AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

DBWG Session
by
Simon Seruyinda

DBWG purpose

- Announce new developments or updates.
- Engage the community in testing new developments.
- Call for comments or suggestions regarding any technical aspect of the WHOIS.
- Engage the community with regards to the database inconsistencies and how we can work together to have them resolved.
- Call for presentations and researches around the WHOIS and database-related subjects.
- Gather ideas of the community regarding improvements to the current DB-related services.
- Help the community in terms of DB tools or objects migration.

Session agenda

RPKI IRR integration (30 Min)
WHOIS new features and updates (20 Min)
RDAP (20 Min)
Database business rules / policy compliance (20 Min)

Break

Abuse contacts and IRT (20 Min)
BCRYPT authentication and auto-protection of person and role objects (20 Min)
Gather ideas of the community regarding improvements to current DB-related services (15 Min).
Discuss choice of a community co-chair (15 Min)

AFRICA INTERNET SUMMIT'19 KAMPALA - UGANDA 9 - 21 JUNE 2019

WHOIS

New Features and Updates

overview

Lame delegation

Intra RIR Transfers (partial and full)

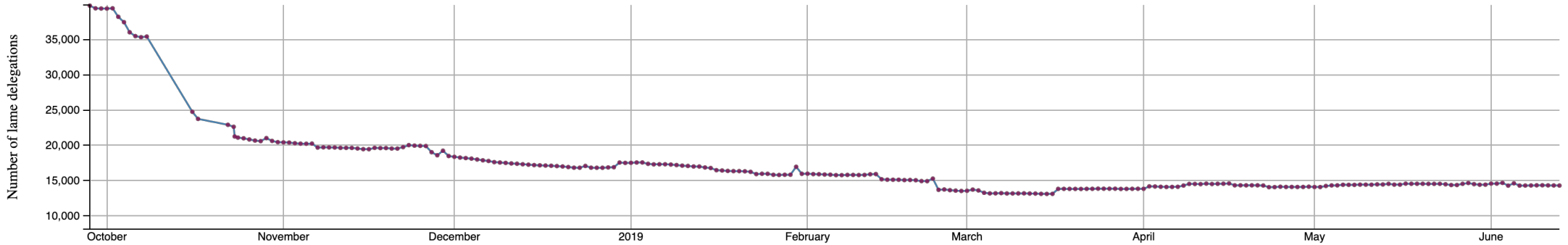
RDAP RIR alignment

Restriction to minority space redirection

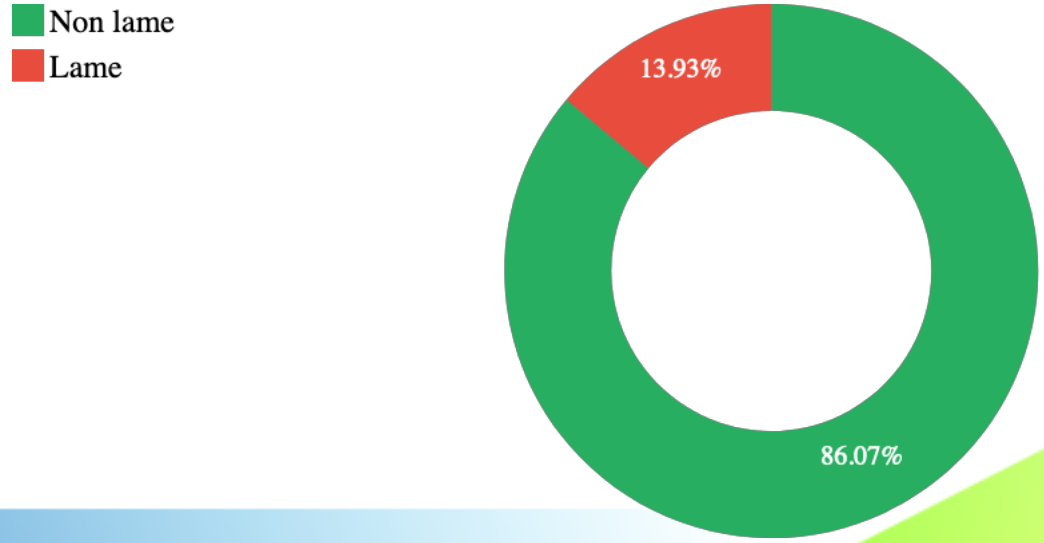
IRR aut-num authentication

Upgrade to some libraries e.g bouncy castle to improve stability and security

Lame delegation



Currently we stand at 14,296 objects which is a 64% reduction from 39,814



Implementation details

- JNDI for the checks.
- As fall back, we use dig.
- Daily job. If last check was not successful, or if 30 days have passed since last check.
- The job picks the delta (update/deletion/new objects) and determines which ones to test and course of action to take.

