

Wsreset tool of Windows 10 Store was used by hackers to bypass anti-virus software

Wsreset.exe is a legitimate debugging tool used by many users to identify problems and reinstall caching in the Windows Store.

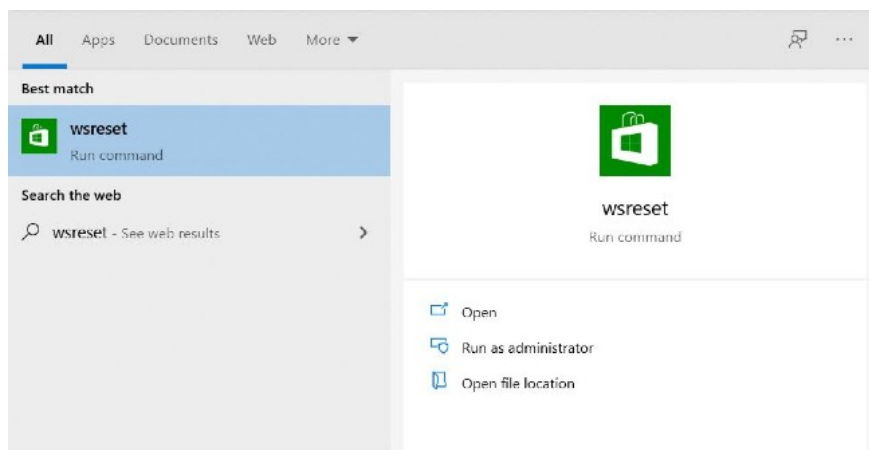
Recently, security researcher Daniel Gelbert and Pentester discovered that the Wsreset.exe tool could be used to delete any file. Wsreset.exe is a legitimate debugging tool built into windows used to identify problems and reinstall caching in the Windows Store.

Use Wsreset.exe to delete files

The Windows Store stores cached files and temporary cookies that it creates in the following folders:

`%UserProfile%\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\ACINetCache`

After a thorough analysis of Wsreset, Gelbert realized that the tool could delete files contained in the above directories to reinstall the cache and cookies for the Windows Store application.



The Wsreset tool is built into Windows 10

Taking advantage of this and relying on the directory connection function on Windows, the hacker technique is quite simple. Hackers can delete any folder when launching Wsreset by pointing the **INetCookies** path to the folder to be deleted. This has always been successful because Wsreset is granted the highest privilege by default.

Hackers start the setup by deleting the **INetCookies** folder, which Wsreset always prioritizes deleting at launch. To delete this directory, hackers do not need Administrator rights, just find a way to control the user's account or use malicious code.

```

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

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

PS C:\Users\user> Get-Acl "C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\AC\InetCookies" | fl

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Users\user\AppData\Local\Packages\Microsoft.WindowsStore_8wekyb3d8bbwe\AC\InetCookies
Owner     : TESTVM\user
Group     : TESTVM\None
Access    : S-1-15-2-1609473798-1231923017-684268153-4268514328-882773646-2760585773-1760938157 Allow FullControl
          NT AUTHORITY\SYSTEM Allow FullControl
          BUILTIN\Administrators Allow FullControl
          TESTVM\user Allow FullControl
Audit    :
Sddl     : O:5-1-15-21-231341539-3027085644-391807904-1001G:5-1-15-21-231341539-3027085644-391807904-513D:AI(A;OICIIDCR;FA;
          ;S-1-15-2-1609473798-1231923017-684268153-4268514328-882773646-2760585773-1760938157)(A;OICIID;FA;;;SV)(A;OIC
          IID;FA;;;BA)(A;OICIID;FA;;;S-1-15-21-231341539-3027085644-391807904-1001)

PS C:\Users\user>

```

Without Administrator privileges, the InetCookies folder still has full privileges
 Next, the hacker creates a link to replace **InetCookies** with the folder they want **Wsreset** to delete.

In the example below, the hacker is replacing the **InetCookies** folder with "**C: WindowsSystem32driversetc**".
 The etc directory contains important configurations and files, including server files, that define local DNS configuration rules.

