



Disrupting the Internet in the name of copyright: An Italian Story

Raffaele Sommese, Anna Sperotto, Antonio Prado,
Jeroen van der Ham, Antonia Affinito

IETF 124 – Thursday 6, November 2025 – IAB

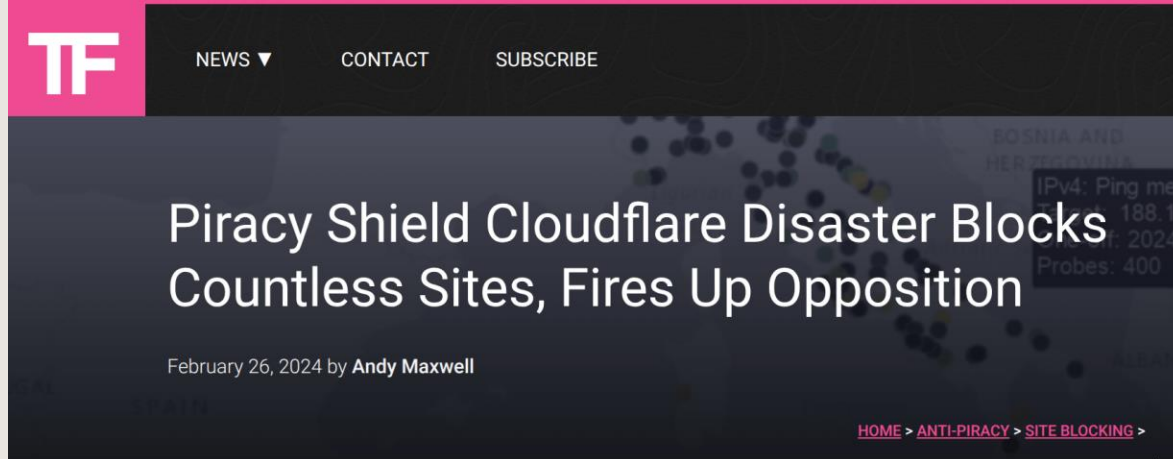
This is an Italian Story

- Of how a small group of (influential) people can convince a country to implement draconian filtering rules
- And of how this can easily go wrong
- All in the name of football
- But **how was** Piracy Shield born?

The Law (Jul 2023)

- Law 93/2023, voted on 12 July 2023
- Unanimously approved by both Chamber and Senate, from all political parties
- The law allows **copyright holders** to request the blocking of IP(v4) addresses and domain names involved as the **sole activity** in **illegal football streaming** – within **30 minutes** of detection
- AGCOM oversees providing a platform to communicate these blocks
- There was no unblocking concept

Bumps down the road...



The new law (Oct 2024)

- IP addresses now need to be used **predominantly** for illegal activities
 - Not the sole activity...
 - There is an official **unblock concept** now (must be requested within 5 days)
 - But the list of blocks is not public!
- VPN and DNS providers are also subject to applying filtering
 - Independently of where they are located
- If an ISP has any suspicion or indication of illegal activity from a user, they need to contact the police
 - Otherwise, they risk 1 year in jail

