Sources of Abuse Contact Information for Abuse Handlers

Authors: L. Aaron Kaplan, Mirjam Kühne, Christian Teuschel
Document ID: ripe-658
Date: February 2016

Table of Contents:

1. Abstract

This document aims to describe the different datasets listing abuse contacts and computer emergency response teams (CERTs). The goal is to provide an overview of available datasets together with a description of the quality of the data, access restrictions and potential known issues.

This is likely not a complete list. If you are aware of additional useful data sources, please contact the authors.

2. Terminology

Term	Explanation
Abuse Handler	General role of a person or institution dealing with abuse cases.
ASN	Autonomous System Number (see RFC 1771, RFC 4893)

Term	Explanation
BGP	Border Gateway Protocol (see RFC 4271)
CERT	Computer Emergency Response Team. Synonymous with CSIRT
Constituency	In this context, this refers to the constituency/community (group of people, networks, ASNs, etc.) that a CERT is responsible for
CSIRT	Computer Security Incident Response Team, equivalent to “CERT”
FIRST	Forum for Incident Response and Security Teams (http://www.first.org)
LIR	Local Internet Registry. See (1) for more details
Object	In this context, it refers to a RIPE Database object: Objects contain a piece of information relating to an Internet resource or a supporting or administrative function. See (2) for more details
Resource	Or Internet resource: An ASN, IP address, IP prefix, domain name or hostname
Registrant	A person registering a domain name for individual or business usage
Registrar	Often called domain registrar. An organisation handling the registration of domain names on behalf of a registrant
RIPE NCC	The RIR serving Europe, the Middle East and parts of Central Asia. See (3)
RIR	Regional Internet Registry. See (1) for more details
RIS	Routing Information Service
TI	Trusted Introducer

Table: Terminology

(1) https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system
(2) https://apps.db.ripe.net/docs/03.RIPE-Database-Structure/01-Database-Object.html#database-objects
(3) https://www.ripe.net

3. Intended Audience

This document is targeted towards CERTs and abuse handlers as well as professionals working on automating IT security incident handling.

4. Problem Statement

CERTs and other abuse handlers need to look up contact information frequently for different resources on the Internet. Examples of such lookups might be:

- Given the IP address 1.2.3.4, give me the best matching abuse contact email address.
- Given the domain www.example.com, what is the best contact for sending IT security incident notifications to?

There are a number of ways to look up contact information for abuse reporting:

- Name-based Whois services for looking up domain name related contacts
- Number-based Whois services for looking up IP or ASN related contacts (sometimes combined with domain related information)
- The Registration Data Access Protocol (RDAP) as developed by the IETF as a successor for Whois.

Each lookup mechanism has its own issues to find high-quality contact information. Some of them are listed below.

- Information registered in Whois databases becomes outdated
- Different services use different API and output formats
- Contacts for abuse reporting can be unresponsive or invalid
- Most RIR Whois services have limitations on the amount of retrievable information (especially personal information, which contact information could consist of)
- APIs and output formats are not necessarily consistent among RIRs

This document is intended to document existing data sources for abuse handlers. As a next step we would like to define a standard API for abuse contact lookups.

5. Ways to Look Up Abuse Contacts

Finding the right abuse contact for a name-based or number-based resource can be tricky. Figure 1 shows potential lookups in different datasets. Please note that a name-based resource (domain name, hostname) can be mapped to IP addresses easily. For a name-based resource, you can always find the host, server or ASN on which a domain name or hostname is operating. However, the reverse direction might not always be feasible or useful.

