



# The GuardXP project: Strengthening cybersecurity through privacy

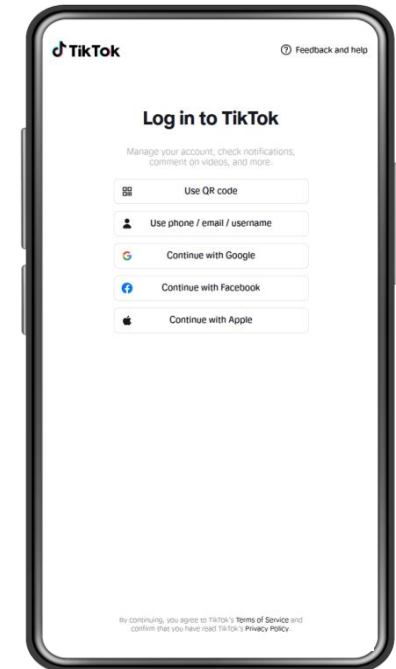
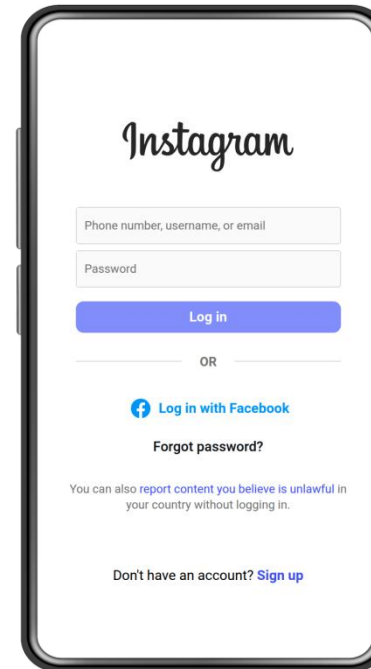
**Pere Barlet-Ros** ([pere.barlet@upc.edu](mailto:pere.barlet@upc.edu))  
Universitat Politècnica de Catalunya (UPC)

23rd SIG-NOC meeting – 14 Oct. 2025

This project is sponsored by Ripe NCC (2024 Community Projects Fund)



# The problem



# Consent managers

The screenshot shows the EL PAÍS consent manager interface. It features a dark background with white text. At the top, it says "EL PAÍS" and "It offers the following browsing modes:". Below this, there are two columns of text. The left column lists several data processing activities, and the right column describes the subscription options. At the bottom, there are two buttons: "ACCEPT AND CONTINUE" and "SUBSCRIBE AND DECLINE".

**EL PAÍS**  
It offers the following browsing modes:

- Storage and access to information,
- Sharing data and profiles for analytics and personalized advertising from advertisers for our advertising campaigns,
- Sharing data and profiles for analytics and personalized advertising from advertisers and advertising agencies on the Internet,
- Precise geolocation data and identification through device analytics.

**Subscribe and decline**  
This option will allow you, among other services, unlimited reading of El País on the website and App, access newsletters with exclusive content, unique cultural experiences and comment on news.

If you decide to subscribe, and in accordance with the preferences you grant, you will be able, for example, browse our website without us, or third parties, being able to track you or show you personalized advertising and content.

**ACCEPT AND CONTINUE** **SUBSCRIBE AND DECLINE**

Legal warning | Cookies policy | Know more

The screenshot shows the Le Monde consent manager interface. It features a dark background with white text. At the top, it says "Le Monde" and "Soutenez un journalisme fiable". Below this, there is a paragraph explaining the benefits of accepting cookies. At the bottom, there are two buttons: "Accepter et continuer" and "S'abonner".

**Soutenez un journalisme fiable**  
Accéder gratuitement en acceptant l'utilisation de cookies.  
L'accès gratuit au site (hors contenus exclusifs abonnés) est subordonné à votre consentement sur l'utilisation des cookies. Vous pouvez retirer votre consentement à tout moment.

