AFRINIC
The Internet Numbers Registry for Africa

African Network Information Centre

OVERVIEW
AFRINIC WHOIS DATABASE
ACCURACY REPORT

AFRINIC | 11th Floor Standard Chartered Tower
19 Cybercity, Ebene | Mauritius
t: +230 403 5100 | f:+230 466 6758

Published Date: January 21, 2021 1:22 PM

Filename: whois_report_overview V1

This report is the outcome of an internal comprehensive audit of IPv4 number resources following the misappropriation of IPv4 number resources in the AFRINIC WHOIS Database. The report details the background, scope, methodology, findings of the audit and the associated risks with regards to reclaiming the resources.

It also highlights the actions taken by AFRINIC, so far, notably to keep its stakeholders informed about the situation, infrastructural improvements regarding its database and a review of its operational business rules and procedures, including but not limited to a review of infrastructural user access.

Finally, the report provides for recommendations to AFRINIC's community so that such policies may be developed through the existing Policy Development Process which may then assist AFRINIC in ensuring at all times an accurate WHOIS Database.

The report has the following scope:

1. Investigating IPv4 resources known or suspected to have been misappropriated from AFRINIC's pool;
2. Investigating the rightful custodianship of Legacy IPv4 resources falling under the jurisdiction of AFRINIC;
3. Investigating AFRINIC's inventory of available, delegated, and legacy space(IPv4) since 2005 and subsequent replenishment of AFRINIC managed IP resources;
4. Verifying that all Resource Members underwent the normal registration process for membership;
5. Verifying that all Resource Members submitted resource request(s) for all the resources they hold;
6. Making such recommendations on how the existing WHOIS Database and MyAFRINIC features could be improved.

The report also highlights the findings and actions taken by AFRINIC. A summary of the findings and actions taken by AFRINIC are as follows:

1. 2,371,584 of IPv4 addresses were, without any lawful authority, misappropriated from AFRINIC's pool of resources and attributed to organisations without any justification;
2. Since February 2020, a total of 1,060,864 IPv4 resources have been reclaimed, i.e deregistered from the AFRINIC WHOIS Database and are presently in 'quarantine' for a period of 12 months. Following the 'quarantine' period, the resources may be added to AFRINIC's pool of resources available for new allocations;
3. A total of 1,310,720 IPv4 resources, related to two distinct organisations, are yet to be reclaimed due to ongoing due diligence;
4. 1,799,168 IPv4 addresses, deemed to be legacy address space appeared to have been compromised and actions have been taken to contact the source-holders thereof;
5. 394,496 legacy IPv4 addresses have subsequently been consolidated at the request of the holding company of the organisations to which the resources were registered;
6. Unsubstantiated changes to 467,968 legacy IPv4 addresses have been reversed;
7. 936,704 legacy IPv4 addresses are currently under dispute and pending determination of rightful custodianship.

Misappropriation of IPv4 resources

In or about March 2019, upon receipt of a Court Order from the Supreme Court of Mauritius following an application made by the United States Federal Investigation Bureau (FBI), AFRINIC became aware of certain suspicious activities regarding several IPv4 address blocks which it held. A preliminary investigation carried out internally also revealed that internal staff may, without any lawful authority, have acted in collusion with other third parties. These unlawful acts were the misappropriation of IPv4 resources, held by AFRINIC, which resulted in prejudice to the company and by extension to AFRINIC's Resource Members and its Community at large.

In this respect, in July 2019, AFRINIC's Board of Directors commissioned an investigation to be conducted on the matter and with the assistance of the AFRINIC's sister-RIR, APNIC.

On 01 September 2019,, an online publication entitled "The big South African IP address heist – How millions are made on the "grey" market" by a well-known media company MyBroadband contained serious allegations pertaining to a possible 'hijacking' of IP number resources within the African region. The information published by MyBroadband also indicated that some resources' registration data in the AFRINIC WHOIS Database may have been compromised.

In December 2019, APNIC submitted the findings of an initial internal investigation. The findings were serious enough such that it led to the dismissal of a former AFRINIC staff who was found to have made an abusive use of his rights and privileges as being the then AFRINIC's hostmaster. Further, the said former employee was even found to have misappropriated IP number resources forming part of AFRINIC's own pool of resources to the benefit of a private company owned and controlled by the latter himself, and which in turn engaged in sale transactions of the impugned resources to third parties. This matter has also been reported to the Mauritian Central Criminal Investigation Division and an enquiry is presently on-going.

The report provides details on the misappropriation of IPv4 resources and organisations that were primarily concerned with the audit exercise. The status of the IPv4 resources is also provided and the audit revealed that 2,371,584 IPv4 addresses were misappropriated from AFRINIC's pool of resources and attributed to organisations without any justification.

1. A total of 1,060,864 IPv4 resources have been reclaimed, i.e deregistered from the AFRINIC WHOIS Database since February 2020 and are presently in 'quarantine' for a period of 12 months, and thereafter, the said resources may be added to AFRINIC's pool of resources available for new allocations;
2. A total of 1,310,720 IPv4 resources are yet to be reclaimed due to ongoing diligence being carried out.

