ANTI-BOTS AND TROLLS SHIELD
BASED ON CROSS-PLATFORM INTERNET TRAFFIC ANALYSIS

Main goal:

Public Digital Infrastructure, Political Parties, and NGOs are obvious and very often a vulnerable target for mass attacks of automated bots and trolls. All across the world democracies evaluate and respond to this vulnerability.

In unprecedented step, as of 2018 all EU institutions have been preparing against disinformation on many fronts. **ABTSHIELD** fills the technological gap that by now has not been filled by anyone else. It offers real time protection against machines – not users – which are used to distribute and falsely amplifies messages that destroy our democracies.

Apply for funding – if you are an NGO and our team will decide to support you or match you with potential sponsors for implementing this protection. Contact us regarding solutions for governmental and political parties.

Given the dispersed nature of comparatively long duration of the European Parliament elections,
they present a tempting target for malicious actors.
Everyone needs to take responsibility for this – a system is only as secure as the weakest link in the chain.

Julien King, European Commissioner for Security

Why join?

Every modern, opinion-forming public institution has to prepare for influences and manipulations caused by third parties.
A political party or NGO can now be easily deprived of voice by exhausting its campaign budget by malicious attacks.
Recipients of social communication can easily be manipulated by an artificial crowd of trolls that will affect their attitudes.
We do not want to let this happen and that is why we have launched a non-profit organisation support program.

- High-quality audit of websites and online campaigns for a fraction of price for public institutions (NGOs, political parties, non-profit foundations)
- Detection and capability to block malicious traffic
- Analytics fundamental to reaching “living audience”
- Cooperation with security centres and authorities, allowing for undertaking all necessary steps related to the identification and legal management of attacks
- Tracking machines’ behaviour, not users
- ABTShield identification lasts longer than cookies-based
- Aggregated data can be used in developing next generation public tools built in national cybersecurity system
- Data available to researchers – our project is perfectly compatible with R&D and primary research efforts

Why ABTShield is the best solution?

ABTSHIELD learns patterns and tracks bots and trolls behaviour on the basis of analysis of a high volume of internet traffic.

ABTSHIELD uses advanced and scalable device tracking methodology. The technology is based on a unique method for the identification and tagging of incoming internet traffic through analysis of the deep layers of TCP/IP stack. Various activities of individual users' "machines" (computers, laptops, smartphones) operating on websites are being integrated into one central "instance"/service.

ABTSHIELD identifies bot or troll-infected users' devices regardless of the hardware and regardless of the operating system.

ABTSHIELD is a lightning-fast AI-based firewall. Connection sources tied to organised disinformation attacks show characteristics different from the behaviour of an average user. AI models and optimised heuristics then score in order to block or alert the session as desired. ABTSHIELD returns data ina fraction of a second, which makes it possible to take proper action.

ABTSHIELD API allows for building your own decision models based on the ABTSHIELD mechanism.

ABTSHIELD provides reporting for analysed traffic and threats via a web-based tool. Attacks may easily be filtered for view by time and risk score. They can be further grouped by country, IP, user, and customer-defined parameters.

ABTSHIELD is designed for high scalability and frictionless integration. Integration involves placing an HTML tag referring to the ABTSHIELD system and handling the data it returns.

ABTSHIELD has a neutral impact on the user experience. The system is provided as a service discrete from a customer's own delivery infrastructure and therefore doesn't affect site performance. It is fully compatible with CDNs and cloud services at any scale, as well as customer-managed equipment.

Project partners:

Google AGORA SA VISEGRAD INSIGHT ringier axel springer VOX europ

The project is supported by the Google Digital News Initiative

DIGITAL NEWS INITIATIVE

Google