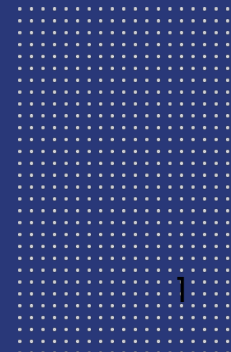




DNS Abuse Workshop

APTLD86

2024-09



Please Ask Questions

The NetBeacon Institute

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

Functionally separate from the operation of the registry

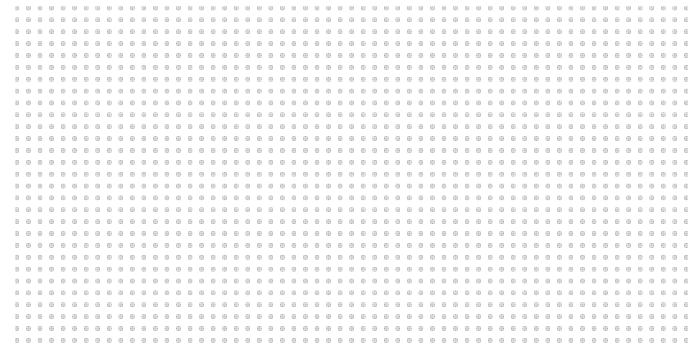
Graeme: Executive Director – 12 years of DNS industry experience, 4 years as Chair of the Registrar Stakeholder Group

Everything we do is **FREE**

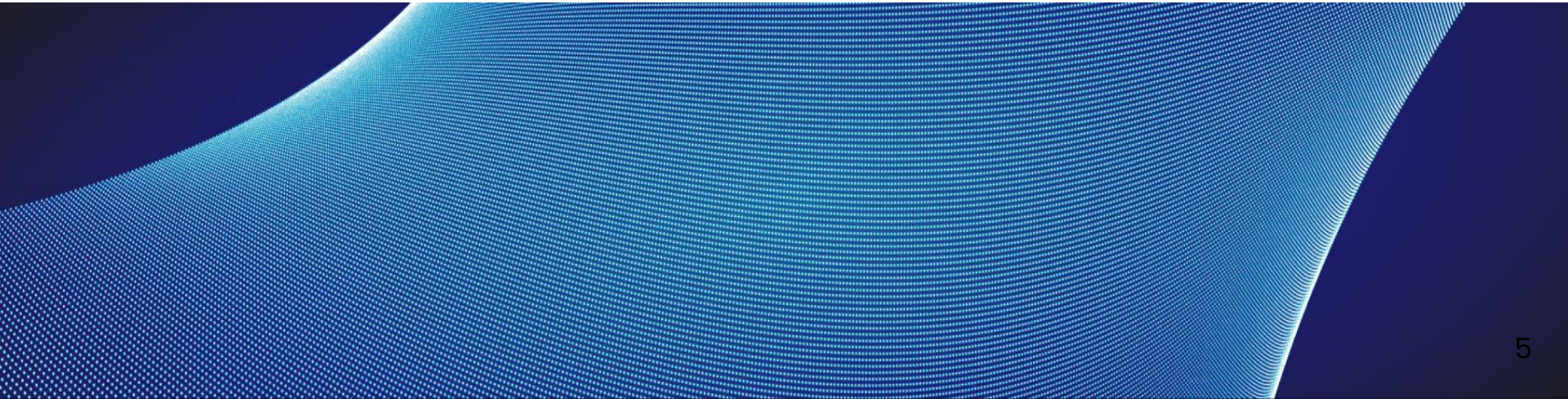
Mission: Reduce DNS Abuse.

Why is this Important for ccTLDs?

- gTLD changes may make ccTLDs more attractive for criminals
- Changes in technology make targeting smaller audiences cheaper and more effective
- Regulatory context is changing
- Registrars want homogeneity



What is DNS Abuse?



Why do we use the term DNS Abuse?

Every single person new to the discussion disagrees with both the name and the definition

Term – largely a settled term-of-art. No one is enamoured with it.

Definition – largely settled within ICANN community

Agreement that there is work to do on the current definition, and we can argue about the gray areas later

Gets to the core of what is typically appropriately mitigated at the DNS level

What is DNS Abuse?

“DNS Abuse means **malware, botnets, phishing, pharming, and spam** (when spam is used as a delivery mechanism for any of the other four types of DNS Abuse) as these terms are defined in Section 2.1 of the Security and Stability Advisory Committee Report on an Interoperable Approach to Addressing Abuse Handling in the DNS (SAC 115)”

[Advisory: Compliance With DNS Abuse Obligations in the Registrar Accreditation Agreement and the Registry Agreement](#)

Two Flavours:

Malicious registrations

A domain registered for malicious purposes (i.e., to carry out DNS Abuse).

Compromised websites

A benign domain name that has been compromised at the website, hosting, or DNS level.

Extremely important distinction

- Impacts mitigation and the assessment of collateral damage.
- Typically, compromised websites are **not** appropriately mitigated at the DNS level, they require a referral to the hosting provider or engagement with the registrant to close the vulnerability (~ 30% phishing, ~70% malware).
- Related to wider public policy cybersecurity hygiene.

Why phishing, malware, botnets, pharming, (and Spam)?

- In short: they are usually* appropriately addressed at the domain name level
 - Use a domain name
 - The harm is visible to a registrar
 - The harm is comprehensible to a registrar
 - Collateral damage is limited

