WINDOWS MALWARE

Kamenica Kristiano

- Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite

```
00402871   push    eax             ; ulOptions
00402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877   push    HKEY_LOCAL_MACHINE ; hKey
```

```
004028A8   push    ecx             ; lpValueName
004028A9   push    edx             ; hKey
004028AA   call    ds:RegSetValueExW
```

In sostanza, il malware prima apre la chiave di registro e successivamente imposta il valore. Questo permette al malware di avviarsi automaticamente ogni volta che si avvia il computer.

- Identificare il client software utilizzato dal malware per la connessione ad Internet

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

Come possiamo notare il client software utilizzato e Internet Explorer 8.0

- Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL

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

In queste tre righe è evidente l'inizializzazione del parametro dell'URL e il suo passaggio alla funzione InternetOpenUrl. Ciò consente l'utilizzo dell'handler che gestisce la connessione hInternet e l'apertura dell'URL