



GAC DISCUSSION ON DNS ABUSE MITIGATION

Keeping Indonesia's DNS Secure and Trusted

Stronger domain abuse mitigation through technology, digital literacy, collaboration, and policy.

ICANN87 | BALI

Ashwin Sasongko Sastrosubroto - Indonesian GAC Member
Ery Punta Hendraswara - PANDI .id Registry

● National Basic Policy

Legal foundation and government–registry cooperation on DNS abuse

01

Based on Indonesian Act on Electronic Information and Transaction, DNS abuse is considered criminal activities.

02

MCDA, the Ministry of Communication and Digital Affairs (Komdigi) as the Regulator, the National Cyber and Crypto Agency (BSSN) and Indonesia National Police work together to make sure that DNS abuse can be minimized.

03

To carry it out, the Government works together with PANDI, the .id registry.

04

With the plan of several new gTLD applications from Indonesian institutions, the above cooperation will certainly need to be enlarged.

• DNS Abuse and Content Abuse Are Not the Same

Effective mitigation calls for the right actor at the right layer.



DNS Abuse (ICANN Definition)

Threats that exploit domain names or DNS to facilitate malicious activity.

PHISHING

MALWARE

BOTNET

PHARMING

SPAM (AS A VECTOR)

Spam is included when used to deliver the four threats above.



Domain / Content Misuse

National rules and registry policies may cover a broader range of conduct.

ONLINE
GAMBLING

BRAND
IMPERSONATION

ILLEGAL CONTENT

COMPROMISED SITES

Not all harmful or illegal content meets the ICANN definition of DNS Abuse.

KEY POINT • Mitigation requires registries, registrars, infrastructure providers, government and users.

● A National Framework for DNS Abuse Response

Effective response draws on public policy, cybersecurity, law enforcement and .id operations.

REGULATION AND PUBLIC ACTION

Komdigi

Policy oversight, public awareness, and national negative-content handling.

CYBERSECURITY COORDINATION

BSSN

Cyber resilience expertise and coordination on security risks and incidents.

INVESTIGATION AND ENFORCEMENT

Indonesian National Police

Criminal investigation where applicable laws and supporting evidence warrant action.

.ID DOMAIN OPERATIONS

PANDI & Registrars

Domain-abuse monitoring, validation, notification and proportionate registry-level action.

POLICY CONTEXT • Illegal online activity, content enforcement and DNS Abuse must be assessed at the appropriate legal and technical layer.

● Cyber Threat Landscape in Indonesia

LATEST VERIFIED INDICATORS

● Phishing & Online Scams

Fake sign-in pages, impersonation and deceptive links can steal credentials or money. OJK's Anti-Scam Centre received 702,342 financial fraud reports through September 2026, covering multiple scam types.

● Malware & Ransomware Exposure

BSSN monitored around 5.16 billion anomalous internet traffic events during 2025. These are warning signals of potentially malicious activity—not confirmed ransomware cases or successful breaches.

● Online Gambling Transactions

PPATK traced IDR 86.82 trillion (USD 4.84 billion) in online-gambling fund turnover across 467.32 million transactions in the first half of 2026. The turnover value was 12.9% lower than in H1 2025.

FINANCIAL SCAM REPORTS

702,342

OJK / IASC · Nov 2024–Sep 2026

Not phishing-only

TRAFFIC ANOMALIES MONITORED

5.16B

BSSN · Jan–Dec 2025

Not confirmed attacks

GAMBLING-RELATED FUND TURNOVER

USD 4.84B

PPATK · Jan–Jun 2026

*467.32M
transactions*

SOURCES • OJK (Sep 2026) | BSSN / ANTARA (Aug 2026) | PPATK (Aug 2026)

● Komdigi: National Content Enforcement

OFFICIAL CONTENT-HANDLING DATA | AS OF 29 SEPTEMBER 2026

Outcomes monitored by MCDA

- All data on DNS abuse and related Mitigation, are registered by MCDA
- Slides below shows some results

Two reporting windows show the scale of national action against negative online content.

