The DNS Abuse Institute

SSAC Update, ICANN79, 3 March 2024

DNS ABUSE INSTITUTE

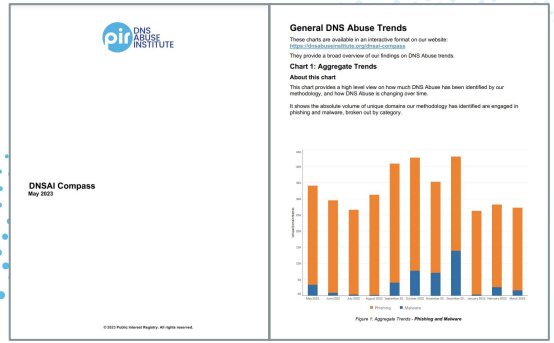
Today

- Compass
- NetBeacon
- Other updates
- Any other questions ?

DNS ABUSE INSTITUTE

Compass

- 19 Months of public Aggregate Data
- 9 Months of Specific Reporting
- Individualized Dashboards


DNS ABUSE INSTITUTE

DNSAI Compass

May 2023

General DNS Abuse Trends

These charts are available in an interactive format on our website:
https://dnsabuseinstitute.org/dnsai-compass

They provide a broad overview of our findings on DNS Abuse trends.

Chart 1: Aggregate Trends

About this chart

This chart provides a high level view on how much DNS Abuse has been identified by our methodology, and how DNS Abuse is changing over time.

It shows the absolute volume of unique domains our methodology has identified are engaged in phishing and malware, broken out by category.

Figure 1: Aggregate Trends - Phishing and Malware

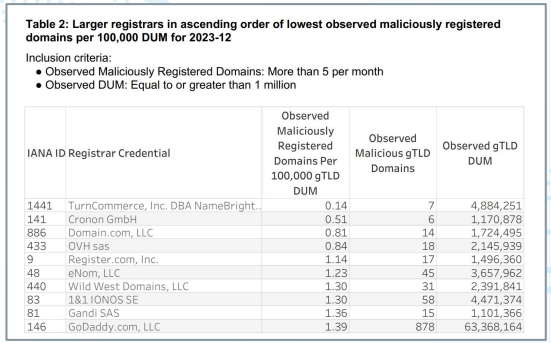


Table 2: Larger registrars in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-12

Inclusion criteria:

- Observed Maliciously Registered Domains: More than 5 per month
- Observed DUM: Equal to or greater than 1 million

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per 100,000 gTLD DUM	Observed Malicious gTLD Domains	Observed gTLD DUM
1441	TurnCommerce, Inc. DBA NameBright..	0.14	7	4,884,251
141	Cronon GmbH	0.51	6	1,170,878
886	Domain.com, LLC	0.81	14	1,724,495
433	OVH sas	0.84	18	2,145,939
9	Register.com, Inc.	1.14	17	1,496,360
48	eNom, LLC	1.23	45	3,657,962
440	Wild West Domains, LLC	1.30	31	2,391,841
83	1&1 IONOS SE	1.30	58	4,471,374
81	Gandi SAS	1.36	15	1,101,366
146	GoDaddy.com, LLC	1.39	878	63,368,164

