Collaborative approach to reduce online abuse

Sourena MAROOFI, Karen YOUSEFI

URLAbuse **(urlabuse.com)**

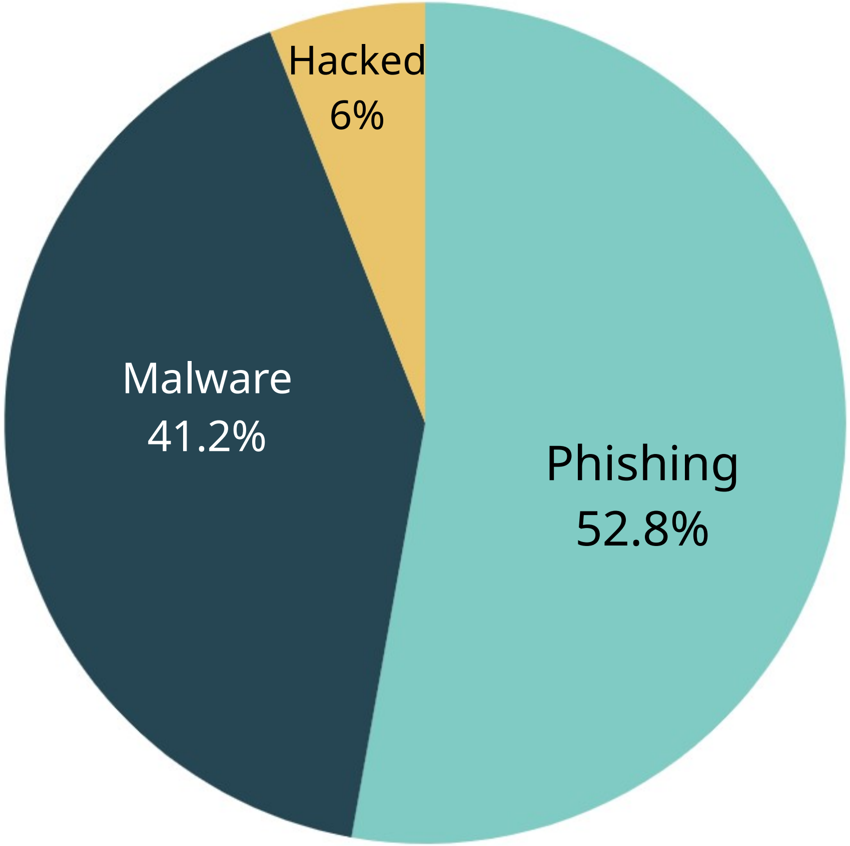
Overview

- Who we are and what we do
- Reports and Achievements of the past two years
- How the system works?
- Collaboration is the key
- Conclusion

URLAbuse:

- **Who we are**: Operating as **URLAbuse** (urlabuse.com)
- **Established**: Launched in 2023
- **Our service**: Accurate and actionable blocklist feed
- **Our mission**: To identify and report a wide range of DNS abuse cases
  - Phishing, malware links, hacked, scam, bet, fake-shops, lame delegation
- **Our goal**: reducing DNS abuse – keeping netizens safe
- **Our approach**: Collaborating with registries, registrars, hosting services, public resolvers, CERTs, payment systems, and researchers

Statistics



- Number of phishing: 225,943
- Number of Malware link: 175,937
- Number of hacked: 25,665

Total: 427, 545

- All the URLs with the same FQDN are considered as one entry

Top Targets of phishing attacks

This table has NO added value!

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

Target	Frequency
USPS	15.37%
Telegram	10.56%
E-Zpass NY	8.61%
Microsoft	7.30%
EZDriveMA	6.82%
Generic Email	3.69%
Crypto	3.30%
SunPass	2.88%
The Toll Roads	2.43%
Others	39.03%

