Compass Dashboards

Benchmarking the prevalence and persistence of malware and phishing for registries and registrars

Rowena Schoo,
Director of Programs and Policy,
DNS Abuse Institute

DNS ABUSE INSTITUTE

Today

- About the Institute
- Compass: How, what and why?
- Challenges
- Public Reporting
- Private Reportng: Dashboards
- Q&A

DNS ABUSE INSTITUTE

DNS Abuse Institute (“The Institute”)

- Created & funded by PIR (.org) in pursuit of nonprofit mission
- DNS Abuse = technical abuse: phishing, pharming, malware, botnets, and spam (when used as delivery mechanism).
- Cover all TLDs and registrars
- Everything we do is **free**
- Multi-Stakeholder Advisory Council

DNS ABUSE INSTITUTE

Compass: Purpose

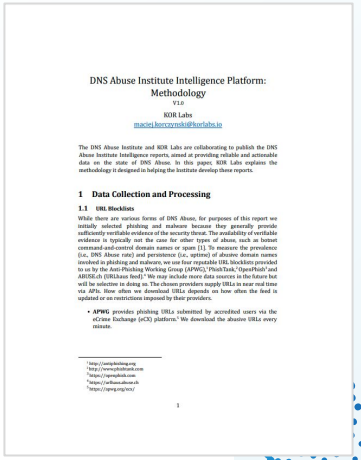
- Inform Institute mission & activities
- Empower the DNS community with sufficiently granular, accurate, and comparable data
- Inform efforts to develop best practices
- Ultimately reduce abuse at DNS level

Compass: Principles

- Transparency
- Credibility and independence
- Accuracy and reliability

Results in:

- Public methodology
- Academic collaboration: KOR Labs led by Dr Maciej Korczynski - Grenoble University
- Optimized for accuracy > coverage of all harm



DNS Abuse Institute Intelligence Platform: Methodology

V1.0

KOR Labs

maciej.korczynski@korlabs.io

The DNS Abuse Institute and KOR Labs are collaborating to publish the DNS Abuse Institute Intelligence reports, aimed at providing reliable and actionable data on the state of DNS Abuse. In this paper, KOR Labs explains the methodology it designed in helping the Institute develop these reports.

1 Data Collection and Processing

1.1 URL Blocklists

While there are various forms of DNS Abuse, for purposes of this report we initially selected phishing and malware because they generally provide sufficiently verifiable evidence of the security threat. The availability of verifiable evidence is typically not the case for other types of abuse, such as botnet command-and-control domain names or spam [1]. To measure the prevalence (i.e., DNS Abuse rate) and persistence (i.e., uptime) of abusive domain names involved in phishing and malware, we use four reputable URL blocklists provided to us by the Anti-Phishing Working Group (APWG),[2] PhishTank,[3] OpenPhish[4] and ABUSE.ch (URLhaus feed).[5] We may include more data sources in the future but will be selective in doing so. The chosen providers supply URLs in near real time via APIs. How often we download URLs depends on how often the feed is updated or on restrictions imposed by their providers.