DNS ABUSE INSTITUTE

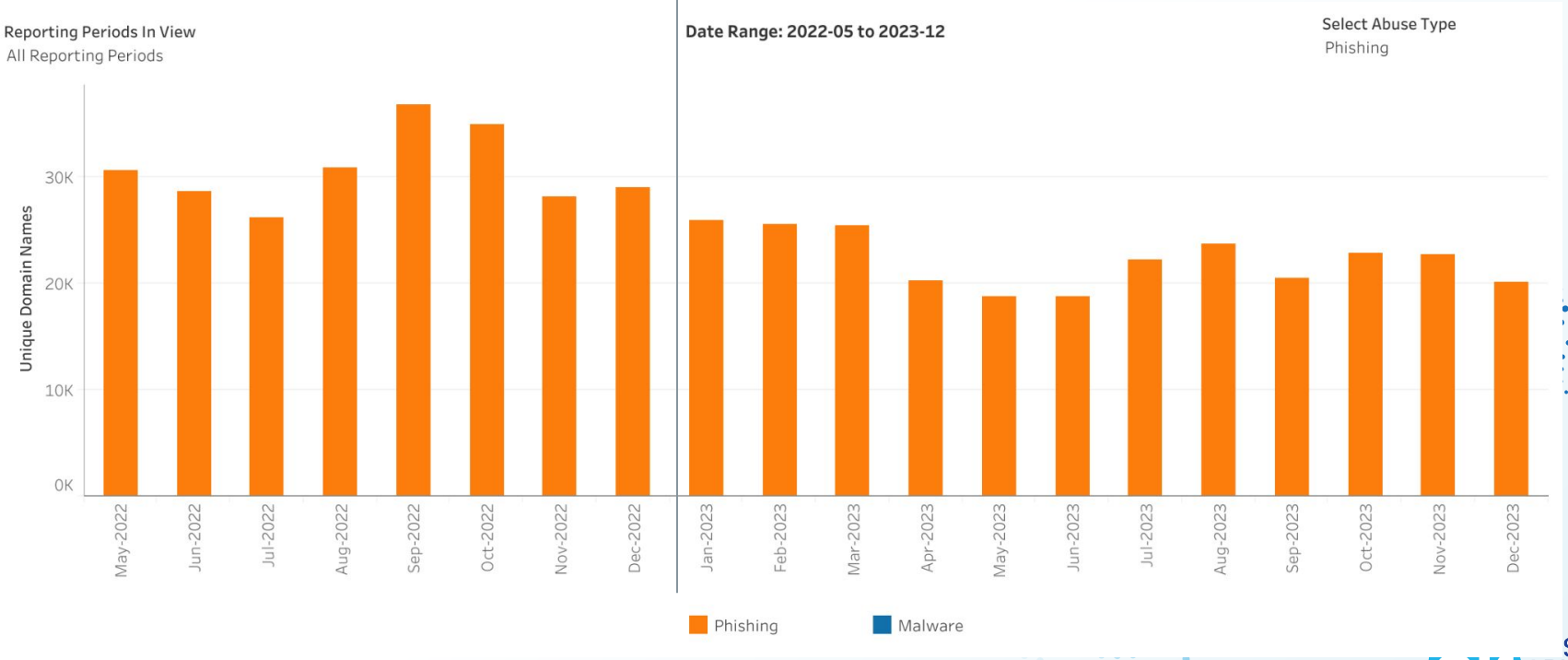
Compass

- Which enables: year on year
- Can we see overall trends yet?
- Issue specific: Measuring the impact of the contract amendments?
- Commentary v Observed Data
- Movement in the concentration of DNS Abuse

