BRANDEFENSE COUNTRY REPORT · TÜRKIYE 2026

Brandefense Türkiye Siber Tehdit Görünümü Raporu 2026

Kimlik bilgilerinin kötüye kullanılması, tedarikçi olayları ve bağlantılı bir ekonomide fidye yazılımı iddiaları

Yapay zekâ ile çevrilmiştir

Bu sürüm İngilizce ana metinden yapay zekâ ile çevrilmiştir. Farklılık olması hâlinde İngilizce sürüm esas alınır.

Odin by Brandefense

Araştırma dönemi: paylaşım tarihine göre 1 Ocak–21 Kasım 2026

Sürüm 1.0 · Kamuya Açık Araştırma Sürümü · TLP:CLEAR · 22 Kasım 2026

250
on iki sektörde kuruluş alan adı değerlendirmesi

4.131.687
gözlem döneminde Türkiye etiketli paylaşım

3
ayrı yol: listelemeler, kampanya araştırması ve kanal iddiaları

30
seçilmiş bankacılık ve finans alan adı

İÇİNDEKİLER

İçindekiler

Yapay zekâ ile çevrilmiştir

Bu sürüm İngilizce ana metinden yapay zekâ ile çevrilmiştir. Farklılık olması hâlinde İngilizce sürüm esas alınır.

01	Yönetici özeti	04
	Rapor haritası	08
02	Türkiye'nin dijital ve güvenlik bağlamı	09
03	Ulusal maruziyet: seçilmiş 250 kuruluş alan adı	12
04	Karanlık ağda gördüklerimiz	21
05	Sektörlere göre hedefleme örnekleri	38
06	Haktivizm ve DDoS	44
07	Tehdit aktörleri ve desteklenen ilişkiler	48
08	Dolandırıcılık ekonomisi	58
09	Bankacılık ve finans incelemesi	64
10	Düzenleyici ve ulusal yanıt	68
11	Görünüm	72
12	Eylem planı	75
A	Ek A. Yöntem ve sınırlar	80
B	Ek B. Kanıt kaydı	82
C	Ek C. Kaynaklar	83
D	Ek D. Sözlük	85
E	Ek E. Resmî bildirim kaydı	86
F	Ek F. Ek iddia ve piyasa temaları	92
	Bu rapor hakkında	99

Yönetim kurulu ve CISO	01 05 11 12
SOC ve olay müdahalesi	04 06 07 12
Kimlik ve altyapı	03 05 07 12
Dolandırıcılıkla mücadele ve bankacılık	08 09 12
Hukuk ve satın alma	05 10 12

Bu sürüm hakkında

Yapay zekâ ile çevrilmiştir. Anlam farkı oluşursa İngilizce sürüm esas alınır.

Araştırma ve taslak hazırlığında yapay zekâ kullanılmıştır. İddialar, resmî bildirimler ve analist yorumları rapor boyunca ayrılır. Kapsam ve güven düzeyi Ek A'da açıklanır.

Türkiye'ye ilişkin 2026 bulguları açık bir önceliğe işaret ediyor: kimlik bilgilerinin kötüye kullanımını sınırlamak, tedarikçi olaylarına hazırlanmak ve temel hizmetlerin kurtarılabildiğini göstermek.

66/100 (C)	4.131.687	157	250
Seçilmiş portföyün ulusal Atlas derecesi	Türkiye etiketli paylaşımlar; olay sayısı değil	Fidye yazılımı listeleme iddiası	Seçilmiş kuruluş alan adı

İçindekiler ve okuma yolları

Rapor; güvenlik yöneticilerine, operasyon ekiplerine, kimlik, altyapı ve dolandırıcılıkla mücadele sorumlularına yöneliktir. On iki bölüm, kararlardan kanıtlara ve sorumlusu belirlenmiş eylemlere uzanır.

Bölüm	Soru	İlk okuyucu
1. Yönetici özeti	Bulgular hangi kararları destekliyor?	Yönetim
2. Dijital bağlam	Hangi ulusal özellikler güvenlik planlaması için önemli?	Yönetim
3. Kuruluşların maruz kalma durumu	Bu sürüm seçilmiş kuruluşlar hakkında neyi ölçebiliyor?	Altyapı
4. Karanlık ağ bulguları	Neler teklif ediliyor, neler doğrulanmamış durumda?	Tehdit istihbaratı
5. Sektör örnekleri	İddialar ve resmî açıklamalar öncelikleri nasıl değiştiriyor?	Sektör sorumluları
6. Haktivizm ve DDoS	Duyuru ile gösterilmiş kesinti arasındaki fark nedir?	Operasyon
7. Tehdit aktörleri	Hangi ilişkiler ve atıflar destekleniyor?	Tehdit istihbaratı
8. Dolandırıcılık ekonomisi	Kimlik, hesaplar ve iletişim nasıl birleşiyor?	Dolandırıcılıkla mücadele
9. Bankacılık	Hangi finansal kontroller ortak sorumluluk gerektiriyor?	Finans ve kimlik
10. Düzenleyici yanıt	Hangi yükümlülükler geçerli, hangi metinler taslak?	Hukuk ve uyum
11. Görünüm	Hangi gelişmeler değerlendirmeyi değiştirir?	Yönetim
12. Eylem planı	Kim harekete geçer, tamamlandığını ne gösterir?	Tüm sorumlular

Yönetim yolu: Bölüm 1, 3, 5 ve 10–12. **Operasyon yolu:** Bölüm 4, 6–7 ve 12. **Kimlik ve dolandırıcılıkla mücadele yolu:** Bölüm 3, 8–9 ve 12.

Gözlemlendi, malzemenin veya ölçümün elimizde bulunduğu anlamına gelir. **İddia edildi**, paylaşımın veya listelemenin bir şey öne sürdüğünü belirtir. **Resmen bildirildi**, veri sorumlusunun veya yetkili makamın belirtilen kapsamda açıklama yaptığını gösterir.

Analist yorumu, kanıtı bir karara bağlar. Erişim, atıf, etkilenen kişiler veya kayıplar hakkında eksik kanıtın yerini doldurmaz.

BÖLÜM 01

Yönetici özeti

01

BU BÖLÜMÜN YANITLADIĞI SORU

Türkiye bulguları hangi güvenlik kararlarını destekliyor?

4

sorumlusu ve tamamlanma kanıtı belirlenmiş karar

Yöneticiler için dört karar 06

Yılın rakamları 06

BÖLÜM 01

Yönetici özeti

KISACA

Fidye yazılımı listelemeleri, kimlik verisi teklifleri ve resmî tedarikçi bildirimleri farklı yanıtlar gerektiriyor. Ransompedia, bu dönemde Türkiye için 157 listeleme kaydediyor; 2025 yılının tamamındaki sayı 53. Resmî bildirimler fidye yazılımını, önceden ele geçirilmiş parolayla e-posta hesabına erişimi ve tedarikçi olaylarını anlatıyor. Karanlık ağ teklifleri eski verileri de yeniden dolaşıma sokuyor. Seçilmiş portföyün ulusal Atlas derecesi 66/100 (C). Kimlik doğrulamasına, tedarikçi bildirimine, bağımsız kurtarmaya ve kanıta dayalı iletişime öncelik verin.