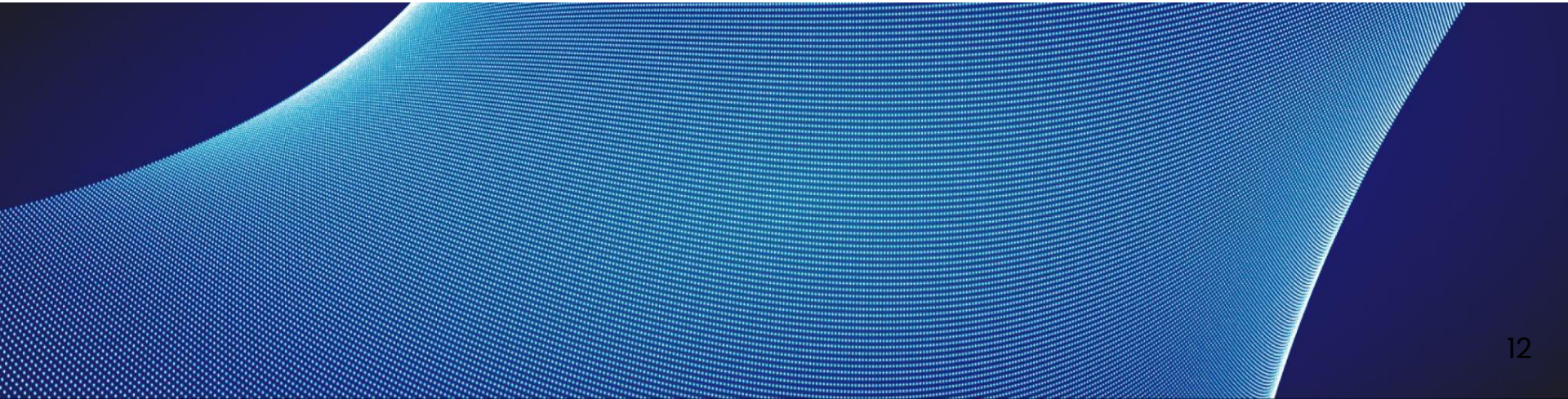
*Note: compromised websites

Appropriate Mitigation

Mitigation techniques ought to be:

- **Effective** – the harm is mitigated
- **Quick** – the mitigation can be implemented with due speed
- **Simple** – the harm can be mitigated without involving multiple layers, players, or technologies
- **Precise*** – there is a minimum of collateral damage
- **Proportional*** – the effort and scope of the mitigation is commensurate with the harm
- **Cost effective** – the cost of mitigation should be commensurate with the harm
- **Necessary** – other mechanisms for mitigation are not available

DNS Abuse Examples



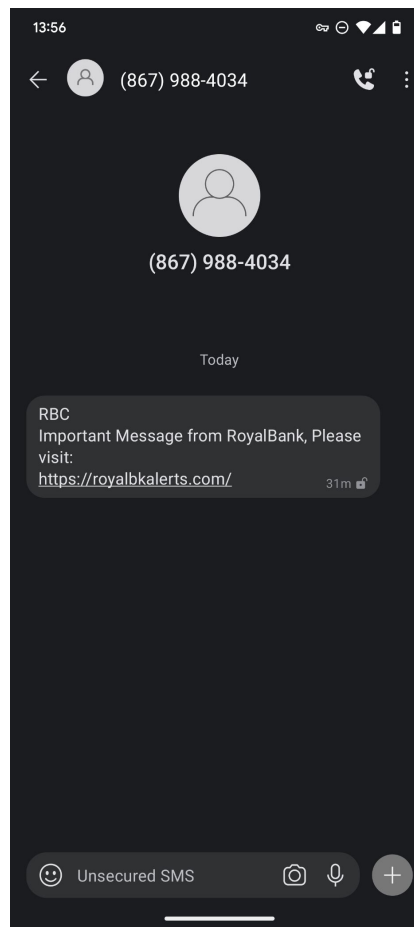
Phishing

- Deception in *identity*
- Attempt to capture sensitive information
- Emails, SMS, messages, website*
- Malicious: Login-payppal-service.tld

***Smishing** can also be included depending on if it involves a domain name

Phishing with a malicious domain

royalbkalerts[.]com



Your account are currently suspended.



Royal Bank

Your account has been suspended.

We have detected unusual activity on your account starting with 4519 0*** **** *****.

For your protection, we have temporarily placed your account on hold and any pending payments or deposits on hold as well.

Your account will remain on hold until we are able to confirm that you are the authorized owner of the payment method used in the recent transaction. To restore access to your account, sign in and follow the on-screen instructions.

Sign In

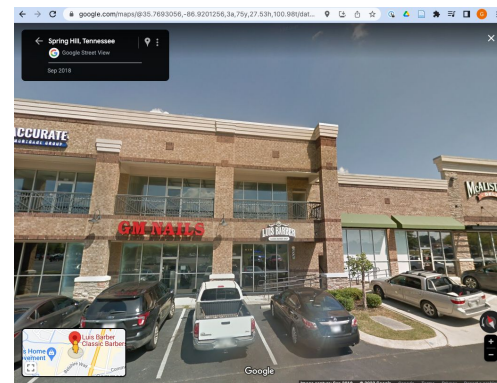
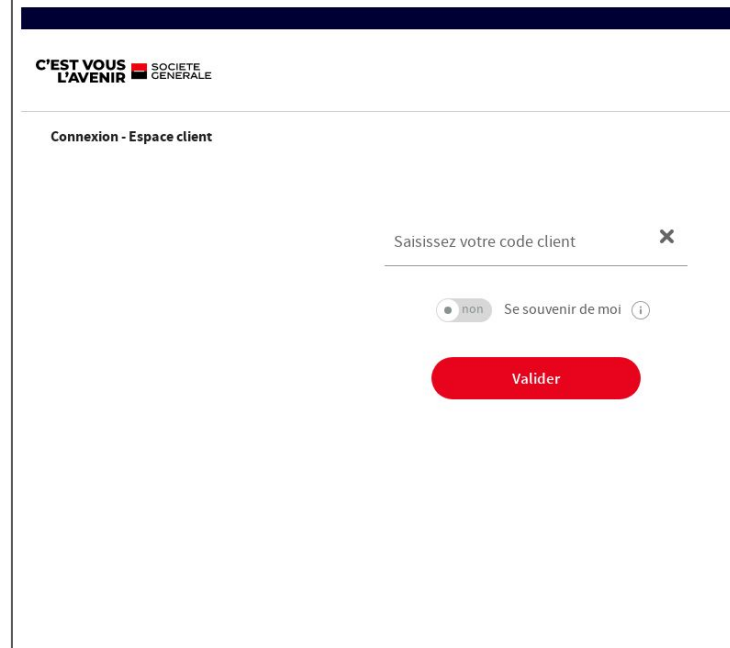
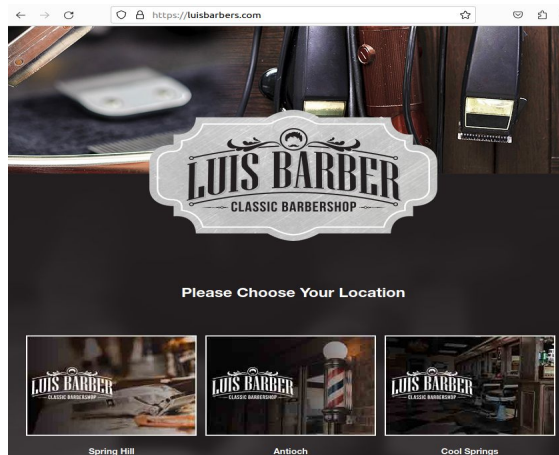
Once you have provided the required information, we will review it and respond within 24 hours.

