

Progetto S11-L1

Studente: Simone Mininni

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"**

1) Evidenziare come il malware ottiene la persistenza, analizzando il seguente codice assembly:

```
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:
00402882 lea ecx, [esp+424h+Data]
00402886 push ecx ; lpString
00402887 mov bl, 1
00402889 call ds:strlenW
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
```

La persistenza viene ottenuta, andando a modificare le chiavi di registro del sistema, permettendo al programma malevolo di andare in esecuzione all' avvio del sistema operativo.

Tale modifica viene effettuata con l' utilizzo di due funzioni di windows:

- RegOpenKeyEx:<https://learn.microsoft.com/it-it/windows/win32/api/winreg/nf-winreg-regopenkeyexw>
- RegSetValueExW:<https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regsetvalueexw>

```
5F push 2 ; samDesired
71 push eax ; ulOptions
72 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
77 push HKEY_LOCAL_MACHINE ; hKey
7C call esi ; RegOpenKeyExW
```

In questa sezione vediamo la chiamata di funzione per aprire la chiave HKLM relativa al path "Software\\Microsoft\\Windows\\CurrentVersion\\Run" passando i parametri secondo la sintassi

Sintassi

C++

```
LSTATUS RegOpenKeyEx(  
    [in] HKEY hKey,  
    [in, optional] LPCWSTR lpSubKey,  
    [in] DWORD ulOptions,  
    [in] REGSAM samDesired,  
    [out] PHKEY phkResult  
);
```

```
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
```

Qui viene settato un nuovo valore passando i parametri come da sintassi:

Syntax

C++

```
LSTATUS RegSetValueExW(  
    [in] HKEY hKey,  
    [in, optional] LPCWSTR lpValueName,  
    [in] DWORD Reserved,  
    [in] DWORD dwType,  
    [in] const BYTE *lpData,  
    [in] DWORD cbData  
);
```

2) Connessione verso un sito remoto.

```
-----  
.text:00401150 ; SUBROUTINE  
.text:00401150  
.text:00401150  
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)  
.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  
.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 utilizzato per la connessione a internet è "Internet Explorer 8.0", si può notare nella sezione della chiamata di "InternetOpenA", dove viene passato lo user-agent.

L'url al quale il malware tenta di connettersi è "<http://www.malware12COM>", infatti viene passato come parametro nella chiamata di funzione InternetOpenUrlA.

```
push 0 ; dwContext  
push 80000000h ; dwFlags  
push 0 ; dwHeadersLength  
push 0 ; lpszHeaders  
push offset szUrl ; "http://www.malware12COM  
push esi ; hInternet  
call edi ; InternetOpenUrlA
```

3) Bonus:

Istruzione lea:

- carica in un registro l'indirizzo effettivo di una variabile.