Bu sürüm, saklanan Brandefense Blackhole paylaşımlarını, Ransompedia listelemelerini, pasif gözlemleri ve kaynağından doğrulanan kamu haberlerini birleştirir. Bu gruplar ayrı tutulur. Paylaşım olay değildir; listeleme doğrulama değildir; kuruluş örneklemi ulusal yaygınlık tahmini değildir [S1][S2][S3][S4].

1. Fidye yazılımı listelemeleri iş sürekliliği yatırımını destekliyor. Türkiye için belirtilen 2026 döneminde 157 listeleme var. Aynı görünümde Polonya için 56, İsrail için 46, Yunanistan ve Romanya için ayrı ayrı 20 listeleme bulunuyor. Bunlar görünürlük karşılaştırmalarıdır; ülke riski sıralaması değildir. Türkiye listelemelerinin 17'si Qilin, 15'i Nightspire, 14'ü Thegentlemen etiketi taşıyor [S3].

Karşılaştırma ülkeleri yalnızca bağlam sağlamak için örnek olarak seçilmiştir, bir sıralama ya da siyasi değerlendirme içermez.

2. Geçerli hesapların kötüye kullanımına resmî bir örnek var. Bir belediyenin bildirimi, e-posta hesaplarına erişimi sunucu açığı yerine önceden ele geçirilmiş bir parolaya bağlıyor. Bildirim; posta kutusu içeriğinin dışarı aktarılmasını, ileti silme kurallarını, spam gönderimini ve değiştirilen imzaları anlatıyor. Bu, kimlik ve posta kutusu incelemesini destekliyor; parolanın ilk nasıl alındığını açıklamıyor [S15].

3. Tedarikçi erişimi teknik olayları müşteri bildirimine bağlıyor. Bir perakendecinin bildirimi, veri işleyendeki olay sonrasında etkilenmiş olabilecek kişi sayısını 323.052 olarak tahmin ediyor. Başka bir bildirimde 592 nihai müşteri ve 4 yönetim paneli kullanıcısı yer alıyor. Bir yatırım hizmetleri bildirimi, yabancı veri işleyene yönelik oltalamayı anlatıyor; veri aktarımı doğrulanmış değil. Bunlar ayrı bildirimlerdir [S16][S17][S20].

4. Büyük ilan rakamları yeni etkilenen kişileri ölçmüyor. Seçilmiş teklifler arasında 2025 kaynaklı olduğu söylenen hastane çalışanı dosyası, 2023 etiketli taşınmaz verisi ve Kasım tarihli kripto varlık işletmesi teklifi var. Sonuncusu kimlikleri, tabloları ve işlem satırlarını karıştırıyor. İlan edilen birimler toplanamaz; hiçbiri doğrulanmış müşteri kaybı tutarı vermiyor [S1].

5. Resmî fidye yazılımı açıklaması veri aktarımının sınırını koruyor. KVKK, Yıldız Teknik Üniversitesinin sanallaştırma altyapısını ve sunucularını etkileyen fidye yazılımını bildirdi. Bildirimde yaklaşık 140.000 öğrenci ve 4.500 personelin etkilenmiş olabileceği belirtildi. Üniversitenin sonraki açıklaması, sistem dışına veri aktarıldığına ilişkin bulgu bulunmadığını söyledi. Her iki açıklama da önemlidir [S12][S13][S14].

6. Maruziyet doğrulaması farklı sorumlular gerektirir. Seçilmiş 250 alan adlı portföyün ulusal Atlas derecesi 66/100 (C). Portföy, en az 1.140.618 cihaz ve 4.649.139 kimlik bilgisi kaydı ilişkilendirmesi içeriyor. Güncel ilanlar 171 alan adıyla ilişkili. Bunlar örtüşen dış sinyallerdir; doğrulanmış sızmalar değildir [S2].

7. Paylaşım hacmi görünürlüğü ölçer. Türkiye etiketli toplam 4.131.687; saklanmış anlatım korpusu 177.648 benzersiz paylaşım içerir. Ülke karşılaştırmaları aynı paylaşım tarihi aralığını kullanır. Tekrarlanan ilanlar, pazar referansları ve eşit olmayan görünürlük ulusal risk sıralamasını engeller [S1].

8. Kampanya araştırmaları ağ geçidi ve yönetim incelemesini destekliyor. FortiBleed araştırması, Türkiye etiketli 3.032 cihaz listeliyor. Ayrı sanallaştırma araştırması Türkiye'yi en büyük beş ülke grubu arasında sayıyor [S94][S96]. Kaynağa atfedilen altyapı gözlemleri benzersiz kuruluşları belirlemiyor veya kampanyaları rapordaki erişim ilanlarına bağlamıyor. Yerel olay açıklamadan önce güncel varlıkları, erişimi ve kalıcı erişim yollarını doğrulayın.

Yöneticiler için dört karar

1. **İşleyişi kesintiye uğratan adımdan önce kimlik sinyalini doğrulayın.** Yeni kimlik bilgisi veya erişim tekliflerini aktif hesaplarla ve yakın tarihli oturumlarla eşleştirme sorumluluğunu kimlik operasyonlarına verin. Doğrulanan yetkisiz kullanımı olay müdahalesine taşıyın; eşleşmeyen veya eski sinyallerin neden kapatıldığını kaydedin.
1. **Tedarikçi bildirimini olay planına alın.** Kimlik, müşteri, rezervasyon ve yatırım verisi tutan veri işleyenleri belirleyin. İlk uyarıyı kimin aldığını, kanıtı kimin koruduğunu ve bildirim yükümlülüğünün başlayıp başlamadığına kimin karar verdiğini sınayın.
1. **Kurtarmanın üretim ortamı yönetiminden bağımsız olduğunu gösterin.** Korunan yedeklerle ve ayrı kurtarma kimlik bilgileriyle temel bir hizmeti geri yükleyin. Başarılı yedekleme işini yeterli saymayın; hizmetin hazır oluşunu, veri bütünlüğünü ve iş birimi onayını ölçün.
1. **İletişimi doğrulanmış hizmet ve veri bulgularına bağlayın.** Durum sayfasını, sözcüyü ve kanıt sorumlusunu önceden belirleyin. Aktör duyurusunu, gözlemlenen hizmet sorununu ve veri işlemeye ilişkin doğrulanmış açıklamayı ayrı tutun.

Yılın rakamları

Aşağıdaki rakamlar farklı grupları anlatır. Her birinin kendi sınırı vardır.

