Winos 4.0 Malware Warning: Protect Your Computer From Fake NSIS Installers!

Stealthy Winos 4.0 malware variant is using a rogue NSIS installer to launch multi-stage attacks.

The stealthy Winos 4.0 malware variant is using a rogue NSIS installer to launch multi-stage attacks. It can even tweak Windows Defender-based security to create an exception, giving it room to operate. The end result is data theft, registry tampering, and PC surveillance. Check out these proven solutions to stop this persistent malware from getting started!

Why is Winos 4.0 malware dangerous?

Winos 4.0 is a sophisticated malware family, originally derived from the Gh0st RAT. "4.0" is just a name, not any specific version of the malware . It has been around for over a year. On May 22, 2025, Rapid 7 announced a Winos 4.0 variant that uses VPN and browser installers to inject the malware.

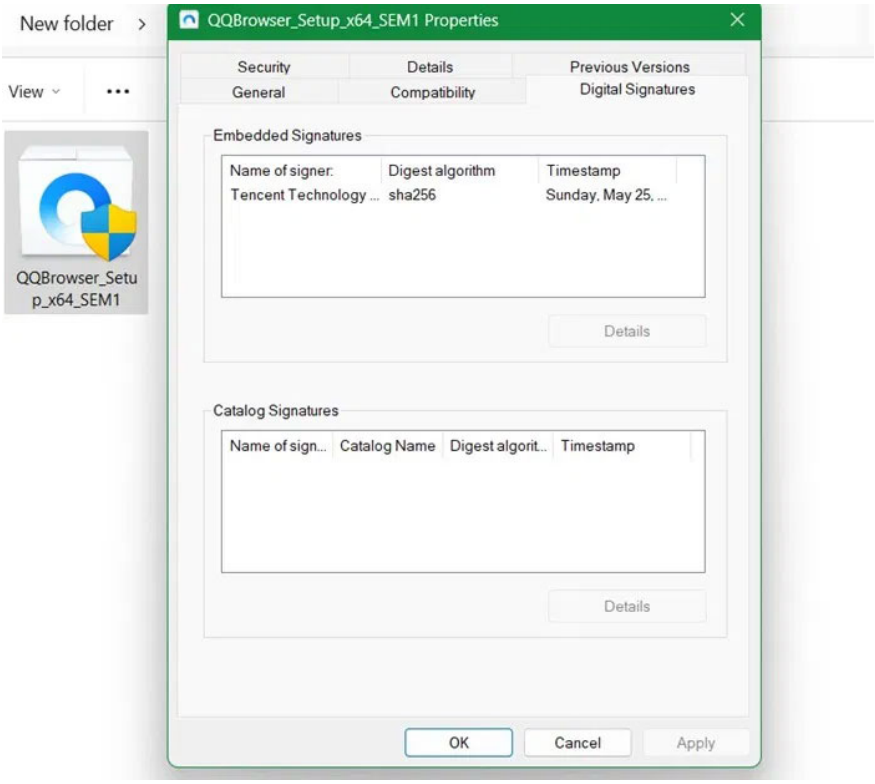
The malware is distributed in a chain reaction, starting with a fake NSIS application, which is a corrupted EXE file. The installer name is unsuspecting, such as **QQBrowser_Setup_x64.exe** or **Lets.15.0.exe.** What makes this malware dangerous is the professional deception tactics that many users will not suspect.

While you install the desired application, it drops additional files such as a VBScript launcher, a PowerShell loader, malicious DLLs, and configuration files. Rapid7 has named the multi-stage payload – Catena loader. For persistence, the silent PowerShell command adds exclusions to protect the payload. Notably, the Winos 4.0 malware can lie dormant for weeks before taking action.

Finally, the Winos 4.0 malware will record passwords and cryptocurrency details, make registry changes, and monitor screenshots, webcams, and microphones. Operating only in memory, as we saw with the Remcos RAT, it leaves no traces on disk, avoiding detection by antivirus software.

Verify digital signatures of all installers

Checking the digital signature of any application you plan to install will help keep your PC safe. To do this, right-click the application, go to **Properties** -> **Digital Signatures** . Click **Details** -> **View Certificate** to check the authenticity of the installer.



