Epicode

Windows Malware Analysis

Indice

Traccia

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, 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
4. 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
```

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

Analisi codice 1

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

```
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:
```

```
004028A8   push    ecx               ; lpValueName
004028A9   push    edx               ; hKey
004028AA   call    ds:RegSetValueExW
```

I malware utilizzano molto spesso il registro per ottenere quella che viene chiamata «persistenza». Ovvero, il malware aggiunge sé stesso alle entry dei programmi che devono essere avviati all'avvio del PC in modo tale da essere eseguiti in maniera automatica e permanente senza l'azione dell'utente.

Questo codice apre una chiave di registro per aggiungere un valore in modo tale da ottenere persistenza.

La chiamata alla funzione ***RegOpenKeyEx*** i parametri della funzione sono passati sullo stack tramite le istruzioni «push». Con questa funzione il malware accede alla chiave di registro prima di modificarne il valore

Una delle chiavi di registro che viene utilizzata dai malware per ottenere persistenza su un sistema operativo Windows è:

Software\\Microsoft\\Windows\\CurrentVersion\\Run

L'altra funzione usata è:

RegSetValueEx che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta

Analisi codice 2

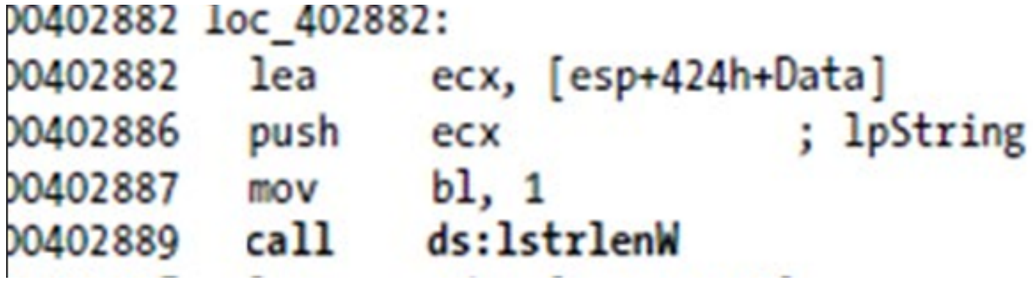
Identificare il client software utilizzato dal malware per la connessione ad Internet.
Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL.

```
.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
```

Il client software per stabilire una connessione ad internet usato dal malware è ***Internet Explorer*, *versione 8.0*.**
L'URL al quale il malware cerca di connettersi è: ***http://www.malware12.com***
La chiamata di funzione che permette al malwae di connettersi a questo URL è:
call edi; InternetOpenUrlA
L'URL viene passato come parametro alla funzione tramite l'istruzione push

Bonus

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



LEA (load effective address) è spesso usato come "trucco" per fare certi calcoli, ma non è il suo scopo primario. Il set di istruzioni x86 è stato progettato per supportare linguaggi di alto livello come Pascal e C, dove gli array sono comuni.
L'istruzione lea invece carica in un registro l'indirizzo effettivo di una certa variabile.