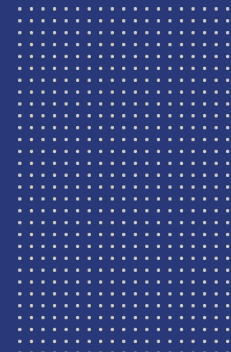




DNS Abuse in LAC region

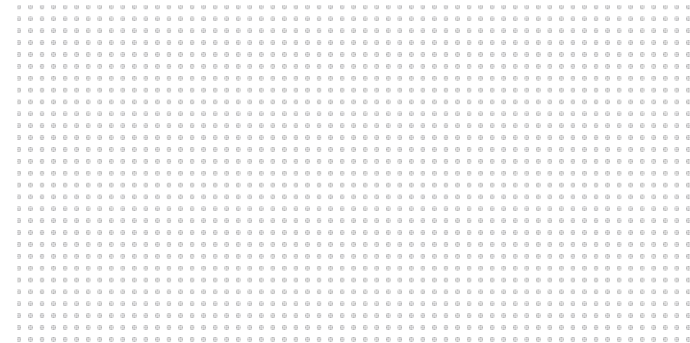
NetBeacon MAP

Rowena Schoo, Director – Policy & Programs



Today

- *Short* intro to the Institute & NetBeacon MAP
- Explore data from the LAC region compared to other regions
- Trends in the LAC regions
- Wrapping up and resources available



The NetBeacon Institute

Created in 2021 by Public Interest Registry (.ORG) in service of its non-profit mission (formerly: The DNS Abuse Institute)

Functionally separate from the operation of the registry

Graeme: Executive Director – 12 years of DNS industry experience, 4 years as Chair of the Registrar Stakeholder Group

Rowena: Director of Policies and Programs – Nominet (.UK), Ofcom, UK Gov

Everything we do is **free**

Mission: Reduce DNS Abuse.

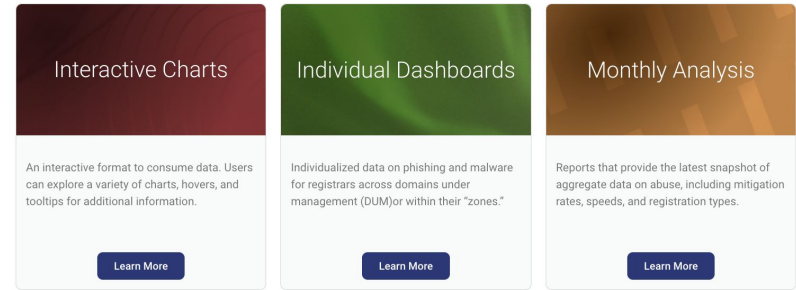
NetBeacon MAP: What

Intended to inform our activities and empower the community with data. [More...](#)

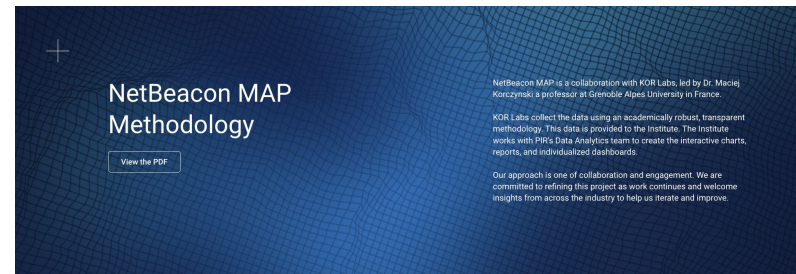
Principles:

- Transparency
- Credibility and independence
- Accuracy and reliability

Collaboration with KOR Labs -
Grenoble University

Three feature cards are displayed in a row. Each card has a colored header, a title, a description, and a 'Learn More' button.

- Interactive Charts** (Red header): An interactive format to consume data. Users can explore a variety of charts, hovers, and tooltips for additional information.
- Individual Dashboards** (Green header): Individualized data on phishing and malware for registrars across domains under management (DUM) or within their "zones."
- Monthly Analysis** (Orange header): Reports that provide the latest snapshot of aggregate data on abuse, including mitigation rates, speeds, and registration types.