2022

2023

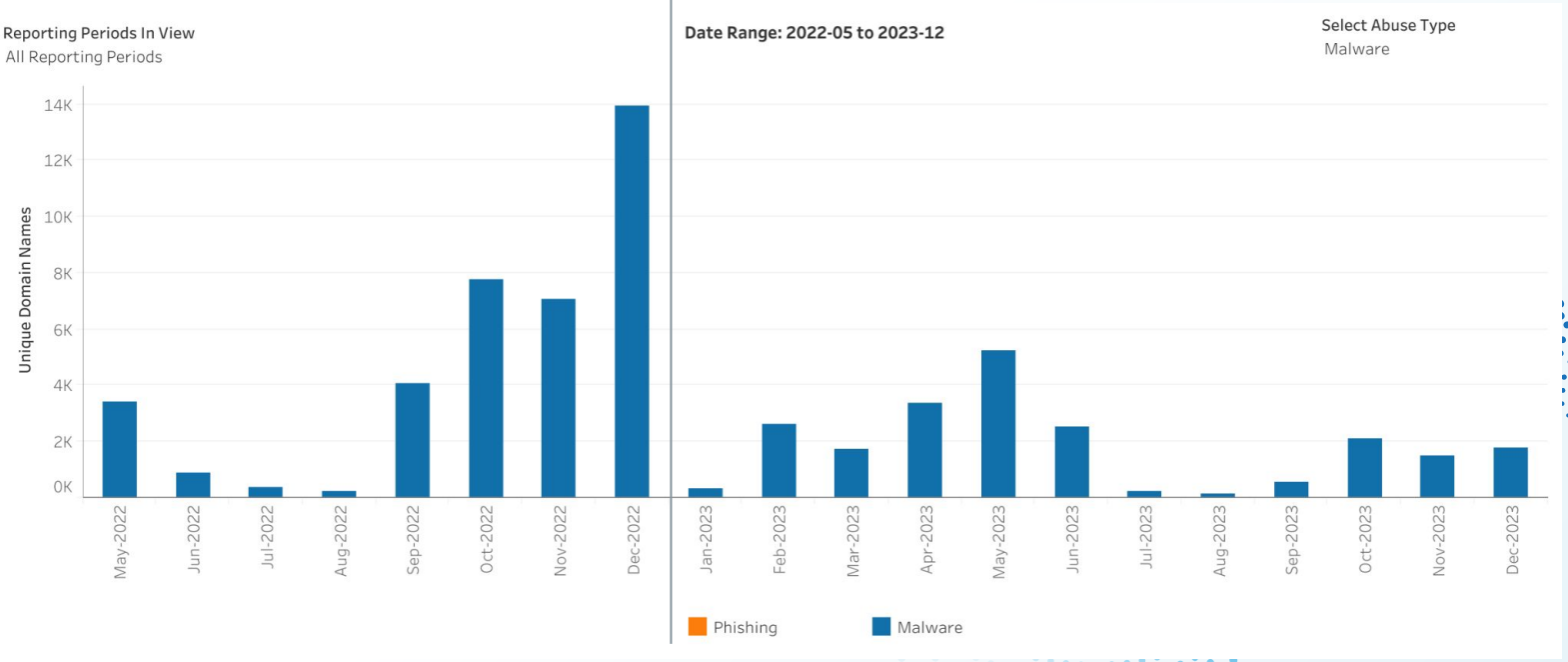
Phishing



2022

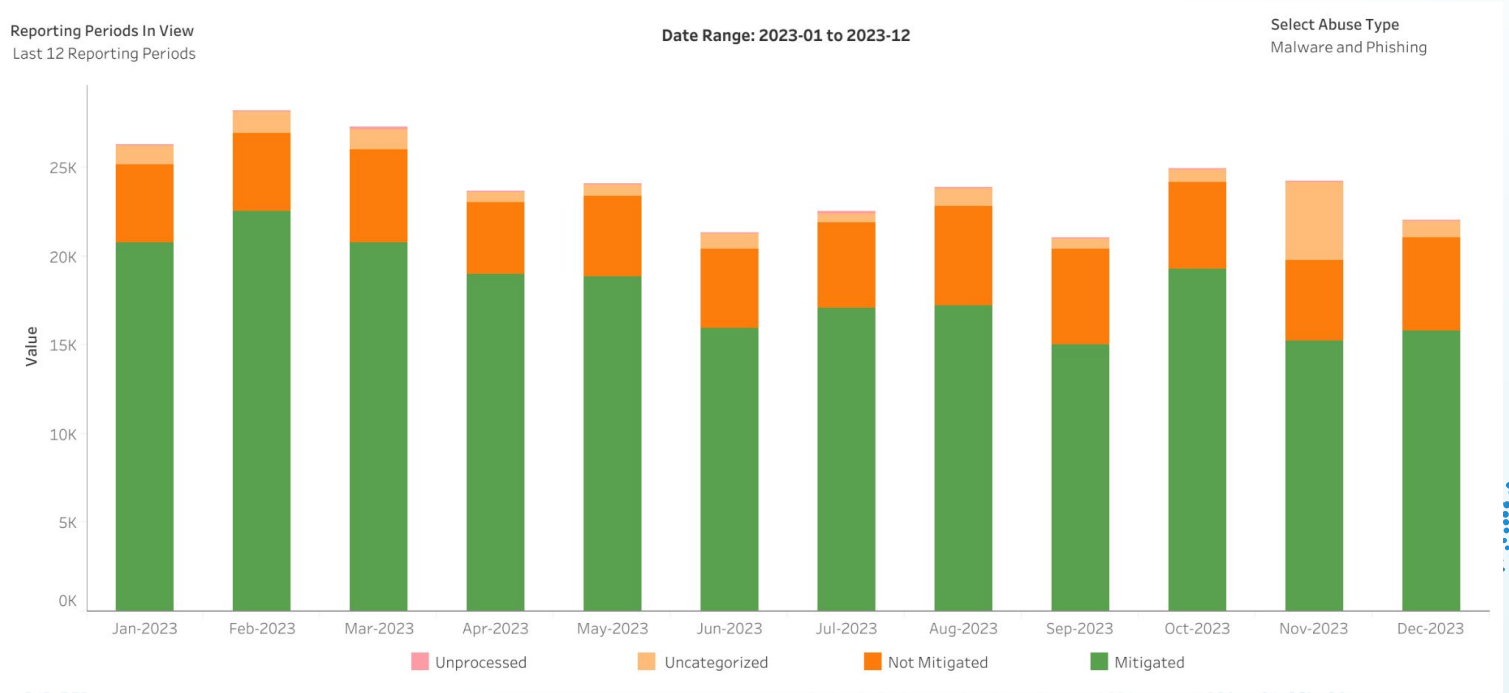
2023

Malware



DNS ABUSE INSTITUTE

Mitigation: 2023



Typically: **~ 70-80% mitigated**

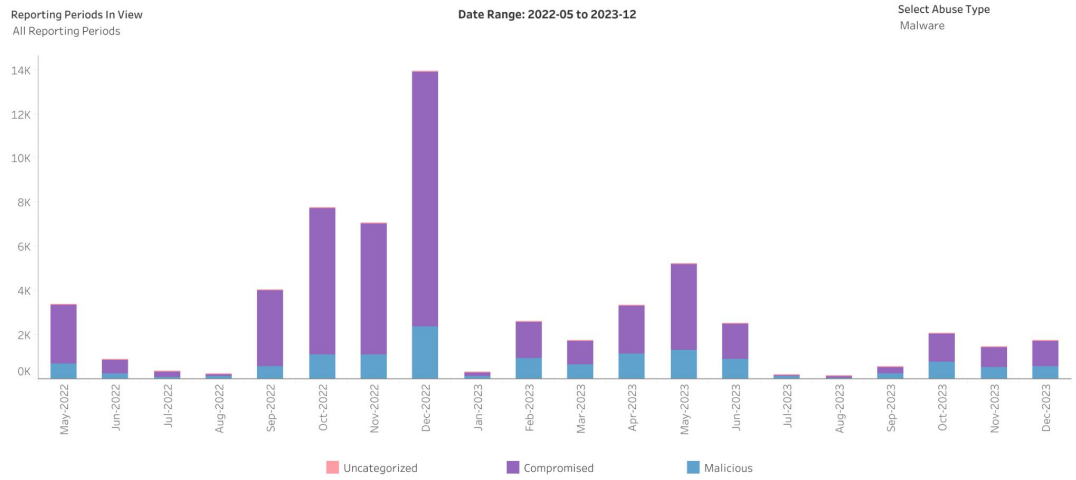
Note: includes compromised and malicious