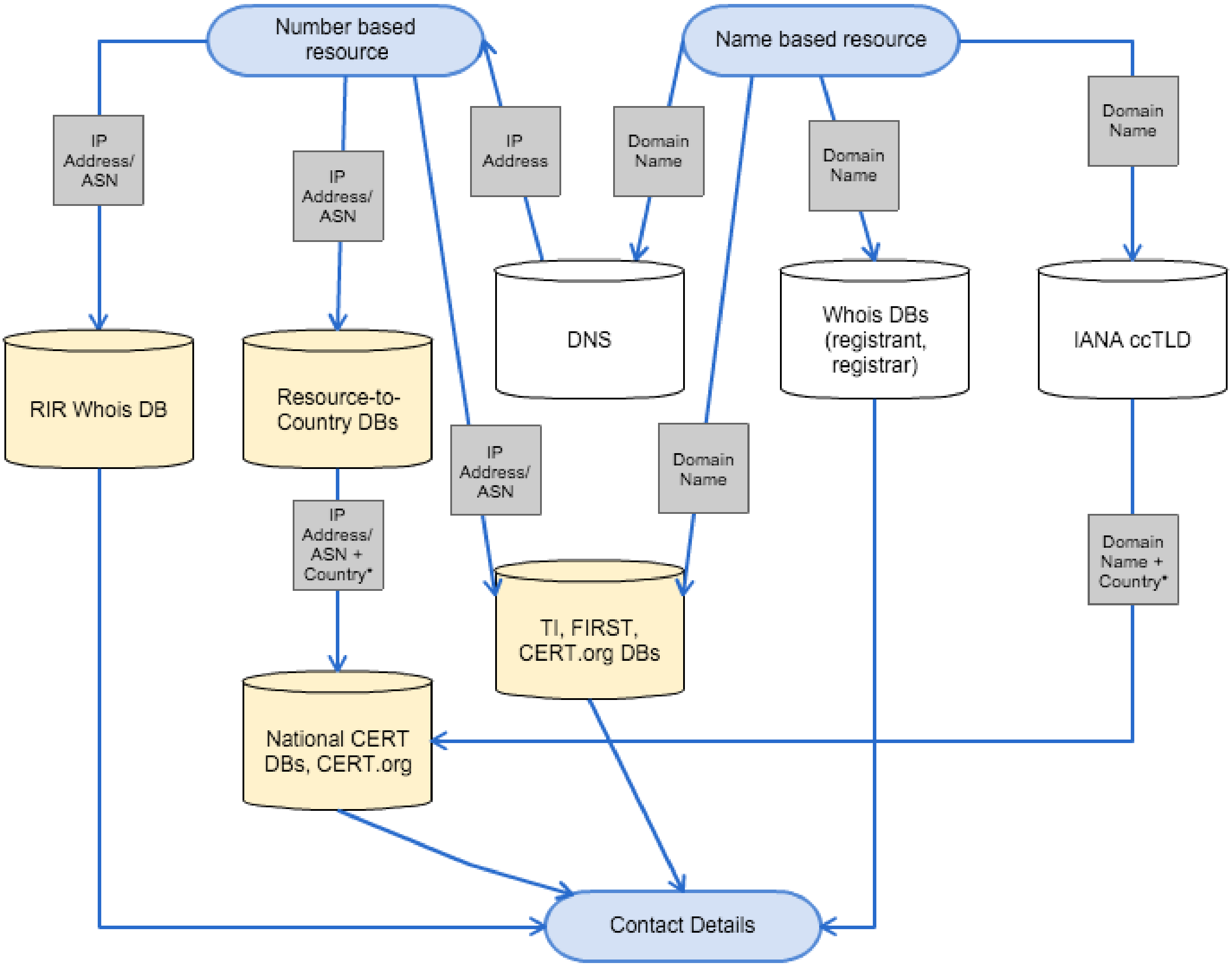

Figure 1 shows possible paths for looking up abuse contact information, starting at a request for a name- or number-based resource on top, walking through some of the datasets described in this document and ending in an email address at the end. Depending on the case and depending on the resource, there might be multiple options for lookups. An incident reporter will have to decide which dataset is the most appropriate or promising for the specific case.

> **Example**: Incident reporter finds a hacked web page. Naturally, she will try to contact the domain registrant (name-based resource lookup) - the admin-c and possibly also the tech-c. However, as time passes, the incident reporter notices more and more hacked webpages. Incidentally, they all turn out to be hosted on the very same IP address block. After some investigations, the incident reporter decides there must be something wrong with the server of the web page’s host. She therefore decides to contact the holder of the IP block (the host) in order to hand him a long CSV file of all web pages that are hacked and residing on the hosts' IP range.

In practice it is often unclear which path to choose.

Sometimes an incident reporter might want to contact a single point of contact (PoC) for a whole country. Typically this would be a national CERT, which in turn will use some kind of contact lookup mechanism (possibly more accurate) to assign the incident report to a locally trusted and well-known incident handler. For this case (sending incident reports to a national CERT), the reporter must find out in which country the resource is used or in which country the organisation the resource has been assigned to is based in. Since there is a well-known dataset of national CERTs (see CERT/CCs national CSIRT database), the problem can be reduced to finding the country code of the resource (for example: given an IP address 1.2.3.4, in which country does this IP address reside?). We will discuss this special case in the section on supporting databases.

