

Webtracking

oder: kommerzielle Internetüberwachung

Gegenmaßnahmen für Firefox

Cryptoparty ÖH, 2014-12-02

Anton

an.to_n-73 at riseup net

PGP: 0B4C DF2C CB22 5DF4 25EA F212 49D1 ABF2 A2A9 7D7D

Grund für kommerzielle Überwachung

“Kennenlernen” der NutzerInnen

Anlegen eines Personenprofils (*de-anonymisierbar!*)

Interessengebiete, Hobbies ...

ähnlich Kundenkarten und Postwurfsendungen

- Verkauf gebündelter Profile an Werbefirmen
- Einblenden zielgerichteter Werbung (teurer)
- Conversion Tracking

(Potentielle) Probleme: Scoring, Datenhandel

Kreditgeber, Versicherung, Arbeitgeber,
Preisdifferenzierung, Wahlkampf

Webtracking kostet Nerven und Ladezeit!

Hier: Abhilfe bei kommerzieller Überwachung, **NICHT** staatlicher Überwachung

- Kein absoluter, nur relativer Schutz!
- Erhöhung der Überwachungshürde, die Kosten werden gesteigert
- Kosten/Nutzen Rechnung der Überwacher wird verschlechtert

Für schwierige Fälle: Tor Browser, JonDoFox

Obacht: MITM Problem bei https, bei Tor treten spionierende Exits auf (“spoiled onions”)!

3rd party Cookies

Beispiel: <http://krone.at> , <http://derstandard.at>

→ 3rd party Cookies abschalten

Individuelle Marker im Cache

Beispiel: Auf populären Seiten rumsurfen

Danach mit AddOn CacheViewer nachgucken

→ Firefox-Verlauf bei jeden Beenden löschen

→ Festplatten-Caches abschalten

AddOn 1: Request Policy <https://www.requestpolicy.com>

Der Löscher (auch Flash Cookies etc.)

BleachBit: <http://bleachbit.sourceforge.net>

mit Vorsicht handhaben, vorher Beschreibung lesen, was gelöscht wird

Browser Fingerprinting

hauptsächlich per Javascript (JS)

Beispielseiten:

<https://panopticklick.eff.org/>

<http://letmetrackyou.org/identify.php>

→ Gegenmaßnahmen mit aktiviertem Javascript
sehr schwierig !

AddOn 2: NoScript <http://noscript.net/>

→ Whitelist nach Installation löschen!

Weitere Trackingmethoden, nicht browserbasiert

IP Adresse (Abhilfe: VPN, Tor, JonDonym)

Clock Skew (individuelle Gang-Ungenauigkeit Uhr),
Abhilfe: Firewall einstellen (TCP Timestamp raus)

"Unsere Messwerte liefern absolut zuverlässige Ergebnisse', versicherte ein Tracking-Experte, der anonym bleiben will, gegen-über c't. Sein Unternehmen plant, Clock-Skew-Fingerprinting insbesondere einzusetzen, um mobile Endgeräte zu tracken, bei denen der Einsatz von Cookies zu viele Unschärfen produziert."

Stille Verfolger - Unternehmen setzen auf Nutzer-Tracking ohne Cookies,
c't 11/2014, S. 161/162,
http://www.heise.de/artikel-archiv/ct/2014/11/160_Stille-Verfolger

Remote physical device fingerprinting, Kohno 2005,
<http://www.caida.org/publications/papers/2005/fingerprinting>

Individuelle X-UIDH Header (Abhilfe: VPN)

Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls , <https://www.eff.org/deeplinks/2014/11/verizon-x-uidh>

Wie kann man wo und womit überwacht werden?

Trace My Shadow

<https://myshadow.org/trace-my-shadow>

Visualisierung von kommerzieller Überwachung

Mozilla Lightbeam

<https://www.mozilla.org/de/lightbeam>

Maßnahmenliste

Suchmaschinen: Startpage, Ixquick, DuckDuckGo, Qwant ...

Einstellungen: Anwendungen: “Immer nachfragen”

Privatsphäre: Do Not Track Header setzen

Drittpartei Cookies untersagen

Browserhistorie bei Beenden löschen

Erweitert/Netzwerk: Cache zu 0 setzen

AddOn 1: NoScript

Ausnahmeliste löschen, JS 2nd level domains zulassen (nur aktuelleseite.at, *nicht* drittpartei1.com, drittpartei2.com, ...)