157

2026 dönemindeki Türkiye fidye yazılımı listelemeleri [S3]

NEYİ GÖSTERMEZ

Doğrulanmış saldırıları, tekil mağdurları veya ulusal fidye yazılımı toplamını

53

Aynı görünümde 2025 yılının tamamındaki Türkiye listelemeleri [S3]

NEYİ GÖSTERMEZ

Eşit süreli karşılaştırma tabanını

66/100 (C)

Seçilmiş portföyün ulusal Atlas derecesi [S2]

NEYİ GÖSTERMEZ

İhlal yüzdesi, olay olasılığı veya sektör sıralaması

4.131.687

Belirtilen dönemde Türkiye etiketli paylaşımlar [S1]

NEYİ GÖSTERMEZ

Doğrulanmış olaylar veya saklanmış anlatım korpusu

1.140.618

Seçilmiş portföyde cihaz ilişkilendirmesi, en az [S2]

NEYİ GÖSTERMEZ

Benzersiz kişiler veya kuruluşun işlettiği cihazlar

4.649.139

Seçilmiş portföyde kimlik bilgisi kaydı ilişkilendirmesi [S2]

NEYİ GÖSTERMEZ

Benzersiz aktif hesaplar veya doğrulanmış sızmalar

250

On iki sektörde seçilmiş kuruluş alan adları [S2]

NEYİ GÖSTERMEZ

Resmî sıralamayı veya ülkeyi temsil eden örneklemi

177.648

Bu sürümde saklanan tekil paylaşımlar [S1]

NEYİ GÖSTERMEZ

Ülke etiketli paylaşımların tamamını veya tekil olayları

860

Saklanan paylaşımlarda açık metin olarak görülen, Türkiye ile ilişkili tekil ödeme kartları [S4]

NEYİ GÖSTERMEZ

Kart hırsızlığını, aktif kartları, kayıpları veya Brandefense'in daha geniş kart kapsamını

323.052

KVKK üzerinden bildirilen bir perakendecinin tahmini olası etki grubu [S16]

NEYİ GÖSTERMEZ

Karanlık ağ dosyasından doğrulanmış sayıyı

140.000 / 4.500

Üniversite bildirimindeki yaklaşık öğrenci ve personel grupları [S12]

NEYİ GÖSTERMEZ

Doğrulanmış veri aktarımını veya kesin tekil kişi toplamını

72 saat

KVKK'nın, öğrenmeden sonra Kurula bildirim süresine ilişkin yorumu [S8]

NEYİ GÖSTERMEZ

Tüm siber bildirim yükümlülükleri için ortak süreyi

TEMEL ÇIKARIMLAR

01

Listelemeleri, paylaşımları ve resmî olayları ayrı karar yollarında tutun.

02

Sistem genelinde olay sonucu çıkarmadan hesapları ve tedarikçi erişimini doğrulayın.

03

Kurtarma ve bildirim tatbikatlarına sorumlusu belirlenmiş bütçe ayırın.

Rapor haritası

Sorumlu olduğunuz karardan başlayın; ardından kanıtı ve tamamlanma ölçütünü izleyin.

Yönetim kurulu ve CISO	Hangi riskler bugün bütçe gerektiriyor?	01 05 11 12
SOC ve olay müdahalesi	Dış iddia ne zaman incelemeye dönüşür?	04 06 07 12
Kimlik ve altyapı	Hangi erişim yolları ve bağımlılıklar doğrulanmalı?	03 05 07 12
Dolandırıcılıkla mücadele ve bankacılık	Hangi kişisel bilgiler işlem yetkisi vermemeli?	08 09 12
Hukuk ve satın alma	Kim, kime, hangi metne göre bildirim yapmalı?	05 10 12

Kanıt yolu	Yanıtladığı soru	Sınır
Karanlık ağ paylaşımları	Neler ilan, talep veya duyuruluyor?	Gerçeklik ve sonuçlar ayrıca kanıtlanmalı
Fidye yazılımı listelemeleri	Listeleme görünümünde neler var?	Listeleme tarihi, yetkisiz erişimin gerçekleştiği tarihten farklı olabilir
Pasif gözlemler	Dışa açık yapılandırmalar ne gösteriyor?	Başarılı sızma veya kontrol etkinliği kanıtı değil
Resmî açıklamalar	Veri sorumlusu veya makam ne bildiriyor?	Tahminler ve incelemeler değişebilir
Üretici araştırmaları	Araştırmacı ne gözlemlemiş ve kime atfetmiş?	Kampanya bulguları Türkiye'deki bir mağduru anlatmayabilir

BÖLÜM 02

Türkiye'nin dijital ve güvenlik bağlamı

02

BU BÖLÜMÜN YANITLADIĞI SORU

Hangi ulusal özellikler savunma planını şekillendirmeli?

%90,4

2026 sonu için bildirilen internet kullanım oranı

2.1 Bağlantılı nüfus ve çok sayıda kimlik temas noktası 10

2.2 Temel hizmetler ve tedarikçiler 10

2.3 Ulusal koordinasyon ve güncel kanallar 10

2.4 Siyasi çerçeve ve atıf 11

2.5 Değişen düzenleme takvimi 11

BÖLÜM 02

Türkiye'nin dijital ve güvenlik bağlamı

KISACA

Bağlantılı hizmetler iş fırsatlarıyla birlikte kimlik bağımlılıkları da yaratır. DataReportal'ın Kasım sürümü, 79,5 milyon internet kullanıcısı ve %90,4 kullanım oranı bildiriyor. Resmî siber koordinasyon da değişiyor; dayanıklılık ve denetim metinleri son tarihte görüşe açık taslaklardı. Hizmet bağımlılıklarını, güncel bildirim kanallarını ve hesap kötüye kullanımını tedarikçi olaylarından ayıracak kanıtları temel alarak plan yapın.

2.1 Bağlantılı nüfus ve çok sayıda kimlik temas noktası

DataReportal, Digital 2027 Türkiye sürümünü 5 Kasım 2026 tarihinde yayımladı. Raporda 79,5 milyon internet kullanıcısı, 85,9 milyon mobil bağlantı ve 61,0 milyon sosyal medya kullanıcı kimliği bildiriliyor. Bunlar 2026 sonuna ilişkin tahminler; sosyal medya kimlikleri Ekim tarihli. Bağlantılar ve kimlikler tekil kişileri temsil etmez [S5].

Savunma açısından çıkarım bağımlılıklarla ilgilidir. Müşteri aynı kuruluşla mobil mesajlaşma, e-posta, hesap portalı ve tedarikçi üzerinden karşılaşabilir. Doğru ad veya telefon numarası, dolandırıcılık amaçlı iletişimi inandırıcı kılabilir. Arayanın yetkili olduğunu göstermez.

Dijital hizmet envanteri; uygulamaları kimlik sağlayıcılarına, kurtarma kanallarına, veri işleyenlere ve hizmet sorumlularına bağlamalıdır. Sunucu envanteri tek başına müşteri verisini kimin dışarı aktarabildiğini, hesap sıfırlayabildiğini veya güvenilen bir mesaj yayımlayabildiğini açıklamaz.

2.2 Temel hizmetler ve tedarikçiler

Rapor, seçilmiş portföy için on iki analitik sektör grubu kullanır [S2]. Bu gruplar, bir kuruluşu hukuken kritik altyapı olarak belirlemez.

Operasyon sorusu, hangi bağımlılıkların temel iş akışını durdurabileceğidir. Bordro süreci bankaya ve kimlik sağlayıcısına bağlı olabilir. Rezervasyon süreci veri işleyene ve mesajlaşma hesabına dayanabilir. Kurtarma hedefi belirlemeden önce gerçek bağımlılıkları çıkarın.

Bölüm 5'teki resmî tedarikçi bildirimleri bunun önemini gösteriyor. Veri sorumlusu olayı ilk kez veri işleyenden öğrenebilir. Veri işleyenin teknik incelemesiyle veri sorumlusunun etkilenen kişileri değerlendirme yükümlülüğü farklı zaman çizelgelerinde ilerleyebilir [S16][S17][S20].

