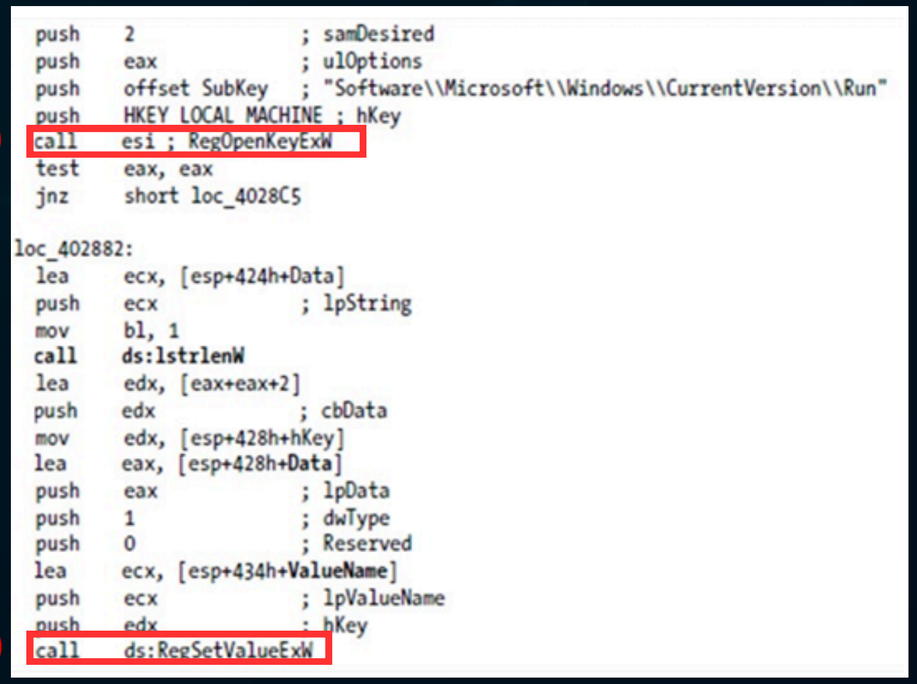
S11-L1

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"



```
push    2               ; samDesired
push    eax             ; ulOptions
push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey
call    esi ; RegOpenKeyExW
test    eax, eax
jnz     short loc_4028C5

loc_402882:
lea     ecx, [esp+424h+Data]
push    ecx             ; lpString
mov     bl, 1
call    ds:lstrlenW
lea     edx, [eax+eax+2]
push    edx             ; cbData
mov     edx, [esp+428h+hKey]
lea     eax, [esp+428h+Data]
push    eax             ; lpData
push    1               ; dwType
push    0               ; Reserved
lea     ecx, [esp+434h+ValueName]
push    ecx             ; lpValueName
push    edx             ; hKey
call    ds:RegSetValueExW
```

1)

2)

Questo codice assembly fa riferimento a una tecnica di persistenza tipicamente utilizzata nei malware. Il codice modifica una chiave del registro di Windows per assicurarsi che un programma venga eseguito automaticamente all'avvio del sistema.

La chiave in questione è questa:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Questa chiave è comunemente utilizzata per avviare automaticamente applicazioni quando il sistema operativo Windows viene avviato. Il malware aggiunge una nuova voce a questa chiave, che contiene il percorso di un programma che verrà eseguito ad ogni avvio del sistema.

Le due chiamate a funzione che permettono ciò sono: 1) RegOpenKeyExW e 2) RegSetValueExW

Chiamata a funzione RegOpenKeyExW:

```
push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey
call    esi ; RegOpenKeyExW
```

Queste righe aprono la chiave del registro Run sotto HKEY_LOCAL_MACHINE. Il registro di Windows è uno dei principali metodi utilizzati dai malware per ottenere persistenza, poiché la chiave Run consente di specificare programmi che devono essere eseguiti automaticamente.

Chiamata a funzione RegSetValueExW:

```
lea     ecx, [esp+434h+ValueName]
push    ecx         ; lpValueName
push    edx         ; hKey
call    ds:RegSetValueExW
```

Questa parte imposta un nuovo valore nella chiave Run. Il valore immesso in questa chiave assicura che il programma associato venga eseguito automaticamente al riavvio del sistema.

```
; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

; DWORD __stdcall StartAddress(LPVOID)
StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
                push    esi
                push    edi
                push    0               ; dwFlags
                push    0               ; lpszProxyBypass
                push    0               ; lpszProxy
                push    1               ; dwAccessType
                push    offset szAgent  ; "Internet Explorer 8.0"
                call    ds:InternetOpenA
                mov     edi, ds:InternetOpenUrlA
                mov     esi, eax

loc_40116D:                             ; CODE XREF: StartAddress+30↓j
                push    0               ; dwContext
                push    80000000h       ; dwFlags
                push    0               ; dwHeadersLength
                push    0               ; lpszHeaders
                push    offset szUrl    ; "http://www.malware12COM
                push    esi             ; hInternet
                call    edi ; InternetOpenUrlA
                jmp     short loc_40116D
StartAddress    endp
```

Possiamo vedere che il malware utilizza le API di Windows per connettersi a Internet. In particolare, sta utilizzando la funzione InternetOpenA e InternetOpenUrlA, che fanno parte della WinINet API.

push offset szAgent ; "Internet Explorer 8.0"
call ds:InternetOpenA

InternetOpenA: Questa funzione inizializza l'uso delle funzionalità di Internet per il programma. Imposta un agente utente (in questo caso "Internet Explorer 8.0") e specifica le opzioni per il proxy, il bypass del proxy e il tipo di accesso. Questa funzione restituisce un handle che viene usato per successive chiamate di rete.

push offset szUrl ; "http://www.malware123.com"
call ds:InternetOpenUrlA

InternetOpenUrlA: Questa funzione apre una connessione HTTP o FTP per accedere a una risorsa remota specificata dall'URL. Nel codice, viene utilizzata per connettersi a "http://www.malware123.com", che presumibilmente è un server di comando e controllo (C&C) del malware.

Il comando LEA (Load Effective Address) in assembly è utilizzato per calcolare e caricare un indirizzo di memoria in un registro. A differenza di altre istruzioni di assembly che accedono effettivamente ai dati memorizzati in un indirizzo di memoria, LEA si limita a calcolare l'indirizzo stesso e caricarlo in un registro senza leggere o scrivere dati in memoria.

sintassi :

LEA destinazione, sorgente

destinazione : È il registro in cui verrà memorizzato l'indirizzo calcolato.
sorgente: È un'espressione che rappresenta un indirizzo di memoria.

LEA esegue un calcolo di indirizzo, ma non accede alla memoria, calcola l'indirizzo risultante e lo carica nel registro di destinazione. Questo è particolarmente utile per calcolare puntatori o eseguire aritmetica sui registri senza modificare la memoria effettiva.

lea ecx, [esp+434h+ValueName]