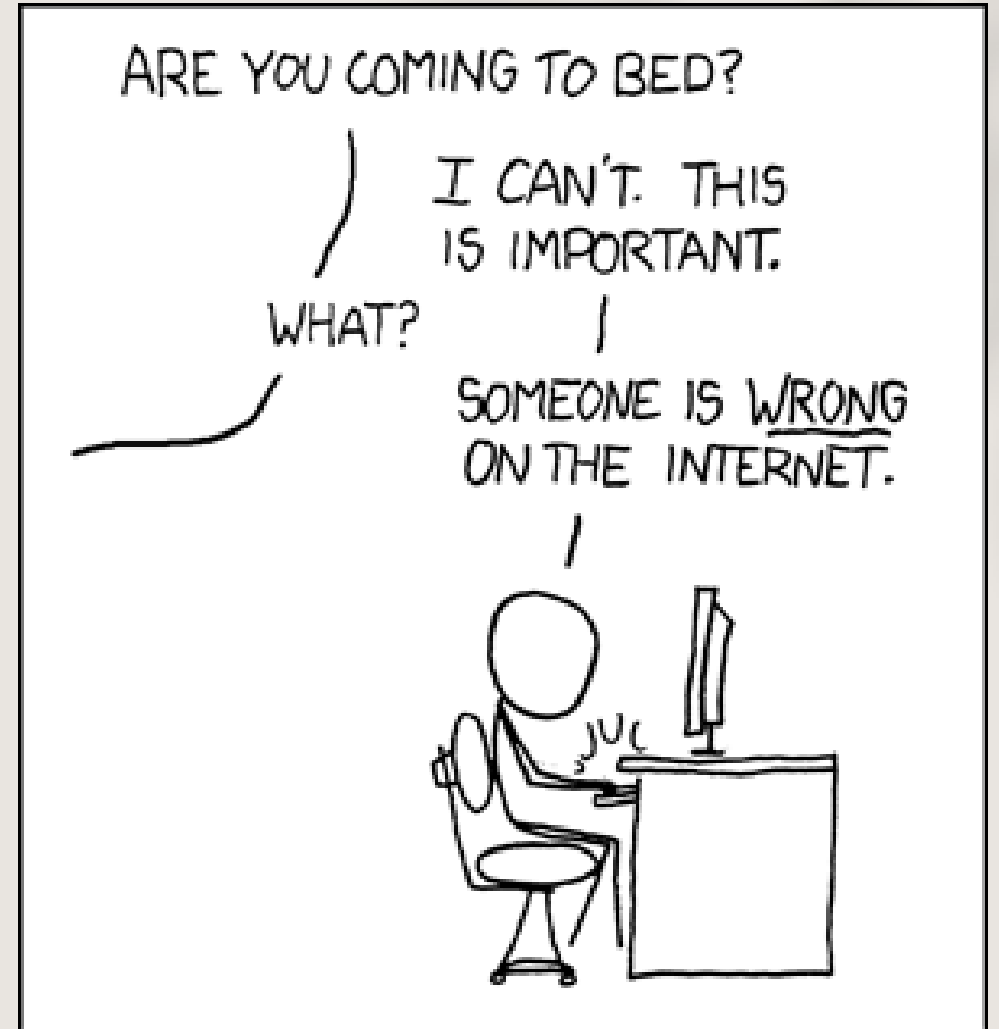
Piracy Shield: A success?

- In short:
 - **Unvetted blocking powers** granted to private entities
 - **No clear expiration** or review process for block orders
 - **Lack of transparency:** no public registry of blocked resources (not even under FOIA)
 - **Collateral damage** incidents affecting legitimate services (e.g., Google Drive, Cloudflare)
- Despite what appears to be a **recipe for disaster**, the Italian communications authority (**AGCOM**) has **defended Piracy Shield**, highlighting the **large number of IPs and domains blocked** as a sign of effectiveness.
- But what is behind the more than 10K IPv4 and 40K FQDNs blocked?
 - What lies **behind** these impressive numbers?
 - Can we **shed light** on the real **costs** of this platform's so-called "success"?

Reconstructing Transparency

The **absence of a public list** of blocked resources made assessing **collateral damage** nearly impossible.

- To overcome this:
 - We used an **unverified leaked list** published on GitHub
 - We **validated entries** through the official AGCOM verification tool and the Infotech (an Italian ISP) website
 - Solving thousands of CAPTCHAs!



Reconstructing Transparency

- Blocking activity (Feb 2024 – June 2025):
 - **10,918 IPv4 addresses** and **42,654 FQDNs** blocked
 - Originating from **3,782 blocking requests** by copyright holders
 - **98% of IPs** and **44% of FQDNs** remained blocked as of **June 2025**
 - Blocking activity **peaked during weekends**
- While the dataset does not include blocks issued **before 2024**, it provides a **solid basis** for understanding the platform's activity.

