DNS Abuse & NetBeacon Institute

Rowena Schoo, Director - Programs & Policy

Today

- About the Institute
- DNS Abuse & policy
- NetBeacon: Free products & services
- Q&A

- Sobre el Instituto
- Abuso y política de DNS
- NetBeacon: Productos y servicios gratuitos
- Preguntas y respuestas

All translation is courtesy of Google: treat with caution

About

Created in 2021 by Public Interest Registry (.ORG) in service of its nonprofit mission

- An initiative within PIR, with operational separation from the registry
- Non commercial: all services are completely free and always will be

Vision: A Safer Internet for Everyone.

Mission: To provide a world class, comprehensive, free suite of tools to create a safer Internet

Creado en 2021 por Public Interest Registry (.ORG) en cumplimiento de su misión sin fines de lucro.

- Una iniciativa dentro de PIR, con separación operativa del registro.
- Sin fines comerciales: todos los servicios son completamente gratuitos y siempre lo serán.

Visión: Una internet más segura para todos.

Misión: Proporcionar un conjunto de herramientas gratuito, integral y de primera clase para crear una internet más segura.

DNS Abuse

- Phishing
- Pharming
- Malware
- Botnets
- Spam*

*when used as a delivery mechanism

As defined in SAC115

Website Content Abuse

- Child Sexual Abuse Material (CSAM)
- Controlled substances & regulated goods
- Violent Extremist Content
- Hate speech
- Extremist content
- IP infringement

