Privacy Policy

Sinkhole

Date
28 May 2021

Classification
Public

Author
SIDN Labs

Page
1/3

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Title of application/study	Botnet research
Policy start date	28 May 2021
Purpose of application/study	The study involves setting up a sinkhole to gather data on the behaviour of botnet clients. A botnet is a network of malware-infected home computer equipment and servers, known as botnet clients. The clients are controlled by a so-called 'botnet shepherd'. The shepherd can give instructions to the bots in the network. So, for example, bots may be instructed to do anything from gathering private data (spying) to participating in a DDoS attack (offensive behaviour). Such activities have adverse implications, both for the owners and/or users of the infected clients and for the targets of the offensive behaviour. The clients in a botnet periodically make contact with a central 'command and control' server, to get instructions from the shepherd or to upload stolen data, for example. The central server needs to have a domain name and, by analysing DNS query data, it is sometimes possible to identify a .nl domain name intended for use with a botnet server, before it is even registered. Having identified such a domain name, the SIDN Labs team intends to register the name and set up a

sinkhole in order to monitor and log the botnet clients that make contact.

The set-up would also enable the identification of any resolver bugs that could cause operational problems and be vulnerable to abuse.

Personal data

The following items of data would be recorded for each botnet client:

- Time
- Domain name
- IP address
- Country (linked to IP address)
- AS number (linked to IP address)

Legitimate basis

The detection and removal of botnet infections are in the interest of infected computer owners, who are liable to be targeted by spyware and whose machines can be used in DDoS attacks.

Detection and removal also serve the public interest, since botnets can be used to render servers on the internet unreachable by means of DDoS attacks.

Hence, botnet infections impact negatively on internet users whose own machines are not infected.

The identification of resolver bugs supports the minimisation of DDoS attack-based abuses and contributes to internet security.

Filters

None

Retention

The data will be retained for no more than eighteen months.

Retention for that period is necessary to observe whether and, if so, how infections diminish over time. For example, it might be possible to observe geographical differences in the infection rate decline (e.g. between Asia and USA).

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.

Publication/sharing	No raw data will be shared or published. Only aggregated statistical data will be published, on stats.sidnlabs.nl and in academic papers.
Type	Research and development
Other security measures	None