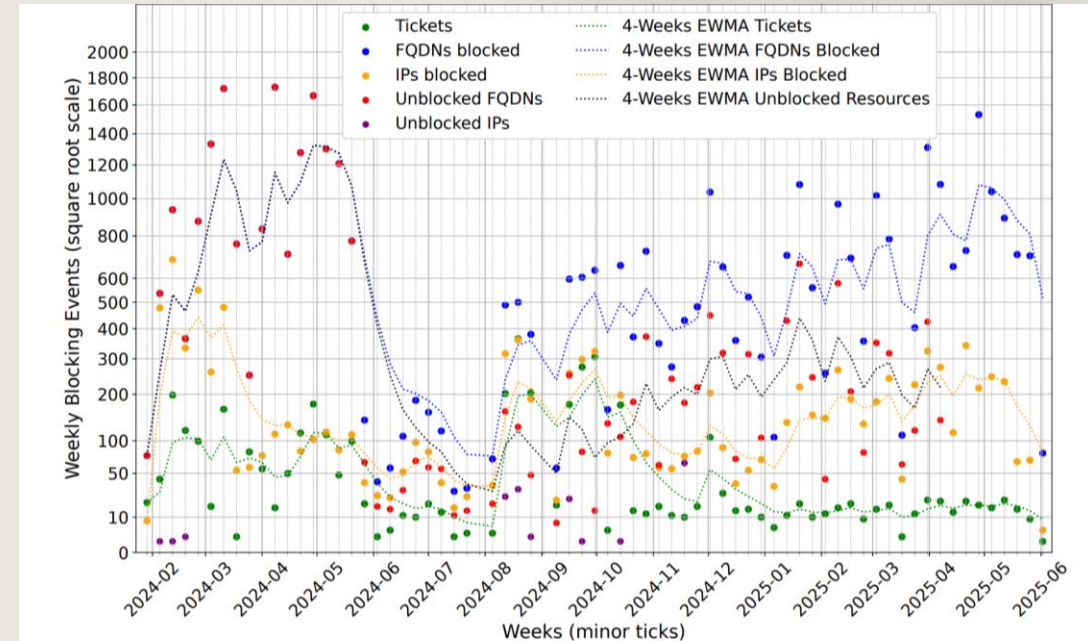


Fig. 1: Weekly blocking and unblocking events with 4-weeks Exponentially Weighted Moving Average (square-root scale)

Pirates with an EU flag on the boat

Of the **10,918 blocked IPs** (across **2,134 /24s** and **262 ASNs**):

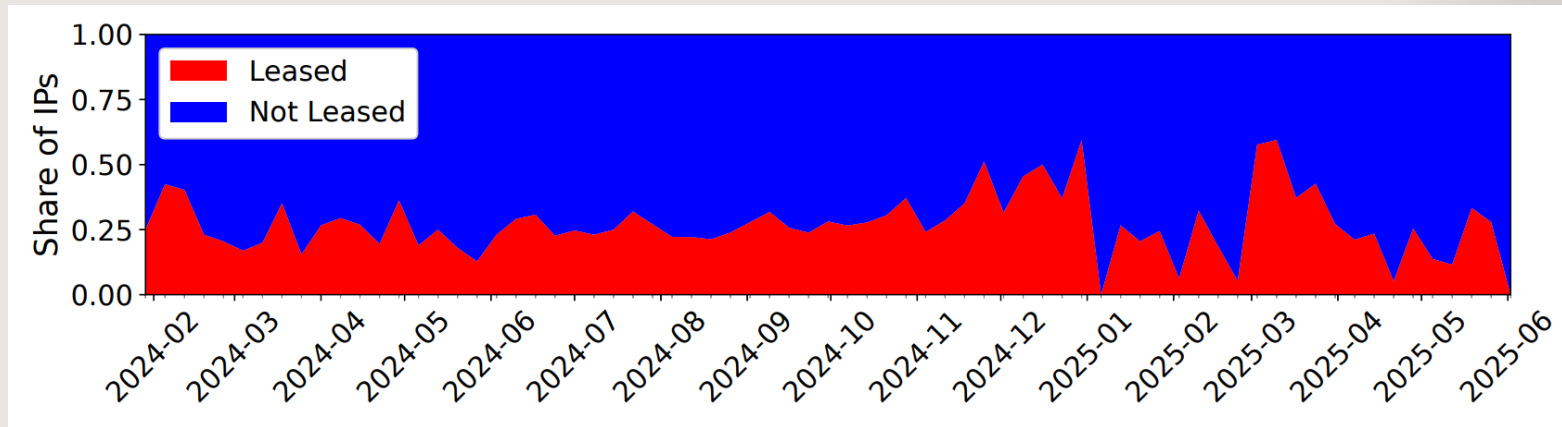
- **77%** geolocated within the **EU**, with **38% in the Netherlands**
- GZ Remittance alone hosted **>9.5%** of all blocked IPs, concentrated in **15 /24s**
- OVH, Scaleway, Hetzner show a different pattern: IPs spread across **diverse /24s**, suggesting **reuse of shared infrastructure** from streamers.



