

The DNS Abuse Institute

SSAC Update, ICANN79, 3 March 2024

Today

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

Compass

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

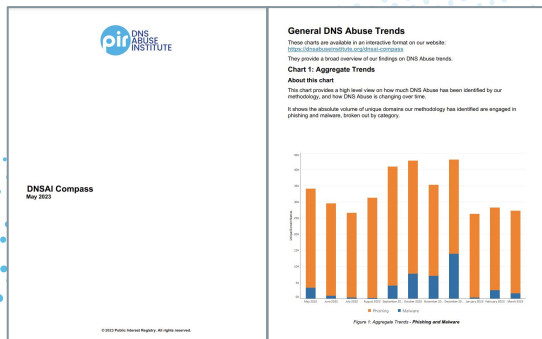


Table 2: Larger registrars in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-12

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



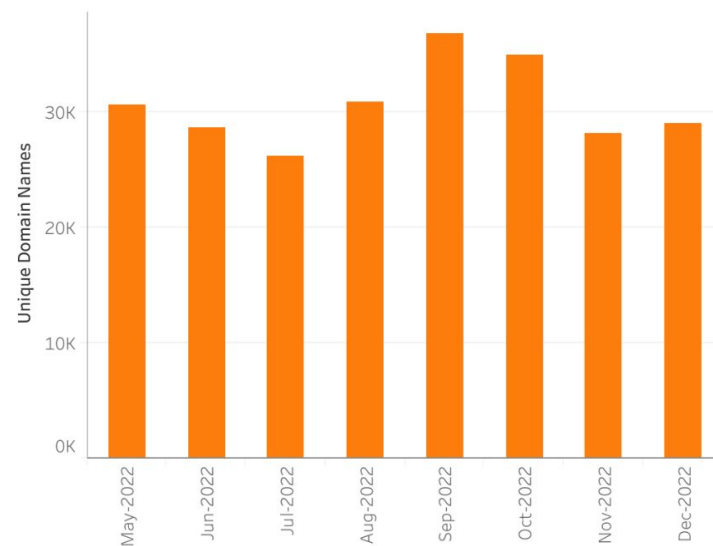
Compass

- 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

Phishing

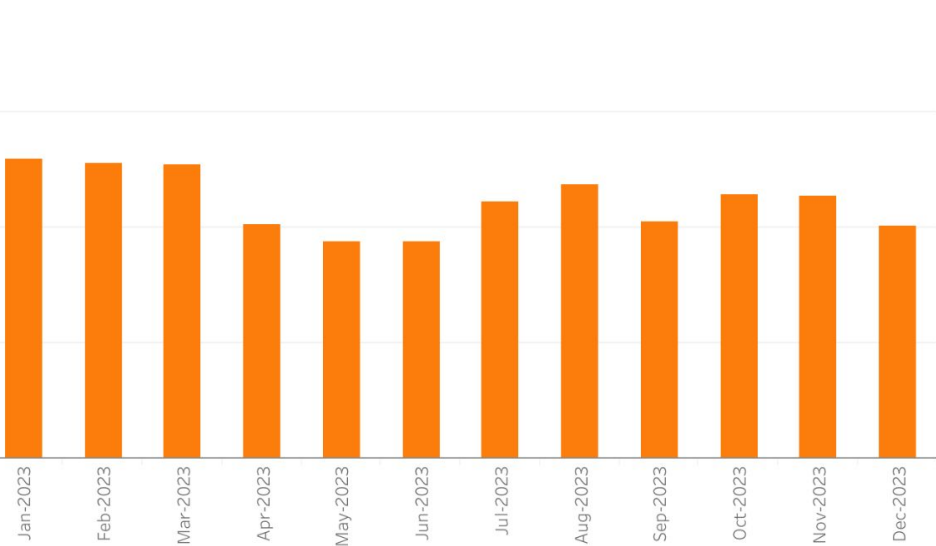
Reporting Periods In View
All Reporting Periods