...ou s'abonner au Monde pour profiter de tous les contenus.  
L'accès au site avec abonnement vous permet de consulter tous les contenus et archives du Monde depuis notre site et nos applications mobiles. En cliquant sur le bouton « S'abonner », vous pouvez refuser les cookies ou paramétrer vos choix (hors cookies de fonctionnement et de mesure d'audience).

**Accepter et continuer** **S'abonner**

The screenshot shows the Bild consent manager interface. It features a dark background with white text. At the top, it says "Bild" and "Datenschutz und Nutzungserlebnis auf BILD.de". Below this, there are two columns of text. The left column describes the benefits of not using tracking and cookies, and the right column describes the benefits of using tracking and cookies. At the bottom, there are two buttons: "Jetzt BILD Pur abonnieren" and "Alle akzeptieren".

**Ohne Tracking und Cookies\* nutzen**  
Nutzen Sie BILD.de ohne Tracking, Cookies und personalisierte Werbung für 3,99 EUR/Monat (rabattiert für BILDplus-Abonnenten 2,99 EUR/Monat). Informationen zur Datenverarbeitung im BILD Pur-Abo finden Sie in unserer [Datenschutzklärung](#) und in den FAQ.

**Mit Tracking und Cookies nutzen**  
Sie können unser Angebot auch nutzen, ohne einen Vertrag abzuschließen. Wir übermitteln in diesem Fall personenbezogene Daten an bis zu 280 [Datenanbieter](#), die uns helfen, unser Webangebot zu verbessern und zu finanzieren. In diesem Zusammenhang werden auch Nutzungsprofile (u.a. auf Basis von Cookie-IDs) gebildet, mit Daten von anderen Webseiten angereichert und auch außerhalb des EWR verarbeitet. Hierzu übermitteln wir an diese Drittanbieter auch Ihre Privatsphäreinstellungen bzw. Präferenz in Form einer codierten Zeichenfolge (sog. TC-String). Hierfür und um bestimmte Dienste zu nachfolgend aufgeführten Zwecken verwenden zu dürfen, benötigen wir Ihre Einwilligung, indem Sie "Alle akzeptieren" klicken. Sollen Sie bereits BILDplus-Abonnent sind und BILD Pur zusätzlich abonnieren, können Sie auch die BILDplus-Inhalte ohne Tracking und Cookies\* lesen.

**Jetzt BILD Pur abonnieren** **Alle akzeptieren**

# The privacy paradox

## What Do You Typically Do When You See a Pop-Up Asking You To Accept Cookies?



Based on a survey of 1,000 U.S. adults.



# Second-party trackers

**For what purposes my information is used and who uses it?** ✕

This Site uses its own and other entities cookies, in order to access and use your information for the below purposes. If you do not agree with any of these purposes, you may customize your choices below.

We and the companies that collaborate with us will use your information obtained through cookies. To know the collaborating companies that incorporate their cookies on our website, such as advertisers, advertising operators and intermediaries, you can access through the button **See our partners**. You can set your consent preferences separately for each of the mentioned partners.


**Additional information:** You can know the complete information about the use of cookies, their configuration, origin, purposes and rights in our [Cookies Policy](#).

You allow the use of cookies for the following purposes:

+ Storage and access to information	Disagree	Agree
+ Select basic ads	Disagree	Agree
+ Create a personalised ads profile	Disagree	Agree
+ Select personalised ads	Disagree	Agree
+ Create a personalised content profile	Disagree	Agree
+ Select personalised content	Disagree	Agree
+ Measure ad performance	Disagree	Agree
+ Measure content performance	Disagree	Agree
+ Apply market research to generate audience insights	Disagree	Agree
+ Develop and improve products	Disagree	Agree
+ Sharing data and profiles for analysis and personalised advertising from advertisers for our advertising campaigns	Disagree	Agree
+ Actively scan device characteristics for identification	Disagree	Agree
+ Sharing data and profiles for analysis and personalised advertising for advertisers and advertising companies on the Internet.	Disagree	Agree
+ Use precise geolocation data	Disagree	Agree

By giving consent to the purposes above, you also allow this website and its partners to operate the following data processing: Ensure security, prevent fraud, and debug, Link different devices, Match and combine offline data sources, Receive and use automatically-sent device characteristics for identification, and Technically deliver ads or content

[View our partners](#)

PRIVACY MANAGEMENT BY DIDOMI 


Disagree to all **Agree to all**

**Select partners for Prisa** ✕

You can set your consent preferences for every partner listed below individually. Click on a partner name to get more information on what it does, what data it is collecting and how it is using it.

