

DNS Abuse Mitigation Strategies: Ensuring a Secure Online Environment

Sourena Maroofi, Karen Yousefi

DNS Abuse?

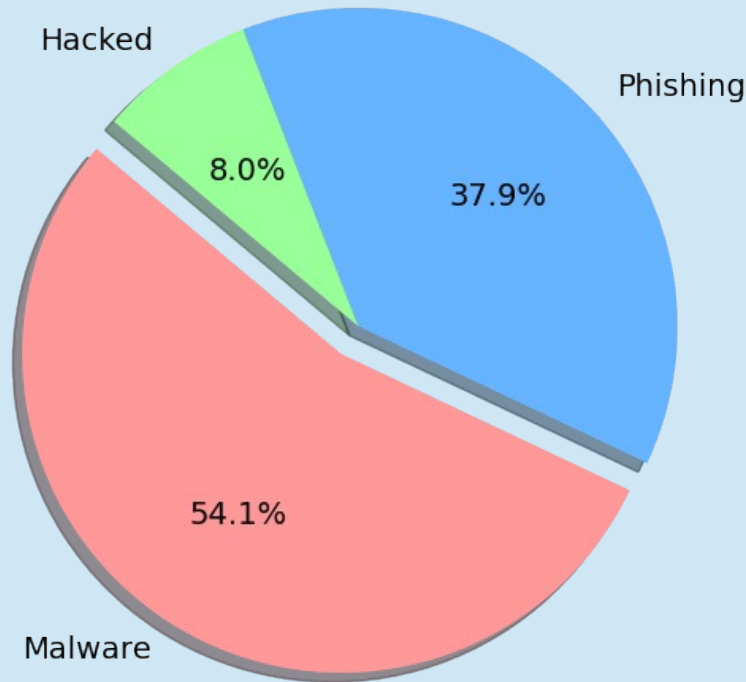
- What is DNS abuse?
 - The Definition by DNS Abuse Framework¹
- DNS Abuse Detection vs. Mitigation
- What we do at URLAbuse (urlabuse.com)
 - Detection and mitigation (sometimes even more)

