JShelter for browsing securely

[Libor Polčák <polcak@fit.vutbr.cz>]

https://www.fit.vutbr.cz/~polcak/p/p.php?p=libreplanet2023

Why JShelter?

JS is omnipresent on web

JavaScript Requests

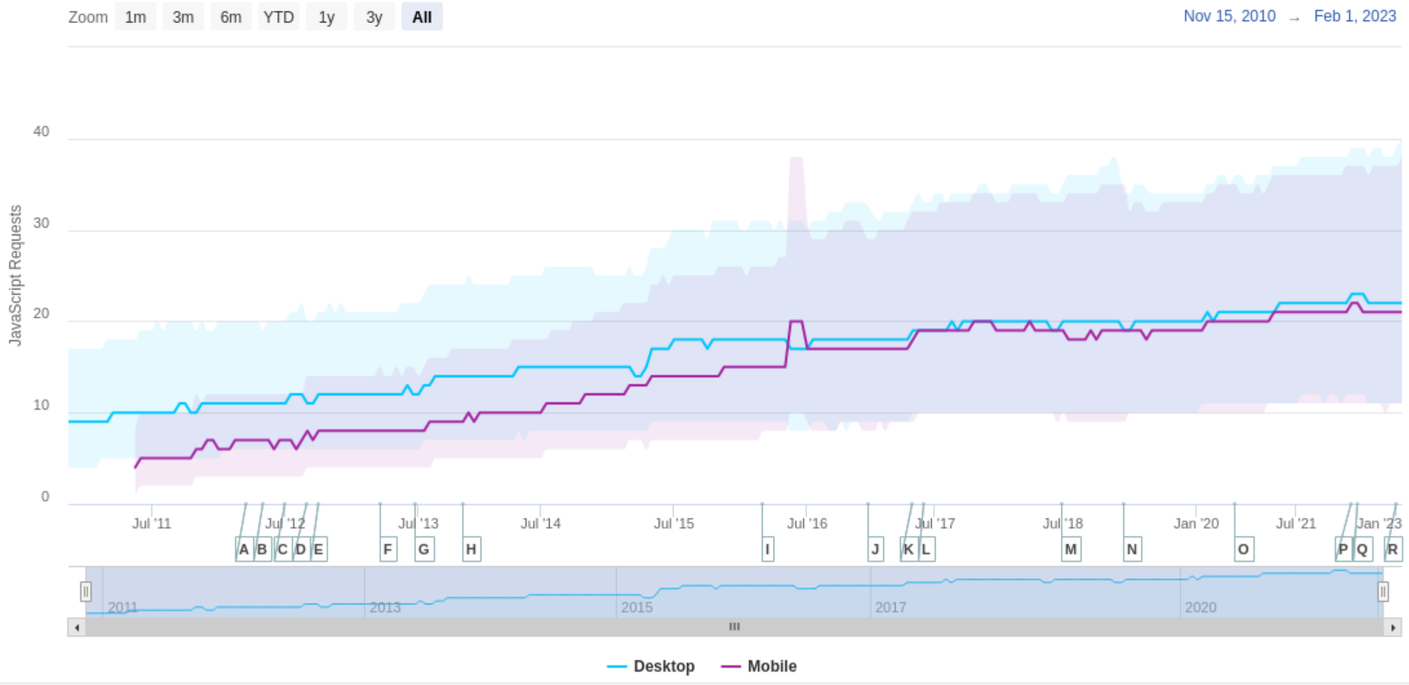
The number of external scripts requested by the page. An external script is identified as a resource with the `js` or `json` file extensions or a MIME type containing `script` or `json`.

See also: State of JavaScript

MEDIAN DESKTOP
22 Requests
▲144.4%

MEDIAN MOBILE
21 Requests
▲425.0%

Timeseries of JavaScript Requests
Source: httparchive.org



Zdroj: https://httparchive.org/reports/page-weight?start=earliest&end=latest&view=list#reqJs

The JavaScript Trap

The JavaScript Trap

by Richard Stallman

You may be running nonfree programs on your computer every day without realizing it—through your web browser.

> Webmasters: there are several ways to indicate the license of JavaScript programs in a web site.

In the free software community, the idea that any nonfree program mistreats its users is familiar. Some of us defend our freedom by rejecting all proprietary software on our computers. Many others recognize nonfreeness as a strike against the program.

Many users are aware that this issue applies to the plug-ins that browsers offer to install, since they can be free or nonfree. But browsers run other nonfree programs which they don't ask you about, or even tell you about—programs that web pages contain or link to. These programs are most often written in JavaScript, though other languages are also used.

JavaScript (officially called ECMAScript, but few use that name) was once used for minor frills in web pages, such as cute but inessential navigation and display features. It was acceptable to consider these as mere extensions of HTML markup, rather than as true software, and disregard the issue.

Some sites still use JavaScript that way, but many use it for major programs that do large jobs. For instance,

- I recommend reading the whole essay

Zdroj: https://www.gnu.org/philosophy/javascript-trap.html

The problem from the point of free software

- Browsers load program that (often) misses the four freedoms:
  - The freedom to run the program as you wish
  - The freedom to study the source code and make changes
  - The freedom to redistribute if you wish, either with or without modifications, either gratis or charging a fee for distribution, to anyone anywhere
  - The freedom to release your modified versions as free software

https://www.gnu.org/software/librejs/index.html

Malicious Free software

FingerprintJS

Lint and test passing | npm v3.4.0 | downloads 1.2M/month | jsdelivr 304M/month

DISCORD 37 ONLINE

FingerprintJS is a browser fingerprinting library that queries browser attributes and computes a hashed visitor identifier from them. Unlike cookies and local storage, a fingerprint stays the same in incognito/private mode and even when browser data is purged.

FingerprintJS is 100% open-source, but its accuracy is limited because it's only a client-side library without a backend.

