MALWARE ANALYSIS

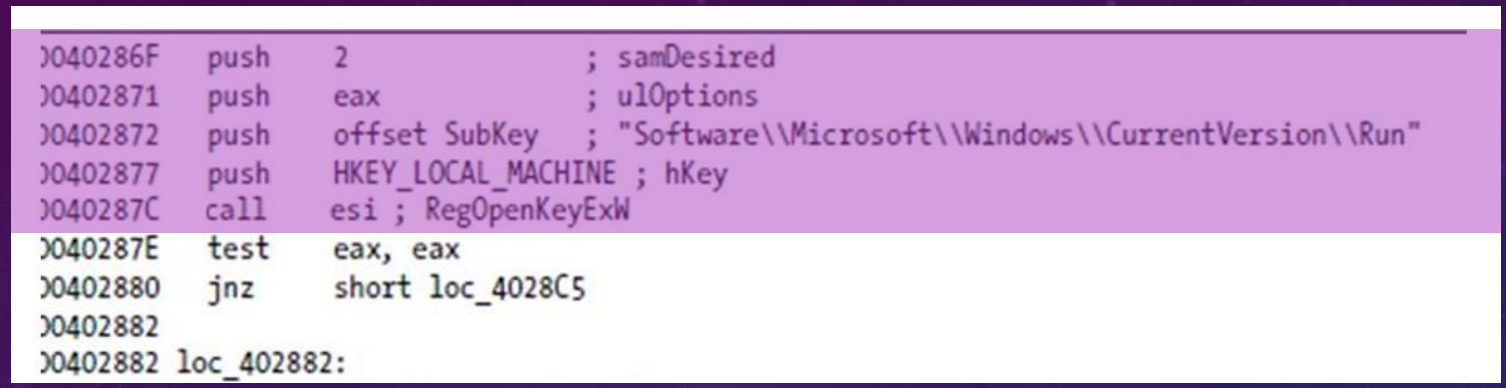
WINDOWS MALWARE

S11/L1

Con riferimento agli estratti di un malware reale, andiamo a 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

ANDIAMO AD ANALIZZARE IL 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
)040287E   test    eax, eax
)0402880   jnz     short loc_4028C5
)0402882
)0402882 loc_402882:
```

Il malware manipola il registro di sistema utilizzando le funzioni RegOpenKey e RegSetValueEx per ottenere la persistenza, inserendo una nuova voce all'interno della sezione di avvio automatico del registro di sistema Il software dannoso acquisisce la capacità di persistere nel sistema operativo mediante l'inserimento di una nuova voce all'interno della sezione di avvio automatico del registro di sistema.
Questa sezione, situata nel percorso **Software\Microsoft\Windows\CurrentVersion\Run**, contiene le informazioni sui programmi da avviare all'avvio del sistema operativo.
Per raggiungere questo obiettivo, il malware utilizza alcune funzioni del sistema operativo. In particolare, fa uso di RegOpenKey, una funzione che consente di aprire la chiave del registro desiderata. I parametri necessari per questa operazione vengono passati attraverso lo stack utilizzando le istruzioni "push" prima di chiamare la funzione stessa.
Successivamente, il malware sfrutta RegSetValueEx per aggiungere una nuova voce alla chiave di registro appena aperta. Questa funzione consente al software dannoso di inserire le informazioni necessarie per garantire che venga avviato automaticamente all'avvio del sistema operativo.

Il software dannoso si serve di Internet Explorer, nella sua versione 8, come client per stabilire connessioni a Internet.

```
.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
```

Il malware tenta di comunicare con l'URL www.malware12.com utilizzando la funzione "InternetOpenURL".
Questa funzione è responsabile di aprire una connessione Internet verso un URL specifico. L'URL stesso viene passato come parametro alla funzione tramite un'istruzione "push" nello stack.