

The DNS Abuse Institute

Malicious Domains: Where they are, and what we can do about them

What we want you to leave with

- A better understanding of the DNS industry
- To know the difference between malicious and compromised domains, and why it's important
- An understanding of the distribution of abuse across the ecosystem
- To know how to report malicious domains

Overview

- About the DNSAI
- What is DNS Abuse?
- Malicious vs. Compromised
- The Domain Name Industry
- Where are abusive domains concentrated?
- How do we reduce abuse?
- How to report abusive names

About the DNSAI

- A project of Public Interest Registry (.org)
- Launched in 2021
- Education, Collaboration, Innovation
- Solving the collective action problem

What is DNS Abuse?

Definitions range from narrow:

- Malware, botnets, pharming, phishing, (spam)

To broad:

- Anything bad on the Internet that uses a domain name

And can differ between using the DNS for abuse, and abusing the DNS, or both

Consensus Definition

Technical harms appropriately resolved at the DNS

- Phishing
- Malware
- Botnets
- Pharming
- Spam*

*when used as a delivery mechanism

Malicious vs. Compromised

- **Malicious:** a domain registered for malicious purposes (i.e., to carry out DNS Abuse).
- **Compromised:** A benign domain name that has been compromised at the website, hosting, or DNS level.

Mal vs. Comp Cont.

- Relatively recent development within domain registration community
- Growing understanding and sophistication of what layer should deal with what harms

The Domain Name Industry

- ~2500 ICANN accredited Registrars, ~500 corporate families
- ~1500 Top level domains,
 - ~1250 generics: .org, .com, .horse,
 - ~250 country codes: .au, .ca, .de
- Primarily managed by contract

Economic Context

- High volume
- Low cost
- Globally competitive market
- Registrar owns customer relationship - mitigation typically belongs here (instead of the TLD level)