"Hackers can do this by using **mklink.exe** with the **/J** parameter or via the new-item powershell command with the **-ItemType**. """, Gelbert explained.

```

Command Prompt
Microsoft Windows [Version 10.0.19041.229]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\user>mklink
Creates a symbolic link.

MKLINK [[/D] | [/H] | [/J]] Link Target

/D      Creates a directory symbolic link. Default is a file
        symbolic link.
/H      Creates a hard link instead of a symbolic link.
/J      Creates a Directory Junction.
Link    Specifies the new symbolic link name.
Target  Specifies the path (relative or absolute) that the new link
        refers to.

C:\Users\user>

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

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

PS C:\Users\user> New-Item -ItemType Junction -Path "SOURCE" -Target "TARGET"

```

Use **mklink.exe** to create a path to the directory you want to delete
 Use **Wsreset** to disable antivirus software

Researchers have demonstrated that by taking advantage of **Wsreset**, hackers can disable anti-virus software on the victim's computer. For example, here's how to disable Adaware software:

"Adaware antivirus software stores configuration files in the **C: ProgramDataadawareadaware antivirus** directory. It needs these files to interact with the malware signature and definition it downloaded earlier. Typically, users cannot delete this directory," Gelbert wrote.

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

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

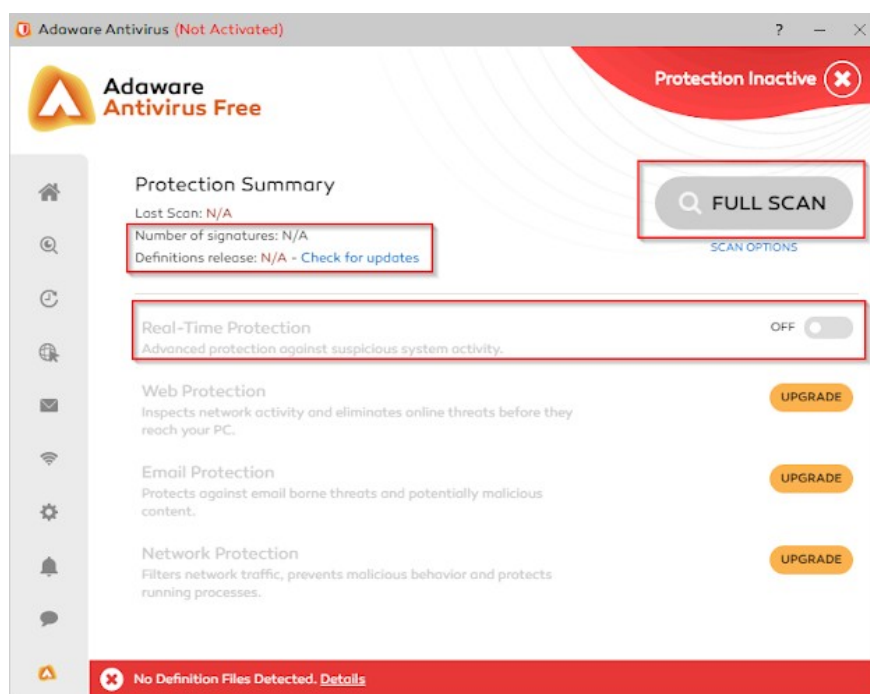
PS C:\Users\user> get-acl "C:\ProgramData\adaware\adaware_antivirus" | fl

Path      : Microsoft.PowerShell.Core\FileSystem::C:\ProgramData\adaware\adaware_antivirus
Owner     : BUILTIN\Administrators
Group     : TEST\N\None
Access    : NT AUTHORITY\SYSTEM Allow FullControl
           BUILTIN\Administrators Allow FullControl
           CREATOR OWNER Allow 268435456
           BUILTIN\Users Allow  ReadAndExecute, Synchronize
           BUILTIN\Users Allow  Write
Audit     :
Sddl     : O:BAG:S-1-5-21-231341539-3027885644-301807904-5130:AI(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIID;GA;;;CO)(
           A;OICIID;0x1200a9;;;BU)(A;CIID:DCLCRPCR;;;BU)

PS C:\Users\user>
```

The Adaware configuration directory cannot be deleted by a user without Administrator rights. When a hacker replaces **INetCookies** with the **adaware antivirus** folder and runs **Wsreset**, the files in this folder will be deleted by **Wsreset** given the highest privilege. Although there are still some files in the **adaware antivirus** folder, this will completely disable the Adaware antivirus software.

After reboot, Adaware will be disabled. This comes from the malicious signature / definition and its core files being removed from the system.



Adaware antivirus software is completely disabled. With great potential, the vulnerability of the **Wsreset.exe** tool can be exploited by hackers for other purposes. For example, 2019 developer Hashim Jawad proved that **Wsreset** can disable the User Account Control (UAC) feature of Windows.

You finished reading the article "**Wsreset tool of Windows 10 Store was used by hackers to bypass anti-virus software**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.