

# 14

- 1    OpenProcess
  - 2    C++    CreateProcess API    calc.exe
  - 3    P/Invoke        OpenProcess    calc.exe
  - 4    D/Invoke    OpenProcess    calc.exe
  - 5 D/Invoke        **GetPebLdrModuleEntry**    DLL        D/Invoke    README
  - 6        VBA    PowerShell    OpenProcess    calc.exe
  - 7 .NET    Shellcode **VirtualAlloc Marshal.Copy**    Shellcode **CreateThread WaitForSingleObject**  
          API        C#        P/Invoke    D/Invoke
  - 8    PE Bear **ws2\_32.dll**
  - 9 **calc\_dllmain()**    CreateThread **WaitForSingleObject**
  - 10    C# **P/Invoke D/Invoke explorer.exe PID**
  - 11 133 4869 51203
  - 12        **LoadLibraryA**    DLL **ws2\_32.dll**
- ```
mov rsi, 0x6c6c;  
_____  
mov rsi, _____;  
push rsi;  
_____  
sub rsp, ____;  
call rax;  
_____;
```
- 13    WinDBG    ws2\_32.dll    PE Bear                    IAT    RVA
  - 14        calc.exe **WinExec CreateProcessA**

|    |       |           |     |       |           |
|----|-------|-----------|-----|-------|-----------|
| 15 | Shell | Shellcode |     |       |           |
| 16 | x86   | x64       | x86 | Shell | Shellcode |

---

Revision #10

Created 1 May 2023 13:42:53 by

Updated 28 January 2024 05:10:12 by