We are sorry for any inconvenience this may have caused.

For further information, please refer to the [RBC Terms and Conditions](#).

Phishing with a compromised website

- <https://coolsprings.luisbarbers.TLD/dbs/sg/SG22/>
- Phishing at URL, not at domain root
- Benign content at domain
- Real business



DNS Abuse: Malware

Malicious software that may:

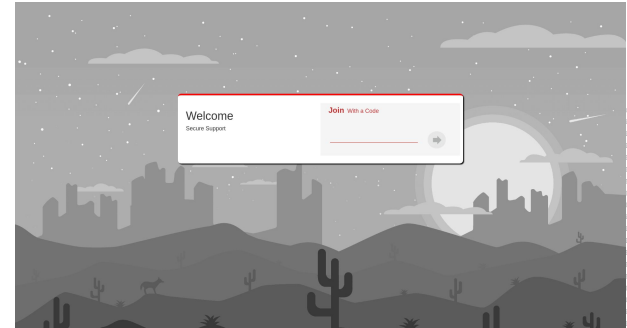
- Steal credentials
- Join device to a botnet
- Install ransomware*

Distributed via deceptive domains, compromised websites, and email



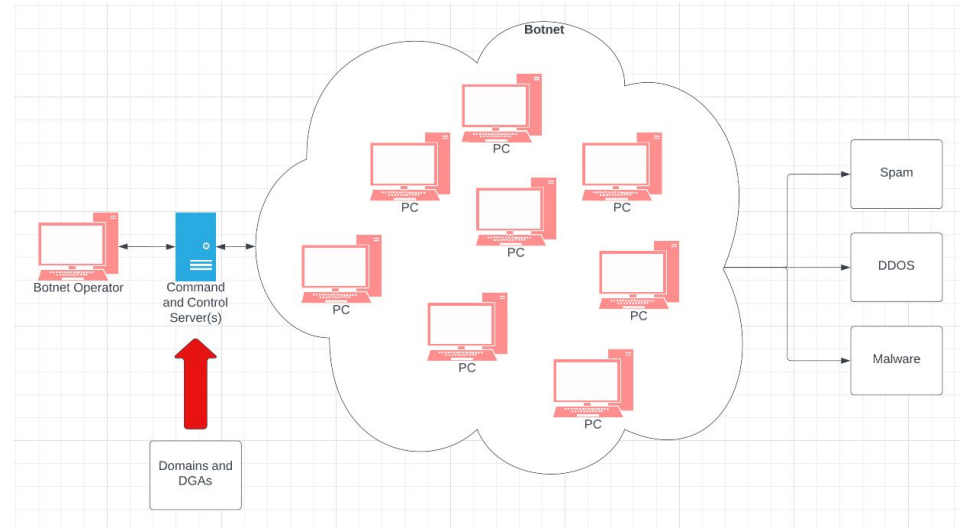
geek47.tld

pcsupport.tld



DNS Abuse: Botnets

- Insecure, hacked computers or IoT devices
- Used for Spam, Malware, DDos etc.
- Domains used for “command and control”
- Domain Generation Algorithms
- Currently rare to see abuse reports for botnets using domains.



DNS Abuse: Pharming

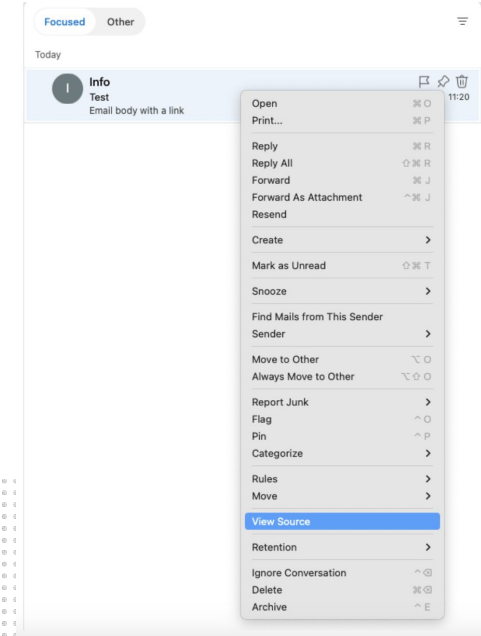
- Malware + Phishing
- Local DNS hijack or DNS poisoning
- Redirects user to phishing/malware site
- Almost never reported (like, never ever)
- Limited visibility and action at DNS

DNS Abuse: Spam*

*Included only where it's being used for preceding harms

Aside: reporting DNS Abuse that *only* involves email is **hard**.

- It's VERY easy to fake who sent an email
- **Email headers** and/or source are required
- Sharing headers is beyond most people, and getting harder to do over time



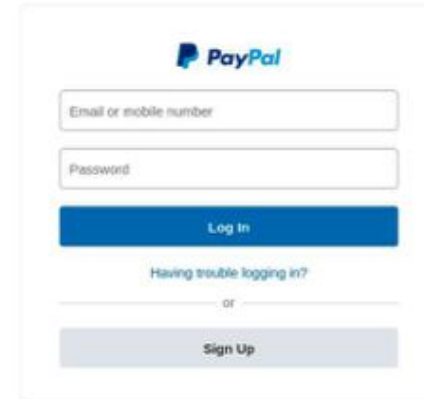
+ POP QUIZ

Time to be Identify Abuse!

Phishing Test #1

- Deception?
- Attempt to gather credentials?
- Where is the abuse?
- Suspend, refer, or neither?

