

CS0304

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.
- **RegSetValueEx**, che permette al malware di inserire un nuovo valore all'interno della chiave di registro appena aperta

Il client utilizzato dal malware per connettersi ad internet è Internet Explorer, più precisamente la versione 8.

```
.text:00401154      ; lpszProxyBypass
.text:00401156      ; lpszProxy
.text:00401158      ; dwAccessType
.text:0040115A      ; "Internet Explorer 8.0"
.text:0040115F      ; ds:InternetOpenA
.text:00401165      ; ds:InternetOpenUrlA
.text:0040116B      ; esi.eax

push 0
push 0
push 1
push offset szAgent
call ds:InternetOpenA
mov edi, ds:InternetOpenUrlA
mov esi, eax
```



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

```
.text:0040116D      ; dwContext
.text:0040116F      ; dwFlags
.text:00401174      ; dwHeadersLength
.text:00401176      ; lpszHeaders
.text:00401178      ; "http://www.malware12COM"
.text:0040117D      ; hInternet
.text:0040117E      ; edi ; InternetOpenUrlA
.text:00401180      ; jmp short loc_40116D
.text:00401180      ; StartAddress
push 0
push 80000000h
push 0
push 0
push offset szUrl
push esi
call edi ; InternetOpenUrlA
jmp short loc_40116D
endp
```

Cercando su internet ho capito che Il comando assembly "lea" sta per "Load Effective Address" ed è utilizzato per caricare l'indirizzo effettivo di una variabile o di un'area di memoria in un registro della CPU.

Esempio: *lea eax, var*

In cui *eax* è il registro in cui verrà caricato l'indirizzo effettivo di *var*.