Privacy Policy

Shoelace

Title of application/study

Shoelace

Policy start date

01-09-2018

Purpose of application/study

Within .nl, we have detected numerous fake webshops: websites designed to mislead users by pretending to sell legitimate products at low prices. People who use fake websites are liable to be defrauded and have their identities stolen.

In partnership with Delft University of Technology, we have therefore started the Shoelace Project to detect fake webshops. The project is intended to map the whole ecosystem associated with fake webshops. That implies establishing which registrars, hosting service providers and e-mail service providers are involved, and revealing any other patterns that could help us identify the various actors.

Our hypothesis is that fewer than five actors are responsible for more than a thousand fake webshops.

The study can help to boost the efficiency of the investigative agencies' efforts to tackle fake webshops.

Date
1 September 2018

Classification
Public

Page
2/3

Personal data

The project will make use of DMAP data.

The DMAP data in question will include the following personal data:

- Tabulated crawl_result_dns data (to be anonymised)
    1. dns_ns (list of name servers – IP addresses)

- Tabulated crawl_result_http data (the following data will not be shared)
    - bus_coc_no: Chamber of Commerce registration number
    - numberbus_vat_no: VAT registration number
    - bus_bank_no: bank account number
    - bus_bic_no: BIC number
    - bus_phone_no: phone number
    - bus_address: visiting or postal address

- Tabulated crawl_result_smtp data:
    - smtp_hots: mail server details, including IP addresses
    - smtpHostIPs.ip (address, to be anonymised)
    - smtpHostIPs.banner (welcome message received from server, not to be shared)

Legitimate basis

Reasonable interest

Filters

Within SIDN, the complete DMAP dataset will be processed, but only certain items of data will be extracted and made available to TU Delft.

None of the personal data referred to above will be shared. Only the following data will be shared:

- dns_ns : DNS server IP addresses (to be anonymised)
- smtpHostIPs.ip (address, to be anonymised)

Retention

1 year (duration of the project).

Access

Access to the data will be restricted to SIDN Labs staff. Access will be by means of strong user name-password combinations or public/private keys. The relevant SIDN Labs personnel have received detailed guidance on the importance of privacy.

The data is to be stored on a virtual server and two-way data traffic between SIDN Labs users and the server will be encrypted.

Publication/sharing	The filtered data will be shared with a PhD student and an Assistant Professor at Delft University of Technology (Faculty of EWI).
Type	Research
Other security measures	N/a