CUMULATIVE | 2016–29 SEP 2026

13,057,478

Content blocking actions

Websites: 9,980,543 | Social platforms: 3,076,935

RECENT PERIOD | 20 OCT 2024–29 SEP 2026

5,282,855

Content-handling actions

Websites: 4,528,320 | Social platforms: 754,535



These are negative-content enforcement statistics, not counts of unique DNS-abuse domains. The time periods overlap and must not be summed.

● Komdigi: Website Content Enforcement

CUMULATIVE REPORTING | 2016–29 SEPTEMBER 2026

WEBSITE CONTENT ACTIONS

9,980,543

ONLINE GAMBLING

7,819,734

PORNOGRAPHY

2,091,322

COMPLETE CATEGORY BREAKDOWN

Online gambling **7,819,734**

Pornography **2,091,322**

Intellectual property rights (IPR) **30,105**

Fraud **29,068**

Agency-referred negative content **8,083**

Information security violations **1,148**

Terrorism / radicalism **572**

SARA **191**

Regulated product sales **133**

False information / hoaxes **43**

Violence / child abuse **28**

Socio-cultural violations **26**

Unregistered PSEs **26**

Content causing public concern **24**

Separatism / prohibited groups **18**

Defamation **14**

Personal data protection **8**

Website statistics are content-handling counts, not a count of distinct DNS-abuse domains.

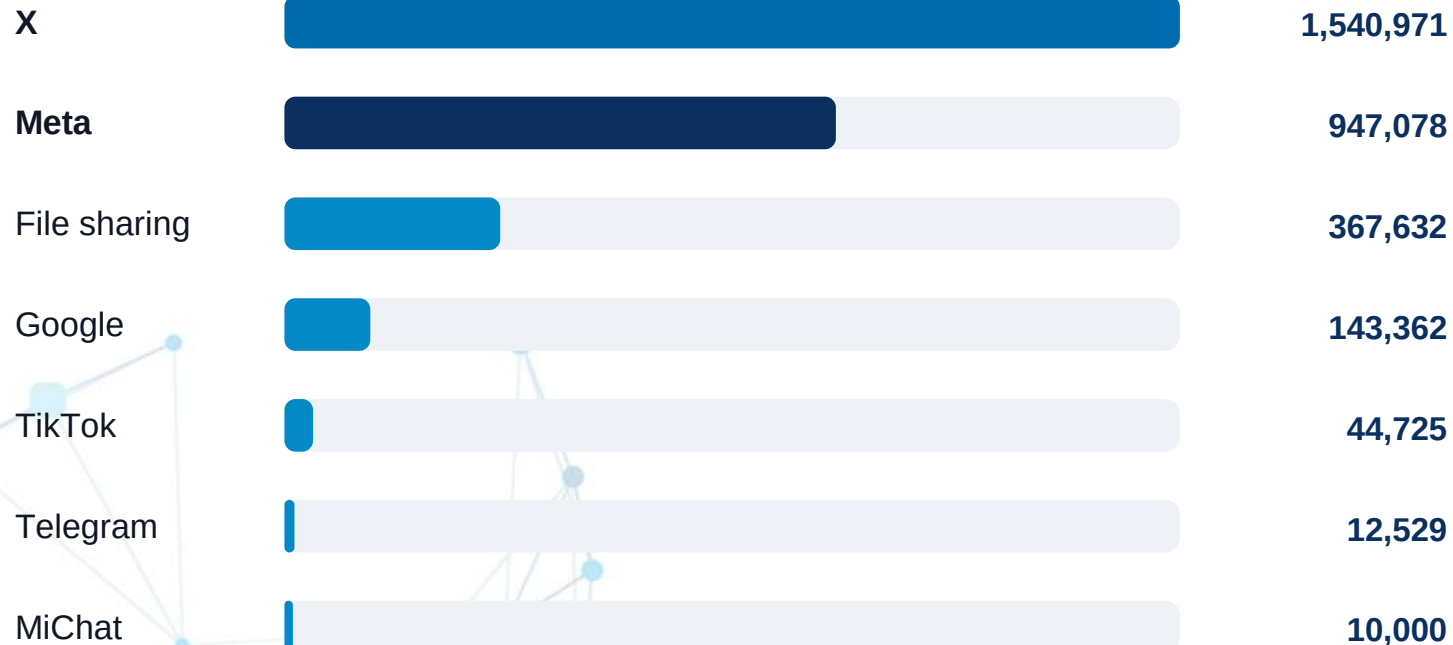
Komdigi: Social Media Enforcement

PLATFORM-LEVEL ACTIONS | 2016–29 SEPTEMBER 2026

TOTAL SOCIAL-MEDIA CONTENT ACTIONS

3,076,935

LARGEST PLATFORM CATEGORIES



OTHER PLATFORMS

Mango Live	4,757
Threads	2,328
Bigo Live	2,092
Snack Video	531
App Store	372
Pinterest	267
Hello-app	241
LINE	43
Grab	6
Yahoo	1