2.3 Ulusal koordinasyon ve güncel kanallar

USOM'un kamu duyurusu; güvenlik bildirimlerini, teknik içerikleri, zararlı bağlantı bilgilerini ve CVE süreçlerini Siber Güvenlik Başkanlığının sitesine yönlendiriyor. Metin biçimindeki bir paylaşım hizmetinin 1 Haziran 2026 itibarıyla sona ereceğini de duyuruyor [S7]. Savunma ekipleri, operasyon bağlantılarının ve kullandıkları bilgi hizmetlerinin güncelliğini doğrulamalıdır.

Başkanlığın Ekim ayındaki PHP duyurusu, ulusal güvenlik kontrollerinin başlatıldığını ve ilgili kuruluşlara acil bildirim yapıldığını söylüyor. Bu, resmî müdahale çalışmasının kanıtıdır. Türkiye'de başarılı istismar sayısı değildir [S24].

Mayıs tarihli olay müdahale rehberi; hesap yönetimi, ağ ayrımı, uzaktan erişim ve günlük kayıtlarında tekrarlanan eksiklikleri anlatıyor. Kontrol incelemesini destekler. Türkiye'deki tüm kuruluşları temsil eden bir ölçüm tabanı sunmaz [S33].

2.4 Siyasi çerçeve ve atıf

Saklanan bazı paylaşımlar veri iddialarına siyasi dil ekliyor. Rapor bu iddiaları, sloganları veya tanımlamaları benimsemez. Üyelik verisi teklifi, kuruluş adı çıkarılmış doğrulanmamış veri iddiası olarak ele alınır. Siyasi destekçi belirlemek için temel sağlamaz [S1].

Aynı yaklaşım; toprak sorunları, etnik veya dinî kimlikler, bölgesel çatışmalar, seçimler ve hükûmet kararları için de geçerlidir. Aktörün belirttiği gerekçe kendisine aittir. Bir nedeni kanıtlamaz, eylemi meşrulaştırmaz veya devlet yönlendirmesi göstermez.

Bölüm 6'daki Kasım DDoS malzemesi özellikle sınırlıdır. Bir kanal, Türkiye'de hedef seçme niyetini duyuruyor. Bu, savunma hazırlığı için bir işarettir; burada saldırı girişimi veya kesinti kanıtı yoktur [S1].

2.5 Değişen düzenleme takvimi

7545 sayılı Kanun, 19 Mart 2025 tarihinde yayımlanarak yürürlüğe girdi. Güncel metin, 31 Temmuz 2026 tarihinde yürürlüğe giren değişiklikleri içeriyor [S9]. İlk kabul dönemindeki özetlerin her hükmü hâlâ doğru anlattığını varsaymayın; güncel metni okuyun.

Başkanlık, 18 Kasım 2026 tarihinde dayanıklılık ve denetim taslaklarını görüşe açtı. İki duyuruda da 3 Aralık 2026 tarihine kadar görüş istendi [S10][S11]. Rapor bunları son tarihte taslak olarak ele alır. Görüş tarihi, önerilen yükümlülüklerin yürürlük tarihi değildir.

TEMEL ÇIKARIMLAR

01
Kimlik ve tedarikçi bağımlılıklarını sunucu ve uygulamalarla birlikte haritalayın.

02
Ulusal koordinasyon bağlantılarını ve güvenlik bilgi kanallarını güncel tutun.

03
Siyasi ve devlet bağlantısı iddialarını kaynağına bağlayın, belirsizliği koruyun.

BÖLÜM 03

Ulusal maruziyet: seçilmiş 250 kuruluş alan adı

03

BU BÖLÜMÜN YANITLADIĞI SORU

Seçilmiş ulusal portföyde hangi dış sinyaller doğrulama gerektiriyor?

250

on iki sektörde kuruluş alan adı değerlendirmesi

3.1 İncelenen evren 13

3.2 Ulusal Atlas notunun anlamı 14

3.3 Cihaz ve kimlik bilgisi ilişkilendirmeleri yoğunlaşıyor 14

3.4 Güncel piyasa ilanları hesap doğrulaması gerektirir 16

3.5 Anılmalar ve benzer alan adları bağlam sağlar 17

3.6 Pasif kontroller kendi paydalarını korur 18

3.7 Portföyü ayrı doğrulama kuyruklarına dönüştürün 19

BÖLÜM 03

Ulusal maruziyet: seçilmiş 250 kuruluş alan adı

KISACA

Seçilmiş portföyde cihaz ve kimlik bilgisi ilişkilendirmeleri ile güncel piyasa ilanları yaygın. Ulusal Atlas derecesi 66/100 (C). Bu derece Türkiye'deki tüm kuruluşları değil, seçilmiş portföyü anlatır. Kanıtlar en az 1.140.618 cihaz ve 4.649.139 kimlik bilgisi kaydı ilişkilendirmesi içeriyor. Bunlar örtüşen kayıtlardır; benzersiz kişiler veya doğrulanmış sızmalar değildir. Güncel hesap doğrulamasına, çalışan cihazı incelemesine ve kurtarma kontrollerine sorumlu atayın.

3.1 İncelenen evren

Portföy, önde gelen kamu kurumlarını, hizmet sağlayıcılarını ve ticari kuruluşları kapsar. Seçilmiş örneklemin sınırlarını koruyarak farklı sektörlerden geniş bir görünüm sunar [S2].

Kalem	Tanım
Portföy	On iki sektörde seçilmiş 250 kuruluş alan adı
Seçim	Kamu kurumları, büyük hizmet sağlayıcıları ve sektörlerinde öne çıkan işletmeler
Sektör grupları	Kamu 50; bankacılık ve finans 30; eğitim 30; imalat 30
Diğer gruplar	Enerji, perakende ve ulaşım için 20'şer; diğer beş sektör için 10'ar
Maruziyet görünümü	21 Kasım 2026
Anılma bağlamı	19 Kasım 2025–18 Kasım 2026
Pasif gözlem	21 Kasım 2026 UTC; yerel saatte 22 Kasım
Yayım	Ulusal başlık derecesi ve kimliksiz sektör toplamları
Kimlik sınırı	Alan adları markaları, kurumsal hizmetleri veya ilişkili tüzel kişileri temsil edebilir
Çıkarım sınırı	Ulusal yaygınlık tahmini, kuruluş sıralaması veya olay olasılığı vermez

Değerlendirme birimi seçilmiş alan adıdır. Bazıları ilişkili kuruluşlara veya hizmetlere aittir. Portföyün bir bölümü için sahiplik doğrulaması tamamlanmamıştır. Bu nedenle 250 değerlendirme, birbirinden bağımsız sahipliği bulunan 250 işletme olarak okunmamalıdır.

Yayımlanan en küçük sektör grubu 10 seçilmiş alan adı içerir. Bu paydalar kimliksiz betimlemeyi destekler; sektörün işverenlerini, kullanıcılarını veya ekonomik büyüklüğünü temsil ettiğini göstermez.

Maruziyet gözlemleri ile pasif kontroller farklı soruları yanıtlar. Eski bir kimlik bilgisi kaydı, bugün doğru yapılandırılmış bir hizmetle birlikte görülebilir. Yayımlanmış e-posta politikası da güncel hesap olayıyla bir arada bulunabilir. Biri için gereken inceleme diğerinin yerine geçmez.