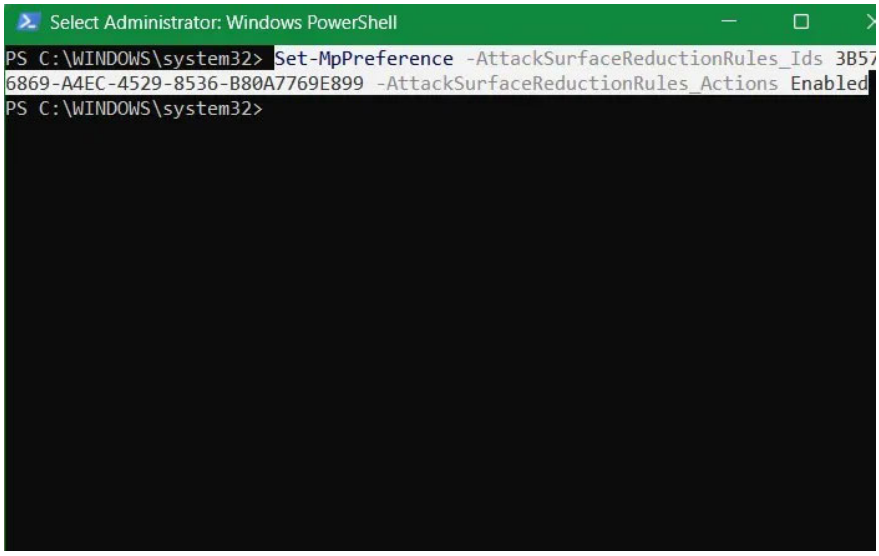
Here, we are checking the digital signature of QQBrowser, which has malware variants with fake NSIS installers. However, this signature has the real valid signature of Tencent Technology., the company behind QQBrowser.

Turn on Windows Security application protection

Although the Winos 4.0 malware fools Windows Defender, there are certain security steps you can take inside the Windows Security app.

You can prevent the NSIS installer from executing. To do this, open PowerShell with admin rights and run the following command to reduce the Attack Surface Area (ASR). This is a great command that does not impose a blanket ban, but only removes malicious installers.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids 3B576869-A4EC-4529-8536-B80A77
```



Next, open the Windows Security app. Go to **Virus & Threat Protection** -> **Virus & Threat Protection Settings** -> **Manage Settings** . Check to make sure **Real-time Protection** is turned on.

Also, under Virus & Threat Protection, scroll down to select **Manage Ransomware Protection** . If **Controlled Folder access** is turned off, turn it back on. You can also click **Allow an App Through Controlled Folder Access** to whitelist trusted apps.

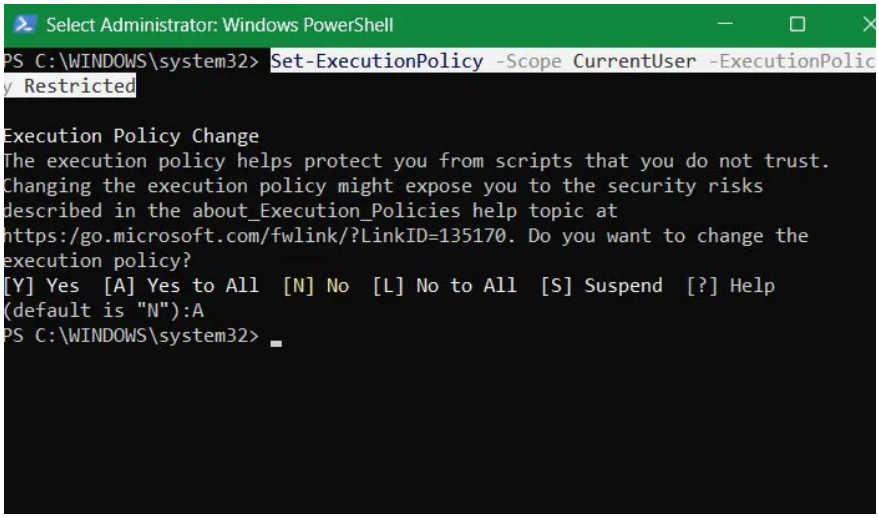
Implementing these minimal Windows Security safeguards is sufficient. Advanced Windows users can also configure their firewalls to disallow Winos 4.0 malware.

Prevent Winos 4.0 malware from adding exclusions to Windows Defender

One sneaky way the Winos 4.0 malware spreads in your system is by adding exclusions to Windows Defender scans. You can block it in advance.

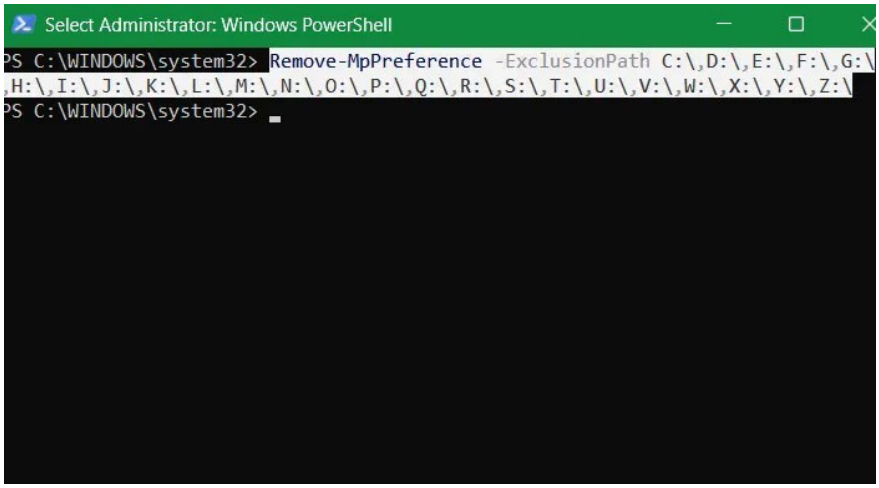
Open PowerShell with admin rights. Use the following command to add an execution policy for bad scripts. Click **A** to confirm.

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted
```



