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.

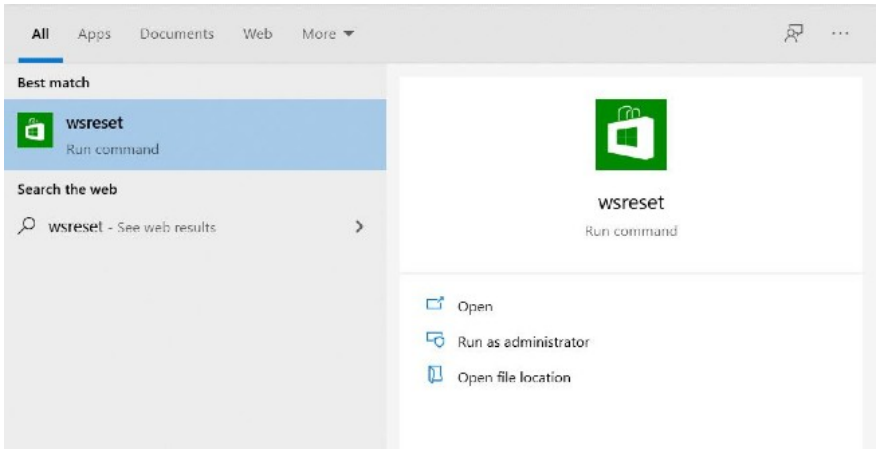
Recently, security researcher Daniel Gelbert and Pentester discovered that the Wsreset.exe tool could be used to delete any file. Wsreset.exe is a legitimate debugging tool built into windows used to identify problems and reinstall caching in the Windows Store.

Use Wsreset.exe to delete files

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

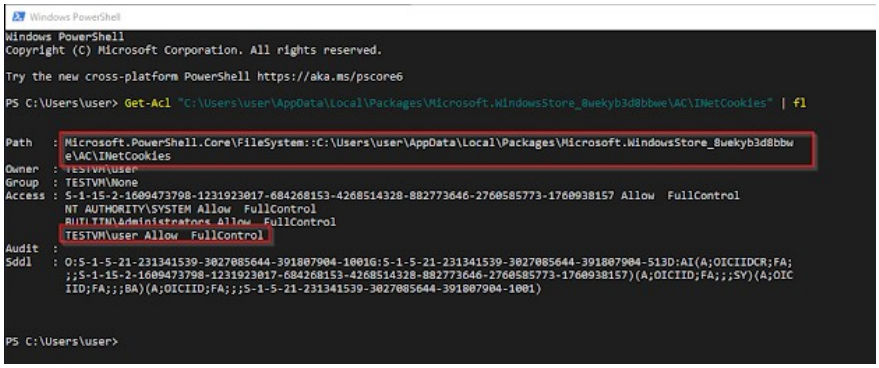
```
%UserProfile%AppDataLocalPackagesMicrosoft.WindowsStore_8wekyb3d8bbweACINetCache
```

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.

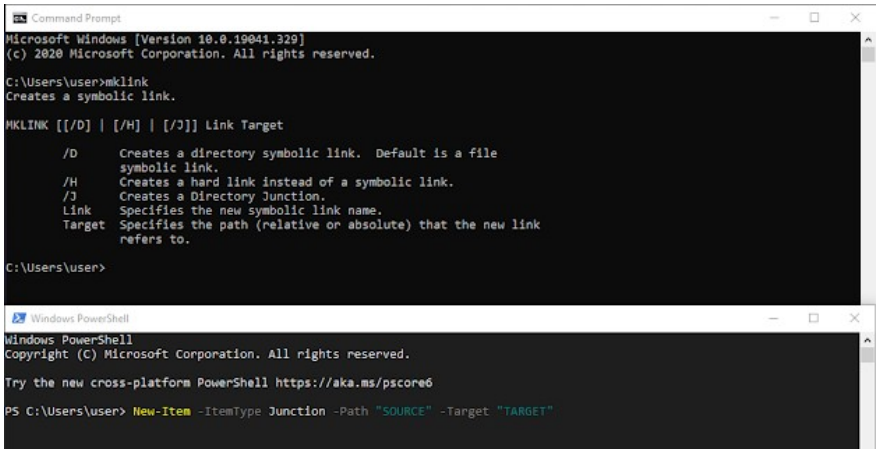
Hackers start the setup by deleting the **INetCookies** folder , which Wsreset always prioritizes deleting at launch. To delete this directory, hackers do not need Administrator rights, just find a way to control the user's account or use malicious code.