● Komdigi: Recent Enforcement by Category

WEBSITE + SOCIAL MEDIA | 20 OCT 2024–29 SEP 2026

ALL CATEGORIES

5,282,855

ONLINE GAMBLING

4,134,295

PORNOGRAPHY

985,167

FRAUD

57,927

ALL 22 CONTENT CATEGORIES

Online gambling	4,134,295	SARA	1,348
Pornography	985,167	Defamation	1,071
Fraud	57,927	Content causing public concern	847
Agency-referred negative content	29,154	Separatism / harmful organizations	740
DFK (source acronym)	23,512	Tobacco advertising	407
Terrorism / radicalism	17,046	Socio-cultural violations	214
False information / hoaxes	11,413	Violence / child abuse	150
Intellectual property rights (IPR)	9,447	Personal data protection	131
Other	5,306	Unregistered PSEs	26
Information security violations	2,781	Account recovery	3
Regulated product sales	1,867	Animal violence	3

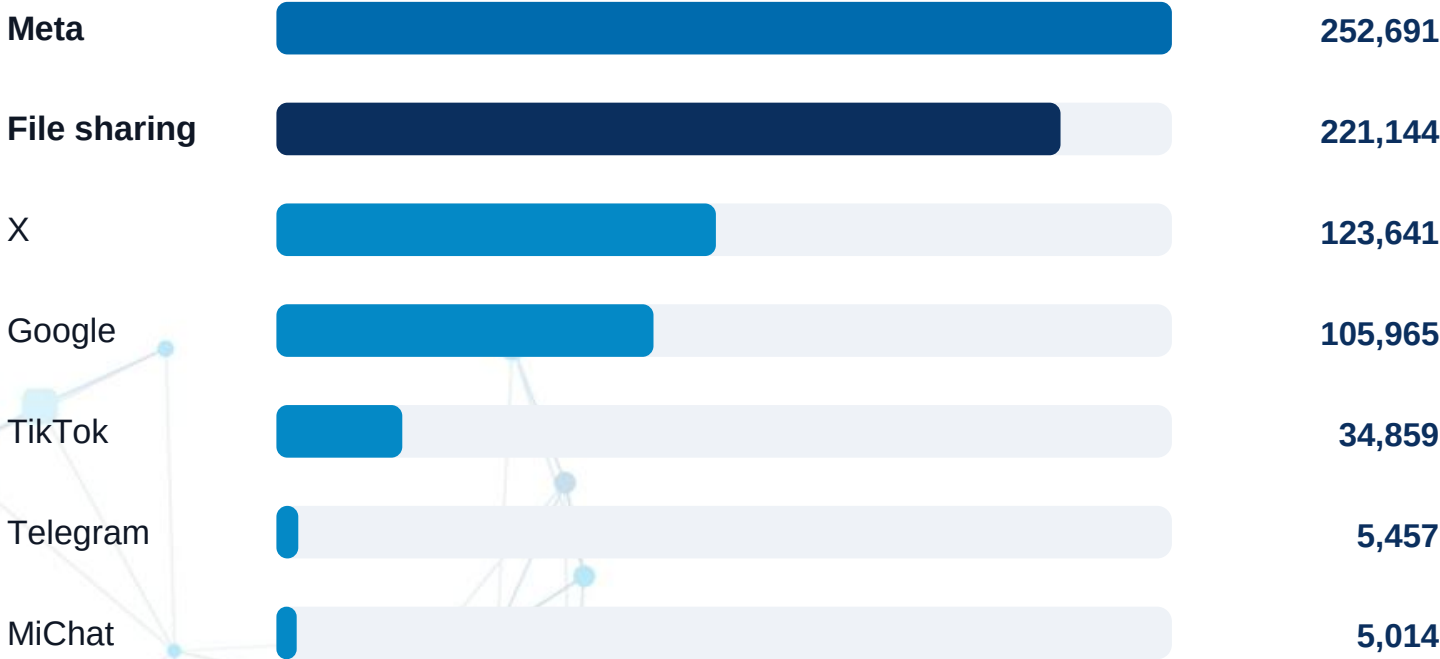
Komdigi: Recent Social Media Enforcement

