Amplify the signal:
Investigating phishing domains through domain clustering

APWG eCrime 2026 | November 02 2026

ABUSE.ch | SPAMHAUS

Meet the speaker



Sven Krohlas
Detection Engineer
Spamhaus

sven@spamhaus.org

ABUSE.ch | SPAMHAUS

abuse.ch & Spamhaus

Not-for-profit

20+
years

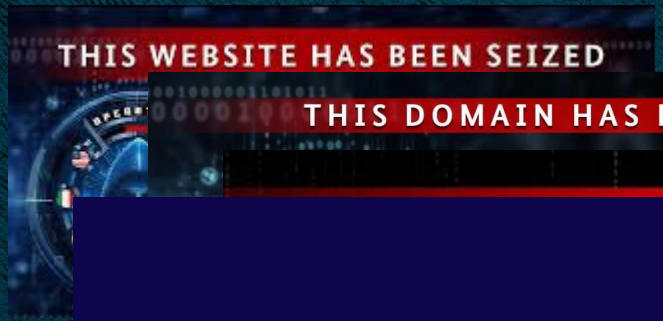


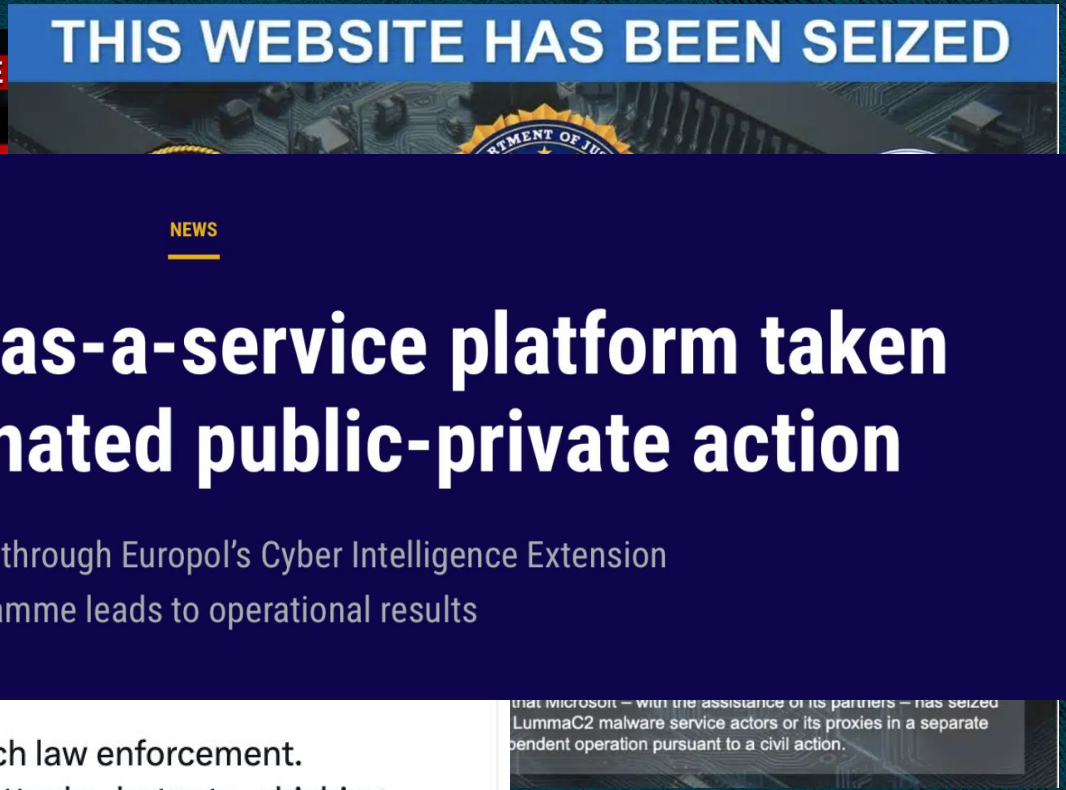
Independent

ABUSE.ch | SPAMHAUS

Let’s start with some motivational slides ...

If you are not interested in boring slides that’s your chance to grab your laptop from your hotel room!





NEWS

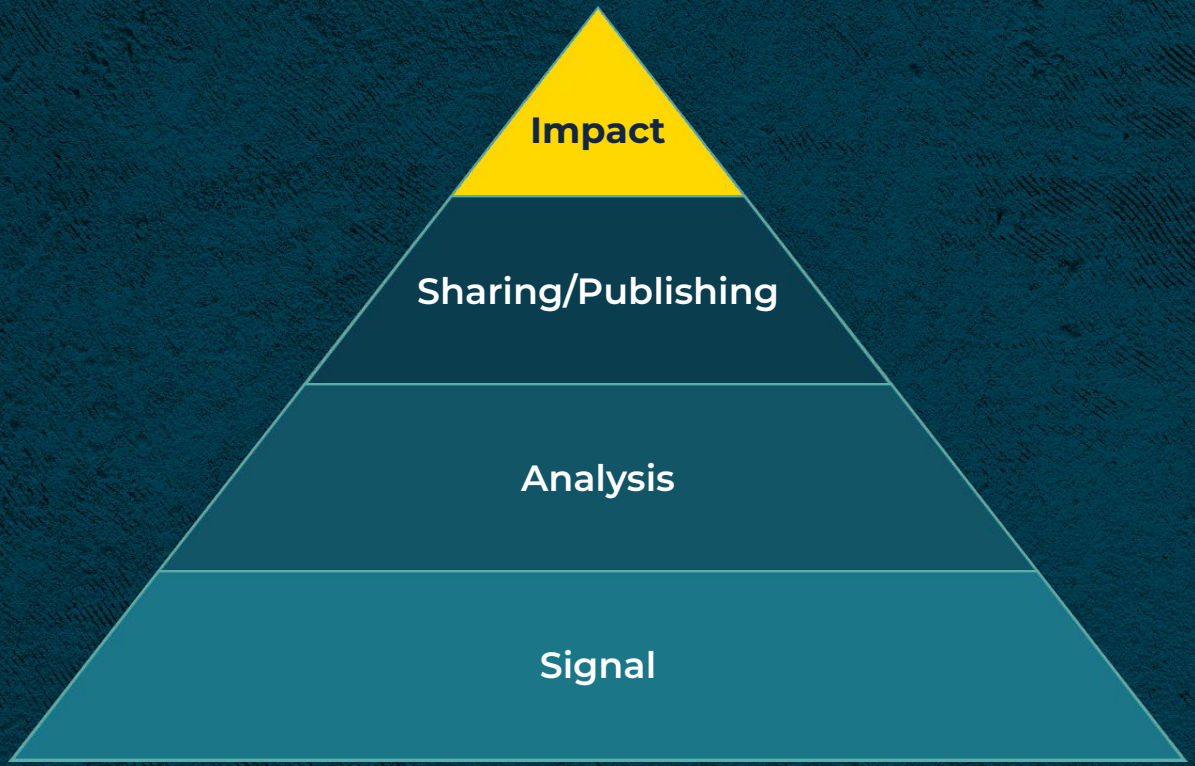
Global phishing-as-a-service platform taken down in coordinated public-private action

