Browser Extensions Report

Task 07
Soumil Gupta

Types of Malicious Extensions and Their Behaviours

First, the usual suspects, the kinds of malicious extensions you might stumble upon. Here's a table summarizing the main types and what they do, with examples from the report:

Type	What They Do	Examples
Adware Extensions	Inject ads, redirect to sponsored sites	Adrozek, Superfish
Browser Hijackers	Change homepage, search engine, or new tab page	Babylon Toolbar, Best Searcher
Data Harvesting Extensions	Steal passwords, browsing data, or social media info	Fake Bitwarden Extension, Shapeshifting Extension
Cryptocurrency Mining	Use your computer to mine crypto, slowing it down	Generic names like "Optimizer"
Fake Security Extensions	Pose as security tools but install malware	Adware Doctor, LizaMoon

Let's dive into each:

- **Adware Extensions**: Imagine you're browsing the web, and suddenly, pop-ups and banners start appearing out of nowhere, or your search results take you to weird sites you didn't ask for. That's what adware extensions do, they turn your peaceful browsing into an ad-filled nightmare. Examples like "Web Companion" can inject ads and change search results, while "Shopping Assistant" variants might promise coupons but redirect you to affiliate links.
- **Browser Hijackers**: Ever opened your browser and found that your homepage has changed to something you don't recognize, or your

search engine is now some shady site? That’s a browser hijacker at work, taking control of your browser settings without asking. "Search Manager" is a classic example, switching your search to ad-heavy domains, and "Quick Search" sends your queries through monetized portals.

- **Data-Stealing Extensions**: These are the creepy ones. They’re all about grabbing your personal info, like passwords, what you browse, or even your social media logins. They might pretend to be helpful, like fake "Password Managers" or "Form Fillers," but they’re really snooping on your keystrokes, taking screenshots, or stealing cookies to hijack your accounts.
- **Cryptocurrency Mining Extensions**: These secretly use your computer’s power to mine cryptocurrency, making money for the bad guys while your device suffers. You might notice your computer slowing down, your fan running non-stop, or your electricity bill spiking. It’s like they’re running a marathon on your hardware without permission.
- **Fake Security Extensions**: These are the wolves in sheep’s clothing. They pose as antivirus tools but actually put you at risk, showing fake alerts to scare you or even installing malware while claiming to protect you. Names like "Security Scanner" or "Malware Detector" might sound safe, but they’re anything but “safe”.

Real-Life Horror Stories

Let’s look at some real examples to see how serious this can get:

- **The "Great Suspender" Fiasco**: This was a popular extension for managing browser tabs, used by over 2 million people. But in 2021, it got sold to shady folks who added tracking code and malware. It’s a wake-up call—even extensions you trust can turn bad.
- **Facebook Account Heists**: Some extensions pretending to boost your Facebook experience were actually stealing logins and personal info from millions of users. It’s a betrayal, right? You think you’re enhancing your social media, but they’re stealing your data.
- **Fake AdBlock Scams**: Fake ad blockers have tricked users into installing extensions that, instead of blocking ads, pile on more of

them. It's like hiring a guard who lets thieves in instead of keeping them out.

How They Pull It Off

So, how do these extensions get away with it:

- They ask for way more access than they need, like reading or changing data on every website you visit, snooping through your browsing history, or talking to sketchy servers behind your back. It's like giving a stranger the keys to your house.
- They use names that sound like trusted tools, fake glowing reviews, or urgent messages like "Install now to stay safe!" They might promise free versions of paid software or claim they'll fix your computer's problems, making you click without thinking.
- They sneak into official stores like the Chrome Web Store with misleading descriptions, pop up in spam emails or social media ads, or hitch a ride with free software downloads. They even use SEO tricks to rank high in search results or spread through hacked websites.

Staying Safe: Your Game Plan

Now, let's talk about how to protect yourself. It's not rocket science, but it does take a bit of caution. Here's what to do:

- **Before You Install**:
    - Check out the developer's website and credentials. Read reviews, but watch for fake ones look for patterns in complaints. Google the extension's name with "malware" or "scam" to see what pops up, and check security blogs for red flags.
    - Look closely at what the extension wants access to. Ask yourself: Why does a simple tool need to control everything? Skip extensions asking for too much power, like "read and change all data on any page"

    - Only download from official stores like Chrome Web Store or Firefox Add-ons. Make sure the developer's website looks legit and has proper documentation or support contacts.

- **During Installation**:
    - Take it slow. Read every permission request carefully, don't rush through the install process, and avoid installing a bunch of extensions at once.
- **After Installation**:
    - Keep an eye out. Do a monthly check of your extensions, watch for slowdowns or weird browser behaviour, and check for odd network activity. Revisit permissions to make sure nothing's changed, and delete extensions you don't use anymore.
    - **Warning Signs**: Look out for ads popping up where they shouldn't, your homepage or search engine changing on its own, your browser acting slow, new toolbars or buttons you didn't add, search results taking you to weird sites, random pop-ups, or high CPU usage.

Tools to Help You Stay Safe

- Turn on Chrome's "Enhanced Safe Browsing," use Firefox's "Strict" tracking protection, keep your browser updated for the latest security patches, and use your browser's malware scanning features.
- Get a trusted antivirus with browser protection, use anti-malware software that checks extensions, consider security extensions from reputable developers, and set up tools to monitor your network for weird traffic.
- Use the Task Manager to spot high CPU usage, watch for strange network connections, check your browser settings for unexpected changes, and look at your extension list for anything unfamiliar.

What to Do If You Suspect Trouble

1. Go offline to stop any data leaks.
2. Open your browser in safe mode or incognito to limit what the extension can do.

3. Head to the extension management page, write down all installed extensions, and delete anything that looks suspicious.
4. Clear your browser's cache and cookies, run a full antivirus scan, and change passwords from a clean device.
5. Get back on track by resetting your browser to default settings, only reinstalling extensions you trust, keeping an eye on your accounts for weird activity, turning on two-factor authentication wherever you can, and reporting bad extensions to your browser's store.

I had done an assessment of the extensions on my browser, and here is a report on the same, as I did not find any harmful ones:

Extension Security Assessment Results

CLEAN - All Extensions Appear Legitimate

Analysis by Category:

Productivity & Utility (Safe):

- Dark Reader - Very popular dark mode extension
- Video Speed Controller - Common video playback tool
- StayFocusd - Established productivity/focus extension

Security & Privacy (Safe):

- Bitwarden - Reputable password manager
- uBlock Origin - Highly trusted ad/tracker blocker
- FoxyProxy - Legitimate proxy management tool

Google Official (Safe):

- Google Docs Offline - Official Google extension
- Google Translate - Official Google extension

Professional/Development (Safe):

- Wappalyzer - Legitimate web technology identifier
- Always active Window - Developer/productivity tool
- Weekday - Job search/recruiting tool