However, we must remember that the problem of whom to contact is a choice that must be made on a case-by-case basis. Therefore, any framework must be flexible enough to support different approaches.

Also note that not all countries have national CERTs. So, the areas of responsibilities might vary from country to country.

6. Existing Datasets

In this section we list various datasets that can be used by incident reporters to determine the right contact information. For each dataset we describe what kind of data it consists of, how often it gets updated, who maintains the data and if there are any known issues. Furthermore we explain if the data is original or taken from a different data source. In this context, 'first-hand' means that the data is provided by the authoritative source and 'second-hand' means that the data is taken from other sources. It's possible that second-hand data is less up-to-date and/or deviating from the original data.

A table providing an overview of all datasets described in this section is provided in the appendix.

6.1. Trusted Introducer

6.1.1. Overview

Trusted Introducer (http://trusted-introducer.org) (TI) maintains a directory of IT security teams and TI members. While the scope of the database is global, there is a strong focus on Europe. TI assigns different maturity levels to CERTs: listed, accredited and certified. TI also offers a CSV export of its database to TI members (you need to be logged into the TI website to access this CSV list). The CSV list is searchable by resources such as ASN, country code or IP range. However, at the time of writing this document, there are still some issues with automating the querying of the TI data.

6.1.2. Data in the Dataset

The data in the TI database contains, amongst other fields, the following information:

- Team name
- TI level (Listed, Accredited, Certified)
- URL of the team description on the TI webpage
- Country
- The constituency of the CERT:
    - ASN
    - netblocks
    - domains
- Email address(es) of the CERT
- PGP key IDs of the CERT's team key

- Telephone number
- Postal address
- Business hours
- Time zone
- Team representative
- Website (URL) of the CERT

Example: One example can be seen at: http://trusted-introducer.org/directory/teams/certat.html.

All the above information is available to the public. Members have access to more information.

TI also provides an automatic transfer from ASN/netblock/domain names to the ACDC information sharing service. Teams can choose to submit all or part of their TI constituency description to ACDC, which allows the TI service as a "trusted" party to provide such information.

6.1.3. Is the data first- or second hand?

First-hand.

6.1.4. Where can the data be found?

http://trusted-introducer.org/

6.1.5. Who has access to the data?

The public has access to a searchable list of teams via the website. TI members have access to the members' view and can download a CSV file of the database (there are two versions of the CSV file, v2 is preferred). The CSV file contains more than the public information but not the full information per team, only information that might be useful for incident or vulnerability management tasks.

6.1.6. Is there an API?

Currently, a logged-in user (TI member) can download a CSV file dump of the database in the internal section and query the (downloaded CSV) data automatically. The access is X.509 client certificate protected and can therefore be automated and imported.

6.1.7. Who maintains the data?

Trusted Introducer Service (https://www.trusted-introducer.org).

6.1.8. How up-to-date is the data?

TI members on the accredited and certified level have the obligation to report any updates or changes at least every four months. While a grace period is available, the use of the self-service function has greatly reduced the number of reminders that are sent out by the Trusted Introducer Service. If a TI team does not mark the information about the team as up-to-date or report any update then the team is suspended until it conforms to the defined standards.

6.1.9. Known issues

There have been issues with netblock information and domain names in the past. As strong import filters are now enforced, three fields (ASN, netblock and domain) are clean, while a free-text field still allows arbitrary texts to describe the constituency if necessary.

6.2. FIRST Database

6.2.1. Overview

The Forum for Incident Response and Security Teams (FIRST https://www.first.org/) is one of the world's oldest IT security forums (formed in 1990). As such, FIRST maintains an extensive list of IT Security teams (FIRST's members) around the world.

6.2.2. Data in the dataset

The data in the FIRST directory contains, amongst other fields, the following information:

- Team info
    - Short team name
    - Team representative
    - Membership type
    - Date of establishment
    - Website (URL)
- Constituency
    - Type of constituency
    - ASNs
    - Internet domain addresses
    - Country of constituency
- Team contact information
    - Telephone number
    - Email address
    - Postal address
    - Time zone
- Business hours
    - Business hours
    - Reachability outside of business hours
- Services
    - Textual description: reactive, proactive, etc.
- Cryptography
    - PGP key ID
    - PGP fingerprint
    - The full team PGP key (ASCII armoured)
- Team members
    - A list of names of team members

Example: one example can be seen at https://www.first.org/members/teams/cert-at.

