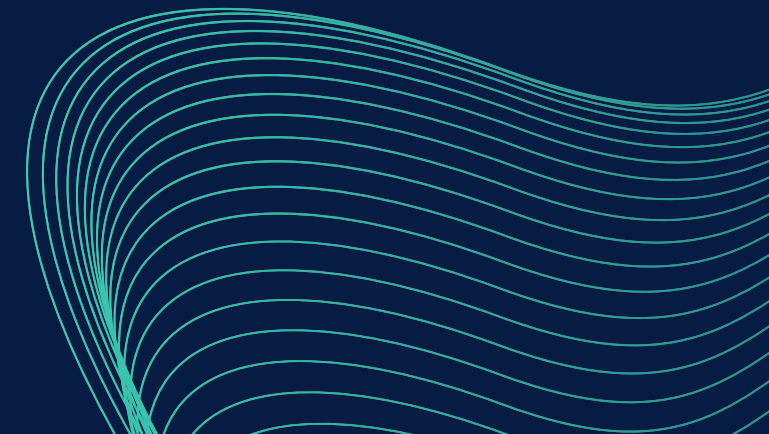




Traccia:

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**"
- 

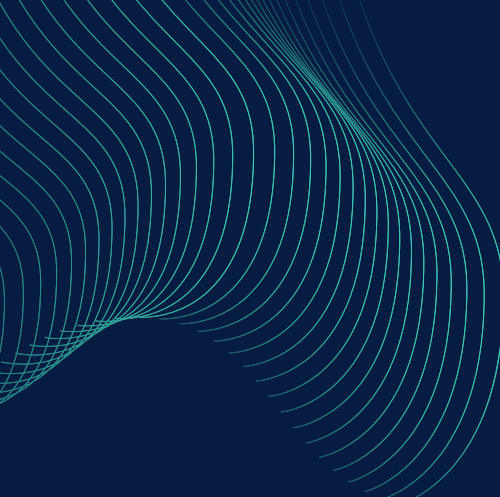
RegSetValueExW

Funzione permette invece di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati. Accetta come parametri la chiave, la sottochiave e il dato da inserire.

I valori sono passati sullo stack tramite le istruzioni «pushecx» e «pushedx».

La funzione viene utilizzata dal malware per modificare il valore del registro ed aggiungere una nuova entry in modo tale da ottenere la persistenza all'avvio del sistema operativo.

```
0040289D  push 1 ; dwType
0040289F  push 0 ; Reserved
004028A1  lea ecx, [esp+434h+ValueName]
004028A8  push ecx ; lpValueName
004028A9  push edx ; hKey
004028AA  call ds:RegSetValueExW
```



E' una delle chiavi di registro che viene utilizzata dai malware per ottenere persistenza su un sistema operativo Windows.

```
0402872 push offset SubKey ; "Software\Microsoft\Windows\CurrentVersion\Run"
```

"Software\Microsoft\Windows\CurrentVersion\Run"

URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione

