

T.I.S.P./T.P.S.S.E. Community Meeting 2025

Berlin, 04. - 05.11.2025

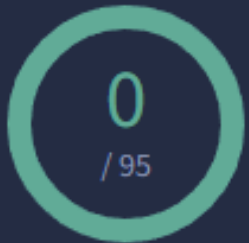
Spam erkennen - Wie Mustererkennung und Datenanalyse das nächste Level der Spam-Abwehr erreichen

Antonia Scherz, Stefan Cink, Net at Work GmbH

spectra.adshoes.shop

spectra.adshoes.shop/8d818bdc0d31de.jpg?fo=pltagjlnuwojbl&i=aaq9
rwcw





Community
Score



No security vendors flagged this domain as malicious

adshoes.shop

Spam, Suspicious (alphaMountain.ai)

DETECTION

DETAILS

RELATIONS

COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Spam

Spam

78:5b:3d:78:t7:70:e4:0a:fa:33:25:ba:t7:bb:8t: 3e:81:89:1b:e7

X509v3 Subject Alternative Name:

DNS:adshoes.shop, DNS:ascend.adshoes.shop, DNS:beauty.adshoes.shop, DNS:clarity.adshoes.shop, DNS:gallery.adshoes.shop, DNS:gam
DNS:goalhub.adshoes.shop, DNS:goto.adshoes.shop, DNS:home.adshoes.shop, DNS:ideas.adshoes.shop, DNS:inspire.adshoes.shop, DNS:s
DNS:vantage.adshoes.shop

News

Global Dispatch

Uncovering Today's International Headlines and Top Stories



Palestinians Flee as Israeli Troops Push Into Gaza City

Posted by Thomas on September 2025



He Fled Putin's War. The U.S. Deported Him to a Russian Jail.

Posted by Thomas on September 2025



Trump Leaves Tense America Behind for Royal Retreat on U.K. State Visit

Military officers taking part in rehearsals at Windsor Castle, west of London, on Monday, before a state visit by President Trump.

Posted by Thomas on September 2025



Submitted URL: <http://spectra.adshoes.shop/WXljTEU0UmVocWVrRzFzbHh3QWE1NklwMVk4emI5TWI0d0R0SDItYTNzWEpWcjhMMmR4OUhCRjJIN3NuSWZEdVRrYiYwOW1n...>

Effective URL: <https://www.google.com/>

Submission: On September 17 via manual (September 17th 2025, 7:18:35 am UTC) from  — Scanned from 

Summary HTTP 35 Redirects Links 17 Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted **6 IPs** in **2 countries** across **4 domains** to perform **35 HTTP transactions**. The main IP is **216.58.206.68**, located in **United States** and belongs to **GOOGLE, US**. The main domain is **www.google.com**. The Cisco Umbrella rank of the primary domain is **3**. TLS certificate: Issued by **WE2** on September 8th 2025. Valid for: 3 months.

spectra.adshoes.shop scanned **16 times** on urlscan.io

Show Scans 16

www.google.com scanned **10000+** times on urlscan.io

Show Scans 10000+

urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  No classification for www.google.com

Current DNS A record: 142.250.186.36 (AS15169 - GOOGLE, US)

Domain created: September 15th 1997, 09:00:00 (UTC)

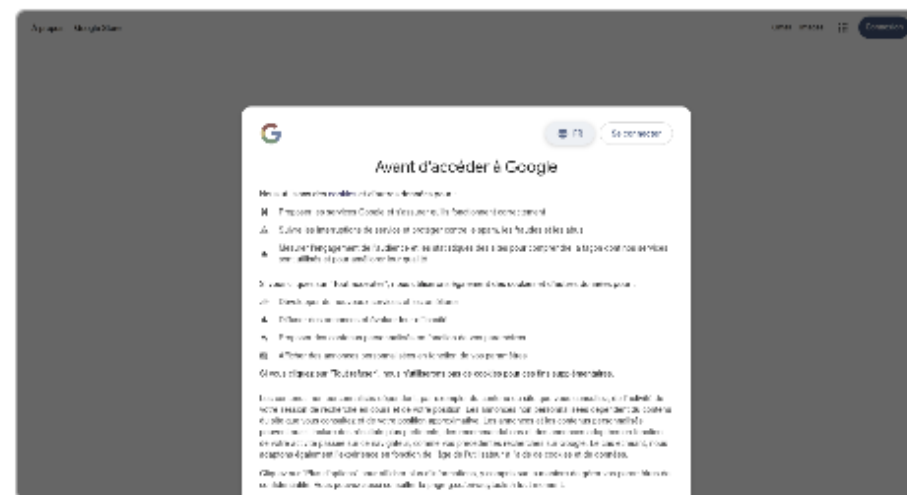
Domain registrar: MarkMonitor, Inc.

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

Screenshot

Live screenshot Full Image



Page Title

Google

Page URL History

Show full URLs

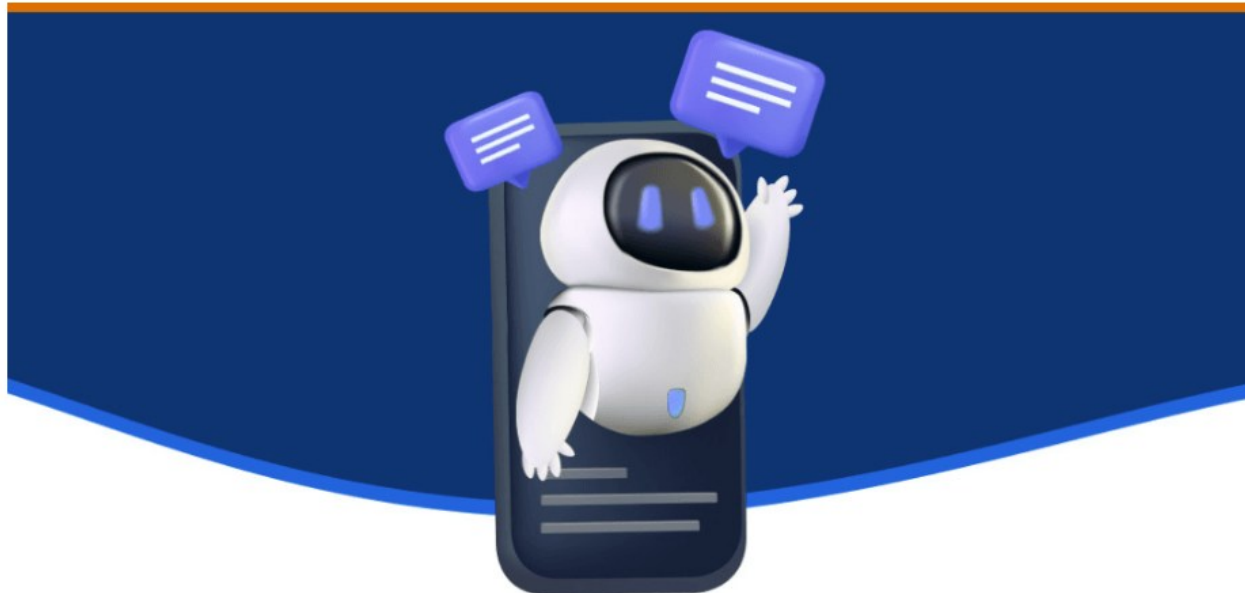
- <http://spectra.adshoes.shop/WXljTEU0UmVocWVrRzFzbHh3QWE1NklwMVk4emI5TWI0d0R0SDItYTNzWEpWcjhMMmR4OUhCRjJIN3NuSWZEdVRrYiYwOW1n...> HTTP 307 <https://spectra.adshoes.shop/WXljTEU0UmVocWVrRzFzbHh3QWE1NklwMVk4emI5TWI0d0R0SDItYTNzWEpWcjhMMmR4OUhCRjJIN3NuSWZEdVRrYiYwOW1n...>

Weiterleitung für Link von spectra.adshoes.shop

- `hxxp://spectra.adshoes.shop/WXljTEU0UmVocWVrRzFzbHh3QWE1NklwMVk4emI5TWl0d0R0SDltYTNzWEpWcjhMMmR4OUhCRjJIN3NuSWZEdVRrYlYwOW1nMnRpa1ZCMzBzNjBEWXhIMS81Q0hXUkVVC2l0QnpnRElFUDA9`
Status Code: 302 ->
`hxxps://theonlineonline.com/?a=4186&oc=24194&c=63247&m=3&s1=1982210&s2=34811_65&s3=253_344881_11888_1111639_md`
Status Code: 302 ->
`hxxps://unting.art/?a=4186&oc=24194&c=63247&m=3&s1=1982210&s2=34811_65&s3=253_344881_11888_1111639_md&ckmguid=bcd474fe-3c57-4e31-9ade-016a79f130d8`
Status Code: 302 -> `hxxps://vibeshopy.com/Chat-GPT-Trader-de/?so=Chat-GPT-Trader-DE&sub=GPT-Trader-EN&ai=2958136&ci=160&gi=148&MPC_3=4186&MPC_4=407006459&MPC_5=CHATGPT_TRADER_DE`
Final URL: 200 -> `hxxps://vibeshopy.com/Chat-GPT-Trader-de/?so=Chat-GPT-Trader-DE&sub=GPT-Trader-EN&ai=2958136&ci=160&gi=148&MPC_3=4186&MPC_4=407006459&MPC_5=CHATGPT_TRADER_DE`



Die Zukunft des Krypto-Handels ist da: Warum ChatGPT Trader ändert sich das Spiel



KI-Handel erobert die Welt im Sturm. In den letzten Jahren hat sich die Weltwirtschaft dramatisch verändert. Angesichts anhaltender Inflation, unsicherer Märkte und sich entwickelnder digitaler Trends suchen die Menschen zunehmend nach innovativeren und zuverlässigeren Methoden zur Verwaltung ihrer Finanzen. Ein Tool sorgt insbesondere für Schlagzeilen und begeistert sowohl erfahrene Anleger als auch Neueinsteiger: ChatGPT Trader.

Diese revolutionäre, KI-gestützte Plattform verändert die Art und Weise, wie Menschen mit Kryptowährungen und Finanzanlagen handeln. Durch die Nutzung der künstlichen Intelligenz ermöglicht ChatGPT Trader seinen Nutzern, fundierte Handelsentscheidungen zu treffen – ganz ohne umfassende Marktkennntnisse oder ständiges Beobachten der Märkte. Sie definiert intelligentes und effizientes Trading in einem sich schnell wandelnden Finanzumfeld neu.

Was ist ChatGPT Trader?



CHATGPT

ALGO TRADING

+20097%



Die Zukunft des Krypto-Handels ist da: Warum ChatGPT Trader das Spiel verändert

KI-Handel erobert die Welt im Sturm. In den letzten Jahren hat sich die Weltwirtschaft dramatisch verändert. Angesichts anhaltender Inflation, unsicherer Märkte und sich entwickelnder digitaler Trends suchen immer mehr Menschen nach innovativeren und zuverlässigeren Methoden zur Verwaltung ihrer Finanzen. Ein Tool sorgt insbesondere für Schlagzeilen und begeistert erfahrene Anleger und Neueinsteiger gleichermaßen: ChatGPT Trader.

Diese revolutionäre KI-gestützte Plattform verändert den Handel mit Kryptowährungen und Finanzanlagen. Durch die Nutzung künstlicher Intelligenz ermöglicht ChatGPT Trader seinen Nutzern

Hallo,

Ein kurzer TV-Ausschnitt sorgt derzeit für Diskussionen – darin geht es um ein finanzielles Thema, das unerwartet unterbrochen wurde.

Wir haben das Originalmaterial erhalten und stellen es aus redaktionellem Interesse zur Verfügung:

[>> Zur Aufzeichnung \(klicken Sie hier\)](#)

Lesedauer: 5 Minuten



Viele Grüße





CYBERKRIMINALITÄT

Anlagebetrug mit Bitcoin: So erkennen Sie die Angebote von Kriminellen

02. April 2025, 09:50 Uhr

 [ARTIKEL HÖREN](#)

Auch Kriminelle versuchen, den Boom von Bitcoins zu nutzen und mit einer speziellen "Cybertrading-Masche" Millionen abzuzocken: mit geschickt gefälschten Onlinetrading-Portalen. Wir erklären, woran Sie diese erkennen!



E-Mail Metadaten

E-Mail

Message ID: <20250916115600.427F5E2D4D69D75C@arizonaproshop.com>
Mail Source-IP: 94.156.175.64
- CName: treat.arizonaproshop.com.
- CName A-Record: 94.156.175.64
MAIL FROM: arizonaproshop.com
- A-Record: 94.156.175.64
- MX-Record: arizonaproshop.com
Header-From: arizonaproshop.com
- A-Record: 94.156.175.64
- MX-Record: arizonaproshop.com
RCPT TO:

SPF 

DKIM 

S/MIME 

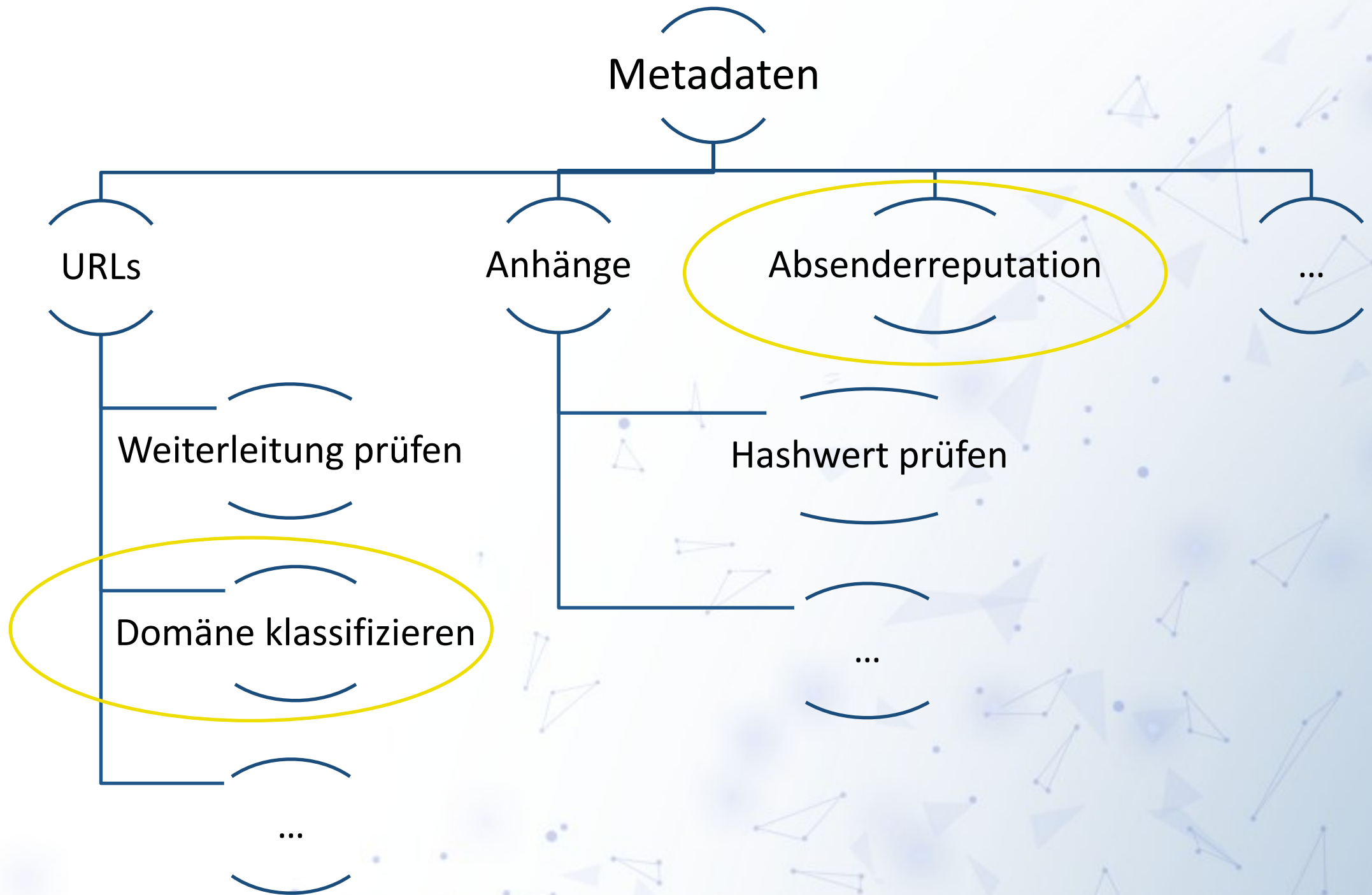
CSA 

No TLS client certificate present in this report

URLs

☐ dgpj.cv/.well-known/acme-challenge/otguy/WEBMAIL1.html?email=cmVpbXVuZC5tYX1lckB3cy1zdGFobC5kZQ==







