


Insights into Blocklist Feeds and Phishing Detection

Sourena MAROOFI, Karen YOUSEFI

 URLAbuse(urlabuse.com)

October 7, 2025

Topics We'll Cover

- Phishing by the Numbers
- Why Phishing Is on the Rise
- Current take-down procedure
- Current blocklist feed methodologies
- Why do we need a modern blocklist feed
- How things work at URLAbuse (urlabuse.com)
- News: Our new platform is alive!

Phishing by the Numbers

Interisle yearly statistics of maliciously registered domain names:

- 2022 → 2023: **+23.3%**
- 2023 → 2024: **+21.0%**
- 2024 → 2025: **+35.8%**

APWG, PhishTank, OpenPhish, Spamhaus

NETBEACON Institute July statistics of maliciously registered domain names:

- July 2022 → July 2023: **-14.6%**
- July 2023 → July 2024: **+60.9%**
- July 2024 → July 2025: **+8.1%**

APWG, PhishTank, OpenPhish

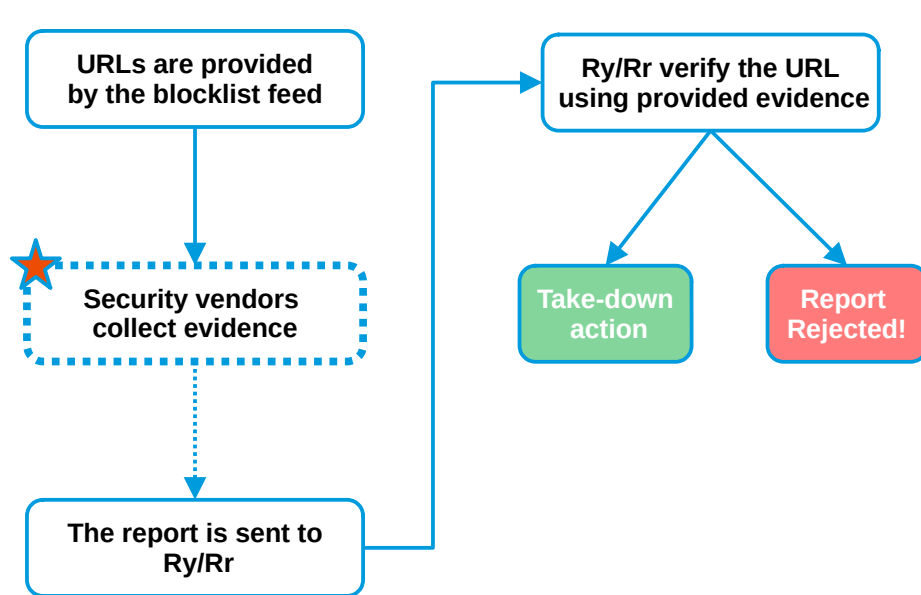
* They both use the same methodology similar to COMAR for distinguishing maliciously registered domains from compromised ones

Time to ask ourselves these questions!

- Why is the amount of phishing increasing each year?
- What factors are driving the increase in phishing attacks?
- Which part of the phishing-fighting ecosystem has a flaw?
 - Registries ?
 - Registrars ?
 - Reporters ?
 - Source of data ?

