DNS RESEARCH FEDERATION

Measuring Internet Abuse through IP Addresses

Alex Deacon

Senior Research Fellow

DNS Research Federation

About us

- The DNSRF, a not for profit organisation based in the UK
- Mission: to advance the understanding of the Domain Name System’s impact on cybersecurity, policy and technical standards
- Areas of activity:
  - Education and research
  - Access to data
  - Engagement in technical standards

Roadmap

- Introduction to the project - research questions
- Methodology
- Indicators

Introduction

- Develop live indicators that provide information about how numbering resources are misused in **Phishing** and **Malware** attacks
- Funded via a grant from ARIN to raise awareness of the issues of IP Address based abuse

Research Questions

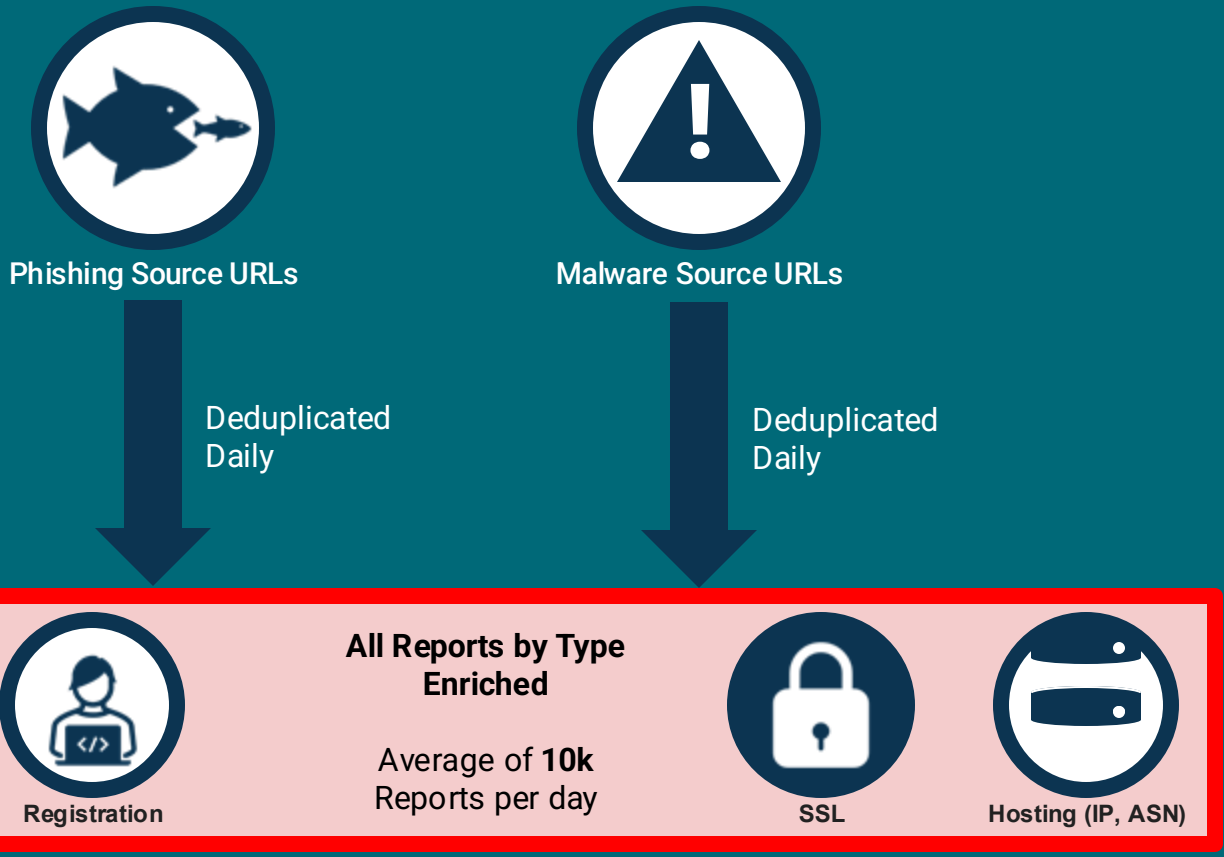
- What percentage of Reported Malware URLs rely on IP Addresses for distribution
- What percentage of Reported Phishing URLs rely on IP Addresses for distribution
- What is the geographical distribution of IP addresses used for Malicious purposes
  - By Regional Internet Registry (RIR)
  - By Country

