Manuel Di Gangi

S11_L1

Malware analysis

04 aprile 2024

INDICE

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. Persistenza

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.

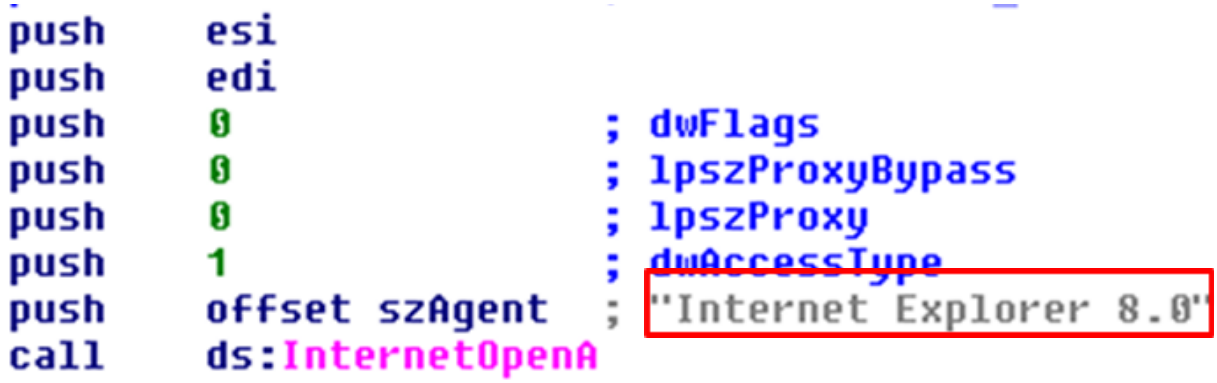
RegOpenKeyEx: questa funzione permette di aprire una chiave di registro al fine di modificarla. Come potete vedere dalla figura, essa accetta come parametri, tra gli altri, la chiave da aprire.

```
)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
```

RegSetValueEx: questa funzione permette invece di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati. Accetta come parametri la chiave, la sottochiave e il dato da inserire.

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

2. Client utilizzato dal malware



Il client utilizzato dal malware per connettersi ad internet viene passato come parametro di tipo stringa alla funzione InternetopenA, a giudicare dal commento del codice tale client è Internet Explorer 8.0

3. URL di connessione

L'url a cui il malware tenta di connettersi viene passato come parametro di tipo stringa ala funzione IntenetOpenUrlA ed è http://www.malware12.com

4. Comando lea

Il comando LEA (Load Effective Address) in assembly viene utilizzato per caricare l'indirizzo effettivo di un'operando in un registro, anziché caricare il valore di quel'operando stesso. L'istruzione LEA calcola l'indirizzo effettivo dell'operando e lo memorizza nel registro di destinazione, senza eseguire un accesso effettivo alla memoria per recuperare il valore memorizzato all'indirizzo calcolato.

Ad esempio, l'istruzione LEA può essere utilizzata per calcolare l'indirizzo di una variabile o di un'area di memoria e memorizzarlo in un registro, in modo che il registro contenga l'indirizzo effettivo al quale è archiviato il dato desiderato. Questo può essere utile per calcolare gli indirizzi dei dati senza doverli effettivamente leggere o scrivere in memoria, ma solo per eseguire calcoli basati su quegli indirizzi.

Un esempio di utilizzo di LEA potrebbe essere:

```css
LEA EAX, [EBX + ECX*2]
```

Questo comando carica nell registro EAX l'indirizzo effettivo di EBX + ECX*2, senza effettuare alcun accesso effettivo in memoria.