You can also prevent any unauthorized exclusions from running in PowerShell . Do so with the following command, including all drive letters.

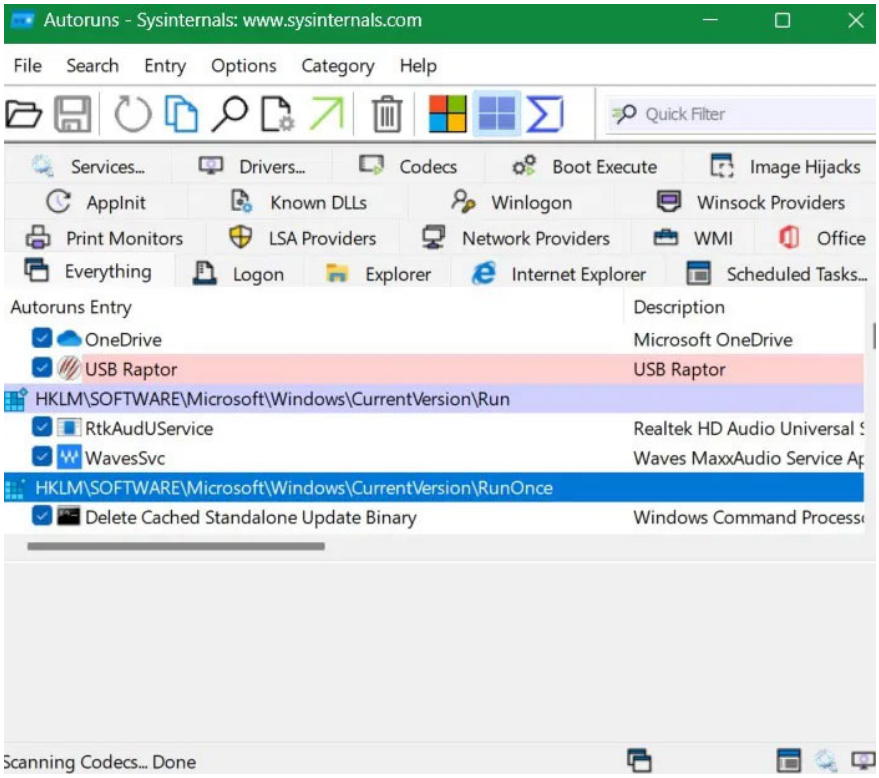
```
Remove-MpPreference -ExclusionPath C:,D:,E:,F:,G:,H:,I:,J:,K:,L:,M:,N:,O:,P:,Q:,
```



Using Autoruns to Detect Fake NSIS Entries

Microsoft's Autoruns program can be used to monitor for bad startup programs, including fake NSIS entries. This is one of the easiest ways to detect Winos 4.0 malware and its variants before they can execute their payloads.

Download the Autoruns ZIP file from the Sysinternals website . No installation required. Just unzip the file and double-click the Autoruns64 file (for Windows 64 systems). Here you will get a complete view of all active logons, scheduled tasks, and processes. You may notice entries marked in red. Pay attention to any NSIS-related entries, they will be properly marked.



We rarely question legitimate Windows app installers. Once they pass SmartScreen (which you shouldn't disable) and Windows Security checks, we generally assume the app is safe, whether it's a VPN or a browser. That's where the Winos 4.0 malware author found easy access.

That is why the article recommends that you verify the reliability of the installer using the methods above. Protecting your PowerShell window from script execution ensures absolute safety. You can use VirusTotal and other websites to scan the installation packages for malware.

You finished reading the article "**Winos 4.0 Malware Warning: Protect Your Computer From Fake NSIS Installers!**" 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.