AddOn 2: Request Policy: Ausnahmeliste löschen

Beide AddOns: Leichte Komforteinschränkung, Anlernphase für benötigte Drittparteien (z. B. Content Delivery Networks)

Optional: AdBlock Edge statt Request Policy, Filterlisten wählen!

Trackertest: 1x ohne, 1x mit Maßnahmen

<http://www.wieistmeineip.at>

<http://www.heise.de>

<http://derstandard.at>

<http://www.zalando.de>

<http://www.spiegel.de>

<http://diepresse.com>

<http://www.zeit.de>

<http://www.propublica.org>

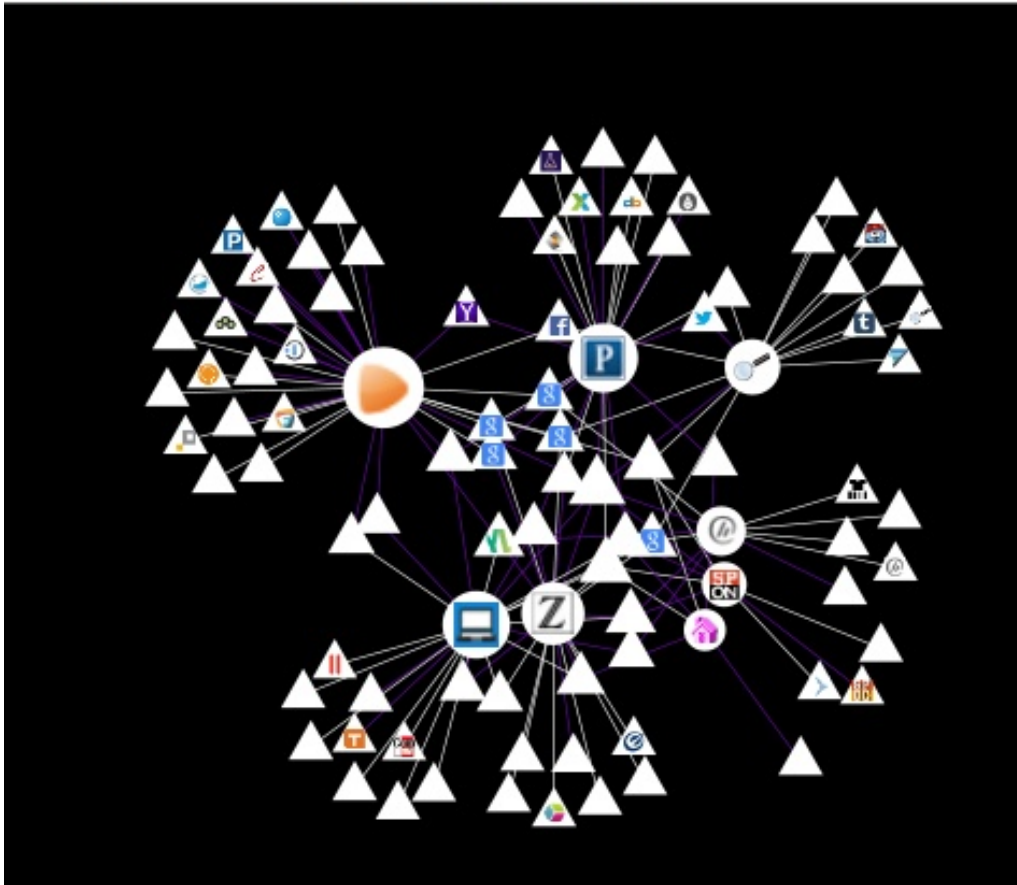
<http://www.reddit.com>

<http://www.ebay.at>

“Besuchte” Drittparteien, Visualisierung mit Lightbeam

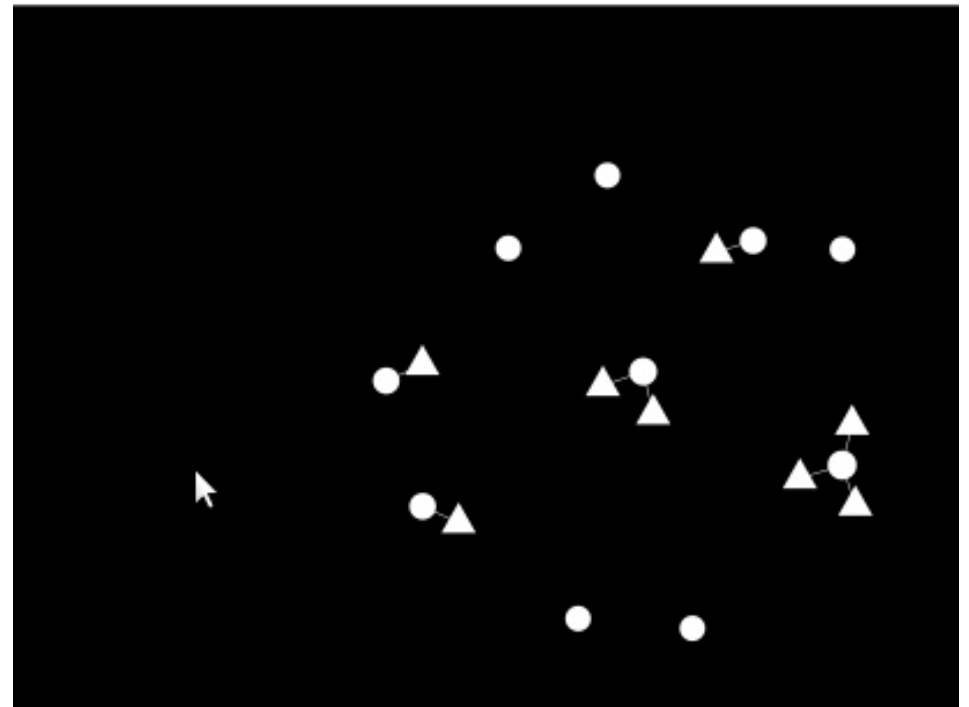
Ohne Maßnahmen

YOU HAVE VISITED 9 SITES
YOU HAVE CONNECTED WITH 136 THIRD PARTY SITES



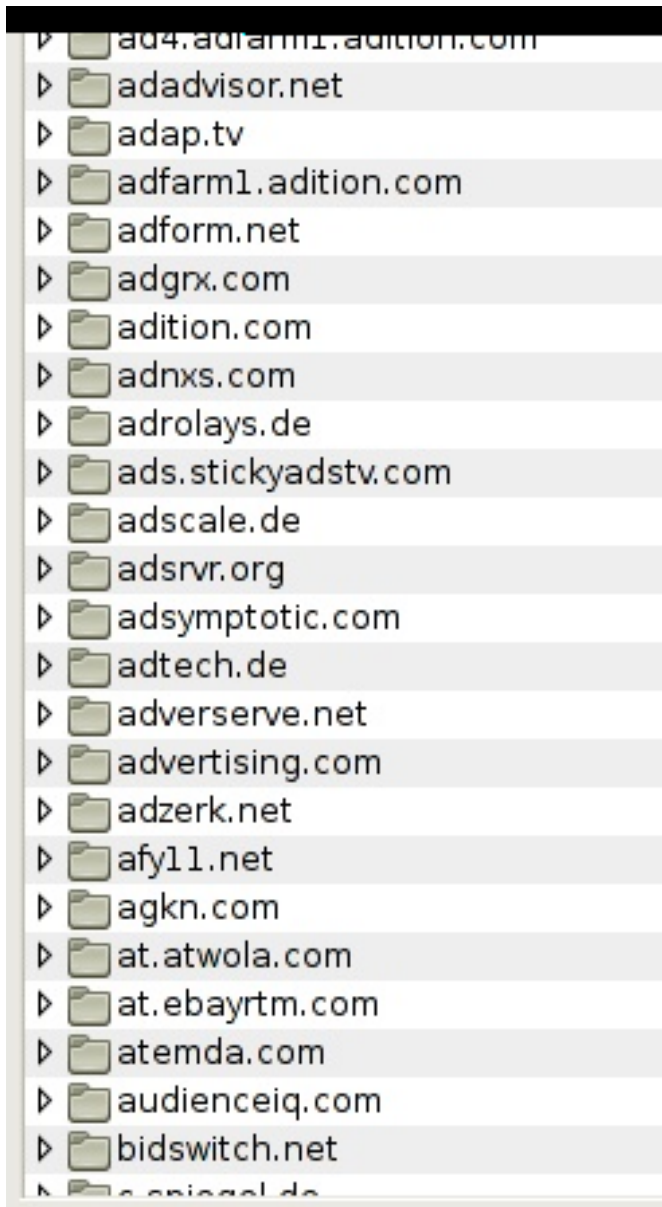
mit Maßnahmen

YOU HAVE VISITED 10 SITES
YOU HAVE CONNECTED WITH 8 THIRD PARTY SITES



Cookies

Ohne Maßnahmen



mit Maßnahmen



Cache

Ohne Maßnahmen

| Key |
|--|
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://s322.meetrics.net/bb-mx/submit?/rMJQH66GAlklFBtkzFtGg4BAAAAQ7... |
| http://adserve.quality-channel.de/RealMedia/ads/adstream_lx.ads/www.spie... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://smart.styria-digital.com/h/aip?siteid=53612&pgid=392404&fmtid=... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://d.turn.com/r/du/id/L2NzaWQvMS9tcGlkLzE4MMDM3MTM5/mpuid/69095... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://dc84.s290.meetrics.net/bb-mx/submit?/wk2MRRYFBLklFBtkzFtPfiCIDA... |
