What is Adrozek Virus? How to protect yourself from Adrozek virus

Technically, Adrozek is not a virus. It's a browser hijacker, also known as browser modifier. That means that the malware was installed on your computer without your knowledge.

See some ads that look a little different when you search online? Maybe your computer is running a bit slow, or the browser seems to be taking you to places you didn't think you asked for. Be careful! You may be experiencing the effects of Adrozek, a nasty program that Microsoft says has been quietly attacking users around the world since May 2020.

What is Adrozek Virus?

Technically, Adrozek is not a virus. It's a browser hijacker, also known as browser modifier. That means the malware has been installed on your computer without your knowledge.

Adrozek's goal is to take over browser activities that push you to illegal "advertisers", help them profit through affiliate marketing or steal personal information in other ways. other.

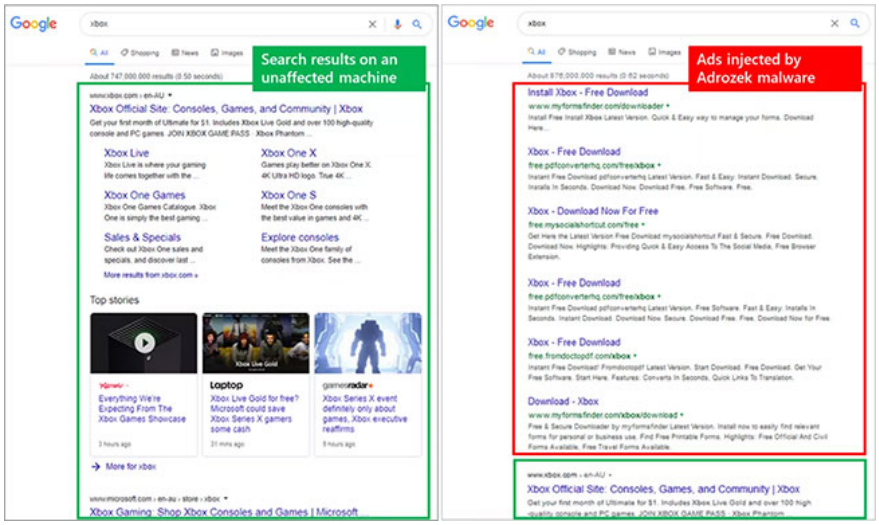
If Adrozek has infected your computer, you will see search results that don't really match current search engine results or see unwanted ads on legitimate websites that can't be blocked by door blockers. pop-up window. Finally, Adrozek can even redirect you to sites you never asked for.

The ads seem harmless, but the 'advertiser' is simply a cover for hackers to gain access to important information about you, including financial information.

How does Adrozek work?

This malware works by changing settings in your browser to make you find the search results are essentially fake. The threat was spread evenly across popular browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox and Yandex Browser. Other browsers can be hacked at any time.

Adrozek modifies browser DLL libraries to insert unauthorized ads into what you think are typical search results. These ads show alongside perfectly legitimate ones, which makes it even more difficult to determine what is safe to click. The attackers then make money through affiliate advertising programs, which pay according to the number of traffic that goes to sponsored affiliate sites, Microsoft says.



Adrozek's general approach is nothing new, but anti-virus software makers and companies like Microsoft are warning that the attack campaign appears to be a more complex version than usual. Adrozek's access to multiple browsers and the stealing of website credentials prompted Microsoft to issue a security warning in December 2020.

Microsoft is warning that password theft appears to be part of the attack, meaning the program can track and steal your passwords on financial and other sensitive websites.

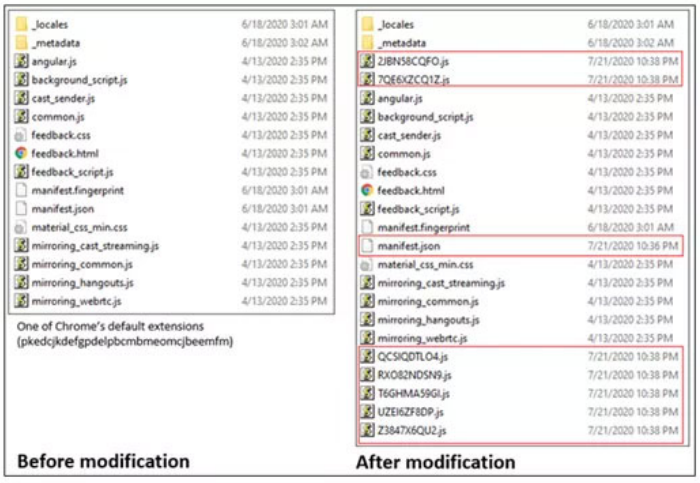
How do I know if the Adrozek browser hijacker is on my computer?

If Adrozek has hacked your system, three things will happen:

- The extension path in your browser will be changed.

You will notice that search results suddenly look different from what the search provider normally offers you. They won't look very different, but resemble the old fashioned results instead of the results given by today's search engines.

You will see a new randomly named .exe file in the **% temp%** folder under **Program Files** . The filename will be different depending on the case, but it can be **Audiolava.exe, QuickAudio.exe** and **converter.exe** . Microsoft confirms that the malware installed like a regular program can be accessed through **Settings> Apps & features** and registered as a service with the same name.



