Domain Abuse Reporting

DNS Abuse Report

Atak Domain Bilgi Teknolojileri A.Ş. ("Atak Domain") is responsible for preventing, detecting, and responding promptly to domain name misuse (DNS Abuse) in accordance with ICANN regulations and the Registrar Accreditation Agreement (RAA).
This policy applies to all domain names registered through Atak Domain.

What is DNS Abuse?

In parallel with ICANN's definition, DNS Abuse includes the following core categories:

Phishing

Fraudulent websites designed to obtain confidential information such as banking credentials or login details.

Malware

Distribution or hosting of malicious software such as viruses, trojans, and ransomware.

Botnet

Using a domain name to operate or control a network of compromised devices (botnet).

Pharming

Manipulating DNS records to redirect users to fraudulent websites.

Spam

Only when used to distribute or facilitate the types of DNS Abuse listed above.
(Ordinary commercial e-mail complaints are not considered DNS Abuse.)

The following issues are generally **not** part of DNS Abuse and fall under other processes such as UDRP, URS, court procedures, or notifications to hosting providers:

- Trademark or trade name disputes
- Copyright, content, or personal rights violations
- General hosting content complaints

How to Report DNS Abuse

If you believe a domain registered through Atak Domain is being used for DNS Abuse, you may contact us via the following channels:

- Abuse email 1: domain@apiname.com
- Abuse email 2: hukuk@atakdomain.com
- Support / contact form: Support ticket system in the customer panel or the contact form on our website
- Telephone (for abuse reporting): +90 262 325 9222

Information Required in Your Report

To ensure accurate and efficient investigation, please include as much of the following information as possible:

• Description of the abuse
(Example: “Phishing login page”, “Malware distribution”, “Botnet C2 server”)
• Domain name involved
(Example: exampledomain.com – preferably stated clearly in the email subject line)
• Exact URL or URLs involved
(Example: https://exampledomain.com/login/verify – can be provided defanged if necessary)
• Evidence
o Screenshots
o Defanged URLs (example: hxxps://example[.]com)
o Email headers (for phishing or spam cases)
o Relevant logs or technical details (if available)
• Your contact information
A valid email address and, if applicable, institutional information.

Reports with missing details are still accepted, but providing complete information helps accelerate the investigation.

What Happens After You Submit a Report

When Atak Domain receives a DNS Abuse report, the general process is as follows:

1. Acknowledgment

• Your report is recorded in our system.
• You receive an acknowledgment e-mail as soon as possible.

This acknowledgment typically includes:
• Date and time the report was received
• Subject of the report (domain name, type of abuse)
• A unique Ticket ID or reference number

2. Preliminary Review

• The relevant domain and URLs are checked by our technical teams.
• We attempt to verify the existence of phishing, malware hosting, botnet activities, pharming, etc.
• If necessary, the registrant, reseller, or hosting provider is contacted.

3. Necessary Actions

Depending on the investigation results, one or more of the following actions may be taken:

• Requesting the registrant to remove or correct the harmful content
• Temporarily suspending or modifying DNS records

- Reporting the issue to the registry operator, relevant TLD authorities, or government entities
- Other technical or legal measures required under ICANN / RAA 3.18

4. Closure and Feedback

- Once the review is completed, we inform the complainant as much as possible.
- In certain cases (for example official investigations or confidentiality obligations), details may be limited.

Investigation and Enforcement Actions

Situation | Action
Phishing, malware, botnet, or direct abuse | If sufficient evidence is confirmed, the domain is suspended (clientHold). The registrant is notified. A transfer lock may be applied if necessary.
Compromised website or subdomain | Registrant is notified and given time to resolve the issue. If the content is not cleaned, intervention is performed.

Response Timeline

- Urgent cases requiring immediate action: After necessary checks, immediately or within 2 business days
- Compromised websites: Within 3 business days
- Mass or critical threats (Botnet, etc.): Action within 6 hours or coordination with authorities

Record Keeping and Reporting

All processes are recorded and kept ready for ICANN audits.
Records are retained for at least 2 years.

Communication for Government Authorities

Requests from official authorities are processed promptly via hukuk@atakdomain.com,domain@apiname.com
Legal processes or governmental demands are evaluated separately.

Legal Notice

Under ICANN rules, requests outside the scope of DNS Abuse such as legal disputes or trademark conflicts cannot be evaluated within this process.
Such matters must be addressed through UDRP procedures or courts.

1. Inaccurate WHOIS Information – Review and Correction Process

In accordance with ICANN regulations, Atak Domain is required to ensure the accuracy of WHOIS information. Any report of inaccurate WHOIS data follows the steps below:

- Within 2 business days after receiving the request, an investigation of the WHOIS record begins. The Registered Name Holder (RNH) and Customer Account Holder (CAH) are notified by email.
- RNH/CAH is given 7 days to provide documents proving the accuracy of the WHOIS information.
- After reviewing the documents, one of the following actions is taken:
  - If documents are valid and WHOIS data is accurate, the case is closed successfully.
  - If documents are outdated and WHOIS data is incorrect, the information is updated and the case is closed.
  - If no documents are provided or the information is insufficient, the domain may be suspended or deleted due to failure to correct WHOIS data.

