TEKNİK RAPOR · ÖNERİLEN ÇERÇEVE · SÜRÜM 1.0

Tespitten müdahale tedbirlerinin uygulanmasına

DNS Abuse müdahalesi için ölçülebilir bir mimari: kanıtın kaynağı ve gözetim zinciri, orantılı eylem, kamusal hesap verebilirlik ve hızlı itiraz—yalnızca ileri sürülmek için değil, test edilmek üzere tasarlanmıştır.

- 2 Ağustos 2026 tarihinde yayınlandı
- PhishDestroy Araştırma
- Halkın görüşüne sunulan taslak
- Hakem değerlendirmesinden geçmemiştir

PD-WP-2026-01 · Sürüm 1.0 · 2 Ağustos 2026 tarihinde yayınlanmıştır
Kalıcı URL: https://phishdestroy.io/tr/dns-abuse-enforcement-framework

ÖZET

BAĞIMSIZ TEKLİF · “ICANN” PROGRAMI DEĞİLDİR

Doğrudan sonuç. gTLD’in sözleşmeye dayalı ekosisteminde, bir alan adının teknik olarak doğrulanmış kötü niyetli kullanımı ile etkili önleme tedbirleri arasında ölçülebilir bir boşluk bulunmaktadır. Yayınlanan araştırmalar, birçok kimlik avı kampanyasının saatler veya günler boyunca devam ettiğini, buna karşın sözleşmeye uygunluk prosedürlerinin iş günü zaman dilimlerinde gerçekleşebileceğini göstermektedir. Açıklanan senaryo modeli, gecikmenin beklenen kampanya getirisini nasıl artırdığını göstermektedir; %60–85 aralığı, makalenin bildirim sonrası zarara ilişkin temel test edilebilir tahminidir, tüm küresel dolandırıcılık vakaları için belirlenmiş bir istatistik değildir. 100–150 dolarlık mühendislik tahmini, yasal inceleme veya yaptırımın tam maliyetini değil, tanımlanmış bir bölge, Sertifika Şeffaflığı ve kamuya açık besleme verileri kümesinin toplanması ve ilk aşama işlenmesini kapsamaktadır. Makale, imzalı kanıtlar, ölçülebilir yanıt hedefleri, doğrulanmış vakaların otomatik olarak üst mercilere iletilmesi, orantılı çözümler, kamuya hesap verebilirlik ve hızlı itiraz süreçlerini önermektedir. Rapor edenlere etki alanı askıya alma kontrollerine doğrudan erişim izni verilmesini önermemektedir.

● BİRİNCİL KAYNAK
Resmi bir belge veya yayınlanmış bir araştırma ile doğrudan desteklenmektedir.

● AÇIKLAYICI MODEL
Girdileri piyasa ortalamaları değil, varsayımlar olan ve tekrarlanabilir bir hesaplama.

● POLİTİKA ÖNERİSİ
Danışma, test ve düzeltme amacıyla sunulan bir tasarım.

01 Araştırma sorusu, kapsam ve ispat standardı

Soru, “kim başarısız oldu?” sorusundan daha dar kapsamlıdır: **Doğrulanmış kanıtlarla orantılı önlemlerin alınması arasında gözlemlenebilen gecikmelerden hangileri önlenebilir ve hangi müdahale, kabul edilemez düzeyde yanlış pozitif sonuçlara veya ikincil hasara yol açmadan mağdurun zararını azaltır?**

Kapsam, sözleşmeye tabi gTLD ekosistemidir: kayıt sahipleri, yeniden satıcılar, kayıt operatörleri, kayıt merkezleri ve ICANN’un sözleşmeye uygunluk birimi. Barındırma sağlayıcıları, CDN’ler, tarayıcılar, ödeme hizmetleri, reklam platformları, ulusal CERT’ler ve ceza adaleti yetkilileri, yalnızca kanıt veya

müdahale zincirini etkilediği durumlarda kapsama dahil edilir. Ülke kodu TLD'leri farklı bir yönetişim yapısına sahiptir ve ICANN adresindeki gTLD sözleşmelerine tabi olduğu varsayılmaz.

Temel tezlerin durumu

- Bu makale, ICANN adresini, gTLD ekosistemi içindeki özel bir yönetişim ve sözleşmeye uyum kurumu olarak analiz etmektedir. ICANN, bir devlet düzenleme kurumu veya kolluk organı değildir; ancak kayıt kuruluşlarını akredite eder, kayıt defteri işletmecileriyle sözleşmeler yapar ve bu sözleşmelerin uygulanmasını sağlar; bu sınırlı yetki alanı, kurumsal hesap verebilirliği ortadan kaldırmaz.
- %60–85 aralığı, makalenin zarar modelinde merkezi bir nicel tahmin niteliğindedir. Bu tahmin, tüm küresel dolandırıcılık vakaları için önceden belirlenmiş bir istatistik olarak değil, açık varsayımlardan ve vaka gözlemlerinden türetilmiş, test edilebilir bir tahmin olarak sunulmaktadır. Tespit, bildirim, etki azaltma ve zarar zaman damgalarını birbiriyle uyumlu hale getiren olay düzeyinde bir veri setinin yayınlanması, bir sonraki kanıtlama adımıdır.
- 100–150 dolarlık rakam, erişilebilir bir bölge kümesi, Sertifika Şeffaflığı ve temel altyapıdaki kamuya açık veri akışları üzerinden sürekli veri toplama ve ilk ön eleme işlemleri için test edilebilir bir mühendislik bütçe tahmini niteliğindedir. Bu rakam, tam küresel görünürlük, hukuki inceleme, itirazlar, yüksek kullanılabilirlik veya yaptırımların maliyetini yansıtmamaktadır. Bu nedenle makale, bu rakamı halihazırda kanıtlanmış evrensel bir fiyat olarak değil, yayınlanmış bir iş yükü, kaynak envanteri ve maliyet günlüğü ile tekrarlanabilir bir referans noktası olarak ele almaktadır. Bu ayrım, test edilen maliyet asimetrisini ortadan kaldırmadan iddiayı sınırlamaktadır.
- Makalede yer alan üç haftalık karşılaştırma, uyum gecikmesiyle ilgilidir; evrensel bir alan adı kaldırma hizmet seviyesi anlaşması (SLA) ile ilgili değildir. ICANN's Sözleşme Uyumluluğu SSS belirtilmektedir ki, çoğu şikayet türü resmi bir üst makama iletilmeden önce arka arkaya üç adet beş iş günü süren yanıt süresinden geçebilir; oysa birçok kötü niyetli kampanya saatler ya da günler boyunca devam eder. Sözleşmelerde ayrıca, eyleme geçilebilecek kanıtların ortaya çıkmasının ardından derhal ve uygun şekilde önlem alınması şartı getirilmiştir. [2] [4]
- Doğrulanmış, tek amaçlı bir kötü niyetli kayıt için, `serverHold` DNS düzeyindeki en büyük aksaklıklara yol açan çözümlerden biridir, çünkü bölgeden yetkilendirmeyi kaldırır. Bu çözüm evrensel değildir: posta hizmetlerini, alt etki alanlarını ve meşru hizmetleri de aksatabilir; önbelleğe alınmış yanıtlar TTL süresi dolana kadar kalabilir; ayrıca güvenliği ihlal edilmiş veya paylaşılan hizmetler için daha dar kapsamlı önlemler gerekebilir. [4] [7]

> ARAŞTIRMAYA KATKI
>
> Bu öneri, yanlışlanabilir niteliktedir. Bir pilot çalışma kapsamında, tedavi grubu ile kontrol grubu arasında triyaj süresine, müdahale süresine, kurban kaybı göstergelerine, nüksetme oranına, yanlış pozitif sonuçlara, durumun tersine dönme süresine ve ikincil etkilere ilişkin karşılaştırmalar yapılabilir.

