S11/L1

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
- BONUS: qual è il significato e il funzionamento del comando assembly "lea"

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

```
)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
```

Individuazione delle istruzioni assembly finalizzate all'ottenimento della persistenza da parte del malware

- I malware usano il registro per ottenere la persistenza: si introducono nei registri per ottenere l'accesso all'avvio in maniera automatica e permanente senza azioni dall'utente.
- Una delle chiavi di registro che vengono utilizzate dai malware per ottenere la persistenza su windows è "Sofware\\microsoft\\ Windows\\CurrentVersion\\Run".
- Per ottenere la persistenza, il malware chiama due funzioni:
- RegOpenKeyEx per l'accesso alla key.
- RegOpneKeyEx con questa funzione il malware ha accesso alla chiave di registro prima di modificarne il valore.
- RegSetValueEx la funzione viene utilizzata dal malware per modificarne il valore di registro aggiungendo una nuova entry in modo da ottenere una persistenza all'avvio del sistema operativo.

IDENTIFICAZIONE DEL CLIENT SOFWARE UTILIZZATO PER L'ACCESSO A INTERNET

- Il malware tenta di inizializzare una connessione a internet. Il client sofware utilizzato per l'accesso a internet è Internet explorer 8.0.

```
.text:0040115A                push    offset szAgent  ; "Internet Explorer 8.0"
```

Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzion eche permette al malware di connettersi ad un URL

- Microsoft coloca delle APIs per gestire il networking ad ampio raggio, vengono chiamate WinInet APIs, incluse nella libreria WinInet.dll.
- Le funzioni della libreria includono implementazione di protocolli di rete come HTTP e FTP.
- Le più comuni sono:
- InternetOpen la funzione viene utilizzata per inizializzare una connessione a internet.
- InternetOpenUrl la funzione viene utulizzata per la connessione ad un determinato URL.

```
.text:0040115F                call    ds:InternetOpenA
.text:00401165                mov     edi, ds:InternetOpenUrlA
```

BONUS: qual è il significato e il funzionamento del comando assembly"lea"

- Listruzione lea (Load Effective Address) viene utilizzata per il posizionamento a un indirizzo di memoria nella destinazione indicata.