Note: Both the registrant and the registrar are responsible for ensuring WHOIS information remains accurate and up to date.

2. Cybersquatting and Trademark Infringement Reports

As an ICANN-accredited registrar, Atak Domain processes trademark infringement and cybersquatting reports impartially.

- The RNH and CAH are notified within 2 business days after receiving the complaint.
- If WHOIS information is public, it is shared with the complainant.
- If WHOIS data is protected but available within the system, guidance is provided to the complainant regarding next steps.
- If WHOIS information is protected under GDPR, the complainant must provide an official, written, and GDPR-compliant request.

Important Notice: Atak Domain is a technical and administrative intermediary. Without a court order or an ICANN UDRP decision, Atak Domain cannot suspend, delete, or transfer a domain name.

Situation	**Action**
Phishing, Malware, Botnet or similar direct abuse	If sufficient evidence is confirmed after the investigation, the domain name is suspended (clientHold). The domain owner is notified. A transfer lock is added if necessary.
Compromised website or subdomain	The domain owner is notified and given time to resolve the issue. If the malicious content is not removed, intervention is taken.

Aşağıda metnin tamamının **profesyonel İngilizce çevirisi** yer almaktadır:

Process Timeline

• **Urgent Cases Requiring Immediate Action:** Action is taken immediately or within a maximum of 2 business days after necessary checks are completed.
• **Compromised Websites:** Action is taken within a maximum of 3 business days.
• **Mass or Critical Threats (such as Botnet activity):** Action is taken within 6 hours or coordination with the relevant authorities is established.

Record Keeping and Reporting

All processes are logged and kept ready for ICANN audits. Records are retained for at least 2 years.

Communication for Government Authorities

Requests from government authorities are promptly processed via hukuk@atakdomain.com. Legal proceedings or official requests are evaluated separately.

Legal Notice

Under ICANN rules, requests that fall outside the scope of DNS Abuse, such as legal disputes or trademark conflicts, cannot be evaluated under this process.
For such matters, you must initiate a UDRP proceeding or pursue legal action through the courts.

1. Inaccurate WHOIS Information – Review and Correction Process

In accordance with ICANN regulations, Atak Domain is responsible for ensuring the accuracy of WHOIS data. Any report of inaccurate information follows the process below:

• Within 2 business days after receiving the report, a review of the WHOIS data begins. The Registered Name Holder (RNH) and Customer Account Holder (CAH) are notified by email.
• RNH/CAH is given 7 days to submit the necessary documents proving the accuracy of the WHOIS information.
• After reviewing the submitted documents, one of the following actions is taken:
o If the documents are valid and the WHOIS information is accurate, the case is successfully closed.
o If the documents are outdated and the WHOIS data is incorrect, the information is updated and the case is closed.
o If no documents are provided or the information is insufficient, the domain name may be suspended or deleted due to failure to correct WHOIS data.

Note: Keeping all WHOIS information accurate and up to date is the responsibility of both the registrant and the registrar.

2. Cybersquatting and Trademark Infringement Reports

As an ICANN-accredited registrar, Atak Domain handles trademark infringement or cybersquatting complaints impartially.

- Within 2 business days after receiving the complaint, the RNH and CAH are notified.
- If WHOIS information is publicly available, it is provided to the complainant.
- If WHOIS data is masked but available internally, guidance is given to the complainant on how to proceed.
- If WHOIS data is protected under GDPR, the complainant must submit an official, written, GDPR-compliant request.

Important Notice: Atak Domain acts only as a technical and administrative intermediary. Without a court order or an ICANN UDRP decision, Atak Domain cannot suspend, delete, or transfer a domain name.

UDRP Filing Page

Types of Abuse

Abuse Type	Name
Phishing	A website that impersonates another site in order to steal login or personal identification information.
Privacy concerns	For concerns related to privacy or GDPR.
Malware	A site or downloadable URLs involved in distributing malware or viruses. You may also report computer or network hacking activities, as well as sites engaging in such actions.
Network abuse	A site performing network attacks such as brute-force or denial-of-service (DoS) attacks. Unsolicited emails, texts, or SMS messages, including bank transfer fraud attempts and similar scams.
Spam	Disturbing images, violence, and similar harmful content.
Copyright complaints	For this matter, review ICANN’s Uniform Domain-Name Dispute-Resolution Policy (UDRP). If you suspect that a domain name was registered using false information.
Trademark complaints	A website hosted on Atak Domain products that uses a trademarked item without your permission.
Domain disputes	Bu konuda ICANN'in bu politikasını inceleyin: Uniform Domain-Name Dispute-Resolution Policy.
Invalid WHOIS	Bir alan adının sahte bilgilerle kaydedildiğinden şüpheleniyorsanız.

Abuse Type	Name
Content complaints	Fake technical support websites that do not phish login credentials but mislead users.
Child abuse	Material found on a website that promotes, encourages, or engages in the exploitation or abuse of children.