Intelligence shared through Europol's Cyber Intelligence Extension Programme leads to operational results

🚨CrazyRDP has been taken down by Dutch law enforcement. Responsible for carrying out ransomware attacks, botnets, phishing activities and distributing child p*rnography (CSAM). Police said to have seized thousands of servers.

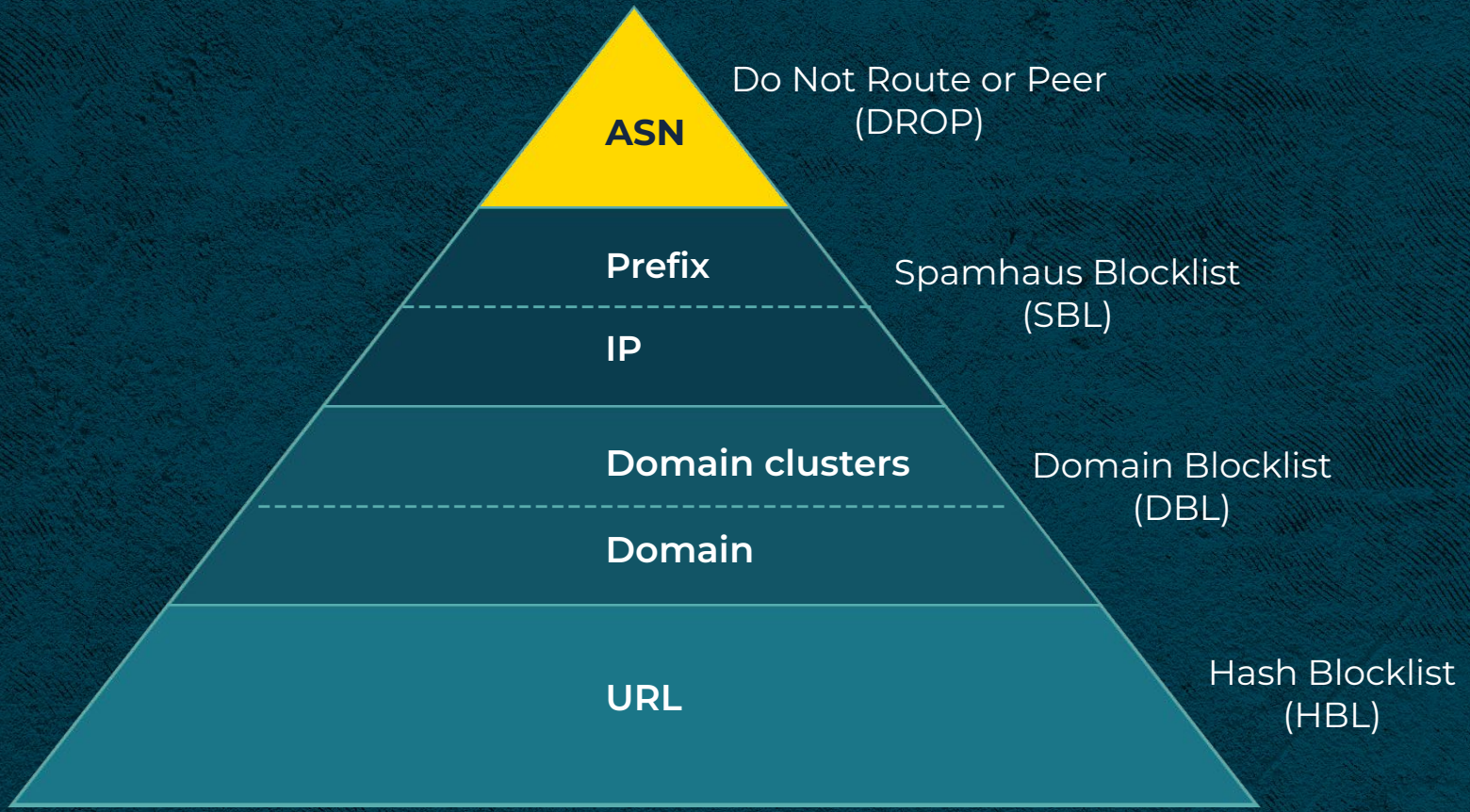
ABUSE.ch | SPAMHAUS

The path from “signal to impact”