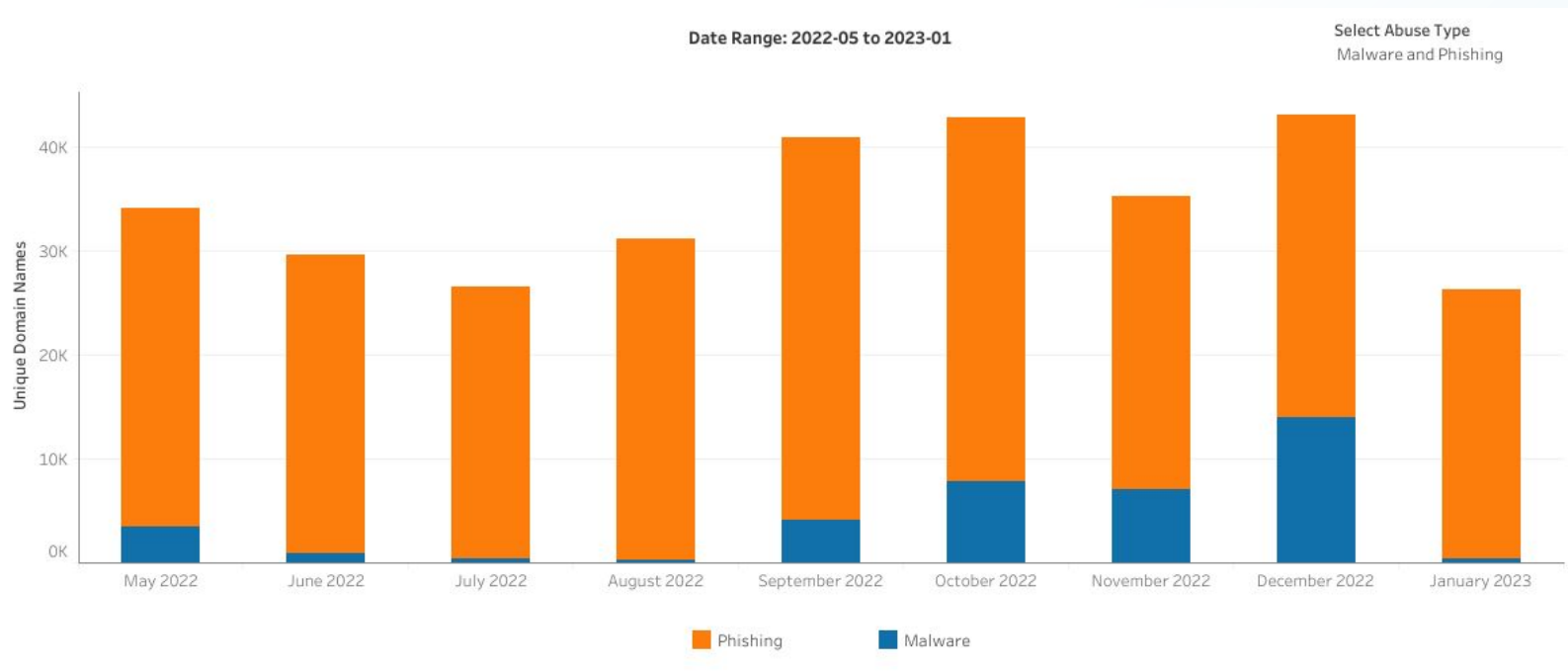
Measuring DNS Abuse

~~Ballpark~~Cricket Pitch Figures

ICANN's [DAAR](#) counts 658,774 abusive domains on 216,178,426 total, or 0.3%

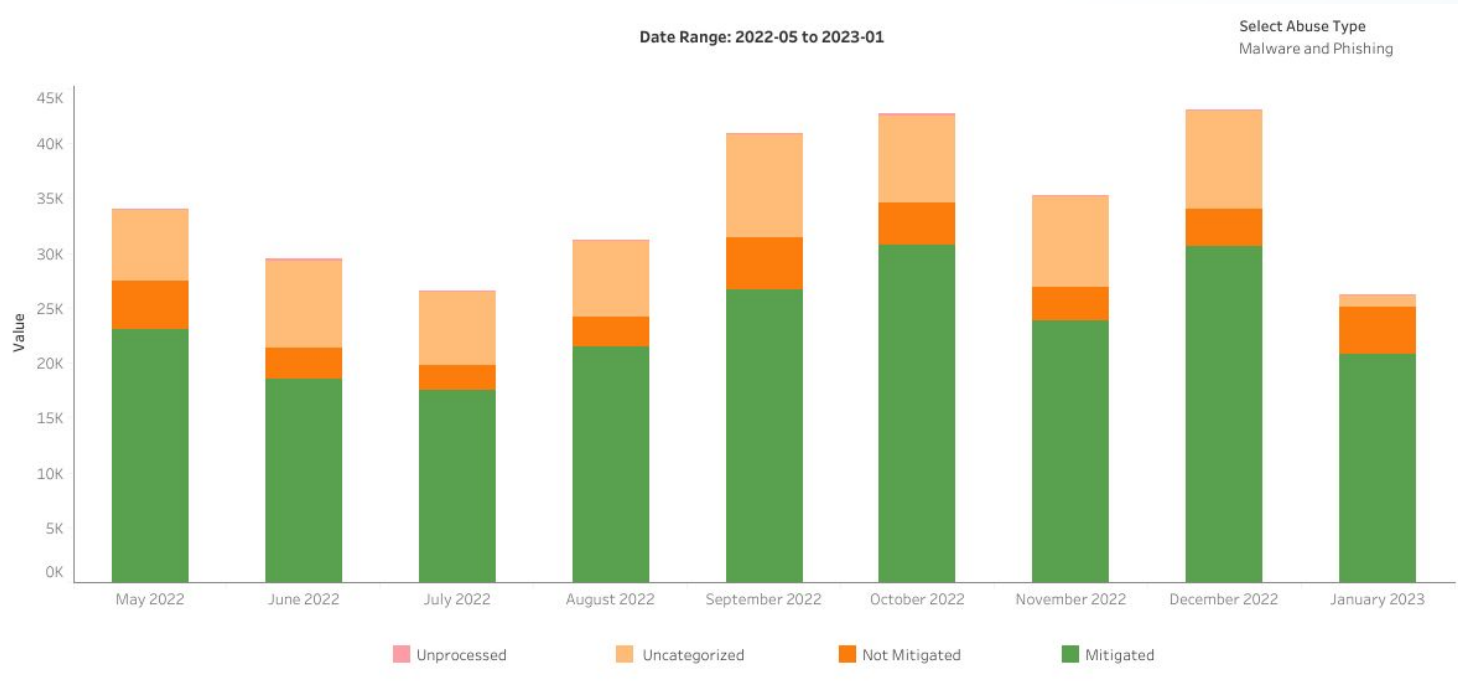
- Approx 76% of that is spam
- Leaving ~155,000 for malware, phishing, botnets (0.07%)