PLATFORM-LEVEL ACTIONS | 20 OCT 2024–29 SEP 2026

TOTAL SOCIAL-MEDIA CONTENT ACTIONS

754,535

LARGEST PLATFORM CATEGORIES



OTHER PLATFORMS

Mango Live	2,978
Threads	2,131
App Store	273
Pinterest	267
Snack Video	83
LINE	15
Bigo Live	11
Grab	6

Komdigi: Website vs Social Media Actions

CATEGORY-LEVEL SPLIT | 20 OCT 2024–29 SEP 2026

WEBSITE ACTIONS

4,528,320

SOCIAL PLATFORM ACTIONS

754,535

COMBINED TOTAL

5,282,855

CATEGORY	WEBSITES	SOCIAL
Defamation	1	1,070
False information / hoaxes	6	11,407
Violence / child abuse	15	135
Agency-referred negative content	922	28,232
Socio-cultural violations	0	214
Content causing public concern	0	847
Other	0	5,306
Account recovery	0	3
Intellectual property rights (IPR)	9,274	173
Information security violations	756	2,025
Fraud	10,787	47,140

CATEGORY	WEBSITES	SOCIAL
Regulated product sales	3	1,864
Online gambling	3,636,974	497,321
Personal data protection	8	123
Pornography	869,529	115,638
SARA	1	1,347
Separatism / harmful organizations	2	738
Terrorism / radicalism	16	17,030
DFK (source acronym)	0	23,512
Tobacco advertising	0	407
Unregistered PSEs	26	0
Animal violence	0	3

• From National Monitoring to Global Coordination

An Indonesian perspective: content outcomes, domain evidence and cross-border action complement one another.

01 PUBLIC POLICY

National oversight

Komdigi content-handling statistics show the breadth of national action, but do not count unique DNS Abuse incidents.

02 OPERATIONAL RESPONSE

Evidence-led escalation

PANDI, registrars and providers need validated domain evidence, clear referral pathways and proportionate action.

03 FUTURE READINESS

Scalable cooperation

Potential new gTLD applications make consistent reporting, trained contacts and interoperable practices more important.

GAC DISCUSSION • How can multistakeholder cooperation make mitigation more consistent, timely and evidence-based?

• What DNS Abuse Looks Like in Practice

Illustrative attack paths help distinguish technical DNS Abuse from broader site misuse.

01

PHISHING

DNS ABUSE

A fake banking sign-in page is promoted through a deceptive email to steal user credentials.

Risk: account compromise and identity theft

02

PHARMING

DNS ABUSE

A poisoned DNS response sends a user to a counterfeit site—even when the correct URL was typed.

Risk: silent redirection and credential theft

03

ONLINE SCAM

BROADER
MISUSE

A fake store or support page persuades a victim to pay a fraudulent invoice or transfer funds.

Classification: assess the underlying conduct

04

COMPROMISED SITE

SITE MISUSE

A hacked school website displays gambling material or redirects visitors without its owner's consent.

Response: incident handling and site recovery

ICANN ALSO INCLUDES MALWARE, BOTNETS AND SPAM WHEN USED TO DELIVER OTHER DEFINED DNS ABUSE.

● IDADX and BIMA: Detection and Coordination

Published figures for H1 2026 (January 1–June 30, 2026).



32,535

URLs flagged for potential abuse



25,815

Domains monitored

1



2



3



4

Data & reports

IDADX analysis

BIMA support

Coordination

Leading Report Categories

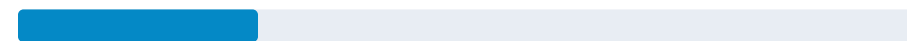
Online gambling

24,523



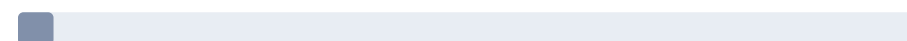
Phishing

6,491



Malware

961



Category figures reflect report totals published by PANDI.