2023

Date Range: 2022-05 to 2023-12

Select Abuse Type
Phishing



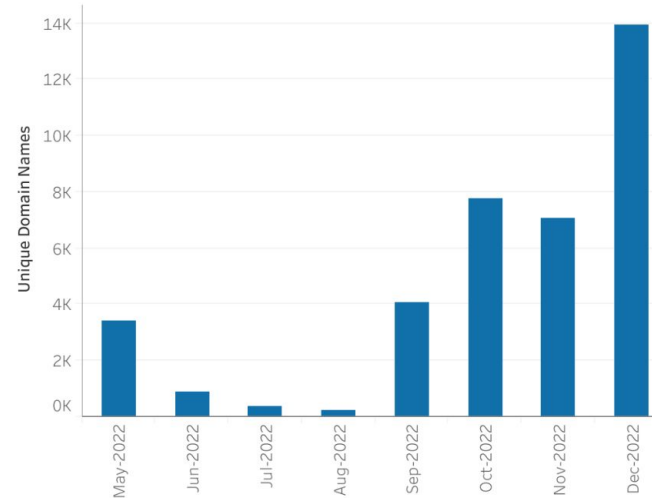
Phishing

Malware

2022

Malware

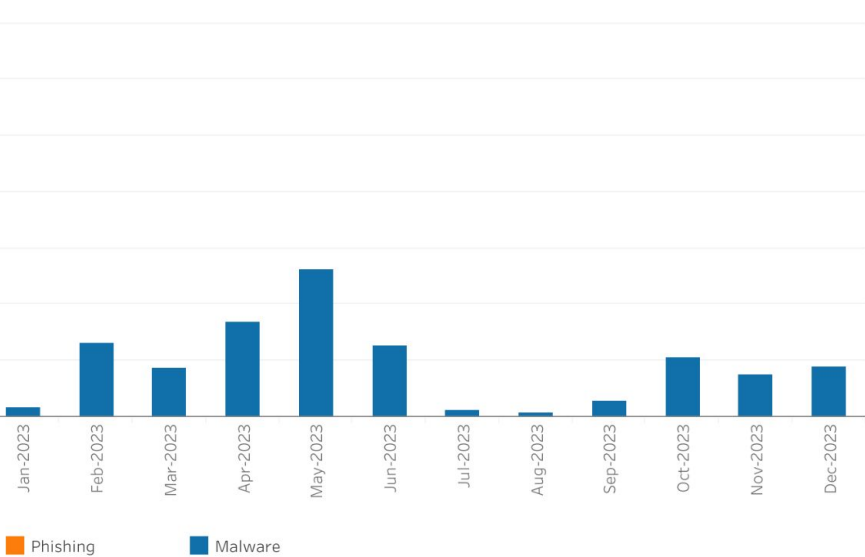
Reporting Periods In View
All Reporting Periods



2023

Date Range: 2022-05 to 2023-12

Select Abuse Type
Malware



Phishing Malware

Mitigation: 2023

Reporting Periods In View
Last 12 Reporting Periods

Date Range: 2023-01 to 2023-12

Select Abuse Type
Malware and Phishing



Typically: **~70–80% mitigated**

Note: includes compromised and malicious

Measuring the Amendments

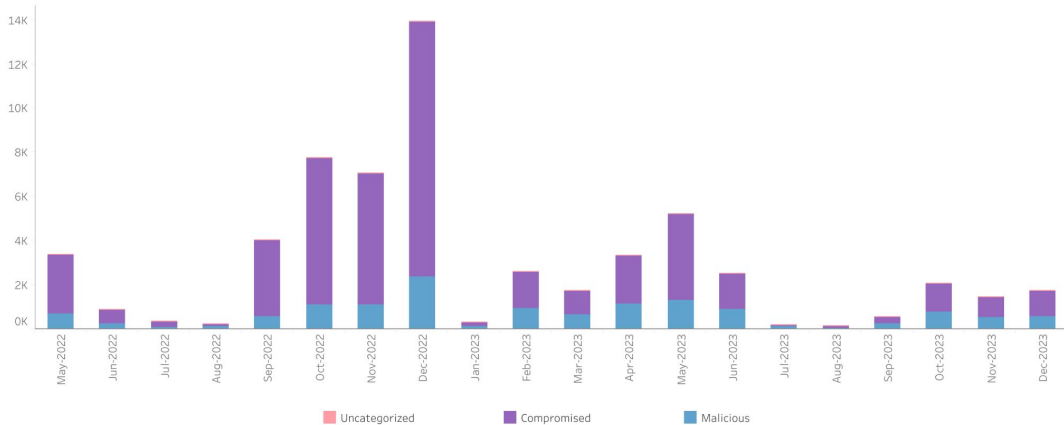
- Rates of DNS Abuse?
- Concentration rates?
- Abuse mitigation rates for maliciously registered domain names?
- Speed of mitigation?
- Malicious registrations vs. compromised?
- Migration to ccTLDs? Subdomains?

More on this soon...