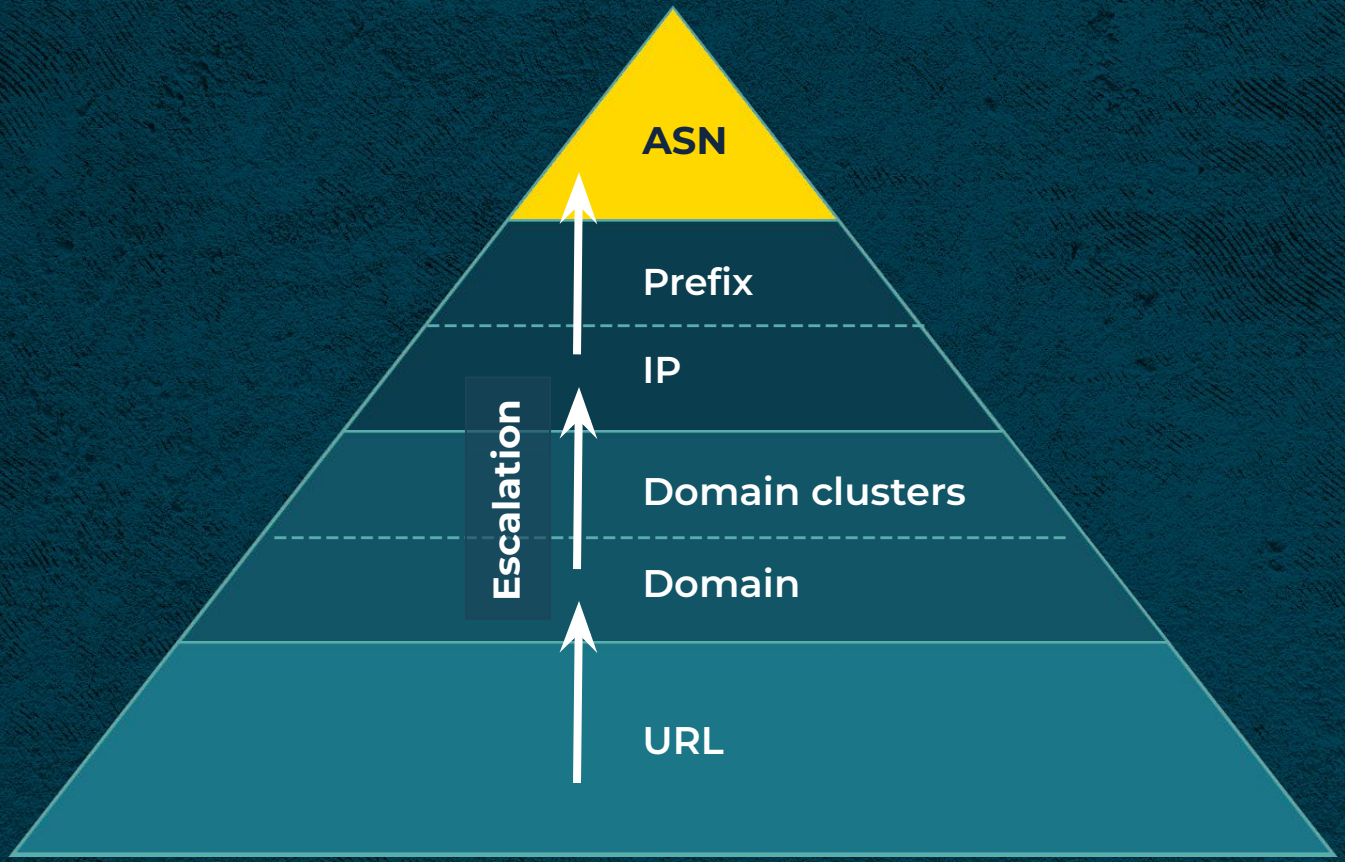



“Turn the pyramid upside down.”
COMEDY CENTRAL

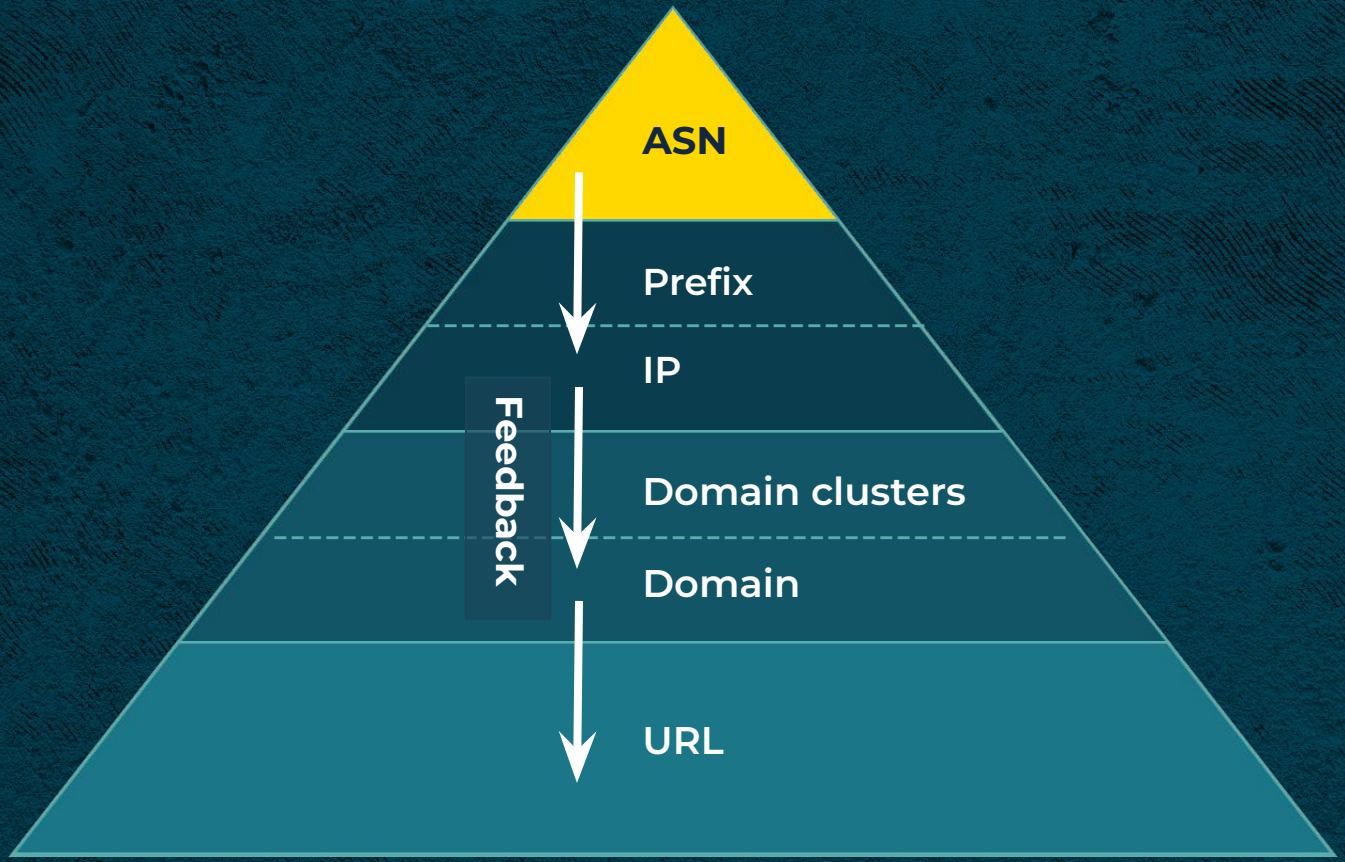
Amplification of signal



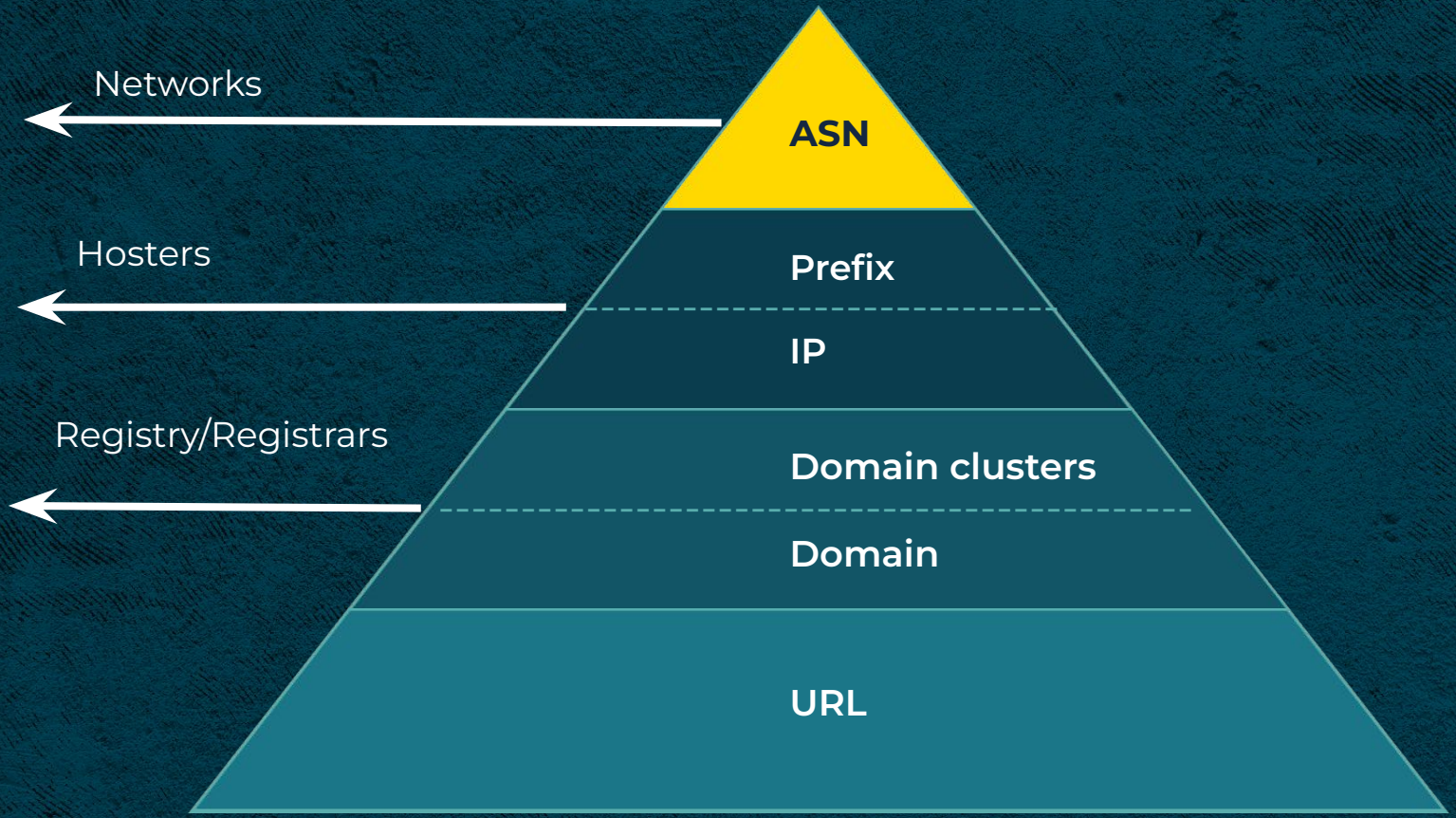
Amplification of signal | Escalation



Amplification of signal | Feedback

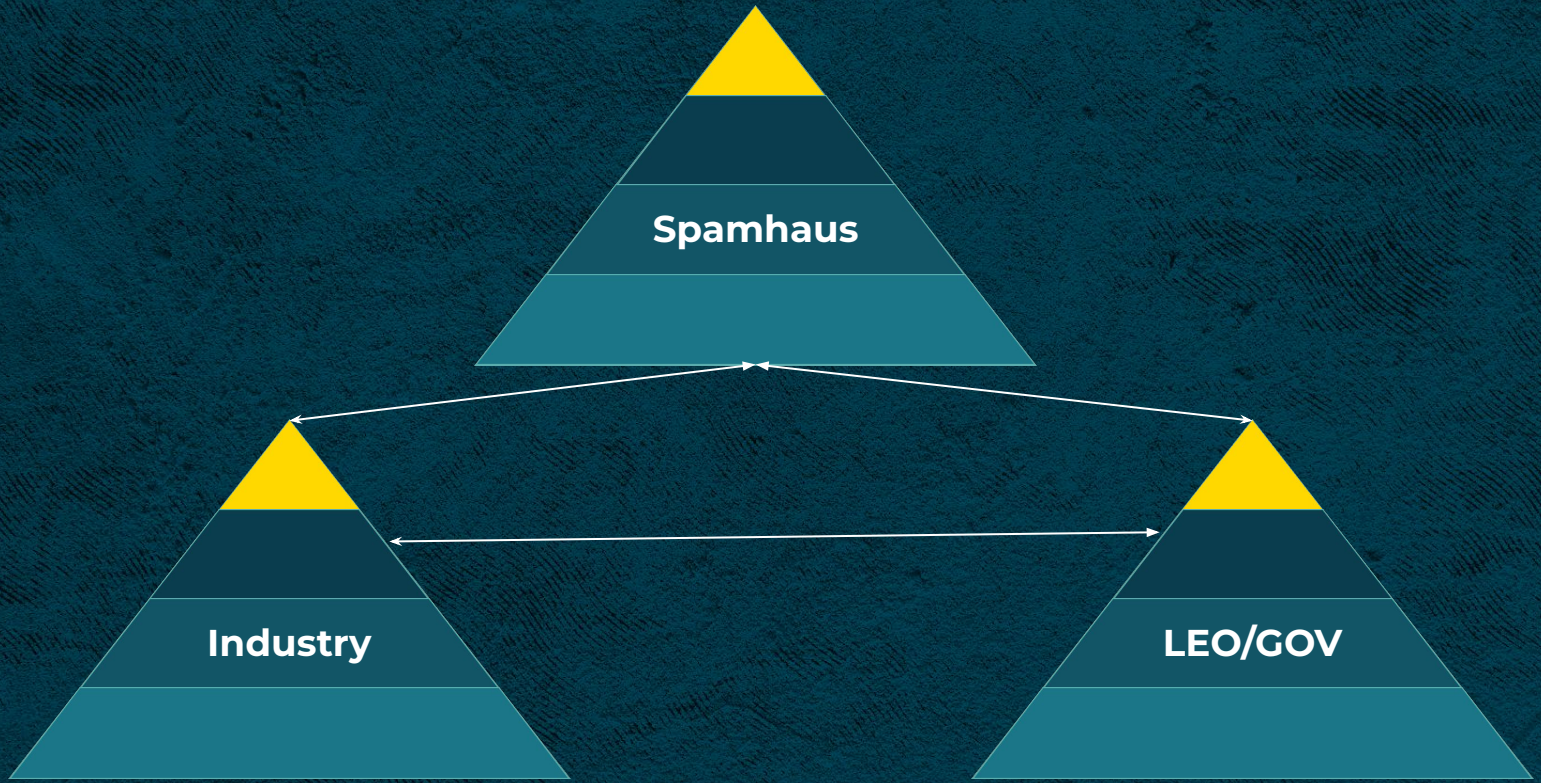


Amplification of signal | Interconnected exchange



But the amplification doesn’t stop there …

Amplification of new signals | Interconnected ecosystem




FIREWORKS
EVERYWHERE
makeameme.org

CrazyRDP | November 12, 2025 takedown

POLITIE

Spamhaus @spamhaus · Nov 17, 2025

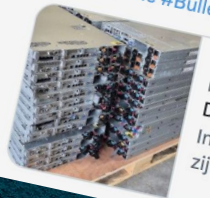
On November 12, around 250 physical servers were seized by the Dutch police at two datacenters in the Netherlands 👉 politie.nl/nieuws/2025/no...

We assess the unnamed bulletproof hosting provider (BPH) is **CrazyRDP**, a major cybercrime hub previously operating front companies such as 🇺🇸 Delis LLC (AS211252), 🇺🇸 Limenet LLC (AS394711) and, most recently, 🇺🇸 Sovy Cloud Services (AS401110) and its downstreams (all incorporated in 🇺🇸 as well): AS401115 (EKABI), AS401116 (Nybula LLC), AS401109 (Zhongguancun LLC) and AS401120 (cheapy.host LLC). 