Voluntary Framework to Address Abuse

Abuso de DNS

- Phishing
- Pharming
- Malware
- Botnets
- Spam*

*Cuando se utiliza como mecanismo de entrega

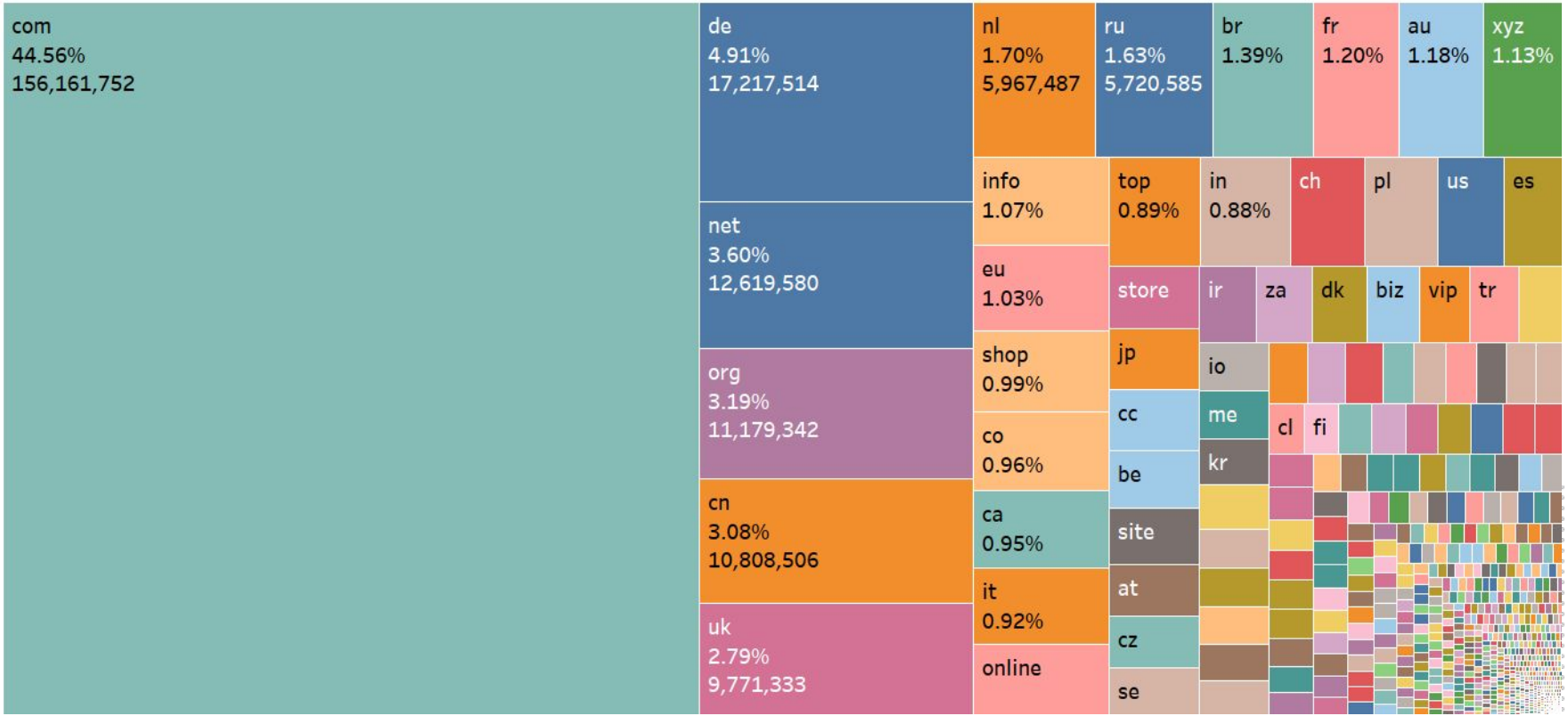
Según la definición de SAC115

Abuso de contenido del sitio web

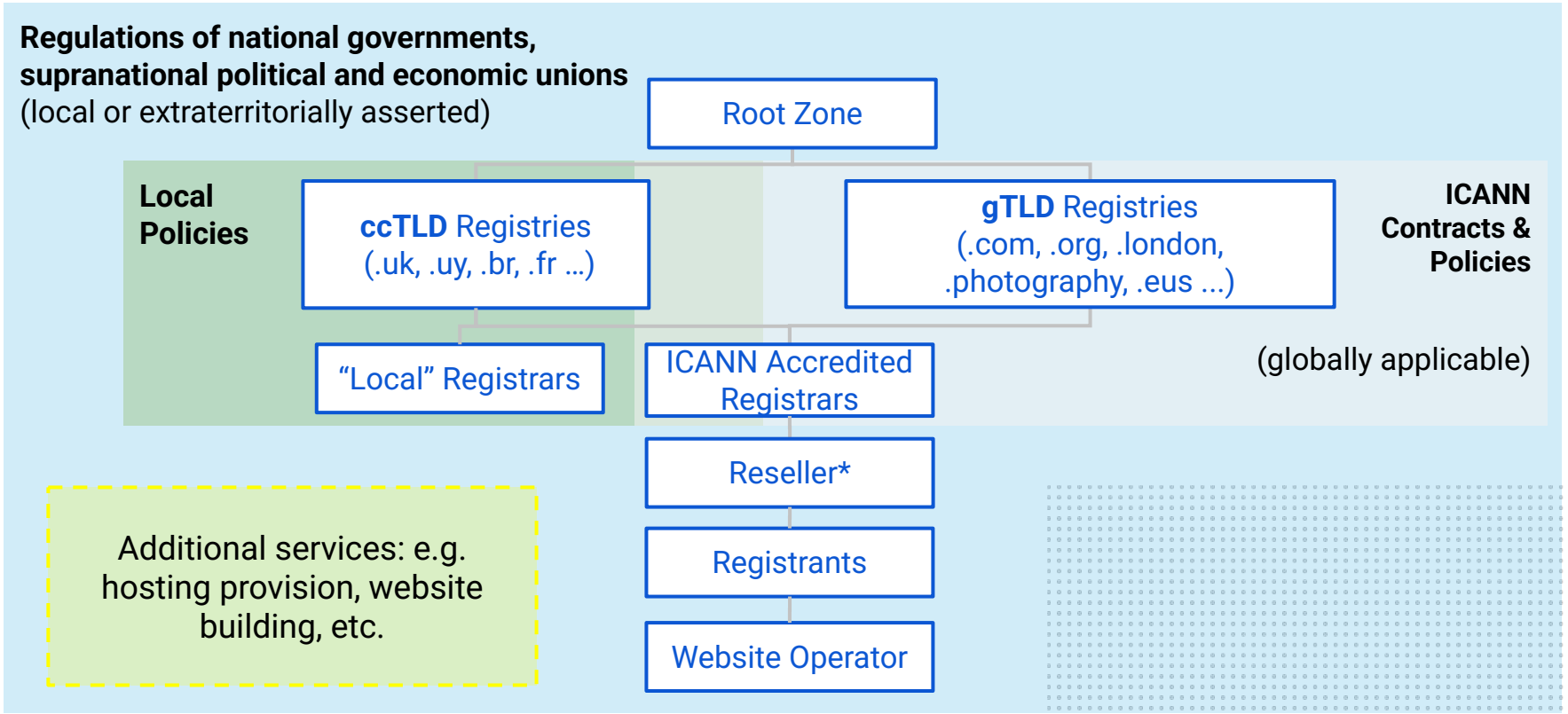
- Material de abuso sexual infantil (MASI)
- Sustancias controladas y productos regulados
- Contenido extremista violento
- Incitación al odio
- Contenido extremista
- Violación de la propiedad intelectual