Reporting Periods In View
All Reporting Periods

Date Range: 2022-05 to 2023-12

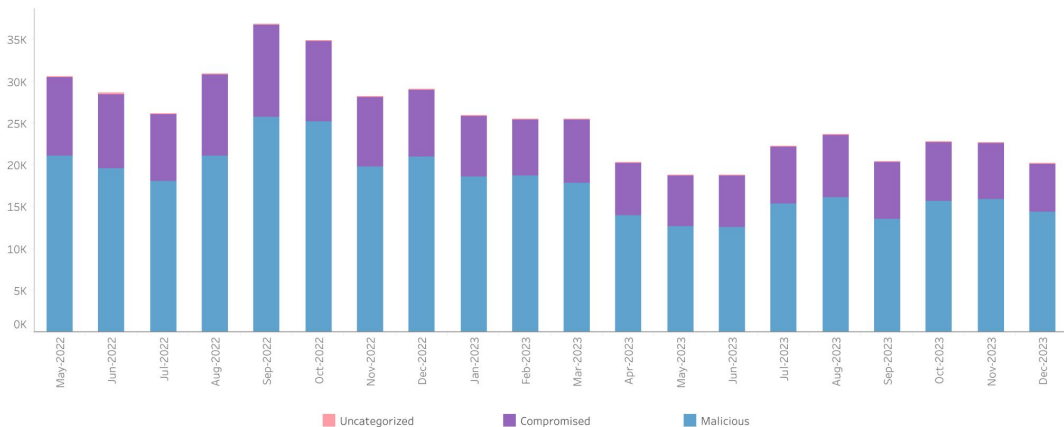
Select Abuse Type
Malware



Reporting Periods In View
All Reporting Periods

Date Range: 2022-05 to 2023-12

Select Abuse Type
Phishing



Compromise

Typically:

~ 30% phishing

~ 50-80%
malware
distribution

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

Submit a New Phishing Abuse Report

For icann.org

Phishing Abuse:

Phishing attempts to trick people into sharing important personal information—banking information, logins, passwords, credit card numbers. Information gained in phishing attempts can be sold and used to defraud individual victims.

Required Information:

Registrars need to see clear evidence of abuse before they're able to take action. We'll need:

- The date on which you encounter this harm. (step 1)
- The name of the company or organization being impersonated. (step 2)
- A brief description of the issue. (step 3)

Helpful Information:

The following will greatly help investigators but are not required.

- The website of the company or organization being impersonated. (step 2)
- Any files or screenshots that might help an investigation. (step 4)
- Where it was accessible from. (step 5)
- If the phish was sent via email, the sender's email address. (step 6)
- The email message headers. (step 7)
- The email message body. (step 7)

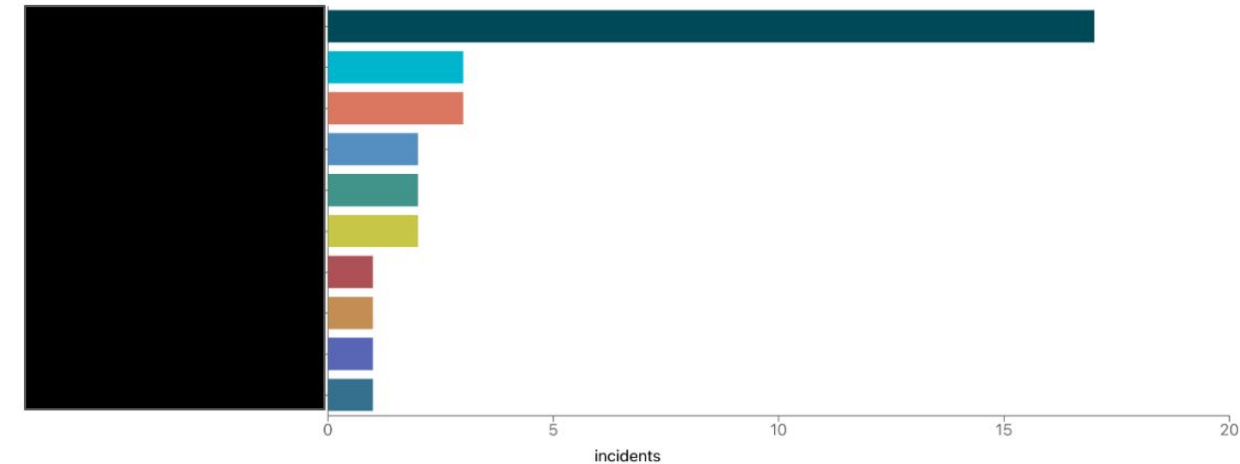
BACK

RESUME

- 1 Date of incident
The date on which you encounter this harm.
- 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 investigator.
- 5 Your location
Some harms are restricted to particular places, it can be helpful to provide your location.
- 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 you.

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

INCIDENTS BY REGISTRAR

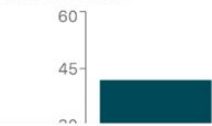


EXPORT

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