| http://dc84.s290.meetrics.net/bb-mx/submit?/wk2MQ1gGAlklFBtkzFeGhIDA... |
| http://adserve.quality-channel.de/5/www.spiegel.de/homepage/center/L30/... |
| http://adserve.quality-channel.de/RealMedia/ads/Creatives/qc/sp-zaehler-0... |
| http://ww251.smartadserver.com/track/comp.asp?keyword=A2%3D3%3BA... |
| https://us-u.openx.net/w/1.0/sd?id=537072980&val=CAESEOKVGWrI8z7w... |
| http://c.spiegel.de/nm_empty.gif?url=http%3A/www.spiegel.de/&referrer=... |
| http://pixel.ad.mlnadvertising.com/sync.ashx?cktst=1&partner=2591&psi... |
| http://uk-ads.openx.net/w/1.0/ri?ts=1fHU9MXxyaWQ9NTk5ZTZjNDQtOTgxZ... |
| http://uk-ads.openx.net/w/1.0/ri?ts=1fHjpZD1kOGjMmEzYi1iNDNkLTQ3M2it... |
| http://e.nexac.com/e/xrefid.xgi?na_exid=4035113658967848417&na_pid... |
| http://www.spiegel.de/static/svs/pixel.gif |
| Memory: 264 entries 0.33/23.55 Disk: 1647 entries 20. |

mit Maßnahmen

| Key |
|---|
| http://derstandard.at/s/14166761-5752-D899-3643-46645A5A55D0/1/141... |
| http://derstandard.at/s/1477307/7813/1/14166761-5752-D899-3643-466... |
| http://derstandard.at/s/arb/false/false |
| http://derstandard.at/s/arb/false/true |
| http://prophet.heise.de/288689636920174/wt?p=322,www.heise.de.start... |
| https://track.zalando.de/789345933667438/wt?p=324,www.zalando.de%2... |
| http://ww251.smartadserver.com/h/aip?visit=s&pubid=23&statid=12&cki... |