Methodology: Input sources

- Phishing Reports
  - OpenPhish, APWG, Malware Patrol, URL Abuse

- Malware Reports
  - URLHaus, Malware Patrol, URL Abuse

Methodology: Aggregation and Enrichment

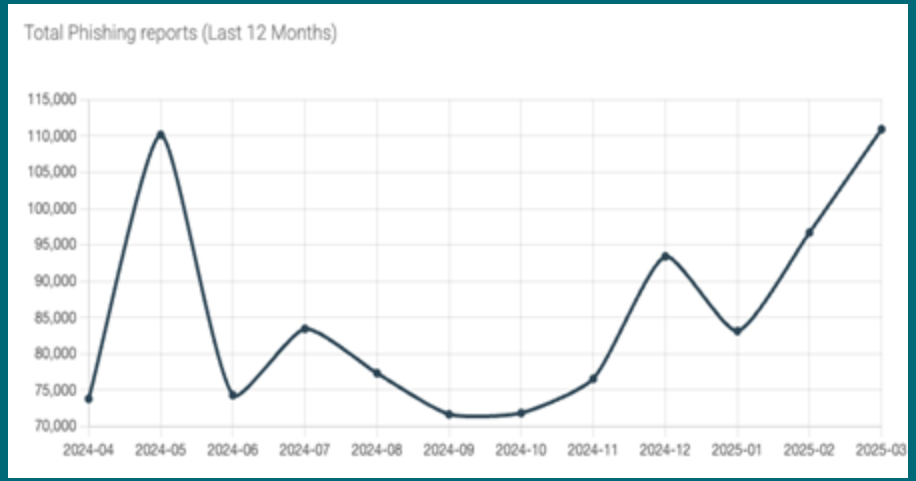


Methodology: Geographical Indication

- BGP data at point of IP abuse report used to determine which ASN is originating the prefix for the given IP address.
- RIR stats data is used to determine which RIR and country the ASN is operating from.

Indicators

Malware and Phishing Reports (Last 12 Months)



Average Per Month:

58802

Average Per Month:

85285

Indicator 1. IP Address Use in Malware

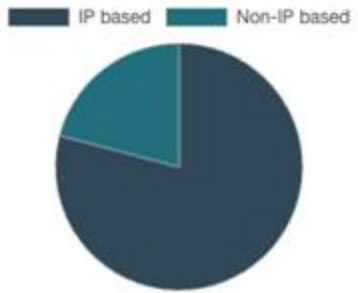
This indicator explores what percentage of reported malware URLs rely directly on the use of IP addresses.

Percentage of reported malware URLs that use IP addresses in the last month/30 days

Percentage

79.1132

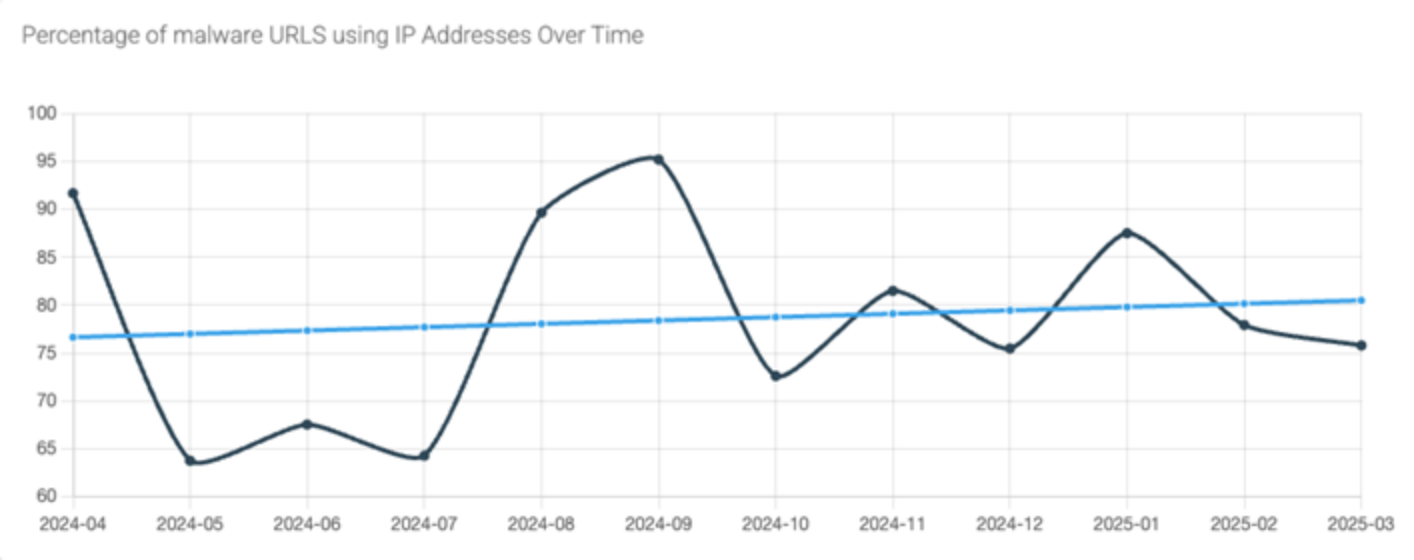
Percentage of reported malware URLs that use IP addresses in the last month/30 days