Kontinuierlicher Strom
an Daten

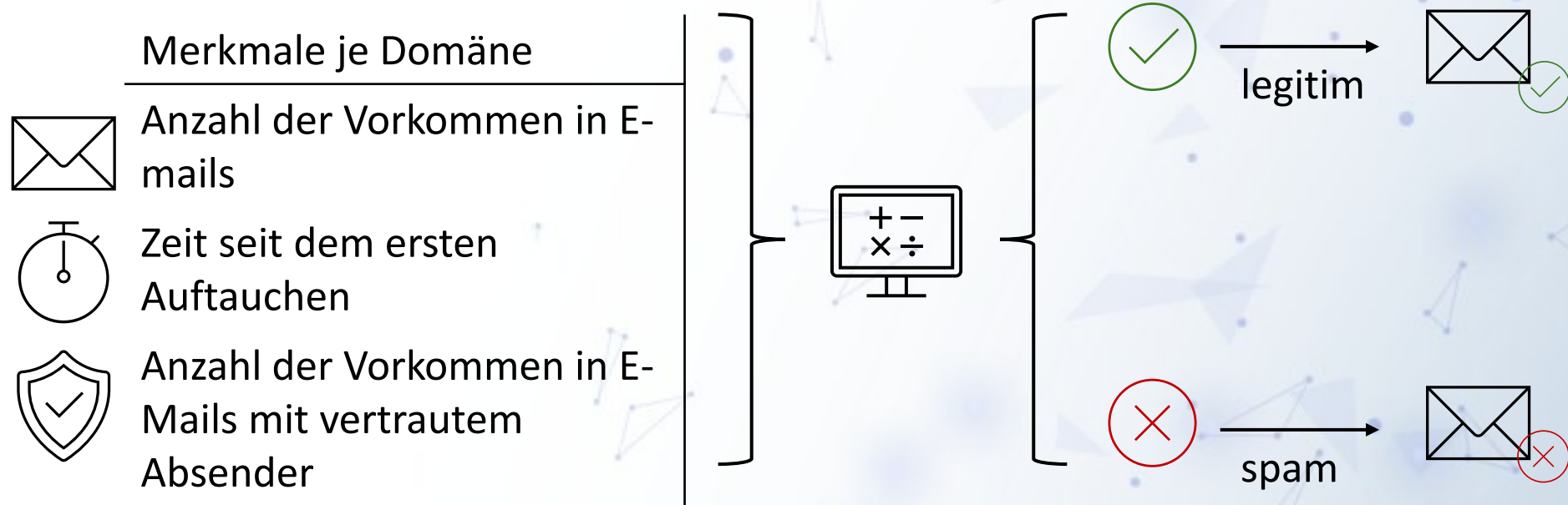
Millionen URLs

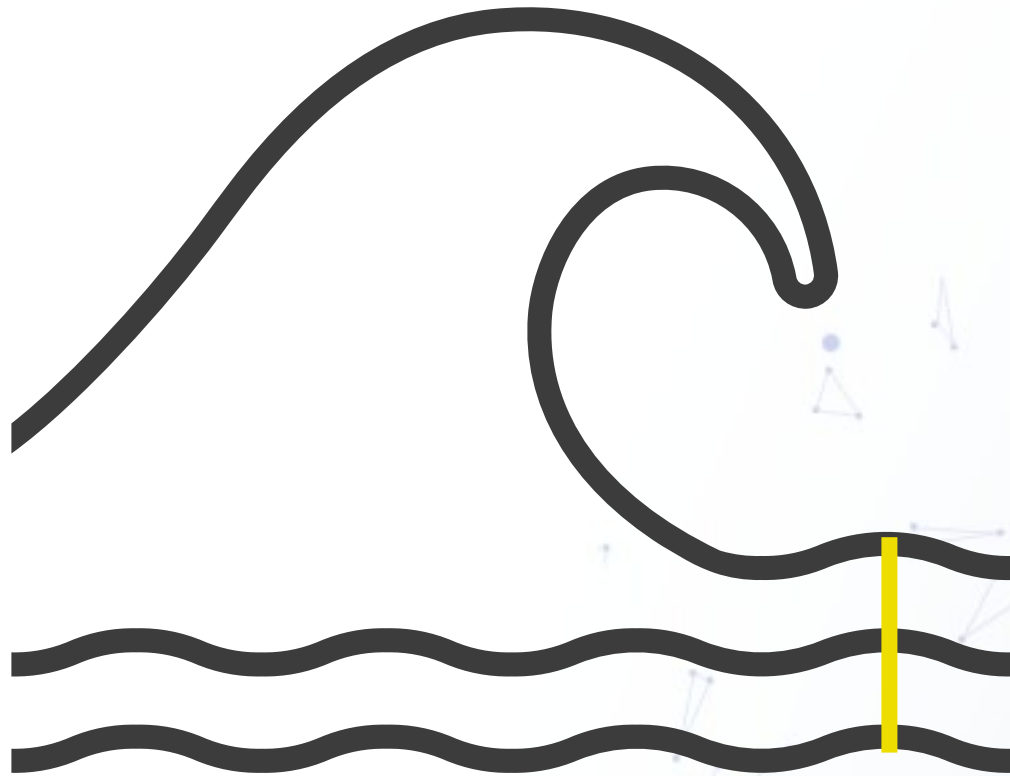
Sofortige Erkennung
notwendig



Klassifizierung von Domänen

kl.deqf9.shop/wpa?id=26845045-859#my@email.de

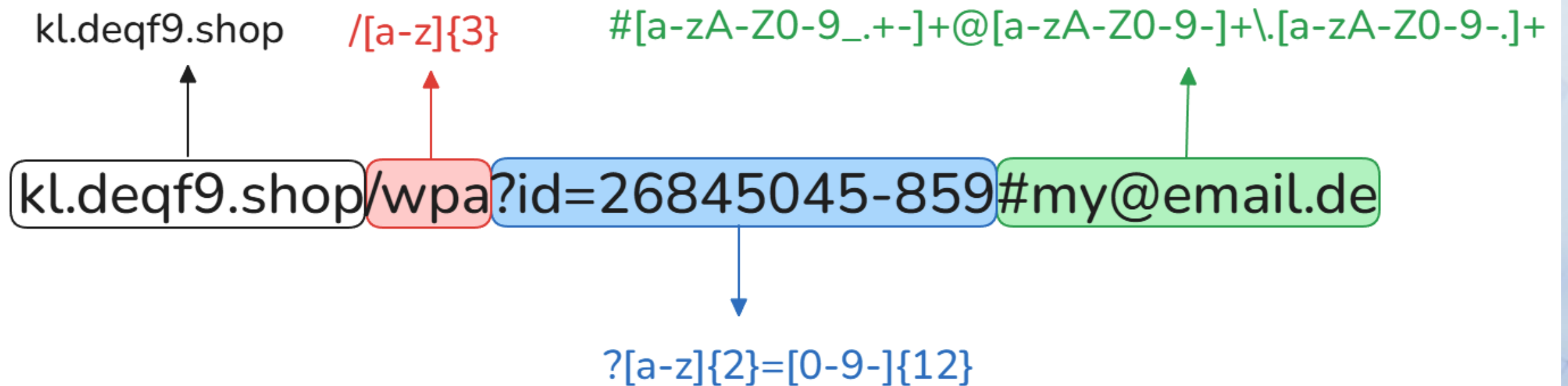




Wie
klassifizieren
wir Domänen
sofort?