Daily operations

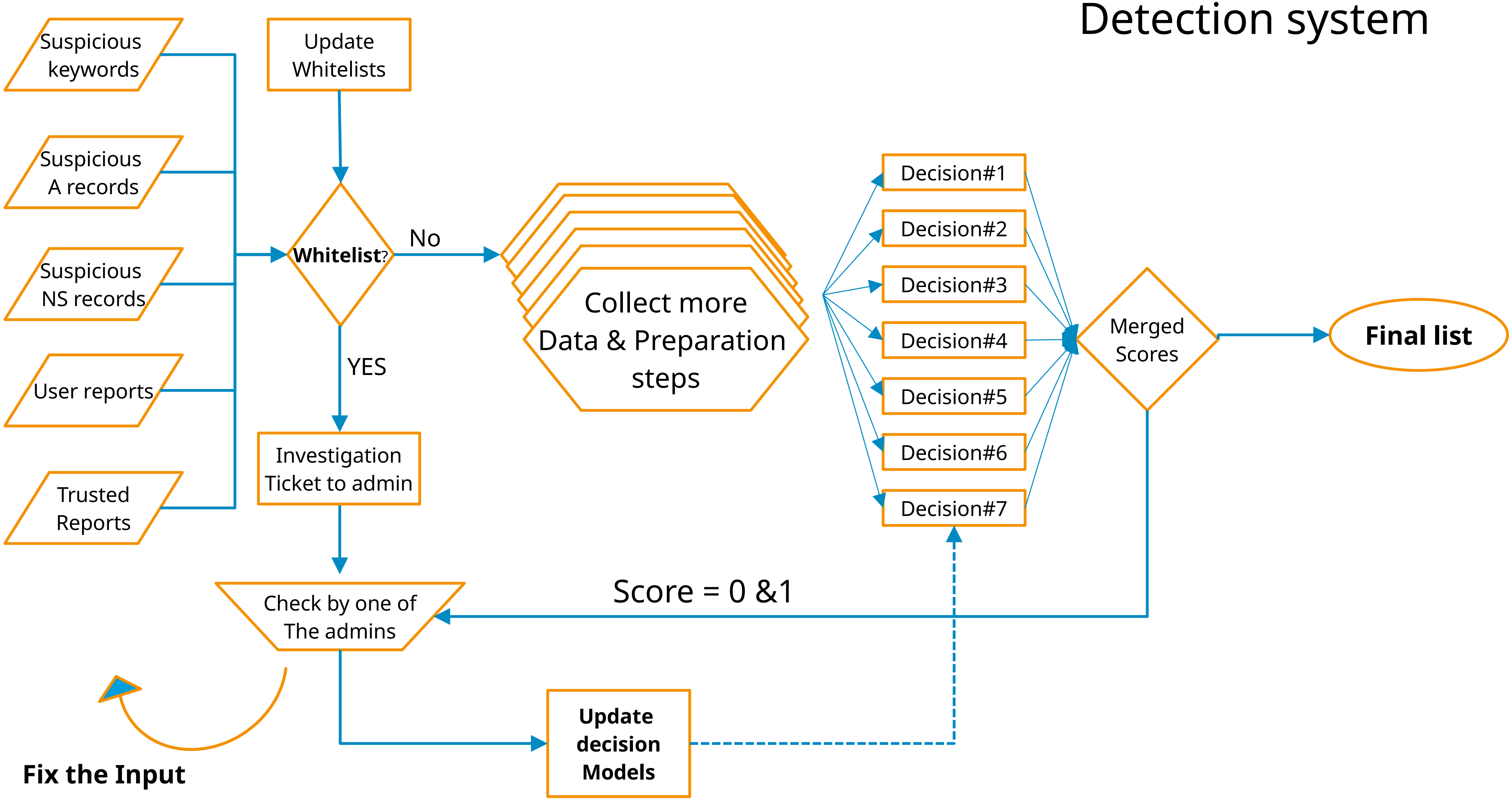
- 74K daily requests from 2.38K unique IP addresses
- Sharing data with Cloudflare (Trusted reporter)
- Sharing data with Quad9 (DNSBL)
- Running our own DNSBL (dbl.urlabuse.com)
- Sharing data with registries and registrars
- Sharing data with European MISP
- Receiving URLs, and domain names from security researchers, and companies
- Measuring DNS records of more than 200M domain names per day
- Measuring records (Detection, collection, screenshots) of 4M URLs per day.
- Following more than 16 phishing-as-a-service campaigns (currently)

