Consegna S11 L1:

EPICODE

Esercizio
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**"

Traccia:

```
)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
```

Traccia:

```
.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
```

SVOLGIMENTO:

Meccanismo di Persistenza

- **Descrizione:** Il malware ottiene la persistenza modificando il Registro di Windows, specificamente la chiave Run, che viene comunemente utilizzata per avviare automaticamente le applicazioni all'accesso dell'utente.

- **Codice Rilevante:**
  - Il segmento di codice fornito include una chiamata a RegOpenKeyExW per aprire la chiave del registro "Software\\Microsoft\\Windows\\CurrentVersion\\Run".
  - Successivamente, viene impostato un valore utilizzando la funzione RegSetValueExW. Il valore aggiunto alla chiave Run garantirà che il malware venga eseguito ogni volta che il sistema si avvia.

- **Istruzioni Specifiche:**
  - **RegOpenKeyExW:** Apre la chiave del registro per la scrittura.
  - **RegSetValueExW:** Scrive un nuovo valore (di solito il percorso dell'eseguibile del malware) per garantire la persistenza.

0040286F push 2 ; samDesired (specifica i diritti di accesso)

00402871 push eax ; ulOptions (opzioni specifiche per l'apertura della chiave)

00402872 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run " (chiave di registro da modificare)

00402877 push HKEY_LOCAL_MACHINE ; hKey (il contesto della chiave del registro)

0040287C call esi ; RegOpenKeyExW (apre la chiave di registro specificata)

00402881 test eax, eax ; Verifica se l'apertura della chiave ha avuto successo

00402883 jnz short loc_4028C5 ; Se non ha successo , salta alla locazione di errore

00402882 loc_402882: 00402886 lea ecx, [esp+424h+Data] ; lpString (carica l'indirizzo della stringa in ecx)

Software Client Utilizzato per la Connessione a Internet

- **Descrizione:** Il malware utilizza la funzione InternetOpenA, che fa parte delle API di Windows, per iniziare una connessione a Internet.

- **Codice Rilevante:**
  - Il codice include una chiamata a InternetOpenA, passando la stringa "Internet Explorer 8.0", suggerendo che il malware sta impersonando o utilizzando Internet Explorer per effettuare richieste di rete.

- **Istruzioni Specifiche:**
  - **InternetOpenA:** Inizializza le funzioni internet e consente al malware di impostare lo user agent su "Internet Explorer 8.0".

0040288B mov ecx, eax ; Memorizza il valore dell'handle della chiave di registro

0040288D call ds:lstrlenW ; Calcola la lunghezza della stringa

0040288F lea edx, [eax+eax+2] ; Prepara i dati per l'inserimento nel registro

00402894 mov edx, [esp+428h+hKey] ; Carica l'handle della chiave di registro in edx

00402899 lea eax, [esp+428h+Data] ; Carica l'indirizzo dei dati da scrivere

0040289C push eax ; lpData (dati da scrivere nel registro) 0040289D push 1 ; dwType (tipo di dati: REG_SZ)

0040289F push 0 ; Reserved (riservato , impostato a 0)

004028 A8 push ecx ; hKey (handle della chiave di registro)

004028 AA call ds:RegSetValueExW ; Scrive i dati nel registro per garantire la persistenza

• push offset szAgent: Questo comando inserisce l'indirizzo della stringa "Internet Explorer 8.0" nello stack, definendo cos`ı l'user-agent utilizzato dal malware.

• call ds:InternetOpenA: Inizializza una connessione Internet, utilizzando l'user-agent specificato. Questo permette al malware di operare in modo simile a un normale browser.

• call ds:InternetOpenUrlA: Questa chiamata di funzione apre una connessione all'URL specificato. In questo caso, si tratta dell'URL maligno http://www.malware12.COM.

.text :00401150 push offset szAgent ; "Internet Explorer 8.0" (specifica l'user□agent)

.text :00401155 call ds:InternetOpenA ; Inizializza una connessione Internet

.text :0040115A mov edi, ds:InternetOpenUrlA ; Prepara la funzione per aprire l'URL

.text :0040115F push offset szUrl ; "http://www.malware12.COM" (URL di destinazione)

.text :00401167 call edi ; Esegue la connessione all'URL specificato

Connessione a un URL

- **Descrizione:** Il malware tenta di connettersi a un URL utilizzando la funzione InternetOpenUrlA.

- **Codice Rilevante:**
  - Il codice contiene una chiamata a InternetOpenUrlA con l'URL "http://www.malware12.com", che probabilmente è il server di comando e controllo o un sito per scaricare ulteriori payload.

- **Istruzioni Specifiche:**
  - **InternetOpenUrlA:** Apre l'URL specificato utilizzando l'handle di internet precedentemente inizializzato.

Bonus: Spiegazione del Comando LEA

- **Descrizione:** L'istruzione lea (Load Effective Address) in assembly viene utilizzata per calcolare l'indirizzo di un operando di memoria e memorizzarlo in un registro.
- **Funzionamento:**
  - Invece di accedere al valore all'indirizzo, lea calcola l'indirizzo stesso e lo memorizza nel registro. Viene spesso utilizzato per l'aritmetica dei puntatori, come il calcolo degli indici di array o l'accesso ai membri di una struttura.