3.2 Ulusal Atlas notunun anlamı

Portföyün ulusal Atlas derecesi 66/100 (C). Daha yüksek değer, bu portföyde daha fazla gözlemlenen maruziyete işaret eder. Not, seçilmiş portföyde önceliklendirmeyi destekler. İhlal edilen kuruluşların yüzdesi, gelecekte sızma olasılığı veya kontrollerin etkili çalıştığına ilişkin belge değildir [S2].

Yalnızca ulusal not yayımlanır. Aşağıdaki sektör satırları, gözlemlenen maruziyet sayılarını ve paydalarını gösterir. Sektörleri birleşik bir puana göre sıralamaz. Kuruluş puanları ve kimlikleri raporda yer almaz.

Derece, tarihli maruziyet görünümüne aittir. Paylaşım dönemi, yıllık anılma bağlamı ve pasif gözlem tarihi ayrı etiketlenir. Bunlar, tüm sinyallerin ilk kez 2026 içinde ortaya çıktığı iddiasına dönüştürülemez.

Belirli bir hesap için düzeltme yapılmış olsa da derece yüksek kalabilir. Eski kayıtlar, tekrarlanan ilanlar ve ortak müşteri cihazları dış kanıtlarda kalmayı sürdürebilir. Kapanış için kuruluş içinden doğrulama gerekir; sonuç ilgili sinyale bağlanmalıdır.

İlk iş, gözlemin aktif bir hesaba, yönetilen çalışan cihazına, müşteri cihazına veya eski kayda ilişkin olup olmadığını belirlemektir. Sorumlu ekip ve uygun işlem bu ayrımdan çıkar.

3.3 Cihaz ve kimlik bilgisi ilişkilendirmeleri yoğunlaşıyor

Portföy en az 1.140.618 cihaz ilişkilendirmesi içerir. Bunların içinde 52.548 çalışan cihazı ilişkilendirmesi vardır. Kimlik bilgisi kaydı ilişkilendirmeleri 4.649.139 düzeyindedir. İlişkilendirmeler farklı alan adları arasında örtüşebilir [S2].

Müşteriye hizmet veren bir alan adıyla ilişkili cihaz, kendiliğinden o hizmeti işleten kuruluşun cihazı sayılmaz. Alan adıyla ilişkili kimlik bilgisi kaydı da kaynağın kuruluşun kendi dizini veya altyapısı olduğunu göstermez.

Sektör	Alan adı	Cihaz, en az	Çalışan cihazı	Kimlik bilgisi kaydı
Kamu	50	196.180	6.273	278.104
Bankacılık ve finans	30	175.336	1.643	393.538
Eğitim	30	202.764	24.272	2.863.146
İmalat	30	18.231	1.373	186.812
Enerji ve altyapı	20	17.321	466	79.430
Perakende ve holding-ler	20	297.274	1.394	143.853
Ulaşım ve lojistik	20	86.160	745	89.309
Telekom ve teknoloji	10	101.887	14.666	453.352
Sağlık	10	5.705	371	35.227
Sigorta	10	14.488	142	28.527
Konaklama ve turizm	10	12.459	599	20.213
Medya ve eğlence	10	12.813	604	77.628
Toplam	250	1.140.618	52.548	4.649.139

Tablodaki cihaz ve çalışan cihazı sayıları ilişkilendirmedir; ülke çapında benzersiz uç noktalar değildir. Çalışan ilişkilendirmeleri cihaz görünümünün içinde sunulur ve toplama ayrıca eklenmez. Kimlik bilgisi kayıtları ayrı bir grupdur.

Eğitim, 2.863.146 kimlik bilgisi kaydı ilişkilendirmesi içerir. Bu, portföy toplamının %61,6 bölümüdür. Yoğunlaşma, odaklı kimlik doğrulama çalışmasını destekler; eğitimin güncel ele geçirilme oranının en yüksek olduğunu göstermez.

Perakende ve holdingler en az 297.274 cihaz ilişkilendirmesi içerir. Eğitim, kamu, bankacılık ve telekom satırlarında da büyük cihaz grupları vardır. Müşteri erişimi, alan adının kullanım biçimi ve geçmiş görünürlük bu toplamları etkileyebilir.

Az sayıda, yüksek hacimli alan adı bir sektör toplamına hâkim olabilir. Ulusal toplam, tek bir kuruluş için beklenen maruziyet sayısı olarak kullanılamaz. Her sorumlu, kendi hesap ve hizmetlerine ilişkin tarihli kanıta ihtiyaç duyar.

İlk doğrulama sorusu güncelliktir. Kaydın aktif bir hesaba ait olup olmadığını, parolanın değişip değişmediğini ve ilgili oturumların kullanılabilir kalıp kalmadığını belirleyin. İkinci soru yetkidir: gözlem tarihinde hesabın nereye erişebildiğini saptayın.

Çalışan cihazıyla ilişki doğrulandığında, kapanıştan önce uç nokta ve kimlik kanıtlarını koruyun. Oturumları, kurtarma yöntemlerini, devredilmiş erişimi ve ayrıcalıklı işlemleri inceleyin. Yalnızca parola sıfırlamak, hesapla ilişkili tüm yolların kapatıldığını göstermez.

Müşteri cihazı ilişkilendirmesinde sorumlu ekip dolandırıcılıkla mücadele, müşteri desteği veya hesap koruma olabilir. Dış materyalde banka alan adı görülmesi, müşteriyi çalışan cihazı saymak veya banka altyapısı olayı açmak için tek başına yeterli değildir.

Sektörlerin cihaz ve kimlik bilgisi grupları büyüklük ve anlam bakımından farklı

EN AZ CİHAZ İLİŞKİLENDİRMESİ (ÇALIŞAN İLİŞKİLENDİRMELERİ MERCAN RENGİNDE)



KİMLİK BİLGİSİ KAYDI İLİŞKİLENDİRMELERİ (AYRI ÖLÇEK)



Kaynak: Odin by Brandefense, seçilmiş 250 alan adı portföyü, 22 Kasım 2026 [S2]. İlişkilendirmeler örtüşebilir ve doğrulanmış sızma değildir.

3.4 Güncel piyasa ilanları hesap doğrulaması gerektirir

Seçilmiş 250 alan adının 171 tanesi güncel piyasa ilanlarıyla ilişkilidir. Aynı görünümde 242 alan adı kimlik bilgisi kayıtlarıyla, 235 alan adı cihazlarla ilişkilidir. Bunlar farklı ve örtüşebilen sinyallerdir [S2].

Sektör	Alan adı	Güncel ilan	Belge
Kamu	50	31	1.100
Bankacılık ve finans	30	18	128

Sektör	Alan adı	Güncel ilan	Belge
Eğitim	30	25	508
İmalat	30	12	153
Enerji ve altyapı	20	11	78
Perakende ve holdingler	20	19	233
Ulaşım ve lojistik	20	15	53
Telekom ve teknoloji	10	7	84
Sağlık	10	9	42
Sigorta	10	8	20
Konaklama ve turizm	10	6	21
Medya ve eğlence	10	10	176
Toplam	250	171	2.596

Güncel ilan sütunu, maruziyet görünümünde güncel bir ilanla ilişkili alan adlarını sayar. Tamamlanmış satışları, denenmiş kimlik bilgilerini veya iç sistemlere sızıldığı doğrulanan kuruluşları saymaz. İlan, ilgili hesap ve hizmet üzerinden doğrulanmalıdır.