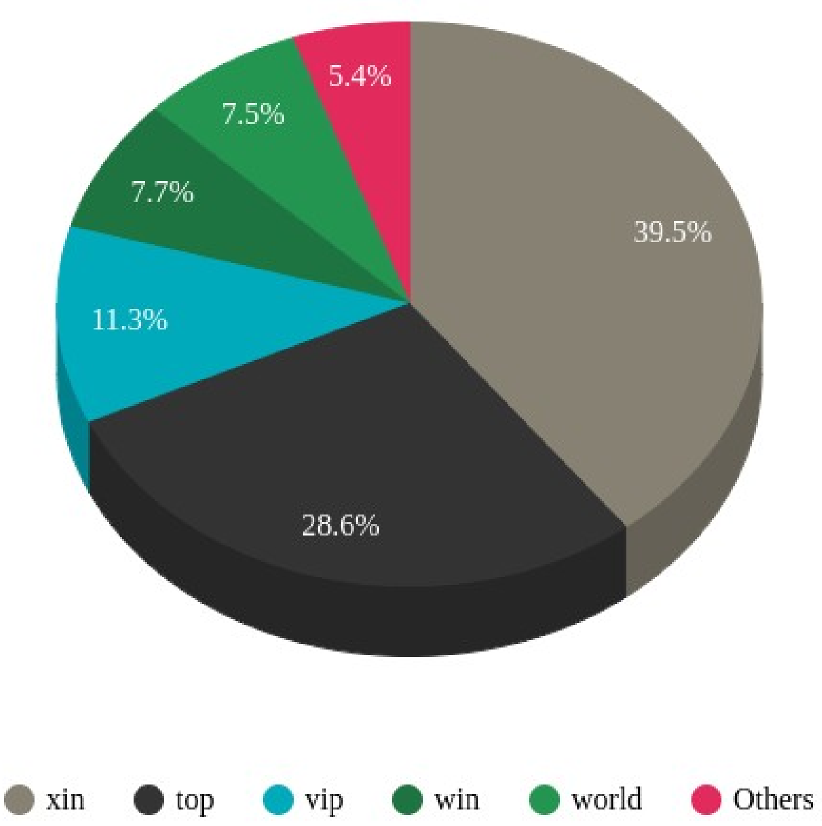
```
(globalenv) srn@srnpc:~$ dig @dbl.urlabuse.com uspsfio.top.dbl.urlabuse.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @dbl.urlabuse.com uspsfio.top.dbl.urlabuse.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55888
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;uspsfio.top.dbl.urlabuse.com.          IN      A

;; ANSWER SECTION:
uspsfio.top.dbl.urlabuse.com. 300 IN    A       127.0.0.2

;; ADDITIONAL SECTION:
uspsfio.top.            300     IN      TXT     "TARGET: USPS"

;; Query time: 51 msec
;; SERVER: 135.181.151.12#53(dbl.urlabuse.com) (UDP)
;; WHEN: Fri May 16 10:45:14 CEST 2025
;; MSG SIZE  rcvd: 109
```

We wrote our own DSN server to serve DNSBL. You can also give it a shot!

github.com/maroofi/bulkDNS

Detection system

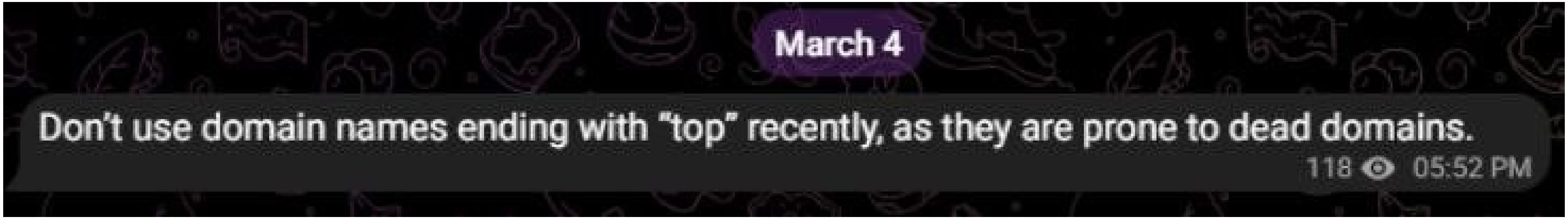




- **We have taken down 132,203 maliciously registered domain names in the past 12 months!**
- **We sent 16,476 domains to Cloudflare API**