🥷 Of course, all of them are listed in DROP and ASN-DROP.) 🛡️

All this time, the physical infrastructure appears to have been hosted by 🇳🇱 Serverion BV, though iterations of this BPH saw attempts to obfuscate its physical location and hamper investigation attempts. 🧐

Congratulations to all parties involved in this takedown! Looking forward to seeing more of them soon! 👏

#Cybercrime #BulletproofHosting #DROP



politie.nl

Duizenden servers in beslaggenomen in omvangrij...

In een onderzoek naar een malafide hostingbedrijf zijn door het team cybercrime Oost-Nederland ...

Case study | Phishing

Submission Info:

Type: Domain

Threat Type: Phish

Reason

phishing targeting olx and/or its customers

Object

```
mel2ri.top
```

Case study | Phishing

Submission Info:

Type: Domain

Threat Type: Phish

Reason

phishing targeting olx and/or its customers

Object

```
mel2ri.top
```

Domain
ulv2ri.top
mel2ri.top
qen2ri.top
rel7xo.top
sel3ri.top
orv3ri.top
nel7xo.top
pel8xo.top
tel8xo.top
betbonanzacasino.com
seometer.io
iaooba.com
zvsdov.com
bnbasd.com
scboab.com
pnasvb.com
yvaivo.com
aivaoo.com
fnnabh.com

Case study | Banking phish

Submission Info:

Type: URL

Threat Type: Phish

Reason

Phish: https://imgur.com/a/c0QMUEA

Object

```
https://apo-verfahren.icu/WL62/login
```

Case study | Banking phish

Submission Info:

Type: URL

Threat Type: Phish

Reason

Phish: https://imgur.com/a/c0QMUEA

Object

```
https://apo-verfahren.icu/WL62/login
```



ABUSE.ch | SPAMHAUS

Case study | Banking phish

Submission Info:

Type: URL

Threat Type: Phish

Reason

Phish: https://imgur.com/a/c0QMUEA

Object

```
https://apo-verfahren.icu/WL62/login
```





ABUSE.ch | SPAMHAUS

Case study | Smishing

Submission Info:

Type: URL

Threat Type: Phish

Reason

[DRAGONFIRE][SMS][Amazon-Recall-Lure] Observed in SMS phishing

Object

```
https://yubr.evpaj.top/m5B5DqAq?i7m=WtH
```

Case study | Smishing

Submission Info:

Type: URL

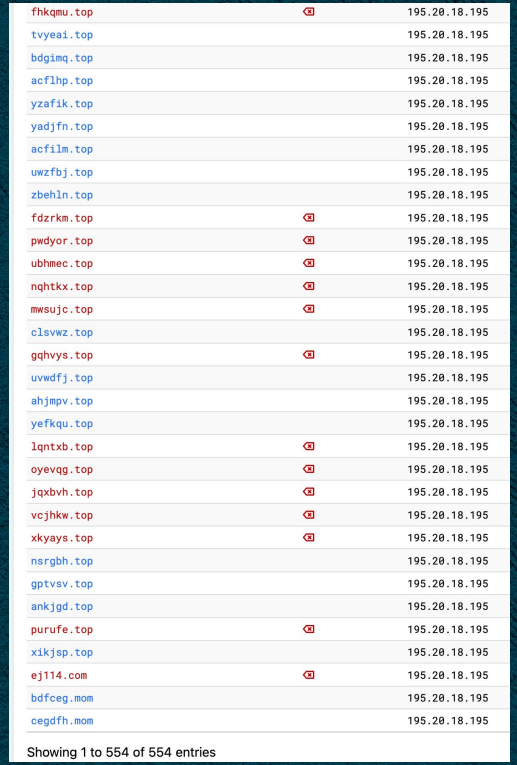
Threat Type: Phish

Reason

[DRAGONFIRE][SMS][Amazon-Recall-Lure] Observed in SMS phishing

Object

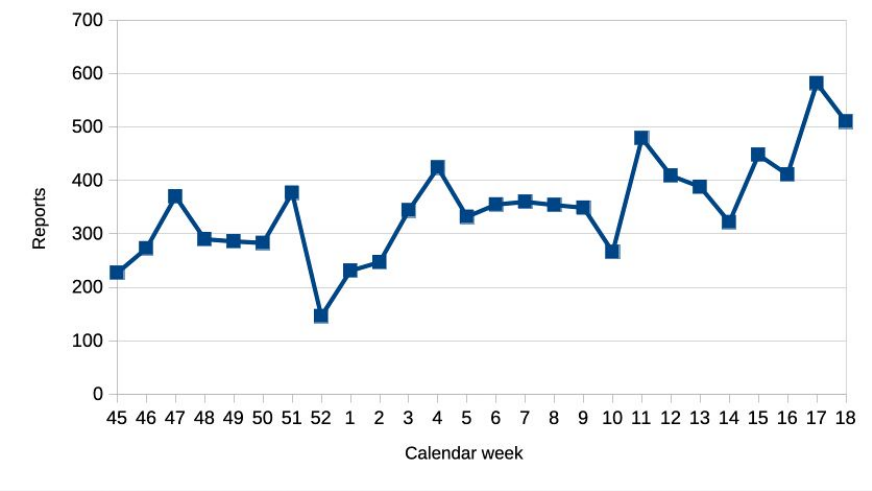
```
https://yubr.evpaj.top/m5B5DqAq?i7m=WtH
```



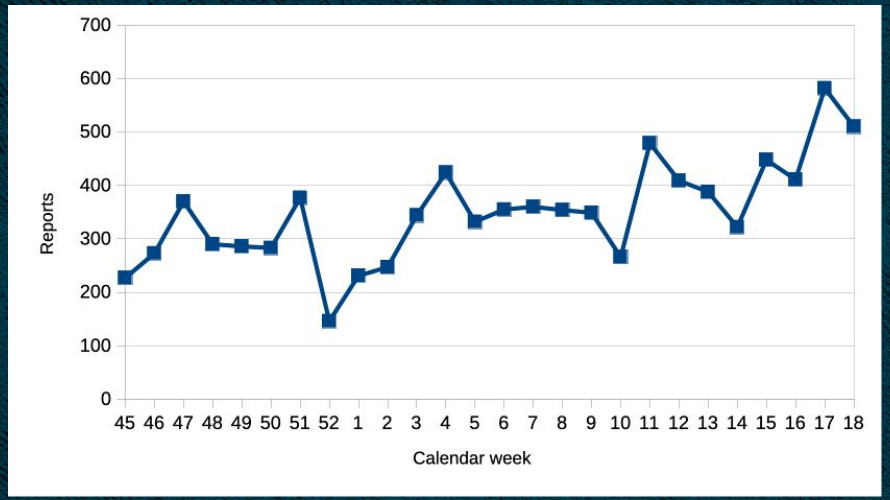
fhkqmu.top	⌫	195.20.18.195
tvyeai.top		195.20.18.195
bdgimq.top		195.20.18.195
acflhp.top		195.20.18.195
yzafik.top		195.20.18.195
yadjfn.top		195.20.18.195
acfilm.top		195.20.18.195
uwzfbj.top		195.20.18.195
zbehln.top		195.20.18.195
fdzrkm.top	⌫	195.20.18.195
pwdyor.top	⌫	195.20.18.195
ubhmec.top	⌫	195.20.18.195
nqhtkx.top	⌫	195.20.18.195
mwsujc.top	⌫	195.20.18.195
clsvwz.top		195.20.18.195
gqhvys.top	⌫	195.20.18.195
uvwdfj.top		195.20.18.195
ahjmpv.top		195.20.18.195
yefkqu.top		195.20.18.195
lqntxb.top	⌫	195.20.18.195
oyevqg.top	⌫	195.20.18.195
jqxbvh.top	⌫	195.20.18.195
vcjhkw.top	⌫	195.20.18.195
xkyays.top	⌫	195.20.18.195
nsrgbh.top		195.20.18.195
gptvsv.top		195.20.18.195
ankjgd.top		195.20.18.195
purufe.top	⌫	195.20.18.195
xikjsp.top		195.20.18.195
ej114.com	⌫	195.20.18.195
bdfceg.mom		195.20.18.195
cegdfh.mom		195.20.18.195