Belge sütunu, seçilmiş 204 alan adına ilişkin 2.596 belge ilişkilendirmesi içerir. İlişkilendirme; belgenin gizli olduğunu, hukuka aykırı elde edildiğini veya saldırgan tarafından indirildiğini göstermez. Kamuya açık belgeler ve tekrarlanan materyal olası açıklamalar arasındadır.

İlan ve belge toplamları birbirine eklenmez. Aynı kuruluş ikisinde de bulunabilir. Tek bir kimlik bilgisi veya belge birden çok alan adıyla ilişkilendirilebilir. Tablo benzersiz dosya veya etkilenen kişi sayısı vermez.

Güncel ilanı sınırları belli bir inceleme başlatmak için kullanın. İlan edilen hizmeti belirleyin, hesabın varlığını ve aktifliğini doğrulayın, iddiayı güncel kimlik doğrulama kanıtlarıyla karşılaştırın. Yalnızca başlık veren ilanda bilinmeyenleri kaydedin.

Rutin doğrulama kapsamında satıcıyla iletişime geçmeyin veya üçüncü tarafın ilan edilmiş kimlik bilgilerini denemeyin. Kuruluşlar kendi kayıtlarını ve yetkili olay süreçlerini kullanabilir. Kamu raporu, açığa çıkan hesabın kullanımını kolaylaştıracak materyali tekrar yayımlamamalıdır.

İlgisiz veya eski sinyali gerekçesiyle kapatın. Güncel yetkisiz erişim doğrulanırsa ayrı incelemeyi sürdürün. Böylece her ilan doğrulanmış olaya dönüştürülmeden kararların kanıtı tutulur.

3.5 Anılmalar ve benzer alan adları bağlam sağlar

Kuruluşların anılması, belirtilen yıllık dönem için ek bağlam sağlar. Haber, müşteri konuşması, reklam, meşru hizmet veya kötüye kullanım söz konusu olabilir. Alan adının konuşmada geçmesi, tek başına yetkisiz erişim kanıtı değildir [S2].

Yıllık görünümde 98 seçilmiş alan adı sohbetlerde, 56 alan adı web kaynaklarında anılıyor. İki popülasyon örtüşür. Sayılar alan adı görünürlüğünü anlatır; her anılmayı olay olarak sınıflandırmaz.

Benzer alan adı gözlemleri, sahiplik ve kullanım denetimi gerektirir. Benzer adlar yetkili bayiye, ilişkili işletmeye veya tamamen başka bir kuruluşa ait olabilir. Kötüye kullanım iddiasından önce sahiplik ve ilişkili işletme kontrolleri gerekir.

Anlamlı bir üst inceleme, olası taklit ilişkisini yetkisiz giriş sayfası veya yanıltıcı ödeme talebi gibi zararlı kullanımla birleştirir. Benzerlik incelemeyi destekler; alan adını kaydeden kişi hakkında kamuya açık suçlama için yeterli değildir.

Aynı sınır belge ve anılmalar için de geçerlidir. Güncel hizmeti, aktif kimliği veya zararlı kullanıcı etkileşimini belirleyen kanıta öncelik verin. Ek kanıt yoksa düşük güvenli bağlam gözlemini açık bırakın veya gerekçesiyle kapatın.

3.6 Pasif kontroller kendi paydalarını korur

Pasif gözlemler, DNS çözümlemesi yapılabilen 239 alan adını kapsar. Diğer 11 seçilmiş alan adı bu görünümde yorumlanabilir gözlem sağlamadı. Bu eksiklik, başarısız güvenlik kontrolü olarak puanlanmamalıdır [S2].

Gözlem	Sayı	İncelenen grup
DMARC ret veya karantina politikası	155	Çözümlenen 239 alan adı
SPF gözlendi	231	Çözümlenen 239 alan adı
DNSSEC delegasyon kaydı gözlendi	9	Çözümlenen 239 alan adı
TLS sertifika kontrolü geçerli	214	Çözümlenen 239 alan adı
TLS sertifika doğrulaması başarısız	12	Çözümlenen 239 alan adı
TLS sonucu belirsiz	13	Çözümlenen 239 alan adı
Ana sayfada HSTS gözlendi	136	Yanıt veren 184 ana sayfa
Ana sayfa yanıtı kaydedildi	184	Çözümlenen 239 alan adı
Ana sayfa kontrolü sonuçsuz	55	Çözümlenen 239 alan adı

TLS satırları, çözümlenen alan adı toplamıyla uzlaşır. Başarısız sertifika doğrulaması yapılandırma incelemesi gerektirir; belirsiz kontrol ise sertifika hakkında hüküm vermez. Ana sayfa sonuçlarında da yanıt veren sayfa ile sonuçsuz gözlem ayrı tutulur.

Pasif politika gözlemleri incelenen sektör paydalarını korur

	DMARC reject / quarantine	SPF gözlemi	DNSSEC delegasyonu	TLS doğrulaması
Kamu	31/45	43/45	0/45	39/45
Bankacılık ve finans	21/29	29/29	2/29	25/29
Eğitim	20/29	28/29	0/29	26/29
İmalat	14/29	27/29	0/29	25/29
Enerji ve kamu hizmetleri	14/20	20/20	0/20	16/20
Perakende ve holdingler	11/20	20/20	1/20	20/20
Ulaşım ve lojistik	14/19	18/19	1/19	17/19
Telekom ve teknoloji	6/9	9/9	0/9	7/9
Sağlık	6/10	10/10	1/10	10/10
Sigorta	4/9	7/9	0/9	9/9
Konaklama ve turizm	7/10	10/10	3/10	10/10
Medya ve eğlence	7/10	10/10	1/10	10/10

Kaynak: pasif gözlemler, 21 Kasım 2026 UTC; sektör paydaları korunmuş 239 gözlemlenen alan adı [S2]. Politikalar kontrol etkinliğini göstermez.

Yayımlanmış DMARC ret politikası, bir politika sinyalidir. Her iletinin doğru kimlik doğrulamasından geçtiğini kanıtlamaz. İzleme politikası ret politikasından farklıdır. Yapılandırma sorumluları değişiklikten önce etkili ve üst alan adından gelen politikaları denetlemelidir [S34][S35].

SPF kaydının görünmesi, bütün meşru göndericilerin kapsandığını göstermez. DKIM kaydının gözlenmemesi de imzalama bulunmadığı anlamına gelmez. Kuruluşun kullandığı seçicileri ve giden ileti başlıklarını doğrulayın [S35] [S36].

DNSSEC gözlemi, her hizmetin korunduğunu göstermez. Geçerli TLS sertifikası sınırlı bir sertifika denetimini doğrular. Uygulamanın yamalı veya erişimin yetkili olduğunu göstermez [S37][S38].

Web başlığı değişiklikleri de uygulama bağlamı gerektirir. Eksik başlık inceleme gerektirebilir; ancak değişiklik gömülü hizmeti veya entegrasyonu bozabilir. Uygulama sorumlusuna denenebilir değişiklik, beklenen sonuç ve geri dönüş planı verin.

3.7 Portföyü ayrı doğrulama kuyruklarına dönüştürün

Kanıtlar; güncel hesap doğrulaması, çalışan cihazı incelemesi, müşteri hesabı koruması ve yapılandırma denetimi için ayrı kuyrukları destekler. Sorumluluk, varlığa ve destekleyici kanıta göre belirlenmelidir. Ortak ulusal başlık bu işleri birbirinin yerine geçebilir kılmaz.