¹ <https://dnsabuseframework.org/>

History and statistics

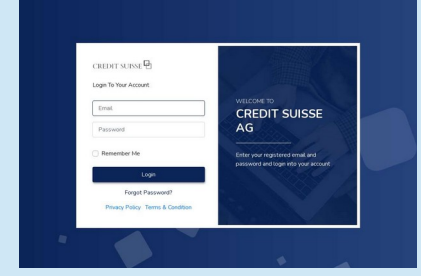
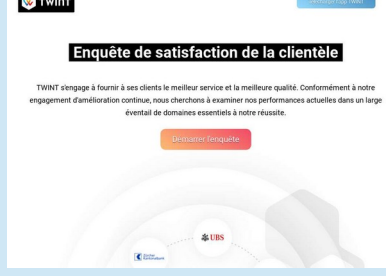
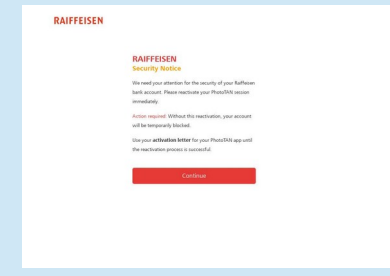
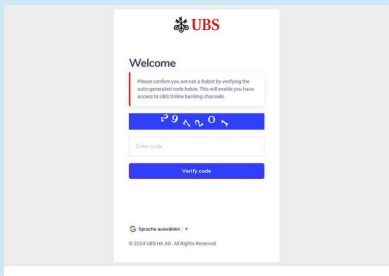
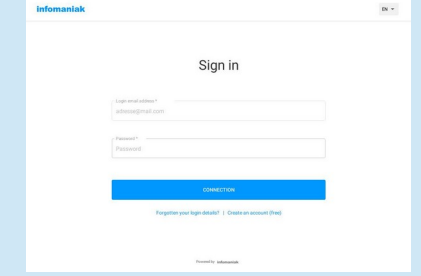
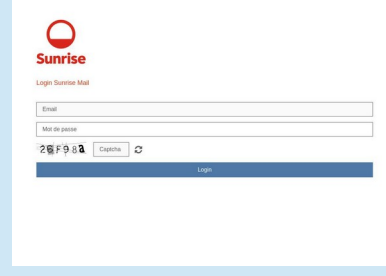
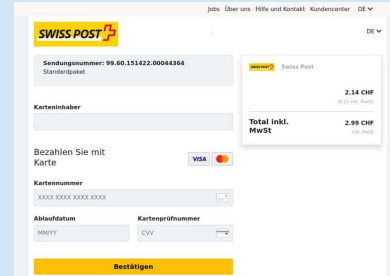
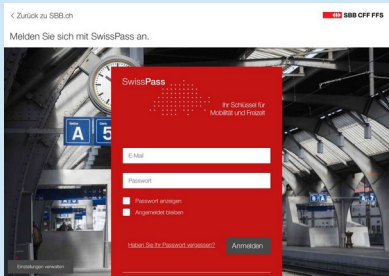
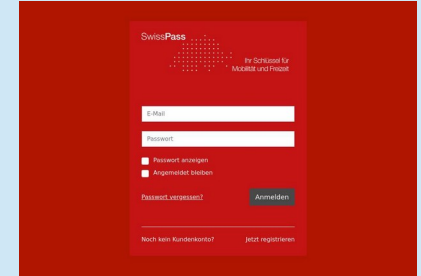
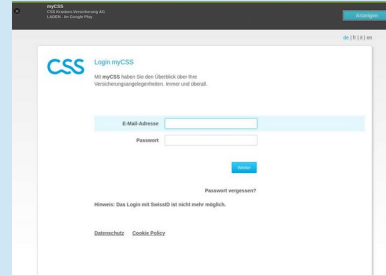
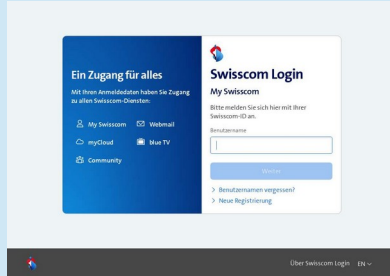
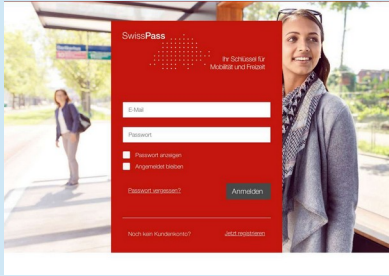
- Project started in September 2023
 - We wanted to have an open, free feed
 - Any company, organization can benefit from it
 - More publicity helps us taking down malicious domains faster
 - Providing actionable evidence for each record
 - Everyone can participate in the feed
 - Design your own algorithm, publish data under your name
 - Permissive license (CC-BY 4.0)

