

Fake GoogleTranslate Chrome Extension Lets Attackers Remotely Control Your Browsers

CSN cybersecuritynews.com/fake-googletranslate-chrome-extension

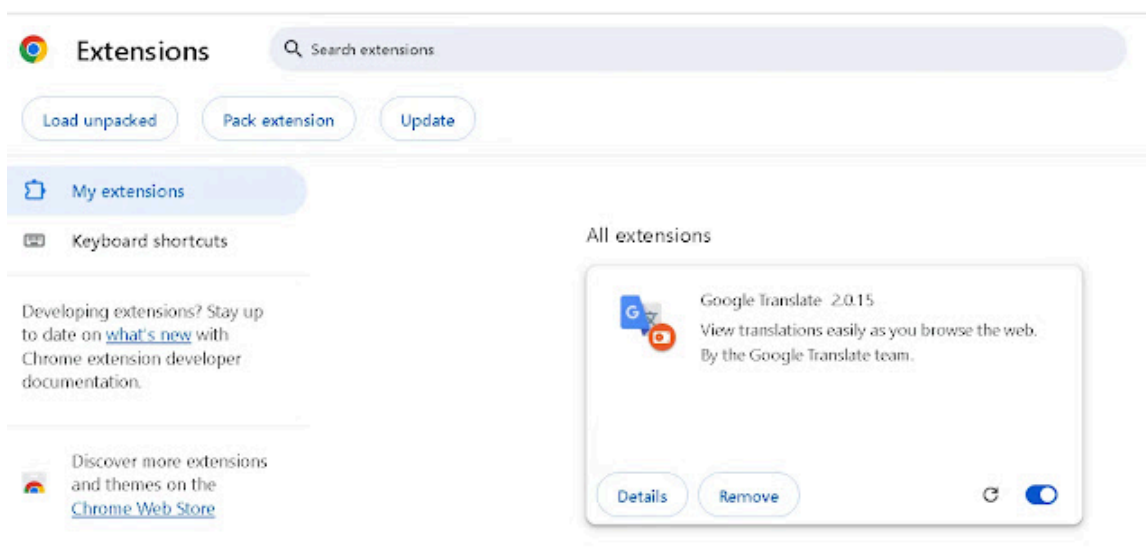
Guru Baran

August 10, 2026

[Chrome Extension fake malware](#)

A malicious Chrome extension masquerading as GoogleTranslate that can steal sensitive browser data, live-stream web sessions, and allow threat actors to remotely interact with Chrome windows while keeping their activity out of the victim's view.

The operation begins with a suspected Rust-based malware loader. VMRay researchers found that the binary drops a malicious Chrome extension alongside an AutoIt script, which subsequently deploys the Stealcv2 information-stealing malware.



GoogleTranslate Chrome Extension

The multi-stage infection chain gives attackers both traditional endpoint-stealing capabilities and unusually deep control over the victim's browser environment.

Once installed, the fraudulent extension can collect a broad range of browser-resident data. This includes browsing history, saved bookmarks, installed extension details, cookies, and stored credentials.

Such information can help attackers hijack online accounts, bypass session-based protections, profile victims, and identify high-value services such as email, cryptocurrency platforms, cloud consoles, and corporate applications.

```

{
  "manifest_version": 3,
  "name": "Google Translate",
  "key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuTZORmDxindggHjBm1J+NzakbAv5d/2mNRQrdaIRLBvFHValg1C
ydbDPzsXStVF13SErKZr5ffVn7V2GbNxnWOU+OBZOW/yvpcGrOGrM4S00qPpaP0dyrrvMc3yEqm9Dun7JNYIjftT9KeR70qCF
81f00hVgtbDgwRGGgpa74FMYLVtSpKq3QIDAQAB",
  "version": "2.0.15",
  "description": "View translations easily as you browse the web. By the Google Translate team.",
  "...",
  "permissions": [
    "cookies",
    "history",
    "storage",
    "alarms",
    "tabs",
    "management",
    "bookmarks",
    "scripting",
    "notifications",
    "proxy"
  ],
  "host_permissions": [
    "<all_urls>"
  ],
  "background": {
    "service_worker": "service-worker-loader.js",
    "type": "module"
  },
  ...
}

```

GoogleTranslate Chrome Extension

The most concerning capability is its ability to provide attackers with a real-time view of Chrome windows and let them operate websites remotely using mouse clicks and keyboard input.