6.2.3. Is the data first- or second-hand?

First-hand.

6.2.4. Where can the data be found?

The data is available via: http://www.first.org -> members.

6.2.5. Who has access to the data?

The data is publicly accessible.

6.2.6. Is there an API?

At the time of writing, there is an experimental API inspired by the RIPEstat API.

The API is documented at http://api.first.org/.

Example:

Query:

```
wget "https://api.first.org/data/v1/teams.json?country=AT"
```

Output:

```
{
  "status": "OK",
  "status_code": 200,
  "version": "1.0",
  "total": 3,
  "last-modified": "Thu, 31 Dec 2015 17:07:24 +0000",
  "data": [
    {
      "id": "aconet-cert",
      "team": "ACOnet-CERT",
      "team-full": "ACOnet-CERT",
      "host": "Vienna University",
      "establishment": "2003-01-01",
      "address": "ACOnet-CERT\r\nVienna University Computer Center\r\nUniversitaetsstrasse
7\r\nA-1010 Vienna",
      "country": "AT",
      "website": [
        "http://cert.aco.net/"
      ],
      "email": "cert@aco.net",
      "phone": [
        "+43-1-4277-14045",
        "+43-1-4277-9140 (fax)",
        "+43-1-4277-9140"
      ],
      "fax": "+43-1-4277-9140",
      "timezone": "UTC+0100",
      "timezone-dst": "UTC+0200",
      "operating-hours": "Mon - Fri 9:00 - 17:00",
      "constituency": "Research & education",
      "constituency-description": "Customers of ACOnet, Austrian Academic Computer Network",
      "last-modified": "2015-12-31T17:07:24+00:00"
    },
    ...
  ]
}
```

6.2.7. Who maintains the data?

FIRST.org Inc. maintains the database.

6.2.8. How up-to-date is the data?

FIRST members can update their data via a web form.

6.2.9. Known issues

The First directory is often lacking ASNs and netblocks for FIRST team members.

6.3. CERT/CC's National CSIRT Database

6.3.1. Overview

CERT/CC hosts a yearly national CSIRT meeting: https://www.cert.org/incident-management/national-csirts/meeting/. As part of these meetings, CERT/CC also maintains a fairly accurate list of national CSIRTs: https://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

A CSIRT with National Responsibility (or “National CSIRT”) is a CSIRT that has been designated by a country or economy to have specific responsibilities in cyber protection for the country or economy. A National CSIRT can be inside or outside of government, but must be specifically recognised by the government as having responsibility in the country or economy.

6.3.2. Data in the dataset

- Organisation (i.e. the CSIRT)
    - Team name
    - Team short name
    - Country
    - Telephone hotline
    - Email address
    - Website
- Organisational Units
- Groups
- Personal data on CSIRT team members
- Cryptography
    - S/Mime or PGP or Kerberos information
    - PGP key id

Example (from the publicly visible website):

Field	Value
Country	Austria
Team short name	CERT.at
Team name	National Computer Emergency Response Team of Austria
Website	http://www.cert.at

6.3.3. Is the data first- or second-hand?

First-hand.

6.3.4. Where can the data be found?

The data is accessible via: https://nationalcsirts.cert.org/ and https://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

6.3.5. Who has access to the data?

Some of the data is publicly available at: https://www.cert.org/incident-management/national-csirts/national-csirts.cfm.

6.3.6. Is there an API?

The list of national CSIRTs is publicly available on http://www.cert.org/incident-management/national-csirts/national-csirts.cfm. The data is in JSON format.

6.3.7. Who maintains the data?

The CERT Coordination Center Software Engineering Institute at Carnegie Mellon University (http://cert.org/about/) maintains the data.

6.3.8. How up-to-date is the data?

The data is updated at least annually via information gathered at the annual meeting. It is also updated on an ongoing basis as the organisation becomes aware of new national CSIRTs. Teams are encouraged to update their contact info via email or web form at: https://www.cert.org/incident-management/contact.cfm.

6.3.9. Known issues

Depends on Javascript.

6.4. ENISA's CERT Inventory

6.4.1. Overview

ENISA maintains a meta-directory of CERTs in Europe on their website. The list comes from TI as well as FIRST. Additionally, there are a handful of entries that are manually maintained (they are neither in the TI nor in the FIRST database).