Open Source library accuracy	Fingerprint Pro accuracy
FingerprintJS has limited accuracy (40% - 60%) and functionality, because it's not possible to do many things without a backend.	Fingerprint Pro is a high-scale device identity platform that has both client-side and server-side components and identifies browsers and mobile devices with a 99.5% accuracy. Fingerprint Pro is free for developers, production plans start at $200/mo.
FingerprintJS library demo: https://fingerprintjs.github.io/fingerprintjs	Fingerprint Pro demo: https://fingerprint.com/demo

Browser security: Same-origin policy (SOP)

https://libreplanet.org:443/2023/

- Origin = schema, domain name, port
- Broser employs SOP to isolate pages belonging to different origins
  - Scripts of page X cannot directly access page Y

```
var url = 'https://bank.example/account/XYZ';
```

```
var xhr = new XMLHttpRequest();
```

```
xhr.open('GET', url, true);
```

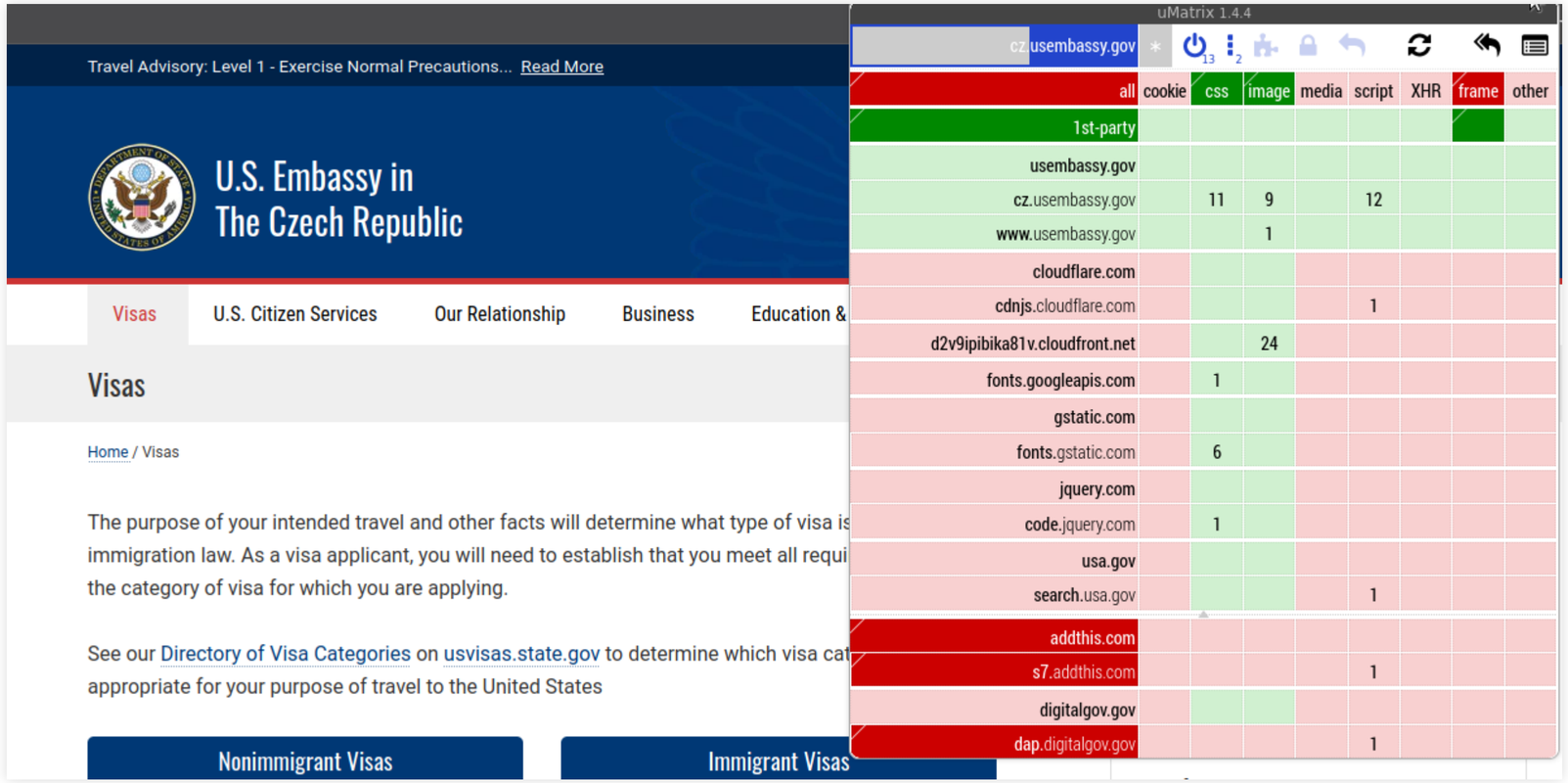
```
xhr.onreadystatechange = () => console.log("XHR ready");
```

```
xhr.send();
```

```
Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at https://bank.example/account/X
```

SOP has limitations

- Scripts share the same JS runtime



Microarchitectural attacks

- Page deduplication in JavaScript and other platforms
  - Gruss et al.: Practical Memory Deduplication Attacks in Sandboxed Javascript, European Symposium on Research in Computer Security 2015, str. 108-122.
- Rowhammer
  - Modification of neigghbor cells (rows) in RAM
  - Gruss et al.: Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript, International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment 2016, str. 300-321.
  - Gruss et al.: Another Flip in the Wall of Rowhammer Defenses, Preprint of the work accepted at the 39th IEEE Symposium on Security and Privacy 2018, https://arxiv.org/abs/1710.00551
- Spectre
  - JavaScript program can read data of the browser, or other programs
  - Kocher et al.: Spectre Attacks: Exploiting Speculative Execution, https://arxiv.org/abs/1801.01203
  - Spectre mitigation in V8

Blockers have limitations

- Some extensions cotain lists of URLs that are malicious and should be blocked

Georg Merzdovnik, Markus Huber, Damjan Buhov, Nick Nikiforakis, Sebastian Neuner, Martin Schmiedecker, and Edgar Weippl. Block me if you can: A large-scale study of tracker-blocking tools. In 2017 IEEE European Symposium on Security and Privacy (EuroS&P), pages 319–333, 2017.

