poi chiama diversi parametri e con il comando push li carica nella funzione (ad esempio lpszproxy è un puntatore ad una stringa che contiene l'elenco dei server proxy). Poi indica il motore di ricerca usato (internet explorer 8) che

andrà ad indicare il software client usato per la connessione e chiama due fuinzioni importanti : internet opena (che viene usata per inizializzare una connessione ad internet) ed internetopenurlA (che reindirizza la connessione aperta ad uno specifico URL).

Poi memorizza nella funzione diversi parametri che appartengono al client software usato per la connessione (dwheaderslenght,lpszheaders) e memorizza anche l'url malevolo al quale la funzione vuole che ci si connetta (http://malwre12com), ,poi con la chiamata Internetopenurl termina il suo compito, quindi apre e indirizza il software client all'url memorizzato nella riga di codice poco precedente.