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.

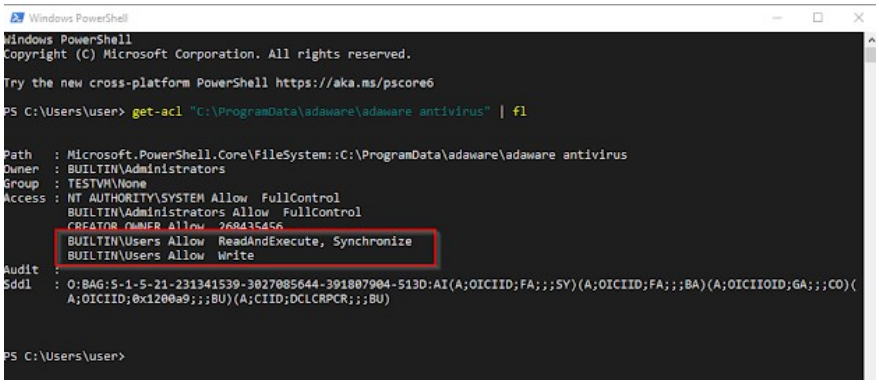
"Hackers can do this by using mklink.exe with the" / J "parameter or via the new-item powershell command with the" -ItemType. "" , Gelbert explained.



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

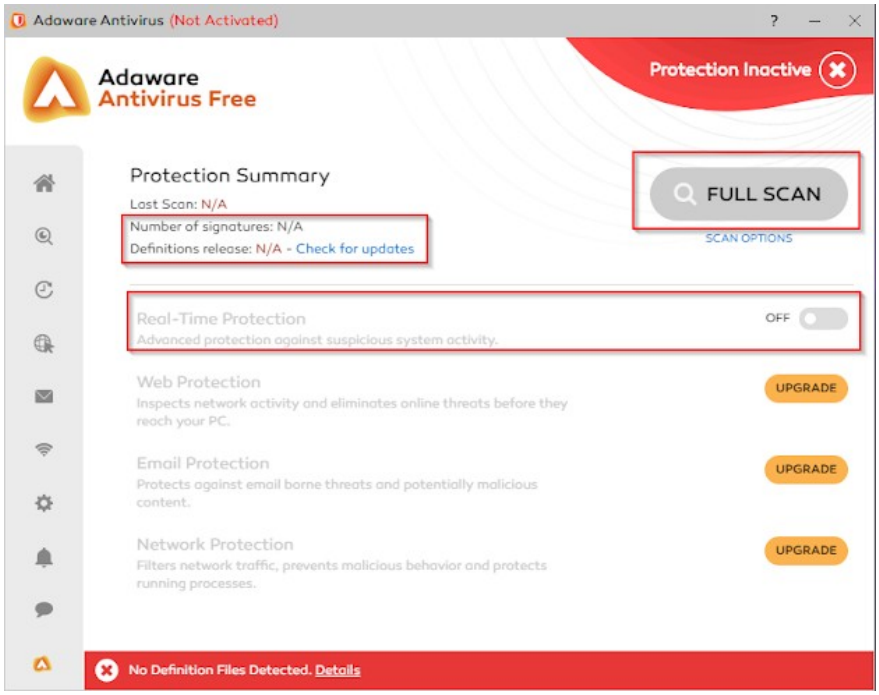
Researchers have demonstrated that by taking advantage of Wsreset, hackers can disable anti-virus software on the victim's computer. For example, here's how to disable Adaware software:

"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.



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.