02

Birincil kaynakların ortaya koyduğu gerçekler

$165.1M

ICANN FY27 operasyon finansmanı

FY27'ın bütçesi kabul edildi. Bağlamsal ölçek; DNS Abuse harcamaları değil. [1]

191,561

2025 IC3 kimlik avı/kimlik taklidi şikayetleri

Sayı bakımından en büyük IC3 şikayet kategorisi; doğrudan atfedilen zararlar 215,8 milyon dolar. [10]

24 saat

2021 yılında yapılan bir çalışmada belirlenen medyan ömür

1.288 kimlik avı etki alanı üzerinde elde edilen, veri setine özgü sonuç; genel bir ömür değeri değildir. [11]

Sabit bir SLA yok

Evrensel kaldırma son tarihi

2024 değişikliklerinde, tek bir genel son tarih yerine "derhal" ve "uygun" azaltma önlemleri öngörülmüştür. [2] [3]

ÖNERİ	DURUM	NELER SÖYLENEBİLİR?
Kimlik avı DNS Abuse kapsamındadır	DOĞRULANMIŞ	Kimlik avı, 2024 gTLD sözleşme değişikliklerinin açıkça kapsadığı beş kategoriden biridir. [2]
Kayıt kuruluşları harekete geçmelidir	DOĞRULANMIŞ	Kayıt kuruluşları, sponsor oldukları bir alan adının DNS Abuse amacıyla kullanıldığına ilişkin eyleme geçirilebilir kanıta sahip olduklarında derhal harekete geçmelidir. [2]
Kayıt operatörleri harekete geçmelidir	DOĞRULANMIŞ	Kayıt operatörleri, eyleme geçirilebilir kanıta dayanarak kayıtlı bir alan adının DNS Abuse amacıyla kullanıldığını makul biçimde belirlediklerinde derhal harekete geçmelidir; uygun önlem bağlama göre değişir. [3]
`serverHold` yetki devrini kaldırır	DOĞRULANMIŞ	Bu, sunucu tarafından ayarlanan bir "EPP" durumudur. Önbelleğe alınmış "DNS" yanıtları, geçerlilik süresi dolana kadar kalabilir ve bu işlem, kayıtlı alan adının tamamını etkiler. [7]
Tüm DNS Abuse vakaları CZDS veya CT üzerinden görülebilir	YANLIŞ	CZDS ve Certificate Transparency değerli sensörlerdir; ancak tüm alan adı kullanımının eksiksiz veya gerçek zamanlı görünümünü sunmaz. [8] [9]

ICANN'ın 2024 değişiklikleri kapsamında sözleşme şartlarının uygulanmasına ilişkin ilk altı aylık raporunda, 192 soruşturma, 2.700'den fazla askıya alınmış alan adı, 350'den fazla devre dışı bırakılmış kimlik avı sayfası ve iki adet İhlal Bildirimi kaydedildi. Bu rakamlar, mevcut denetimlerin yeterli olduğunu kanıtlamasa da, sistemin hiçbir önlem almadığı yönündeki mutlak iddiayı çürütmektedir. [5]

03

Tepki gecikmesi neden hâlâ geçerli bir araştırma konusu olmaya devam ediyor?

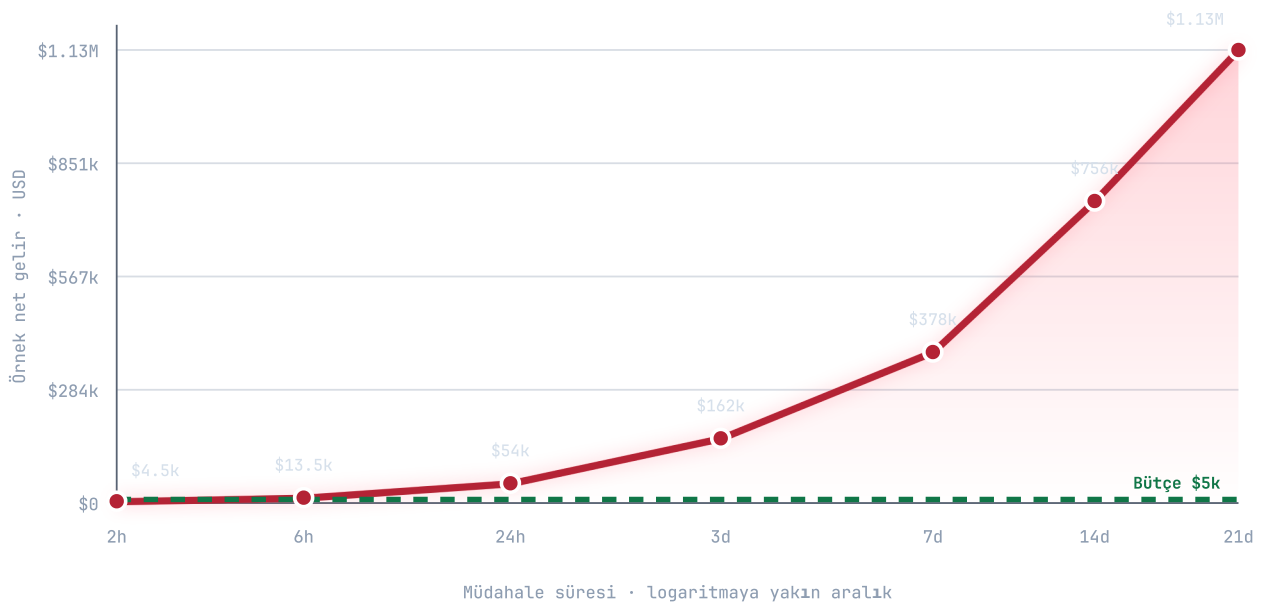
Bazı kimlik avı operasyonları saatler veya günler sürer. Bijmans ve arkadaşları, 2021 yılında yaptıkları bir çalışmada 1.288 kimlik avı etki alanı için gözlemlenen ortalama ömür süresinin 45 saat, medyan ömür süresinin ise 24 saat olduğunu bildirmiştir. [11] 2026 yılında yeni kaydedilen kimlik avı alan adları üzerine yapılan bir araştırmada, son derece çarpık bir dağılım ortaya çıktı: ömürleri ölçülebilen 14.112 alan adı için ortalama ömür 8,6 gün, medyan ömür ise bir gündü. [12] Her iki örnek de tüm tehdit sınıflarına genelleştirilemez, ancak her ikisi de yalnızca iş günleri bazında ölçülen bir sürecin, kısa süreli dolandırıcılık ve kimlik avı operasyonlarını neden gözden kaçırabileceğini göstermektedir.

ÖLÇÜLEN ZAMANSAL UYUMSUZLUK

Bu çalışmalar, bildirimden sonra meydana gelen mali zararın payını belirlemese de, bir zaman uyuşmazlığını ortaya koymaktadır: Erken aşamalarında gayri resmi uyum sürecinin on beş iş gününe kadar sürebileceği bir süreç, ortalama süresi bir güne yakın olan kampanyalar için tek başına bir olay müdahalesi işlevi göremez. Dolayısıyla, aşağıda belirtilen 21 günlük süre, evrensel bir "ICANN SLA" etiketi değil, bir uyum gecikmesi senaryosudur.

