Blokkeer fingerprinting …

Ruud Uphoff

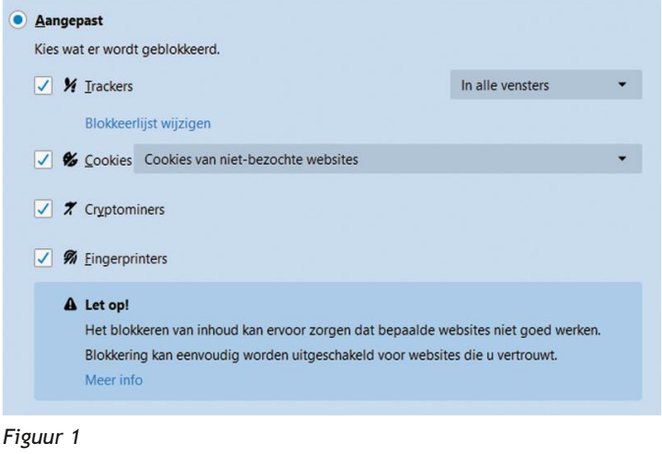
Oftewel: de marketing-maffia het handwerk verzieken.

Ik weet het, ik ben niet aardig, maar de bedrijvers van marketing die blijven proberen zonder toestemming ons met tracking cookies en 3rd party-script te volgen, geef ik de verzamelnaam 'marketing-maffia'. Momenteel wordt de AVG (Algemene Verordening Gegevensbescherming) massaal met voeten getreden en de Autoriteit Persoonsgegevens lijkt op een hondje dat flink blaft, maar niet bijt.

We kunnen wel deze marketing-maffia het handwerk prima verzieken. Nu ben ik mij ervan bewust dat er, ook onder de lezers van SoftwareBus, mensen zullen zijn die ik hiermee verdrietig maak. Het probleem is namelijk dat er met een beetje relativeren van onze privacy veel geld te verdienen is. Maar: er is niets op tegen als je medelijden met hen hebt en de adviezen in dit artikel niet opvolgt. Er zijn geen strafbepalingen!

Gebruik Firefox

Deze browser, gratis voor Windows, Mac, Linux en Android, is uitgerust om af te rekenen met tracking cookies en andere vormen van volgen. En dat doen ze beter dan de Autoriteit Persoonsgegevens, die niet in staat lijkt keihard tegen overtreders van de AVG op te treden. Zorg dat je de laatste versie van Firefox gebruikt en stel deze als volgt in: (*Zie figuur 1*)



Figuur 1

- Open het menu (rechts bovenin, drie streepjes onder elkaar).
- Kies ***Inhoudsblokkering***.
- Kies ***Aangepast*** en zet daaronder alle vier de vinkjes aan.
- Open het afrolmenu naast ***Trackers*** en selecteer ***In alle vensters***.
- Klik onder ***Trackers*** op ***Blokkeerlijst wijzigen*** en kies ***niveau 2***. Mijn ervaring is dat hierdoor alleen minder-bonafide sites niet goed werken.
- Open het afrolmenu naast ***Cookies*** en kies ***Cookies van niet-bezochte websites***. Hiermee worden cookies van derden toegestaan die puur technisch noodzakelijk zijn.
- Onder ***Websites een niet volgen signaal sturen…*** Kies ***Altijd***.
- Onder ***Cookies en websitegegevens***, zet het vinkje ***uit***, dus niets verwijderen bij afsluiten.

Wanneer je nu een website bezoekt, zul je vaak in de adresbalk een schildje zien. Klik daarop om te zien wat Firefox heeft geblokkeerd. Daar kun je ook een website uitzonderen van de blokkering.

De figuur is uit Firefox 67, die 21 mei 2019 werd uitgebracht. De twee onderste opties waren tot dan toe niet aanwezig. Firefox wil tegen die tijd ook bescherming bieden tegen 'fingerprinting', maar de optie werkte in mijn bètaversie totaal nog niet.

