Beacon

explorer.exe

CreateToolhelp32Snapshot PID

```
HANDLE CreateToolhelp32Snapshot(
  [in] DWORD dwFlags,
  [in] DWORD th32ProcessID
);
```

TH32CS_SNAPPROCESS **Process32First**

```
BOOL Process32First(
  [in]      HANDLE           hSnapshot,
  [in, out] LPPROCESSENTRY32 lppe
);
```

PID

```
DWORD FindExplorerProcessId()
{
    HANDLE hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    if (hSnapshot)
    {
        PROCESSENTRY32 pe32;
        pe32.dwSize = sizeof(PROCESSENTRY32);
        if (Process32First(hSnapshot, &pe32))
        {
            do
            {
                if (_wcsicmp(pe32.szExeFile, L"explorer.exe") == 0)
                {
                    CloseHandle(hSnapshot);
                    return pe32.th32ProcessID; // Returns the first instance's PID
                }
            } while (Process32Next(hSnapshot, &pe32));
        }
        CloseHandle(hSnapshot);
    }
    return 0;
}
```

PID OpenProcess

```
HANDLE parentProcessHandle = OpenProcess(MAXIMUM_ALLOWED, false, pid);
```

STARTUPINFOEX lpAttributeList CreateProcess

```
typedef struct _STARTUPINFOEXW {
  STARTUPINFOW                 StartupInfo;
  LPPROC_THREAD_ATTRIBUTE_LIST lpAttributeList;
} STARTUPINFOEXW, *LPSTARTUPINFOEXW;
```

PROC_THREAD_ATTRIBUTE_PARENT_PROCESS

```
BOOL InitializeProcThreadAttributeList(
  [out, optional] LPPROC_THREAD_ATTRIBUTE_LIST lpAttributeList,
  [in]            DWORD                        dwAttributeCount,
                  DWORD                        dwFlags,
  [in, out]       PSIZE_T                      lpSize
);
```

InitializeProcThreadAttributeList lpAttributeList NULL

```
SIZE_T attributeSize;
InitializeProcThreadAttributeList(NULL, 1, 0, &attributeSize);
```

attributeSize LPPROC_THREAD_ATTRIBUTE_LIST (lpAttributeList) **InitializeProcThreadAttributeList**

```
si.lpAttributeList = (LPPROC_THREAD_ATTRIBUTE_LIST)HeapAlloc(GetProcessHeap(), 0,
attributeSize);
InitializeProcThreadAttributeList(si.lpAttributeList, 1, 0, &attributeSize);
```