- Regular expressions » a change in the URL evades the list
- Maintaining the list is not easy, some malicious resources are missing

Powerful APIs

> *Service workers essentially act as proxy servers that sit between web applications, the browser, and the network (when available). They are intended, among other things, to [...] intercept network requests and take appropriate action [...]*

Zdroj: https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API

- Beware of:
  - TLS proxies (like hotels, ad hoc networks ...)
  - Sites where multiple users create content (blogs, personal pages ...)
  - Third party scripts have way to install Service Workers so they can access more data

Powerful APIs

Sensor	Permission Policy Name
`AbsoluteOrientationSensor`	`'accelerometer'`, `'gyroscope'`, and `'magnetometer'`
`Accelerometer`	`'accelerometer'`
`AmbientLightSensor`	`'ambient-light-sensor'`
`GravitySensor`	`'accelerometer'`
`Gyroscope`	`'gyroscope'`
`LinearAccelerationSensor`	`'accelerometer'`
`Magnetometer`	`'magnetometer'`
`RelativeOrientationSensor`	`'accelerometer'`, and `'gyroscope'`

Zdroj: https://developer.mozilla.org/en-US/docs/Web/API/Sensor_APIs

Browser fingerprinting

Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser Fingerprinting: A Survey. ACM Trans. Web 14, 2, Article 8 (May 2020), 33 pages.

- https://coveryourtracks.eff.org/
- https://AmIUnique.org/

SCREEN SIZE AND COLOR DEPTH

1280x1024x24

Bits of identifying information: *7.71*
One in x browsers have this value: *209.4*

SYSTEM FONTS

Arial, Arial Narrow, Bitstream Vera Sans Mono, Bookman Old Style, Calibri, Cambria, Century Schoolbook, Courier, Courier New, Helvetica, Palatino, Palatino Linotype, Times, Times New Roman (via javascript)

Bits of identifying information: *9.32*
One in x browsers have this value: *639.07*

ARE COOKIES ENABLED?

Yes

Bits of identifying information: *0.15*
One in x browsers have this value: *1.11*

LIMITED SUPERCOOKIE TEST

DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: false, indexed db: true

Bits of identifying information: *1.15*
One in x browsers have this value: *2.22*

Our tests indicate that you have **strong protection against Web tracking**.

IS YOUR BROWSER:

Blocking tracking ads?	**Yes**
Blocking invisible trackers?	**Yes**
Protecting you from fingerprinting?	**your browser has a randomized fingerprint**

Still wondering how fingerprinting works?

LEARN MORE

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

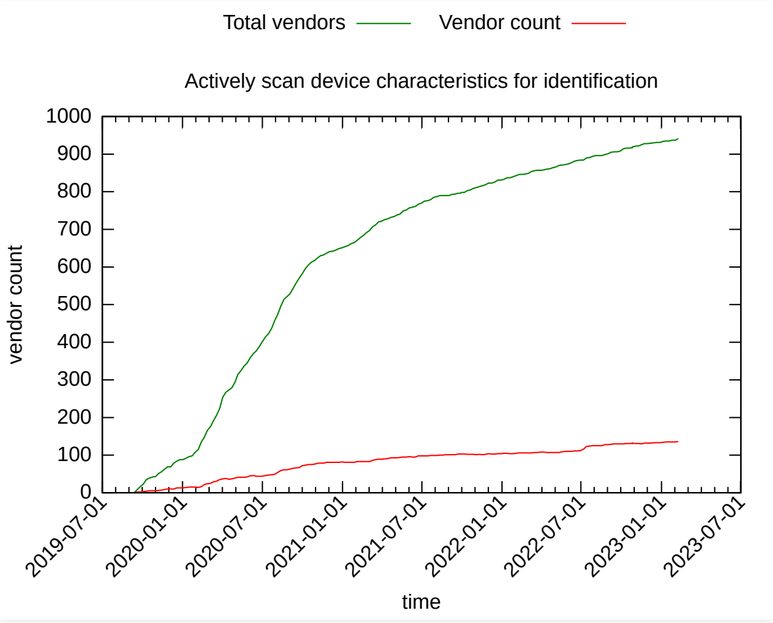
Your Results

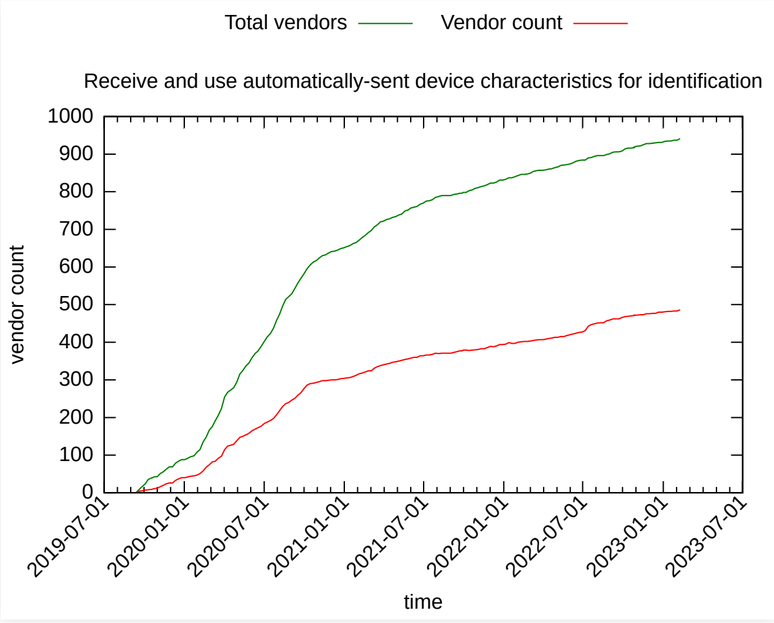
Your browser fingerprint **has been randomized** among the 172,549 tested in the past 45 days. Although sophisticated adversaries may still able to track you to some extent, randomization provides a very strong protection against tracking companies trying to fingerprint your browser.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.4 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Adtech data from TCF

