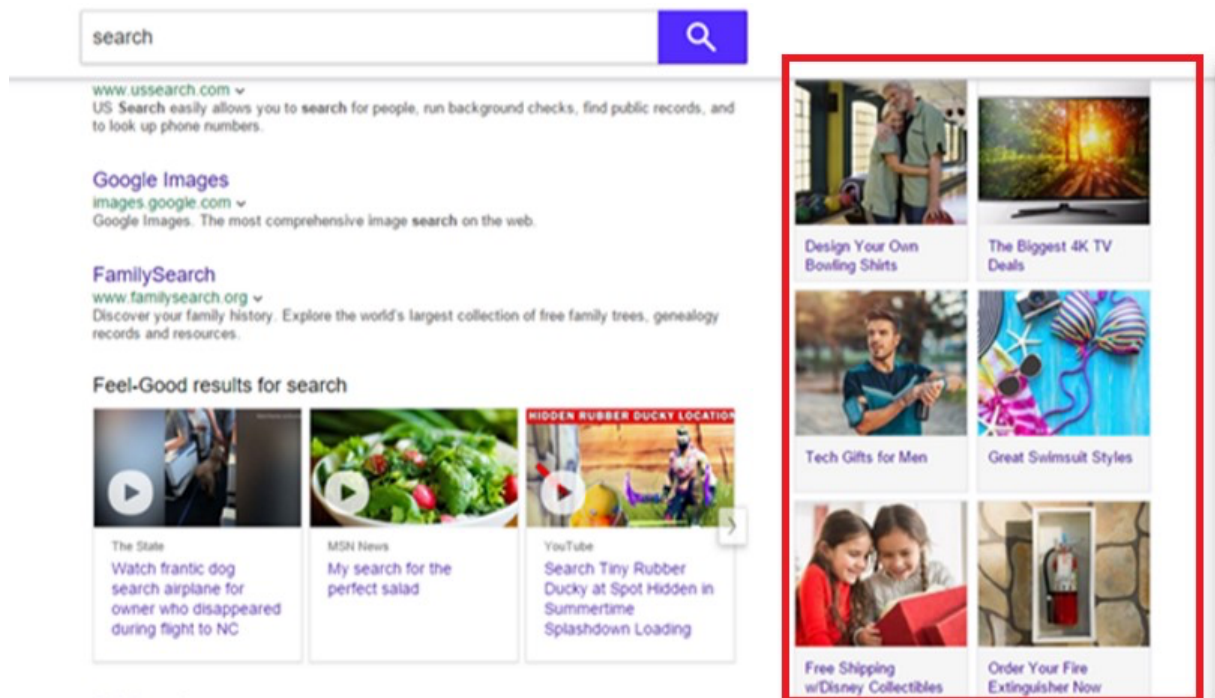




## **1.3 million users encountered browser extension threats in the first half of 2022**

Kaspersky researchers have analyzed what risks innocent-looking browser extensions pose to users and the activities of cybercriminals hiding threats under add-ons. In the first half of 2022, more than 1.3 million users were affected by threats, hiding in browser extensions, at least once, which is over 70% of the number of users affected by the same threat throughout the whole of 2021 – with still another half of the year to go. Mimicking popular apps, such as Google Translator or extensions with useful functionality like PDF Converter or Video Downloader, threats in browser extensions can insert advertisements, collect data about users' browsing histories and even search for login credentials, making it one of the most desirable tools for cybercrim

Since the beginning of 2020, Kaspersky products have prevented approximately 6 million users from downloading threats disguised as browser extensions. During the first half of 2022, Kaspersky researchers observed a rise in the number of affected users – with 1.3 million users encountering threats in add-ons over this period, more than 70% of the number of users affected by the same threat throughout the entire previous year. The most prominent threat spread under the guise of browser extensions has been adware – unwanted software designed to throw advertisements up on the screen. Such advertisements are usually based on the browsing history to catch users' interest, embed banners in web pages or to redirect them to affiliate pages that the developers can earn money from, instead of legitimate search engine ads. From January 2020 to June 2022, Kaspersky experts observed more than 4.3 million unique users faced adware hiding in browser extensions, which means approximately 70% of all affected users have encountered this threat.