Generalisierung von URLs anhand von Regex Mustern

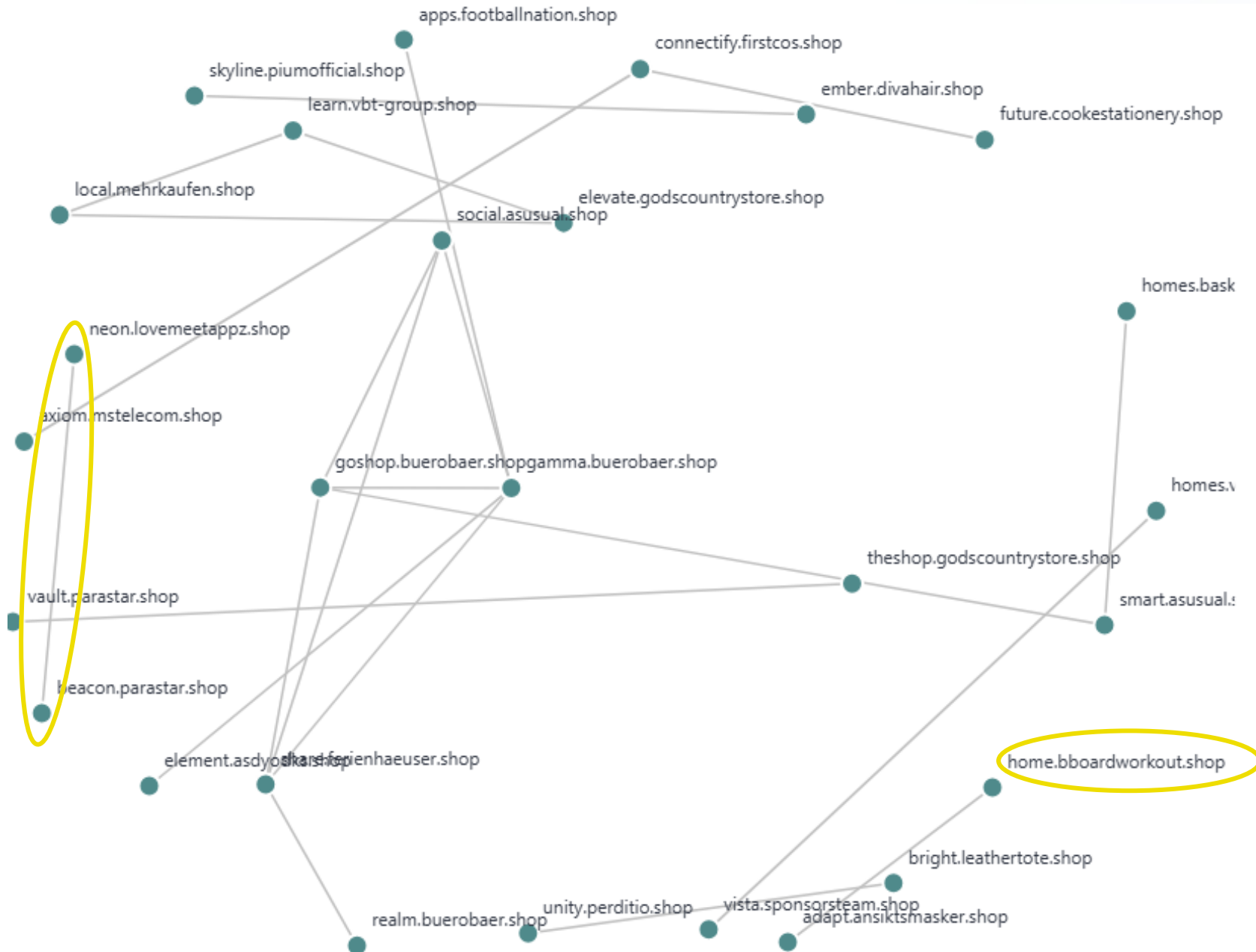




Die Erkennung
einzelner
Domänen
ermöglicht das
Erkennen von
Spam-Wellen.



Beispiel: /[a-z0-9]{15}.jpg/?[a-z]{2}=[a-z]{13}&[a-z]{1}=[a-z0-9]{10}



...

elevate.godscountrystore.shop
ember.divahair.shop
future.cookestationery.shop
gamma.buerobaer.shop
goshop.buerobaer.shop
home.bboardworkout.shop
homes.basketnation.shop
homes.vbt-group.shop
learn.vbt-group.shop
local.mehrkaufen.shop
neon.lovemeetappz.shop
realm.buerobaer.shop
share.ferienhaeuser.shop

...



Submitted URL: <http://home.bboardworkout.shop/>

Effective URL: <https://home.bboardworkout.shop/>

Submission: On September 09 via manual (September 9th 2025, 12:24:53 pm UTC) from DE  — Scanned from UK

[Summary](#)[HTTP 67](#)[Redirects](#)[Links 54](#)[Behaviour](#)[Indicators](#)[Similar](#)[DOM](#)[Content](#)[API](#)[Verdicts](#)

Summary

This website contacted **10 IPs** in **3 countries** across **6 domains** to perform **67 HTTP transactions**. The main IP is **51.89.197.93**, located in **London, United Kingdom** and belongs to **OVH OVH SAS, FR**. The main domain is **home.bboardworkout.shop**.
TLS certificate: Issued by **E7** on September 1st 2025. Valid for: 3 months.

This is the only time *home.bboardworkout.shop* was scanned on urlscan.io!

urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  No classification for *home.bboardworkout.shop*
Current DNS A record: 51.89.197.93 (AS16276 - OVH OVH SAS, FR)

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
	IP Address	AS Autonomous System				
5	51.89.197.93 	16276 (OVH OVH SAS)				

[Lookup](#)[Go To](#)[Rescan](#)[Add Verdict](#)[Report](#)

Screenshot

[Live screenshot](#)[Full Image](#)



Page Title

Worldwide Pulse - Exploring the Latest in International Breaking News and Features

Page URL History

Show full URLs

1. <http://home.bboardworkout.shop/> HTTP 307
<https://home.bboardworkout.shop/> Page URL

Worldwide Pulse

Exploring the Latest in International Breaking News and Features



Live Updates: Parliament and Leaders' Homes Set Ablaze as Nepal Protests Rage

Protesters set fire to the Nepali Congress Party office in Kathmandu on Tuesday during a second day of street protests.

Posted by Thomas on September 2025



Israel Orders Total Evacuation of Gaza City, Threatening Full Invasion

Leaflets dropped in Gaza City by the Israeli military on Tuesday calling on residents to evacuate.

Posted by Thomas on September 2025



Gaza-Bound Flotilla Struck by Drone in Tunisia, Aid Group Says

A Global Sumud Flotilla vessel at the Tunisian port of Sidi Bou Said early Tuesday, flanked by National Guard vessels.

Posted by Thomas on September 2025

News

Global Dispatch

Uncovering Today's International Headlines and Top Stories



Live Updates: Parliament Burns In Nepal as Protests Force Prime Minister to Quit

Protesters set fire to the Nepali Congress Party office in Kathmandu on Tuesday during a second day of street protests.

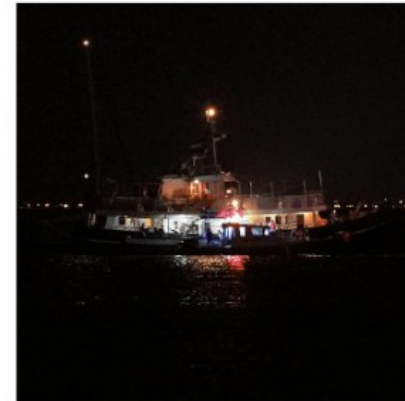
Posted by Thomas on September 2025



Israel Orders Total Evacuation of Gaza City, Threatening Full Invasion

Leaflets dropped in Gaza City by the Israeli military on Tuesday calling on residents to evacuate.