Transfers

- Involve movement of resources between member organizations
- Subnetting and creating new inet(6)nums in the database

Prefix length	count
/17	1
/18	1
/20	3
/21	2
/22	4
IPv6	
/32	1
ASN	1

RDAP Alignment

- CIDR Ranges for IP Network issue was Fixed . We Used the extension proposed by ARIN.
- Organization entity is not returned in ip or aut-num query responses issue is now fixed. In case of IP or aut-num, the organization role is "registrant".
- HTTP 400 (bad request) for IP Networks with Multiple Countries issue. Fixed using coma-separated list of values.

RIPE NONAUTH

Last year RIPE moved all OOR objects to the ripe-nonauth source database. This meant that operators could potentially filter these route(6) objects based on the source

Our IRR was not allowing creation of route(6) with OOR aut-num. Therefore, we had to implement this in our database.

For route(6), we skip the aut-num authentication.

Minority redirection

Implemented in May 2016

Has been source of DDOS and OOM issues

Changes

1. Only 4 external Whois clients: one per external RIR.

2. These Whois clients are controlled by a ReentrantLock. Only one thread can use a specific External WHOIS at a time.

3. While an external Whois client is busy, other requests for the same Whois client are dropped with a message. Requests for other clients will be processed.

Library upgrades

Upgrade to some libraries to improve stability and security e.g bouncy castle, c3pO (connection pooling) ,guava etc.

The bouncy castle are a group of APIs used in cryptography. Used in our SMIME, PGP and X509 implementations.

AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

Thank you

Questions?

AFRICA INTERNET SUMMIT'19 KAMPALA - UGANDA 9 - 21 JUNE 2019

RDAP

Introduction

Registration data access protocol

Developed by WEIRDS working group at IETF

Alternative protocol to query resource data

Standard way to query WHOIS data across RIRs

Redirection mechanism

AFRINIC has an RDAP service available at https://rdap.afrinic.net/rdap

IP networks

https://rdap.afrinic.net/rdap/ip/<IP prefix>/<prefix length>

This query will return the "most-specific" or smallest IP network which completely encompasses it in a hierarchy of IP networks.

For example, the following URL would be used to find information for the most specific network containing 196.1.0.0/24:

https://rdap.afrinic.net/rdap/ip/196.1.0.0/24

The following URL would be used to find information for the most specific network containing 2001:42d0::/32

https://rdap.afrinic.net/rdap/ip/2001:42d0::/32

AS Numbers

AS Numbers

https://rdap.afrinic.net/rdap/autnum/<AS number>

Used to identify autonomous system registrations and associated data referenced, for example, https://rdap.afrinic.net/rdap/autnum/37388

RDNS

RDNS

https://rdap.afrinic.net/rdap/domain/<rdns object key>

Used to identify reverse DNS information and associated data referenced, for example, https://rdap.afrinic.net/rdap/domain/112.192.196.in-addr.arpa

Entity

Entity

https://rdap.afrinic.net/rdap/entity/<entity string>

Used to retrieve entity related information using an entity string identifier.

This can be an org-handle or nic-handle, for Example:

https://rdap.afrinic.net/rdap/entity/TEAM-AFRINIC

https://rdap.afrinic.net/rdap/entity/ORG-AFNC1-AFRINIC

Client

- The NicInfo https://github.com/arineng/nicinfo open source RDAP client developed by ARIN can be used to query RDAP records from the command line.
- Curl
- Web browser

Redirection mechanism

Uses HTTP 301 as response, with headers pointing to the correct URL

Example of an IP resource 198.0.0.0 that belongs to the ARIN region https://rdap.afrinic.net/rdap/ip/198.0.0.0

```
HTTP/1.1 301
Moved Permanently
Date: Wed, 15 May 2019 08:10:20 GMT
Server: AfriNIC RDAP
Access-Control-Allow-Origin: *
Content-Type: application/rdap+json;
charset=UTF-8 Location: https://rdap.arin.net/registry/ip/198.0.0.0
```

AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

Thank you

Questions?