Belangrijke uitbreidingen (extensies) op Firefox

Echt, ik ben graag aardig. Elk lid van de marketing-maffia laat ik met een vriendelijke buiging binnen. Maar eenmaal binnen wordt de tracker, zoals in maffiakringen gebruikelijk, door de achterdeur naar buiten gemept. Om te beginnen willen we geen last hebben van gezeur aan de voordeur over toestemming voor cookies.
De eerste van drie extensies:

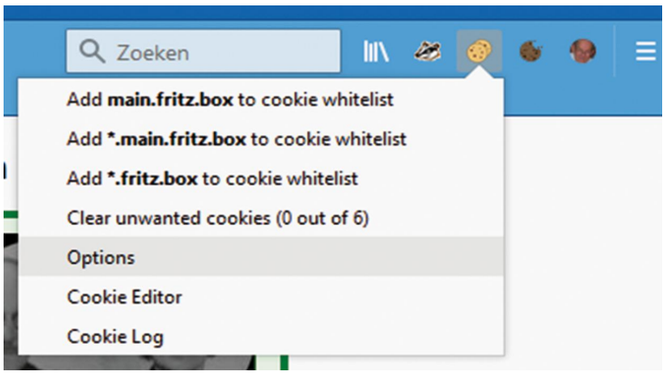
I don't care about cookies detecteert de diverse pop-ups voor toestemming en staat alles gewoon automatisch toe. Zo, daar hebben we geen last meer van. In sommige gevallen wordt een cookiemelding niet ontdekt. Je kunt die site dan simpel rapporteren, en vaak is dat dan binnen een dag geregeld. Er zijn ook pop-ups op een geblokkeerd scherm, waar de extensie niet werkt en waardoor je die site niet in komt. Dan kun je de extensie tijdelijk uitschakelen voor die site.
Klinkt als een hoop mogelijke problemen? Ik noem ze, maar ze zijn uiterst zeldzaam.

Privacy Badger ontdekt vaak nog een of meer trackers die aan Firefox zijn ontsnapt. In geval van problemen kun je per boosdoener aangeven wat ie mag: niets, alleen geen cookies, of alles (*Zie figuur 2*).

Figuur 2

Privacy Badger is geen ‘adblocker’. De extension is daarvoor niet ontworpen, maar aangezien veel advertenties worden getoond door derden, die tevens je surfgedrag volgen, worden die als neveneffect geblokkeerd.

Cookiebro gooit alle aanwezige cookies weg zodra we een andere site bezoeken. Opgehoepeld jullie! Maar er zijn soms cookies die je wilt bewaren, zoals van je favoriete zoekmachine, of om gemakkelijker ergens in te loggen. Dan is er de ***whitelist*** (*Zie figuur 3*) en onder ***Options*** kun je het hele gedrag van de extensie tot in detail instellen. Meestal echter, is de standaard OK.



Figuur 3

Canvas Fingerprint Defender is te gebruiken om de meest geavanceerde vorm van fingerprinting tegen te gaan. Fingerprinting is een techniek waarbij informatie die je browser standaard doorgeeft, wordt gebruikt om je systeem vrijwel uniek te identificeren zonder dat tracking cookies nodig zijn. Vrijwel uniek? Ja met behulp van het HTML5-element ***Canvas***. Deze extensie blokkeert dat element niet, maar levert volkomen willekeurige informatie. De tracker wordt dus belazerd! Let op: de bijna gelijknamige extension ***Canvas Defender***, die ik ook heb getest, geeft geen enkele bescherming.

Andere browsers

Ook andere browsers hebben faciliteiten om je privacy te beschermen. Ik laat hier Internet Explorer en Edge buiten beschouwing. Microsoft verstaat onder privacy iets dat meer rekening houdt met de mate waarin de commercie privacy weet te realiseren. De reden dat ik uitga van Firefox, is het feit dat deze browser echt multiplatform is, inclusief de meeste extensies.

Voor wie toch iets anders zoekt:
Chrome, afkomstig uit de omgeving van Google, heeft uiteraard ook iets andere belangen, maar ondersteunt wel dezelfde extensies als genoemd onder Firefox. Helaas ondersteunt de versie voor Android weer helemaal geen extensies, en is naar mijn smaak nog net geen spyware te noemen. Heb je een Android-telefoon, log dan op de pc niet onder Chrome in op je Google-account.