DNS RESEARCH FEDERATION

Indicator 1. IP Address Use in Malware

This indicator explores what percentage of reported malware URLs rely directly on the use of IP addresses.



Indicator 2. IP Address Use in Phishing

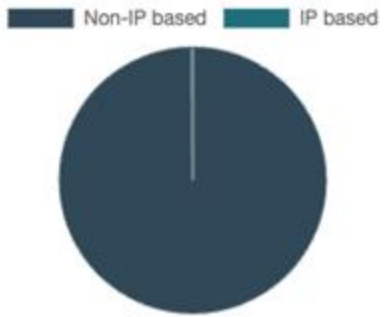
This indicator explores what percentage of reported phishing URLs rely directly on the use IP addresses.

Percentage of reported phishing URLs that use IP addresses in the last month/30 days

Percentage

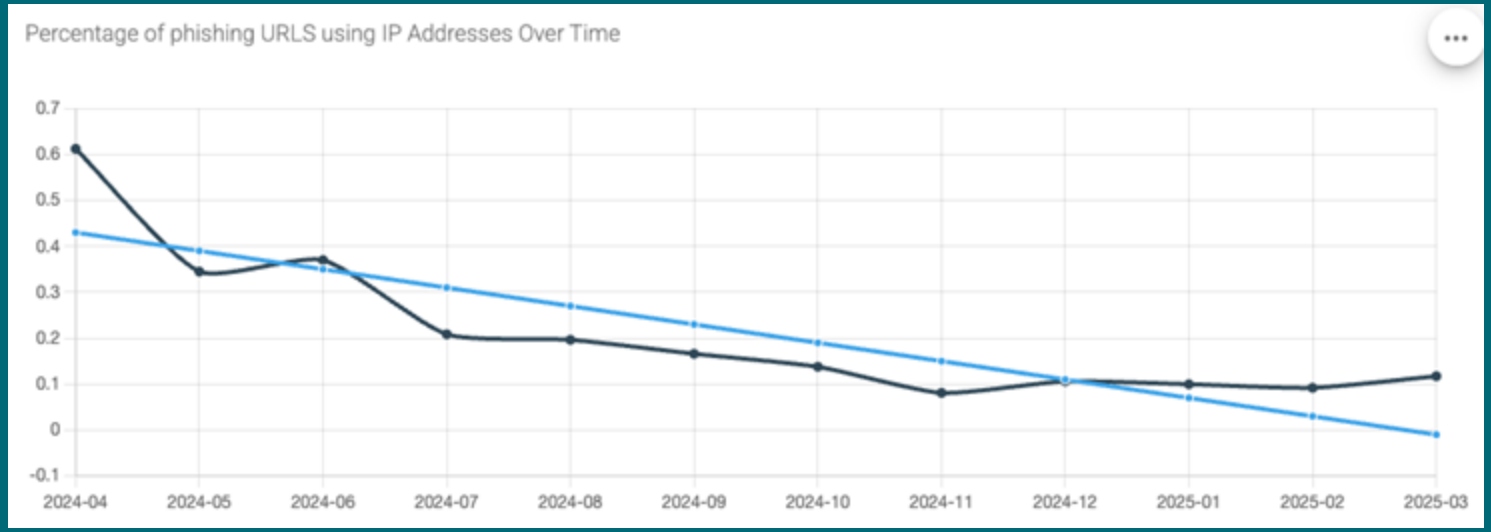
0.1207

Percentage of reported phishing URLs that use IP addresses in the last month/30 days