IDADX: data exchange and follow-up | BIMA: identifying and monitoring potential .id abuse

● The Scale of .id Domain Abuse

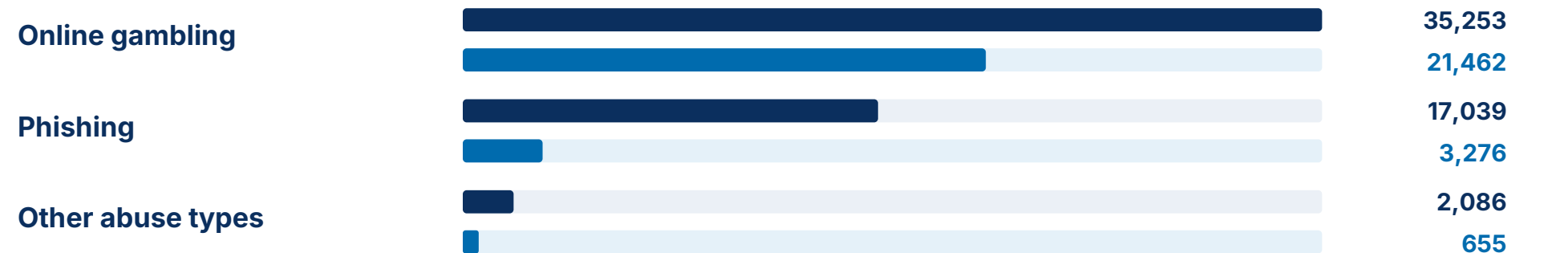
Cumulative IDADX figures as reported in the waf proxy collaboration brief, through June 2026.

53,157
Flagged .id abuse domains

24,887
Using waf proxy nameservers

46.8%
Share of flagged .id domains

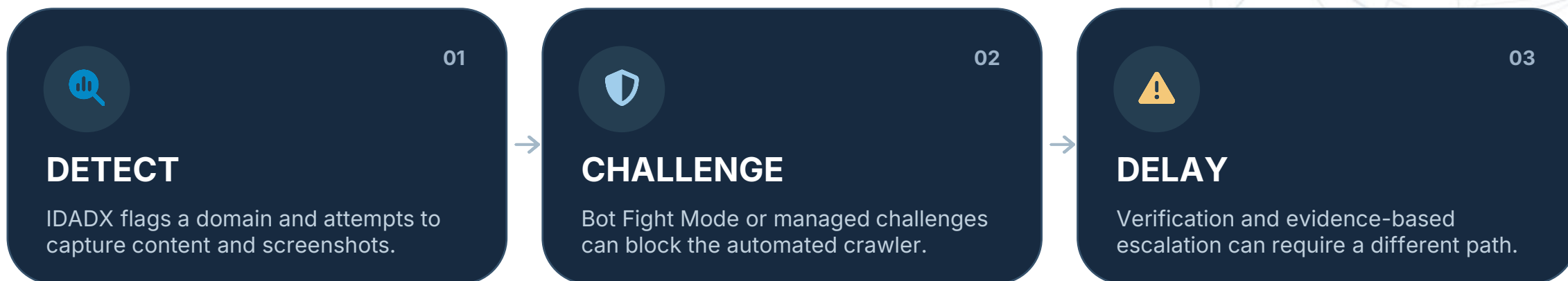
Reported Categories



Category counts should not be added to reproduce the headline totals; confirm the source methodology.

• The Evidence-Verification Bottleneck

Anti-bot protections can interrupt IDADX automated evidence collection—not the existence of a case itself.