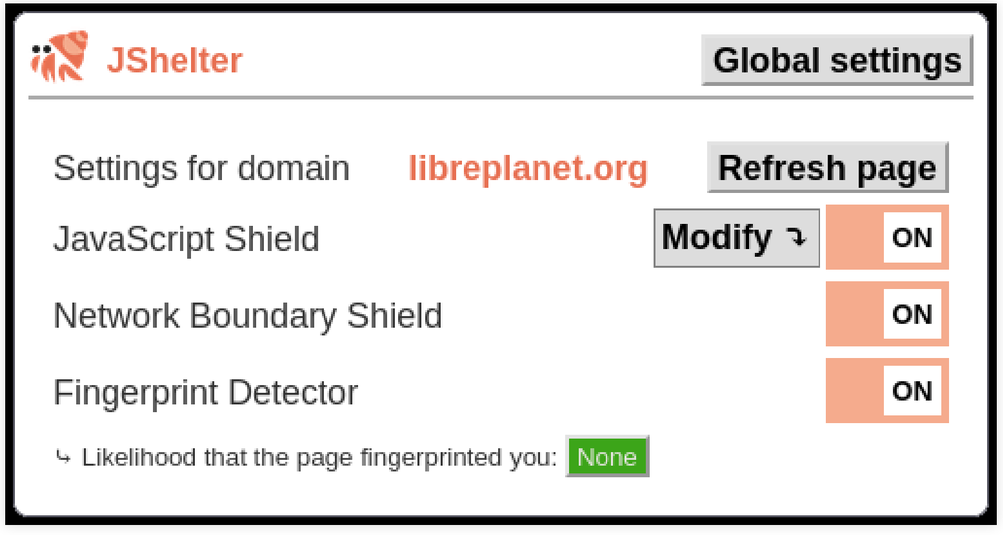




Zdroj: https://www.fit.vutbr.cz/~polcak/tcf/tcf2.html

What JShelter does?

JShelter

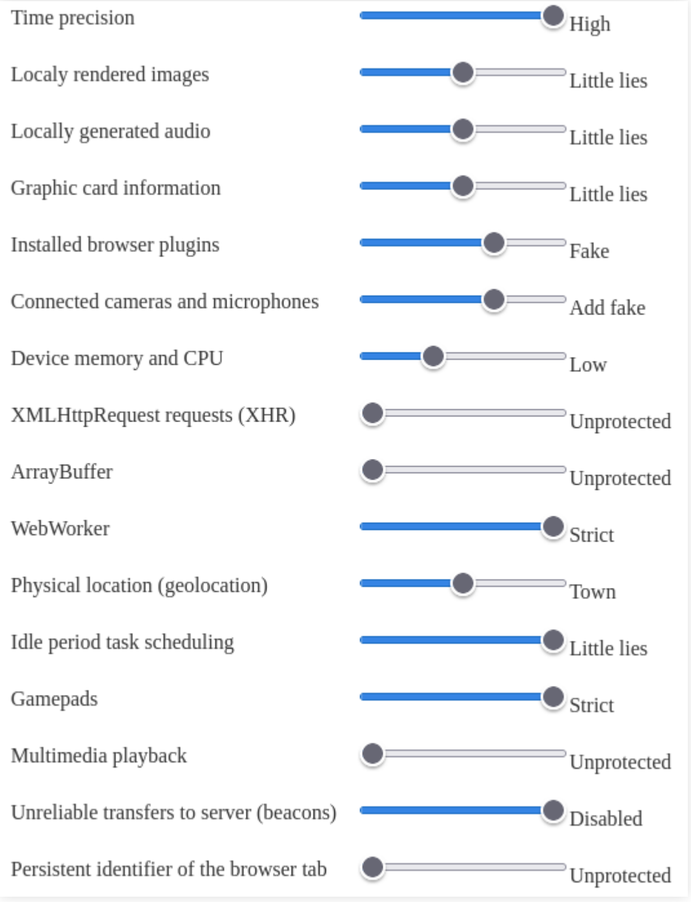

JShelter
Global settings
Settings for domain
libreplanet.org
Refresh page
JavaScript Shield
Modify
ON
Network Boundary Shield
ON
Fingerprint Detector
ON
Likelihood that the page fingerprinted you:
None

JavaScript Shield

- Limit the powers of problematic APIs
  - Modify the real value
  - Provide fake value
  - Do not do an action (e.g., Web Beacon API)
  - etc.