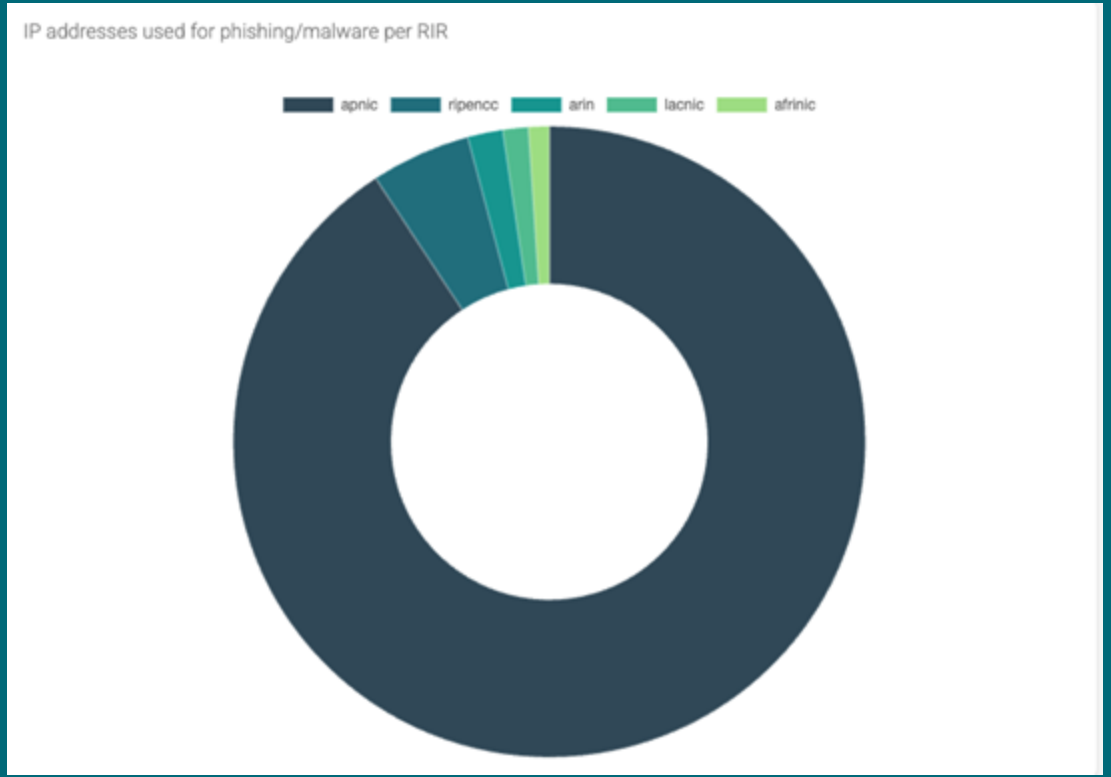
Indicator 2. IP Address Use in Phishing

This indicator explores what percentage of reported phishing URLs rely directly on the use IP addresses.



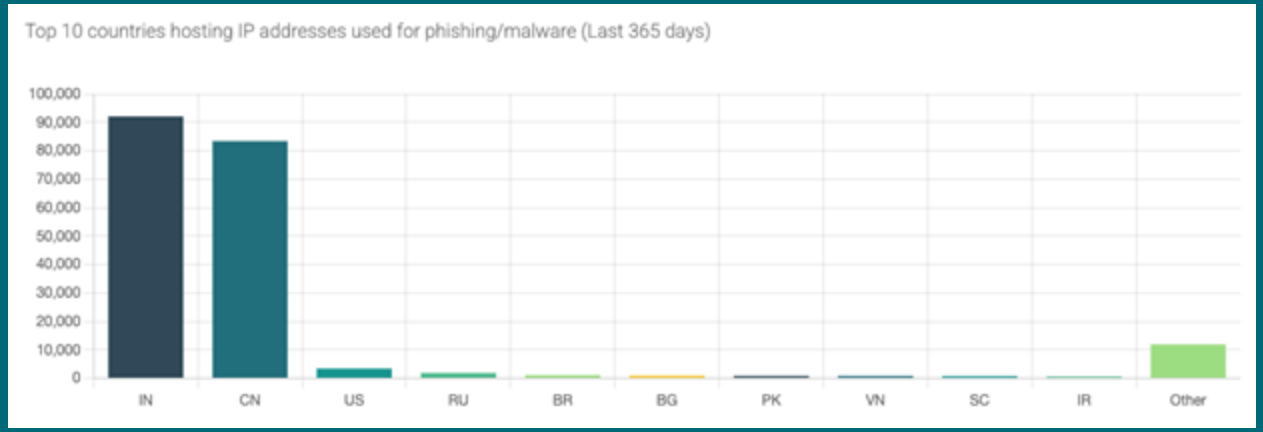
Indicator 3: Geographic Analysis based on hosting Autonomous System