Voluntary Framework to Address Abuse

Top Level Domain (TLD) Ecosystem



Policy: Domain Names



*not always present

This means:

- **Domain names ≠ ‘the Internet’.** Registries & registries typically do not host content & therefore cannot delete content. Other important entities include: hosting providers, platforms, users.

- **ICANN gTLD policy must focus on a global ‘floor’** which is content neutral, technical practicable, geopolitically palatable and developed through multi-stakeholder input.

- Local regulations tend to be more specific and reflect values, norms, expectations.

- Global interconnected economy means these things can sometimes collide.

- **Nombres de dominio ≠ «Internet».** Los registros no suelen alojar contenido y, por lo tanto, no pueden eliminarlo. Otras entidades importantes incluyen: proveedores de alojamiento, plataformas y usuarios.

- La política de gTLD de la ICANN debe centrarse en un mínimo global neutral en cuanto al contenido, técnicamente viable, geopolíticamente aceptable y desarrollado mediante la participación de múltiples partes interesadas.

- Las regulaciones locales tienden a ser más específicas y reflejan valores, normas y expectativas.

- La economía global interconectada implica que estos elementos a veces pueden colisionar.

DNS Abuse

Means: Phishing, Pharming, Malware, Botnets, Spam* (*when used as a delivery mechanism): As defined in SAC115

Why? Mitigation In the case of a well evidenced maliciously registered domain name, it's typically appropriate to mitigate these harms at the DNS level, as it's: **Effective** - globally, **Quick, Simple, Cost Effective, Necessary.**

Typically the DNS is not appropriate for mitigation action on website content because it's not **Precise** or **Proportionate**. Often not **Effective** - the content still exists and can be reconnected to another domain name.

Medios: Phishing, pharming, malware, botnets, spam* (*cuando se utiliza como mecanismo de entrega): Según la definición de SAC115.

¿Por qué? Mitigación
En el caso de un nombre de dominio registrado con fines maliciosos y con pruebas sólidas, es relativamente apropiado mitigar estos daños a nivel de DNS, ya que es: efectivo a nivel global, rápido, simple, rentable y necesario.

Dependiendo del contenido del daño:
Normalmente, el DNS no es adecuado para mitigar el contenido de un sitio web porque no es preciso ni proporcionado. A menudo, no es eficaz: el contenido sigue existiendo y puede reconectarse a otro nombre de dominio.

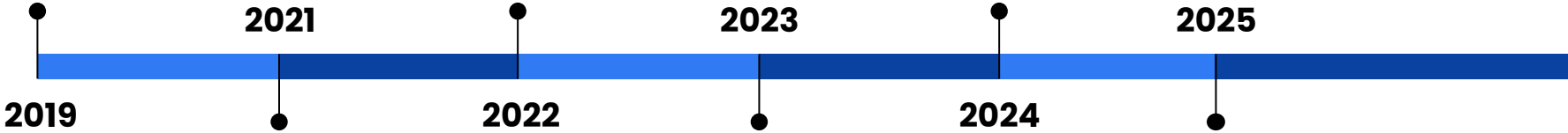
https://netbeacon.org/dns-abuse-definition-attributes-of-mitigation/

Framework to Address DNS Abuse
Leading registrars and registries create an industry wide voluntary commitment.

NetBeacon Reporter launched to simplify reporting

NetBeacon MAP launched to improve measurement.

New gTLD contracts come into effect. ICANN begins enforcement.