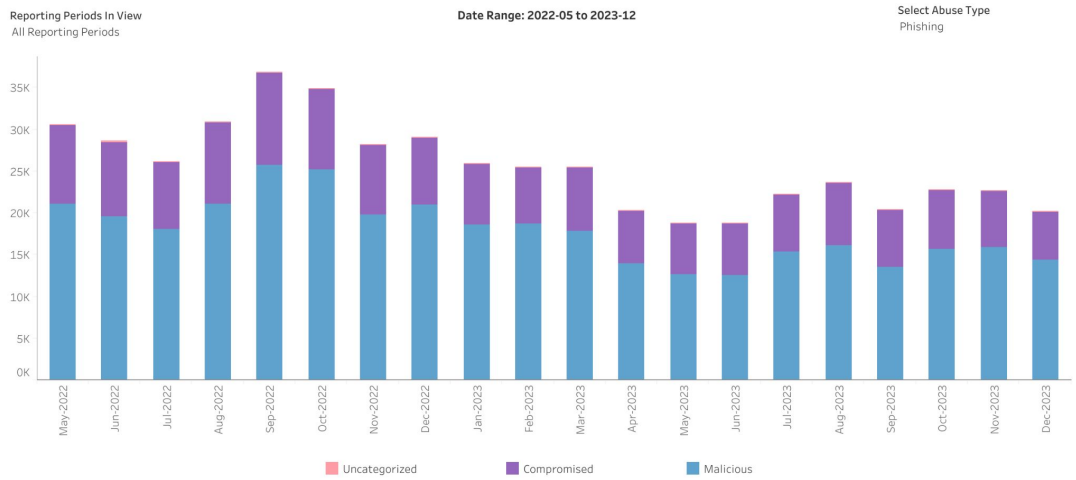
DNS ABUSE INSTITUTE

Measuring the Amendments

- Rates of DNS Abuse?
- Concentration rates?
- Abuse mitigation rates for maliciously registered domain names?
- Speed of mitigation?
- Malicious registrations vs. compromised?
- Migration to ccTLDs? Subdomains?