Trends in Abusive Names



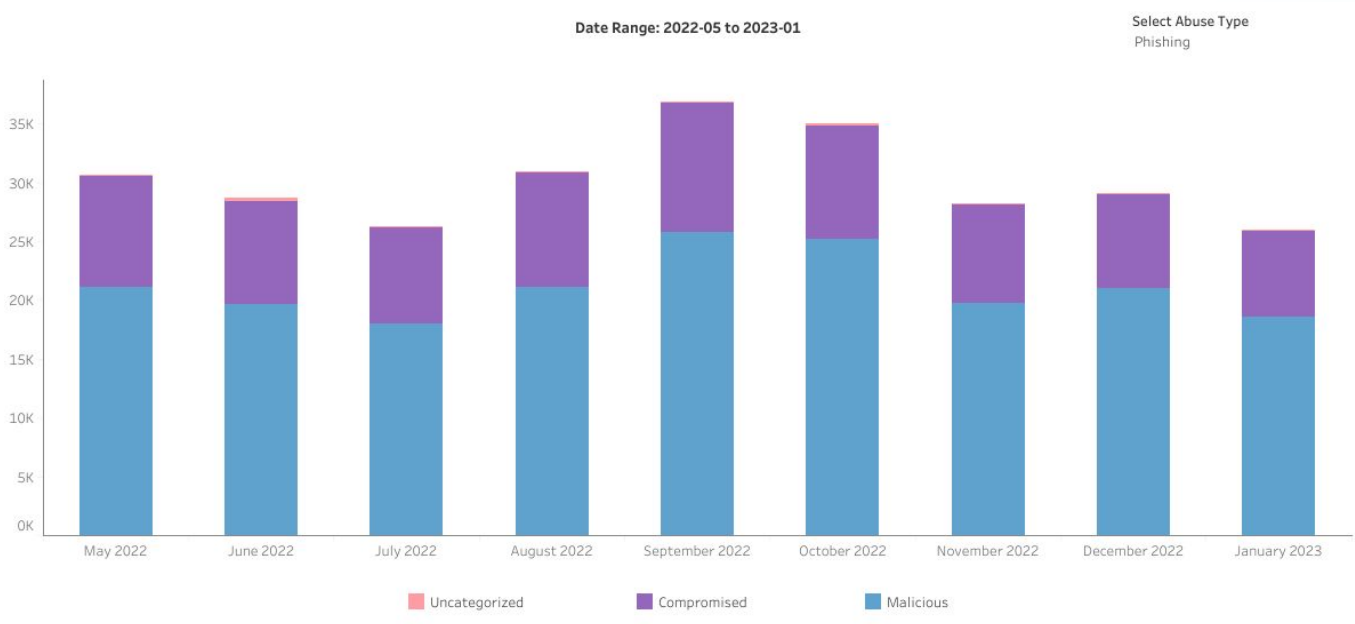
<https://dnsabuseinstitute.org/dnsai-compass/>