UpdateProcThreadAttribute

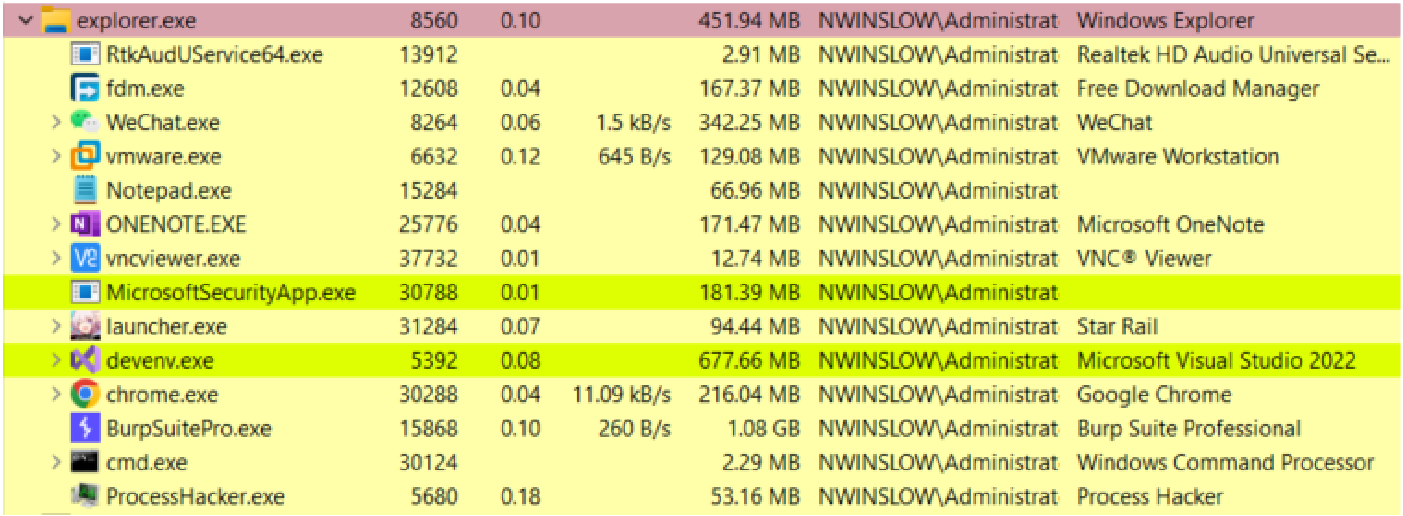
```
BOOL UpdateProcThreadAttribute(
  [in, out]       LPPROC_THREAD_ATTRIBUTE_LIST lpAttributeList,
  [in]            DWORD                        dwFlags,
  [in]            DWORD_PTR                    Attribute,
  [in]            PVOID                        lpValue,
  [in]            SIZE_T                       cbSize,
  [out, optional] PVOID                        lpPreviousValue,
  [in, optional]  PSIZE_T                      lpReturnSize
);
```

dwCreationFlags EXTENDED_STARTUPINFO_PRESENT

```
UpdateProcThreadAttribute(si.lpAttributeList, 0, PROC_THREAD_ATTRIBUTE_PARENT_PROCESS,
&parentProcessHandle, sizeof(HANDLE), NULL, NULL);
si.StartupInfo.cb = sizeof(STARTUPINFOEXA);
CreateProcessA(NULL, (LPSTR)"notepad", NULL, NULL, FALSE, EXTENDED_STARTUPINFO_PRESENT, NULL,
NULL, &si.StartupInfo, &pi);
```

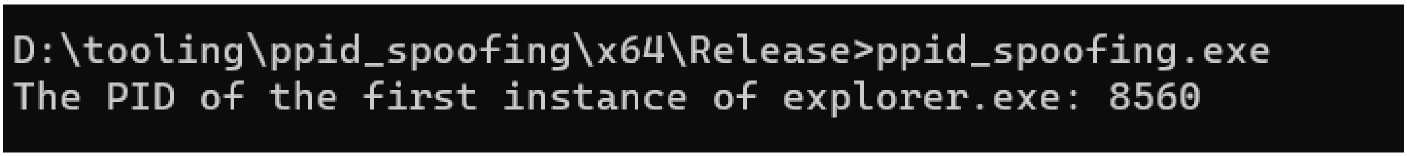
```
#include <windows.h>
#include <TlHelp32.h>
#include <iostream>

DWORD FindExplorerProcessId()
{
    HANDLE hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    if (hSnapshot)
    {
        PROCESSENTRY32 pe32;
        pe32.dwSize = sizeof(PROCESSENTRY32);
        if (Process32First(hSnapshot, &pe32))
        {
            do
            {
                if (_wcsicmp(pe32.szExeFile, L"explorer.exe") == 0)
                {
                    CloseHandle(hSnapshot);
                    return pe32.th32ProcessID; // Returns the first instance's PID
                }
            } while (Process32Next(hSnapshot, &pe32));
        }
        CloseHandle(hSnapshot);
    }
    return 0;
}




int main()
{
    DWORD pid = FindExplorerProcessId();
    if (pid != 0)
    {
        printf("The PID of the first instance of explorer.exe: %lu\n", pid);
    }
    else
    {
        printf("explorer.exe is not running.\n");
    }

    STARTUPINFOEXA si;
    PROCESS_INFORMATION pi;
    SIZE_T attributeSize;
    ZeroMemory(&si, sizeof(STARTUPINFOEXA));
    HANDLE parentProcessHandle = OpenProcess(MAXIMUM_ALLOWED, false, pid);
    InitializeProcThreadAttributeList(NULL, 1, 0, &attributeSize);
    si.lpAttributeList = (LPPROC_THREAD_ATTRIBUTE_LIST)HeapAlloc(GetProcessHeap(), 0,
attributeSize);
    InitializeProcThreadAttributeList(si.lpAttributeList, 1, 0, &attributeSize);
    UpdateProcThreadAttribute(si.lpAttributeList, 0, PROC_THREAD_ATTRIBUTE_PARENT_PROCESS,
&parentProcessHandle, sizeof(HANDLE), NULL, NULL);
    si.StartupInfo.cb = sizeof(STARTUPINFOEXA);
    CreateProcessA(NULL, (LPSTR)"notepad", NULL, NULL, FALSE, EXTENDED_STARTUPINFO_PRESENT, NULL,
NULL, &si.StartupInfo, &pi);

    return 0;
}
```

