

1. Soluzione – Persistenza Il malware ottiene la persistenza inserendo un nuovo valore all'interno della chiave di registro Software\\Microsoft\\Windows\\CurrentVersion\\Run, che include tutti i programmi che sono avviati all'avvio del sistema operativo. Le funzioni utilizzate sono: 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
2. Soluzione – Client utilizzato per la connessione ad Internet Il client utilizzato dal malware per connettersi ad internet è Internet Explorer, più precisamente la versione 8.

```

.text:00401154      push     0                ; lpzProxyBypass
.text:00401156      push     0                ; lpzProxy
.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:00401168      mov      esi, eax

```

3. Soluzione – URL di destinazione Il malware cerca di connettersi all'URL www.malware12.com. La chiamata di funzione che consente al malware la connessione verso un URL è «Internet OpenURL». L'URL è passato come parametro di questa funzione sullo stack, tramite l'istruzione push.

```

.text:0040116D      push     0                ; dwContext
.text:0040116F      push     80000000h        ; dwFlags
.text:00401174      push     0                ; dwHeadersLength
.text:00401176      push     0                ; lpzHeaders
.text:00401178      push     offset szUrl     ; "http://www.malware12.com"
.text:0040117D      push     esi              ; hInternet
.text:0040117E      call     edi ; InternetOpenUrlA
.text:00401180      jmp      short loc_40116D
.text:00401180      StartAddress      endp

```