SETTIMANA 11 ESERCIZIO 1

1)

Il malware assicura la sua persistenza nel sistema operativo mediante l'inserimento di un nuovo valore nella chiave di registro Software\Microsoft\Windows\CurrentVersion\Run. Questa chiave contiene i programmi avviati automaticamente all'avvio del sistema. Per fare ciò, il malware utilizza le funzioni RegOpenKey, che apre la chiave di registro desiderata, e RegSetValueEx, che consente di aggiungere un nuovo valore a quella chiave. I parametri necessari vengono passati attraverso lo stack tramite istruzioni "push" prima della chiamata della funzione. In sostanza, il malware sfrutta queste funzioni per garantire che il suo codice venga eseguito ogni volta che il sistema si avvia, assicurandosi così una presenza persistente nel sistema.

2)

```
.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
```

Il malware utilizza Internet Explorer, specificamente la versione 8, come client per connettersi a Internet. In altre parole, questo programma viene sfruttato dal malware per stabilire una connessione alla rete.

3)

```
.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 tenta di stabilire una connessione con l'URL www.malware12.com utilizzando la funzione di chiamata "InternetOpenURL". Questa funzione consente al malware di connettersi a un determinato indirizzo web. L'URL viene passato come parametro attraverso lo stack, utilizzando l'istruzione "push". In sostanza, questa

azione permette al malware di avviare una comunicazione con il server ospitato all'indirizzo specificato.