Statistics

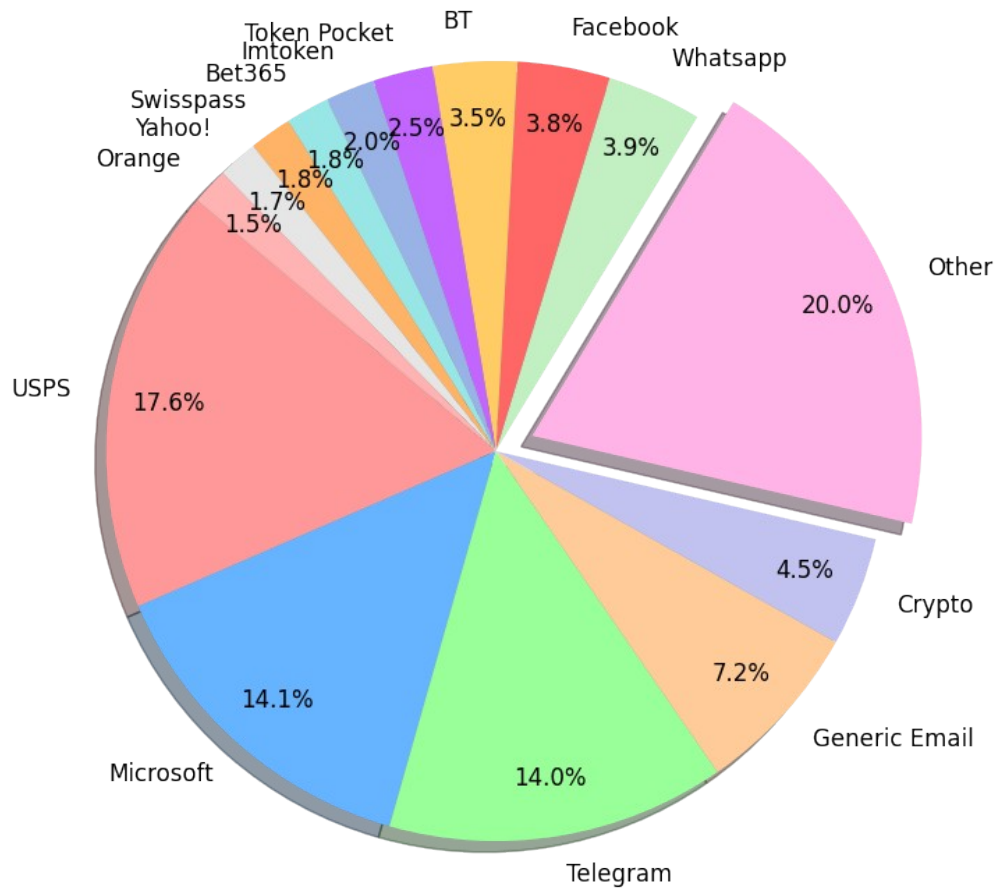


- Number of phishing: 102,980
 - Number of Malware delivery: 146,881
 - Number of hacked: 21,721
-
- Total: 271,582
-
- All the data (even the whole database) are publicly available on the website, receiving updates (every day).

Statistics (Switzerland)



- This is just the statistics of URLAbuse, not necessarily the global picture of phishing.
- The region, companies and brands we are working with, heavily affect the final results.