All partners	Block	Authorize
+ 152 Media LLC IAB TCF	Block	Authorize
+ 1Agency IAB TCF	Block	Authorize
+ 1plusX AG IAB TCF	Block	Authorize
+ 2KDirect, Inc. (dba iPromote) IAB TCF	Block	Authorize
+ 33Across IAB TCF	Block	Authorize
+ 3Q GmbH IAB TCF	Block	Authorize
+ 42 Ads GmbH IAB TCF	Block	Authorize
+ 6Sense Insights, Inc. IAB TCF	Block	Authorize
+ 7Hops.com Inc. (ZergNet) IAB TCF	Block	Authorize

+ View user information

PRIVACY MANAGEMENT BY DIDOMI 

**Save**

# Second-party trackers

**For what purposes my information is used and who uses it?** ✕

This Site uses its own and other entities cookies, in order to access and use your information for the below purposes. If you do not agree with any of these purposes, you may customize your choices below.

We and the companies that collaborate with us will use your information obtained through cookies. To know the collaborating companies that incorporate their cookies on our website, such as advertisers, advertising operators and intermediaries, you can access through the button **See our partners**. You can set your consent preferences separately for each of the mentioned partners.


**Additional information:** You can know the complete information about the use of cookies, their configuration, origin, purposes and rights in our [Cookies Policy](#).

You allow the use of cookies for the following purposes:

+ Storage and access to information	Disagree	Agree
+ Select basic ads	Disagree	Agree
+ Create a personalised ads profile	Disagree	Agree
+ Select personalised ads	Disagree	Agree
+ Create a personalised content profile	Disagree	Agree
+ Select personalised content	Disagree	Agree
+ Measure ad performance	Disagree	Agree
+ Measure content performance	Disagree	Agree
+ Apply market research to generate audience insights	Disagree	Agree
+ Develop and improve products	Disagree	Agree
+ Sharing data and profiles for analysis and personalised advertising from advertisers for our advertising campaigns	Disagree	Agree
+ Actively scan device characteristics for identification	Disagree	Agree
+ Sharing data and profiles for analysis and personalised advertising for advertisers and advertising companies on the Internet.	Disagree	Agree
+ Use precise geolocation data	Disagree	Agree

By giving consent to the purposes above, you also allow this website and its partners to operate the following data processing: Ensure security, prevent fraud, and debug, Link different devices, Match and combine offline data sources, Receive and use automatically-sent device characteristics for identification, and Technically deliver ads or content

[View our partners](#)

PRIVACY MANAGEMENT BY DIDOMI 


Disagree to all **Agree to all**

**Select partners for Prisa** ✕

You can set your consent preferences for every partner listed below individually. Click on a partner name to get more information on what it does, what data it is collecting and how it is using it.

All partners	Block	Authorize
+ 152 Media LLC IAB TCF	Block	Authorize
+ 1Agency IAB TCF	Block	Authorize
+ 1plusX AG IAB TCF	Block	Authorize
+ 2KDirect, Inc. (dba iPromote) IAB TCF	Block	Authorize
+ 33Across IAB TCF	Block	Authorize
+ 3Q GmbH IAB TCF	Block	Authorize
+ 42 Ads GmbH IAB TCF	Block	Authorize
+ 6Sense Insights, Inc. IAB TCF	Block	Authorize
+ 7Hops.com Inc. (ZergNet) IAB TCF	Block	Authorize