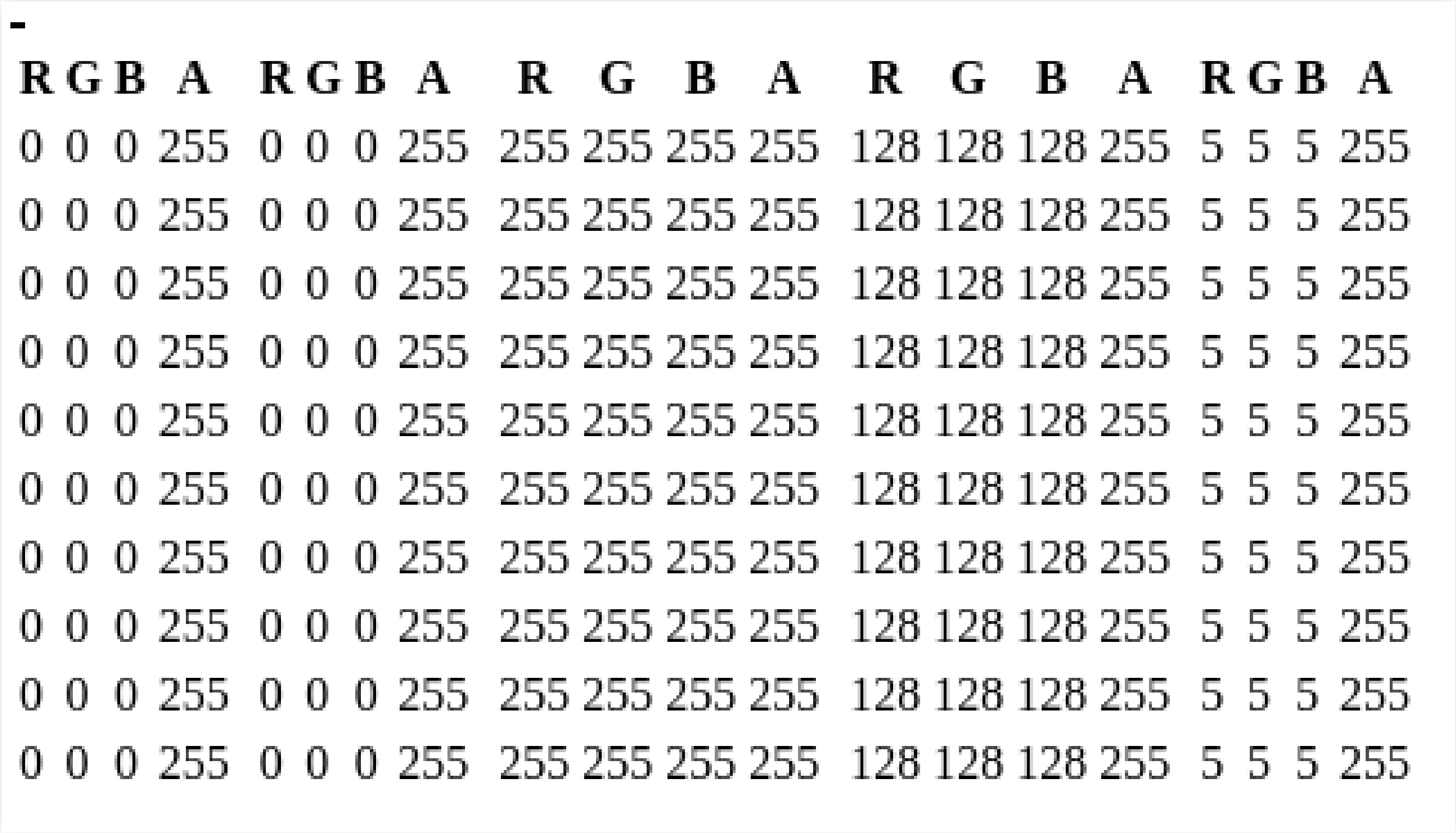
JavaScript Shield - More than 100 APIs

- Schwarz et al. Javascript zero: Real javascript and zero side-channel attacks. In Network and Distributed Systems Security Symposium 2018, 2018. ISBN 1-1891562-49-5. https://github.com/IAIK/ChromeZero
- Iqbal et al. Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. In IEEE Symposium on Security & Privacy, 2021.
- Peter Snyder et al. Most Websites Don't Need to Vibrate: A Cost-Benefit Approach to Improving Browser Security. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). ACM, New York, NY, USA, 179–194.
- APIs declined by Apple


Time precision
High
Localy rendered images
Little lies
Locally generated audio
Little lies
Graphic card information
Little lies
Installed browser plugins
Fake
Connected cameras and microphones
Add fake
Device memory and CPU
Low
XMLHttpRequest requests (XHR)
Unprotected
ArrayBuffer
Unprotected
WebWorker
Strict
Physical location (geolocation)
Town
Idle period task scheduling
Little lies
Gamepads
Strict
Multimedia playback
Unprotected
Unreliable transfers to server (beacons)
Disabled
Persistent identifier of the browser tab
Unprotected

