Privacy Policy

Joint Threat Intelligence Enrichment

Date
01 August 2017

Classification
Public

Author
SIDN Labs

Page
1/3

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	Joint Threat Intelligence Enrichment (JTIE)
Policy start date	01-08-2017
Purpose of application/study	The purpose of JTIE is to develop a mechanism for combining the threat intelligence relating to .nl domain names that is held by Fraudehelpdesk (FHD) and SIDN, thus enabling both parties to classify domain names as suspect with a greater degree of accuracy. The ultimate aim of the work is to make the internet more secure. The system involves FHD sending SIDN lists of .nl domain names used in e-mails reported by FHD users. SIDN responds by sending FHD the following data regarding each listed domain name: number of DNS queries in the last seven days, registration date and registrar pseudonym. FHD is no longer told whether the registrant is Dutch (yes/no). Furthermore, FHD now sends SIDN a list of URLs for .nl domain names, rather than a list of second-level domain names only. After performing its evaluation, FHD sends SIDN feedback indicating whether an e-mail has been classified as malicious. FHD makes its classification using the data provided by SIDN and other data.
Personal data	SIDN processes the following personal data relating to each domain name: Number of DNS queries in the last seven days, registrar's name, domain names associated with URLs in the suspect email. To do that, SIDN has to process DNS queries, which include IP addresses. Registrar pseudonyms are relevant because malicious domain names are often registered through registrars that are

	associated with a high level of malicious registrations. Any URLs that contain personal data are anonymised by FHD before being shared with SIDN.
Legitimate basis	The legitimate basis for processing is a reasonable interest. It is known from earlier research that a surge in DNS queries is a sign of possible domain name abuse. The registration date is relevant for distinguishing between malicious domain name registration and the hacking of established websites. URLs are useful for identifying phishes associated with old and probably hacked domain names.
Filters	Because only the absolute number of DNS queries is relevant, the IP addresses are removed from the DNS query data and not therefore processed. SIDN processes the name of the registrar, but shares only the associated pseudonym with FHD. As far as possible, FHD removes any personal data from the URLs shared with SIDN.
Retention	Domain names associated with malicious behaviour are recorded indefinitely. That facilitates future study of the domain names, and thus the ongoing refinement of detection methods. In the context of future research, the processed information will no longer include any personal data.
Access	The information is accessible by the SIDN Labs team and by SIDN managers. The access arrangements comply with the requirements set out in the general ENTRADA policy.
Publication/sharing	SIDN shares information with Fraudehelpdesk, a private foundation based in the Netherlands. The following data is shared: Number of queries per domain name (excluding source data), registration date, registrar pseudonym. SIDN has a Data Sharing Agreement with FHD. If a domain name is identified with a very high degree of probability as being used for phishing, but has not been taken down by a registrar, hoster or other party, we share the domain name with relevant stakeholders using the Netcraft tool. The information thus shared does not include any personal data. The process forms part of SIDN's takedown procedure.
Type	Production

Other security measures

An encrypted connection is used for the exchange of information between SIDN and FHD. No third party has access to the connection.