WINDOWS MALWARE

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**"

```
)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:
)0402882   lea     ecx, [esp+424h+Data]
)0402886   push    ecx             ; lpString
)0402887   mov     bl, 1
)0402889   call    ds:lstrlenW
)040288F   lea     edx, [eax+eax+2]
)0402893   push    edx             ; cbData
)0402894   mov     edx, [esp+428h+hKey]
)0402898   lea     eax, [esp+428h+Data]
)040289C   push    eax             ; lpData
)040289D   push    1               ; dwType
)040289F   push    0               ; Reserved
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   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
```

1. **Descrivere come il malware ottiene la persistenza.**
   I malware usano spesso il registro per ottenere persistenza, ovvero il malware va ad aggiungere 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.

```
)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
```

   In questo caso il codice aggiunge un nuovo valore nella chiave di registro "**Software\\Microsoft\\Windows\\CurrentVersion\\Run**", chiave di registro spesso utilizzata dai malware per ottenere persistenza, e tramite una ulteriore instruzione "push" passa anche il parametro "**HKEY_LOCAL_MACHINE**" (HKLM), una delle 5 macrocategorie di Root Key, dove sono contenuti i record e le configurazioni della macchina.
   Passa poi alla chiamata della funzione **RegOpenKeyExW**, che permette di aprire una chiave di registro al fine di modificarla, passando sullo stack tramite "push" i parametri della funzione, così da accedere alla chiave di registro prima di modificarne il valore.

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

   Il codice passa poi alla chiamata della funzione **RegSetValueExW** sempre passando i valori sullo stack tramite le istruzioni "push" ("push ecx" e "push edx"), che permette di aggiungere aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati.

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

```
.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
```

Il client software utilizzato dal malware per la connessione ad internet risulta essere "**Internet Explorer 8.0**" chiamando la funzione "**InternetOpenA**" utilizzata per inizializzare la connessione.

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

```
.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 malware tenta di connettersi all'URL "http://www.malware12.com" utilizzando per la connessione la funzione "**InternetOpenUrlA**", che accetta tra i parametri oggetti "handler" ad una connessione inizializzata con InternetOpen e l'URL per la connessione, passati all'interno dello stack tramite istruzioni "push".

4. **BONUS: significato e funzionamento del comando assembly "lea".**

```
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]
```

Il comando "**lea**" (**Load Effective Address**) è un'istruzione Assembly che **serve per caricare in un registro l'indirizzo effettivo di una certa variabile**, quindi l'indirizzo della locazione di

memoria al quale si vuole accedere. Molto simile all'istruzione "mov", che a differenza di "lea", che sposta il valore presente in una locazione di memoria in un registro.
"Lea" consente di effettuare operazioni in linea, anche molto complesse, che non possono essere effettuate con "mov", permettendo quindi di far risparmiare istruzioni quando si lavora con offset.

Per concludere, è molto probabile che il malware importi la libreria **Wininet.dll,** che include funzioni per l'implementazione di protocolli di rete (http ed FTP), utilizzando appunto le funzioni InternetOpen e InternetOpenUrl per la connessione ad un determinato URL tramite http.
Questa libreria include le APIs WinInet, APIs per la gestione del networking a più ampio raggio.