+ View user information

PRIVACY MANAGEMENT BY DIDOMI 

**Save**

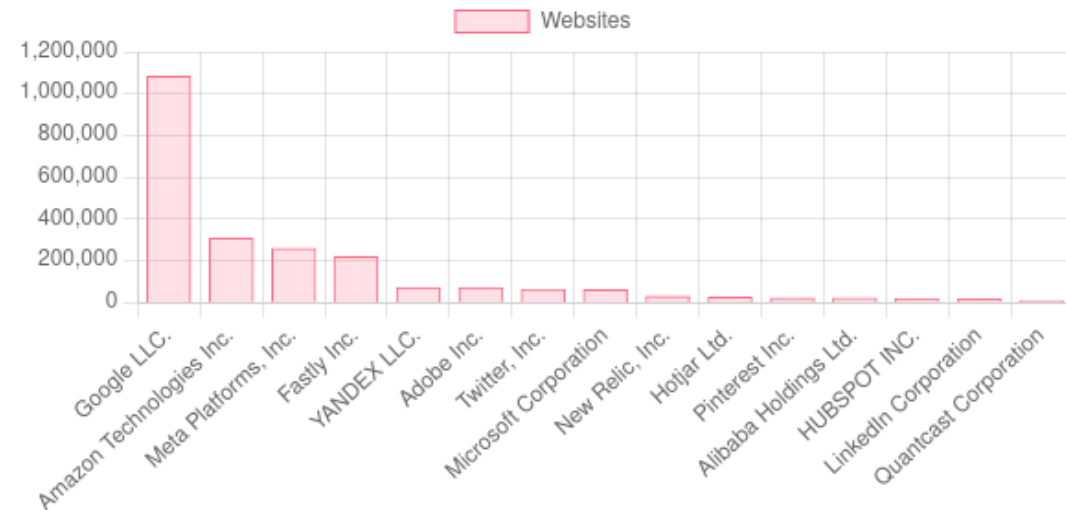
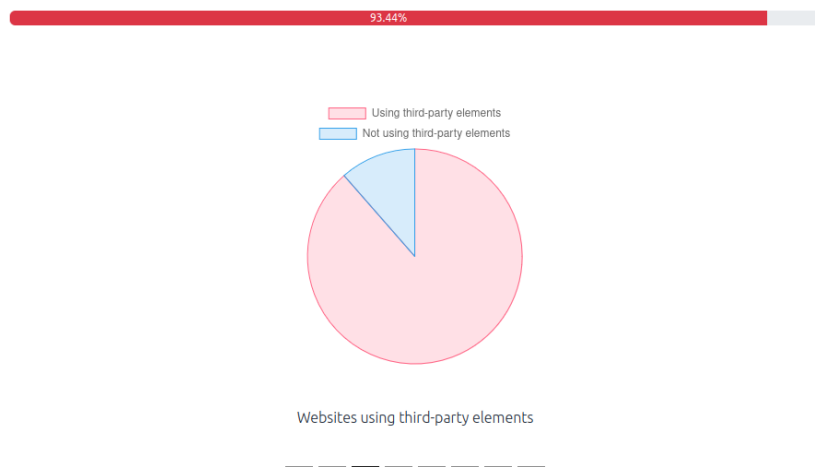
943 “partners”



# User tracking

- Trackers are present in >90% of the websites
- They can easily recover our *browsing history* (at least)
- They can track us even if we delete cookies, use private mode, DNT, VPN, etc.

Percentage of domains using web tracking



# Why should we care about that?

- Data brokers: Companies whose primary source of revenue is selling user personal information in data market places [1]
- Dangers for the user
  - Profiles may be (most surely) incorrect
  - There is no easy way to discover and correct it (despite GDPR)
  - There is no easy way to know to whom our info was sold to [2,3]
  - There is no easy way to know how this is impacting us!!