The actions undertaken by AFRINIC has, so far, led to one application for an Interim Injunction jointly lodged against AFRINIC by Afri Holdings Ltd, Netstyle A. Ltd, and one Mr. Elad Cohen before the Hon. Judge in Chambers of the Mauritian Supreme Court viz Cause Number SC/COM/WRT/000295/2020.

Since there is an ongoing court case, subject to legal advice, the quarantine period may be extended beyond the 12 months.

Misappropriation of Legacy Resources

In 2019, the detection of the cases where resources misappropriated from the AFRINIC pool were given the legacy status, reinforced the need for continuous audits in regard to the resources with legacy status and their holders. There have been further queries from AFRINIC's Community in regard to some changes that happened in the WHOIS Database for some IPv4 addresses that were migrated in 2005 with legacy status. This report will also provide clarification on these cases.

In regard to legacy resources, the present audit revealed the following:

> 1,799,168 IP addresses which were correctly labelled as legacy address space appeared to have been compromised.

The report summarises the outcome of the investigation in regard to legacy resources that could have been compromised.

The analysis of the records related to these IPv4 addresses and correspondence with the resource holders brought to light the following elements:

1. Dormant resources (i.e. those resources not visible in routing tables) were mainly targeted;
2. Holders of the resources may also be defunct;
3. Some legacy resources appeared to have changed hands several times and that without informing AFRINIC;
4. Email domains were also transferred as part of the 'sale' of IPv4 resources, thus rendering it almost impracticable to contact the initial source holder;
5. Outdated or lack of contact information for most holders of legacy resources, notably the records were transferred from ARIN without email addresses and phone numbers;
6. Maintainer passwords also appeared to have been handed over to subsequent buyers, AFRINIC's validation has so far indicated that out of 9 maintainers passwords listed and all 9 passwords were incorrect;
7. The privileged status attributed to holders of legacy resources have made it less encouraging for buyers of IPv4 legacy resources to sign a Registration Services Agreement with AFRINIC;
8. In most cases, details of the organisational administrative/technical contacts appearing its WHOIS Database are no longer in employment with the organisations concerned;
9. Some holders of legacy resources appeared to have undergone a change of name so that it is no longer practicable to trace down the concerned organisations;
10. As per WHOIS historical records, some of these contacts, between 2012 and 2015 had been updated with emails bearing domain names that matches the organisation holding the resources, the evaluation and validation process could establish that these domains were recently registered and could not align with the length of time the organisation has held the resources for.

Other observations

1. In 2005, legacy resources were migrated to the AFRINIC WHOIS Database from the other RIRs WHOIS Databases. The verification also highlighted the following blocks of IPv4 addresses that were misappropriated from AFRINIC pool, notably 196.48.0.0/16, 196.52.0.0/14, 196.197.0.0/16, 196.198.0.0/16 and given legacy status.

2. Some blocks of IPv4 addresses, notably 192.96.0.0/16, 198.54.0.0/16, 196.6.0.0/16, 196.10.0.0/16, 196.11.0.0/16 and 196.13.0.0/16 migrated to AFRINIC WHOIS Database in February 2005. These blocks of IPv4 addresses had the WHOIS status set to ALLOCATED PA and their usage were recorded as ASSIGNED PA. The custodian of these resources was the UNINET Project. In August 2005, the organisation whose predecessor was the UNINET project indicated to AFRINIC that they would like to return the aforementioned /16 block of IPv4 addresses. Consequently the following actions were taken by AFRINIC:

    a. AFRINIC created organisation objects with the holdership information (name, address, telephone number and contacts, where available) to get their Organisation ID (ORG-HDL).

    b. Some IP addresses in these blocks of IPv4 addresses were in use and assigned to organisations domiciled in South Africa on the AFRINIC WHOIS Database. These IPv4 addresses were updated on the WHOIS Database to have the status "ASSIGNED PI" and tagged with the Organisation ID (ORG-HDL).

    c. These IPv4 addresses retained the legacy status of their parent /16.

    d. AFRINIC then deleted the IPv4 blocks of IPv4 addresses 192.96.0.0/16, 198.54.0.0/16, 196.6.0.0/16, 196.10.0.0/16, 196.11.0.0/16 and 196.13.0.0/16 from its WHOIS Database.

    e. The IPv4 addresses that were not delegated to any organisation in 196.6.0.0/16 , 196.10.0.0/16 , 196.11.0.0/16 , 196.13.0.0/16 were then marked as available in the AFRINIC Pool and delegated to its Resource Members in accordance with the policies in place.

3. The number of Legacy Resource Holders in the AFRINIC service region increased after the registration of the smaller blocks of IPv4 address to their actual users in the AFRINIC WHOIS Database, after the conclusion of this exercise.

