

# WINDOWS MALWARE

## DISASSEMBLED CODE

04-03-2023

Blocco 1:

```
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+d24h+Data]
00402886 push ecx        ; lpString
00402887 mov bl, 1
00402889 call ds:strlenW
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:RegSetValueEx
```

**Punto di codice in cui  
l'attaccante ottiene  
persistenza nella macchina  
vittima**

Blocco 2:

```
.text:00401150 ; ///////////////////////// S U B R O U T I N E /////////////////////
.text:00401150
.text:00401150
.text:00401150 DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress proc near      ; DATA XREF: sub_401040+ECT
.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:00401150     push offset szAgent ; "Internet Explorer 8.0"
.text:0040115F     call ds:InternetOpenA
.text:00401165     mov   edi, ds:InternetOpenUrlA
.text:00401168     mov   esi, eax
.text:0040116D
.text:0040116D loc_40116D:           ; CODE XREF: StartAddress+30/j
.text:0040116D     push  0              ; dwContext
.text:0040116F     push  80000000 ; dwFlags
.text:00401174     push  0              ; dwHeadersLength
.text:00401176     push  0              ; lpszHeaders
.text:00401178     push offset szUrl ; "http://www.malware12.com/"
.text:0046117D     push  esi         ; hInternet
.text:0040117E     call edi; InternetOpenUrlA
.text:00401180     jmp  short loc_40116D
.text:00401180 StartAddress endp
.text:00401180
```

**In questo punto viene  
dichiarato il client software  
Internet Explorer per effetturare  
una successiva connessione**

**Punto di codice in cui  
viene inserito e chiamato  
un url**

## BONUS

La funzione lea usata anche in questo codice è simile alla funzione mov ma invece di copiare il contenuto di un indirizzo di memoria copia semplicemente l'effettivo indirizzo a cui punta, quindi il contenuto rimane invariato e il solo indirizzo viene spostato nel registro.