Posted by Thomas on September 2025



Gaza-Bound Flotilla Struck by Drone in Tunisia, Aid Group Says

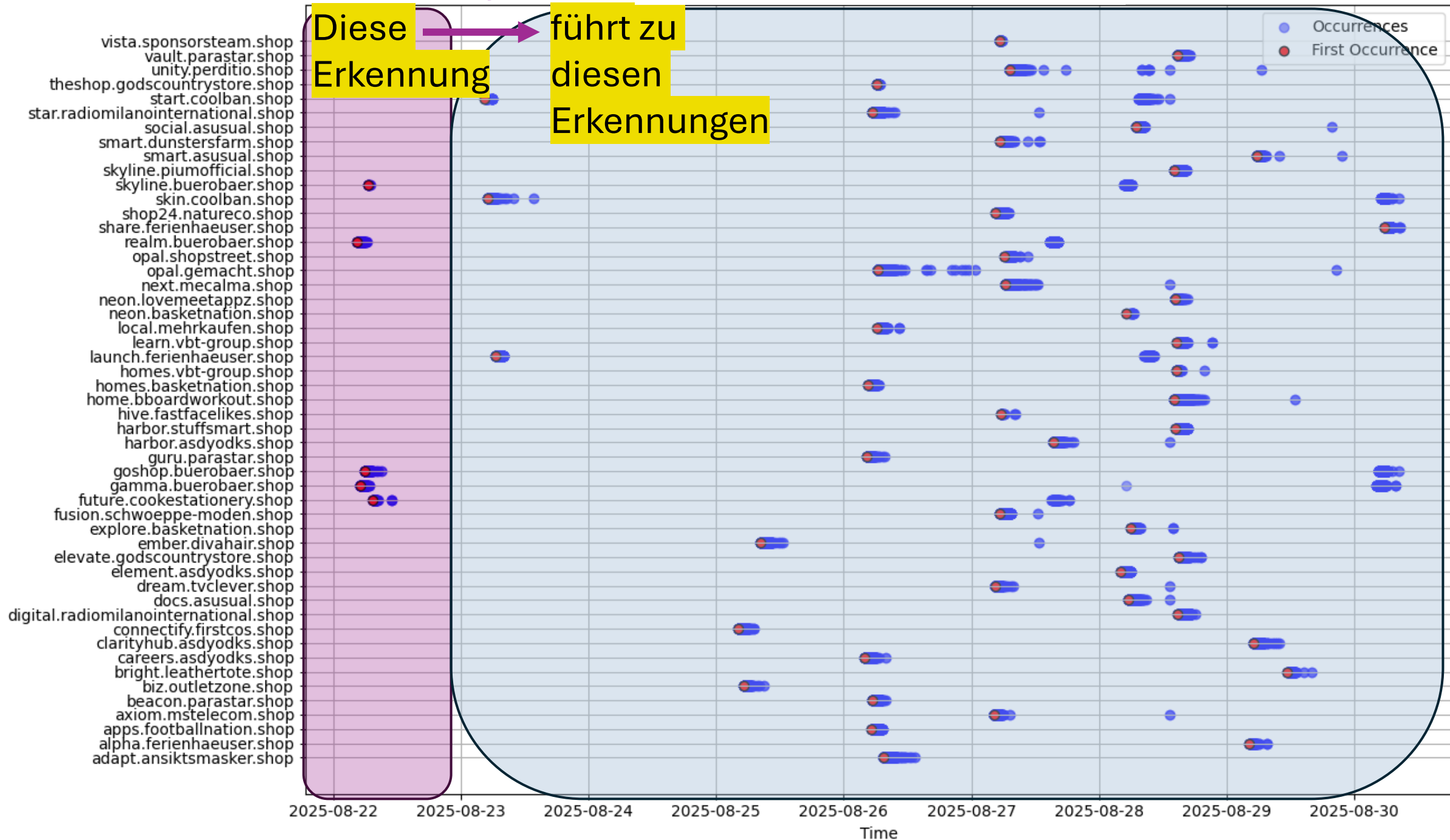
A Global Sumud Flotilla vessel at the Tunisian port of Sidi Bou Said early Tuesday, flanked by National Guard vessels.