ŞEKİL 1 · DOLANDIRICILIK VE KİMLİK AVI OPERASYONUNUN AÇIKLAYICI NİTELİKTEKİ KÜMÜLATİF SONUCU

MODEL · LOGARİTMİK ZAMAN ARALIKLARI



Bu eğri, 4. Bölüm'deki senaryoyu görselleştirmektedir; gözlemlenmiş piyasa verileri değildir. Okunabilirliği artırmak amacıyla uzun aralıklar yatay olarak sıkıştırılmıştır. Kaynak: girdileri açıklanmış, tekrarlanabilir model.

NEDENSEL İHTİYAT

Bir alan adının ömrünün kısalması, otomatik olarak mali kaybın önlendiği anlamına gelmez. Saldırganlar, tespit edilmeden önce başka yerlere geçebilir, ele geçirilmiş siteleri kullanabilir, dağıtım kanallarını değiştirebilir veya paralarını nakde çevirebilir. Nedensel etki, yalnızca sitenin kapatılma hızından hareketle çıkarılmamalı, ölçülmelidir.

04 Tekrarlanabilir bir senaryo olarak dolandırıcılık ve kimlik avı operasyonunun ekonomisi

Ekonomik açıdan önemli olan varlık, genellikle kayıt ücreti değil, bir alan adı etrafında biriken trafik, yaratıcı içerik, altyapı ve güvendir. Bu sezgi makul görünmektedir; bunun boyutu ise dolandırıcılık ve kimlik avı operasyonlarına göre değişiklik gösterir. Bu nedenle, aşağıdaki hesaplayıcı, varsayımsal bir sonucu gözlemlenen ortalama olarak sunmak yerine her bir girdi değerini ayrı ayrı göstermektedir.

MODEL TANIMI

```
visits(T)   = daily_traffic × T / 24
victims(T)  = visits(T) × conversion_rate
proceeds(T) = victims(T) × average_loss × (1 - cashout_attrition)
profit(T)   = proceeds(T) - campaign_budget
```

Senaryo hesaplayıcı

Herhangi bir varsayımı değiştirin. Değerler sadece örnek niteliğindedir ve tipik bir kimlik avı pazarının tahminlerini yansıtmamaktadır.

AÇIKLAYICI MODEL

Dolandırıcılık ve kimlik avı operasyonu bütçesi (USD)

5000

Günlük ziyaretler

2000

Mağdura dönüşüm oranı (%)

1.5

Mağdur başına ortalama kayıp (USD)

2400

Nakit çıkış kayıp oranı (%)

25

Eyleme kadar geçen süre (saat)

24

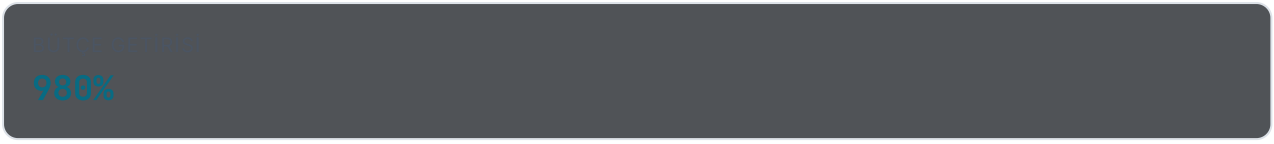
2,000

30

$54,000

$49,000

2.2 h



Model bir beklenen değer ifade ettiği için tahmini mağdur sayısı ondalıklı olabilir. Trafik azalması, tespit sonrası davranış değişikliği, kampanyanın başka altyapıya taşınması, yinelenen mağdurlar ve belirsizlik dağılımları hesaba katılmaz.

▶ Model kaynak tablosunu görüntüle

05 Hassaslık uydurmadan önlenebilir zararın ölçülmesi

“Tespitten sonra meydana gelen kayıp”, ancak tespit, iletim ve zarar kavramları tutarlı bir şekilde tanımlandığında yararlı bir sonuç haline gelebilir. Kara liste zaman damgası, kayıt kuruluşunun eyleme geçirilebilir kanıt aldığının kanıtı değildir. Bir cüzdan işlemi, otomatik olarak tek bir alan adıyla ilişkilendirilemez. Bir alan adının erişilemez hale gelmesi, bu değişikliğe hangi aktörün neden olduğunu belirlemez.

Asgari etkinlik şeması

ETKİNLİK	GEREKLİ ZAMAN DAMGASI	ASGARİ KANIT
İlk gözlem	`t_obs`	Sensör, istek/yanıt hash değeri, yakalama yöntemi, saat kaynağı.
Teknik doğrulama	`t_valid`	Tekrarlanabilir gösterge, gözden geçirenin kimliği, tehdit kategorisi ve güven derecesi.
Bildirim tebliğ edildi	`t_bildirim`	Onaylı teslimat makbuzu ve kanıt dosyası sürümü.
Sorumlu taraf şunu kabul eder:	`t_ack`	Vaka Kimliği ve hedef rol: ana bilgisayar, kayıt kuruluşu, kayıt merkezi, platform veya yetkili kurum.
Azalma gözlemlendi	`t_mitigate`	DNSi, HTTP, ödeme veya platform durumu; çeşitli bakış açılarından ölçülür.
itiraz / geri yükleme	`t_restore`	Karar dayanağı, değişen deliller ve geri kazanım doğrulaması.
Zarar olayı	`t_harm`	Kişisel bilgileri gizlenmiş mağdur raporu, atfedilebilir işlem veya başka bir belgelenmiş gösterge.

ÖNERİLEN SONUÇ ÖLÇÜTÜ

$$\text{Post-notice harm share} = \frac{\text{attributable harm with } t_{harm} > t_{notice}}{\text{all attributable harm in the observation window}}$$

Pay ve payda aynı atıf kuralını kullanmalıdır. Sonuçlarda kohort, güven aralığı, sağdan sansürleme, eksik kaynaklar, mükerrer mağdurların ele alınışı ve gözlem penceresine duyarlılık bildirilmelidir. “Önlenebilir” etiketi, nedensel bir tasarım veya en azından eşleştirilmiş bir karşılaştırma için ayrılmalıdır — bildirimden sonraki her olay için değil.

ORTALAMA TAHMİN · %60-85

Bu makale, modellenen olay sınıfında tespit ve bildirimden sonra meydana gelen atfedilebilir zararın payı için %60–85’i merkezi tahmin olarak kabul etmektedir. Bu, açıklanan varsayımlardan ve vaka gözlemlerinden türetilmiş bir senaryo tahminidir; dünya çapındaki tüm dolandırıcılık vakaları için ölçülmüş bir istatistik değildir. Olay düzeyinde bir veri kümesi, gözlemleri, doğrulanmış kanıtları, bildirim, hafifletme ve zararın meydana geldiği zaman damgalarını birbiriyle uyumlu hale getirene kadar, bu tahmin duyarlılık analizi için kullanılmalıdır. Bu veri kümesinin yayınlanması, tezin kanıtlanabilirlik testidir; tezin silinmesi için bir neden değildir.

06 Kurumsal şema: Yetenekler dağınık bir şekilde yer almaktadır

Hiçbir aktör olayı bütünüyle göremez veya kontrol edemez. Kayıt memuru, kayıt sahibi ile kayıt kuruluşu arasındaki ilişkiyi bilir; kayıt kuruluşu, kendi belirlediği alan adı durumunu kontrol eder; barındırma hizmeti sağlayıcısı ve CDN içerik dağıtımını kontrol eder; tarayıcılar ve güvenlik sağlayıcıları uyarıları kontrol eder; ödeme ve cüzdan sağlayıcıları transferleri durdurabilir; yetkili makamlar ise verilerin muhafaza edilmesini veya el konulmasını zorunlu kılabilir. ICANN, gTLD ekosisteminde sözleşmeleri hazırlar ve uygulatır, ancak evrensel bir EPP kontrol düzlemi işletmez.