<https://nutribiocrp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html>



[Contact Us](#) [Privacy](#) [Legal](#) [Website](#)

Phishing Test #2

URL: [https://securecgdapp-net\[.\]com/cgd/login.php/](https://securecgdapp-net[.]com/cgd/login.php/)

- Deception?
- Attempt to gather credentials?
- Where is the abuse?
- Suspend, refer, or neither?



Bem-vindo(a) à Caixa

Login

Para verificar a sua conta da Caixa, introduza o seu n° de contrato, seguido com o seu código de acesso e número de telemóvel.

N° de contrato
 Código de Acesso
 N° de telemóvel
 Nome
 Nif

[Esqueceu-se do código?](#)

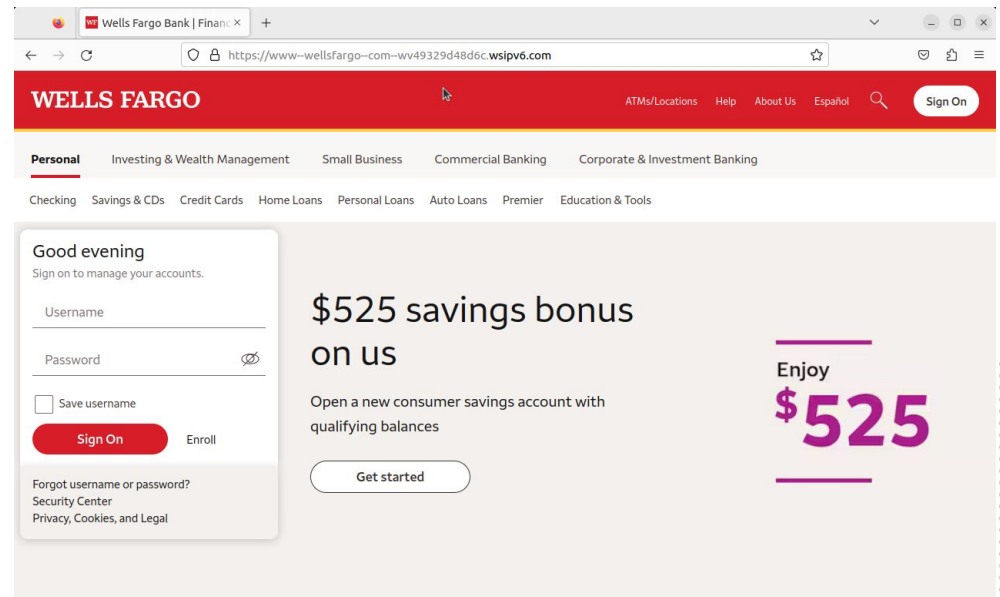
[Ainda não sou cliente](#)

 © 2024 CGD - Todos os Direitos Reservados

Phishing Test #3

URL: [https://www-wellsfargo-com-wv49329d48d6c.wsipv6\[.\]com](https://www-wellsfargo-com-wv49329d48d6c.wsipv6[.]com)

- Deception?
- Attempt to gather credentials?
- Where is the abuse?
- Suspend, refer, or neither?



Phishing Test #4

URL: staltlayer[.]com

- Deception?
- Attempt to gather cred
- Where is the abuse?
- Suspend, refer, or neither?



Connect Wallet

Stake

Portfolio

Rewards



staltlayer[.]com

Claim Rewards

8000.00

ALT

Balance: 8000 stALT MAX

AltLayer



Rewards

APR: 31.4%

Pool TVL:

79,498,151 ALT (\$48,244,486)



Connect Wallet

Stake

Vaults

Portfolio

Rewards

stake.altlayer[.]io/stake

STAKE

0.00

ALT

Balance: 0 ALT MAX

VAULT

Mach Alpha

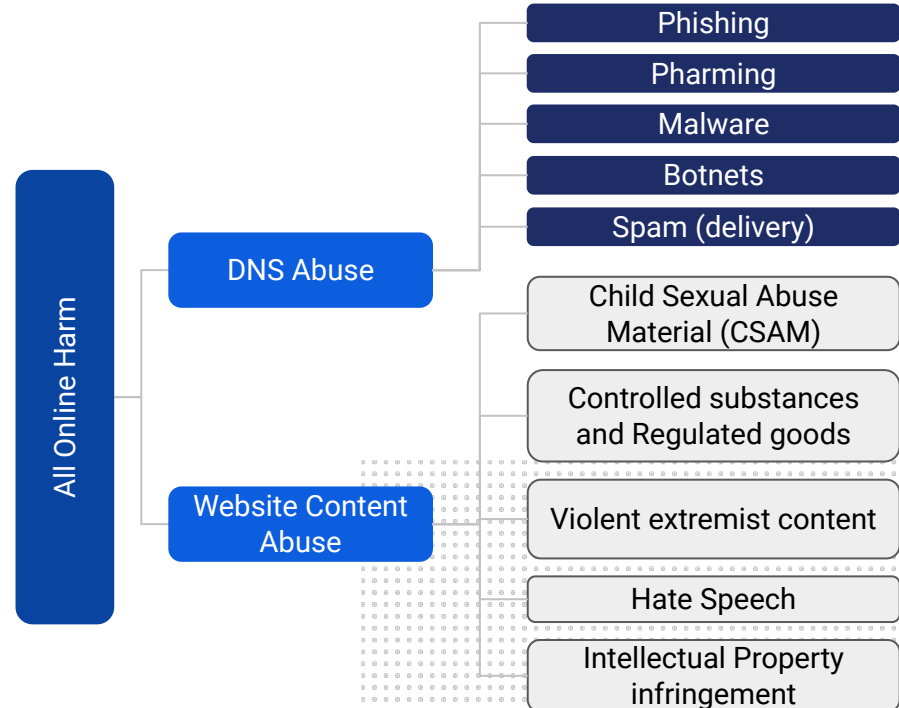
Live



+ How did you score?

Other categories of harm?