As Adrozek expands, you may also notice a large influx of video ads, pop-up ads, banners, and other sales related stuff that are bothersome, and sudden as you browse the web. Ad blocker does not appear to work anymore.

You can also experience significant slowdowns while surfing the web and even experience multiple browser issues, if too many ads or browser windows open at the same time.

The antivirus can also display a pop-up message saying **'Threat was blocked'** . If that happens, you can see the phrase **'Adrozek'** in the warning.

It is important that you remove this threat as soon as it is found, so that it does not continue to steal personal information as you browse the Internet.

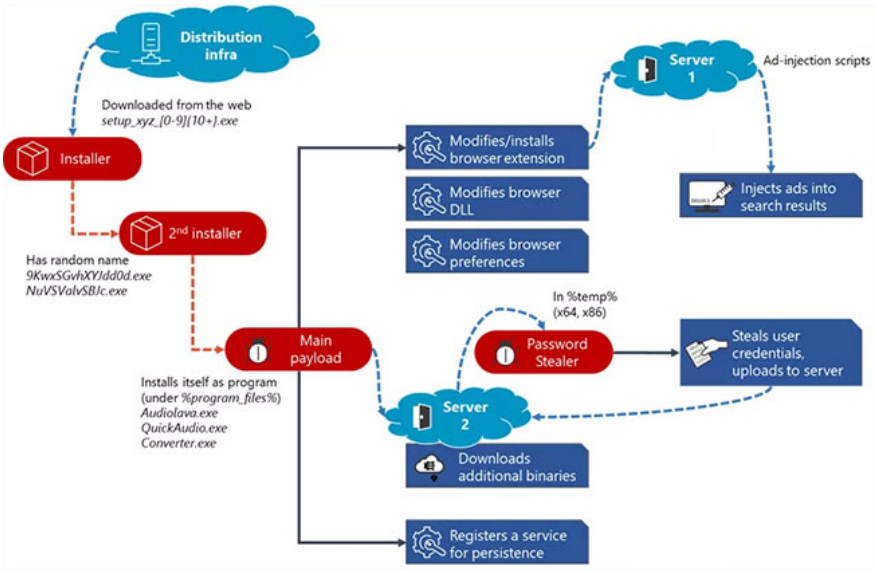
Example of modifying the Google Chrome browser extension path

```
% LocalAppData% GoogleChromeUser DataDefaultExtensionspkedcjkdefgpdelpbcmbmeomcjl
```

How did you get infected with this malware?

Adrozek reaches your system through what's called 'drive-by download'. The malware is bundled with free or pirated programs that you are ready to download somewhere without knowing how dangerous it is.

During the installation of that download, Adrozek quietly enters your computer in the form of a tiny, seemingly harmless piece of software. Then of course, it will work from there to modify the browser and perform malicious behavior. This illustration shows how the general process plays out.



How to get rid of Adrozek?

The most effective way to remove any malware on your computer, including Adrozek, is to use a powerful, professional anti-virus software program that can solve a variety of problems. This may take several hours to do, but these programs provide the most comprehensive ways to remove malicious files.

On Windows 10 computers, Microsoft Defender is built in. Microsoft says they have blocked Adrozek, however, if you have other antivirus software installed or disabled Windows Defender you will need to manually check the Defender console to see what is happening on your computer. and whether you need to take more action.

Other options include:

- You can manually remove suspicious add-ons and extensions from the browser. The process is a little different for disabling extensions in Chrome and managing them in Edge. In Chrome you also have the option to use Chrome Cleaning Tool.

- You can also try removing adware and spyware on your device. In some cases, you can get a persistent malware infection that causes the virus to keep coming back again and again. To deal with that, you can try removing the virus without using an antivirus application, but in most cases both antivirus and anti-malware program will be needed to remove give up this infection.

- You can also use System Restore to go back to the time before being infected with Adrozek on the computer. This is a fairly intensive process; make sure to choose a period where you know for sure that you have not been infected with a virus on your computer.

If the problem is happening on a mobile device, you may need to try different techniques to get rid of the virus from Android or iOS.

How can I avoid getting infected with Adrozek?

There are several main ways to reduce your risk of getting infected with Adrozek (or any other malicious program).

Be extra careful when you download new programs. Always confirm the legitimacy of the program source and the application you download. Trusted sites have lots of small software add-ons you don't need, and that's where malware like Adrozek can lurk.

- Keep anti-virus software and anti-malware protection up to date. New virus definitions are released so often that anti-virus software manufacturers update their software regularly to combat these threats. These updates keep your PC informed of new virus and malware-based threats.

- Block PUP. In the antivirus software, turn on the option to detect PUP programs. (Sometimes it's disabled by default). This will help you spot software that is trying to sneak in its cover when you download other legitimate programs.

Stick with popular websites and stop clicking unknown links. Adrozek and other malware can infect your computer through suspicious websites that you may accidentally visit. Therefore, clicking the wrong link could lead to the download of a program you never wanted. Never download software from a torrent site!

- Don't click on the banner ad. When a pop-up banner appears when you browse a website, resist the urge to click it. If a website floods you with pop-up ads, leave the site immediately and run your antivirus software to confirm that nothing nefarious has entered your system.