01 · SİNYAL

Araştırmacılar ve sensörler

İçerik, altyapı ve mağdur göstergelerini gözlemleyin; kanıtın kaynağını ve gözetim zincirini koruyun.

02 · HİZMET

Sunucu / CDN / platform

İçeriği kaldırabilir veya erişimi hızla sonlandırabilir; bu işlem genellikle alan adını değiştirmeden gerçekleştirilir.

03 · SPONSOR

Kayıt kuruluşu

Kötü niyetli teknik kullanımları inceler, kayıt sahibiyle iletişime geçer ve istemci tarafındaki durumu ayarlayabilir.

04 · BÖLGE

Kayıt operatörü

EPP'ın kayıt defterinde tanımlanan durumunu ve TLD alan adının yetki devrini kontrol eder.

05 · SÖZLEŞME

ICANN Uyum

Sözleşme taraflarının kurallara uyumunu inceler; her dolandırıcılık vakasını karara bağlamaz.

06 · HUKUK

CERT / Yetkili Makamlar

Müdahaleyi koordine etmek ve ilgili yargı bölgesine özgü yasal yetkileri kullanmak.

Yetkinin dağıtılması, sorumluluğun ortadan kalkması anlamına gelmez. Bir sponsor kayıt kuruluşu, kötüye kullanım vakalarının ele alınmasını bir bayiye devretmekle sözleşmesel yükümlülüklerinden kurtulmaz; kayıt merkezi, sunucu tarafında ayarlanan EPP durumunu kontrol eder; ICANN ise sözleşmeye uygunluğu sağlar. Denetim izi, yalnızca kimin harekete geçtiğini değil, aynı zamanda eyleme geçirilebilir kanıtları kimin aldığını, vakayı kimin başka bir birime yönlendirdiğini, kimin yanıt vermediğini veya kimin kendisine verilen görevi yerine getirmediğini de kaydetmelidir. Yasal yetki, bir önlemi uygulama yetkisine sahip olan kişide kalır; hesap verebilirlik, belgelenmiş görev ihlallerini de kapsar.

Finansman yoğunlaşması ve test edilebilir bir teşvik çatışması hipotezi

$165.1M

27. Mali Yıl "ICANN" Operasyonları için ayrılan fon

27 mali yılı temel senaryo bütçesi kabul edildi. [1]

≈98.1%

kayıt defteri ve kayıt memuru ücret gelirleri

165,1 milyon dolarlık finansman planının yaklaşık 162,0 milyon doları. [1]

70.7%

sadece işlem bazlı ücretler

$116.8M tied to billable domain transactions. [1]

Dolayısıyla, finansman yapısı, ICANN adresinde yer alan sözleşmelerin uygulanmasını sağlayan sözleşmeli tarafların ödemelerine büyük ölçüde yoğunlaşmaktadır ve bu payın önemli bir kısmı, faturalandırılabilir kayıt işlemlerine bağlı olarak değişmektedir. Bu durum, yapısal bir bağımlılık ve meşru bir teşvik çatışması sorununu ortaya çıkarmaktadır. Bu, *değil*, tek başına, kasıtlı olarak yetersiz uygulama ya da tam anlamıyla gerçekleşmiş bir "düzenleyici ele geçirme" olduğunu kanıtlamaz. Ele geçirme hipotezi, vaka düzeyindeki müdahale süreleri, uygulama sonuçları, yaptırımlar, tekrarlanan suistimaller ve fon sağlanan paydaşların politika ve uygulama kararlarındaki rolü ışığında sınanmalıdır.

07 2024 sözleşme temel seviyesi — ve bu seviyenin belirtmediği hususlar

Kayıt Kuruluşu Akreditasyon Anlaşması ve Temel Kayıt Anlaşması'nda Nisan 2024'te yapılan küresel değişiklikler, DNS Abuse faaliyetlerini azaltmaya yönelik açık yükümlülükler getirdi. Kayıt kuruluşları, sponsor oldukları bir alan adının DNS Abuse amacıyla kullanıldığına ilişkin eyleme geçirilebilir kanıta sahip olduklarında derhal harekete geçmelidir. Kayıt operatörleri, eyleme geçirilebilir kanıta dayanarak kayıtlı bir alan adının DNS Abuse amacıyla kullanıldığını makul biçimde belirlediklerinde derhal harekete geçmelidir. Her iki durumda da uygun önlem bağlama, ciddiyete ve dolaylı zarara bağlıdır. [2] [3]

Sık sık birbiriyle karıştırılan üç zaman çizgisi

ZAMAN ÇİZELGESİ	HANGİ DURUMLAR İÇİN GEÇERLİDİR?	NE ANLAMA GELMEZ
24 saat	RAA §3.18.3 uyarınca, kolluk kuvvetleri, tüketiciyi koruma, yarı kamusal veya benzeri makamlarca özel irtibat noktasına sunulan, Yasa Dışı Faaliyete ilişkin sağlam temelli bildirimlerin incelenmesi.	Bu, herkes için geçerli olan 24 saatlik bir askıya alma süresi değildir.
"Derhal"	İlgili eyleme geçirilebilir kanıt eşiği aşıldıktan sonra uygun hafifletici önlemlerin alınması.	Bu, sabit bir saat sayısı değildir ve her durumda aynı çözümün uygulanmasını gerektirmez.
21 gün	Resmi bir sözleşmeye dayalı İhlal Bildirimi'nin ardından bir düzeltme süresi olarak ortaya çıkabilir.	Bu, bildirilen her kötü amaçlı alan adına verilen sıradan bir kullanım süresi değildir.

Bu esnekliğin bazı avantajları vardır: Güvenliği ihlal edilmiş bir üniversite alan adı, yeni kaydedilmiş, tek amaçlı bir oltalama alan adı gibi ele alınmamalıdır. Hesap verebilirlik sorununa gelince, yayınlanmış zaman damgaları, vaka kategorileri ve sonuç kodları olmadan "hızlı" ve "uygun" kavramlarını karşılaştırmak zordur. Aşağıdaki öneri, tek bir son tarihin her vakaya uymuş gibi bir izlenim yaratmadan, ölçüm ve inceleme süreçlerini eklemektedir.

08 Sınır sorunu: Kimlik avı konusu ele alınmıştır; ancak bazı finansal dolandırıcılık vakaları ele alınmamış olabilir

Kimlik avı, DNS Abuse sözleşme tanımına açıkça dâhildir. Daha güç sınır, tanımlanabilir bir üçüncü tarafı taklit etmek yerine özgün bir ad altında kullanıcıları aldatan sitelerdir: bazı sahte yatırım platformları, dolandırıcı mağazalar, para kurtarma dolandırıcılıkları ve cüzdan imza düzenekleri. Olgulara göre bunlar sözleşmesel DNS Abuse yerine web sitesi içeriği düzeyinde ihlal, tüketici dolandırıcılığı veya başka bir hukuki kategori olarak değerlendirilebilir.

ÖNERİLEN ARAŞTIRMA ETİKETİ

Doğrulanmış Mali Zarar Amaçlı Kötüye Kullanım (VFHA): marka taklidinden bağımsız olarak aldatma yoluyla para, ödeme bilgisi, özel anahtar veya tohum ifadesi elde etmek için alan adının belgelenmiş kullanımıdır. VFHA, ICANN'ın mevcut terminolojisi değildir ve tek başına sözleşmesel yetki yaratmaz.