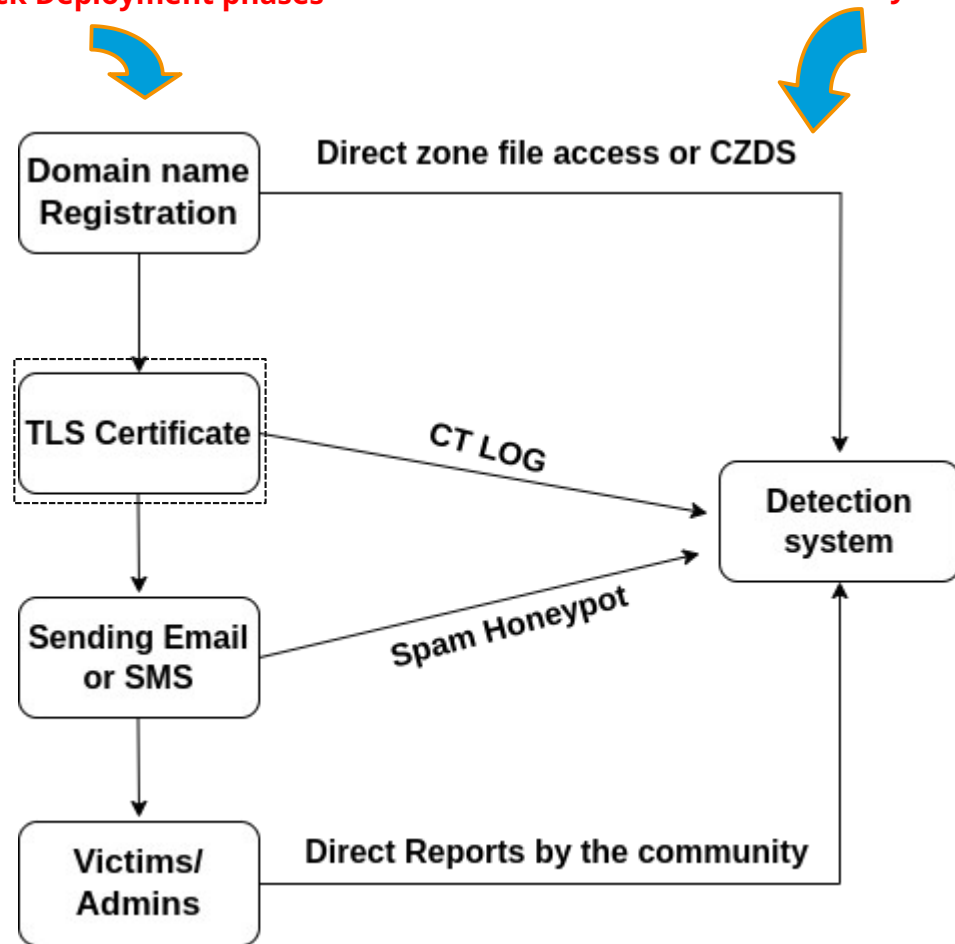
Our Detection system

What are the issues we are facing?

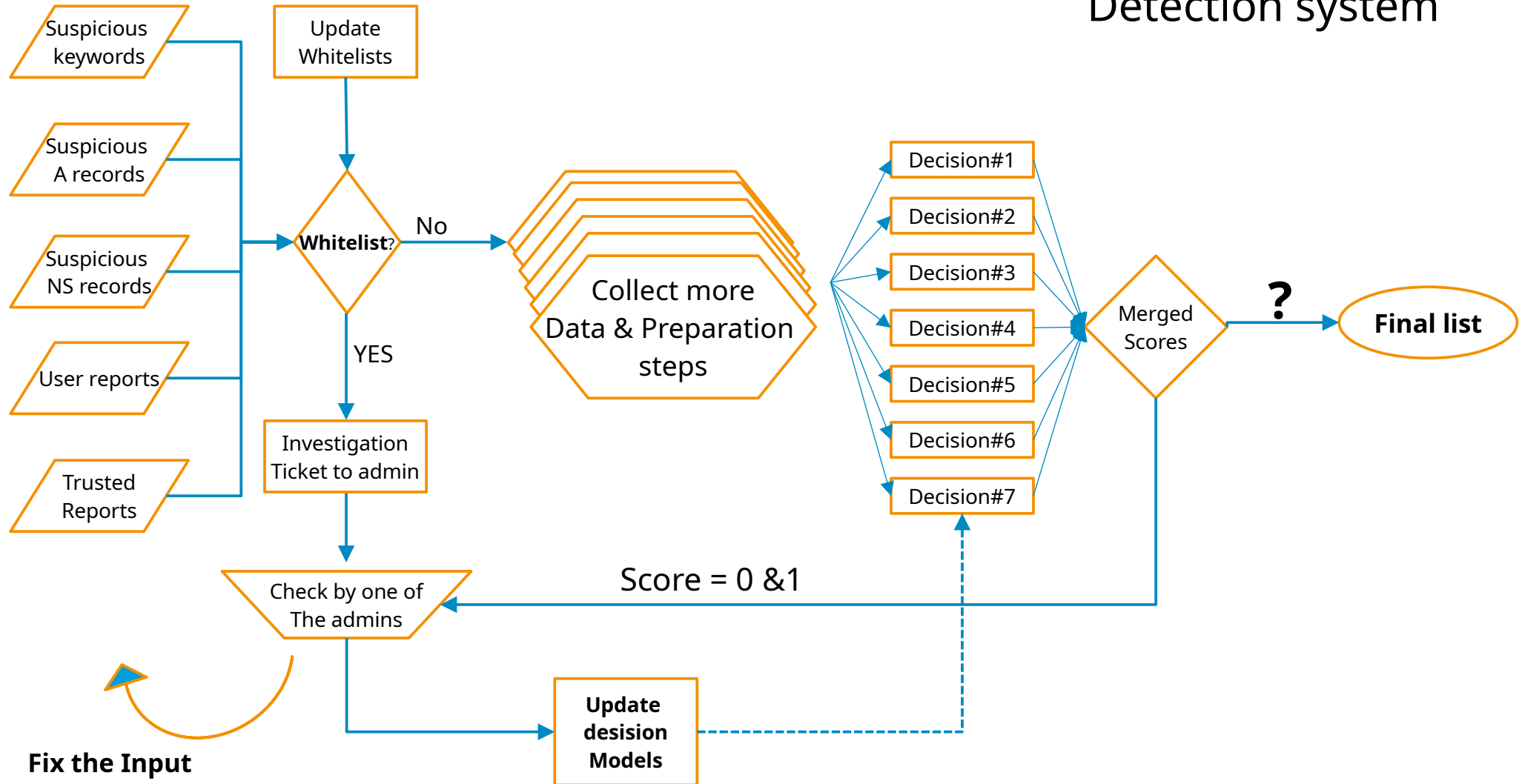
- CZDS: Zone files are updated once per day
- Only a few ccTLDs publish their zone files: ch, se, nu, ...
- We can not always collect WHOIS data
- CT logs are not real-time!
 - Google: almost real-time
 - Comodo: 10 minutes
 - Digicert: 1 hour
 - Cloudflare: 1 hour
- PassiveDNS: Very expensive – needs a lot of resource