NetBeacon Institute created
Originally called the DNS Abuse Institute

gTLD Contract Amendments
Registries and Registrars vote in favour of creating a mitigation requirement for DNS Abuse.

NB Institute **White Paper** setting out policy proposals for addressing DNS Abuse.

gNSO Small Team publishes gap report. New policy development starts… approved by the gNSO Council → Issue Report

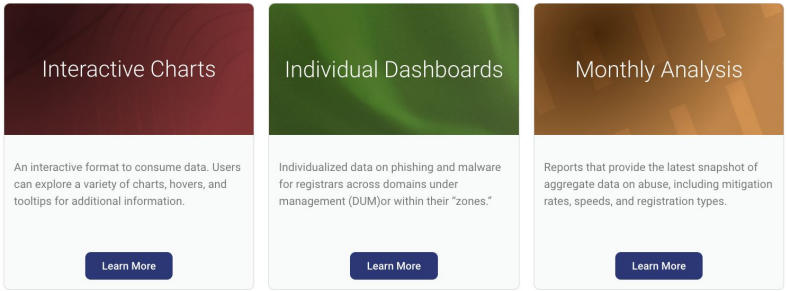
NetBeacon MAP:

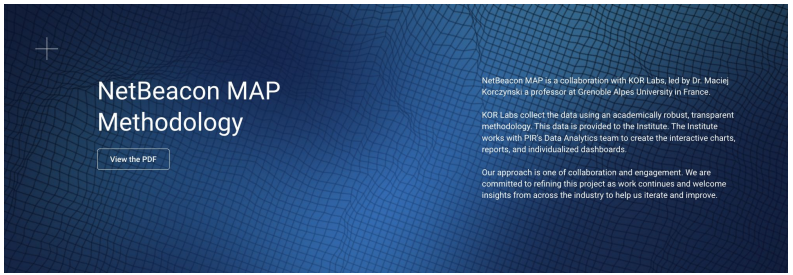
Inform our activities and empowers the community with data. Includes free dashboards. More

Principles:

- Transparency
- Credibility and independence
- Accuracy and reliability

Measures the use of the DNS for phishing and malware, whether the domain is maliciously registered, and whether mitigation has taken place.