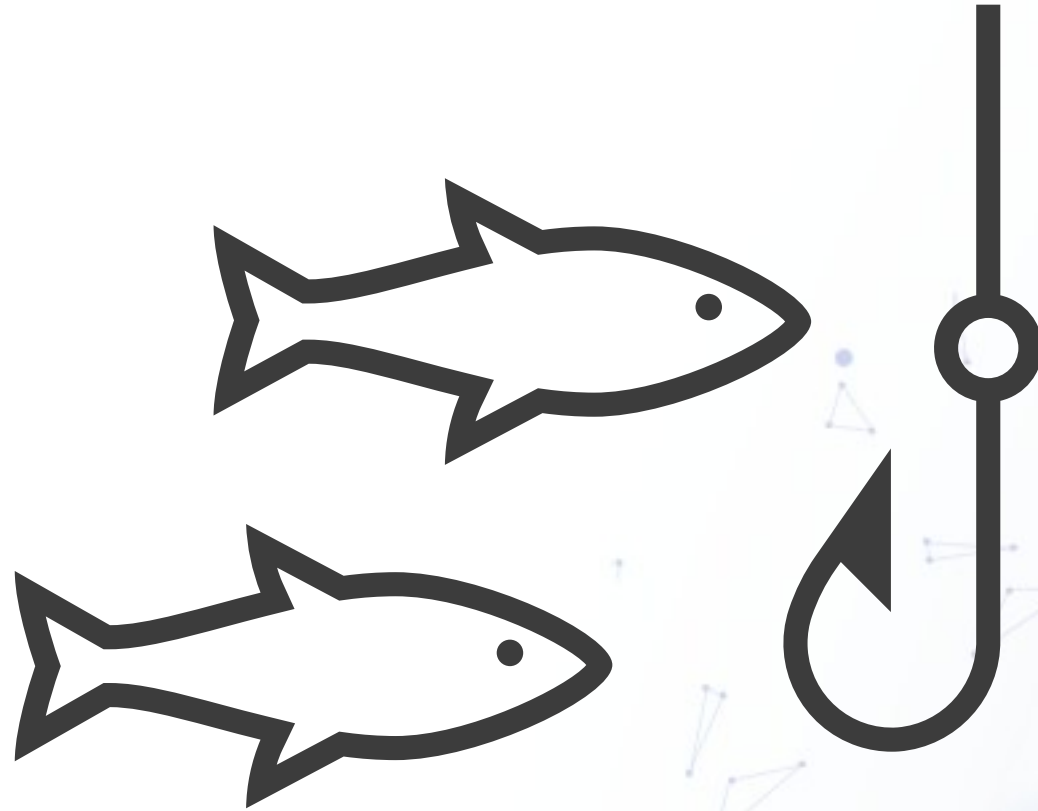
Posted by Thomas on September 2025

Fenster der Analyse

Diese
Erkennung

führt zu
diesen
Erkennungen



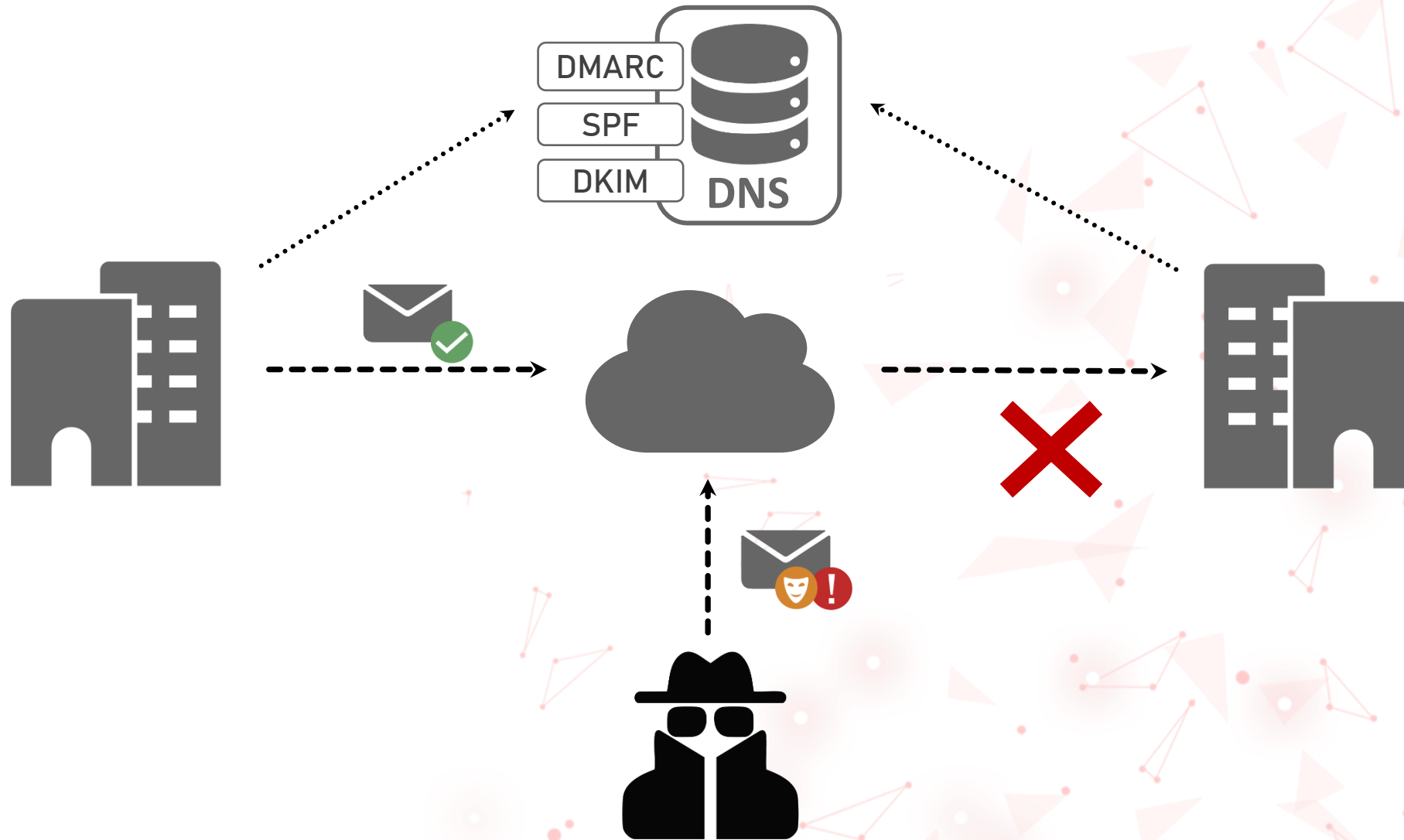


90% der
vorher
unerkannten
böartigen
URLs werden
erkannt.





Absenderreputation



Kein DMARC, keine Kekse



Keine Zustellung legitimer Mails



Neue Newsletter/Dienste werden ohne Anpassung abgelehnt/Quarantäne.



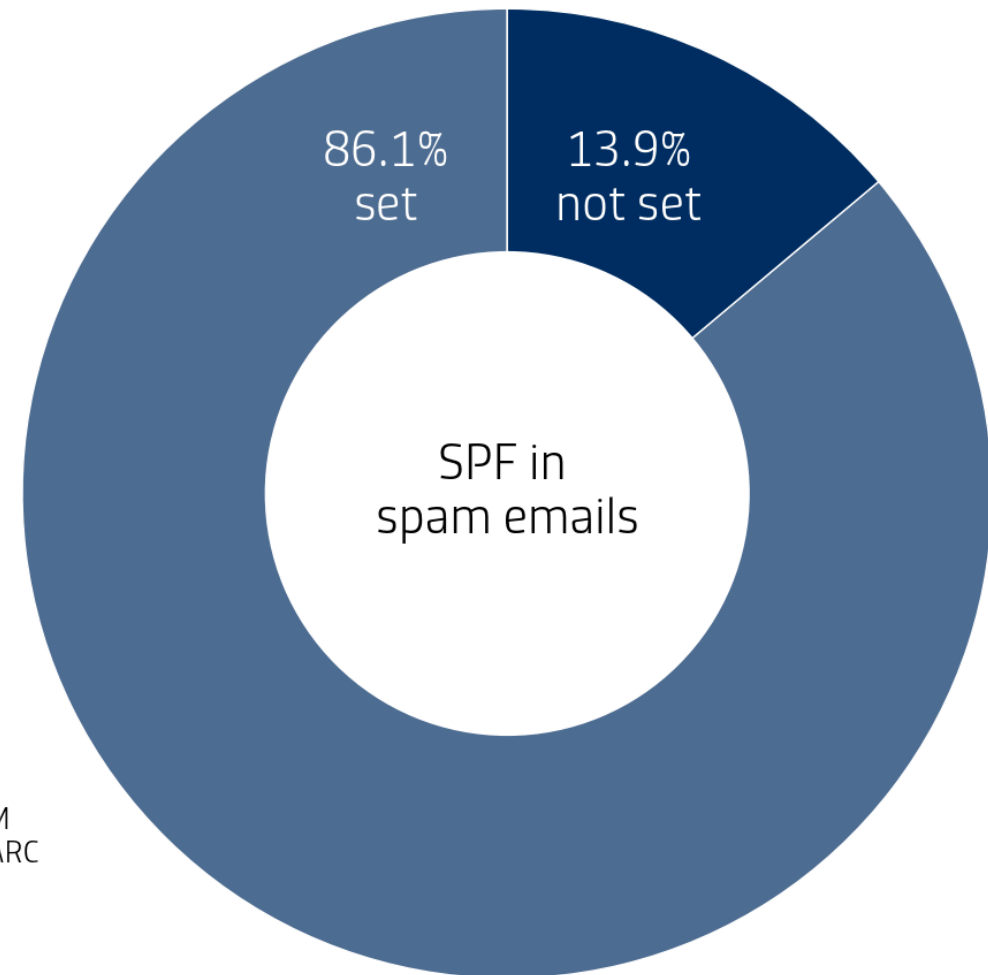
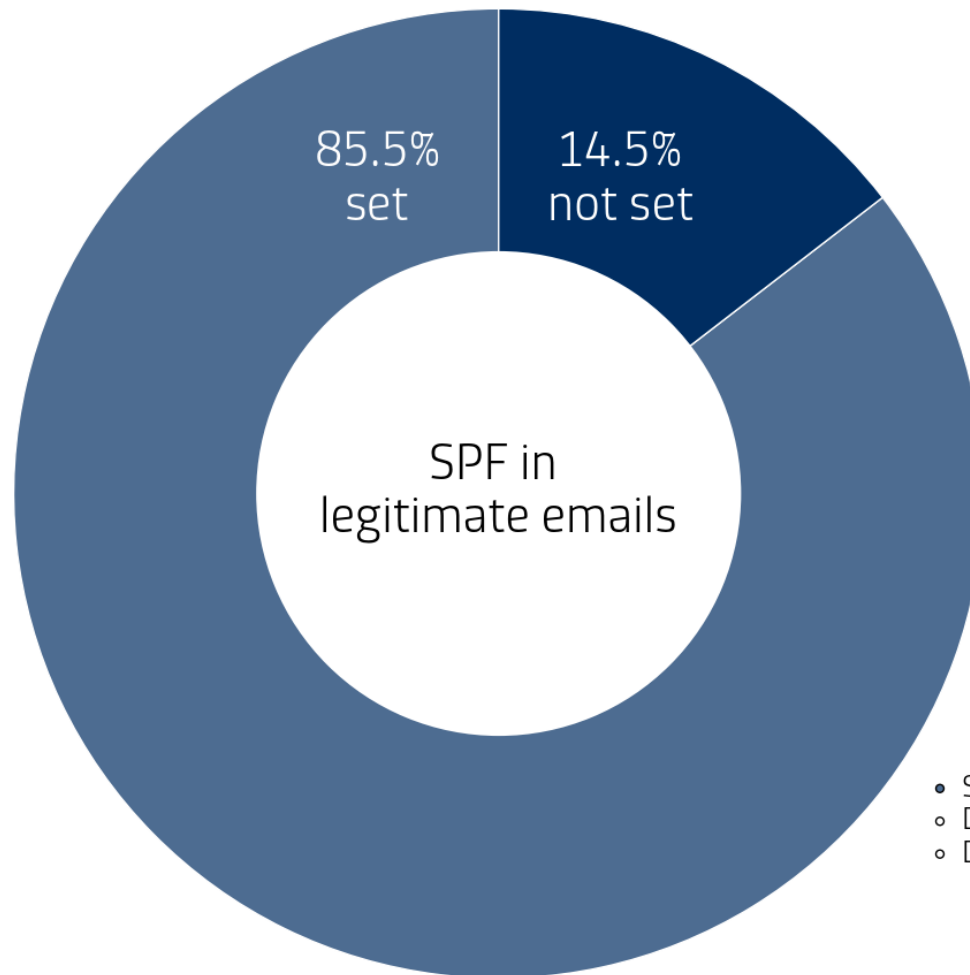
Hacker setzen DMARC auch ein.



