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"

```
push 2    ; samDesired
Push eax  ; ulOptions
Push offset SubKey  ; “Software \Microsoft\Windows\CurrentVersion\Run”
Push HKEY_LOCAL_MACHINE   ; hKey
Call esi   ; RegOpenKeyExw
Test eax, eax
Jnz short loc_4028C5

loc_402882:
Lea ecx, [esp+424h+Data]
Push ecx  ;  lpString
Mov bl, 1
Call ds: lstrlenW
Lea cdx, [eax+eax+2]
Push edx  ;  cbData
Mov edx, [esp+428h+hKey]
Lea eax, [esp+428h+Data]
Push eax  ;  lpData
Push 1 ;  dwType
Push 0 ;  Reserved
Lea ecx ;  [esp+434h+ValueName]
Push ecx  ;  lpValueName
Push edx ;  hKey
Call ds:RegSetValueExW
```

SUBROUTINE

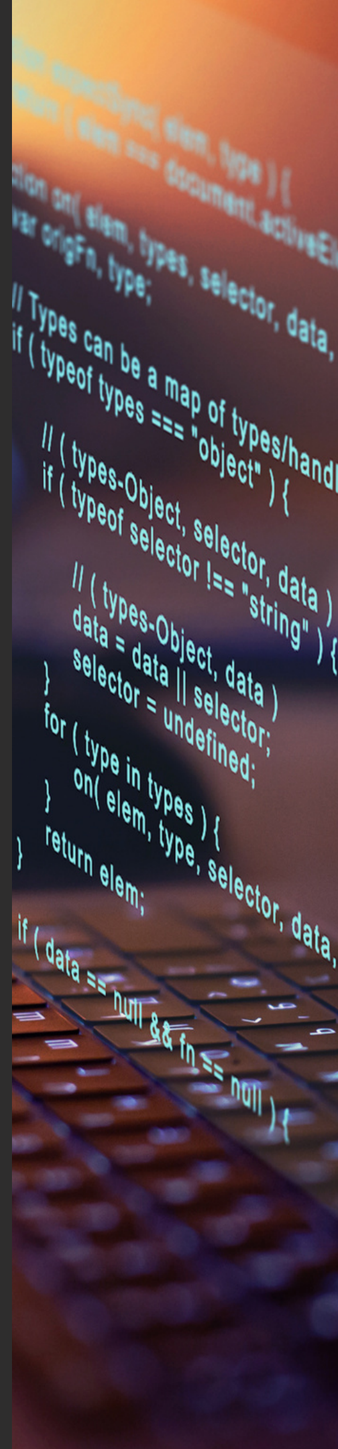
```
DWORD _stdcall StartAddress(LPUOID)
StartAddress proc near ; DATA XREF: Sub_401040+ECTo
push esi
push edi
push 0  ;  dwFlags
push 0 ; lpszProxyBypass
push 0 ; lpszProxy
push 1 ; dwAccessType
push offset szAgent ; “Internet Explorer 8.0”
Call ds:InternetOpenA
Mov edi, ds:InternetOpenUrlA
Mov esi, eax

loc_40116D    ;   CODE XREF : StartAddress+30 j
Push 0  ;  dwContext
Push 80000000h ;  dwFlags
Push 0 ; dwHeadersLength
Push 0 ; lpszHeaders
Push offsetszUrl ; “http://www.malware12.com/
Push esi. ; hInternet
Call edi ; InternetOperUrlA
Jmp short loc_40116D

StartAddress endp
```

```
Push offset SubKey ; "Software \Microsoft\Windows\CurrentVersion\Run"
Push HKEY_LOCAL_MACHINE  ; hKey
Call esi  ; RegOpenKeyExw
```

In questa parte del codice assembly il malware va ad aprire la chiave di registro

```
Push ecx ;  lpValueName
Push edx ;  hKey
Call ds:RegSetValueExW
```

In questa parte invece viene inserito il valore all'interno della chiave, andando a modificare l'originale, così facendo il malware sarà in grado di avviarsi automaticamente all'avvio del pc.

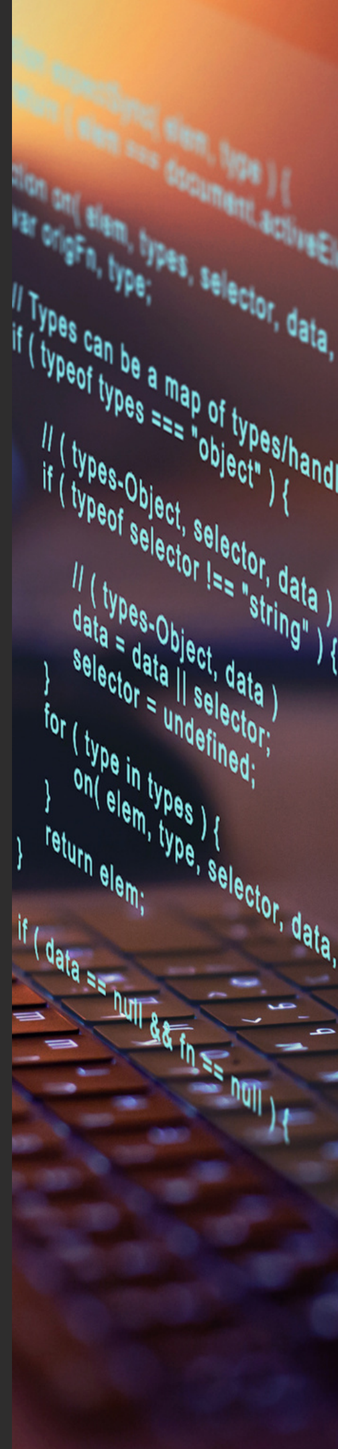


```
push offset szAgent ; "Internet Explorer 8.0"
Call ds:InternetOpenA
Mov edi, ds:InternetOpenUrlA
```

in questa parte della subroutine viene salvato l'indirizzo di memoria in cui è memorizzata la stringa "Internet Explorer 8.0" nello stack. Pertanto possiamo presupporre che il client software utilizzato sia proprio quest'ultimo. La funzione viene spostata nel registro edi

```
Push offsetszUrl ; "http://www.malware12.com/
Push esi. ; hInternet
Call edi ; InternetOperUrlA
```

qui è riportato l'url al quale il malware cerca di collegarsi, l' istruzione, "call edi ; InternetOperUrlA", chiama la funzione indicata dall'indirizzo contenuto nel registro edi per aprire l'url indicato.



BONUS:

"lea" calcola l'indirizzo di memoria dell'operando e carica questo indirizzo in un registro specificato, senza caricare il valore effettivo memorizzato in quell'indirizzo.
La sintassi generale del comando "lea" è:

lea destination, source