Politika istişaresi, VFHA gibi dar ve kanıta dayalı bir kategorinin gelecekteki sözleşmelerde, sektörler arası sevk çerçevesinde veya ulusal hukukta yer alıp almamasını değerlendirebilir. Genişletme; kesin zarar testi, güvenilir kanıt, orantılı çözüm, yargı alanı incelemesi ve itiraz gerektirmelidir. Belirsiz "dolandırıcılık" etiketleri yeterli değildir.

09 Ayda 100–150 dolarlık izleme iddiasının neyi kanıtlaması gerektiği — ve neyi kanıtlayamayacağı

Bir standart sunucu, katılımcı gTLD bölge dosyalarının erişilebilir anlık görüntülerini indirebilir ve değişiklikleri yerel olarak hesaplayabilir, seçilen Sertifika Şeffaflığı olaylarını ve açık beslemeleri alabilir, dizeleri normalleştirebilir, karma değerleri hesaplayabilir ve adayları öncelik sırasına koyabilir. Bu, "İnternet'in tam izlenmesi" değil, kullanışlı ve test edilebilir bir mühendislik karşılaştırma ölçütüdür. Verisign, 2026 yılının ikinci çeyreğinde tüm TLD'lerde toplam 401,6 milyon kayıt olduğunu bildirmiştir; CZDS, tüm TLD'leri değil, katılımcı gTLD bölge dosyalarını kapsar ve CT, her aktif veya zararlı etki alanını değil, kamuya açık olarak kaydedilmiş sertifikaları veya ön sertifikaları kaydeder. [8] [9] [17]

KAPASİTE	STANDART PROTOTİP	ÜRETİM ÖLÇEĞİNDE KAMU YARARI HİZMETİ
Bölge/CT/akış alımı	Tanımlı kaynak kümesi için uygulanabilir	Yedekli toplayıcılar, kaynak sözleşmeleri, boşluk izleme
Dize/özet ön elemesi	Uygulanabilir	Karşılaştırma, sapma tespiti, yanlış negatif çalışmaları
Tarayıcı işleme	Küçük örneklem alt kümesi	Yalıtılmış filo, bölgesel gözlem noktaları, kötü amaçlı yazılım sınırlaması
Hukuki belirleme	Dâhil değil	Nitelikli inceleyiciler, yargı alanı ve yetki eşlemesi
Yüksek erişilebilirlik / kanıt saklama	Genellikle yok	HSM destekli imzalar, denetim günlükleri, yedekler ve olay müdahalesi
İtiraz ve geri yükleme	Dâhil değil	7/24 operasyon, bağımsız eskalasyon ve hizmet hedefleri

ŞEKİL 2 · BÜYÜKLÜK SIRASI BAĞLAMI LOGARİTMİK GENİŞLİK · EŞDEĞER OLMAYAN MALİYETLER

Logaritmik genişlikler, küçük değerlerin de görünür kalmasını sağlar. İlk üç rakam, yayınlanmış bir karşılaştırma ölçütü gerektiren ve satıcı teklifleri olmayan, açıklanmış mühendislik veya program varsayımlarıdır. ICANN Operasyon finansmanı, doğrulanmış kurumsal ölçekte bir rakamdır. Bunlar kasıtlı olarak eşdeğer olmayan bütçelerdir: karşılaştırma, temel toplama ve ön eleme işlemlerinin doğası gereği aşırı maliyetli olup olmadığını test eder; eksiksiz bir uygulama programının aylık 100 dolara mal olup olmadığını değil.

10 Önerilen Doğrulanmış DNS Abuse Müdahale Çerçevesi

Önerilen çerçeve, otomatik bir küresel acil durdurma mekanizması değil, bir referans mimaridir. Bu çerçeve, vaka dosyası, karar kaydı ve zaman damgalarını standart hale getirirken, yetkili operatörün en az aksaklığa yol açan etkili önlemi seçmesine imkân tanır.

01 · ALIM

Edinme ve koruma

Raporları ve gözlemleri toplama; ham verileri işleme; saatleri senkronize etme.

02 · kanıtın kökeni ve işlem geçmişi

Kanıtları normalleştirin

Kaynak, yöntem, işleme geçmişi ve kaynak bağımlılıklarını kaydedin.

03 · DOĞRULAMA

Doğrulamak

Zararlı davranışı yeniden canlandırın ve bağımsız kanıtları ayırt edin.

04 · DEĞERLENDİRME

Risk ve teminat

Kötü niyetli kayıtları, güvenliği ihlal edilmiş hizmetleri, paylaşımlı barındırma hizmetlerini ve kritiklik düzeylerini sınıflandırın.

05 · YANITLA

Bildir ve etkisini azalt

Sorumlu kişiyi, hedef süreyi ve en az aksaklığa yol açacak etkili çözümü belirleyin.

06 · İNCELEME

Denetim ve itiraz

Sonuç meta verilerini yayınlayın, etkiyi ölçün ve hızlı düzeltme sürecini destekleyin.

Kanıt düzeyleri

E1 **Doğrulanmamış sinyal**

Tek bir ihbar, kelime bazında eşleşme veya itibar iddiası. Gözlem için uygun olmakla birlikte, tek başına askıya alma kararı için asla yeterli değildir.

E2 **Tekrarlanan davranış**

Kimlik bilgilerinin çalınmasını, kötü amaçlı yazılımın yayılmasını veya aldatıcı bir işlem yolunu gösteren, zaman damgası içeren kayıt.

E3 **Bağımsız doğrulama**

En az iki gerçekten bağımsız kaynak ya da tekrarlanabilir bir teknik kanıt artı sahiplik/bağlam kontrolleri.

E4 **Onaylı teyit**

Yetkili kurum, etkilenen hizmet, marka sahibi veya doğrulanmış mağdur kanıtları; gizlilik kurallarına uygun bir kanıt izleme zinciri ile.

BAĞIMSIZLIK KURALI

Aynı üst kaynak kara listeyi kopyalayan üç akış üç değil, tek kaynaktır. Kanıtın kaynağı ve gözetim zinciri grafiği ortak kökeni, eşitlemeyi ve satıcının yeniden yayımlamasını göstermelidir.

11 Asgari kanıt paketi ve birlikte çalışabilir API

API, doğrulanabilir bir vaka oluşturmalı ve denetlenebilir bir müdahale süresini başlatmalıdır; bir raporlayıcı, doğrudan bir durdurma emri verememelidir. Bir E3/E4 vakası, tek amaçlı kötü niyetli bir kayıtla ilgiliyse ve gerekçeli bir karar veya etkili bir önlem alınmadan süresi dolarsa, sistem bunu otomatik olarak kayıt operatörüne veya sözleşmeye dayalı ya da yasal yetkiye sahip başka bir aktöre iletir. A `serverHold` Komut, yalnızca yetkili bir aktör tarafından verilebilir. Süresinin dolması durumunda otomatik yetki yükseltme ve kayıt defteri yetkisi, mevcut yetkiyle ilgili iddialar değil, önerilen politika değişiklikleridir. Her durum geçişi imzalanır ve denetim günlüğüne eklenir.