Brave komt van voormalige medeontwerpers van Firefox, met een andere blik op privacy. Ook onder Brave kun je, vanuit de Chrome Wenstore, op de PC dezelfde extensies installeren als onder Firefox. Maar die zijn weer niet beschikbaar onder de mobiele versies van Brave en Chromium. Brave heeft ingebouwde bescherming tegen ‘fingerprinting’ die echter bij test door de mand valt. De mobiele versie synchroniseert alleen de bladwijzers en instellingen met je PC. De ingebouwde ad blocker is gericht tegen advertenties, niet tegen volgen, al is dat in vele gevallen wel de ‘bijvangst’, maar meer ook niet.

Opera is een gevaarlijk ding: het wil standaard toegang tot de webcam hebben, reden waarom ik deze browser verder laat voor wat ie is.

Meer informatie over fingerprinting

Is het nodig of wenselijk maatregelen te nemen tegen fingerprinting? Ik lig er (nog) niet wakker van. Toepassing ervan valt onder de AVG als het wordt gebruikt om je te volgen met het oogmerk je advertenties aan te bieden, gericht op je vermoedelijke belangstelling. Maar het is ook een prima middel om analytische informatie te verzamelen; daar is niets op tegen, mits de gebruiker geïnformeerd is. Maar ja, wie controleert?

De extensies op de browser geven geen waterdichte bescherming. Echte bescherming, als je bang bent voor de AIVD, CIA of NSA, wordt aangeboden tegen stevige prijskaartjes.

Rein de Jong (Rhino) vertelt er ook iets meer over op zijn site:
https://www.reindejong.nl/kort-goed#Browser-tracking
Ook de Consumentenbond geeft daarover begrijpelijke informatie:
https://www.consumentenbond.nl/internet-privacy/browser-fingerprinting
En ten slotte Wikipedia (Engelstalig)
https://en.wikipedia.org/wiki/Device-fingerprint

Test je bescherming tegen Canvas-fingerprinting

Testsite **https://amiunique.org/fp** is even bezig en levert dan zoiets als figuur 4. Probeer niet de tekst in de figuur te lezen, ze dient alleen om de pagina te herkennen die je als antwoord krijgt. Bezoek de site enkele malen achtereen, want de eerste keer geeft geen uitsluitsel. Wis na elk bezoek alle cookies en de cache van de browser, of, als je weet hoe het moet, alleen het cookie van **amiunique.org**.

Figuur 4

Zie ook het eerder beschreven gebruik van de extensie ***Cookiebro***. Het is essentieel dat het cookie steeds wordt gewist! Van belang is alleen de in de figuur rood omlijnde regel. Negeer het resultaat van de eerste poging. Als je bij de tweede of latere poging deze laatste regel krijgt, is de beveiliging voor de test gezakt:

But only 9 browsers out of the 1127489
observed browsers (0.00 %) have exactly
the same fingerprint as yours.

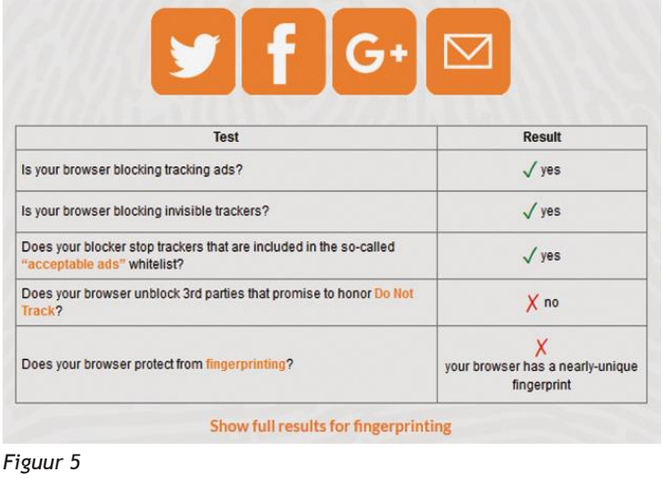
Het cijfer achter het woord ‘only’ is hier gelijk aan het aantal malen dat je de site eerder hebt bezocht. Je bent dus nauwkeurig te traceren. (!)

