Privacy Policy

University of Amsterdam Malware Detection

Date	Classification	Page	Contact
11 December 2015	Public	1/2	T +31 26 352 5500 support@sidn.nl www.sidn.nl
	Author SIDN Labs		

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Title of application/study

Graph theory study for DNS malware detection

Policy start date

31-01-2016

Purpose of application/study

A botnet consists of a group of home computers that have been infected with malware and are under the control of a '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/users of the infected computers 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.

A researcher from the University of Amsterdam will attempt to use graph theory to identify previously unknown malware domain names.

Personal data

The original dataset will include the IP addresses of resolvers. The addresses will be anonymised by an SIDN Labs staff member before being forwarded to the researcher. The data ultimately used for the study will not include personal data.

Legitimate basis

The detection and removal of malware 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, malware infections impact negatively on internet users whose own machines are not infected.

Filters

The resolver IP addresses will be anonymised using a salted SHA-2 hash. The salt will be secret and will be deleted following anonymisation.

Retention

The data will be used for the duration of the study (thirty days) and then deleted.

Access

Access to the data will be restricted to SIDN Labs staff and the researcher from the University of Amsterdam. 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

The data will be shared with the researcher from the University of Amsterdam.

The data to be shared will be one day's DNS query data, consisting of the following items:

- Resolver IP address (anonymised)
- .nl name server IP address
- The domain name in question
- Time

SIDN has a Data Sharing Agreement with the University of Amsterdam.

Type

Research

Other security measures

Data exchange between SIDN and the University of Amsterdam will be by means of e-mail/encrypted downloading.