explorer.exe cmd.exe



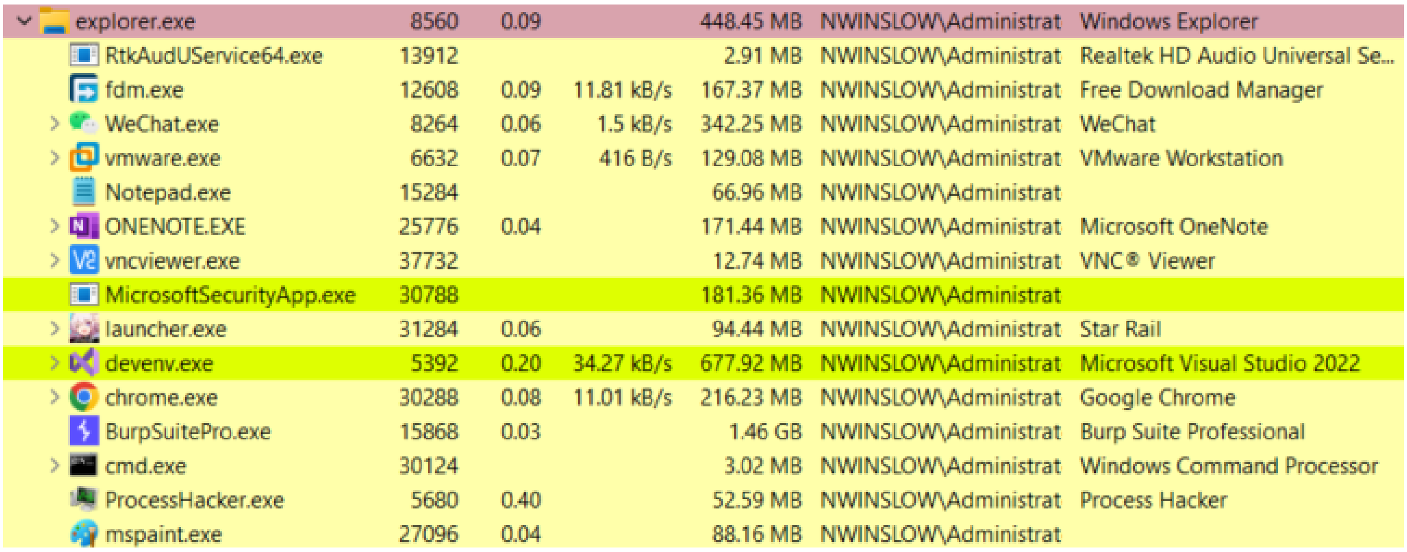
explorer.exe	8560	0.10		451.94 MB	NWINSLOW\Administrat	Windows Explorer
RtkAudUService64.exe	13912			2.91 MB	NWINSLOW\Administrat	Realtek HD Audio Universal Se...
fdm.exe	12608	0.04		167.37 MB	NWINSLOW\Administrat	Free Download Manager
WeChat.exe	8264	0.06	1.5 kB/s	342.25 MB	NWINSLOW\Administrat	WeChat
vmware.exe	6632	0.12	645 B/s	129.08 MB	NWINSLOW\Administrat	VMware Workstation
Notepad.exe	15284			66.96 MB	NWINSLOW\Administrat	
ONENOTE.EXE	25776	0.04		171.47 MB	NWINSLOW\Administrat	Microsoft OneNote
vncviewer.exe	37732	0.01		12.74 MB	NWINSLOW\Administrat	VNC® Viewer
MicrosoftSecurityApp.exe	30788	0.01		181.39 MB	NWINSLOW\Administrat	
launcher.exe	31284	0.07		94.44 MB	NWINSLOW\Administrat	Star Rail
devenv.exe	5392	0.08		677.66 MB	NWINSLOW\Administrat	Microsoft Visual Studio 2022
chrome.exe	30288	0.04	11.09 kB/s	216.04 MB	NWINSLOW\Administrat	Google Chrome
BurpSuitePro.exe	15868	0.10	260 B/s	1.08 GB	NWINSLOW\Administrat	Burp Suite Professional
cmd.exe	30124			2.29 MB	NWINSLOW\Administrat	Windows Command Processor
ProcessHacker.exe	5680	0.18		53.16 MB	NWINSLOW\Administrat	Process Hacker