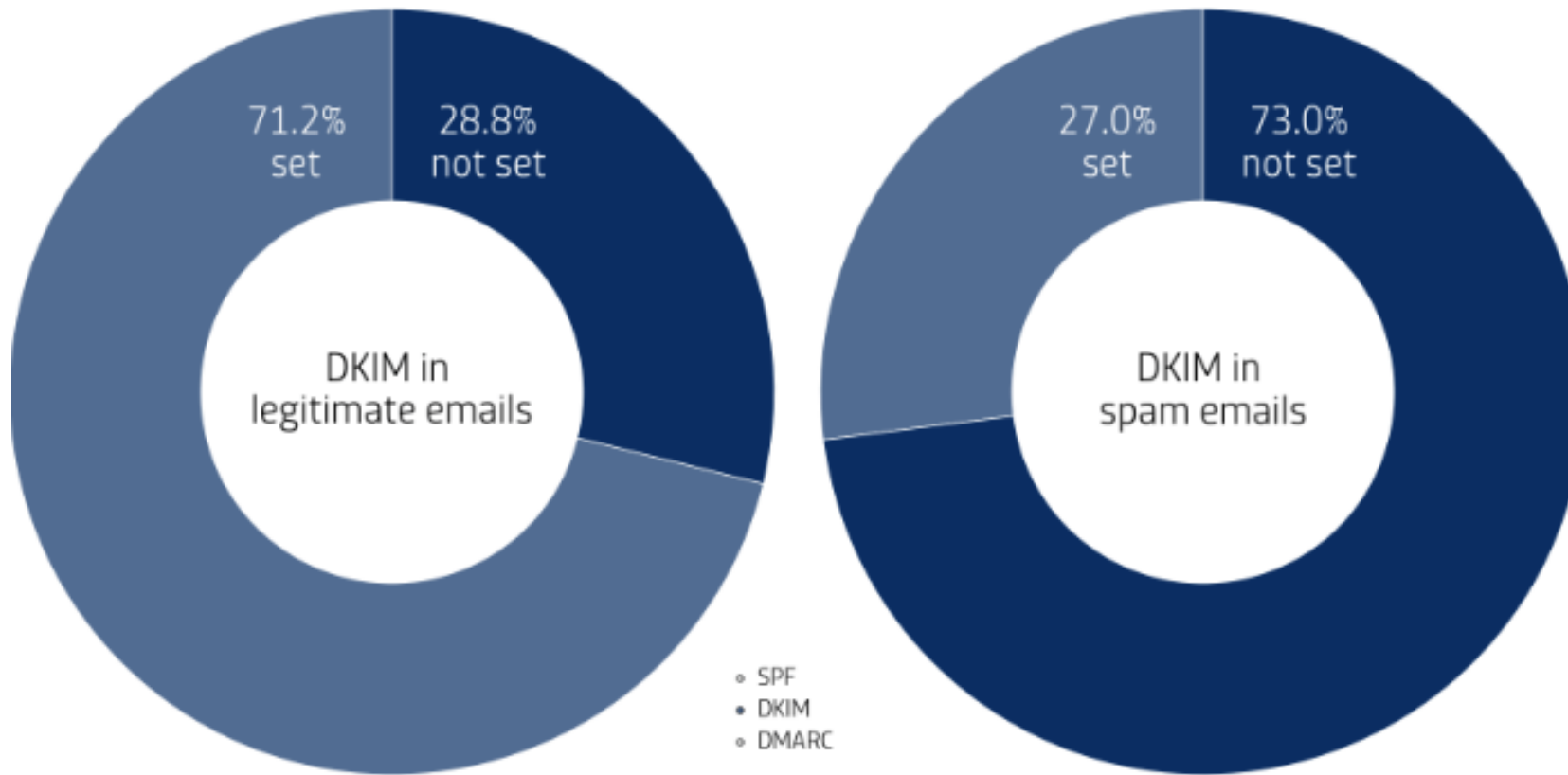
Pflicht für DMARC bei mehr als 5.000 E-Mails pro Tag (seit Februar 2024)

