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** Shellcode **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