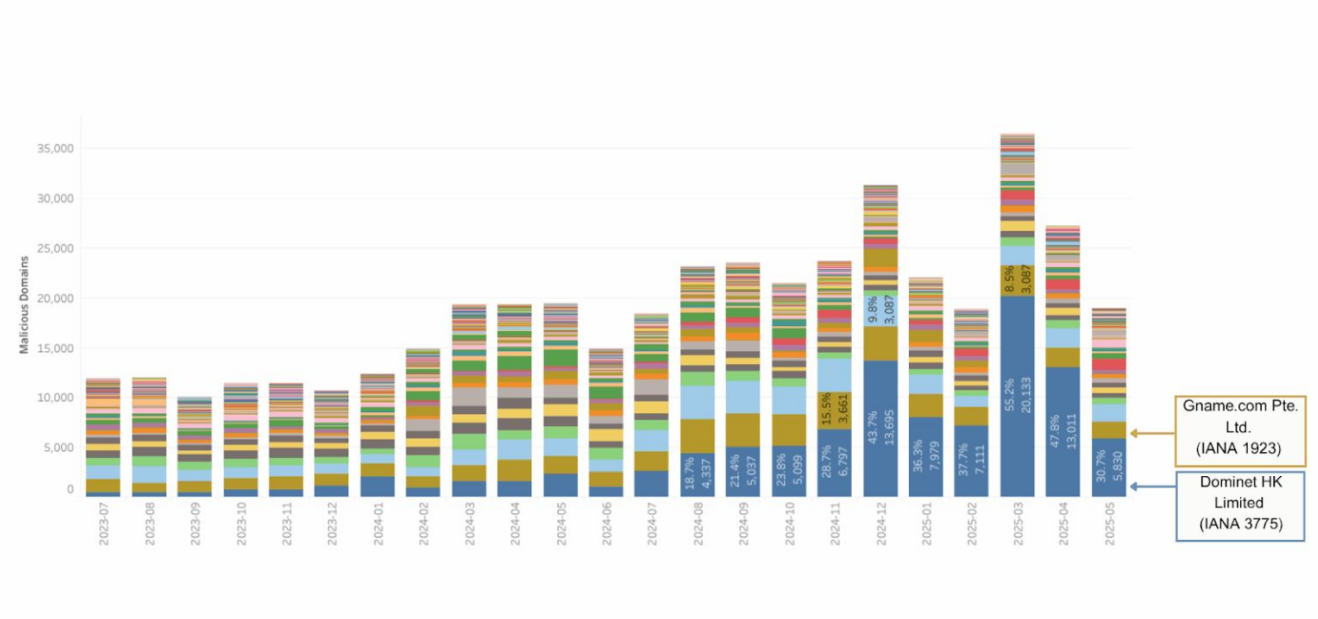


Collaboration with KOR Labs - Grenoble Aples University, France

Malicious Phishing Using Domains Names

Is not evenly distributed across registrars or TLDs.

It's distribution is different to that of domains.



https://netbeacon.org/recent-spike-in-malicious-phishing-concentrated-in-two-registrars/

NetBeacon Reporter

Built to solve two problems:

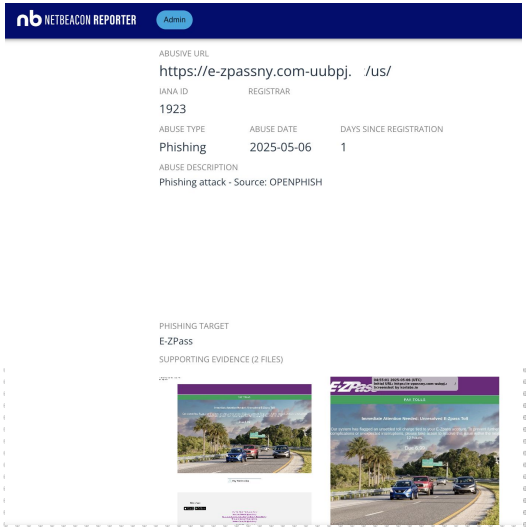
- **Submitters**: Navigating the entire DNS ecosystem, which can be complex, onerous, confusing, and extremely difficult to scale.
- **Recipients**: Improves the quality and actionability of reports registrars/hosts receive by reducing duplication, attaching evidence, and avoiding incomplete or misdirected reports.

NetBeacon Reporter

A free, easy to use, centralized abuse reporting system

- Accepts reports from anyone, via form or API
- Standardizes and enriches reports
- Automatically distributes to ICANN accredited registrars, participating TLDs, and web hosts
- 20,000 phishing reports a month
- Monitoring results, capturing feedback
- ccTLDs can integrate as partners

https://netbeacon.org/cctld-partners/



Education

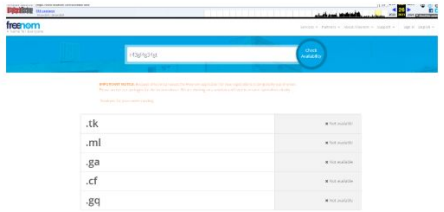
Free resources and information.

E.g. Template Abuse Policy, summarising ICANN activities, sharing bespoke analysis.

Recent spike in malicious phishing concentrated in two registrars

Summary Record Highs in NetBeacon MAP Data In March 2025 we observed two record highs in NetBeacon Measurement and Analytics Platform (MAP) data: the highest number of unique domain names associated with phishing (47,613), and the largest month-on-month increase in unique domain names associated with phishing (63%). See Figure 1: Aggregate Trends

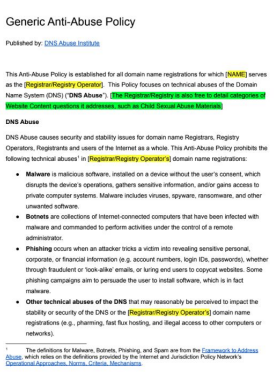
Read More »



How Did the Closure of Freenom Impact DNS Abuse Across the TLD Ecosystem?

Introduction Freenom, the domain name registrar and registry operator, received a great deal of attention in March 2023 when published reported noted that it had stopped allowing new registrations for the five country-code top level domains (ccTLDs) that it operated (.CF for the Central African Republic, .GA for Gabon, .GQ for Equatorial

Read More »



Generic Anti-Abuse Policy

Published by: DNS Abuse Institute

This Anti-Abuse Policy is established for all domain name registrations for which [NAME] serves as the [Registrar/Registry Operator]. This Policy focuses on technical abuses of the Domain Name System (DNS) ("**DNS Abuse**"). The Registrar/Registry is also free to detail categories of Website Content questions it addresses, such as Child Sexual Abuse Materials.