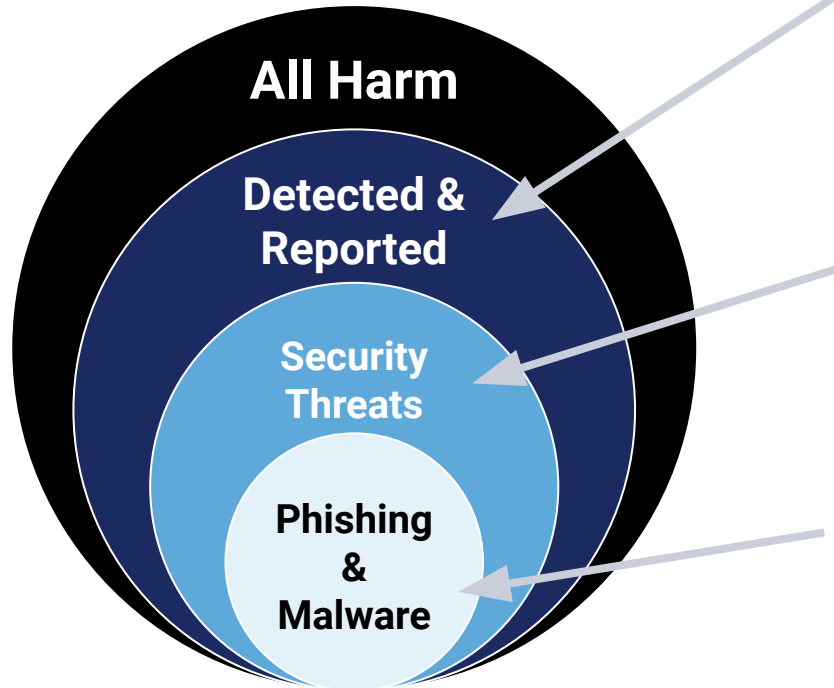
A slide titled 'NetBeacon MAP Methodology' with a blue grid background. It includes a 'View the PDF' button and text describing the collaboration with KOR Labs and the methodology used for data collection and analysis.

NetBeacon MAP is a collaboration with KOR Labs, led by Dr. Maciej Korczynski a professor at Grenoble Alpes University in France.

KOR Labs collect the data using an academically robust, transparent methodology. This data is provided to the Institute. The Institute works with PRIC Data Analytics team to create the interactive charts, reports, and individualized dashboards.

Our approach is one of collaboration and engagement. We are committed to refining this project as work continues and welcome insights from across the industry to help us iterate and improve.

What do we measure?



We can only measure what gets **reported** (“iceberg” principle)

