

Analisi Malware

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

Pratica STI/LI PDF

EPICODE

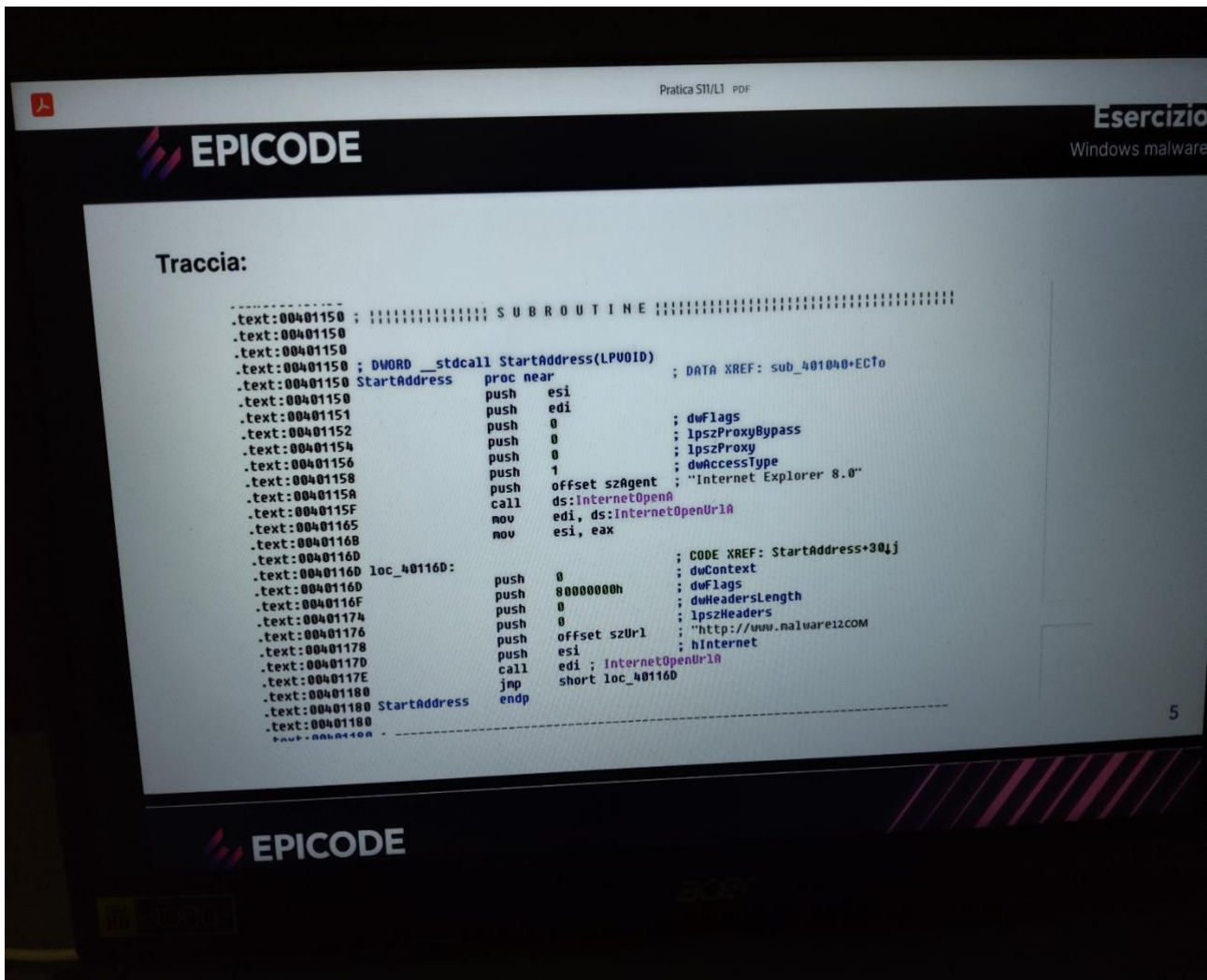
Esercizio
Windows malware

Traccia:

```
X040286F push 2 ; samDesired
X0402871 push eax ; ulOptions
X0402872 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
X0402877 push HKEY_LOCAL_MACHINE ; hKey
X040287C call esi ; RegOpenKeyExW
X040287E test eax, eax
X0402880 jnz short loc_4028C5
X0402882
X0402882 loc_402882:
X0402882 lea ecx, [esp+424h+Data]
X0402886 push ecx ; lpString
X0402887 mov bl, 1
X0402889 call ds:strlenW
X040288F lea edx, [eax+eax+2]
X0402893 push edx ; cbData
X0402894 mov edx, [esp+428h+hKey]
X0402898 lea eax, [esp+428h+Data]
X040289C push eax ; lpData
X040289D push 1 ; dwType
X040289F push 0 ; Reserved
X04028A1 lea ecx, [esp+434h+ValueName]
X04028A8 push ecx ; lpValueName
X04028A9 push edx ; hKey
X04028AA call ds:RegSetValueExW
```

4

Esercizio



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

La persistenza è il modo che ha il malware per resistere all'interno del sistema e avviare tutti i suoi processi

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

Offset subkey: "Software\\Microsoft\\Windows\\Current version\\Run"

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:

Offset szurl <http://www.Malware12.com>