*Adware can track everything the user searches for and then promote these products with affiliate ads on search engine*

Malicious and unwanted add-ons have also been found to be distributed through official marketplaces. In 2020, Google removed 106 malicious browser extensions from its Chrome Web Store. All of them were being used to siphon sensitive user data, such as cookies and passwords, and even take screenshots. In total, these malicious extensions were downloaded 32 million times, putting the data of millions of users at risk.

However, this does not happen often, the main way malicious add-ons are distributed is through third-party resources. One of the threat families analyzed by Kaspersky researchers in the report, dubbed FB Stealer, was spread solely through untrustworthy sites. FB Stealer is one of the most dangerous threat families because, in addition to the traditional search engine replacement and affiliate pages redirection, FB Stealer is able to steal user credentials from Facebook.

When users tried to download a cracked software installer from third-party resources, such as SolarWinds Broadband Engineers Keymaker, they actually received a dangerous NullMixer Trojan. Then NullMixer self-installed FB Stealer on the device, which looked less suspicious to the user because it mimicked the harmless and standard-looking Chrome extension "Google Translate."



solarwinds broadband engineers keymaker



[All](#) [Images](#) [News](#) [Videos](#) [Maps](#) [More](#)

About 815,000 results (0.58 seconds)

<https://cracksgurus.com> › solarwinds+engineers+toolset

[Download solarwinds engineers toolset serial number, crack ...](#)

86 records — **SolarWinds Broadband Engineers Edition Toolset v8.2 keymaker** by ZWT · **SolarWinds Broadband Engineers Edition Toolset v8.2 keygen** by Z.W.T.

<https://cracksgurus.com> › crack › SolarWinds-Broadband-...

[Download SolarWinds Broadband Engineers Edition Toolset v8.1 ...](#)

**SolarWinds.Broadband.Engineers.keymaker.zip** (180820 bytes) · FILE\_ID.DIZ · ZWT.nfo ...

<https://www.solarwinds.com> › engineers-toolset

[Network Engineer Software Tools for Remote ... - SolarWinds](#)

Over 60 great tools to help network **engineers** troubleshoot issues before users are ...  
**Engineer's Toolset** Network software with over 60 must-have tools. **Key** ...

<https://keygensumo.com> › solarwinds+engineers+toolset...

[Solarwinds engineers toolset v9 keygen,serial,crack](#)

*NullMixer Trojan is spread through different hacked software installers, for example, SolarWinds broadband engineers keymaker*

After launching FB Stealer, NullMixer Trojan could extract Facebook session cookies - secrets stored in the browser holding identification data which allows users to stay logged in - and send them to the attackers' servers. Using these cookies, they are able to quickly log into the victim's Facebook account. Once in the account, attackers ask the victim's friends for money, trying to take as much as possible before the user regains access to the account. In the end, after downloading a hacked installer from an unknown resource, users receive a threat they did not expect and many of their friends lose their money.

*“Even browser extensions that do not carry a malicious payload can be dangerous. For example, when the developers of these add-ons sell gathered user data to other companies, potentially exposing their data to someone who was not supposed to see it. Users may wonder whether it is worth downloading browser extensions at all when they can carry so many threats. I am an active user of*

*browser extensions myself and believe that add-ons improve the online experience. Some extensions can even make devices a lot safer, for example, password managers. It is much more important to keep an eye on how reputable and trustworthy the developer is and what permissions the extension asks for. If you follow the recommendations for safe use of browser extensions, the risks of encountering any threats will be minimal,”* comments Anton V. Ivanov, senior security researcher.

To learn more about the danger the innocent-looking browser extensions hold for users, read the full report on Securelist.

**To protect yourself from threats, hiding in browser extensions, Kaspersky recommends the following:**

- Only use trusted sources to download software. Malware and unwanted applications are often distributed through third-party resources where no one will check their security in the same way as official web stores do. These applications may install malicious or unwanted browser extensions without the user knowing about it and can perform other malicious activities.
- Extensions add extra functionality to browsers and require access to various resources and permissions — carefully examine add-on requests before agreeing to them.
- Limit the number of extensions you’re using at one time and periodically review your installed extensions. Uninstall extensions that you no longer use or that you do not recognize.
- Use a robust security solution. Private browsing, like in [Kaspersky Internet Security](#), can help you avoid internet tracking and protect you from threats.