- 'Website Content Abuses' are still important
- Many DNS operators act on certain categories
 - [Voluntary Framework](#) to Address Abuse
 - > 50 signatories
- Appropriate mitigation typically requires:
 - External expertise
 - Wider ecosystem engagement



Part 2: Tackling DNS Abuse

Step 1: Measure DNS Abuse Prevalence

Inputs: Feeds/Lists/"RBLs"*

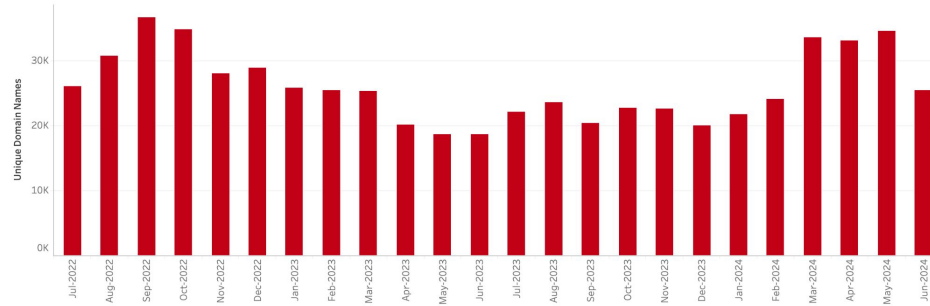
- Variation in quality, cost, shareability, interpretation
- Typically unevidenced
- Built for network and email blocking
 - Very different risk profiles for false positives
 - Not intended for mitigation
 - May even include domains that have never been registered

*RBL: Reputation Block List



Overall picture on DNS Abuse

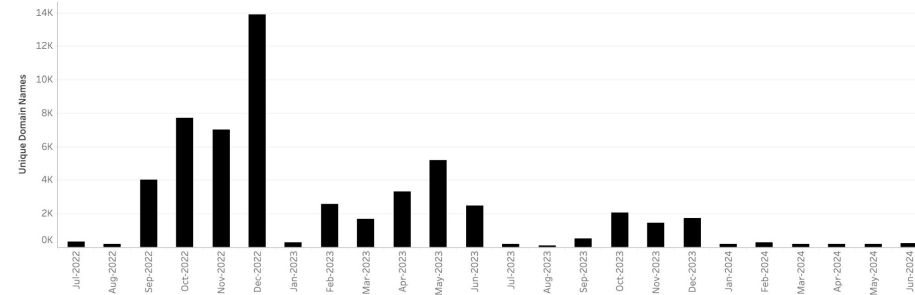
Overall Trends



Phishing fluctuates

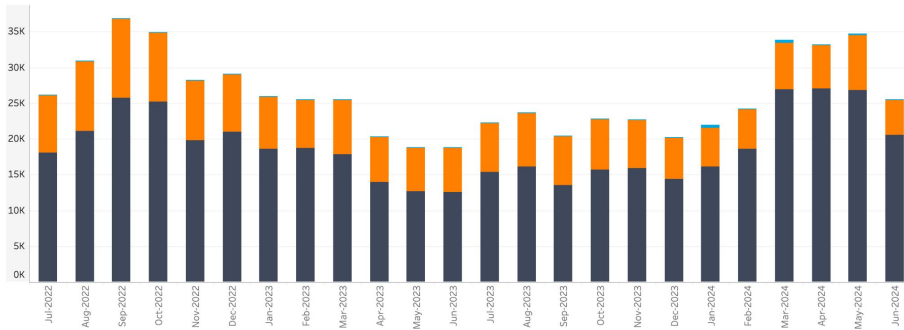
There may be some seasonality.

*Chart scale: 0-37K

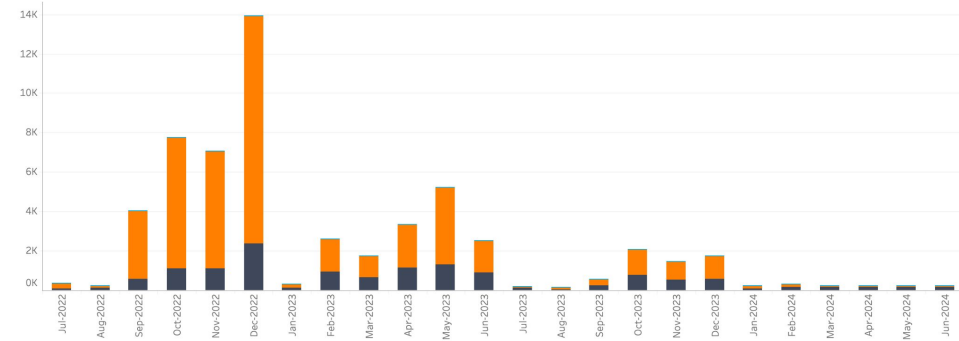


Malware seems to be driven primarily by the activity of criminal groups & law enforcement. *0-14K

Compromised Websites



~ **30%** phishing is associated with **compromise**



~ **60-80%** malware distribution is associated with **compromise**

Mitigation Rates:

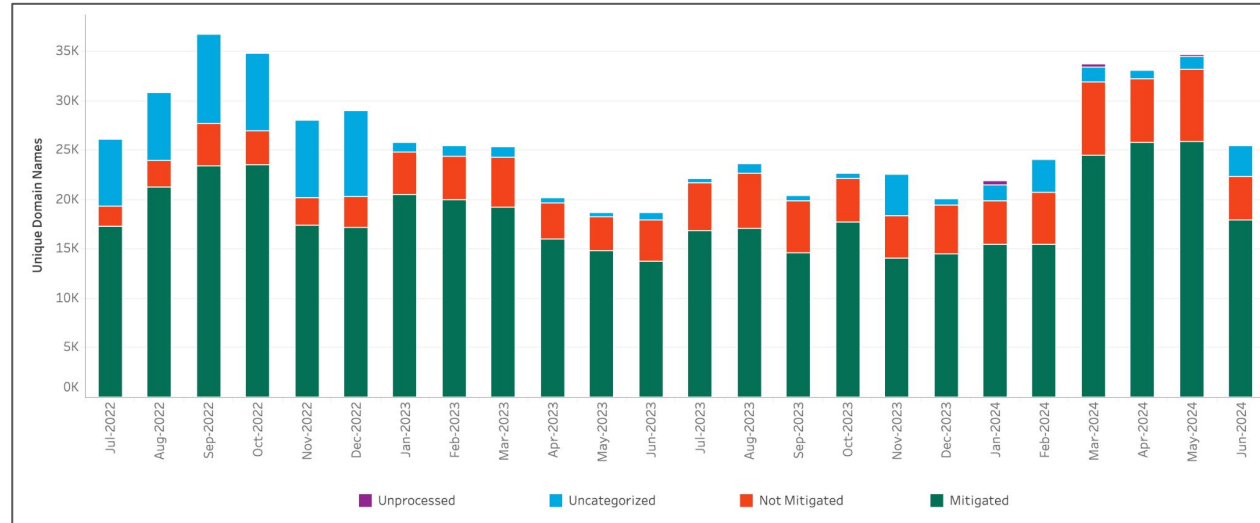
Average over Dec 2023 – Feb 2024

~80% mitigated

~20% not mitigated

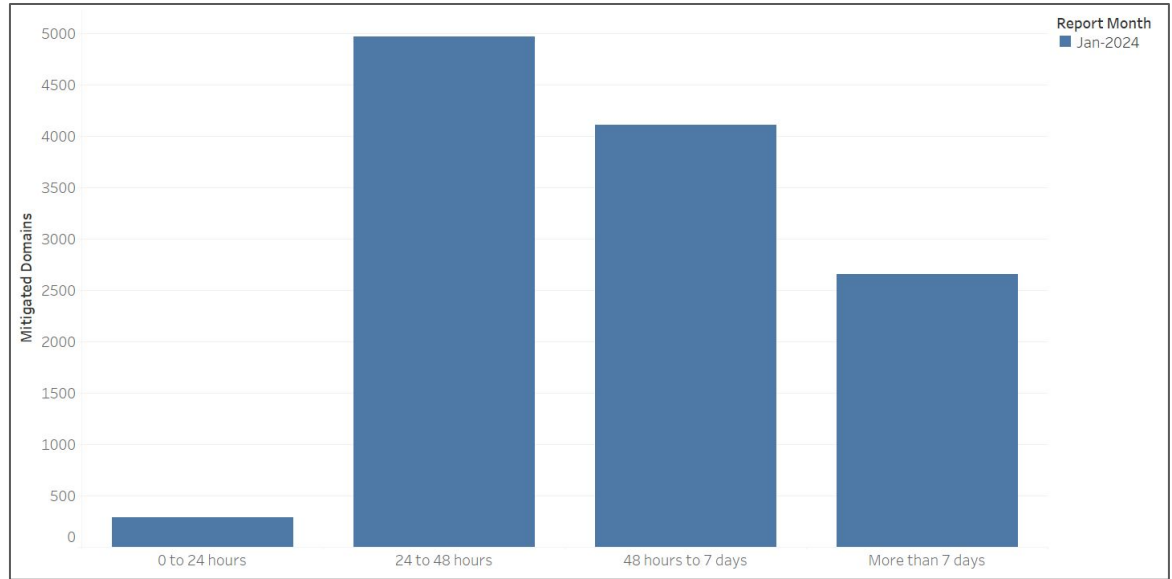
Notes:

- **Uncategorized** have been distributed in ratio.
- **Unprocessed** is small and not very visible on this chart.



Mitigation Speed

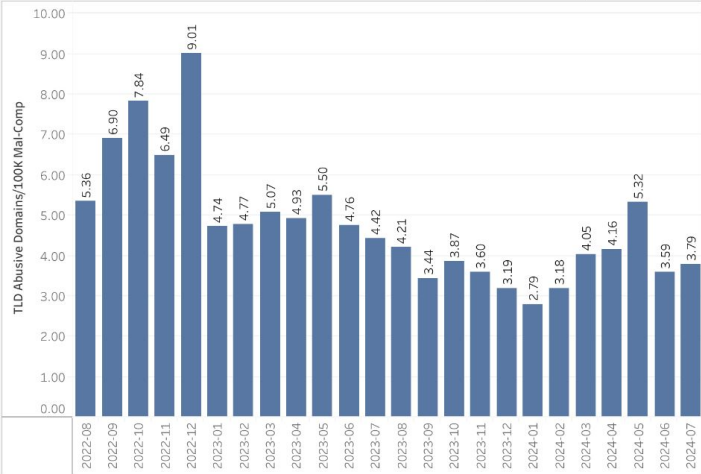
- In January 2024, 5,262 (43.73%) of unique mitigated domains were associated with a registrar which had a median mitigation time of 48 hours or less
- No attribution of action
- Includes compromise