Not all reports are Security Threats and are outside of our scope

Focus on security threats we (KOR Labs) can **currently** **reliably evidence**

Input

APWG
PhishTank
OpenPhish
URLHaus

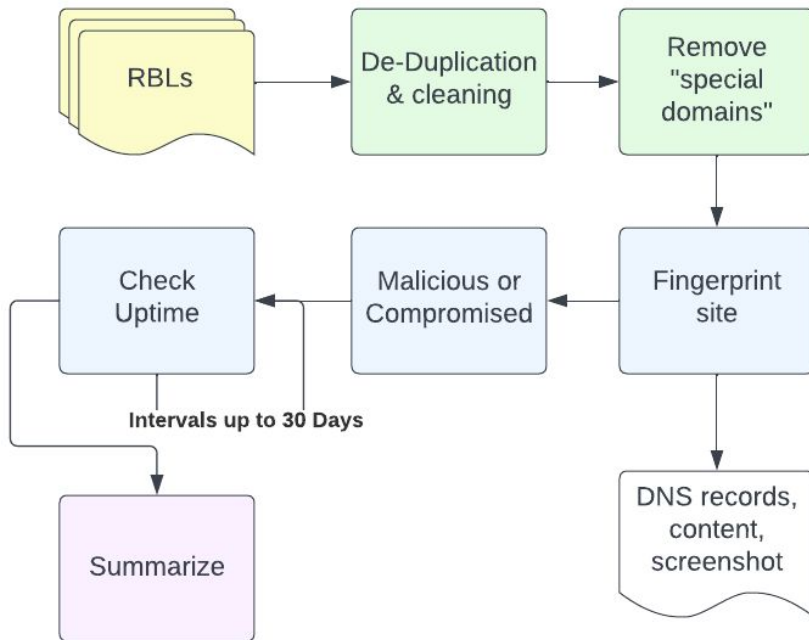
Analysis

Evidence collection
Registration type
Mitigation:
Minutes: 5,15,30.
Hour: 1,2,3,4,5,6,
Days: every 12h for
30 days.

Editorial

Monthly
Abuse 100K DUM
Exclusions*
Consistency &
redaction*
Malicious*

MAP: How?



[Methodology](#) & [Report on Measurement](#)

* applies only to public reporting

Cleaning

Measure:

- Unique domain names (E.g. 70K+ URLs)

Remove IP addresses and **“special domains”**:

- URL shorteners (e.g., bitly.com)
- Subdomain providers, for example, dynamic DNS providers (e.g., duckdns.org),
- file sharing services (e.g., docs.google.com)

Special Domains list is publicly available (methodology). You can help us update this.

Caveats

- We know this isn't perfect, best efforts. Even the best feeds can have false positives
- Optimizes accuracy over coverage; best for comparisons between peers/over time
- Potential geographical/language bias in lists
- Today: an exploration in regional reporting
 - **TLDs** as a proxy for regions; reality is more complex
 - **Raw numbers** (unique domains), not normalized for abuse per 100,000 DUM