Sinyal	Sorumlu	İlk doğrulama	Tamamlama kanıtı
Güncel hesap ilanı	Kimlik operasyonları	Hesap varlığı ve hizmet eşleşmesi	Tarihli hesap kararı ve oturum incelemesi
Çalışan cihazı ilişkisi	Uç nokta müdahalesi	Yönetilen cihaz ve hesap ilişkisi	Sınırlama, kurtarma ve kimlik incelemesi
Müşteri cihazı ilişkisi	Dolandırıcılıkla mücadele ve hesap koruma	Müşteri hesabı ilgisi ve kötüye kullanım göstergeleri	Koruma kararı ve işlem incelemesi
Kimlik bilgisi kaydı	Kimlik operasyonları	Güncellik ve önceki düzeltme	Aktif, eski veya ilgisiz kararı
Belge ilişkilendirmesi	Bilgi sahibi	Hassasiyet, yetki ve güncel erişilebilirlik	Doğrulanmış işleme kararı
E-posta veya web politikası	Hizmet sorumlusu	Etkili yapılandırma ve bağımlılıklar	Denenmiş değişiklik veya gerekçeli istisna

Sorumlu bekleyen inandırıcı sinyalleri, doğrulama süresini ve geciken işleri izleyin. Kaç sinyalin doğrulandığını, eski, ilgisiz veya belirsiz kaldığını bildirin. Bu sonuçlar portföyün işe yarar kararlara dönüşüp dönüşmediğini gösterir. Başlık puanının değişmesi tek başına bunu gösteremez.

Tedarikçiyle ilişkili gözlemde, hangi kiracı ortamının ve iş hizmetinin etkilendiğini belirleyin. Doğrulanan veri işleme sorularını mahremiyet sorumlusuna aktarın. Teknik ekip erişimi ve kalıcılığı incelesin. Bildirim kararı, inandırıcı olay ile belirsiz veri aktarımı arasındaki ayrımı korumalıdır.

TEMEL ÇIKARIMLAR

01
Ulusal Atlas derecesi Türkiye'deki tüm kuruluşlara değil, seçilmiş portföye aittir.

02
Cihaz, kimlik bilgisi, ilan ve belge grupları ayrı doğrulama gerektirir; birbirine eklenmez.

03
Her inandırıcı sinyali kimlik, uç nokta, dolandırıcılıkla mücadele veya hizmet sorumlusuna tarihli kapanış kanıtıyla atayın.

BÖLÜM 04

Karanlık ağda gördüklerimiz

04

BU BÖLÜMÜN YANITLADIĞI SORU

Paylaşım hacimleri neyi gösterir ve hangi teklifler incelenmelidir?

4.131.687

gözlem döneminde Türkiye etiketli paylaşım

4.1 İncelenen evren 22

4.2 Aylık hacimler ve dört karşılaştırma ülkesi 23

4.3 Platformlar ve diller 24

4.4 Suç temaları ve birimler 25

4.5 Dokuz iddia dosyası 27

4.6 Talep, eski malzeme ve hassas iddialar 36

4.7 Olay ekibi neyi saklamalı? 37

BÖLÜM 04

Karanlık ağda gördüklerimiz

KISACA

Belirtilen dönemde Türkiye etiketli paylaşım hacmi 4.131.687. Dört karşılaştırma ülkesinin toplamı da aynı gözlem türünü ölçer; doğrulanmış olayları veya ulusal riski ölçmez. Saklanan gönderi arşivinde veri seti, hesap temini ve erişim ilanları dâhil 177.648 benzersiz paylaşım var. Bazıları eski materyali anlatır. Büyük sayılar kişi, kayıt ve işlemleri karıştırır. Hacmi görünürlüğü anlamak için kullanın; ardından her inandırıcı teklifin temelindeki iddiayı doğrulayın.

Karşılaştırma ülkeleri yalnızca bağlam sağlamak için örnek olarak seçilmiştir, bir sıralama ya da siyasi değerlendirme içermez.

4.1 İncelenen evren

Kesin etiketli paylaşım görünümü ile incelenen gönderi arşivi farklı amaçlara hizmet eder. İlki bildirilen paylaşım hacmini anlatır. İkincisi, tek tek iddiaları okumayı ve değerlendirmeyi sağlar [S1].

Kalem	Kapsam
Dönem	1 Ocak–21 Kasım 2026 tarihli paylaşımlar
Türkiye etiketli hacim	4.131.687 eşleşen paylaşım
Saklanan gönderi arşivi	İncelenen arşivde 177.648 benzersiz paylaşım
Forum grubu	Saklanan 5.210 forum paylaşımı
Diğer platformlar	Saklanan 172.438 paylaşım
Kapsam sınırı	Kapsamları farklıdır; biri diğerinin alt kümesi olarak sunulmaz
Birim	Yanıt, tekrar, ilan ve yorum dâhil paylaşım
Belirlenmeyenler	Benzersiz satıcı, veri seti, tamamlanan satış, güncel erişim veya doğrulanmış olay

İki görünümün kapsamı farklıdır; biri diğerinin alt kümesi olarak sunulmaz. Örneğin, saklanan 5.210 forum paylaşımı ile Türkiye etiketli 3.156 forum paylaşımı farklı görünümleri anlatır. Bu sayılar alt küme ilişkisi ortaya koymaz.

Genel bağlamdaki paylaşımlar görünürlük için tutulabilir; her biri için ayrı olay sonucu çıkarılmaz.

Ülke etiketi bir pazarı, dili, alıntılanan haberi veya çok ülkeli ilandaki ülkelerden birini anlatabilir. Türkiye'deki kuruluşun hedef alındığını veya yazarın burada bulunduğunu göstermez.

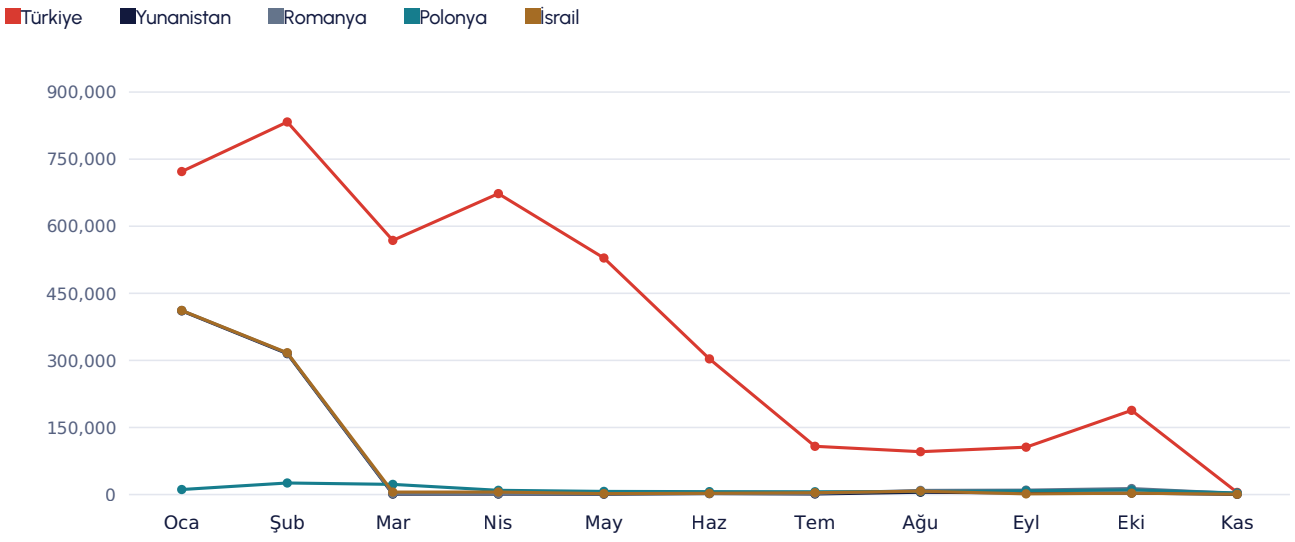
Kapanış haftası güncellemesi 15–21 Kasım dönemini kapsar. Önceki saklanmış gönderi arşivine göre 7 ek benzersiz paylaşım sağlar. Kapsam kaydı yeni materyalin kararını içerir. Güncelleme, ülkedeki bütün olayların görünür olduğunu kanıtlamaz.

