



Privacy Policy Evaluation

University of Amsterdam malware detection

Date	Classification	Page	Contact
31 January 2016	Public	1/4	T +31 26 352 5500 support@sidn.nl www.sidn.nl
	Author		Office
	SIDN Privacy Board		Meander 501 6825 MD Arnhem The Netherlands
			Postal address
			Postbus 5022 6802 EA Arnhem The Netherlands

Policy

Title of policy	Graph theory study for DNS malware detection
Policy start date	31-01-2016
Date of evaluation	31-01-2016

Purpose limitation

Data Protection Act applicable?	Will any personal data be processed? Will personal data be processed on an automated or semi-automated basis, or will personal data contained in a file be processed manually? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---------------------------------	---

Yes, the submitted form states that the following personal data is to be processed:

*IP addresses (of resolvers and other systems that send DNS queries to our server).
The 'raw' address data will not be used for the study; it will be processed to generate an anonymised dataset for use by the researcher.*

Purpose	The purpose must be specific, explicitly defined and legitimate. Is the purpose specific, explicitly defined and legitimate? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No, insofar as
---------	---

The submitted form states that the research has the following purposes:



Tackling botnet infections by identifying domain names addressed by botnet clients.

The purpose is specific, explicitly defined and legitimate.

Legitimate basis

The evaluation must address the proportionality and subsidiarity of the processing (i.e. whether the interest served by processing is important enough to justify any resulting loss of privacy, and whether the purpose could be served by any other, less intrusive means).

Is the legitimate basis clear?

- Yes
 No

The legitimate basis given for processing in the policy is reasonable interest.

Reasonable interest is indeed the appropriate legitimate basis (the other legitimate bases referred to in the Data Protection Act are not applicable).

See the Purpose section for details of the reasonable interests served. The research does not significantly compromise the privacy of the users of the processed IP addresses. Furthermore, the research is partly in the interests of the address-holders themselves.

Safeguards and control measures

Purpose limitation

Are there adequate safeguards to ensure that personal data is not used for purposes other than that for which it was obtained?

- Yes
 No

The submitted form states that the personal data is to be anonymised before being shared with the researcher.

Retention period

Is personal data retained for any longer than necessary for the defined purpose?

- Yes, data is retained for longer than necessary; corrective measures required.
 No

The submitted form states that the data will be retained only for the duration of the study, i.e. for thirty days.

Data set limitation

Is the entire data set necessary for the defined purpose, or could a more limited data set be used?



- Yes
 No; corrective measures required.

The submitted form states that the IP addresses are to be pseudonymised, and that the pseudonymisation key will then be deleted.

The Privacy Board therefore considers that the dataset is to be appropriately limited.

Data reliability

What is done to ensure that the gathered data is accurate?

The processed data is to be gathered (without third-party involvement) by our own systems in the context of normal operational activities (handling DNS queries).

Data processors

Who processes the data? Who else has access to the data?

The submitted form states that personnel of SIDN (the data controller) will have access to the server on which the data is stored, and explains how that access will be limited.

The anonymised data will be made available to a researcher from the University of Amsterdam, with which SIDN has a data sharing agreement.

Data security

How is the data protected against loss and unauthorised processing?

The data is to be processed in-house on a secure system, and the personnel with access to that system have received appropriate instruction.

The shared data will have been anonymised.

Other

Special personal data

Is any special personal data processed?

- Yes
 No

Inclusion in register

Is the processing recorded in the Processing Register?

- Yes
 No

Processing is covered by the declaration for ENTRADA.

Subjects' rights

If the personal data is not obtained from the subjects, but by other means, is the origin recorded?



Date
31 January 2016

Classification
Public

Page
4/4

- Yes
- No

The submitted form states that the processed data will consist of the IP addresses of all systems that send DNS queries to SIDN's name servers.

The data is therefore to be obtained by other means, and the origin is to be recorded.

Retention within EU

Is any data transferred to a country outside the EU?

- Yes
- No

If 'Yes', advice is required from the Privacy Board.

The submitted form states that the data will be shared in anonymised form with a researcher from the University of Amsterdam.

No data is to be transferred to a country outside the EU.

Conclusion

Evaluation

What is the conclusion of the Privacy Board's evaluation?

The Privacy Board believes that the policy satisfies all applicable statutory and internal requirements.