Abuse by ccTLD region: phishing & malware

ICANN Geographic Regions

AF = Africa

AP = Asia/Australia/Pacific

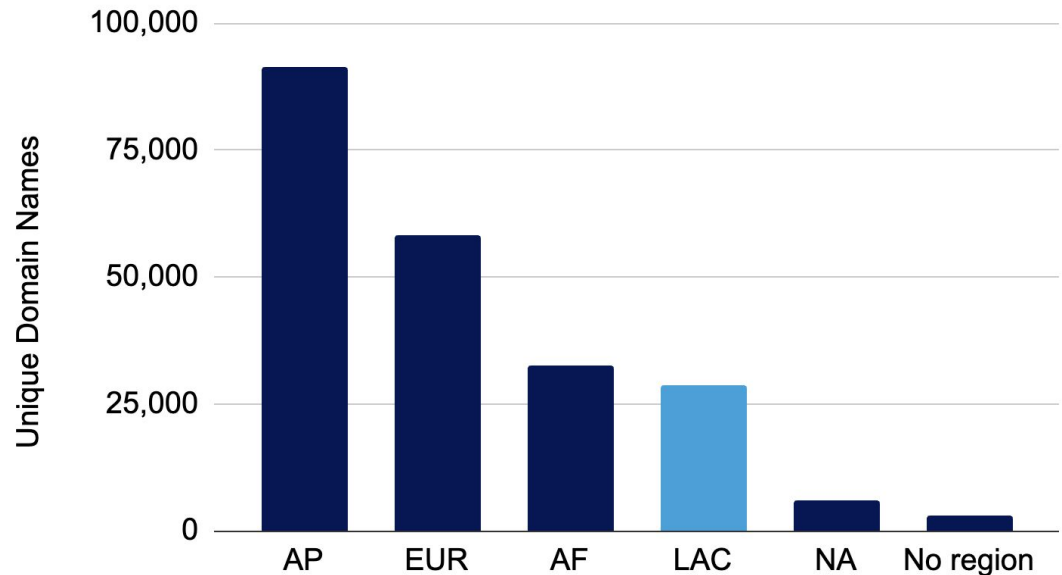
EUR = Europe

LAC = Latin America/ Caribbean

NA = North America

*Note: 'No region' unmapped
in [ICANN](#) e.g. IDNs, .su, .gb, .tp

May 2022 - July 2024



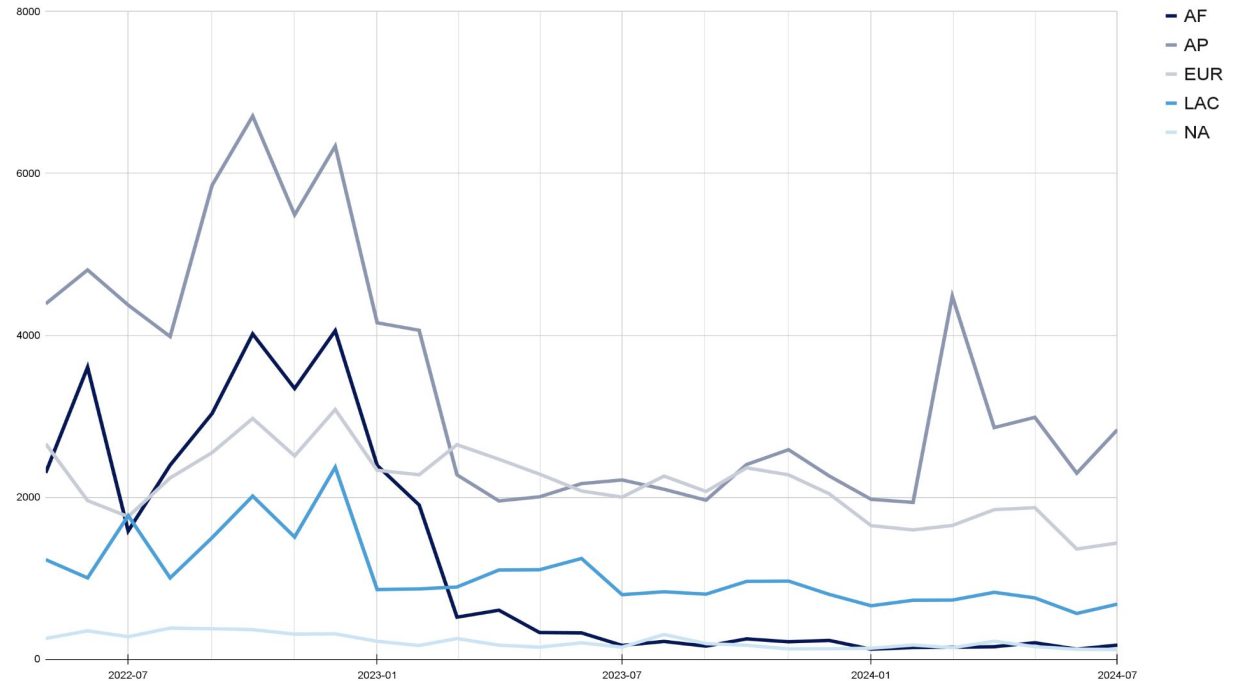
Phishing & Malware Trends

Unique Domain Names

May 2022 - July 2024

LAC: fairly stable, slight downward trend. Similar to **EUR**.

Not as much as **AP** (top grey) and **AF** (dark blue). **NA** trends along the bottom. Note: ccTLDs only.



AF = Africa, **AP** = Asia/Australia/Pacific, **EUR** = Europe, **LAC** = Latin America/ Caribbean, **NA** = North America

DUM Over Time

LAC: fairly stable, slight upward trend. Similar to **EUR**.