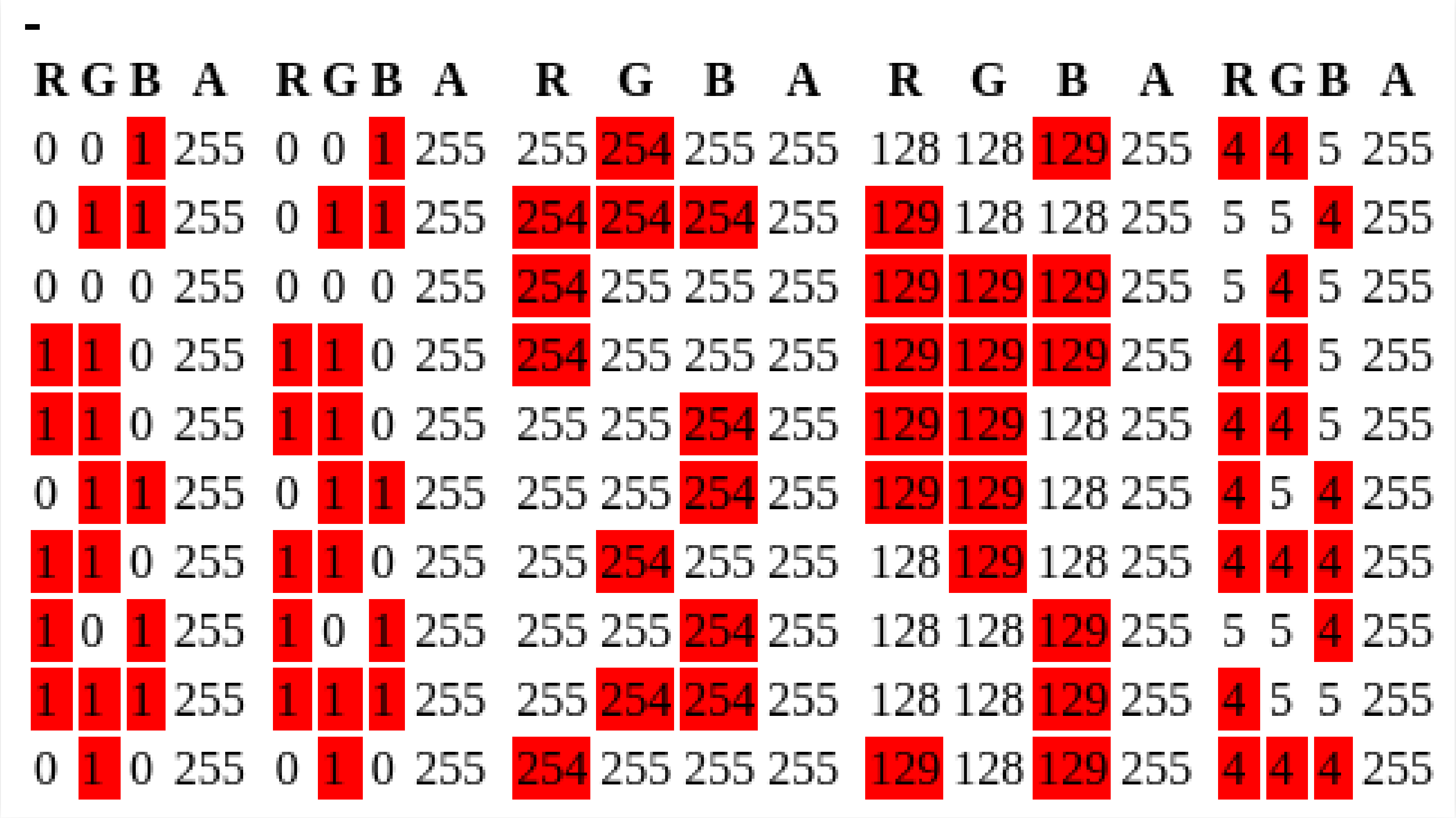
JSShield and browser fingerprinting

- Little lies
  - Similar implementation to Brave
  - Nikiforakis et al. PriVaricator: Deceiving fingerprinters with little white lies. In WWW ’15, pages 820—-830. ISBN 9781450334693.
  - Mishra et al. FPRandom: Randomizing core browser objects to break advanced device fingerprinting techniques. In 9th International Symposium on Engineering Secure Software and Systems, page 17, 2017.
  - The goal is to create a unique fingerprint per session and domain



-

R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255
0	0	0	255	0	0	0	255	255	255	255	255	128	128	128	255	5	5	5	255



-

R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A
0	0	1	255	0	0	1	255	255	254	255	255	128	128	129	255	4	4	5	255
0	1	1	255	0	1	1	255	254	254	254	255	129	128	128	255	5	5	4	255
0	0	0	255	0	0	0	255	254	255	255	255	129	129	129	255	5	4	5	255
1	1	0	255	1	1	0	255	254	255	255	255	129	129	129	255	4	4	5	255
1	1	0	255	1	1	0	255	255	255	254	255	129	129	128	255	4	4	5	255
0	1	1	255	0	1	1	255	255	255	254	255	129	129	128	255	4	5	4	255
1	1	0	255	1	1	0	255	255	254	255	255	128	129	128	255	4	4	4	255
1	0	1	255	1	0	1	255	255	255	254	255	128	128	129	255	5	5	4	255
1	1	1	255	1	1	1	255	255	254	254	255	128	128	129	255	4	5	5	255
0	1	0	255	0	1	0	255	254	255	255	255	129	128	129	255	4	4	4	255

Little lies (cont.)

-

R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A
0	0	1	255	0	0	1	255	255	254	255	255	128	128	129	255	4	4	5	255
0	1	1	255	0	1	1	255	254	254	254	255	129	128	128	255	5	5	4	255
0	0	0	255	0	0	0	255	254	255	255	255	129	129	129	255	5	4	5	255
1	1	0	255	1	1	0	255	254	255	255	255	129	129	129	255	4	4	5	255
1	1	0	255	1	1	0	255	255	255	254	255	129	129	128	255	4	4	5	255
0	1	1	255	0	1	1	255	255	255	254	255	129	129	128	255	4	5	4	255
1	1	0	255	1	1	0	255	255	254	255	255	128	129	128	255	4	4	4	255
1	0	1	255	1	0	1	255	255	255	254	255	128	128	129	255	5	5	4	255
1	1	1	255	1	1	1	255	255	254	254	255	128	128	129	255	4	5	5	255
0	1	0	255	0	1	0	255	254	255	255	255	129	128	129	255	4	4	4	255