Attack Deployment phases

Our detection system



Detection system




Our DNS mitigation system

- Sharing data with Quad9
- Listing domain in our DBL and website
- Direct suspension API from registries
- Trusted report API from registries
- Trusted API from registrars
- Sending emails directly to registries
- Sending emails directly to registrars
- Collaboration through Slack!

But it still doesn't work!

Let's see why it is not effective!

Undeliverable: Urgent Action Required: Phishing Domains

 postmaster@[redacted].com
Thu, 25 Apr 2024 2:13:15 AM +0200
⌚ notify

The mailbox was full for 5 month!

Delivery has failed to these recipients or groups:

[redacted]

The recipient's mailbox is full and can't accept messages now. Please try resending your message later, or contact the recipient directly.

We Submitted a Complaint to ICANN => They fixed it

Let's see why it is not effective!

Complaint Information

Type

Set up phishing and fraud site

Domain

Please enter domain

Please enter url (Not required)

Example: example.com


Example: https://www.example.com/

Add

Description

Please enter 1-1000 digits for details, Please do not enter the above domain and url repeatedly.

Screenshot



Upload

Upload up to 10 images (JPG/PNG), the size of the image shall not exceed 2MB

Complainant Information

Legal Brand URL

Please enter legal brand url

Example: https://www.example.com/ (optional)

Name

Please enter name

For a company, fill in the full name of the company. For an individual, fill in the full name

Contact Email

Please enter contact email

Verification Code

Please enter email verification code

Send code

Submit

☐ I have read and agree to the Declaration.

Send email
verification code for
each report!

Let's see why it is not effective!

Reminder Add task Permalink Snooze

[Redacted]

[Redacted] m

5:14 AM INBOX

karen

Hello

The domain registered is a different company.