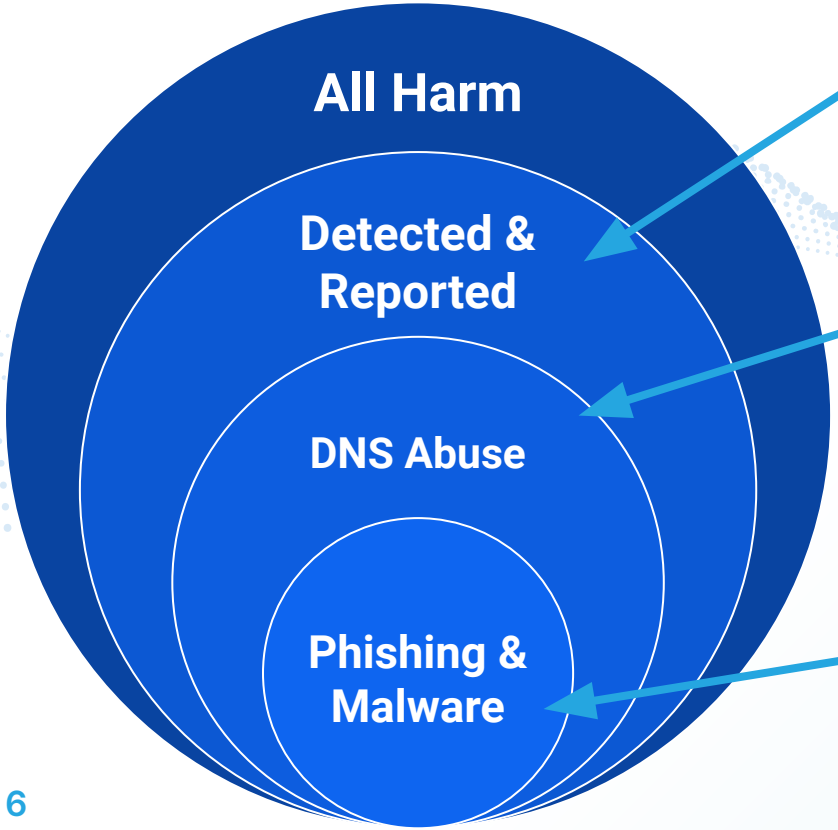
- **APWG** provides phishing URLs submitted by accredited users via the eCrime Exchange (eCX) platform.[6] We download the abusive URLs every minute.

[1] http://antiphishing.org
[2] http://www.phishtank.com
[3] https://openphish.com
[4] https://urlhaus.abuse.ch
[5] https://apwg.org/ecx/

1

DNS ABUSE INSTITUTE

What is measured?



We can only measure what gets **reported** (“iceberg” principle)

Not all reports are DNS Abuse (outside of our scope)

Focus on unique domain names associated with DNS Abuse we (KOR Labs) can **currently reliably evidence**

DNS ABUSE INSTITUTE

What is measured?

- Observed phishing and malware
- Mitigation
- Mitigation speed (registrars)
- Type of registration: compromised v malicious

Malicious: *a domain registered for malicious purposes (i.e., to carry out DNS Abuse).*

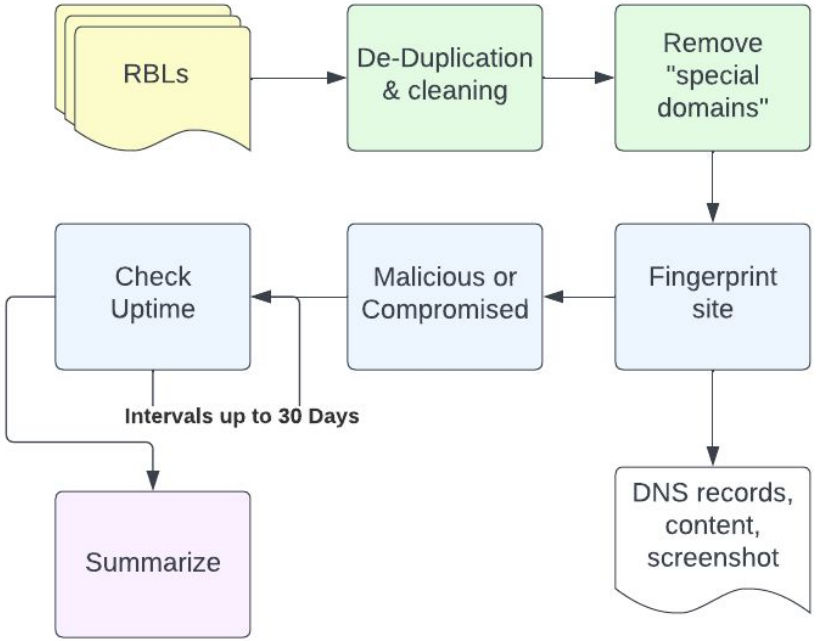
Compromised: *A benign domain name that has been compromised at the website, hosting, or DNS level.*

Compass: How?