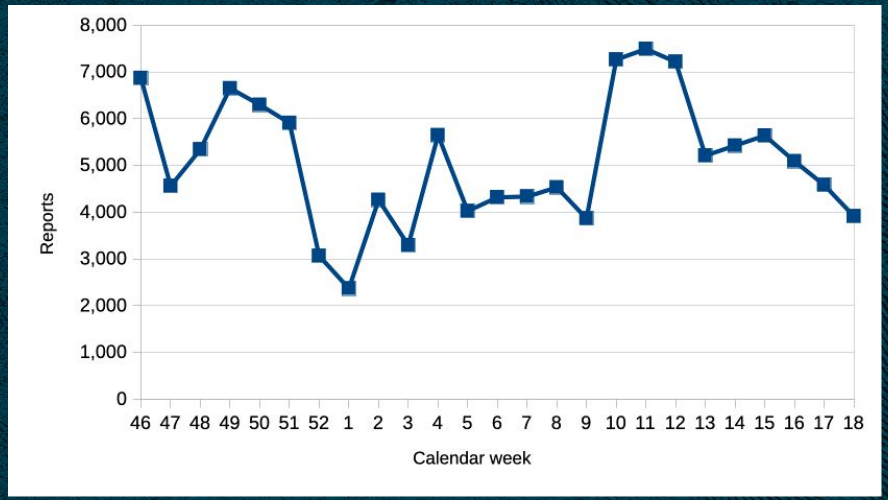
Showing 1 to 554 of 554 entries

Case study | Numbers ...



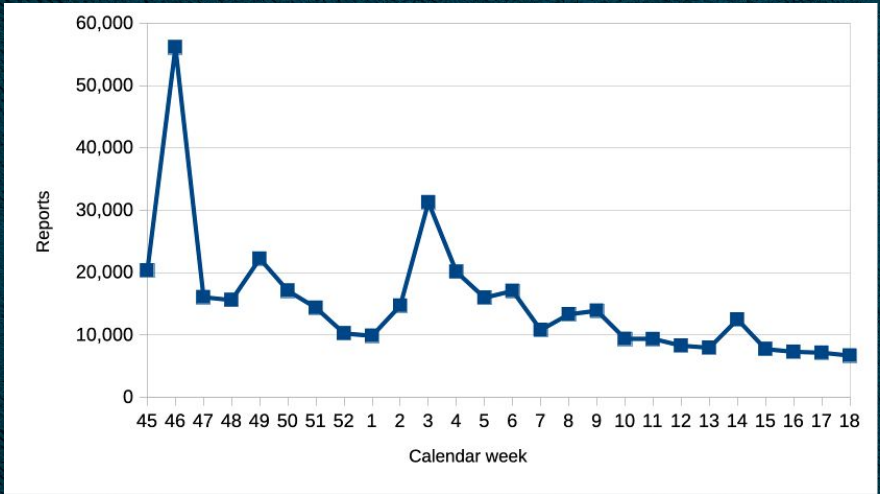
Case study | Numbers ...