urlabuse.com Updated 1 day ago

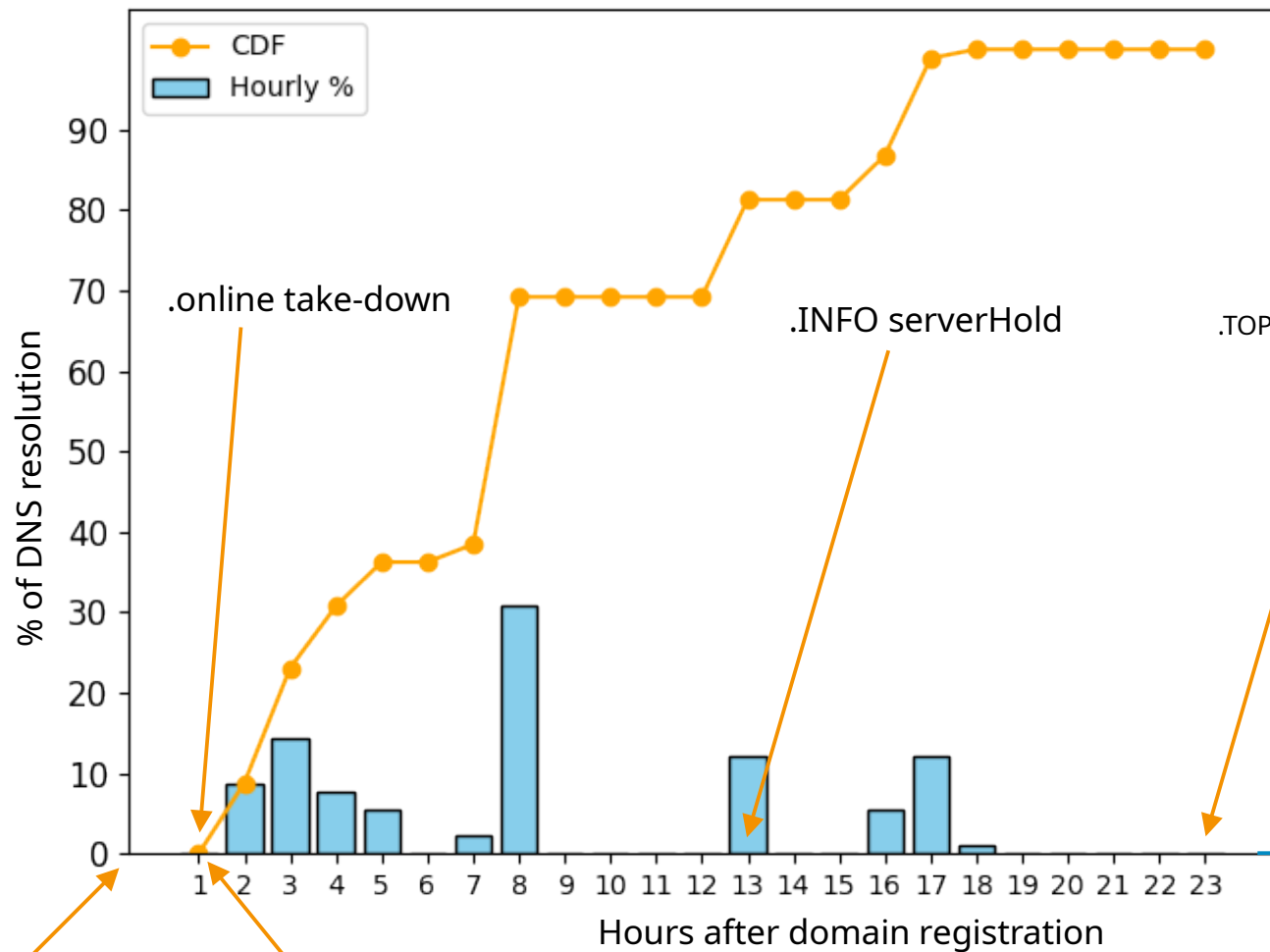
Domain Information	
Domain:	urlabuse.com
Registrar:	NameCheap, Inc.
Registered On:	2023-08-31
Expires On:	2025-08-31
Updated On:	2024-06-03
Status:	clientTransferProhibited
Name Servers:	anna.ns.cloudflare.com chuck.ns.cloudflare.com

@mention a user or group to share this conversation

Hello
The domain registered is
a different company

.TOP Registry case

- 
- Nov/Dec 2023 → Several report to .TOP → no response
 - 5 Apr 2024 → ICANN GLOBAL AMENDMENT TO REGISTRY AGREEMENTS
 - 18 Apr 2024 → Send another batch of domains → no response
 - 24 Apr 2024 → Submitting a Complaint to ICANN
 - 25 Apr 2024 → ICANN sent the report to .TOP
 - 6 May 2024 → got the first response from .TOP
 - 请提供这些域名 DNS 滥用的证据以及凭证。
 - Jul 16 2024 → ICANN issued Notice of Breach for .TOP
 - 21 Jul 2024 → .TOP create an abuse form in their website!
 - 21,28 Jul 2024 → We sent another batch → we got answer!
 - 29 Jul 2024 → .TOP suspended 246 domains
 - 29 Jul 2024 → we reported 4,324 domain names
 - 5 Oct 2024 → .TOP suspended 4,278 domain names



- The chart is based on the data we sampled from our DNS blocklist consumed by Quad9

Natural domain expiration
(1 year)

Conclusions

- Proactive approach is the best and can only be done by registries/registrars
- The fastest approach to take down is to have take-down API access
 - **Not easy to trust third-parties**
- The current approach (sending notification via email) does not work
 - We see more and more phishing everyday
- URLAbuse will continue operating as a public and free feed, encouraging everyone to get involved.
- More visibility → faster malicious domain take-down

Thank You