6.4.2. Data in the dataset

- CERT Name
- CERT Country
- Constituency - national, governmental etc.
- Established date
- Team website (for contact)
- TI/FIRST Status
- Mandate

Example:

Field	**Value**
Country	Austria
Name	CERT.at
CERT type	National
Establishment date	01/01/2008
Contact	http://www.cert.at
TI status	Accredited
FIRST membership	Member
Mandate	Official

6.4.3. Is the data first- or second-hand?

Second-hand: The data is a combination of other datasets.

6.4.4. Where can the data be found?

The data is accessible via: https://www.enisa.europa.eu/activities/cert/background/inv (needs Javascript).

In addition, there is a PDF version at: https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe.

The PDF version also contains a practical change history at the end of the document.

6.4.5. Who has access to the data?

The data is publicly accessible.

6.4.6. Is there an API?

There is no API.

6.4.7. Who maintains the data?

ENISA maintains the data.

6.4.8. How up-to-date is the data?

ENISA updates the list twice a year.

6.4.9. Are there any known issues?

- The data gets manually updated
- It is dependent on Javascript (except for the PDF)
- There is no abuse contact or IP block/ASN information

6.5. CERT.at's National CERT Database

6.5.1. Overview

CERT.at created this national CERT database and offers an online lookup tool at: https://contacts.cert.at to the public.

6.5.2. Data in the dataset

This dataset is a combination of the CERT/CC's national CSIRT database and some manually maintained data (CERTs which are known to CERT.at).

6.5.3. Is the data first- or second-hand?

The data is second-hand.

6.5.4. Where can the data be found?

The data is accessible via: https://contacts.cert.at/.

6.5.5. Who has access to the data?

The data is publicly accessible.

6.5.6. Is there an API?

You can submit any text data (for example a log file) containing IP addresses (IPv4 and IPv6 are supported) in a form. Submission to this form can be either manually or via script (curl, wget, etc.). The result of the form submission will be the national CERT's email address for the specific IP address.

Example:

In your browser, enter the following: https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl?ip=140.78.1.1&bShowNationalCERT=on&sep=TAB

As an answer you will get:

140.78.1.1 AT CERT.at reports@cert.at

6.5.7. Who maintains the data?

CERT.at maintains the data.

6.5.8. How up-to-date is the data?

At the time of this writing, the data is updated manually.

6.5.9. Are there any known issues?

The database needs to be manually synchronised with CERT/CCs national CSIRT database.

6.6. RIPE NCC Datasets

6.6.1. Overview

The RIPE NCC keeps a comprehensive record of all Internet number resources registered within the RIPE NCC service region to ensure that each Resource Holder holds unique and legitimate Internet Protocol (IP) address space and Autonomous System Numbers (ASNs). The collective of this data is generally referred to as the “RIPE Registry”. The RIPE Database provides access to the public data of the Registry. More information is available in the RIPE Document "The RIPE Registry".

Following a proposal made by the RIPE community in June 2011, the RIPE Policy "Abuse Contact Management in the RIPE Database" made it mandatory for every resource object (**inetnum**, **inet6num** and **aut-num**) to have a dedicated abuse contact via the organisation object. This contact is usually referred to as an “abuse-c” contact and it is the preferred way to report any form of abuse.

The **IRT** (incident response team) object was created with a similar idea in mind but its deployment, even though it has been around for years, is very low and so is it is not widely used. There are initiatives to deprecate this object type and replace its functionality by other means.

Apart from registration data, the RIPE NCC provides access to routing information. Routing data is collected by 13 BGP route reflectors called Routing Information Service (RIS) route collectors (https://www.ripe.net/ris/).

6.6.2. Data in the dataset

Registration data:

- RIPE Database (containing IP resource information and contact data)
- RIPE Routing Registry (containing routing policy information)
- Regional Internet Registry Statistics (RIRSTATS): Holds information about the date and the resource holder's location (on country level) for each allocated resource in the RIR's service region.

6.6.3. Is the data first- or second-hand?

First-hand.

6.6.4. Where can the data be found?

The **RIPE Database** can be searched by using the web interface (https://apps.db.ripe.net/search/query.html) or by directing your Whois client to whois.ripe.net. A full-text search is also available via: https://apps.db.ripe.net/search/full-text.html.

FAQ: https://www.ripe.net/manage-ips-and-asns/db/faq

Documentation: https://www.ripe.net/manage-ips-and-asns/db/support/documentation.