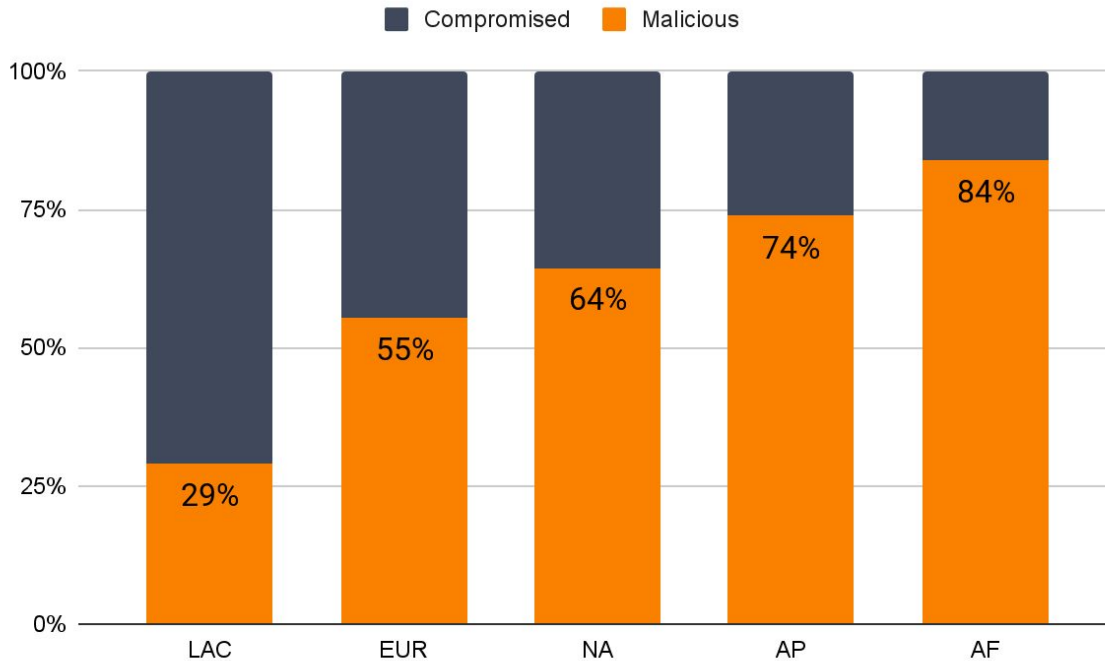
Dips in **AP** (middle grey)

NA trends along the bottom. Note: ccTLDs only.

Big drop for **AF** (dark blue). Freenom?



Type of registration

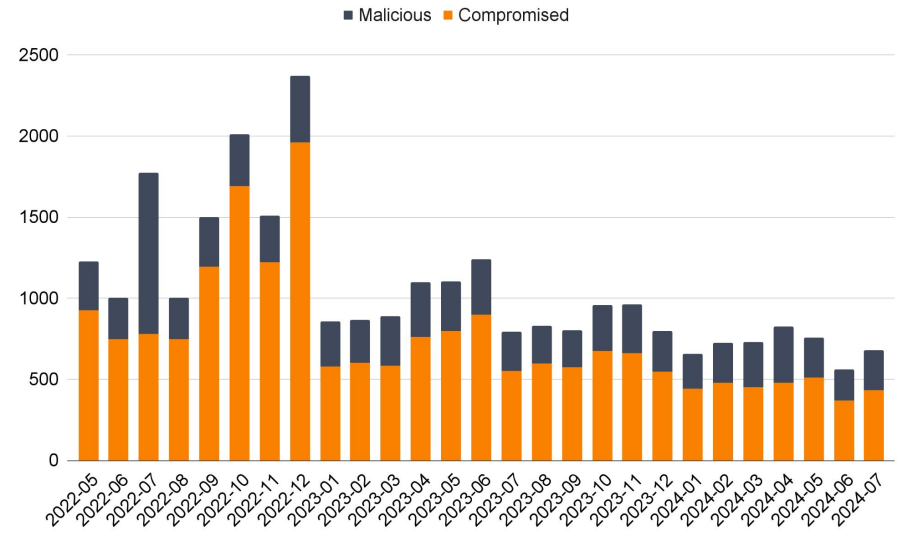
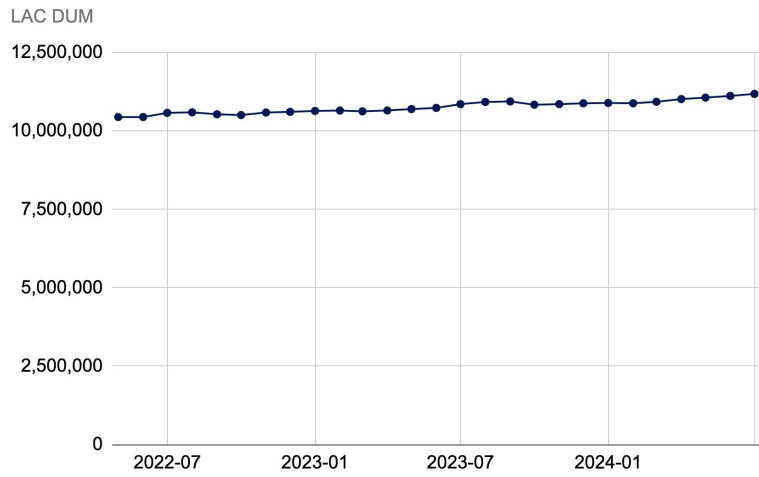