None of them. The gaps appear in coordination, not capability

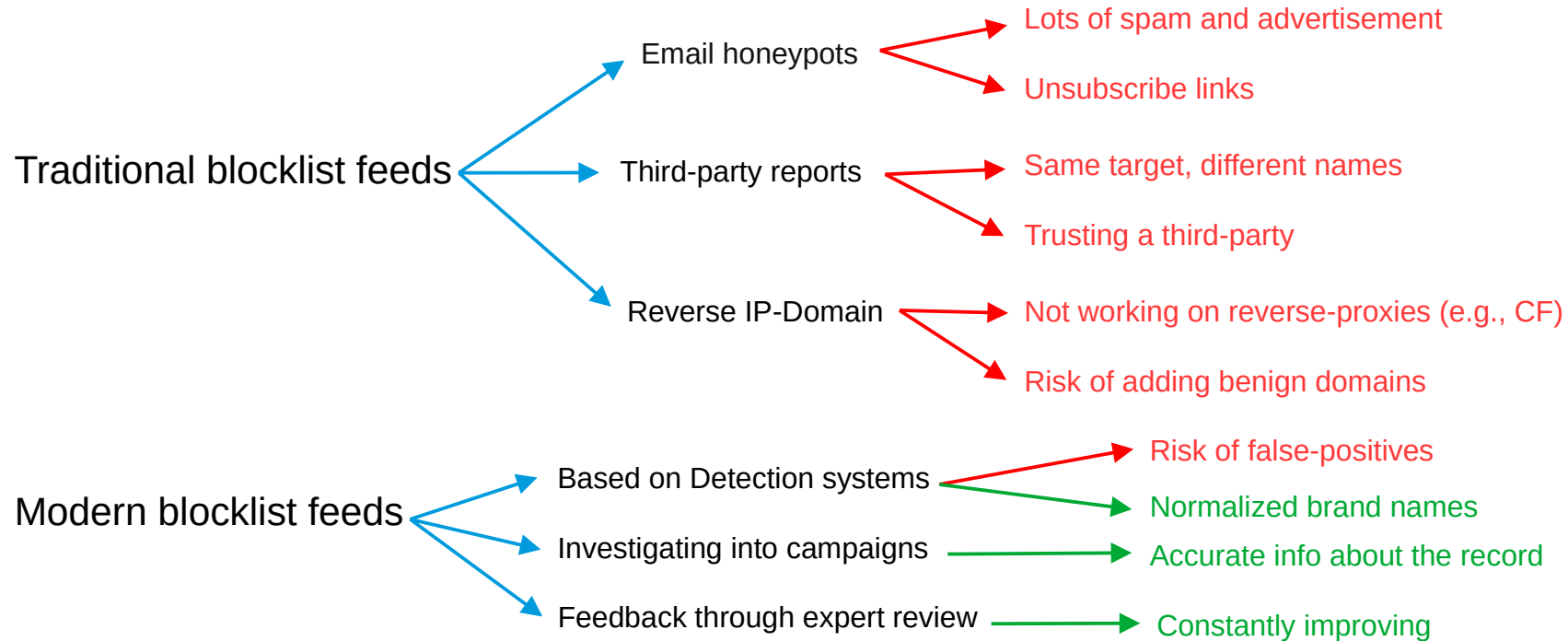
Let's see how the ecosystem works



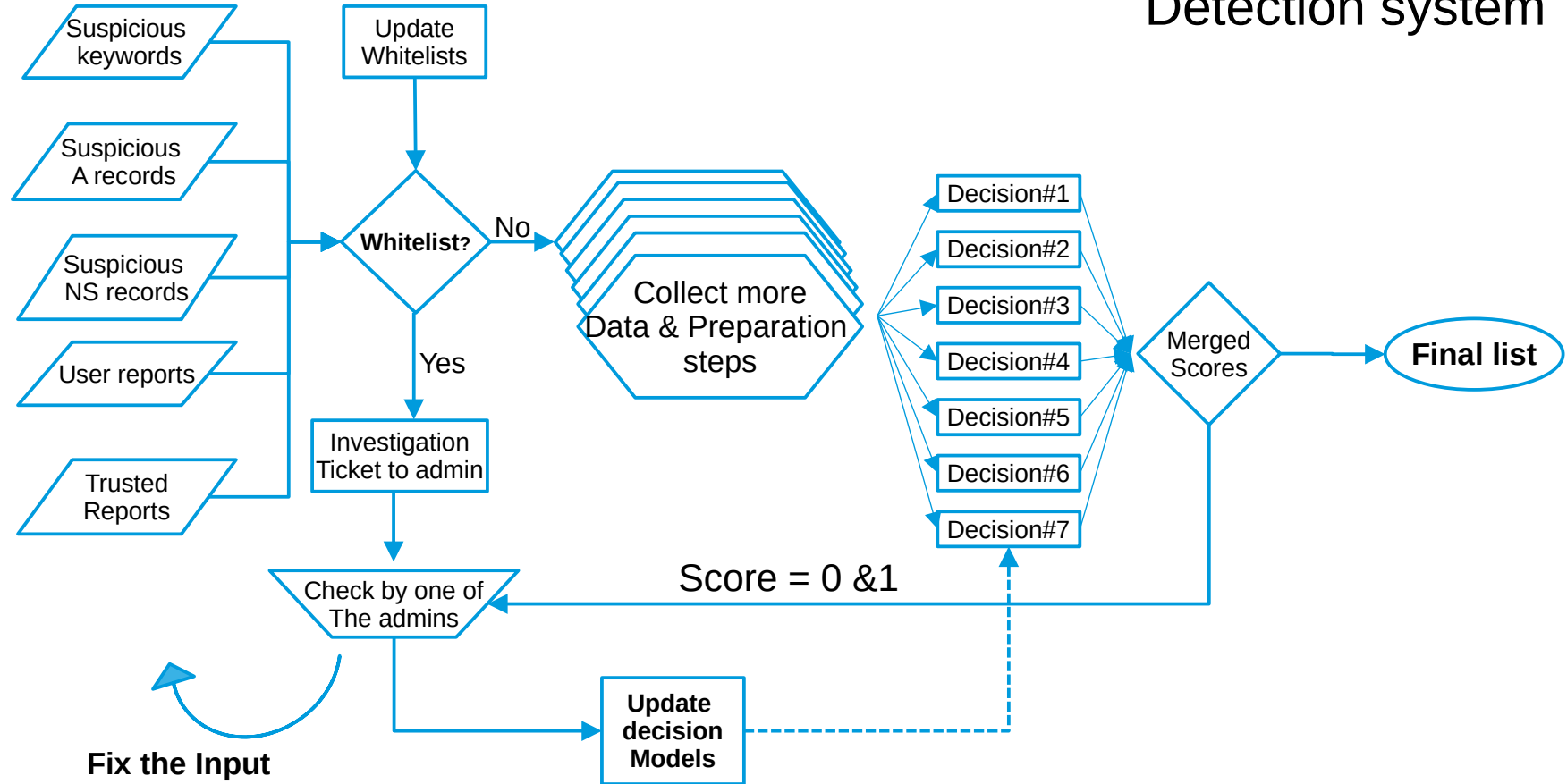
- Are the security vendors able to collect enough evidence based on the received URL from the blocklist feed?
- It's difficult to collect evidence if:
 1. You don't have enough information about the attack!
 2. Not knowing the methodology behind the collected URL
 3. Right IP address
 4. Right time
 5. Right path
 6. Right User-Agent
 7. Right header information

Who is in the best position to collect evidence?

Different types Blocklist feeds



Detection system



What we do at URLAbuse

- Analyze phishing campaigns and phishing-as-a-service infrastructures
- Train robust models for detecting phishing attacks
- Provide actionable intelligence to support the take-down process
- Perform real-time data analysis
- Scan hundreds of millions of FQDNs daily
- Verify every third-party report and data entry for accuracy

Help us fighting DNS Abuse

- If you are a reporter → receive a token from us to report URLs
- If you are a registrar/registry → start consuming data
- If you are a researcher → Use our data, build your own detection system

We're happy to help you improve your system — just reach out and ask!

THANK YOU

Contact: maroofi@urlabuse.com (Email and Slack)