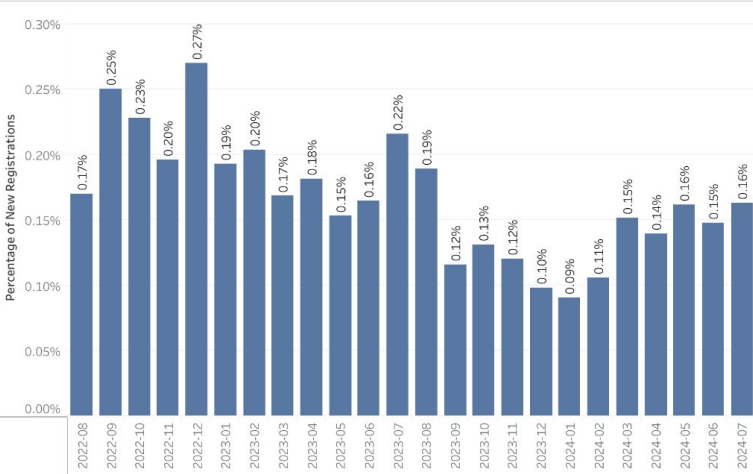
Free abuse
dashboards

Observed Abuse per 100K DUM

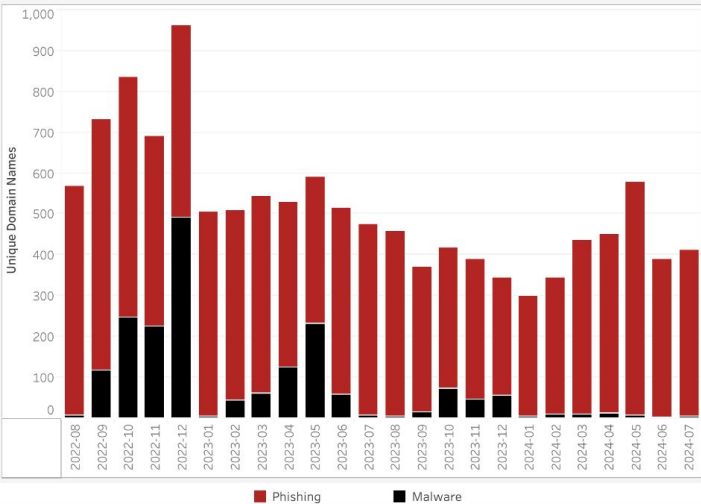
Malicious or Compromised



Percentage of New Registrations Observed as Malicious



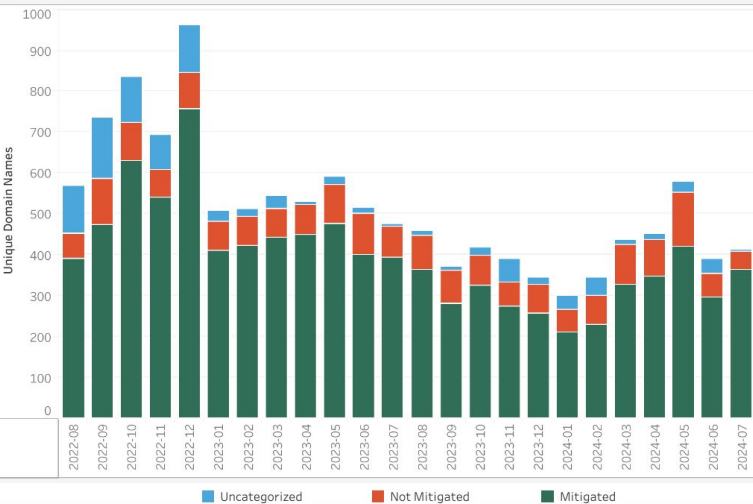
Observed TLD Abuse Trends



Observed TLD Mitigation

Malicious or Compromised

Malicious and Compromised



Distribution between Registrars

01

“Big Guys”

20 largest registrars

~7K malicious
domains per month

As a group they
under index

02

“Over-index”

5-7 registrars

Disproportionate
amount of malicious
registrations

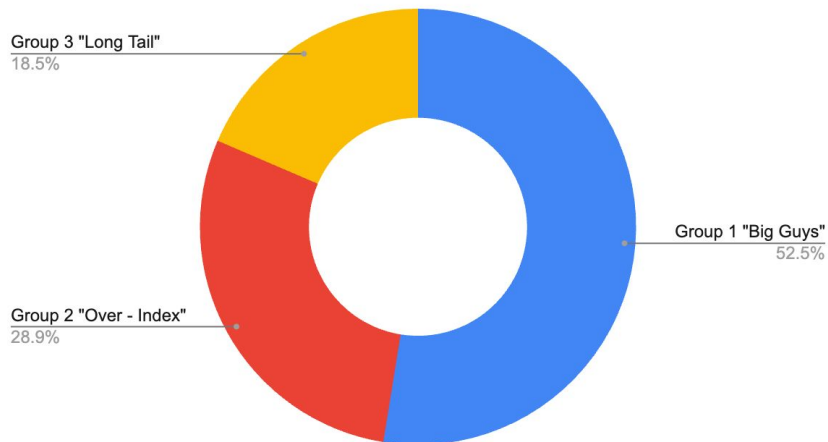
03

“Long tail”

Numbers tend to be
small and difficult to
interpret

Comparison: Size vs concentration

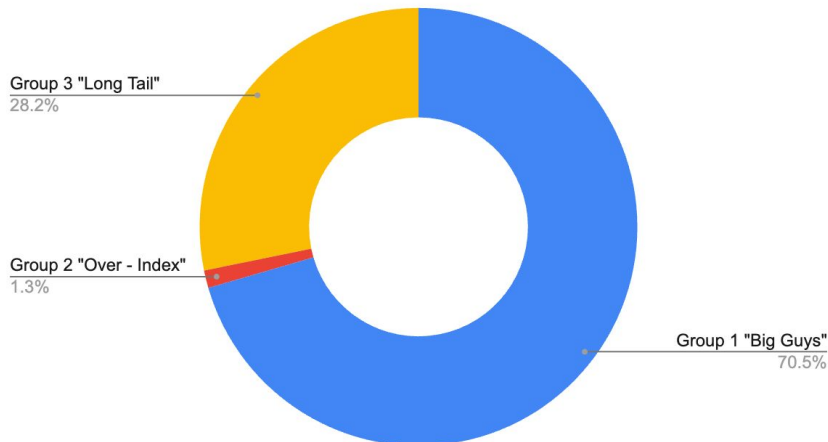
Percentage of Malicious Abuse



Group 1 "Big Guys"

53% (~7K) malicious reg.
70% domains

Percentage of Domains



Group 2 "Over Index"

29% (~3.5K) malicious reg.
1.3% domains

Highest observed rates of abuse

Table 3: Highest observed rates of abuse 2024-06

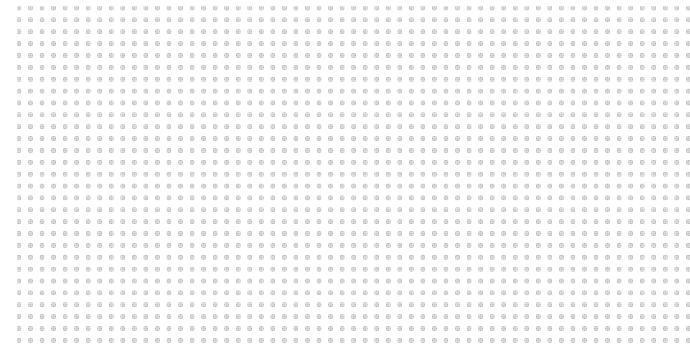
| IANA ID | Registrar Credential | Observed Maliciously Registered Domains Per 100,000 gTLD DUM | Observed Malicious gTLD Domains | Observed gTLD DUM | Number of Months |
|------------|-----------------------------|--|--|----------------------|------------------------|
| 3765 | NICENIC INTERNATIONAL GR.. | 664.39 | 339 | 51,024 | 6 |
| 3775 | ALIBABA.COM SINGAPORE E.. | 397.54 | 1,066 | 268,151 | 6 |
| 3862 | Spaceship, Inc. | 138.39 | 888 | 641,650 | 5 |
| 3858 | Aceville Pte. Ltd. | 108.52 | 116 | 106,889 | 6 |
| 1250 | OwnRegistrar, Inc. | 103.60 | 334 | 322,380 | 6 |
| 1556 | Chengdu West Dimension Di.. | 88.72 | 731 | 823,916 | 5 |
| *Redacted* | *Redacted* | 49.69 | * | * | 1 |
| *Redacted* | *Redacted* | 47.48 | * | * | 1 |
| *Redacted* | *Redacted* | 46.62 | * | * | 1 |
| *Redacted* | *Redacted* | 42.26 | * | * | 2 |

How do we Reduce DNS Abuse?