This last indicator looks at the geographic location of IP addresses being used for malicious purposes. The indicator considers the location of the Autonomous System or entity hosting the abused IP address.



Indicator 3: Geographic Analysis based on hosting Autonomous System

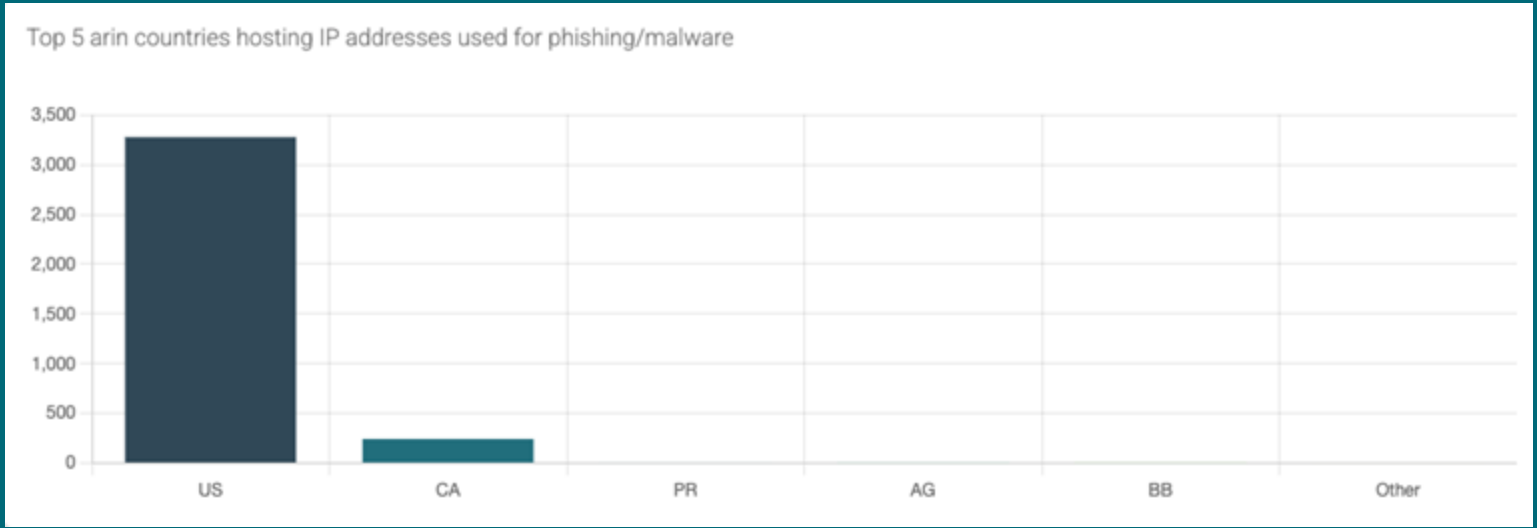
This last indicator looks at the geographic location of IP addresses being used for malicious purposes. The indicator considers the location of the Autonomous System or entity hosting the abused IP address.



