Privacy Policy

COMAR

Date	Classification	Page
09 July 2020	Public	1/2
	Author	
	SIDN Labs	

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

Classification of Compromised versus Maliciously Registered Domains (COMAR)

Policy start date

09-07-2020

Purpose of application/study

COMAR is a joint research project by a consortium formed by SIDN Labs, AFNIC Labs, and Grenoble Alps University. The Franco-Dutch project addresses the problem of automatically distinguishing between domain names registered by cybercriminals for the purpose of malicious activities, and domain names exploited through vulnerable web applications. The project is designed to help intermediaries such as registrars and ccTLD registries further optimize their anti-abuse processes.

The present privacy policy is intended to support development and evaluation of the classifier developed within the COMAR project.

Personal data

SIDN provides Grenoble INP with reports of abusive domain names within the .nl-zone. This includes the domain name itself, metadata about the abuse report (timestamp, channel were the report was published, type of abuse, URL if available) and metadata about the registration (creation timestamp, last update timestamp, registrar).

SIDN does not share personal data about the registrant. The domain name and URL may, however, contain a reference to the registrant and/or other personal data. Also the name of the registrar could contain personal data.

In return, Grenoble INP provides SIDN with an assessment of whether an abusive domain name has probably been registered with malicious intent or has been compromised. In addition to this assessment SIDN will receive a confidence interval and a motivation for the assessment (e.g., which features contributed to the assessment).

Legitimate basis

Sharing examples of abuse reports helps us to develop and evaluate a classifier that could help registrars and ccTLD registries further optimize their anti-abuse processes. In this way it contributes to the stability of the internet and critical services that make use of it.

Filters

n/a

Retention

Grenoble INP will delete the shared abuse reports and all associated data no later than 12 months after the project has ended.

Access

Data is exchanged using a webserver that exposes a RESTful API. All communication between the server and client is encrypted using TLS. The API is secured using a password such that only authorized researchers of SIDN and Grenoble INP can access it.

Publication/sharing

Only authorized researchers of Grenoble INP can access the shared data.

We will sign a data sharing agreement with Grenoble INP, before we provide any data.

None of the parties are located outside the European Union.

Type

R&D research

Other security measures

n/a