Unblocking activity

- OVH hosts the highest number of **unblocked IPs**, possibly indicating later **benign reuse**
- FQDNs seem more likely to be released to overcome **platform limitations** than real reduction of harm.
- Illegal streamers **abandon** older resources over time.
- Only **51%** of the blocked IPs are still responsive to probes!
- So, what about collateral damage?

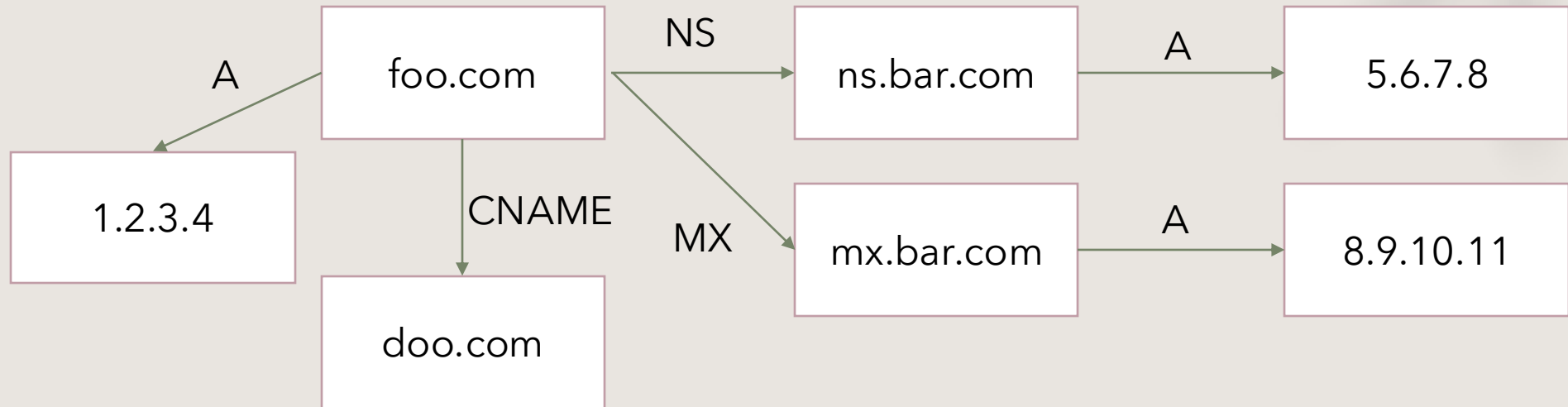
Collateral Damage #1: IP Leasing



- Out of 10,918 blocked IPs, 24% were **leased**.
- Streamers may exploit, consciously or not, the leased IP market, increasing the risk of **collateral damage** for legitimate businesses.
- **4%** of blocked IPs were leased out to new users *after* the block was implemented.
 - With the help of IPXO, we identified **250 IPs** as re-leased to different companies after the blocking date.
- Unsuspecting businesses are acquiring blocked and unusable resources on the Italian Internet.

Collateral Damage #2: Shared Infrastructure

- An IP address can host multiple services or web servers (vHost).
- Collateral damage may happen at several layers:



- Using **OpenINTEL** and **CT Logs**, we assessed collateral damage due to blocking of **web**, **mail** and **DNS** infrastructure.
- We analyzed 262 million domain names, and 1.8 billion FQDNs in search of collateral damage.