Input
APWG
PhishTank
OpenPhish
URLHaus

Analysis
Evidence collection
Registration type
Mitigation:
Minutes: 5,15,30.
Hour: 1,2,3,4,5,6,
Days: every 12h for 30 days.

Editorial
Interactive charts
PDF Reports
Dashboards



Reports & Interactive Charts

Methodology

Cleaning
Measure:
- Unique domain names (E.g. 70K+ URLs)

Remove IP addresses and **"special domains":**
- URL shorteners (e.g., bitly.com)
- Subdomain providers, for example, dynamic DNS providers (e.g., duckdns.org),
- file sharing services (e.g., docs.google.com)

Special Domains list is publicly available (methodology). You can help us update this.

Challenges/Caveats

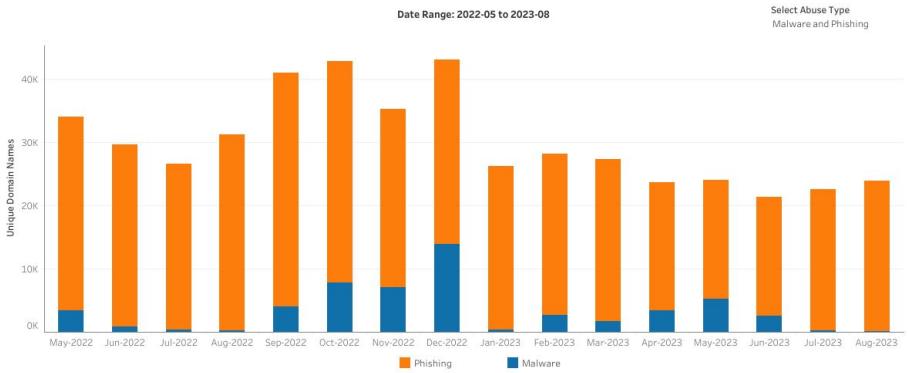
- **All measurement is best efforts** →
  - Quality of input is an issue, false positives, phishing simulations, grey areas: not enough evidence to decide (e.g. Blog)
- **Skewed data** → rarely normal distribution
  - Time & DNS ecosystem
- **Small numbers** → e.g. small ccTLDs
- **Geographical** bias? → is English a target language?
- **ccTLDs** → zone size and new registrations