In effect, the browser becomes a remotely controlled interface for the threat actor. Chrome's extension APIs can legitimately interact with tabs and, when granted relevant permissions, may access sensitive tab properties or inject scripts into matching websites—permissions that can be abused when users [install an untrusted extension](#).

Unlike conventional remote-access malware, this campaign is designed to conceal interactive fraud. The extension reportedly enables remote control of browser windows that are out of focus, meaning attackers can perform actions in the background while the victim works in another application or window. This reduces the chance that a user will notice unauthorized clicks, navigation, or form submissions occurring in Chrome.

Researchers also observed features for setting a proxy and injecting attacker-controlled JavaScript into selected websites. Proxy configuration could help route browser traffic through infrastructure controlled by the attackers, while JavaScript injection can alter the content users see or manipulate sessions on targeted domains. This creates opportunities for account takeover, payment fraud, data theft, and targeted social engineering.

Another major risk is a [man-in-the-browser phishing](#) technique. The extension can overlay a legitimate website with an iframe that loads content from an attacker-controlled phishing page.

The browser's address bar may still show the genuine domain, potentially convincing victims that they are interacting with a trusted login portal. Users could then submit passwords, multi-factor authentication codes, or payment details directly to criminals without realizing that the visible form is fraudulent.

The malware's Google Translate branding is especially dangerous because translation extensions are common, useful, and rarely viewed as high-risk by users.

Threat actors have repeatedly abused trusted-looking browser add-ons to gain access to credentials, cookies, screenshots, and web sessions; a previous campaign linked to the Kimsuky threat actor used a Chrome extension hosted as "GoogleTranslate.crx" to collect account data and browser information.

Users should review installed Chrome extensions immediately, remove unfamiliar or unnecessary add-ons, and scrutinize permission requests—particularly broad access to website data.

Organizations should restrict unmanaged extensions, monitor for suspicious browser-policy changes, and require phishing-resistant multi-factor authentication to limit damage from stolen passwords and session data.

IoCs

IoC Type	IoC Details	Associated Component
Command-and-Control Server	http[:]//87.120.104[.]147:8080	Suspected attacker-controlled infrastructure
Command-and-Control Server	http[:]//160.20.109[.]33:80	Suspected attacker-controlled infrastructure
SHA-256 Hash	7ba2c663d76d2d353a02d815381f22a1b04b2032162b1559455d1f456432340a	Rust-based initial binary/loader
SHA-256 Hash	02e9da11f035bd4e18338ddd78e2818da49e7d1c8f614e9b329afaf581c33301	Fake GoogleTranslate Chrome extension
SHA-256 Hash	4f82542f68d2e677fb64ba986c8d5f3a04017a1bf7a11d375e52f950e32eb262	Autolt script
SHA-256 Hash	45c7d791fab4128fb495f359ed641e217883f132bb8f13c1e181caf5f5279a34	Stealc v2 information stealer

Strengthen Your SOC by Accelerating Threat Detection & Rapid Investigations. -> [Integrate ANY.RUN With Your SOC Now.](#)



[Guru Baranhttps://cybersecuritynews.com](https://cybersecuritynews.com)

Gurubaran KS is a cybersecurity analyst, and Journalist with a strong focus on emerging threats and digital defense strategies. He is the Co-Founder and Editor-in-Chief of Cyber Security News, where he leads editorial coverage on global cybersecurity developments.