1- Persistenza
Il malware si insidia all'interno della macchina infetta inserendosi all'interno dell'ultima configurazione disponibile del PC, pertanto all'avvio del computer il malware si attiverà come eseguibile. Possiamo vederlo dalla stringa "Software\\Microsoft\\Windows\\CurrentVersion\\Run"

```
)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
```

2- Il Client utilizzato è Internet Explorer 8.0, visibile dalla stringa "Internet Explorer 8.0"

```
.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
```

3- L'URL al quale il malware tenta la connessione è www.malware12.com

```
.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
```

4- La chiamata di funzione è "InternetOpenUr1A"

```
.text:0040117E                  call    edi ; InternetOpenUrlA
.text:00401180                  jmp     short loc_40116D
.text:00401180 StartAddress     endp
```