Collateral Damage #2: Shared Infrastructure

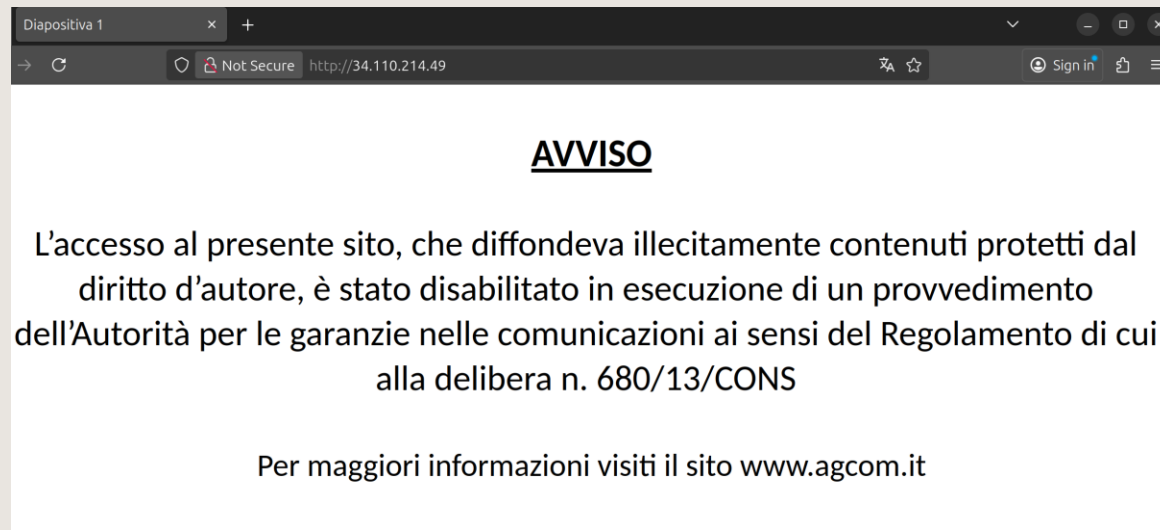
- We identified a total of 7,114 FQDNs collaterally damaged by Piracy Shield
 - Among these, 1,931 responded to HTTP or HTTPS requests.
 - We manually classified **510 non-streaming-related websites** and 617 streaming-related.
 - 131 blocked IP addresses are responsible for 508 cases of collateral blocking.
 - Most legitimate affected websites were in French, Spanish, and German, and **9 in Italian**.
 - One notable case involves **19** legitimate Albanian websites hosted on **a single IP** address assigned to WIIT Cloud. These sites are **still unreachable** from Italy.
- Looking at historical collateral blocking, we found that 7,742 FQDNs were impacted by collateral blocking, 665 of which still active and non-streaming-related.

Delivery Status Notification (Failure)

- Looking at historical blocking, we found an IP address of a major VPS provider (Hetzner) was blocked.
- This IP was rented by a legitimate Portuguese hosting company, immediately disrupting **325** of their domains that used it for nameservers.
- **169** of those domains also relied on the IP for critical email and web hosting.
- The legitimate company was **completely unaware** of the block, only realizing there was a problem after losing email connectivity with their Italian customers.
- Their only recourse was to request a new IP, ignoring that their operations were disrupted as collateral damage of Piracy Shield.

Collateral Damage #3: Anycast and Anti-DDoS

- 176 anycast IPs were blocked.
- With IPs belonging to large Anti-DDoS providers like StormWall, DDoS Guard, and X4B.
 - Websites under attack may rapidly migrate to on-demand DDoS protection, potentially resulting in **unintended disruption** within Italy.
- We found a case of collateral damage involving an anycast Google IP.
 - It was used by **Telecom Italia** to serve a **blocking page** for FQDNs filtered by Piracy Shield.



Do streamers evade the blocking?

- Piracy Shield blocks only IPv4 and FQDNs so far, leaving a **potential loophole** for IPv6.
- Using historical OpenINTEL data, we found:
 - 1,568 blocked FQDNs started **serving over IPv6**.
 - 5,259 FQDNs adopted at least one **new IP**, but only 1,220 of those were blocked afterwards.
- These patterns suggest that illegal streaming operators can evade the platform via IPv6 and IP migration.



Key Takeaways

- We urge AGCOM and Italian policymakers to critically reassess the current blocking framework.
 - Piracy Shield is **currently** causing collateral damage to benign activities
 - IP-level blocking is **indiscriminate** and must be avoided
 - Piracy Shield could have serious consequence of **national security**
 - FQDN blocking can be used only as a **last resort** within **tight time windows**
 - The list of blocked resources should be published immediately to allow **third-party vetting**
- Operators should be **informed**, and report abuses to their national authorities.
- Focus on copyright enforcement **within the EU** where streamers operate
- We can fight piracy **without harming the Internet**.

Questions?

Raffaele Sommese

r.sommese@utwente.nl

Full paper:

<https://ris.utwente.nl/ws/portalfiles/portal/504589587/piracyshield.pdf>

**UNIVERSITY
OF TWENTE.**