The RIPE Database is also accessible via RIPEstat as a widget and as a data call.

Widget API: https://stat.ripe.net/widget/registry-browser.

Data API: https://stat.ripe.net/docs/data_api#RegistryBrowser.

Additionally, RIPEstat provides an API that is tailored towards retrieving abuse contacts. The Abuse-Contact-Finder is described in more detail at: https://stat.ripe.net/docs/data_api#AbuseContactFinder. As with most data calls on RIPEstat, there is a visual frontend (widget) at: https://stat.ripe.net/special/abuse.

Routing information comes in different variations to accommodate multiple use-cases. See these examples to get an idea about the available data:

- https://stat.ripe.net/docs/data_api#AnnouncedPrefixes Lists what prefixes are/were announced from a given AS
- https://stat.ripe.net/docs/data_api#LookingGlass Provides a direct view into the current status of live routing tables. The output is filtered on a given prefix/IP address
- https://stat.ripe.net/docs/data_api#PrefixOverview Simple returns if an IP address/prefix has been seen in the routing table. If it is announced, the network from which it is originated will be included in the result

More examples can be found under: https://stat.ripe.net/docs/data_api.

6.6.5. Who has access to the data?

The data is publicly accessible.

6.6.6. Is there an API?

RIPEstat provides interfaces to provide access to these datasets as mentioned in the paragraph on “Where can the data be found?”. More details on the RIPEstat data API can be found under: https://stat.ripe.net/docs/data_api.

6.6.7. Who maintains the data?

RIPE NCC and RIPE NCC members.

6.6.8. How up-to-date is the data?

The RIPE NCC has the responsibility for keeping the Registry comprehensive, correct and up-to-date. To do this, the RIPE NCC relies on Resource Holders to supply data that pertains specifically to the Resource Holder, as documented in the RIPE NCC Standard Services Agreement [ripe-435] and/or the Independent Assignment Request and Maintenance Agreement [ripe-462].

6.6.9. Are there any known issues?

Abuse-c only applies to the RIPE NCC service region. Legacy IP space and provider independent IP space is not yet fully covered.

6.7. OAS's List of CSIRTs

6.7.1. Overview

The Organisation of American States (OAS.org) keeps a list of CERTs on their website.

6.7.2. Data in the dataset

- Short CERT name
- Official team name
- Team website (for contact)
- Email
- CERT country
- Exact location (GPS) - probably based on the address (which is not displayed to the public)

Example:

Field	**Value**
Short team name	CERTuy
Host institution	Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento
Constituency	Gobierno - Government
Address	Torre Ejecutiva Sur, Liniers 1324 Piso 3, Montevideo, Uruguay
Telephone	+598 2 901 29 29 Ext. 8567
Website	http://www.cert.uy
Email	cert@cert.uy
Report incidents	http://www.cert.uy/inicio/incidentes/como_reportar/
Public PGP Key	http://www.cert.uy/wps/wcm/connect/7db498004f455c2087ca87f04da0fafa/pgp certuy.pub.txt?MOD=AJPERES&ContentCache=NONE

6.7.3. Is the data first- or second-hand?

The data is second-hand.

6.7.4. Where can the data be found?

The data can be accessed via: http://www.oas.org/cyber/.

The data can also be accessed via:
https://www.sites.oas.org/cyber/ES/Paginas/Directory/Default.aspx.

6.7.5. Who has access to the data?

The data is publicly accessible. There is also a private portal for governmental CERTs.

6.7.6. Is there an API?

No.

6.7.7. Who maintains the data?

Organization of American States Cyber Security Program: http://www.oas.org/cyber/.

6.7.8. How up-to-date is the data?

OAS receives updated from its Member States.

6.7.9. Are there any known issues?

Unknown.

7. Supporting Datasets

Often enough, there is a requirement to transform one network resource (e.g. an IP address) into a different network resource (e.g. a country code) in order to look up the abuse contact (e.g. the national CERT) for the IP address. This section describes these supporting additional databases.

7.1. Country Code Lookups

As discussed in the section “General remarks on abuse contact lookups”, some incident reports should simply go to the national CERT. For this task, it is important to find the country code of an IP address or a domain.

In the case of IP addresses, there are a couple of databases that will be discussed below.

7.1.1. Maxmind

Maxmind is one of the most well known databases for IP to country code mappings. There are a couple of versions of Maxmind with varying degrees of accuracy and costs:

- GeoIP City
- GeoIP Country
- GeoIP Lite
- GeoIP Legacy

We advise the reader to check the Maxmind webpage for current offerings. The full description on this service can be found at: http://dev.maxmind.com/geoip/geoip2/geolite2/.