Approaches to Mitigation

Do you have:

- The policies/Terms of Service in place in order to take action?
- The tools to collect, and manage reports of abuse?
- The processes and training to identify and mitigate abusive domains?



Two Approaches to Combating DNS Abuse

Reactive – Responding to reports of abuse

Improvements to:

- speed of abuse discovery
- speed of reporting
- quality of reporting
- mitigation times
- mitigation rates

Proactive – Preventing malicious names from being registered

Improvements to:

- Detection of potentially malicious names
- Detection of fraud
- Pivoting on reports of abuse
- Incentive programs

Reactive Approaches

- Improving speed of abuse discovery*
- Improving speed of reporting*
- Improving quality of reporting*
- Improve mitigation time
- Improve mitigation rates

*What can we fix with the absolute minimum of work for Registrars and Registries?

- Discovery & reporting

What can we improve with education, best practices, and contractual requirements?

- Mitigation time, mitigation rates

Can we improve relationships between those with abuse data and the industry?

Abuse Discovery & Action

- Do you subscribe to feeds/RBLs?
- Do you wait for abuse to get reported to you?
- Do you scan your zone?
- Do you take action yourself?
- Do you refer abuse to registrar?

app.netbeacon.org

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 (and participating ccTLDs)
- Forms are embeddable

Participating ccTLDs:

vn,au,nz,to,co,us,ca,de,pl,eu,se,nu,br,uk,ch,li

Powered by CleanDNS

Community


References in:

- SSAC115
- SSR2
- CCT-RT
- GAC

Communiques

NetBeacon

- ~4,000 reports a month
- Almost all phishing
- **Lots** of crypto phishing
- Most reported domains don't exist on enrichment lists

 **Admin**
Graeme
Bunton

ADMINISTRATION INCIDENTS REPORTS

REPORT ABUSE

SETTINGS

LOG OUT

< BACK TO ALL REPORTS

ABUSIVE URL
canadapost.helpsu.top

ABUSE TYPE
Phishing

ABUSE DATE
3/20/2024

ABUSE ONGOING
Yes

REPORT ID
e1ab03

REPORTED AT
3/21/2024, 3:35:24 PM

REPORTED BY
Graeme Bunton
graeme@dnsabuseinstitut

ABUSE DESCRIPTION

I received a text message pretending to be Canada Post with a URL that links to a fake Canada Post site asking me to update my address.

PHISHING TARGET

Canada Post

SUPPORTING EVIDENCE (2 FILES)



Abuse Management Tools

- CleanDNS
- Abuse Manager from IQGlobal
- Mambo from Knipp

What does your backend provider offer?

Free support for registrars & registries

01

Reporting

[NetBeacon Reporter:](#)

centralized abuse reporting tool

Thanks to:

CleanDNS

02

Education

Guidance, best practice, templates



By Benjamin Burleson, Director of the DNS Abuse Institute

I recently had a registrar approach me with a genuine interest in doing more to address DNS Abuse, but was unsure of where they should start. DNS Abuse is a complex problem, and there's no clear entry point to begin addressing it. This registrar is not alone; there are numerous registries and registrars that are increasingly concerned about abuse and need help getting started.

This post is the first in a three-part series that will attempt to provide reasonable, bite-size introductions to the key components of developing anti-abuse practices. This first post is dedicated to providing a reasonable legal basis, or basic DNS Abuse Policy, for addressing abuse. The next two will address the useful tools for managing DNS abuse and the procedures for actual mitigation.

This policy was developed in concert with the Internet and Jurisdiction Policy Network (IJN), and we're grateful for their contributions and support. IJN has some tremendous content in this space including their Toolkit: DNS Level Action to Address Abuse, which I encourage anyone interested in abuse mitigation to take a look at. The DNS Abuse Institute is also an active participant in the IJN Domain Contact Group.

03

Data

[NetBeacon MAP: Dashboards](#)



04

Events

9 May: Combatting DNS Abuse Workshop



Proactive Approaches

- Detection of potentially malicious names
- Detection of fraud
- Pivoting on reports of abuse
- Incentive programs

Where does our interest in reducing abuse, and registrar interests in reducing costs align?

- Registrars try very hard to reduce friction in domain purchase
- Most malicious names are bought with stolen credit cards. Improved fraud detection may reduce abuse

AI/ML Abuse Detection

- SIDN & DNSBelgium – .nl/.be: RegCheck
- EURid – .eu: PREMADOMA
- Nominet – .uk: DomainWatch

All are ccTLDs, with different national contexts and registrant relationships

Results are mixed

Incentivization Programs

- Registry (or ICANN?) provides discounts for low abuse rates (or other desired outcomes)
- Allows registrars to act how they see fit
- Leverages cost sensitivity in the market
- Quality Performance Index (QPI) from PIR (.org)
- .nl Registrar Scorecard

“Pivoting”

- Rather than treat each report as separate, search data for other uses of attributes:
 - Email
 - IP
 - Credit card
 - Address
- Proactively investigate and act as necessary

In Summary

Takeaways:

- The importance of abuse discussions to ccTLDs
- The different types of abuse
- The distribution of abuse across the ecosystem
- The different approaches to reducing Abuse
- NetBeacon Reporter, and NetBeacon MAP

More Info:

netbeacon.org

info@netbeacon.org

graeme@netbeacon.org

Thank you!