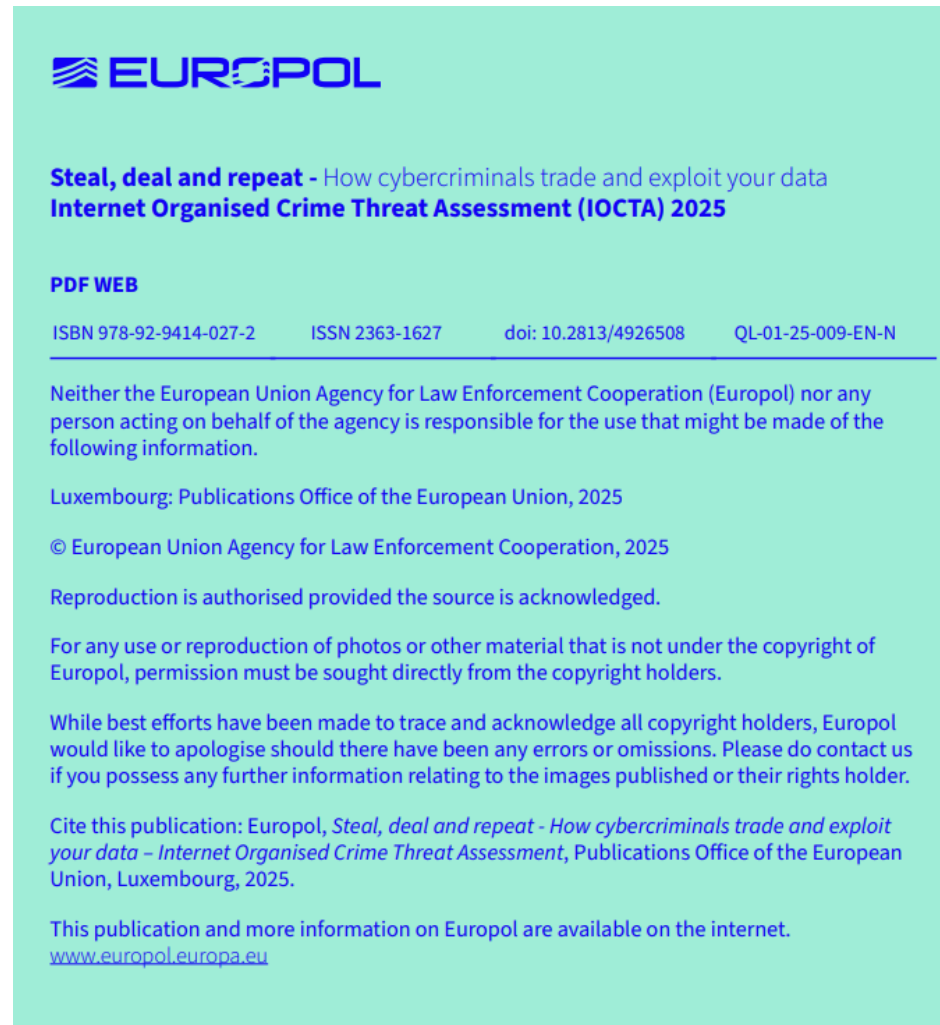


[1] A. Rieke, H. Yu, D. Robinson, and J. van Hoboken, "Data Brokers in an Open Society", Open Society Foundations 2016

[2] <https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/>

[3] <https://techcrunch.com/2023/05/21/the-government-cant-seize-your-data-but-it-can-buy-it/>

# Security implications



## Key findings

Personal data is bought and leveraged by cybercriminals to orchestrate attacks, including phishing and ransomware

LLM and generative AI are effectively used by cybercriminals to increase CTR, and to automate and scale up processes

# Adblockers

- Most popular protection methods
  - Block URLs using pattern lists
  - Difficult to maintain updated and block new methods
  - Easy to evade by periodically changing the hosting domains
  - Adblockers are *too* conservative
- Why are they conservative?
  - “Users want protection that does not break websites” [4]
  - “When extensions break websites, users disable them based on how important the content they are accessing is to them” [5]
- Usually do not block URLs that can impact the website functionality