Public Reporting

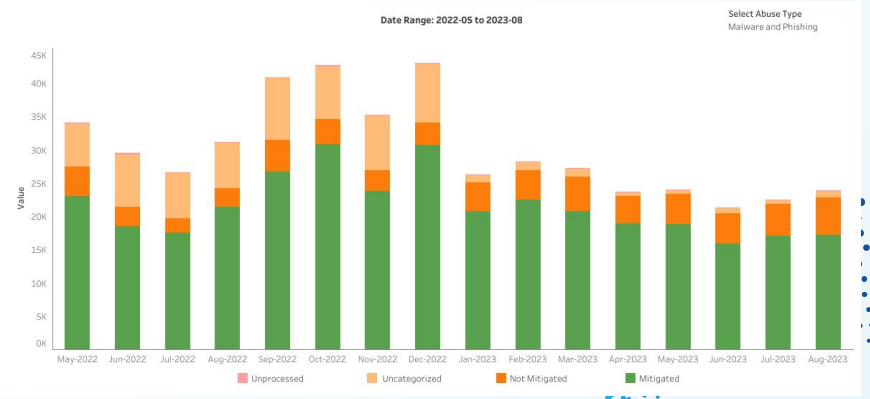
Interactive Charts

DNS ABUSE INSTITUTE

Aggregate Trends



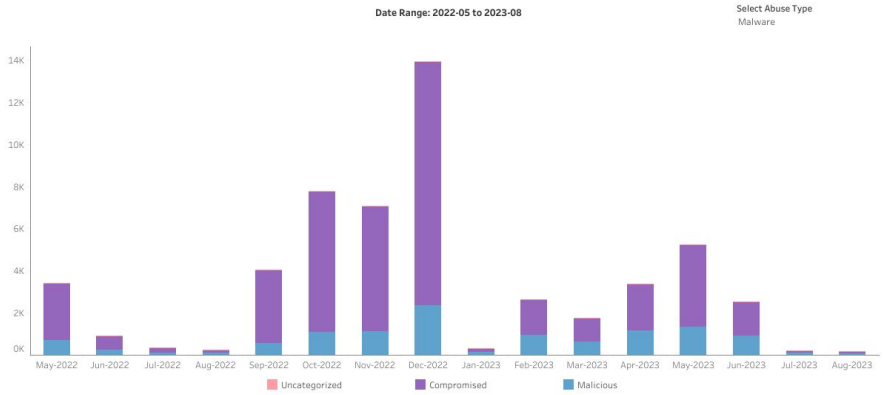
Mitigation

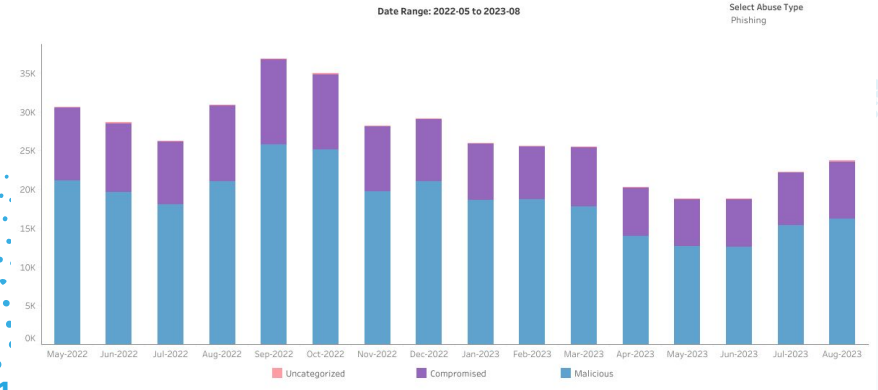


https://dnsabuseinstitute.org/dnsai-compass/

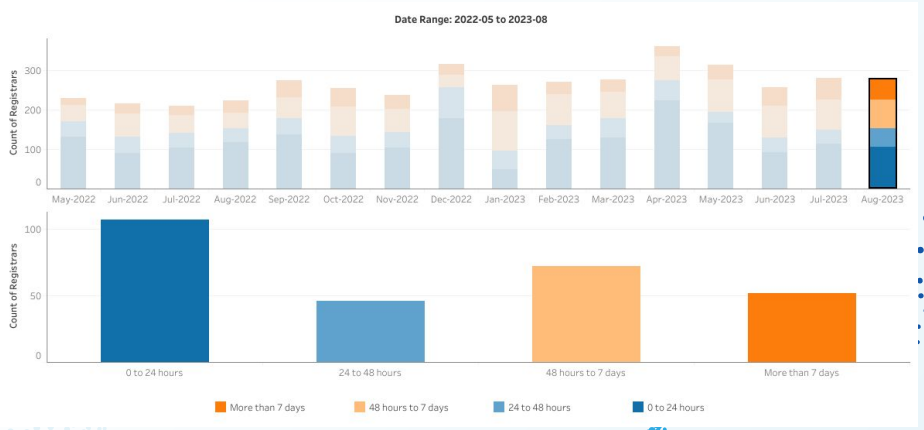
DNS ABUSE INSTITUTE

Malicious vs. Compromised





Registrar Median Mitigation Time



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

DNS ABUSE INSTITUTE

Public Reporting

PDF Reports

DNS ABUSE INSTITUTE

PDF Reports

DNSAI Compass

The DNS Abuse Institute launched DNSAI Compass to measure the use of the DNS for phishing and malware. To ensure accuracy and objectivity, KOR Labs, an experienced, independent, third-party, has developed the methodology and conducts the data gathering and technical analysis. Read the background on this initiative. Register to ensure you receive a complementary copy of the Compass reports.