4. Not all the 65,536 IPv4 addresses of the 192.96.0.0/16 and 198.54.0.0/16 IPv4 addresses are registered in the AFRINIC WHOIS Database. Some of these IP addresses are managed by another RIR, notably ARIN as a result of the redistribution of various registry space between all five RIRs.

5. The analysis of records highlighted some changes as follows in regard to some resources that either:

    a. lost their legacy status, e.g in a transfer to the organisation actually using the resources or, in case where a request was received for the WHOIS status of the resources to be change; or

    b. do not hold legacy status, while their WHOIS records mention a date before 1998-01-01 - These IPv4 addresses were migrated from the RIPE NCC database and did not hold legacy status at the time of the migration.

Actions taken by AFRINIC

AFRINIC Business Rules

The internal business rules that govern how AFRINIC shall provide support to the Legacy Resource holders in its service region have been reinforced to ensure that proper verification of holdership are conducted before any updates are made to the records on the AFRINIC WHOIS Database.

In the case of AFRINIC Resource Members, the latter has to meet the checks in regard to compliance with AFRINIC's Internal business process and policies that include; amongst others, the requirement that only registered contacts are allowed to request for service support, verification of the domain names registration information, cross-verifying of company registration information where applicable services are available.

Communication

AFRINIC embarked upon a communication strategy using monthly email updates and blog articles to keep its stakeholders, notably its Resource Members and Legacy Resource Holders in its service region and informed about the situation so that all concerned organisations may then take such appropriate actions at their end to protect the custodianship of the resources they hold.

This strategy has proved to be effective since a significant number of our stakeholders have shown an interest in the need to update their records, as well as to protect their legal interests in their related IPv4 resources.

Process

Continuous risk assessments and subsequent improvements have been made to the membership and resource evaluation process used by AFRINIC Registration Services staff in order to mitigate the risks of collusion and misappropriation. Automation of some of the process steps have been implemented to reduce the incidence of both human error and abuse of rights. A change control policy will be introduced to add additional checks and balances. It will also ensure that there is traceability for changes to Number Resources records. All resource and membership requests henceforth undergo a final review by a senior staff member before the invoice is issued.

Existing control mechanisms

Continuous improvements have been made to ensure that proper controls are in place for the management of Internet Number Resources.

Whistleblower mechanism

A whistleblower platform hosted by an independent provider, EthicsPoint was launched in June 2020 and is available at https://afrinic.net/whistleblowing. Both staff and members of the community are encouraged to report malpractices or instances where they believe there might have been violations of AFRINIC policies or standards.

Fraud and Corruption Policy

In June 2019, AFRINIC adopted a fraud and corruption policy and staff are required to strictly adhere to same.

Monitoring

1. Daily Inconsistency reports between MyAFRINIC versus WHOIS are generated and include:
   a. Objects appearing on MyAFRINIC but not on WHOIS
   b. Objects where either the ORG-HANDLE or STATUS does not match

The list of inconsistencies are attached to the report

2. Daily Inconsistency reports between WHOIS versus MyAFRINIC are generated and include:
   a. Objects appearing on WHOIS but not on MyAFRINIC
   b. Objects where either the ORG-HANDLE or STATUS does not match

The list of inconsistencies are attached to the report

3. Resource file entries versus AFRINIC delegated extended stats file

Registration Services Team are informed when inconsistencies are detected between the resource file entries and the registry database.

Use of passwords

Staff authorised to perform changes to records on MyAfrinic and WHOIS databases authenticate such changes using their PGP key. Power maintainers only use PGP authentication.

All Resource Holders are formally instructed to adopt secure password mechanisms.

Systems privileges

Staff members shall be given qualified access to AFRINIC systems in accordance with their roles and duties. Updates that cannot be done using the privileges and interfaces available to Registration Services staff are directed to the Database Manager for processing , upon the approval of the Manager or Head of Department.

Training

Senior staff members managing the registry services handle requests pertaining to updates of the legacy resources and Legacy Resource Holders information. Training of other staff members in the registry services is ongoing to ensure that all team members are capable of diligently evaluating the requests and also able to identify any risks involved. Suspicious activities are examined and the subject of thorough discussion in the teams to create awareness for all support staff members.

Recommendations

As a result of the audit that was carried out on the accuracy of the AFRINIC WHOIS Database, the following recommendations were made:

1. The report recommends that all Resource Members keep their contact information updated.
2. The report recommends that organisations ensure that their details appearing on AFRINIC's WHOIS Database are kept up to date all times.
3. The report recommends that AFRINIC devote resources to ensure that Legacy Resource Holders' requests are attended to within the service timelines.
4. The report recommends that the AFRINIC community critically assess how best the accuracy of the information pertaining to Legacy Resource Holders can be improved and consider whether unused legacy resources should be left idle while AFRINIC exhausts its remaining pool of IPv4 addresses.
5. The report also recommends that policies which may assist AFRINIC in ensuring at all times an accurate WHOIS Database are developed.