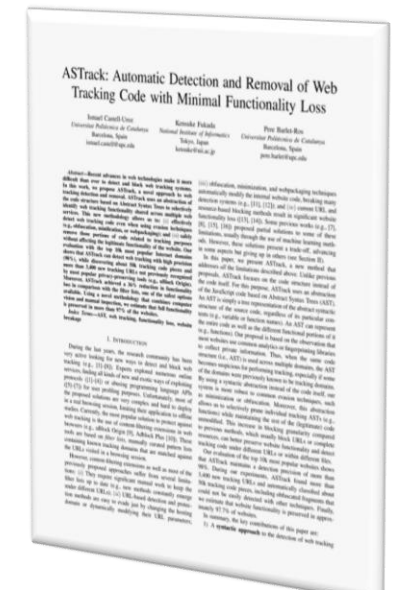
[4] C. E. Wills and D. C. Uzunoglu, “What Ad Blockers Are (and Are Not) Doing,” HotWeb, 2016

[5] G. Merzdovnik, M. Huber, D. Buhov, N. Nikiforakis, S. Neuner, M. Schmiedecker, and E. Weippl, “Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools,” EuroS&P, 2017

# GuardXP

- GuardXP addresses the two main problems of AdBlockers
  - Limitations of blacklists (hard to maintain and easy to evade)
  - Functionality loss (block less than they should)

- GuardXP is based on two previous works:
  - TrackSign: For discovering new tracking methods (INFOCOM 2021) [6]
  - ATrack: For selectively blocking tracking code (INFOCOM 2023) [7]

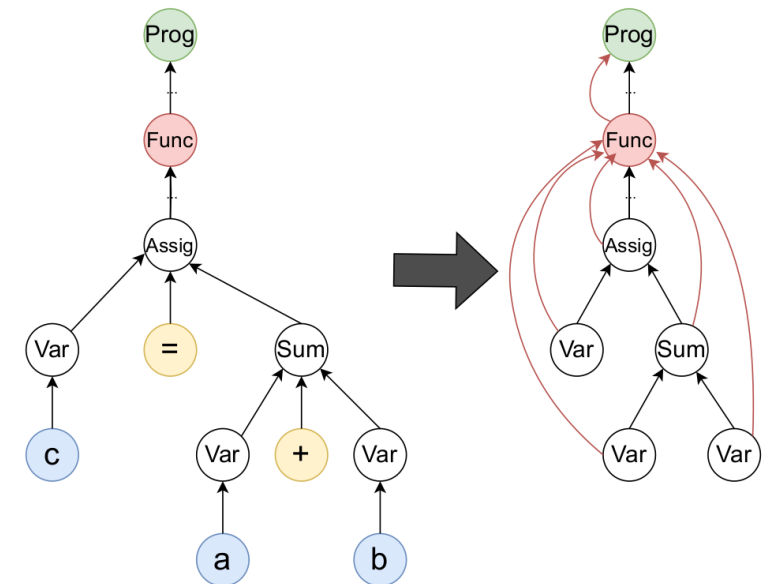


[6] TrackSign: Guided Web Tracking Discovery: <https://personals.ac.upc.edu/pbarlet/papers/TrackSign.Infocom2021.pdf>

[7] ATrack: Automatic Detection and Removal of Web Tracking Code with Minimal Functionality Loss: <https://arxiv.org/pdf/2301.10895.pdf>

# GuardXP technology

- Automatically detect *unknown* web trackers
  - Known trackers under unknown URLs
  - Completely new tracking methods
- Analyze website code instead of URLs
  - Popularity: #resources that use this piece of code
  - Dirtiness: %resources known to perform tracking
- Focus on code structure rather than code content
  - More robust against obfuscation and minification
  - Selectively block tracking AST to better preserve functionality