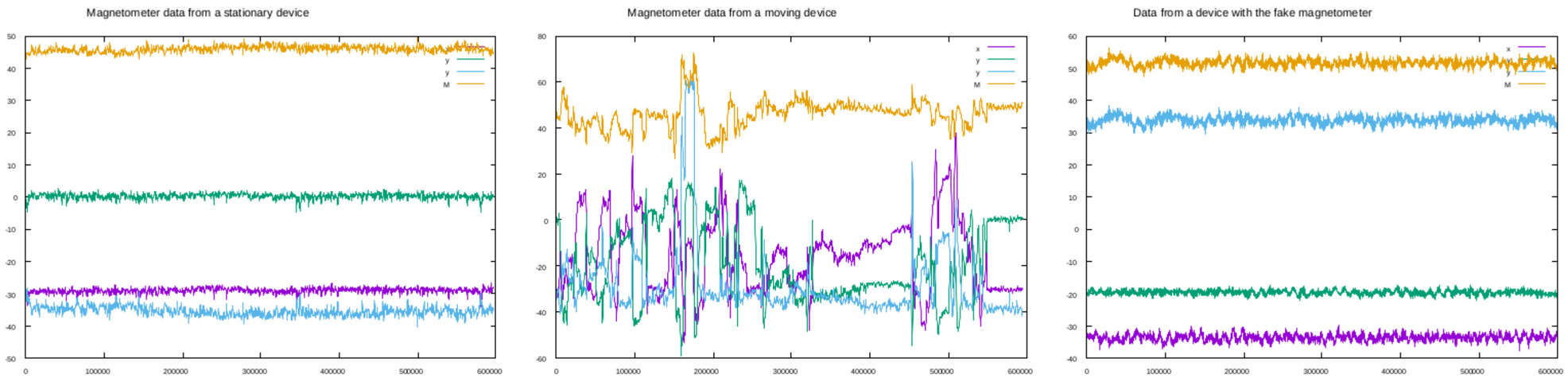
-

R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A	R	G	B	A
0	1	1	255	0	1	1	255	254	255	255	255	129	128	129	255	4	5	4	255
1	1	1	255	1	1	1	255	255	255	254	255	128	128	128	255	5	5	4	255
1	0	0	255	1	0	0	255	255	254	255	255	128	128	128	255	4	4	5	255
1	1	1	255	1	1	1	255	255	254	254	255	128	129	129	255	4	4	4	255
0	0	0	255	0	0	0	255	255	254	254	255	129	128	128	255	4	5	4	255
0	0	0	255	0	0	0	255	255	254	255	255	128	128	129	255	4	5	5	255
1	1	0	255	1	1	0	255	254	254	255	255	129	129	128	255	5	4	5	255
0	1	0	255	0	1	0	255	255	255	254	255	129	129	128	255	4	4	5	255
1	1	0	255	1	1	0	255	255	255	254	255	128	129	129	255	4	4	4	255
1	0	0	255	1	0	0	255	255	255	255	255	129	129	128	255	5	4	4	255

We do not hide in the crowd

- We do not want to make all users the same
- JShelter does not wrap all APIs
- JShelter do not and cannot change IP address and other parameters unavailable to webextensions
- If you like this strategy, use Torbrowser
- Strict level: limit the amount of information available about the system but do not protect from fingerprinting

JSShield and mobile devices



(a) Stationary device (b) Moving device (c) Fake readings

Network Boundary Shield

- Do not allow pages from global web access local resources

```
xhr.open('GET', 'https://192.168.1.1/mikrotik.png', true);
```

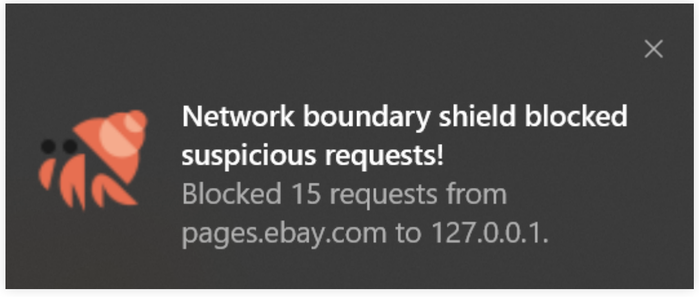
- SOP does not allow reading such resource, but a side-channel allows to learn if such resource exists
  - Additional effects if the target is implmented wrong

Scan of localy running applications by ThreatMetrix Inc.

- Deployed on about 30000 webs including ebay

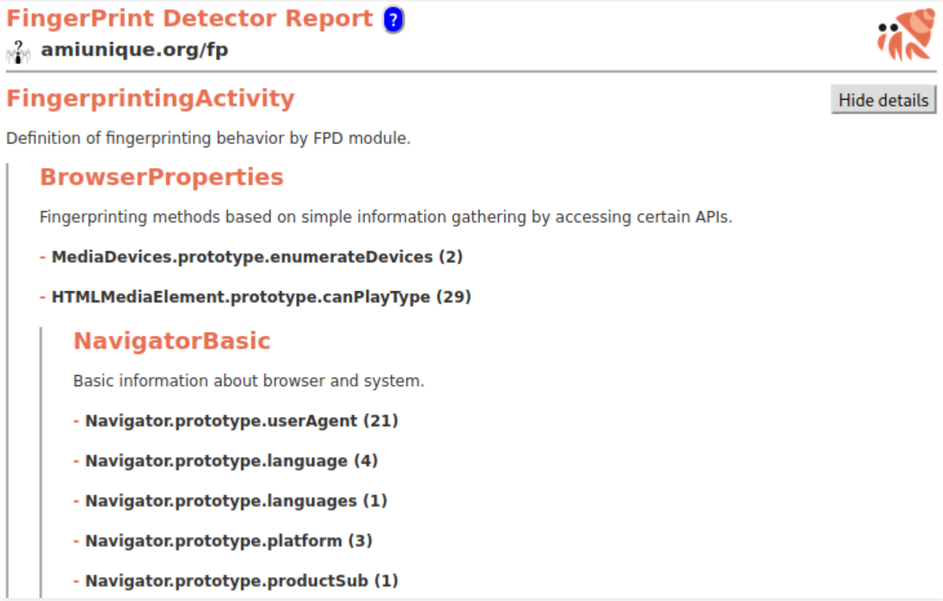
Status	Method	Domain	File	Initiator
204	GET	src.ebay-us.com	8vrNy99Kny-rPzgL?b6da6859bab319a0=-5viBM2jbTMP2t_pm31dmqJ5...	2aKzihsbphg
204	GET	src.ebay-us.com	INgmIIM4IGBIrnvo?cc7aac7988b25487=oLxqfbb3qgqFjDxkw9CT0sKTj...	2aKzihsbphg
204	GET	src.ebay-us.com	INgmIIM4IGBIrnvo?cc7aac7988b25487=oLxqfbb3qgqFjDxkw9CT0sKTj...	2aKzihsbphg
	GET	127.0.0.1:63333	/	2aKzihsbphg
204	GET	src.ebay-us.com	8vrNy99Kny-rPzgL?b6da6859bab319a0=-5viBM2jbTMP2t_pm31dmqJ5...	2aKzihsbphg
	GET	127.0.0.1:5900	/	websocket
	GET	127.0.0.1:5901	/	2aKzihsbphg
	GET	127.0.0.1:5902	/	2aKzihsbphg
	GET	127.0.0.1:5903	/	2aKzihsbphg
	GET	127.0.0.1:3389	/	2aKzihsbphg
	GET	127.0.0.1:5950	/	2aKzihsbphg
	GET	127.0.0.1:5931	/	2aKzihsbphg
	GET	127.0.0.1:5939	/	2aKzihsbphg
	GET	127.0.0.1:6039	/	2aKzihsbphg
	GET	127.0.0.1:5944	/	2aKzihsbphg
	GET	127.0.0.1:6040	/	2aKzihsbphg
	GET	127.0.0.1:5279	/	2aKzihsbphg
	GET	127.0.0.1:7070	/	2aKzihsbphg
204	GET	src.ebay-us.com	INgmIIM4IGBIrnvo?cc7aac7988b25487=oLxqfbb3qgqFjDxkw9CT0sKTj...	2aKzihsbphg
200	POST	pulsar.ebay.com	9?pId=[{"ef":"HOMEPAGE","ea":"PAGEPING","pge":2481888,"pIsUBT":1,...	s0hteylevy4b