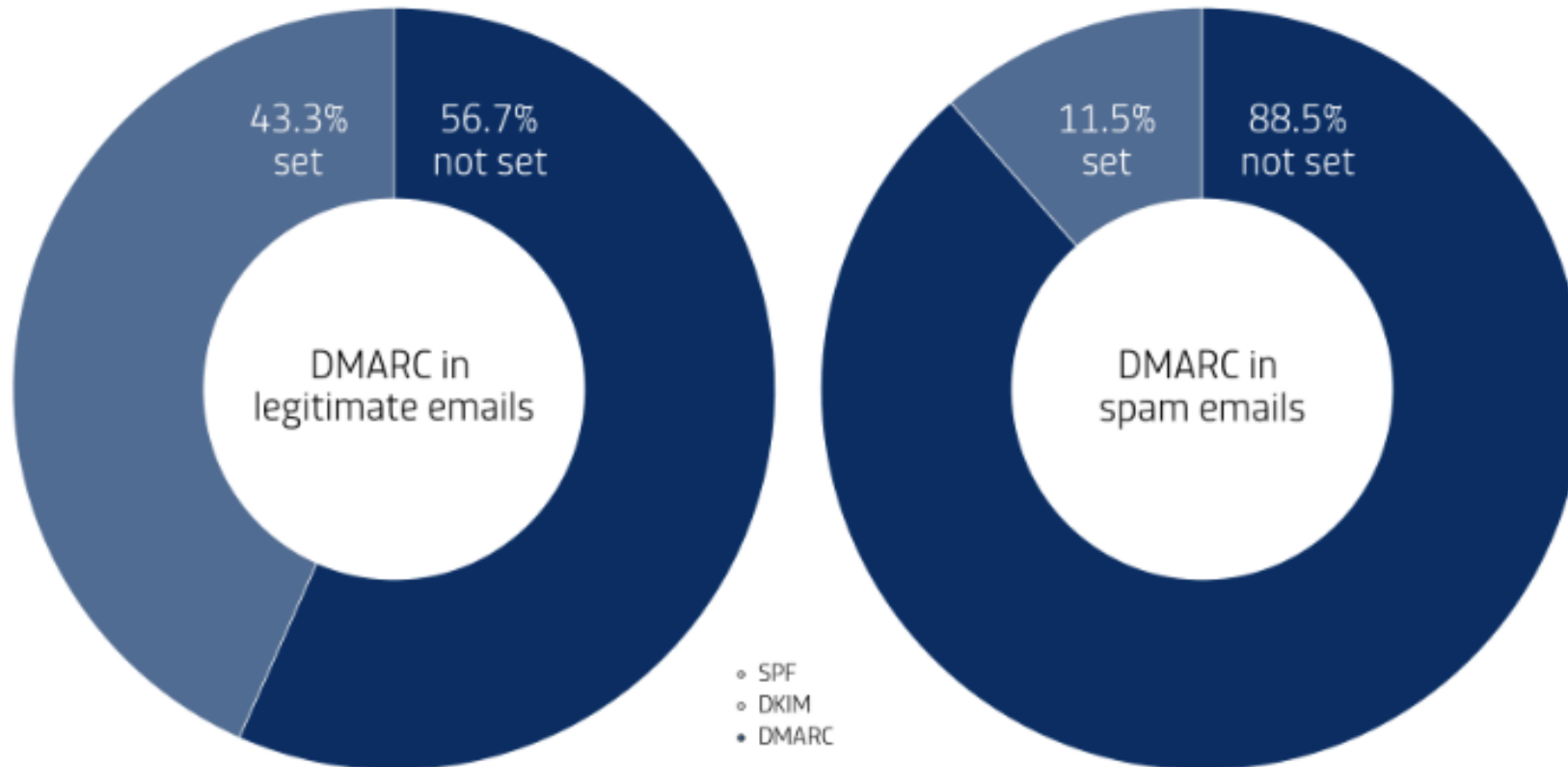


Ähnliche Regelung für Consumer-Dienste (seit Mai 2025)

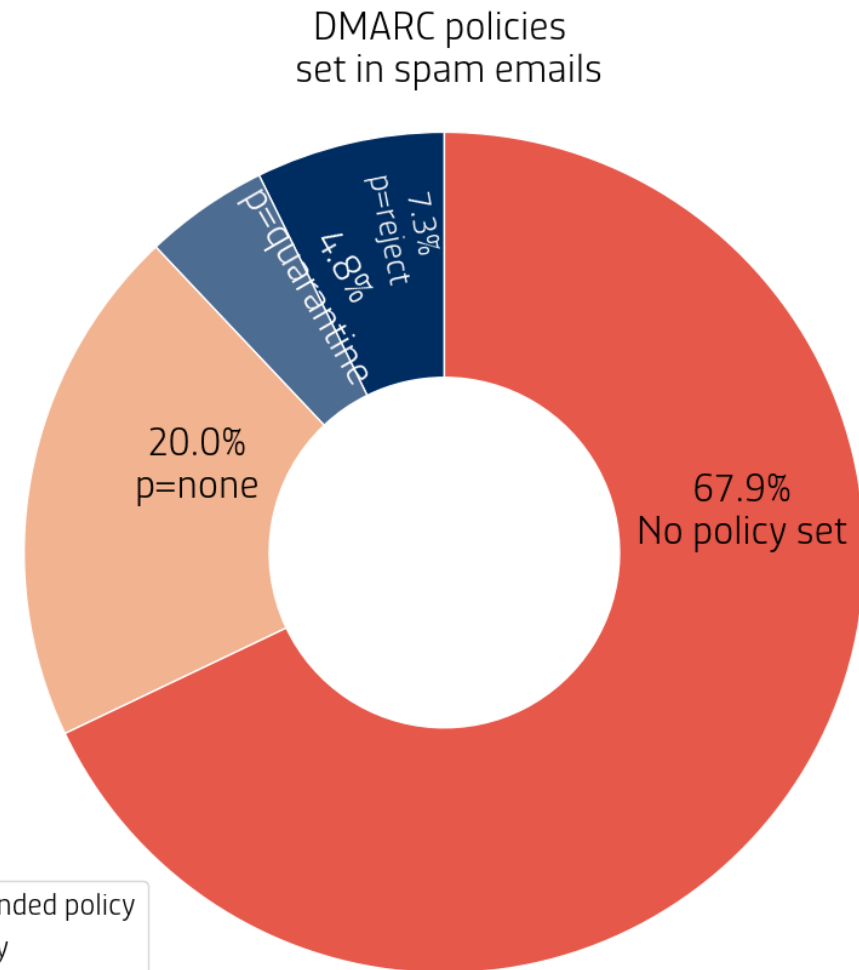
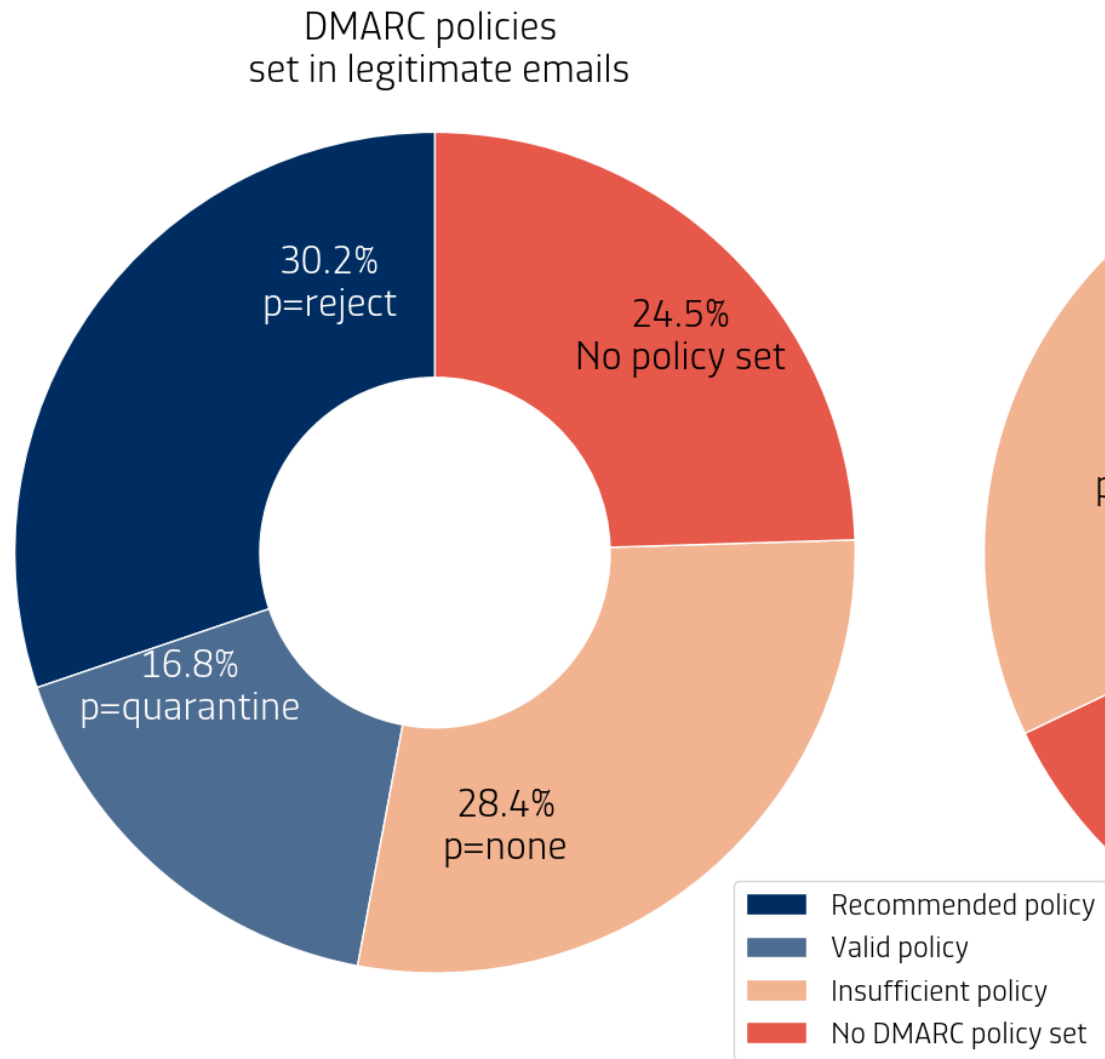


- SPF
- DKIM
- DMARC





Verbreitung der Policysettings





- SPF, DKIM und DMARC sind unerlässlich
- Die Einführung ist mit Hilfe von geeigneten Tools sehr einfach
- Jeder der es nicht macht, hinkt den bösen Jungs hinterher