Esercizio G1

Analisi Statica Avanzata

1

```
)0402871   push    eax             ; ulOptions
)0402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
```

Nell'immagine di sopra troviamo una chiamata di RegOpneKey ed i parametri passati tramite push, che serve per aprire una chiave di registro e modificarne il valore

Qui troviamo RegSetValue dove i parametri passati tramite push. La funzione viene utilizzata per modificare il valore del registro, ed aggiungere una nuova entry per poter ottenere la persistenza all'avvio delle macchina.

```
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

2. Qui troviamo il tipo di browser usato dal malware e la sua funzione chiamante.

```
.text:0040115A                  push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                  call    ds:InternetOpenA
```

3. L'URL al quale il malware tentava di connettersi e la sua funzione chiamante.

```
.text:00401178                  push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                  push    esi             ; hInternet
.text:0040117E                  call    edi ; InternetOpenUrlA
```