Using the GeoIP database in a wide variety of languages is very straightforward. In this document we give an example in Python (from Readthedocs).

```
>>> import geoip2.database
>>> reader = geoip2.database.Reader('/path/to/GeoLite2-City.mmdb')
>>> response = reader.city('140.78.1.1')
>>> response.country.iso_code
'AT'
```

For convenience RIPEstat provides a REST API to the MaxMind data set documented here: https://stat.ripe.net/docs/data_api#Geoloc

7.1.2. Team Cymru

Team Cymru provides an IP address to ASN mapping service via Whois (RFC3912) as well as via netcat, http(s) or DNS based lookups. As part of this lookup mechanism, there are options to also get the country code of a given IP address. To the best of the authors' knowledge, the IP to country mapping is done via the RIR databases.

The full description on how to use this service can be found at: https://www.team-cymru.org/Services/ip-to-asn.html.

Example lookup:

```
$ whois -h whois.cymru.com  " -c   140.78.1.1"

AS      | IP               | CC | AS Name
1205    | 140.78.1.1       | AT | JKU-LINZ-AS University Linz,AT
```

or as a shell script:

```
#!/bin/bash

ip=$1
cmd=$(cat <<EOT;
begin
verbose
 -c
$ip
end
EOT)

echo "$cmd" | nc whois.cymru.com 43
```

Example output:

```
Bulk mode; whois.cymru.com [2016-01-12 19:30:14 +0000]
Error: no ASN or IP match on line 3.
1205    | 140.78.1.1       | 140.78.0.0/16       | AT | ripe     |          | JKU-LINZ-AS University Linz,AT
```

7.2. IP2ASN Service

7.2.1. Team Cyrmu

As described above, Team Cymru also provides an IP2ASN service.

7.2.2. IP2ASN Lookup via BGP Routing Table

If you have access to a BGP full feed, you can easily make your own IP2ASN lookup mechanism with Quagga (http://www.nongnu.org/quagga/).

Required components:

- Quagga routing daemon with a BGP full feed in read-only mode (i.e. make sure that it does not announce routes anywhere)
- A small script that will query Quagga and listen on port 43 (Whois). An example of such a script can be found at: https://github.com/certtools/whois-quagga
- This approach is the preferred approach since it builds on live BGP data

7.2.3. IP2ASN via Maxmind

Maxmind also offers an IP2ASN database for offline lookups:
https://dev.maxmind.com/geoip/legacy/geolite/

7.2.4. IP2ASN in Python

The pyasn library in python is based on a fast ip2asn offline lookup mechanism. It takes its data from weekly snapshots of the Routeviews data:
https://github.com/hadiasghari/pyasn

8. Conclusion

This document lists a number of known datasets that contain abuse contacts and point to computer emergency response teams (CERTs). This is probably not a complete list. If you are aware of additional useful data sources, please contact the authors. As a next step, some of the organisations listed above are working on a common user interface (API) that allows abuse reporters to access these databases more easily and will allow users to find the correct contact information more quickly.

In the future we would like to work with the other RIRs to see if they're implementing similar concepts (such as abuse-c) and determine how we can possibly include that in the next version of this document.

9. Appendix

9.1 Existing Datasets Overview Table

Source	First- vs. second-hand	Access	API	Update cycle	Known issues
Trusted Introducer	First-hand	Public access to searchable list; member view to details	Downloadable CSV file	Every 12 months	Some free text not machine readable
FIRST DB	First-hand	Public	Experimental API http://api.first.org	FIRS members update data via web form	Often lacking ASNs for FIRST team members
National CERT DB	First-hand	Public for parts of the data	Working on downloadable CSV file	Members update their information via web form	No known issues
ENISA's CERT Inventory	Combination of other datasets	Public	No API	Twice a year	Manual updates; dependent on Javascript; no abuse contact & IP/ASN information
CERT.at	Second-hand	Public	Somewhat (a query returns an email address)	Manually	Manual synchronisation with national CERT DB
RIPEstat or RIPE Database	First-hand	Public	https://stat.ripe.net/docs/data_api	Continuously updated	Abuse-c only covers RIPE NCC service region
OAS	Second-hand	Public - private portal for governmental CERTs	No	No	Unknown