

Windows malware

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

Identificazione del client software utilizzato dal malware per la connessione a internet

Identificazione dell'URL al quale il malware tenta di connettersi ed evidenziazione della chiamata di funzione che permette al malware di connettersi ad un URL

Significato e funzionamento del comando *lea*

```

X040286F  push    2                ; samDesired
X0402871  push    eax              ; ulOptions
X0402872  push    offset SubKey    ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
X0402877  push    HKEY_LOCAL_MACHINE ; hKey
X040287C  call    esi ; RegOpenKeyExW
X040287E  test    eax, eax
X0402880  jnz     short loc_4028C5
X0402882
X0402882  loc_402882:
X0402882  lea     ecx, [esp+424h+Data]
X0402886  push    ecx              ; lpString
X0402887  mov     bl, 1
X0402889  call    ds:strlenW
X040288F  lea     edx, [eax+eax+2]
X0402893  push    edx              ; cbData
X0402894  mov     edx, [esp+428h+hKey]
X0402898  lea     eax, [esp+428h+Data]
X040289C  push    eax              ; lpData
X040289D  push    1                ; dwType
X040289F  push    0                ; Reserved
X04028A1  lea     ecx, [esp+434h+ValueName]
X04028A8  push    ecx              ; lpValueName
X04028A9  push    edx              ; hKey
X04028AA  call    ds:RegSetValueExW

```

Funzione che permette di aprire una chiave di registro e modificarla

Funzione che permette di aggiungere un nuovo valore all'interno dell'registro e di settare i rispettivi dati

```

.text:00401150 : ||| S U B R O U T I N E |||
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress proc near ; DATA XREF: sub_401040+EC70
.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
.text:00401165 nov edi, ds:InternetOpenUrlA
.text:00401168 nov esi, eax
.text:0040116D loc_40116D: ; CODE XREF: StartAddress+38↓j
.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.malware12.com"
.text:0040117D push esi ; hInternet
.text:0040117E call edi ; InternetOpenUrlA
.text:00401180 jmp short loc_40116D
.text:00401180 StartAddress endp

```

Client software
utilizzato dal malware

URL al quale il malware
tenta di connettersi

Funzione che viene utilizzata per
inizializzare una connessione verso internet

Load Effective Address

Alcune architetture di set di istruzioni, come Intel x86 e IBM/360 e i suoi successori, hanno un'istruzione di indirizzo efficace del carico.

Ciò esegue un calcolo dell'indirizzo operativo efficace, ma invece di agire su quella posizione di memoria, carica l'indirizzo che sarebbe stato accessibile in un registro.

Questo può essere utile quando si passa l'indirizzo di un elemento di matrice a una subroutine.

Può anche essere un modo intelligente di fare più calcoli del normale in una istruzione; ad esempio, l'utilizzo di tali istruzioni con la modalità di indirizzamento "base + indice + offset" consente di aggiungere due registri e una costante insieme in un'istruzione e memorizzare il risultato in un terzo registro.

fonte: https://en.wikipedia.org/wiki/Addressing_mode#Useful_side_effect