Malicious: appears to be registered for the purpose of phishing and malware.

Compromised: Otherwise benign registration which has been compromised, usually at the website CMS level.

LAC: lowest proportion of malicious registrations.

Trends over time: LAC

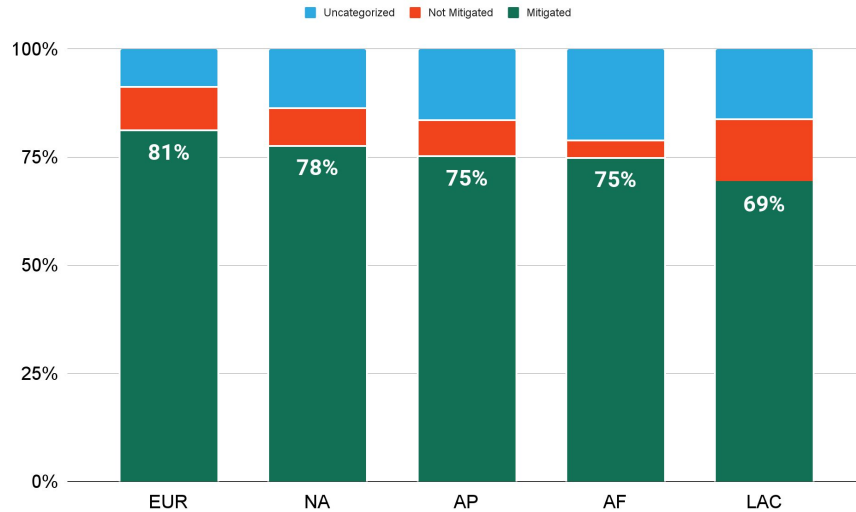


While DUM increased over this 2 year period (~1M)

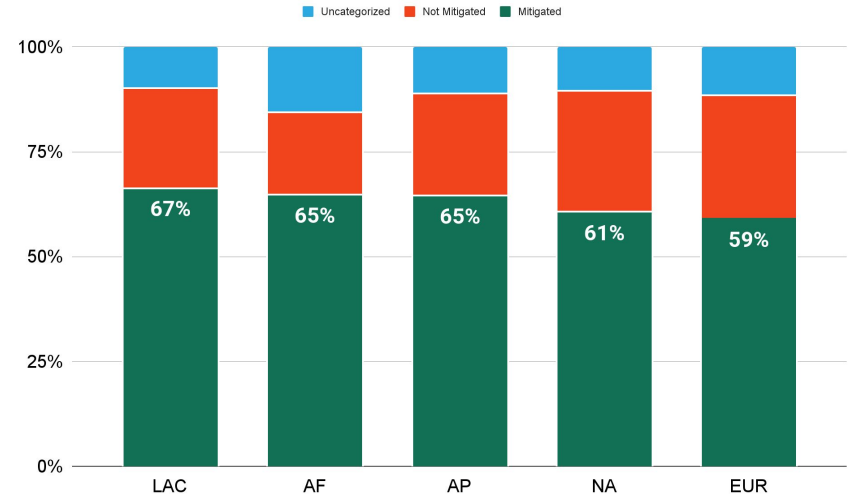
It looks like phishing and malware is trending down for the region. Proportion of Compromised v Malicious seems consistent.