POST /V1/CASES · ÖRNEK

```
{
  "indicator": {"type": "domain", "value": "example.invalid"},
  "alleged_category": "credential_phishing",
  "observed_at": "2026-08-02T06:14:22Z",
  "evidence": [
    {
      "type": "http_capture",
      "sha256": "a3f1c9…",
      "collection_method": "isolated_browser_v2",
      "source_id": "reporter:ed25519:7c2a…"
    }
  ],
  "provenance_graph": "ipfs-or-object-store:sha256:91bd…",
  "collateral_context": {
    "registered_domain_scope": true,
    "shared_service": false,
    "mail_observed": true,
    "suspected_compromise": false
  },
  "requested_action": "review",
  "reporter_signature": "ed25519:…"
}
```

Başarılı bir yanıt, vaka kimliği, alıcı kurum, kanıt düzeyi, eksiklik hataları, hedef inceleme süresi ve kamuya açık şeffaflık URL'sini içerir. Yetkili bir kurum, yetki ve dolaylı etkileri değerlendirmeden önce belirli bir çözüm vaat etmemelidir.

12 Önerilen yanıt hedefleri, genel kaldırma süreleri değil

Hizmet düzeyi hedefleri birbirinden ayrılmalıdır *teşekkür*, *triyaj*, *karar* ve *etkili azaltma*. Bu sayede, süspansiyonun her zaman doğru sonuç olduğu varsayılmadan performans ölçülebilir hale gelir.

VAKA PROFİLİ	ONAYLAYIN	TRİYAJ HEDEFİ	KARAR HEDEFİ	TİPİK YANIT SEÇENEKLERİ
Tek amaçlı kötü niyetli bir kayıt sırasında E3/E4 ödeme kimlik bilgilerinin veya tohum ifadesinin çalınması	15 dakika	1 saat	4 saat	İçerik bloğu; yetkili olduğu durumlarda kayıt kuruluşu/kayıt defteri tarafından uygulanan askıya alma; tarayıcı ve ödeme uyarıları.
E3 markasını kullanan kimlik avı veya kötü amaçlı yazılım dağıtımı	30 dakika	2 saat	6 saat	Kontrol noktasına göre sunucu/CDN'ın kaldırılması, etki alanının etkisiz hale getirilmesi, sinkhole veya uyarı.
Güvenliği ihlal edilmiş meşru alan adı veya paylaşımlı SaaS kiracısı	1 saat	4 saat	12 saat	Yol/hesap yalıtımı ve hesap sahibinin geri kazanımı; mümkün olduğunca kayıtlı alan adlarının askıya alınmasından kaçınılmalıdır.
Tartışmalı sınıflandırmaya dayalı mali dolandırıcılık	4 saat	12 saat	24 saat	Koruma, platform/ödeme müdahalesi, yetkili makama sevk ve gerekçeli karar.
E1 sinyali veya eksik rapor	Otomobil	24 saat	Doğrulanana kadar yok	İzleyin, bilgileri zenginleştirin ve kanıt talep edin.

Bunlar pilot hedeflerdir. Doğru değerler, gözlemlenen tehdit ömürleri, personel sayısı, hata maliyeti ve yasal kısıtlamalar dikkate alınarak belirlenmeli ve tek bir ortalama yerine ulaşım dağılımları ile birlikte yayınlanmalıdır.

13 Güvenlik, adil yargılama, mahremiyet ve arıza durumları

Güvenlik önlemleri alınmadan hızlı müdahale, hatalı verilerin sansüre, ticari sabotaja veya altyapı kesintilerine dönüşmesine yol açabilir. Bu nedenle, meşru bir mimari, yanlış pozitif sonuçları ve dolaylı zararları birinci dereceden güvenlik başarısızlıkları olarak değerlendirir.

ARIZA TÜRÜ	GEREKLİ KONTROL	DENETLENEBİLİR ÖNLEM
Bir rakibe yönelik kötü niyetli ihbar	Muhabirlerin kimlik doğrulaması, kaynakların güvenilirliği, bağımsız yeniden üretim ve kötü niyetli teknik kullanımlara yönelik yaptırımlar	Raporlayıcıya göre reddedilen rapor oranı; teyit edilmiş manipülasyon vakaları
Konsensüs kisvesi altında sunulan besleme döngüselliği	Kanıt kaynağı grafiği ve üst kaynak tekilleştirmesi	Soy düzeltmesi öncesi ve sonrası bağımsız kaynak sayımı
Güvenliği ihlal edilmiş meşru alan adları toplu olarak askıya alındı	Kayıt niyeti sınıflandırması ve yol düzeyinde risk azaltma tercihi	Güvenliği ihlal edilmiş alan adlarının payı; etkilenen meşru hizmetler
Mağdur verileri veya istismar ayrıntıları kamuoyuna sızdırıldı	Aşamalı bilgi paylaşımı, bilgilerin sansürlenmesi, mühürlenmiş deliller ve saklama süreleri	Gizlilik ihlalleri; bilgilerin gizlendirilmesine ilişkin inceleme sonuçları
Haksız eylem devam ediyor	7/24 itiraz üzerinden başvuru kabulü, bağımsız denetçi ve doğrulanmış geri yükleme süreci	Ortalama ve 95. persentil geri dönüş süresi
Kayıt defteri kilitlenmesi, e-posta/alt etki alanı kesintisine neden oluyor	Teminat envanteri, tedbirlerin orantılılığı ve işlem sonrası izleme	Eylem başına kesintiye uğrayan hizmetler; geri alma oranı

Asgari adil yargılama güvenceleri

1. Her kısıtlayıcı önlem için gerekçe kodu, kanıt düzeyi ve karar verici kaydedilir.
2. Kayıt sahibi, gizlilik kurallarına uygun bir gerekçe bildirisi alabilir ve buna karşı deliller sunabilir.
3. Acil durumlar itiraz adresinde, ilk kararı veren kişi dışında bir kişi tarafından incelenir.
4. Geri alma işlemi, orijinal eylemle aynı işaretli kanal üzerinden yayılır.
5. Toplu hata ve geri yükleme istatistikleri herkese açıktır; hassas deliller ise erişim kısıtlamasına tabidir.

14 “Toksisite puanı”ndan hesap verebilir bir Müdahale Kalitesi Endeksi’ne

Bir kayıt kuruluşunun kamuya açık puanı hesap verebilirliği artırabilir; ancak, portföy büyüklüğü, besleme kapsamı, müşteri dağılımı ve alan adlarının kötü niyetle kaydedilip kaydedilmediği ya da daha sonra ele geçirilip geçirilmediği gibi faktörler, yüzeysel sıralamaları çarpıtabilir. Bir puan, hiçbir şekilde bir kayıt kuruluşunun tüm müşterilerinin toplu olarak engellenmesini haklı göstermemelidir.

ÖNERİLEN KALİTE VEKTÖRÜ

```
RQI = report as a vector, not a single opaque rank:

  coverage-adjusted validated-abuse rate
  median / p90 acknowledge, triage and decision times
  mitigation effectiveness and recurrence
  false-positive and reversal rates
  median / p95 appeal-resolution time
  evidence completeness and transparency rate

Always publish N, observation window, confidence intervals,
feed coverage and malicious-registration / compromise split.
```

Yönetişim amacıyla bir bileşik model gerekliyse, değerlendirme öncesinde ağırlıklar belirlenmeli, duyarlılık testleri yapılmalı ve test dışı bırakılan vakalar üzerinde geriye dönük testler gerçekleştirilmelidir. Sonuçlar, TLD, kayıt kuruluşunun büyüklüğü, tehdit sınıfı ve kanıt kaynağına göre sınıflandırılmalıdır. Ortaya çıkan sonuç, bir hesap verebilirlik göstergesidir — otomatik bir alan adı kararı değildir.