DNSAI Compass Dashboards
Visibility with Context

NEW DNSAI Compass Dashboards are available to registrars and registries to better understand the measure of their DNS abuse and their ability to mitigate compared to peers in the industry.

Compass Dashboards provide registries and registrars access to individualized data on phishing and malware that can be used to track and measure the prevalence of abuse as well as how their processes and policies make an impact over time. The data is sharable and can be used to make internal improvements, report on progress and encourage greater awareness and collaboration on future solutions in the industry. **Read our blog post for more detail.**

Registries and registrars interested in accessing the data will need to agree to the DNS Abuse Institute's Terms and Conditions as well as apply for access via an online form. Requests for access can be made to support@dnsabuseinstitute.org.

Methodology

Read detailed information about the academically robust methodology used to generate the DNSAI Compass reports, performed by KOR Labs. Access the full document.

COMPASS REPORTS

Monthly reporting of DNS Abuse data, measurement & analysis

2023

- OCTOBER
- SEPTEMBER
- AUGUST
- JULY
- JUNE
- MAY
- APRIL
- MARCH
- FEBRUARY
- JANUARY

2022

- DECEMBER
- NOVEMBER
- OCTOBER
- SEPTEMBER

Specific Reporting

Table 5: Registrars with a higher volume of new registrations, in ascending order of lowest observed maliciously registered domains per new domain registration for 2023-08

Inclusion criteria:
- Observed Maliciously Registered Domains: More than 5 per month
- Observed Newly Registered Domains: Equal to or greater than 20,000

IANA ID	Registrar Credential	Observed Maliciously Registered Domains Per New gTLD Domain Registration	Observed Malicious gTLD Domains	Observed Newly Registered gTLD Domains	Observed gTLD DUM
120	Xin Net Technology Corpora..	0.02%	12	68,395	1,345,213
1531	Automattic Inc.	0.03%	7	25,496	1,048,221
886	Domain.com, LLC	0.04%	11	30,283	1,690,231
3817	Wix.com Ltd.	0.04%	26	69,702	2,619,834
1915	West263 International Limit..	0.04%	13	33,503	333,209
1697	DNSPod, Inc.	0.05%	25	48,097	875,166
49	GMO Internet, Inc. d/b/a On..	0.05%	128	240,956	4,147,499
1868	Eranet International Limited	0.06%	16	29,065	336,605
83	1&1 IONOS SE	0.06%	33	53,272	4,437,944
146	GoDaddy.com, LLC	0.09%	942	999,857	63,328,838

Table 11: Larger ccTLDs in ascending order of lowest observed maliciously registered domains per 100,000 DUM for 2023-08

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

TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
ca	0.28	9	3,267,450
it	0.35	11	3,164,208
nl	0.35	21	6,039,856
de	0.70	116	16,633,162
uk	0.71	73	10,315,710
tk	0.73	32	4,383,885
ch	0.76	19	2,510,401
es	0.79	16	2,036,154
ir	0.87	11	1,265,606
eu	0.87	32	3,671,624