Mitigation

Malicious

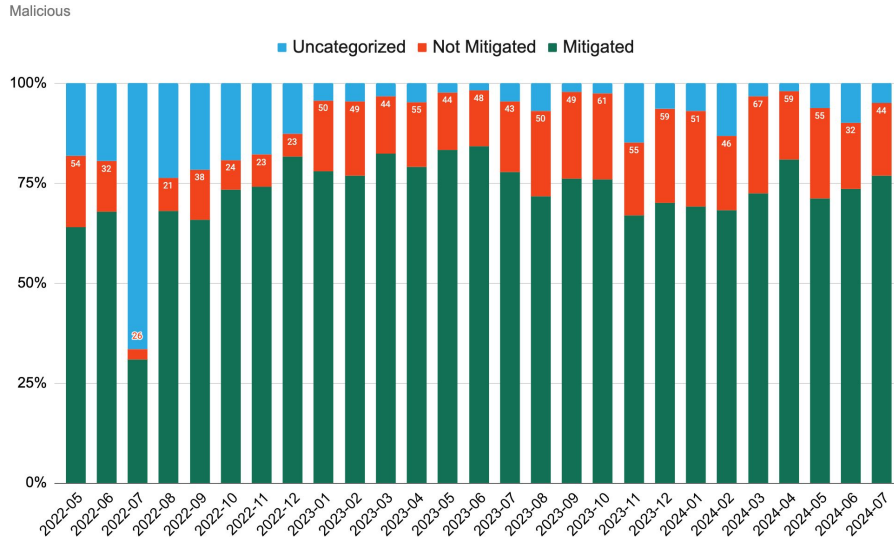


Compromise

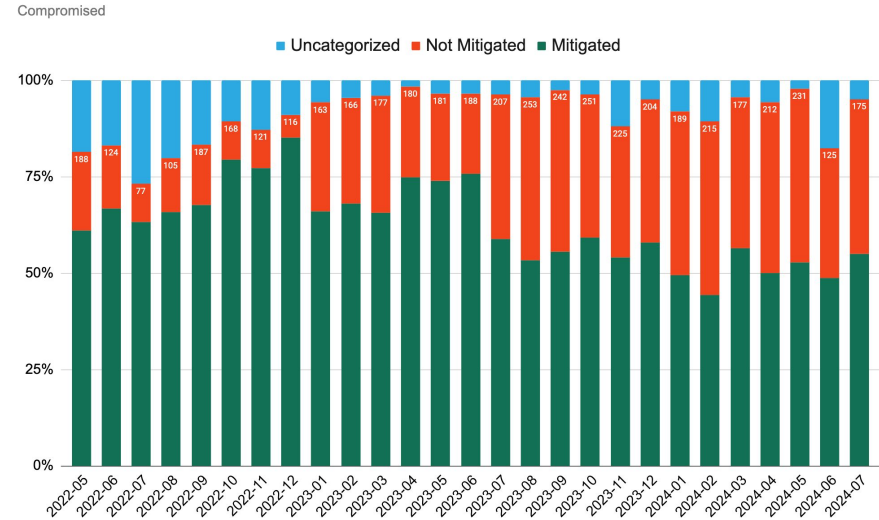


Mitigation: Malicious (LAC)

Malicious



Compromise



Wrapping up

- LAC ccTLDs do not stand out as a problematic region. Your abuse rate (phishing and malware) appears to be trending down while your DUM is growing.
- Every TLD and registrar should dive into their own data with a [free individual dashboard](#)
- Educational tools and articles:
 - E.g. [A Holistic Approach to Tackling DNS Abuse](#) or [Fraud prevention for retail registrars](#)
- You can receive reports through [NetBeacon Reporter](#)

Thank you! Gracias!



Update on IWF Program

- Since launching in February of this year:
 - 43 additional TLDs are now enrolled and covered by the programs
 - 18 registry operators (several have multiple TLD portfolios)
 - More than 35M domains now covered that were not previously receiving IWF alerts
- Includes several many ccTLD registry operators
- Includes “Domain Alerts” and the “TLD Hopping List”
- These programs are free to registries to use
- To sign up visit: <https://www.iwf.org.uk/membership/iwf-domain-services/>



PIR Proprietary