DNS RESEARCH FEDERATION

Indicator 3: Geographic Analysis based on hosting Autonomous System

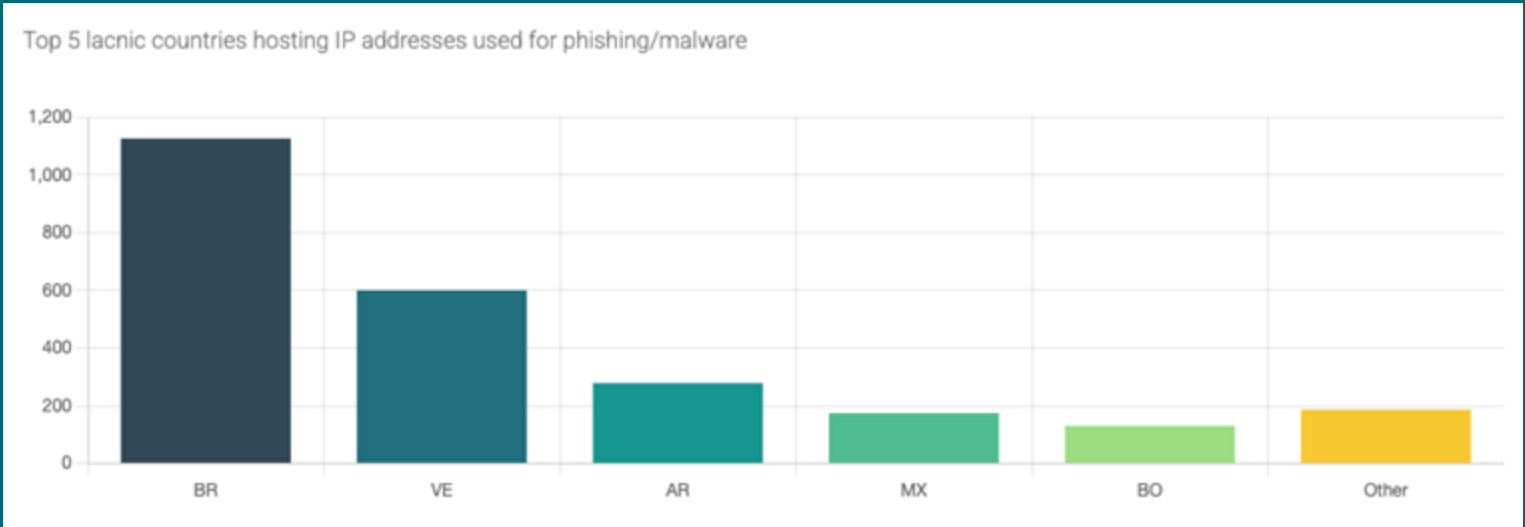
ARIN Focus



DNS RESEARCH FEDERATION

Indicator 3: Geographic Analysis based on hosting Autonomous System

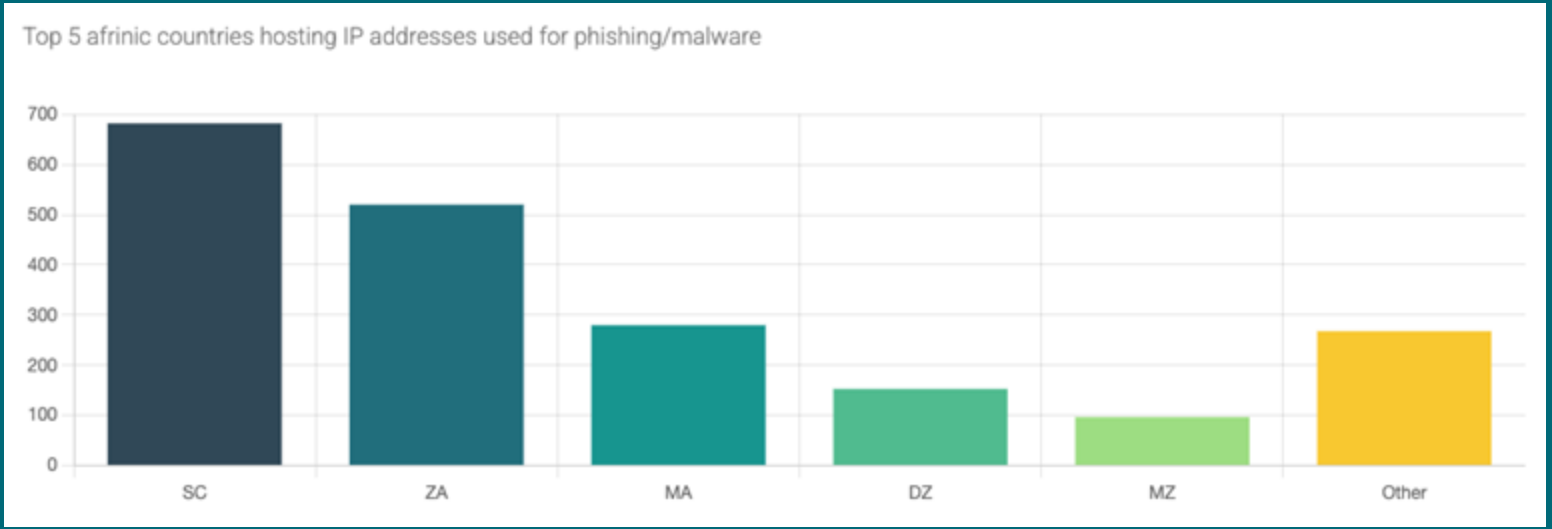
LACNIC Focus



DNS RESEARCH FEDERATION

Indicator 3: Geographic Analysis based on hosting Autonomous System

AFRINIC Focus



DNS RESEARCH FEDERATION

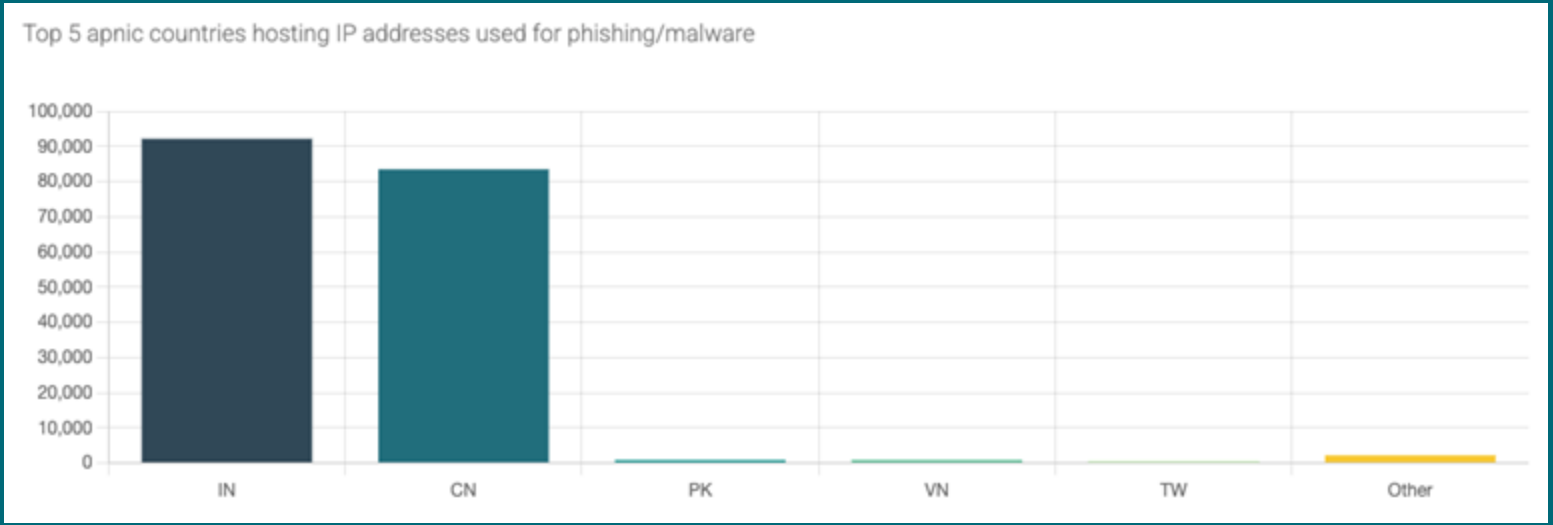
Indicator 3: Geographic Analysis based on hosting Autonomous System

RIPE NCC Focus

DNS RESEARCH FEDERATION

Indicator 3: Geographic Analysis based on hosting Autonomous System

APNIC Focus



DNS RESEARCH FEDERATION

Summary

- Malware IP Address Abuse is significant and on the rise
- AP region accounts for majority of reported IP based abuse
- Country results may benefit from scaled metric based on population size vs. absolute numbers.