60.9% of flagged gambling .id domains route DNS through waf proxy

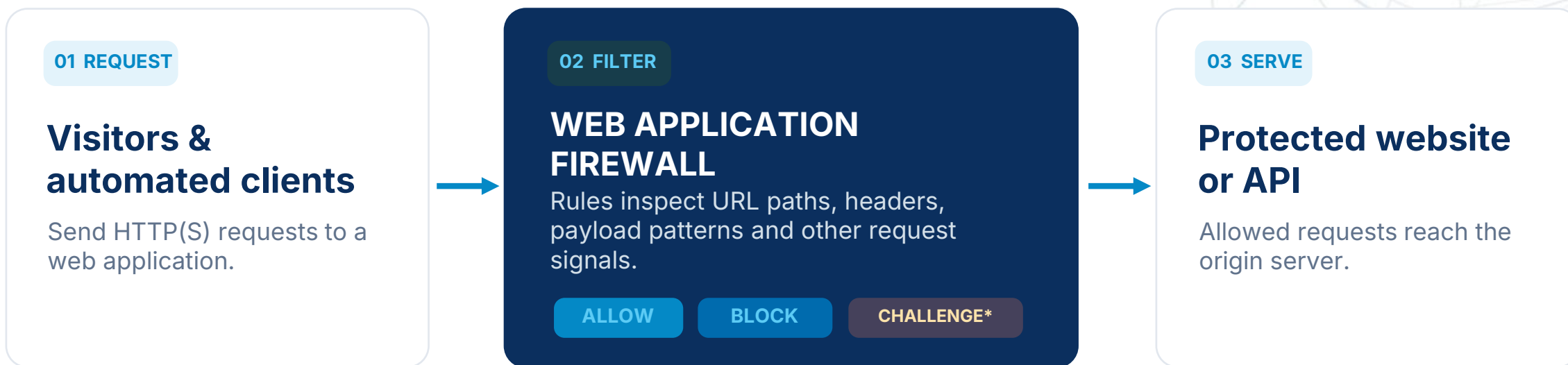
1,905 institutional .id waf proxynameservers

.ac.id 1,003 .sch.id 446 .or.id 242 .go.id 214

These are IDADX monitoring findings, not proof of provider culpability. Verification status should be checked.

● How a Web Application Firewall (WAF) Works

An application-layer filter for incoming web traffic; complementary to DNSSEC and abuse response.



HELPS MITIGATE

SQL injection, XSS and abusive HTTP requests.

DOES NOT REPLACE

DNSSEC, domain investigation and scam reporting.

*** BOT CHALLENGES ARE OFTEN SEPARATE EDGE CONTROLS; THEY MAY ALSO INTERRUPT LEGITIMATE ABUSE CRAWLERS.**

• Three Practical Collaboration Requests

IDADX proposal to Waf proxy Trust & Safety — do not treat as a completed agreement.



01

Verify the crawler

Recognize IDADX as a trusted monitoring bot, or allowlist agreed IP ranges to enable evidence capture.



02

Expedite abuse escalation

Establish a trusted-reporter path for substantiated .id cases, including gambling and compromised institutions.



03

Share data continuously

Exchange cases and outcomes through recurring lists or an API with Waf proxy Trust & Safety.

STATUS

Proposed IDADX–Waf proxy actions; implementation and commitments require confirmation.

● DNS Security Requires Complementary Safeguards

Organizational standards support governance; DNSSEC protects DNS data integrity.



SNI ISO/IEC 27001:2022

Information Security Management System

- ✓ Risk management and security controls
- ✓ Audits and continual improvement
- ✓ Operational resilience and governance



DNSSEC

Digital signatures for DNS responses

1

Signed zone



2

DS at parent



3

Validating resolver

DNS data origin authenticity and integrity



DNSSEC does not inherently stop phishing, assess site content, or replace other security measures.

● Regulation Is the Foundation; Enforcement Is Hard

Clarity of obligations, technical readiness, monitoring and oversight all matter.

REGULATION

Komdigi Regulation No. 5 of 2025

Article 43 includes DNSSEC among the information to be provided by agency domain name officials.

Note: this does not mandate that every domain be signed.

Practical Implementation Challenges

01

Roles and coordination

Domain owners, registrars, DNS/CDN operators and government have distinct roles.

02

DNSSEC readiness

Key management, DS delegation, validation and changes require expertise.

03

Compliance and enforcement

Action must be evidence-based, proportionate and within legal authority.

Focus: adoption metrics + guidance + enforcement

● From Detection to Coordinated Action

Proposed cross-sector priorities to strengthen Indonesia's digital ecosystem.



SUGGESTED METRICS DNSSEC coverage • Verified reports • Response time • Literacy reach

Thank You.