| http://ww251.smartadserver.com/h/aip?visit=s&pubid=23&statid=12&cki... |
| http://ww251.smartadserver.com/h/aip?visit=v&pubid=23&statid=12&cki... |
| http://prophet.heise.de/288689636920174/wt?p=322,www.heise.de.start... |
| https://www.propublica.org/search/auth.php?callback=jQuery1820924042... |
| http://diepresse.com/portal/services/captcha/captchalmage.jsp |
| http://www.wieistmeineip.at/ |
| http://www.zalando.de/ |
| http://diepresse.com/ |
| Memory: 17 entries 0.09/23.55 Disk: 0 entries 0/0 |

Beispiele für Drittparteien Javascript, Spurenloses Tracking

The image shows a screenshot of a web browser displaying the ProPublica website. The browser's address bar shows the URL <http://www.propublica.org/>. The website header includes the ProPublica logo and the tagline "Journalism in the Public Interest". A navigation menu contains links for Home, Our Investigations, Tools & Data, MuckReads, Get Involved, and About Us. The main content area features a large article titled "Leak at Fed Reserve Reveals Confidential Bond-Buying" by Jake Bernstein, with a photo of a man speaking at a podium. Below this are two smaller article teasers: "Now What? Failed Allergan Deal Strains Valeant" by Jesse Eisinger and "Fire War" by T and Nov. The right side of the browser window is overlaid with a list of third-party tracking scripts, each preceded by a red 'S' icon and the text "als nicht vertrauenswürdig einstufen".