Trends in Abusive Names



<https://dnsabuseinstitute.org/dnsai-compass/>

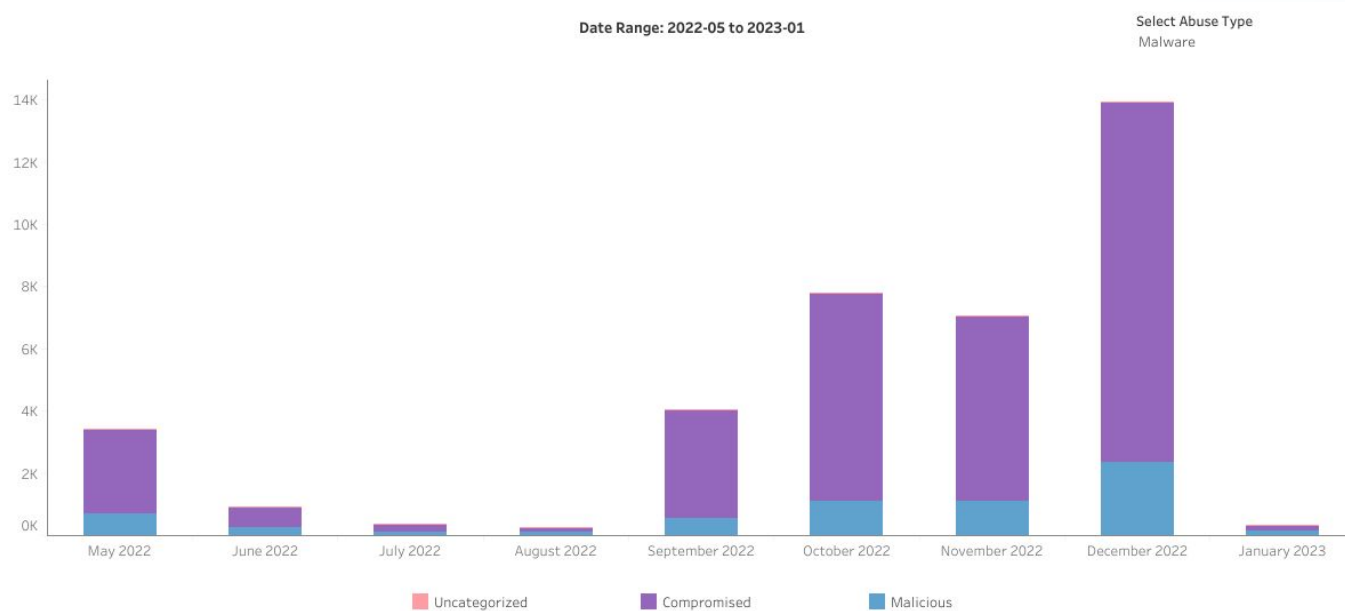
Malicious vs. Compromised



- Typically ~**70%** of **phishing** is malicious

<https://dnsabuseinstitute.org/dnsai-compass/>

Malicious vs. Compromised



- Typically ~14-20% of **malware** is malicious
- Higher in low volume months

<https://dnsabuseinstitute.org/dnsai-compass/>

Phishing and Malware

- Beginning to understand trends over time
 - Malware varies in volume, low rates of malicious registrations
 - Phishing is more stable, higher rates of malicious registrations
- Abuse is not evenly distributed across the ecosystem

Where is abuse concentrated?

Group 1: High volume, high growth registrars:

- Size and business model results in high raw volumes of malicious registration
- Tend to be low on abuse per 100K
- Generally high levels of mitigation
- Most have fast mitigation times

Jan 2023: ~26 RRs, 75% malicious registrations

How can we improve?

Group 1: High volume, high growth registrars:

- Preventative action
- Marginal gains on mitigation rates
- For some, speeding up mitigation

Where is abuse concentrated?

Group 2: Handful of smallish, outliers:

- High malicious domains per 100K
- High rates of new malicious registrations
- Typically unengaged in industry events

January 2023: ~ 6, 10% malicious registrations

How can we improve?

Group 2: Handful of smallish, outliers:

- Active outreach
- Sharing information
- Improvements in policies and processes
- Raising of the 'floor' of contractual expectations

Meaning

- Tackling these two groups and their specific areas for improvement, focuses us on about **85% of the malicious registrations**

Other ways to improve

Compromised registrations

- Engagement from hosting providers & wider industry
- Education of end users
- General cyber security hygiene: updates, patching, password

Other ways to improve

Top Level Domains

- Managing RR channel
- Policies & Processes
- Incentive schemes?

What can you do?

- Prevent Compromise
- Report Abuse
- Educate end users

How to Report Abuse



NETBEACON

Netbeacon.org

- Centralized abuse reporting system
- Simplified, structured abuse reporting
- Easy for reporters
- Better for recipients
- FREE

- Enriches reports
- APIs for reporting at scale
- Expanding to hosts & ccTLDs

The screenshot shows a web browser window with the URL `app.netbeacon.org/new-report/phishing`. The page title is "Submit a New Phishing Abuse Report" for the domain `facebook.com`. The user is logged in as "Admin" (Graeme Burton). The interface includes a navigation menu with options: ADMINISTRATION, INCIDENTS, REPORTS, REPORT ABUSE, SETTINGS, and LOG OUT.

Definitions for fields in step 1:

Date
The date on which you encounter this harm.

1 Date of incident
The date on which you encounter this harm.

Date*
2023-03-21

BACK SAVE CONTINUE

2 Institution targeted
The name of the company or organization being impersonated.

3 What happened?
Provide a brief description of the issue.

4 Additional evidence
Share any files or screenshots that might help an investigation. Screenshots are helpful for phishing sent via text or instant message.

5 Your location
Some harms are restricted to particular places, it can be helpful to know where it was accessible from.

6 Sender Email
If the phish was sent via email, the sender's email address.

7 Email headers and body
Email headers are useful in accurately identifying who sent spam. It can be difficult or impossible to act without these. You can find out how to get them by selecting your email platform here: <https://mxtoolbox.com/public/content/emailheaders/>

8 Submit Report

Privacy Notice Powered by CleanDNS Terms of Use

Education

Share our Best Practices:

- [Secure Your Website, Save the Internet](#)
- [Making Phishing Reports Useful](#)
- [Generic Abuse Policy](#)

Questions?

Contact:

~~@graemebunton,~~

@dotgraeme@mastodon.cloud,

graeme@dnsabuseinstitute.org

rowena@dnsabuseinstitute.org