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

DNS ABUSE INSTITUTE

Private Reporting: Dashboards

pir DNS ABUSE INSTITUTE

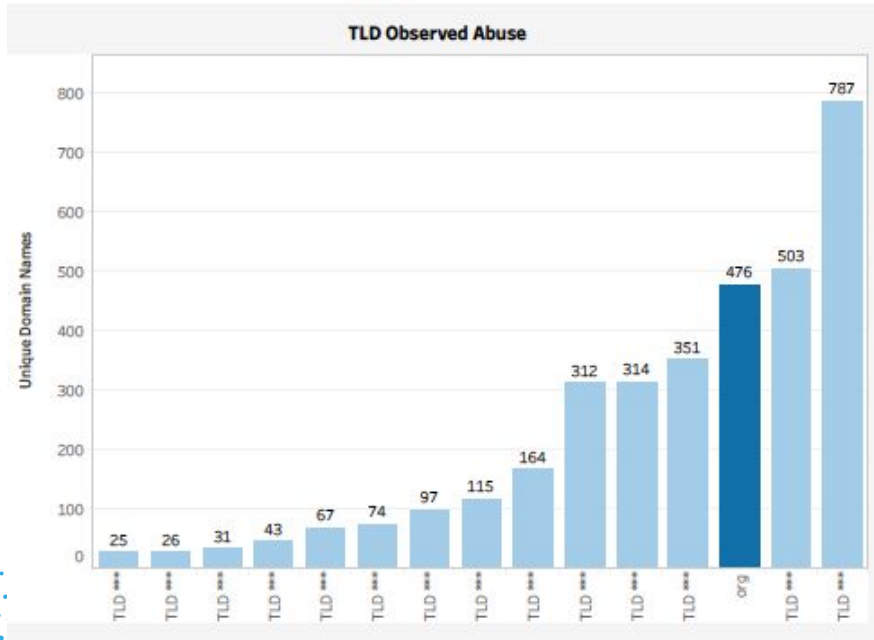
Why?

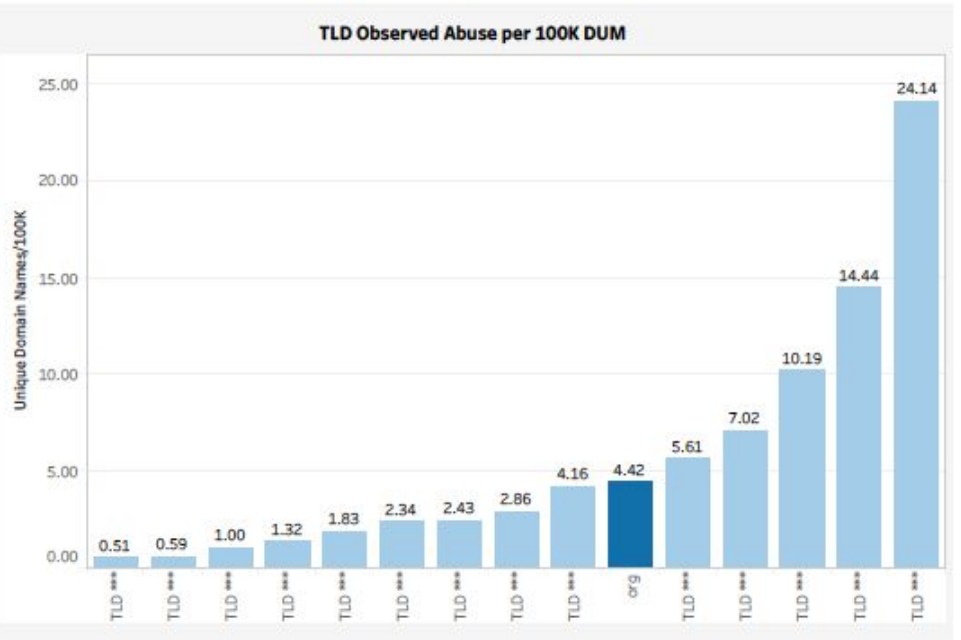
- How much phishing and malware do I have? Is it being mitigated?
- How does this compare to peers?
- How does it change over time?
- If you implement new policies, practices etc. do they make an impact?
- Free!