- What is the sense of scale here?
- Is it effective? Yes and No

Forcing batch registrations to shift to other TLDs



March 4

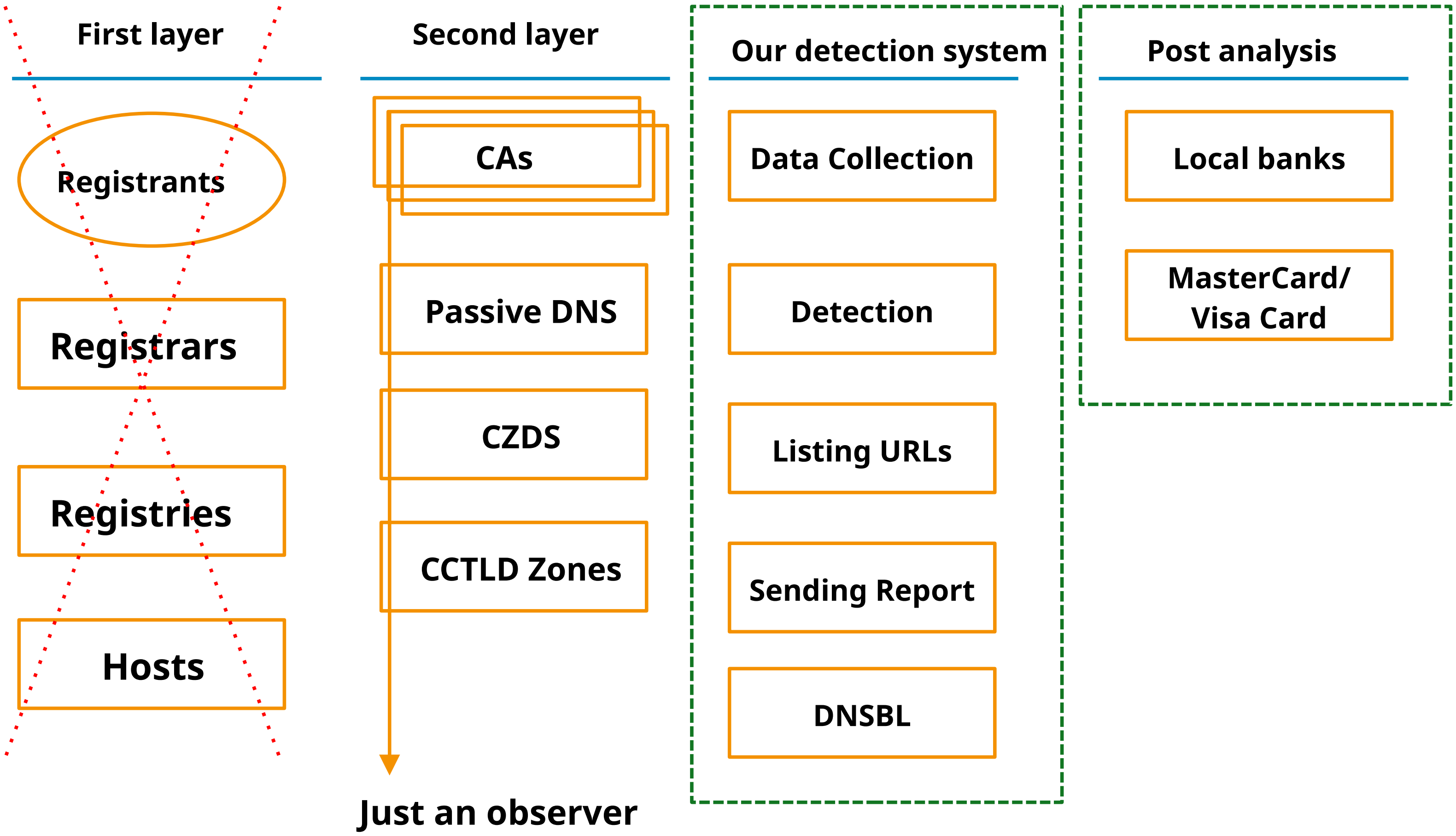
Don't use domain names ending with "top" recently, as they are prone to dead domains.

118 05:52 PM

.TOP → .XIN → .WIN → ?

- Is this something good to force them to switch TLDs? I don't know
- What happens if they move from new gTLDs to ccTLDs or gTLDs?