DB Business rules/ policy compliance

Overlaps

- Overlaps in sub-allocations and assignments by members
- 60 IPv6 objects
- 13284 IPv4 objects
- Total 13344 objects with overlaps

No reverse unless assigned

We still have uncompliant objects. Though the numbers have reduced significantly over the years.

- 636 rdns objects
- 24 Member organizations.

Unprotected rdns objects

Mostly from old whois version

1,389 rdns in total

65 Member organizations

We need a way forward on how to deal with these.

Rdns overlaps

Mostly from old whois version

773 objects

17 Member organizations

Thank you

Questions?

AFRICA INTERNET SUMMIT'19 KAMPALA - UGANDA 9 - 21 JUNE 2019

Abuse contacts and IRT

Current status

Currently no clear way to get abuse contact information from WHOIS

Abuse-mailbox attribute is not very much used

MNT-IRT is also rarely used

Information scattered in descr, remarks, notify and other attributes

infeasible to create API service

Abuse mailbox

- 5 out of 2,502 organization objects have the abuse mailbox attribute set
- 161 organization objects have specified abuse email in the wrong attribute
- 13,523 objects(autnum,inetnum,inet6num) have specified the abuse email in the wrong attribute

MNT-IRT Usage stats

Resources that have added the MNT-IRT:

25 aut-nums out of 1741

30 inet6num out of 30955

255 inetnums out of 124881

Member-based stats

Number of Organizations with IRT in the aut-num = 16

Number of Organizations with IRT in the inetnum = 22

Number of Organizations with IRT in the inet6num = 15

Total number or organizations with IRT in (aut-num, inetnum or inet6num) = 23

AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

Thank you

Questions?

AFRICA INTERNET SUMMIT'19 KAMPALA - UGANDA 9 - 21 JUNE 2019

Object Security

BCRYPT

Brcypt enabled since WHOIS v2.3 in Jan 2017

MD5/CRYPT can authenticate, but cannot be used to update or create new mntner objects

Out of 3787 (mntner and IRT objects), 800 are protected by BCRYPT approximately 21.1%

11 objects are using both PGP and BCRYPT

152 objects are using PGP auth only

2846 objects are using only MD5. = 75.1%

Why abandon MD5

Its not collision resistant. Two sources can have same MD5 hash

Its easy to build rainbow tables

Its fast and memory conserving which means an attacker with enough resources can compute all possible 8-character passwords for a given salt in a matter of hours

Why BCRYPT

Why use BCRYPT

It’s a slow algorithm that needs more CPU cycles to produce a hash. Therefore an attacker will need much more processing power to brute-force your password database if they have it.

It has a configurable parameter that determines how much computational work should be spent to hash the password.

Person/role protection

As from WHOIS v2.3, Jan 2017

All non protected person /role objects have been auto-protected by an auto-generated maintainer.

Password is shared with user. Once auto-generated mntner is no longer referenced, its removed.

16,464 out of 19,677 objects are protected by auto-generated mntner. = 83.67%

3,213 out of 19,677 are protected by normal mntner = 16.43%

Unreferenced person/role

What should we do with unreferenced person/role objects?

9,847 unreferenced person/role objects out of 19,677 approximately 50%

We have a job to cleanup, but its not activated yet.

PGP

We strongly advise the use of PGP

Need help setting up PGP key, see links below.

How to create PGP key <https://afrinic.net/support/whois-db/whois-faq/how-to-create-a-key-cert-object-on-afrinic-whois-database>

PGP authentication <https://www.afrinic.net/support/whois-db/pgp-authentication>

auto-dbm@afrinic.net users are strongly advised to use PGP

AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

Thank you

Questions?

Ideas on improvements to current database services

DBWG community co-chair

AFRICA INTERNET SUMMIT'19
KAMPALA - UGANDA
9 - 21 JUNE 2019

Thank you

Questions?