Don't Miss: [Treatment Tracker](#) | [Tobacco Bonds](#) | [Dollars for Docs](#) | [Segregation](#)

PRO PUBLICA Journalism in the Public Interest

Home | Our Investigations | Tools & Data | MuckReads | Get Involved | About Us

Leak at Fed Reserve Reveals Confidential Bond-Buying
by Jake Bernstein
ProPublica, Today
Then-Chairman ordered an intercept previously und... which found its newsletter for b...

Now What? Failed Allergan Deal Strains Valeant
by Jesse Eisinger
ProPublica, Nov. 26, Noon

Fire War
by T and Nov

Edi Fire Sect

- propublica.org als nicht vertrauenswürdig einstufen
- facebook.com als nicht vertrauenswürdig einstufen
- twitter.com als nicht vertrauenswürdig einstufen
- flashtalking.com als nicht vertrauenswürdig einstufen
- facebook.net als nicht vertrauenswürdig einstufen
- d8k88hv3sn2aj.cloudfront.net als nicht vertrauenswürdig einstufen
- googlesyndication.com als nicht vertrauenswürdig einstufen
- googleadservices.com als nicht vertrauenswürdig einstufen
- doubleclick.net als nicht vertrauenswürdig einstufen
- chartbeat.com als nicht vertrauenswürdig einstufen
- typekit.net als nicht vertrauenswürdig einstufen
- google-analytics.com als nicht vertrauenswürdig einstufen
- googletagmanager.com als nicht vertrauenswürdig einstufen
- googletagservices.com als nicht vertrauenswürdig einstufen
- tumblr.com als nicht vertrauenswürdig einstufen
- twimg.com als nicht vertrauenswürdig einstufen
- d15qhc0lu1ghnk.cloudfront.net als nicht vertrauenswürdig einstufen
- akamaihd.net als nicht vertrauenswürdig einstufen
- rbl.ms als nicht vertrauenswürdig einstufen
- rebelmouse.com als nicht vertrauenswürdig einstufen
- Skripte allgemein verbieten (empfohlen)

Anhang: Weiterlesen

Studie: Web-Tracking-Report

<https://www.sit.fraunhofer.de/de/wtr>

Studie: Kommerzielle digitale Überwachung im Alltag

<http://crackedlabs.org/studie-kommerzielle-ueberwachung>

Congressional Testimony: What Information Do Data Brokers Have on Consumers?

<http://www.worldprivacyforum.org/2013/12/testimony-what-information-d>

Projekt: DataSeal

<https://privacymachine.eu/wiki/de/dataseal>

How Microsoft and Yahoo Are Selling Politicians Access to You

<http://www.propublica.org/article/how-microsoft-and-yahoo-are-selling-politicians-access>

Everything We Know About What Data Brokers Know About You

So they don't sell information about my health?

[http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-al](http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you)

Insurers Test Data Profiles to Identify Risky Clients

<http://online.wsj.com/news/articles/SB100014240527487046486045756207509980729>

Wie Facebook-Einträge einen Kredit verhindern können

<http://www.wsj.de/nachrichten/SB10001424052702303848104579310063733795206>

EC-Datenfirma wollte zur neuen Schufa werden

<http://www.zeit.de/digital/datenschutz/2011-09/easycash-datenschutz-schufa>

Has Google Gone Too Far? Parental Status Demographic Added to AdWords

<http://www.wordstream.com/blog/ws/2014/06/20/adwords-parental-status>

Tricksen und täuschen mit System (Preisdifferenzierung im Internet)

[http://www.sueddeutsche.de/digital/preisdifferenzierung-im-internet-tricksen-und-taeus](http://www.sueddeutsche.de/digital/preisdifferenzierung-im-internet-tricksen-und-taeuschen)

Auktion wie ein Wimpernschlag (Real Time Bidding, Preisfindung für zielgerichtete Internetwerbung)

<http://www.sueddeutsche.de/digital/internet-werbung-auktion-wie-ein-wimpernschlag-1>