Bij een goed resultaat zie je in de laatste regel.

However, your full fingerprint is unique
among the 1127505 collected so far.
Want to know why?

Oplettende lezertjes zullen nu weten: die Uphoff is geschift! Deze laatste test is nu juist fout, want die vertelt dat er een unieke vingerafdruk is gevonden. Begrijpelijk, maar als je de site even later opnieuw bezoekt, is je vingerafdruk wederom uniek. Je wordt dus niet herkend doordat de extensie ***Canvas Fingerprint Defender*** telkens een andere 'unieke' nepvingerafdruk retourneert.
Nogmaals, je moet voor elke nieuwe test het cookie wissen, anders wordt de test als 'duplicaat' door de site genegeerd.

Een andere testsite, die genoemd werd op de site van Rein, is **http://bit.ly/r-pano**, die het net even anders doet. De test levert uitvoerige resultaten, waaronder de Canvas-vinger-afdruk. Wat in figuur 5 verschijnt achter ***Does your browser protect from fingerprinting*** is totaal niet relevant terzake van canvas fingerprinting, negeer dat dus, maar klik op de link ***Show full results for fingerprinting*** onderin figuur 5.



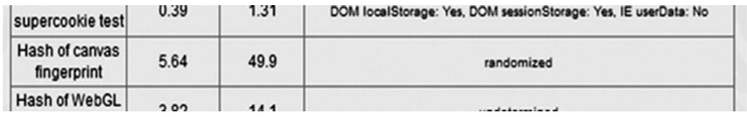
Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a nearly-unique fingerprint

Show full results for fingerprinting

Figuur 5

Daarop verschijnt informatie waarvan het relevante deel te zien is in figuur 6. Daar moet ***Randomized*** verschijnen, of, bij herhaalde tests, telkens een andere waarde. Als de test een fout resultaat geeft, krijg je steeds dezelfde waarde te zien, zoiets als deze:

1c9cbbd36204d05f7a7d2df9ab3cee57



supercookie test	0.39	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	5.64	49.9	randomized
Hash of WebGL	2.82	14.1	

Figuur 6

En geloof mij en vrees het: die is ook na weken nog steeds uniek voor mijn systeem!
Maar is dit nu alles wat er te vertellen valt? Nee, want als we in het voorgaande hebben vastgesteld dat de aangeboden bescherming tegen fingerprinting niet bleek te werken, hebben we niet kunnen testen of de foute test alleen werkte voor pogingen van derden. De eerder genoemde extensie Privacy Badger claimt je te beschermen tegen indirecte (3rd party) technieken, maar vertelt ook dat pogingen je vinger-afdruk te nemen, direct door de site die je bezoekt, niet worden aangepakt. Maar dat is nu juist de gevaarlijkste!

En dan is er de vraag of de de Autoriteit Persoonsgegevens is voorzien van de technisch geavanceerde uitrusting om geboefte op te sporen. Nee dus, want de AP rechercheert niet, maar behandelt klachten. Je moet dus zelf komen met een klacht als: 'Deze stoute site volgt mij via fingerprinting.' Werkt niet hè?

Waarschuwing

Gevaarlijk: **ES File Explorer in Android**

Het was een populaire app op Android. Je kon je netwerk thuis zo ongeveer integreren met je telefoon, inclusief OneDrive. Blader door je hele toko, kopieer, knip en plak van overal naar overal.

Tot het een half jaar terug niet meer mogelijk was te verbinden met OneDrive. Microsoft eiste na installatie een extra verificatie waaraan ES niet ging voldoen. Kort daarop verwijderde Google de app uit de Play Store, omdat in de app een gigantisch veiligheidslek bleek te zitten.

Als je de app nog gebruikt: **Verwijderen!** Niet straks, maar **NU!** Dus ook je betaalde versie! Het ding is echt bloedlink!