Example Compass Dashboard

Example Dashboards: .org

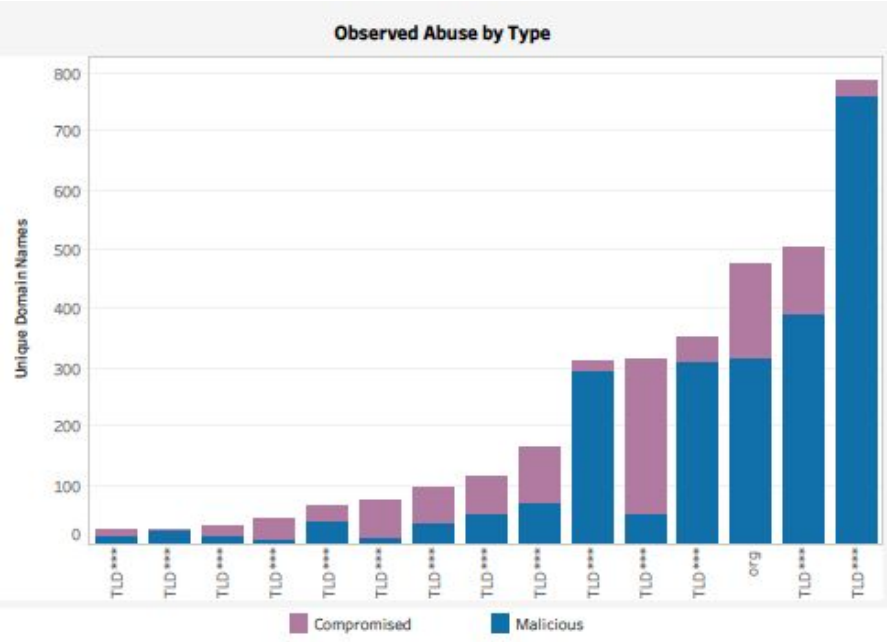
Example Dashboards: .org (peer comparison)

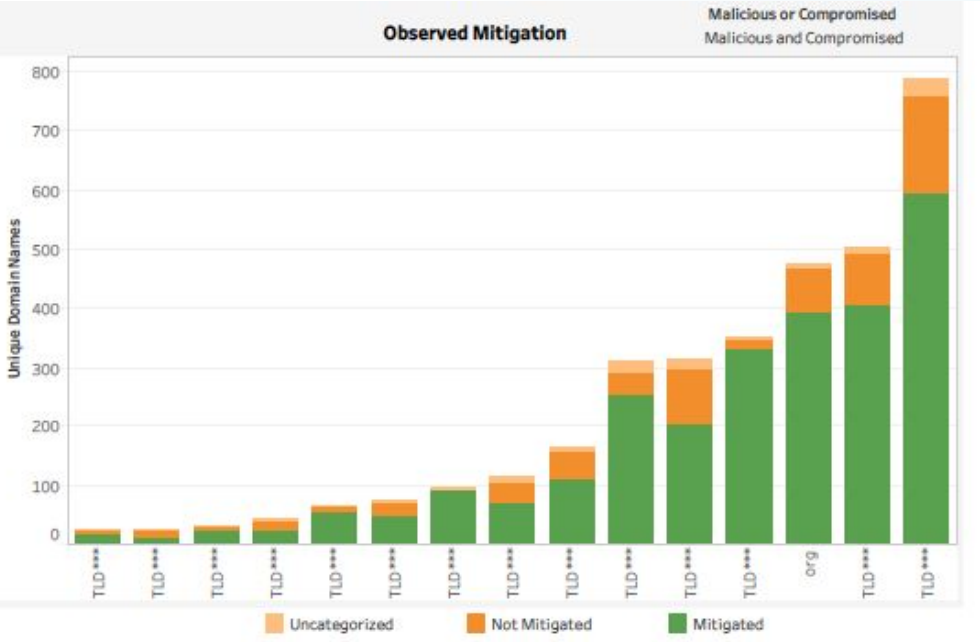




DNS ABUSE INSTITUTE

Example Dashboards: .org





DNS ABUSE INSTITUTE

Summary

Understanding phishing and malware across the ecosystem → visit our public reporting: dnsabuseinstitute.org/dnsai-compass

To access your own data, email support@dnsabuseinstitute.org

DNS ABUSE INSTITUTE

Thank you!

Questions? Feedback?

Rowena Schoo

rowena@dnsabuseinstitute.org

DNS ABUSE INSTITUTE