# DNS Abuse Response Framework

## 1. Purpose and Scope

This DNS Abuse Response Framework (“Framework”) defines Atak Domain’s processes for detecting, validating, and responding to DNS abuse in accordance with ICANN requirements, Registry Operator agreements, and international best practices (DNS Abuse Institute, APWG, M3AAWG).
This Framework applies to all domain names registered, managed, or hosted through Atak Domain.

## 2. Definition of DNS Abuse

According to ICANN, the five primary categories of DNS abuse are:

1. Malware
2. Botnet command-and-control (C2) infrastructure
3. Phishing
4. Pharming / DNS manipulation
5. Spam (only when used as a vector for abuse)

Additionally, certain TLDs (e.g., .BANK, .INSURANCE, .GOV, .TR) impose broader restrictions, which Atak Domain fully adheres to.



## 3. Applicable Regulations and Compliance

Atak Domain strictly complies with the following:

- ICANN Registrar Accreditation Agreement (RAA) Section 3.18
- ICANN gTLD Registration Data Policies
- Expired Registration Recovery Policy (ERRP)
- Transfer Policy
- Whois Data Reminder Policy (WDRP)
- Registry-Registrar Agreement obligations
- TRABIS .TR domain name regulations
- International anti-abuse standards (APWG, M3AAWG, DNS Abuse Institute)

## 4. Abuse Team and Contact Information

Atak Domain maintains a dedicated technical and legal abuse response team.

Abuse reporting channels:

domain@apiname.com

hukuk@atakdomain.com

## 5. DNS Abuse Reporting Process

When a report is received, the following steps are executed:

### 5.1. Initial Verification

- Confirm whether the reported domain is under Atak Domain's management
- Examine evidence (URL, screenshots, logs, email headers, etc.)
- Assess whether the activity is active and verifiable

### 5.2. Evidence Requirements

Reports may include the following:

- Full URL / specific subpage
- Landing page screenshots (for phishing)
- Full email header (for spam cases)
- Malware scan reports
- IP / resolver logs
- Timestamped traffic data

Reports lacking evidence may not be processed.

## 6. Priority Levels and Response Times



Atak Domain responds according to the following prioritization:

**Level 1 – Critical (Immediate Action Required)**

- Active phishing
- Malware distribution
- Botnet C2 infrastructure
- Financial fraud

Response time: 0–2 hours
Action: Immediate suspension or DNS blocking

**Level 2 – High Risk**

- Pharming
- DNS poisoning
- Spam used as an abuse delivery mechanism

Response time: 4–12 hours

**Level 3 – Medium Risk**

- Suspected brand impersonation
- Fake technical support sites

Response time: 12–48 hours

destek@atakdomain.com atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR

**Level 4 – Low Priority / Content-Based Reports**

• Copyright infringement (requires DMCA process)
• Adult content complaints
Response time: 48–72 hours

**7. Abuse Detection Methods**

Atak Domain identifies DNS abuse through the following sources:

• User complaints
• Industry reputation/threat lists (Spamhaus, APWG, PhishTank)
• Google Safe Browsing / Microsoft SmartScreen alerts
• ICANN Compliance notifications
• Registry operator feedback
• Internal security monitoring tools
• Trusted notifier organizations (banks, government entities, etc.)

**8. Customer Notification Process**

When a domain is flagged for abuse:

1. The customer is notified via email
2. A 24-hour window is provided for explanation or remediation (no grace period for critical cases)
3. Relevant evidence is shared
4. If necessary, the domain may be suspended

If the customer does not respond, actions proceed automatically.

**9. Possible Enforcement Actions**

If abuse is verified, Atak Domain may take the following actions:

• Domain suspension (clientHold)
• DNS blocking or redirection removal
• Removal of Whois privacy
• Applying transfer lock
• Account termination
• Reporting to the registry operator
• Permanent domain deletion* (for severe and intentional cases)

**10. Trusted Notifier**

The following are treated as “trusted notifiers” and their reports may be expedited:



destek@atakdomain.com atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR

- Government authorities / Cybercrime units
- Financial institutions
- Registry operators
- ICANN organization
- Anti-abuse bodies

These reports may be actioned without consulting the customer.

**11. Legal Requests and Data Disclosure**

Official requests are accepted only from:

- Public Prosecutor's Offices
- Criminal Courts of Peace
- Law enforcement agencies
- International judicial authorities
- ICANN Compliance

Data disclosure contact:
domain@apiname.com, hukuk@atakdomain.com

**12. Data Retention and Log Management**

Under ICANN RAA requirements, Atak Domain retains:



- Whois verification records
- Transfer records
- IP logs
- Transaction history

Minimum retention period: 2 years.

**13. Transparency Reports**

Atak Domain may optionally publish annual transparency reports, including:

- Total abuse reports
- Number of suspended domains
- Phishing/malware detection statistics
- Response time metrics

Reports follow the "DNS Abuse Transparency Report" format.

**14. Updates to the Framework**

This Framework may be updated in the event of:

- Changes in ICANN policies
- Registry agreement updates
- NIS2 / GDPR regulatory changes
- Changes in Turkish legislation
- Emergence of new abuse techniques



destek@atakdomain.com
atakdomain.com
İstasyon Mahallesi Efe Sadık Caddesi No: 4 İç Kapı No: 2 Kartepe, Kocaeli, TR