DNS Kötüye Kullanım Müdahale Çerçevesi (DNS Abuse Response Framework)

1. Amaç ve kapsam

Bu DNS Kötüye Kullanım Müdahale Çerçevesi (“çerçeve”), Atak Domain’in ICANN gereklilikleri, Registry Operatör sözleşmeleri ve uluslararası en iyi uygulamalar (DNS Abuse Institute, APWG, M3AAWG) doğrultusunda DNS kötüye kullanımını tespit etme, doğrulama ve müdahale süreçlerini tanımlar.

Bu çerçeve, Atak Domain üzerinden kayıt edilen, yönetilen veya barındırılan **tüm alan adlarını** kapsar.

2. DNS kötüye kullanımının tanımı

ICANN tarafından tanımlanan **beş ana DNS kötüye kullanım kategorisi** aşağıdaki gibidir:

1. **Kötü amaçlı yazılım (Malware)**
2. **Botnet komuta-kontrol (C2) altyapısı**
3. **Kimlik avı (Phishing)**
4. **Pharming / DNS yönlendirme manipülasyonu**
5. **Spam (yalnızca kötüye kullanımın dağıtım mekanizması olarak kullanıldığında)**

Ek olarak, bazı uzantılar (ör. .BANK, .INSURANCE, .GOV, .TR) daha geniş yasaklara sahiptir ve bu gerekliliklere uyulur.

3. Uygulanan düzenlemeler ve uyumluluk

Atak Domain, aşağıdaki kurallara kesin olarak uyar:

- ICANN Registrar Accreditation Agreement (RAA) Madde 3.18
- ICANN gTLD Registration Data Kuralları
- Expired Registration Recovery Policy (ERRP)
- Transfer Policy
- Whois Data Reminder Policy (WDRP)
- Registry-Registrar Agreement yükümlülükleri
- TRABIS .TR alan adı kuralları
- Uluslararası kötüye kullanım politikaları (APWG, M3AAWG, DNS Abuse Institute)

4. Kötüye kullanım ekibi ve iletişim

Kötüye kullanım bildirimleri için Atak Domain'in özel teknik & hukuki değerlendirme ekibi bulunmaktadır.

Bildirim adresleri:
domain@apiname.com
hukuk@atakdomain.com

5. Kötüye kullanım bildirim süreci

Bir rapor alındığında aşağıdaki adımlar uygulanır:

5.1. İlk doğrulama

- Raporun Atak Domain'e ait alan adına ilişkin olup olmadığı kontrol edilir
- Kanıt materyalleri incelenir (URL, ekran görüntüsü, log, e-posta başlıkları vb.)
- Aktivitenin **aktif ve doğrulanabilir** olup olmadığı değerlendirilir

5.2. Kanıt gerekliliği

Aşağıdakiler sunulabilir:

- Tam URL / alt sayfa
- Phishing için açılış sayfası görüntüleri
- Spam için tam e-posta başlığı (full header)
- Malware tarama raporları
- IP / resolver logları
- Trafik zaman damgaları

Kanıt sağlanmayan raporlar işleme alınmayabilir.

6. Öncelik seviyeleri ve müdahale süreleri

Atak Domain aşağıdaki öncelik sistemine göre müdahale eder:

Seviye 1 – Kritik (Acil Müdahale Gerektirir)

- Aktif phishing
- Malware dağıtımı
- Botnet C2 altyapısı
- Finansal dolandırıcılık
  Yanıt süresi: 0–2 saat
  Eylem: Anında askıya alma veya DNS'in bloke edilmesi

Seviye 2 – Yüksek Risk

- Pharming

- DNS zehirlenmesi
- Spam'ın kötüye kullanım mekanizması olarak kullanılması
  Yanıt süresi: 4–12 saat

Seviye 3 – Orta Risk

- Marka taklidi şüpheli aktiviteler
- Sahte teknik destek siteleri
  Yanıt süresi: 12–48 saat

Seviye 4 – Düşük öncelik / içerik temelli raporlar

- Telif ihlali (DMCA sürecine girer)
- Yetişkin içerik şikayetleri
  Yanıt süresi: 48–72 saat

7. Kötüye kullanım tespit yöntemleri

Atak Domain kötüye kullanım aktivitelerini şu yollarla tespit eder:

- Kullanıcı şikayetleri
- Kurumsal tehdit listeleri (Spamhaus, APWG, PhishTank)
- Google Safe Browsing / Microsoft SmartScreen uyarıları
- ICANN Compliance bildirimleri
- Registry operatörlerinin geribildirimleri
- İç güvenlik izleme sistemleri
- "Trusted notifier" kuruluşları (bankalar, devlet otoriteleri vb.)

8. Müşteri bilgilendirme süreci

Bir alan adı kötüye kullanım için işaretlendiğinde:

1. Müşteriye e-posta ile bildirim yapılır
2. Açıklama veya düzeltme için 24 saat süre verilir (kritik durumlarda süre verilmez)
3. Kanıtlar iletilir
4. Gerekirse alan adı askıya alınır

Yanıt verilmemesi durumunda işlem otomatik olarak uygulanır.

9. Uygulanabilecek yaptırımlar

Kötüye kullanım doğrulanırsa Atak Domain aşağıdaki yaptırımları uygulayabilir:

- Alan adının askıya alınması (clientHold)
- DNS yönlendirmesinin bloke edilmesi

- Whois gizliliğinin kaldırılması
- Transfer kilidi uygulanması
- Hesabın kapatılması
- Registry operatörüne raporlama
- Alan adının tamamen silinmesi* (ağır ve kasıtlı durumlarda)

10. Trusted notifier (Güvenilir Bildirimci)

Aşağıdaki taraflar “güvenilir bildirimci” olarak hızlı işleme alınır:

- Devlet kurumları / Siber Suçlar
- Finans kuruluşları
- Registry operatörleri
- ICANN organizasyonu
- Anti-abuse organizasyonları

Bu raporlar müşteriye danışılmadan işleme alınabilir.

11. Yasal talepler ve veri paylaşımı

Yalnızca aşağıdaki kaynaklardan gelen resmi talepler kabul edilir:

- Savcılık
- Sulh Ceza Hakimliği
- Emniyet birimleri
- Uluslararası adli otoriteler
- ICANN Compliance
  Veri paylaşımı:
  domain@apiname.com,hukuk@atakdomain.com

12. Veri saklama ve log yönetimi

ICANN RAA gereği Atak Domain:

- Whois doğrulama kayıtlarını
- Transfer işlemlerini
- IP loglarını
- İşlem geçmişini

minimum 2 yıl süreyle saklamakla yükümlüdür.

13. Şeffaflık raporları

Atak Domain, isteğe bağlı olarak yıllık olarak şu verileri yayımlayabilir:

- Toplam kötüye kullanım bildirimi
- Askıya alınan alan adı sayısı
- Phishing/malware tespit raporları
- Yanıt süreleri

Bu raporlar “DNS Abuse Transparency Report” formatındadır.

14. Çerçevenin güncellenmesi

Bu çerçeve, aşağı durumlarda güncellenebilir:

- ICANN politika değişiklikleri
- Registry sözleşmesi güncellemeleri
- NIS2 / GDPR düzenlemeleri
- Türkiye mevzuat değişiklikleri
- Yeni kötüye kullanım tekniklerinin ortaya çıkması

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