S11-L1

Traccia:

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

- 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"

Codice:

```
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
```

```
.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
.text:00401180 ; ---------------------------------------------------------------------------
```

Ottenimento della persistenza

Nel primo estratto di codice, si nota una sequenza di istruzioni che interagiscono con il
registro di sistema di Windows.
Queste istruzioni sono comunemente utilizzate dai malware per ottenere *persistenza*, ovvero per assicurarsi che il codice malevolo venga eseguito ad ogni avvio del sistema.

- Il malware ottiene la persistenza tramite la modifica del registro di sistema di Windows.
  In particolare, la chiave
  `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
  viene aperta e modificata per inserire un valore che permette l'esecuzione automatica del malware ad ogni avvio del sistema.
- Le istruzioni assembly rilevanti includono:
  - `push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"` che indica la chiave di registro da modificare.
  - `call esi ; RegOpenKeyExW`
    Questa chiamata di funzione apre una chiave di registro specificata, in questo caso, la chiave è associata ai programmi che si avviano automaticamente con
    Windows ("Software\\Microsoft\\Windows\\CurrentVersion\\Run").
  - Le istruzioni successive (`lea ecx, [esp+424h+Data]` fino a `call ds:RegSetValueExW`) impostano il valore necessario per la persistenza.

    `call ds:RegSetValueExW` , dopo aver aperto la chiave, questa funzione imposta un valore
    all'interno di essa.
    Il malware usa questa funzione per scrivere un nuovo valore di avvio che punta all'eseguibile del malware stesso, garantendo così che verrà

eseguito ad ogni
avvio del sistema.

Software utilizzato dal malware per la connessione a Internet

Nel secondo estratto di codice, il malware utilizza le seguenti funzioni dell'API di Windows per
connettersi a Internet:

- Il client software utilizzato è **Internet Explorer 8.0**.
  Questo è visibile dall'istruzione
  `push offset szAgent ; "Internet Explorer 8.0"` che imposta l'agente utente per la connessione.
- `call ds InternetOpenA`, questa funzione inizializza l'uso delle funzioni di Internet Win32 API e
  specifica il client software utilizzato per la connessione Internet.

Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione

- L'URL al quale il malware tenta di connettersi è `http://www.malware12.com`.
- La funzione utilizzata per connettersi è `InternetOpenUrlA`, e questo è evidenziato dalla sequenza `call edi ; InternetOpenUrlA` seguita da `push offset szUrl` per impostare l'URL ("http://www.malware12COM").

Significato e funzionamento del comando assembly "lea"

- Il comando `lea` (Load Effective Address) viene utilizzato in assembly per calcolare l'indirizzo effettivo di una variabile e caricarlo in un registro. È simile a un'operazione di puntatore in linguaggi di alto livello. In pratica, `lea` non esegue un'operazione di dereferenziazione, ma semplicemente calcola l'indirizzo e lo carica nel registro di destinazione.

In conclusione, questi estratti di codice mostrano chiaramente come il malware tenti di
garantirsi la persistenza modificando le chiavi di registro di avvio automatico di Windows e
come stabilisca una connessione a Internet utilizzando un client software mascherato da
Internet Explorer 8 per connettersi a un URL malevolo.
Queste tecniche sono tipiche dei malware che cercano di assicurarsi una presenza costante e non rilevata su un sistema infetto, consentendo agli attaccanti di controllare a distanza la macchina compromessa o di esfiltrare dati sensibili.