- Detection of applications for desktop sharing


Network boundary shield blocked suspicious requests!
Blocked 15 requests from pages.ebay.com to 127.0.0.1.

Fingerprint Detector

- Heuristics on JavaScript API calls, including APIs not covered by JS Shield
  - Acar et al. The web never forgets: Persistent tracking mechanisms in the wild. CCS ’14
  - Englehardt a Narayanan. Online tracking: A 1-million-site measurement and analysis. CCS ’16
  - Iqbal et al. Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. IEEE Symposium on Security & Privacy, 2021.
  - Laperdrix et al. Browser fingerprinting: A survey. ACM TWeb '20



Detection accuracy

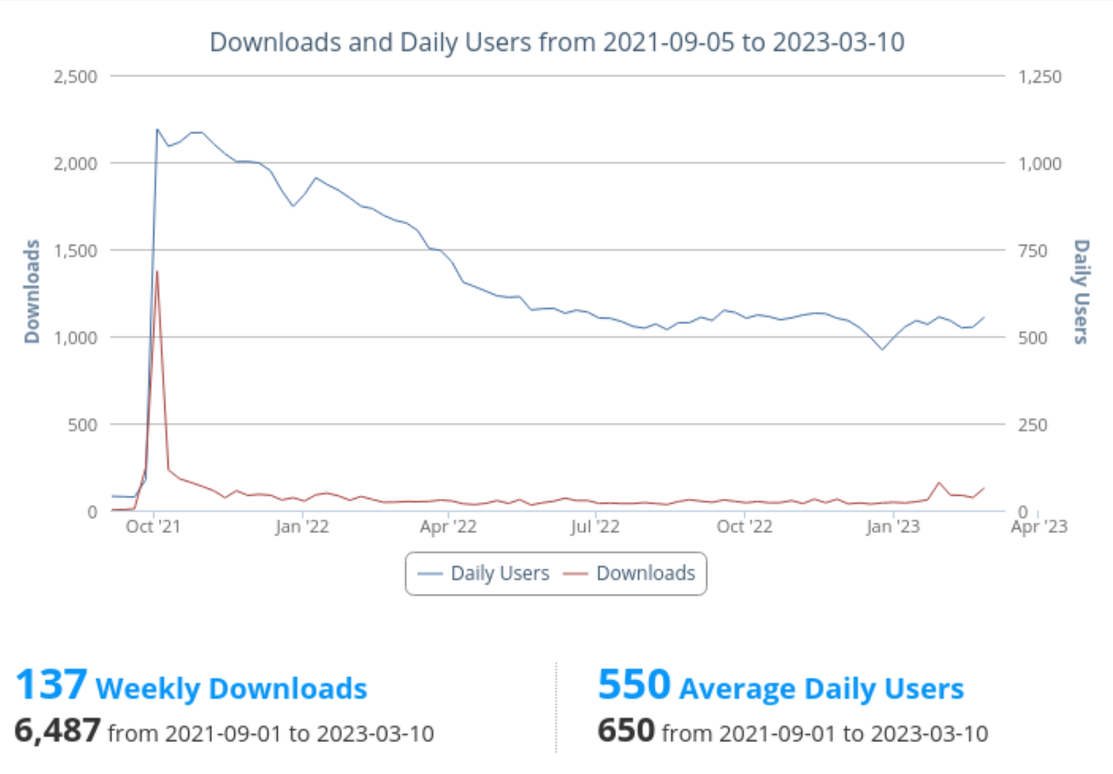
- Comparison with extensions FPMON a Don't fingerprint Me
  - Most visited pages, the 3 extensions scored according to their detection capabilities

		Home pages	**Login pages**
Visited		**98**	**81**
JShelter	correctly detected	96 (98.0%)	77 (95.1%)
FPMON	red	79 (80.6%)	66 (81.5%)
	red/yellow	96 (98.0%)	80 (98.8%)
DFPM	2+ dangers	70 (71.4%)	66 (81.5%)
	1+ dangers	98 (100%)	81 (100%)

- The challenge: how to differentiate between a fingerprint and benign behavior

Project status

Cooperation with FSF



- Giorgio Maone (NoScript) is a part of the team
- Source code
- Paper
- FAQ
- Open issues

Funding

- Thank NLNet Foundation
  - https://nlnet.nl/project/JSRestrictor/
  - JShelter
  - JShelter Manifest V3
- We are looking for research cooperation
  - e.g. HORIZON-CL3-2023-CS-01-02

How can you help?

How can you help?

- Install JShelter and report bugs
- Become tester/developer
  - Read mailinglist, let us know if you want to join
- We are looking for research cooperation
  - e.g. HORIZON-CL3-2023-CS-01-02

Thank you for attention