S11/L1

Windows Malware

Traccia: Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- Identificare il client software utilizzato dal malware per la connessione ad Internet
- 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

```
)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
```

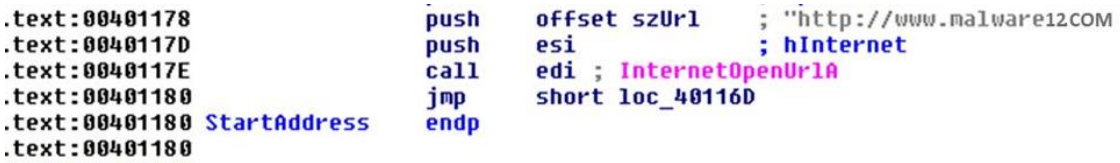
In queste righe di codice si passano i parametri del RegOpenKeyxW sullo stack e successivamente viene usata l'istruzione call per chiamare la funzione dentro "esi".

```
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx               ; lpValueName
)04028A9   push    edx               ; hKey
)04028AA   call    ds:RegSetValueExW
```

In queste righe si modificano i valori del registro utilizzando il set di comandi "lea" e "push" che caricano nello stack i valori che cambiano il registro per fare in modo che il malware abbia l'accesso persistente all'avvio del sistema operativo.

```
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
.text:00401165                 mov     edi, ds:InternetOpenUrlA
.text:0040116B                 mov     esi, eax
```

Il client software utilizzato dal malware è "Internet Explorer 8.0"



L'URL utilizzato dal malware è http://www.malware.12.com", mentre la chiamata di funzione che permette al malware di connettersi all' URL è la funzione "call edi; InternetOpenUrlA"