explorer.exe -> cmd.exe -> ppid_spoofing.exe -> mspaint.exe



```
D:\tooling\ppid_spoofing\x64\Release>ppid_spoofing.exe
The PID of the first instance of explorer.exe: 8560
```

mspaint.exe explorer.exe



explorer.exe	8560	0.09		448.45 MB	NWINSLOW\Administrat	Windows Explorer
RtkAudUService64.exe	13912			2.91 MB	NWINSLOW\Administrat	Realtek HD Audio Universal Se...
fdm.exe	12608	0.09	11.81 kB/s	167.37 MB	NWINSLOW\Administrat	Free Download Manager
WeChat.exe	8264	0.06	1.5 kB/s	342.25 MB	NWINSLOW\Administrat	WeChat
vmware.exe	6632	0.07	416 B/s	129.08 MB	NWINSLOW\Administrat	VMware Workstation
Notepad.exe	15284			66.96 MB	NWINSLOW\Administrat	
ONENOTE.EXE	25776	0.04		171.44 MB	NWINSLOW\Administrat	Microsoft OneNote
vncviewer.exe	37732			12.74 MB	NWINSLOW\Administrat	VNC® Viewer
MicrosoftSecurityApp.exe	30788			181.36 MB	NWINSLOW\Administrat	
launcher.exe	31284	0.06		94.44 MB	NWINSLOW\Administrat	Star Rail
devenv.exe	5392	0.20	34.27 kB/s	677.92 MB	NWINSLOW\Administrat	Microsoft Visual Studio 2022
chrome.exe	30288	0.08	11.01 kB/s	216.23 MB	NWINSLOW\Administrat	Google Chrome
BurpSuitePro.exe	15868	0.03		1.46 GB	NWINSLOW\Administrat	Burp Suite Professional
cmd.exe	30124			3.02 MB	NWINSLOW\Administrat	Windows Command Processor
ProcessHacker.exe	5680	0.40		52.59 MB	NWINSLOW\Administrat	Process Hacker
mspaint.exe	27096	0.04		88.16 MB	NWINSLOW\Administrat	

Revision #18
Created 1 June 2023 03:05:41 by
Updated 24 March 2024 15:18:05 by