15 Kademeli erişimli Kamusal DNS Abuse Şeffaflık Veritabanı

Şeffaflık kayıt sistemi, bir bildirimin var olup olmadığı, ne zaman iletildiği ve bunun ardından hangi önlemlerin alındığına dair anlaşmazlıkları ortadan kaldırabilir. Ancak her türlü kanıtın yayınlanması, mağdurları, kişisel verileri, soruşturma yöntemlerini ve aktif istismar yollarını açığa çıkarabilir. Çözüm, kademeli erişimdir.

P

Kamuya açık kayıt

Vaka Kimliği, gösterge, genel kategori, önemli zaman damgaları, kanıt seviyesi, aktör rolleri, sonuç kodu, itiraz durumu ve mühürlenmiş kanıtların hash değerleri.

C

Sözleşme tarafı görünümü

Tekrarlanabilir teknik kanıtlar, iletişim kanalı, ilgili bağlam ve koruma talimatları.

R

Sınırlı yetki görünümü

Mağdur verileri, finansal atıf bilgileri, aktif soruşturma materyalleri ve sansürsüz delil zinciri.

Her güncelleme yalnızca ekleme amaçlıdır, zaman damgası taşır ve imzalanmıştır. Düzeltmeler geçmişi silmez; yerine geçen yeni bir kayıt ekler. Halka açık arama işlemleri, saklama kurallarına uymalı, mağdurların toplu olarak tespit edilmesini önlemeli ve hatalı kişisel veriler için düzeltme imkânı sunmalıdır.

16 Önceden kayıtlı bir değerlendirme içeren altı aylık bir pilot çalışma

Yararlı bir pilot çalışma, yönetilebilecek kadar küçük ve nedensel zinciri test edebilecek kadar geniş kapsamlı olmalıdır. Önerilen kapsam: üç gönüllü kayıt sorumlusu, iki kayıt operatörü, bir barındırma/CDN ortağı, iki bağımsız araştırma kaynağı ve nitelikli bir itiraz paneli. Çalışma protokolü ve sonuç tanımları, vakalar atanmadan önce kaydedilmelidir.

1. AY

Protokol ve yasal haritalama

Kategorileri, yetki alanlarını, kanıt seviyelerini, gizlilik etki değerlendirmesini ve durdurma koşullarını tanımlayın.

2. AY

Mevcut süreci düzenlemek

Yanıt davranışını değiştirmeden başlangıç zaman damgalarını ve sonuçları ölçün.

3. AY

Kanıt paketini işletin

İmzalı kanıt kaynağını, yinelenen kayıtların kaldırılmasını ve dolaylı etki sınıflandırmasını uygulayın.

4. AY

Test yanıt hedefleri

Uygun vakaları rastgele gruplara ayırın veya kademeli uygulama yöntemini kullanın; hataları günlük olarak izleyin.

5. AY

itiraz'i çalıştırma ve hatalar

Kurtarma tatbikatları düzenleyin, “kırmızı takım” yöntemiyle kötü niyetli saldırı senaryoları oluşturun ve erişim kontrollerini denetleyin.

6. AY

Bağımsız değerlendirme

Etki büyüklüklerini, güven aralıklarını, eksik verileri, istenmeyen olayları, maliyetleri ve tekrarlanabilirlik materyallerini yayınlayın.

Pilot çalışmanın birincil sonuçları

- Doğrulanmış bulgudan etkili önleme tedbirlerinin alınmasına kadar geçen sürenin medyan değeri ve 90. persentili.
- Bildirim sonrası atfedilebilir zarardaki fark ya da önceden belirlenmiş bir mağdur-maruz kalma göstergesi.
- Yanlış pozitif oranı, hatalı eylemin ciddiyeti ve medyan düzeltme süresi.
- Aynı alan adı sahibi, altyapı kümesi ve dolandırıcılık/kimlik avı operasyonu düzeyinde tekrar.
- Doğrulanmış her vaka ve etkili her önleme tedbiri başına doğrudan işletme maliyeti.

KARAR KURALI

Yalnızca pilot uygulama, yanlış pozitifler, gizlilik ihlalleri, itiraz gecikmesi veya dolaylı hizmet kesintileri için önceden belirlenmiş sınırları aşmadan, önemli ölçüde daha hızlı bir etkin azaltma sağladığını gösterirse ölçeklendirme yapılmalıdır.

17 Sonuçlar ve test edilebilir öneriler

DNS Abuse müdahalesi ne yalnızca teknik bir filtredir ne de tek bir kurumun kendi başına çözebileceği bir sorundur. 2024 sözleşme değişiklikleri anlamlı azaltım yükümlülükleri getirmiş, ancak kanıt, zamanlama ve telafi konusunda önemli takdir yetkisi bırakmıştır. Bu takdir yetkisi orantılılık için gereklidir; karşılaştırılabilir kayıtlar olmadığında performans değerlendirmesini de güçleştirir.

1. **Kanıt paketini standartlaştırın.** Bildirim yapanlar, kayıt kuruluşları, kayıt operatörleri ve altyapı sağlayıcıları arasında ortak kanıt kaynağı, zaman damgası ve sonuç alanları kullanın.
2. **Aşamaları ayrı ayrı ölçün.** Tehdit sınıfı ve kanıt kademesine göre bildirimin alındığının teyidi, önceliklendirme, karar, azaltım ve itiraz sürelerini yayımlayın.
3. **Kötü niyetli kayıt işlemlerini, sistemin ele geçirilmesi durumlarından ayırt edin.** Güvenliği ihlal edilmiş meşru hizmetler için yol/hesap düzeltme yöntemini tercih edin ve etki alanı genelindeki önlemleri, bu önlemlerin orantılı olduğu durumlar için saklayın.

4. **Pilot müdahale hedefleri.** Evrensel bir son tarih belirlemek yerine, yüksek güvenilirliğe sahip, tek amaçlı kötü niyetli kayıtlar için saat bazında hedefleri test edin.
5. **Gizlilik kurallarına uygun hesap verebilirlik verilerini yayınlayın.** İmzalanmış geçmiş kayıtları ve sınırlı kanıtları içeren kademeli bir şeffaflık kayıt sistemi kullanın.
6. **Nedensel etkiyi değerlendirin.** Ön kayıtlı bir çalışma mağdur üzerindeki etkileri ve tehdidin başka kanallara kaymasını ölçene kadar, daha hızlı askıya almayı tasarruf edilen parayla eşdeğer görmeyin.

Olumlu sonuç, iddialar sınırlandırıldığında asıl sorunun ortadan kalktığı değildir. Asıl sonuç, temel iddiaların artık test edilebilir hale gelmesidir: Tespit sonrası zararın %60–85 aralığı, açık ve nicel bir hipotezdir; 100–150 dolarlık tutar, tanımlanmış bir sensör ve ön sınıflandırma katmanı için test edilebilir bir mühendislik bütçesi varsayımıdır; saat ölçeğindeki müdahale hedefleri ise yüksek güvenilirliğe sahip, tek amaçlı kötü niyetli kayıtlar için pilot uygulamaya konulabilir. İş yükünü, maliyetleri, zaman damgalarını ve sonuçları yayınlayın, bunları bir referans değerle karşılaştırın ve sapma ile hatayı ölçün. Doğrulama, sözleşme ve politika değişikliklerini haklı çıkaracaktır; reddedilmesi ise hangi varsayımın başarısız olduğunu ortaya çıkaracaktır.

Yayın politikası ve yöntemlere ilişkin açıklama. PhishDestroy bağımsız, ticari amaç gütmeyen bir tehdit istihbaratı projesidir. Bu yayın, bir politika ve mühendislik önerisidir; hukuki tavsiye, bir "ICANN" programı veya hakemli bir makale değildir. "Modeller" olarak belirtilen bütçe aralıkları, planlama varsayımlarıdır. Birincil kaynaklardan alınan iddialara aşağıdaki bağlantılardan ulaşılabilir. Düzeltmeler, sitenin iletişim ve sorumlu bildirim kanalları aracılığıyla iletilebilir.