DNS Abuse

DNS Abuse causes security and stability issues for domain name Registrars, Registry Operators, Registrants and users of the Internet as a whole. This Anti-Abuse Policy prohibits the following technical abuses[1] in [Registrar/Registry Operator's] domain name registrations:

- **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.
- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.
- **Other technical abuses of the DNS** that may reasonably be perceived to impact the stability or security of the DNS or the [Registrar/Registry Operator's] domain name registrations (e.g., pharming, fast flux hosting, and illegal access to other computers or networks).

1 The definitions for Malware, Botnets, Phishing, and Spam are from the Framework to Address Abuse, which relies on the definitions provided by the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria, Mechanisms

GAC Communiqués and Community Activity on DNS Abuse

The DNS Abuse Institute launches a new level of reporting that reveals the spectrum of how malicious phishing and malware is distributed across the DNS registration ecosystem.

Read More »

NETBEACON INSTITUTE

Thank you! Muchas Gracias!

rowena@netbeacon.org
LinkedIn

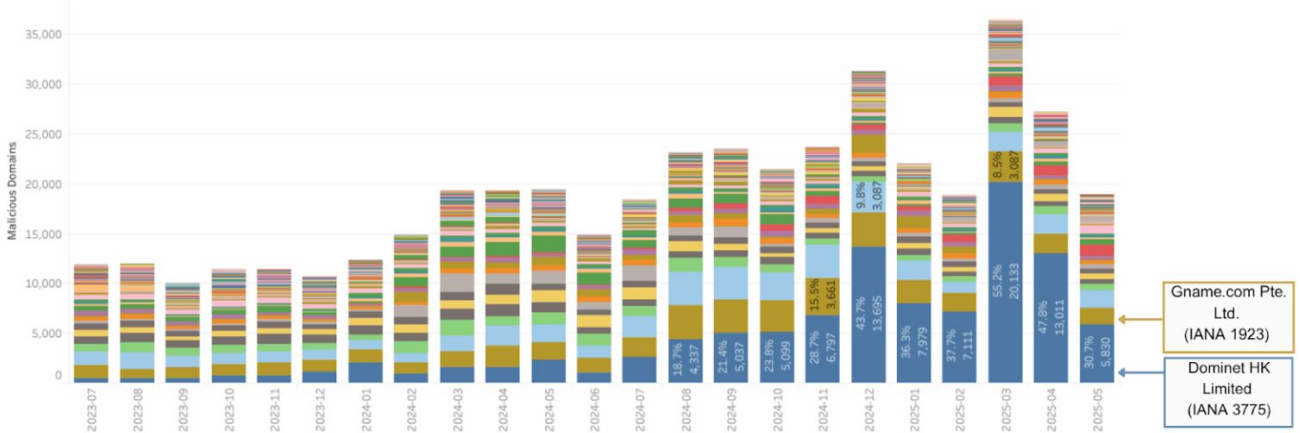
Appendix: Spanish

Only a Google Translation... treat with caution :-)

Phishing malicioso usando nombres de dominio

No se distribuye uniformemente entre registradores o TLD.

Su distribución es diferente a la de los dominios.



https://netbeacon.org/recent-spike-in-malicious-phishing-concentrated-in-two-registrars/

NetBeacon Reporter

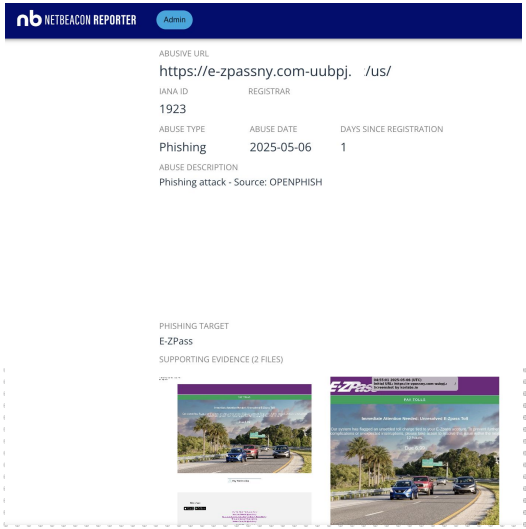
- Diseñado para resolver dos problemas:
  - **Remitentes**: Navegar por todo el ecosistema DNS, que puede ser complejo, oneroso, confuso y extremadamente difícil de escalar.