More on this soon…





Compromise

Typically:

~ 30% phishing

~ 50-80% malware distribution

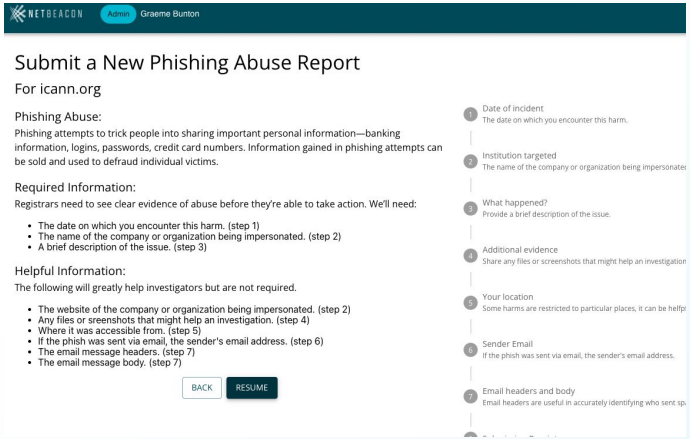
DNS ABUSE INSTITUTE

How SSAC can help?

- What data would you prioritise in making public?
- How would you measure the impact of the amendments?
- Sharing Compass reports
- General Education: e.g. malicious v compromised

NetBeacon

- ~15,000 reports in 2023
- Direct-to-ccTLD integration
  - .co, .uk., .au, .de, .nz, .eu, .pl, .ch, .li, .to
- New Registry dashboard interface
  - Insights into who is reporting what, for which of registrars



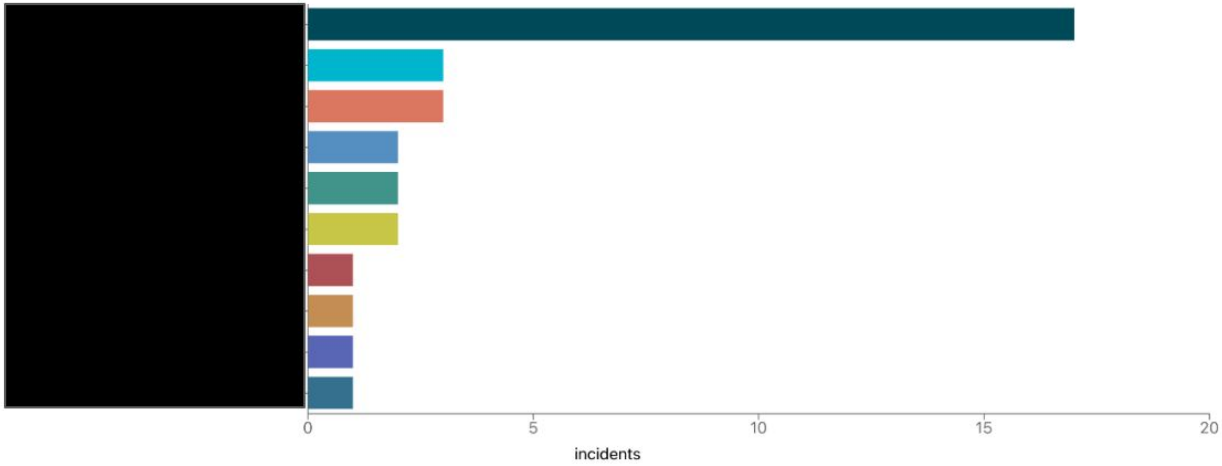
DNS ABUSE INSTITUTE

NETBEACON | Registry | Brian Cimbolic for Public Interest Registry

DASHBOARD | INCIDENTS | REPORTS | REPORT ABUSE | SETTINGS | LOG OUT

Date Granularity: Month | Date: February 2024 | Abuse Type: All

INCIDENTS BY REGISTRAR

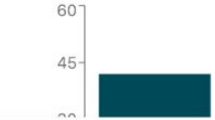


EXPORT

ID	Registrar	Total
[redacted]		17
		3
		3
		2
		2
		2

Rows per page: 100 | 1–19 of 19

INCIDENTS BY TLD



EXPORT

TLD	Total
org	42

NetBeacon: How SSAC can help?

- Spreading the word
- Introducing us to potential reporters / sources of enrichment

Events & Other Updates

- DNS Abuse Workshop, 9 May, Paris
  - Register
  - Draft agenda
- Tracing DNS Abuse through GAC Communiques including SSAC115
- Measuring Abuse Is Difficult blog and report