S11-L1

(Bonaldi Cristian)

Malware analysis - Windows malware

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"

Esercizio e sviluppo:

```
)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
```

Ci viene richiesto dalla traccia dell'esercizio di oggi di analizzare il codice assembly in figura e di descrivere in che modo il malware ottiene la persistenza. Vengono evidenziati i punti principali che descrivono in che modo il malware manipola il registro di Windows, andando a modificare la chiave di registro:

```
)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
```

push offset SubKey ;
“Software\\Microsoft\\Windows\\CurrentVersion\\Run”

In questo caso corrisponde alla chiave di registro che Windows utilizza per gestire i programmi che devono avviarsi automaticamente ogni volta che il sistema viene avviato.

push HKEY_LOCAL_MACHINE ; hKey

Questa corrisponde alla root key HKEY_LOCAL_MACHINE, dove sono contenuti i record e le configurazioni del sistema.

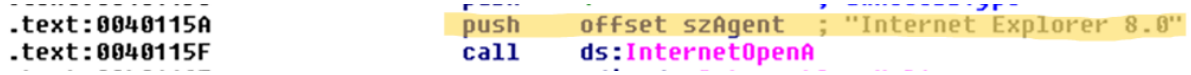
call esi ; RegOpenKeyExW

chiamata alla funzione RegOpenKeyExW per aprire la chiave di registro. I valori vengono pushati nello stack prima della chiamata alla funzione.

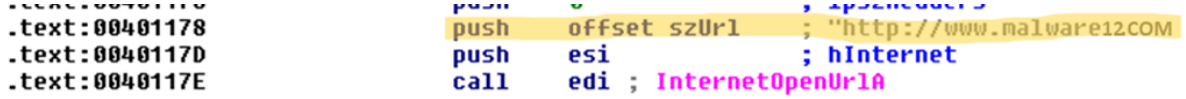
```
)04028A8   push    ecx                 ; lpValueName
)04028A9   push    edx                 ; hKey
)04028AA   call    ds:RegSetValueExW
```

La funzione RegSetValueExW viene chiamata per impostare un valore nella chiave di registro permettendo al programma di avviarsi automaticamente all’accensione del sistema.

Come si può notare nella seconda slide della traccia, il client software identificato che il malware utilizza per connettersi ad Internet fa riferimento a **Internet Explorer 8.0**.
La connessione a Internet avviene attraverso la chiamata alla funzione InternetOpenA (contenuta nella wininet.dll)



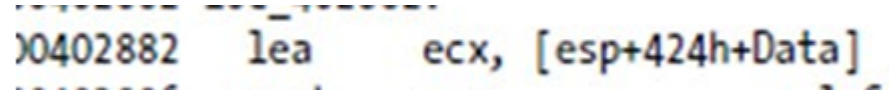
Procedendo con il codice, riusciamo anche ad identificare a quale URL il malware tenta la connessione:



Si può chiaramente notare che tenta la connessione all'indirizzo http://www.malware12.com

La connessione all'URL specificato avviene attraverso la chiamata alla funzione InternetOpenUrlA (anch'essa appartenente alla wininet.dll)

Viene infine richiesto di descrivere il significato e il funzionamento del comando assembly **lea** riportato nel codice, come nell'esempio:



lea sta per **Load Effective Address** e viene utilizzato in assembly per calcolare un indirizzo di memoria e metterlo in un registro specifico, senza leggere o modificare i dati che si trovano a quell'indirizzo.