  - **Destinatarios**: Mejora la calidad y la procesabilidad de los informes que reciben los registradores/hosts al reducir la duplicación, adjuntar evidencia y evitar informes incompletos o mal dirigidos.

NetBeacon Reporter

- Un sistema centralizado, gratuito y fácil de usar para denunciar abusos.
- Acepta denuncias de cualquier persona, mediante formulario o API.
- Estandariza y enriquece los informes.
- Distribuye automáticamente a registradores acreditados por la ICANN, TLD participantes y proveedores de alojamiento web.
- 20 000 denuncias de phishing al mes.
- Supervisión de resultados y recopilación de comentarios.
- Los ccTLD pueden integrarse como socios.

https://netbeacon.org/cctld-partners/



Educación

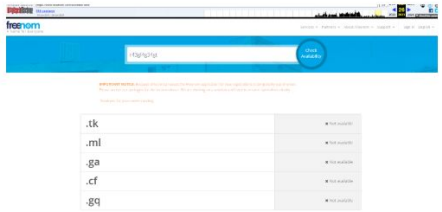
Recursos e información gratuitos. https://netbeacon.org/resources/

Por ejemplo, la Política de Abuso de Plantillas, el resumen de las actividades de la ICANN y el intercambio de análisis personalizados.

Recent spike in malicious phishing concentrated in two registrars

Summary Record Highs in NetBeacon MAP Data In March 2025 we observed two record highs in NetBeacon Measurement and Analytics Platform (MAP) data: the highest number of unique domain names associated with phishing (47,613), and the largest month-on-month increase in unique domain names associated with phishing (63%). See Figure 1: Aggregate Trends

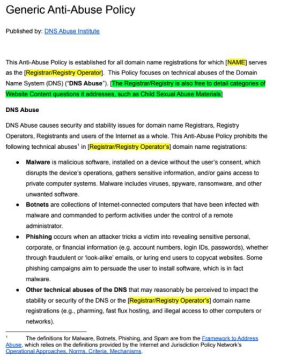
Read More »



How Did the Closure of Freenom Impact DNS Abuse Across the TLD Ecosystem?

Introduction Freenom, the domain name registrar and registry operator, received a great deal of attention in March 2023 when published reported noted that it had stopped allowing new registrations for the five country-code top level domains (ccTLDs) that it operated (.CF for the Central African Republic, .GA for Gabon, .GQ for Equatorial

Read More »



Generic Anti-Abuse Policy

Published by: DNS Abuse Institute

This Anti-Abuse Policy is established for all domain name registrations for which [NAME] serves as the [Registrar/Registry Operator]. This Policy focuses on technical abuses of the Domain Name System (DNS) ("**DNS Abuse**"). The Registrar/Registry is also free to detain categories of Website Content questions it addresses, such as Child Sexual Abuse Materials.

DNS Abuse

DNS Abuse causes security and stability issues for domain name Registrars, Registry Operators, Registrants and users of the Internet as a whole. This Anti-Abuse Policy prohibits the following technical abuses[1] in [Registrar/Registry Operator's] domain name registrations:

- **Malware** is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.
- **Botnets** are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.
- **Phishing** occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.
- **Other technical abuses of the DNS** that may reasonably be perceived to impact the stability or security of the DNS or the [Registrar/Registry Operator's] domain name registrations (e.g., pharming, fast flux hosting, and illegal access to other computers or networks).

1 The definitions for Malware, Botnets, Phishing, and Spam are from the Framework to Address Abuse, which relies on the definitions provided by the Internet and Jurisdiction Policy Network's Operational Approaches, Norms, Criteria, Mechanisms

GAC Communiqués and Community Activity on DNS Abuse

The DNS Abuse Institute launches a new level of reporting that reveals the spectrum of how malicious phishing and malware is distributed across the DNS registration ecosystem.

Read More »