Privacy Policy

Resolver Reputation 1.0

Date
17 March 2015

Classification
Public

Author
SIDN Labs

Page
1/2

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Title of application/study	Resolver Reputation 1.0
Policy start date	2015-03-17
Purpose of application/study	To increase the security and reliability of .nl (and the internet in general) by conducting research into the assignment of reputations to resolvers. The reputation assignments can then be used to tackle various forms of abuse. Specifically, the intention is to improve the capability to act against 'spambots' (botnet clients that send spam). Spambots are detected by the system on the basis of certain characteristics of their DNS behaviour; their IP addresses are then shared with the Abuse Information Exchange for further processing. That processing entails communication of each IP address to the relevant ISP, who can take appropriate action where warranted. The ultimate goal of the activities that are relevant to this policy is to reduce the number of PCs in the Netherlands that are infected with spambot malware.
Personal data	IPv4 and IPv6 addresses of all systems that send DNS queries relating to .nl domains. Also the timings of the most recent DNS queries.
Legitimate basis	The legitimate basis for processing is a reasonable interest.
Filters	IP addresses that have not been associated with any recent activity ('recent' currently implying 'in the last month') are deleted from the database.

	The query data itself is not relevant in the current version of ResRep and is therefore excluded from processing. Analysis is confined to meta-data (whether an MX record is requested, whether the RD bit is set, whether numerous NX domains are involved, etc).
Retention	In the current version of ResRep, an IP address is retained for as long as it continues to feature in traffic to ns1.dns.nl. Once an address has not featured for a period, it is automatically deleted from the database.
Access	All SIDN Labs staff have access. The data is currently held on a server, access to which is controlled on the basis of two-factor authentication (TOTP for SSH and client certificates for web, plus a user name-password combination).
Publication/sharing	IP addresses that display behavioural characteristics associated with spambot malware infection are automatically reported to the AbuseHUB at thirty-minute intervals. Each report includes the timestamp of the last instance of suspicious behaviour associated with the IP address in question within the thirty-minute interval. All other data relating to the IP address is omitted from the report and therefore not shared with the AbuseHUB. Sharing with the AbuseHUB is subject to the condition that an agreement is in place between SIDN and the AbuseHUB, the content of which corresponds to a processing agreement. The AbuseHUB is based in the Netherlands.
Type	Production
Other security measures	None