# Project objectives and status

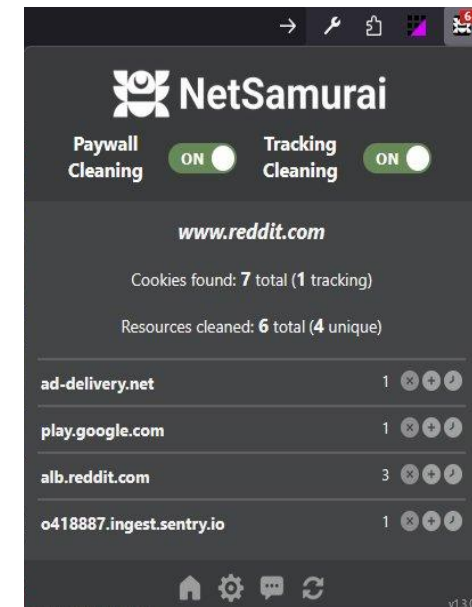
- Integrate TrackSign + ATrack into actual tools that can be used by individual users and companies to protect their privacy and security (GuardXP)

## 1) NetSamurai Plugin

- Cleans tracking code from user browser activity
- Main challenges: Online operation + Browser limitations
- Firefox-based browsers




<https://addons.mozilla.org/en-US/firefox/addon/netsamurai>



# Project status

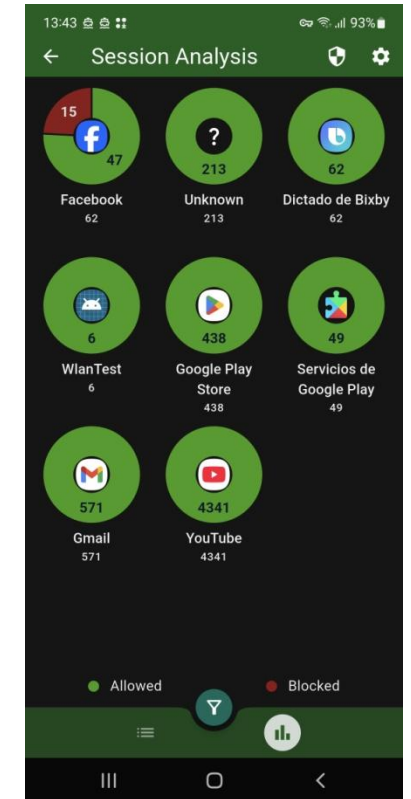
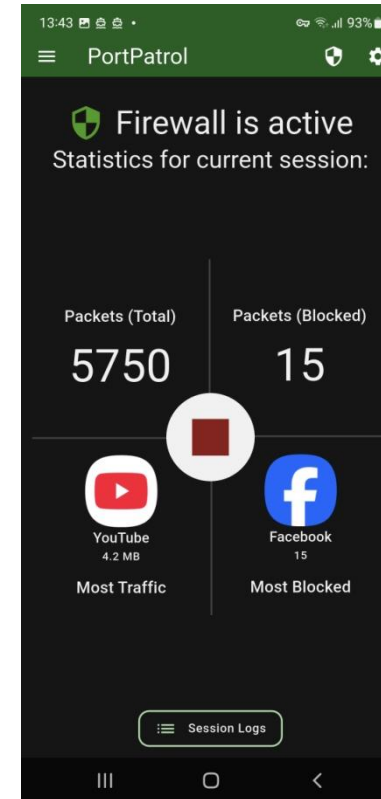
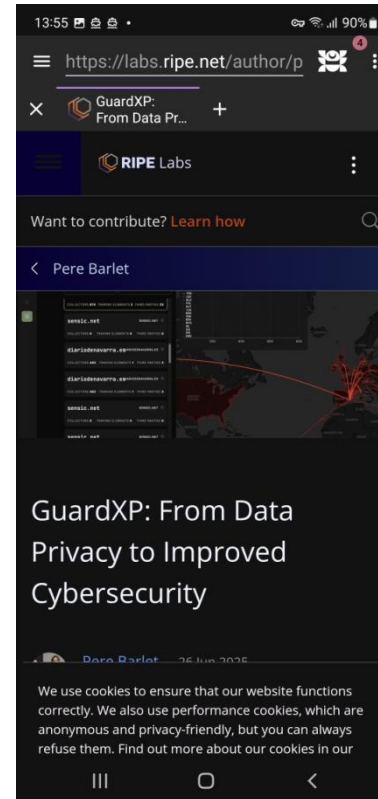
## 2) NetSamurai Browser