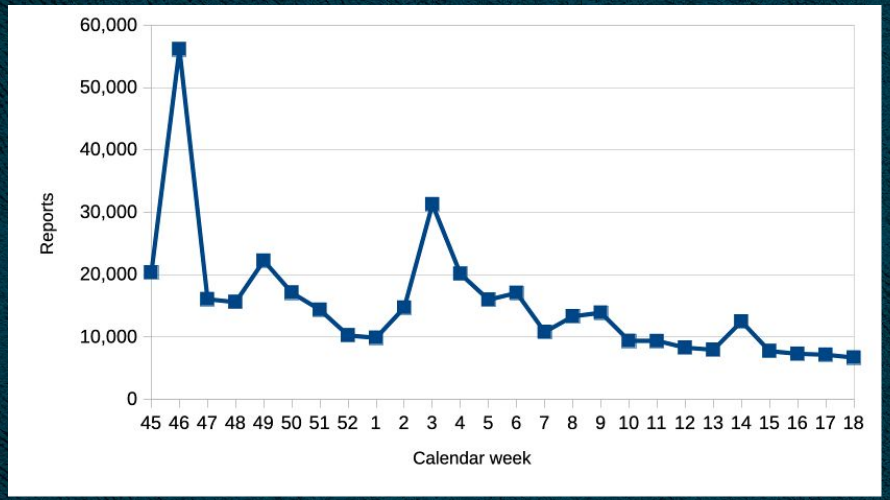


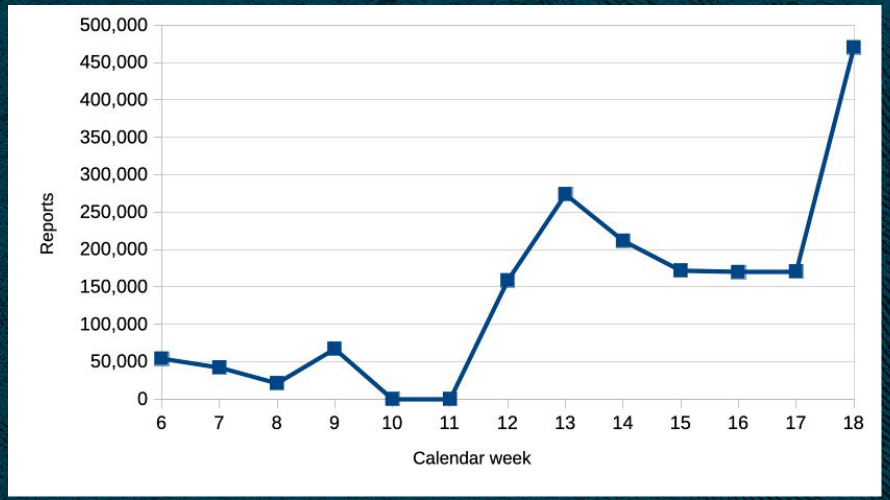
ABUSE.ch | SPAMHAUS

Case study | Bigger Numbers



Case study | Bigger Numbers





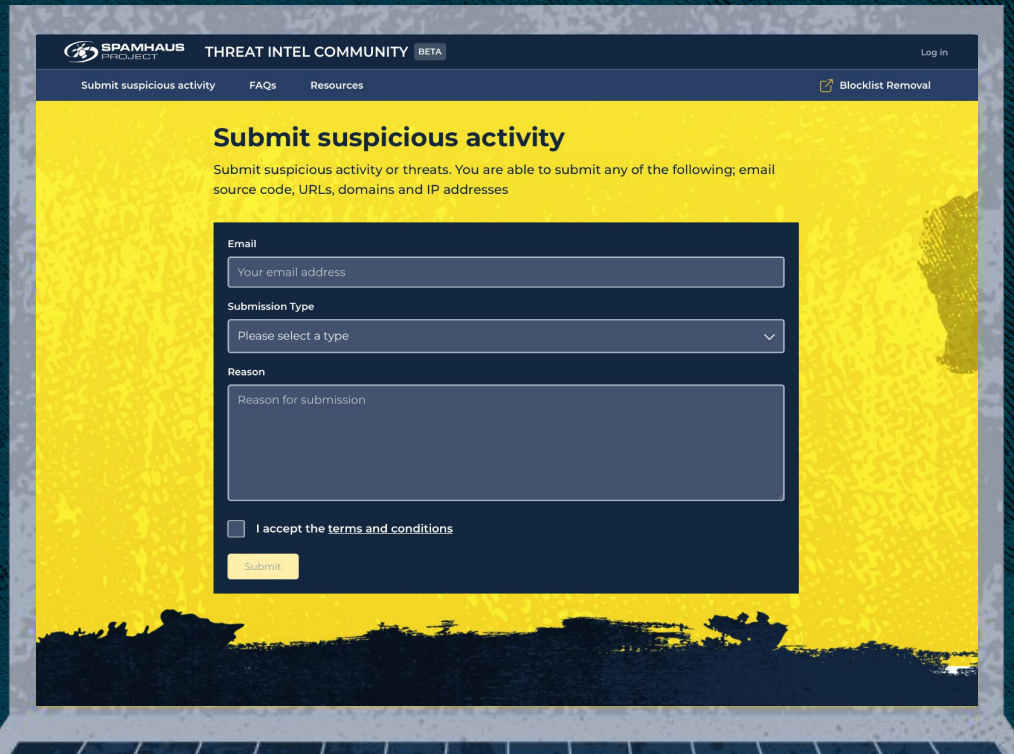
ABUSE.ch | SPAMHAUS

Sharing phishing data | https://submit.spamhaus.org

Who? Threat Hunters, Takedown Organizations, Incident Responders, ...

What? IPs, domains, URLs, raw spam samples (always provide evidence)

How? Web form or via API



Share data. Strengthen signal. Amplify the impact.

ABUSE.ch | SPAMHAUS

Let’s play! – Tools: Intelligence API



Docs:
https://docs.spamhaus.com/sia/docs/source/

Get a token:

```
$ curl -s -d '{"username":"rqnpucxc@91761267",
"password":"z5a5?LG@5H3tqWr8", "realm":"intel"}'
https://api.spamhaus.org/api/v1/login
```



Let’s play! – Tools: Deteqtive Passive DNS

Frontend:
https://ui.deteqtive.com/sso

sven@spamhaus.org
q+Yw,TPzicjaF9t

Static token:

```
sk_pdnsp1_RM26GPVKWH.jgxwVAKfM00T_bqhv7Ha0cMN_nwtFloFfKBzA7UmhqE
```

Let’s play! – Pivoting



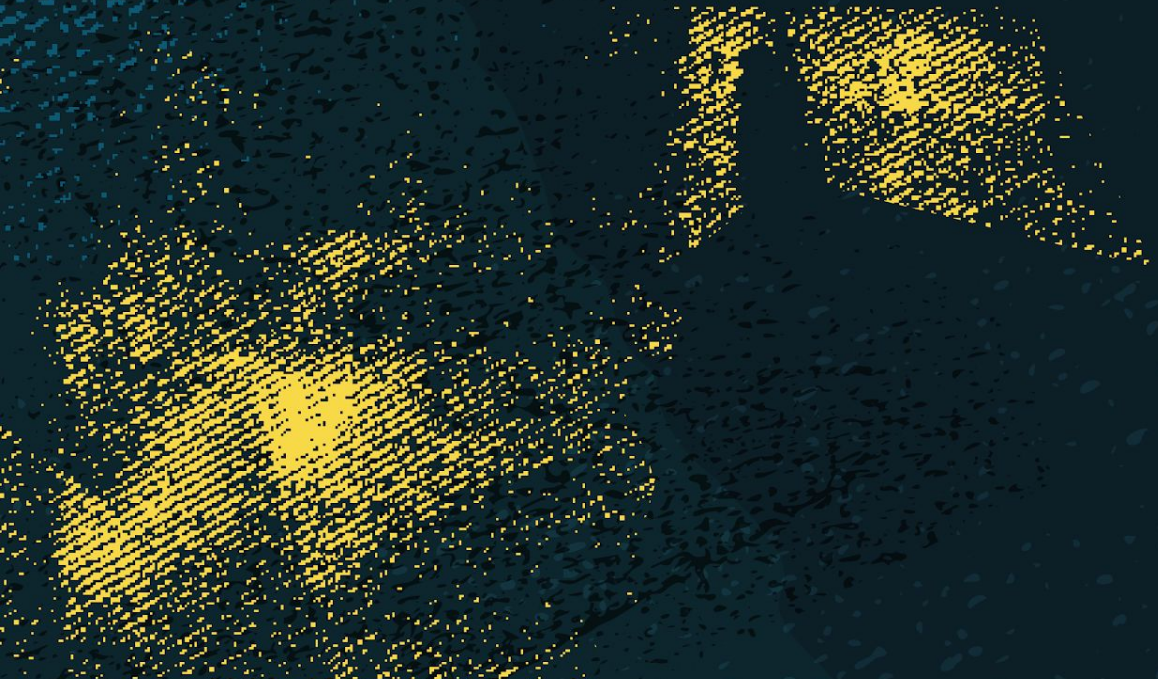
Possible IPs to start from
https://www.spamhaus.org/blocklists/do-not-route-or-peer/

Domains
eCx, our email/SMS inboxes, search for terms on pDNS, …

Domain examples

- advanced-reserv1283.com
- phototanapp-commerzbank.de
- guest-reserv-847219.com
- fedexru.com
- wachat-whatsapp.xyz

Thank you, eCrime 2026!



ABUSE.ch | SPAMHAUS