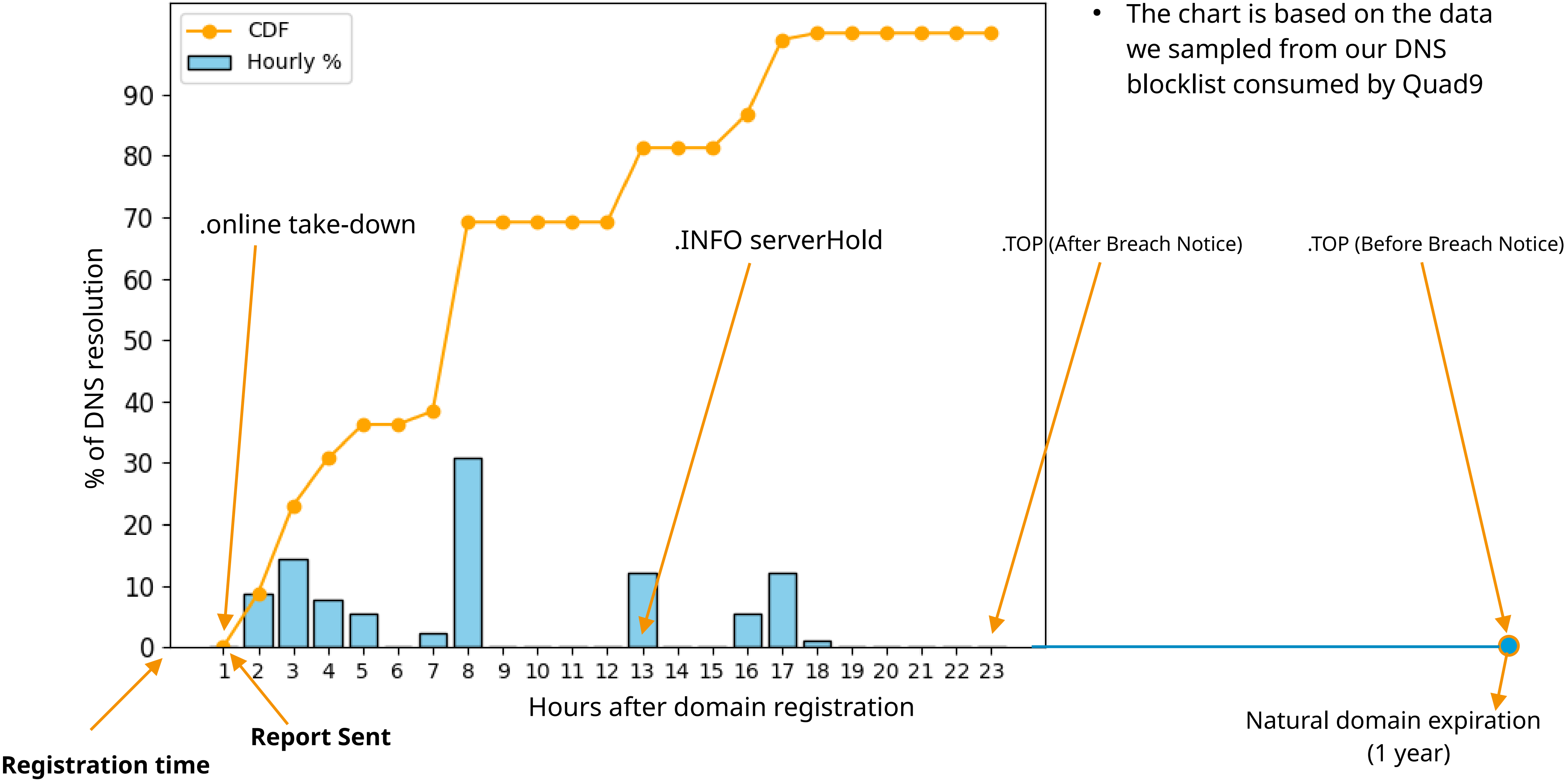
Possible involved entities in this system?



Common problems we have when dealing with registrars and registries?

- Abuse mailbox is full!
  - Took us 5 months to tell them!
- Lack of trust (specially in geofenced attacks)
- Emails marked as spam (constantly happening)
- Webforms instead of emails for notifications
  - Either we have to solve CAPTCHAs or one-time email verifications
- Each registry/registrar has a different request
  - Some need batch report
  - Some ask us to send report to third-party companies
  - Some need .CSV format with specific fields!

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



.online take-down

.INFO serverHold

.TOP (After Breach Notice)

.TOP (Before Breach Notice)

Registration time

Report Sent

Natural domain expiration
(1 year)

What about ccTLDs?

- We don’t work that much with ccTLDs. Why?
  - Cost-benefit trade-off
  - More sophisticated attacks on ccTLDs
  - More Compromised domains rather than maliciously registered ones
  - Closed zone files (most of them)
  - No obligation to respond
  - They don’t share data with us since they can simply take them down
  - Some ccTLDs are super clean (e.g., .nl)

How you can collaborate with URLAbuse

- The data you submit to our system is published publicly
  - We collect all the necessary information related to your record
- You can track the data you submit to our system until it is taken down
- No payment involved in contribution or using the data provided by contributors
  - It is free and it will be always free!

- What we want from YOU?
  - We would like to use your expertise in handling DNS abuse

Conclusion

Collaboration is not a good approach to handle DNS abuse…

IT’S THE **ONLY** POSSIBLE APPROACH

- Time is the key factor.
  - What is the appropriate response time?
- ICANN Registry agreement (Jan 2024) is effective?
  - Yes, it’s probably the best amendment ever

acknowledgment

I would like to thank:

- AFNIC, SIDN and UGA for providing the opportunity for doing PhD
- KOR Labs – for supporting URLAbuse project
- My colleagues at URLAbuse who dedicate their time—entirely on a volunteer basis—to keeping the feed running and accessible

Question? Comment?

Email & Slack: maroofi@urlabuse.com