- GuardXP protection for Android
- Available at Play Store

 <https://play.google.com/store/apps/details?id=com.ikusa.netsamurai>

## 3) NetSamurai Firewall

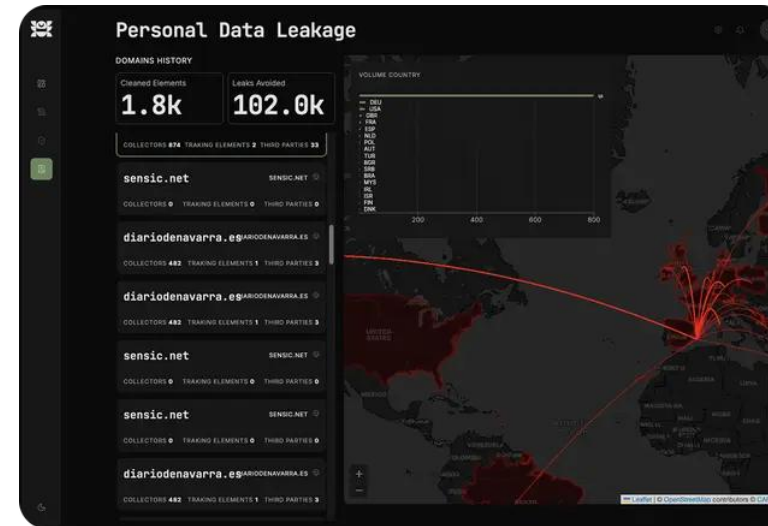
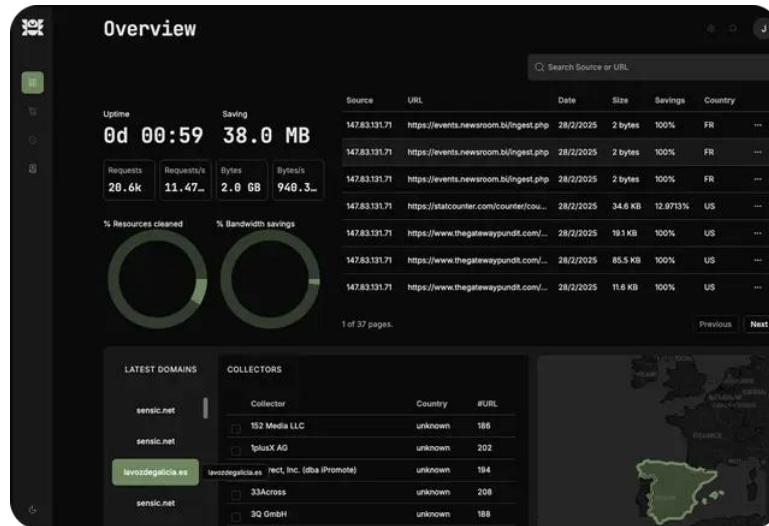
- Protection for mobile apps
- Blocks privacy-invasive connections
- Currently under development



# Project status

## 4) Net Samurai Proxy

- Clean tracking code from company's web traffic by intercepting all web connections
- Main challenges: Online operation + SSL / HTTPS
- Offered as cloud-based SaaS or on-premise





# The GuardXP project: Strengthening cybersecurity through privacy



 **RIPE Labs post:** <https://labs.ripe.net/author/pbarlet/guardxp-from-data-privacy-to-improved-cybersecurity>

 **Plugin:** <https://addons.mozilla.org/en-US/firefox/addon/netsamurai>

 **Browser:** <https://play.google.com/store/apps/details?id=com.ikusa.netsamurai>

**Proxy and firewall:** Coming soon!

This project is sponsored by Ripe NCC (2024 Community Projects Fund)