BİRİNCİ ŞAHIS BAKIŞ AÇISI · HESAP VEREBİLİRLİK, HEM HAREKETE GEÇMEMEYİ HEM DE YETKİ SINIRLARINI AŞMAYI SINIRLAMALIDIR

Yürütme yetkisine ilişkin kişisel sınır

Bir etki alanı engelleme aracına doğrudan erişim talep etmiyorum — ve bunu da istemiyorum. Bu yetki, bağımsız denetim, kamuya açık denetim kayıtları, hızlı itiraz ve geri alınabilirlik gerektirir.

Bu işin bazı kısımlarının emanet edilebileceği pek çok yetkin ve sorumlu şirket olduğuna inanıyorum. Kendi deneyimlerime ve yayınladığım yazılara dayanarak, NameSilo'u bu gruba dahil etmiyorum.

Yasal ABD şirketlerine, çıkar çatışmaları, yeterlilikleri veya davranışları bağımsız bir incelemeye dayanamayacak belirli yüklenicilere hassas suistimal veya güvenlik işlevlerini emanet etmelerini tavsiye etmem. Burada söz konusu olan belgelenmiş eylemlerdir, milliyet değil: Rus kökenli olmak tek başına hiçbir şeyi kanıtlamaz; tıpkı bir Amerikan şirket adresinin de hiçbir şeyi kanıtlamaması gibi.

Adalet ve gerçek anlamda hesap sorulmasını istiyorum Tekrarlanan dolandırıcılık kampanyalarının bir parçası olarak belgelenen alan adlarının tescil edilmesi ve yenilenmesinden gelir elde eden tescil kuruluşları için. Kanıtların, ihmalin ötesinde olası kasıtlı yardım ve yataklık durumuna işaret ettiği durumlarda —ister doğrudan operasyonel katılım olsun, ister tekrarlanan uyarılara rağmen zararlı bir alan adının tescilli ve çevrimiçi kalmasını sağlamakla görevli bilgili bir aracı olarak hareket etmek olsun— bu davranış bağımsız olarak soruşturulmalı ve doğrulanması halinde gerekli yaptırımlar uygulanmalıdır. Şüpheleri kesin bir gerçekmiş gibi sunmuyorum; ancak aracı statüsü, denetimden muafiyet sağlamamalıdır.

İlgili soruşturmayı gözden geçirin ↗

A

Kaynakça ve kaynak notları

[1] **ICANN, Adopted FY27 Budget (2026)** · https://www.icann.org/en/system/files/files/adopted-icann-budget-fy2027-published-2026-en.pdf

165,1 milyon dolarlık FY27 faaliyet finansmanının ve finansman akışlarının bileşiminin kaynağı.

[2] **ICANN, 2024 Global Amendment to the Registrar Accreditation Agreement** · https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-global-amendment-05apr24-en.pdf

Kayıt kuruluşlarının DNS Abuse yükümlülükleri için birincil sözleşme kaynağı.

[3] **ICANN, 2024 Global Amendment to the Base gTLD Registry Agreement** · https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-global-amendment-05-04-2024-en.html

Kayıt operatörlerinin azaltım yükümlülükleri için birincil sözleşme kaynağı.

[4] **ICANN Contractual Compliance, DNS Abuse Obligations Advisory (2024)** · https://www.icann.org/en/contracted-parties/advisories/documents/advisory-compliance-with-dns-abuse-obligations-in-the-registrar-accreditation-agreement-and-the-registry-agreement-05-02-2024-en

Operasyonel yorum, bildirim gereklilikleri ve uygun azaltım örnekleri.

[5] **ICANN, Enforcement of DNS Abuse Mitigation Requirements (2024)** · https://www.icann.org/en/system/files/files/icann-enforcement-of-dns-abuse-mitigation-requirements-08nov24-en.pdf

Altı aylık uygulama raporu; soruşturma ve azaltım sayıları.

[6] **ICANN SSAC, SAC115: Report on an Interoperable Approach to Addressing Abuse Handling (2021)** · https://www.icann.org/en/system/files/files/sac-115-en.pdf

DNS Abuse bildirimlerinin birlikte çalışabilirliği ve kanıt kalitesi hakkında arka plan.

[7] **Hollenbeck, RFC 5731: EPP Domain Name Mapping (2009)** · https://www.rfc-editor.org/rfc/rfc5731.html

EPP etki alanı durum değerlerinin teknik tanımı; sunucu tarafından ayarlanan durum da dahil olmak üzere.

[8] **Laurie et al., RFC 9162: Certificate Transparency Version 2.0 (2021)** · https://www.rfc-editor.org/rfc/rfc9162.html

CT'in bir sensör olarak kullanıma ilişkin resmi protokol özellikleri ve sınırları.

[9] **ICANN, Centralized Zone Data Service** · https://www.icann.org/en/contracted-parties/registry-operators/services/centralized-zone-data-service

gTLD'a katılan bölge dosyaları için kapsam ve erişim modeli.

[10] **FBI Internet Crime Complaint Center, 2025 IC3 Annual Report** · https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Şikayet ve bildirilen kayıp rakamları; bunlara kimlik avı/sahtecilik vakaları da dahildir.

[11] **Bijmans et al., Catching Phishers By Their Bait (USENIX Security, 2021)** · https://www.usenix.org/system/files/sec21-bijmans.pdf

Veri setine özgü kimlik avı altyapısı ölçümleri ve gözlemlenen ömür süreleri.

[12] **Newly Registered Domains and Phishing Lifetimes, Journal of Cybersecurity (2026)** · https://doi.org/10.1093/cybsec/tyag020

Yeni kaydedilen kimlik avı alan adları ve kullanım ömrü dağılımına ilişkin son ampirik bulgular.

[13] **Inferential Analysis of Maliciously Registered Domains — INFERMAL (2024)** · https://www.icann.org/en/system/files/files/inferential-analysis-maliciously-registered-domains-08nov24-en.pdf

ICANN -Kötü niyetli kayıtlar ve ekosistem faktörlerine ilişkin finanse edilmiş analiz; nedensellik iddialarına ilişkin ilgili sınırlamalar.

[14] **Chainalysis, 2026 Crypto Scam Trends** · https://www.chainalysis.com/blog/crypto-scams-2026/

Bir sağlayıcının 2025 yılına ilişkin zincir içi dolandırıcılık girişlerine ilişkin tahmini; alan adı kimlik avı toplamına dahil edilmemiştir.

[15] **APWG, Phishing Activity Trends Report, Q1 2026** · https://docs.apwg.org/reports/apwg_trends_report_q1_2026.pdf

Gözlemlenen kimlik avı saldırıları/URL'ler; bu rakamlar, kayıtlı benzersiz alan adlarının sayısıyla aynı değildir.

[16] **Cybercrime Information Center / Interisle, Phishing Landscape 2025** · https://www.cybercrimeinfocenter.org/phishing-activity-numbers-may-april-2025

Gözlemlenen saldırıları, benzersiz alan adlarını ve kötü niyetle kaydedilmiş alan adlarını birbirinden ayırır.

[17] **Verisign, Domain Name Industry Brief, Q2 2026** · https://blog.verisign.com/domain-names/q2-2026-domain-name-industry-brief-quarterly-report/

Tüm TLD'lerde bildirilen 401,6 milyon kayıt sayısının kaynağı.