4.2 Aylık hacimler ve dört karşılaştırma ülkesi

Aşağıdaki satırlarda bütün ülkeler için aynı paylaşım tarihi aralığı ve gözlem türü korunur. Kasım, kapanış tarihinde biter ve tam ay değildir [S1].

Ay	Türkiye	Yunanistan	Romanya	Polonya	İsrail
2026-01	722.292	410.726	411.615	11.246	411.657
2026-02	833.137	315.057	316.242	25.871	317.075
2026-03	568.298	963	2.104	22.759	5.569
2026-04	672.924	1.062	2.047	9.476	5.691
2026-05	528.914	846	1.770	7.038	2.105
2026-06	303.371	2.138	2.358	6.502	2.799
2026-07	107.910	1.244	2.468	6.273	4.102
2026-08	95.867	5.165	9.281	6.873	7.590
2026-09	105.939	3.548	9.915	8.431	1.535
2026-10	188.243	3.295	13.436	10.338	2.995
2026-11	4.792	488	2.484	3.560	819
Toplam	4.131.687	744.532	773.720	118.367	761.937

Ülke etiketli hacimler ortak gözlem döneminde farklılaşıyor



Kaynak: Brandefense Blackhole, Türkiye etiketli paylaşımlar ve karşılaştırma sayıları, 1 Ocak-21 Kasım 2026; Kasım kısmı [S1]. Etiketli paylaşımlar olay sayısı değildir.

Ocak 722.292, Şubat 833.137 Türkiye etiketli paylaşım içerir. İkisi birlikte dönem toplamının %37,6 bölümünü oluşturur. Yılın başındaki büyük popülasyon, doğrulanmış olayların aynı dağılımı izlediğini göstermez.

Bunlar görünürlük karşılaştırmalarıdır. Nüfusu, internet kullanımını, toplama kapsamını, piyasa katılımını veya ilanın tekrarlanma sıklığını düzeltmez. Büyük toplam, daha yüksek sızma olasılığını gösteremez.

Karşılaştırma ülkeleri bölgesel ve ekonomik bağlam sunar. Seçimleri siyasi yakınlık veya ulusal güvenlik performansı hakkında hüküm içermez. Bölüm 7'deki fidye yazılımı karşılaştırması ayrı bir ilan grubudur.

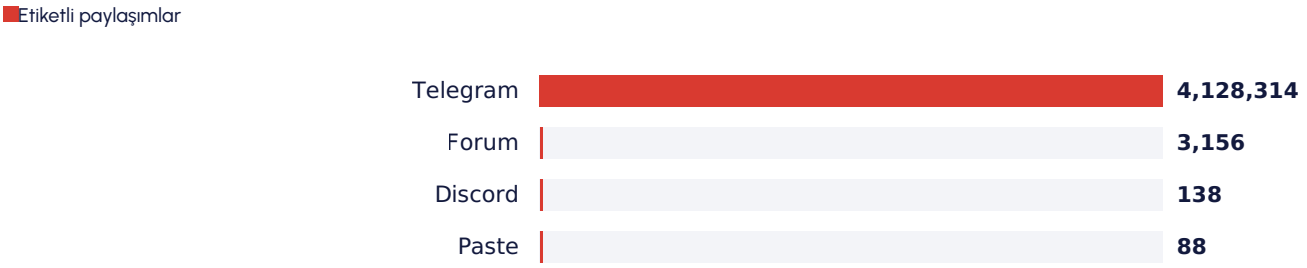
Ülkelerde ortak hareket, görünürlüğü veya geniş dağıtılan materyali yansıtabilir. Yalnızca Türkiye'de görülen hareket de kaynak bileşiminin incelenmesini gerektirir. İki durum da tek başına yeni kampanya veya mevcut kampanyanın başarısının arttığı anlamına gelmez.

4.3 Platformlar ve diller

Aşağıdaki tablolar Türkiye etiketli görünümü gösterir.

Platform	Türkiye etiketli paylaşım
Telegram	4.128.314
Forum	3.156
Discord	138
Paste	88

Platform sayıları doğrulanmış olayları değil, etiketli görünürlüğü anlatır



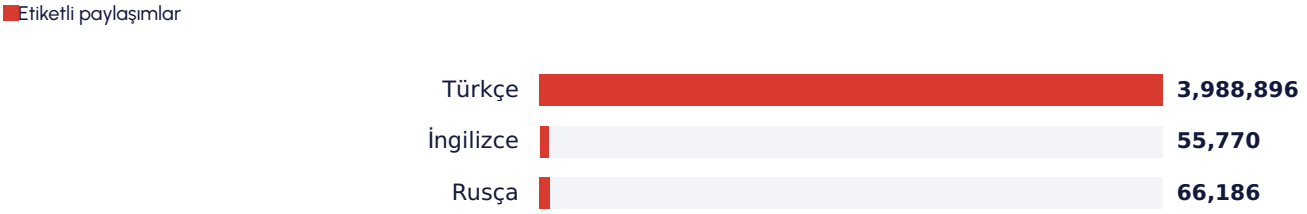
Kategoriler örtüşür; sayılar başarılı saldırıları değil paylaşımları anlatır. Kaynak: Brandefense Blackhole, Türkiye etiketli paylaşımlar ve karşılaştırma sayıları, 1 Ocak-21 Kasım 2026; Kasım kısmı [S1]. Etiketli paylaşımlar olay sayısı değildir.

Platform sayılarının toplamı, ulusal toplamı 9 paylaşım aşıyor. Bunlar ayrı gözlemlerdir ve ulusal toplamın kesin parçaları olarak ele alınmıyor. Etiketli görünürlüğün neredeyse tamamı Telegram kaynaklı. Tekrarlanan tanıtım trafiği bu nedenle ulusal görünen bir toplama hâkim olabilir.

Saklanan forum grubu, bir teklifi eski başlığın yanıtlarından ayırmak için gereken bağlamı sıklıkla sağlar. Yanıtlar bağımsız kanıt eklemeden başlığı, tutarı ve atfı tekrar edebilir. Başlığın temel iddiasını paylaşım sayısından ayrı değerlendirin.

Dil etiketi	Türkiye etiketli paylaşım
TR	3.988.896
EN	55.770
RU	66.186

Dil etiketleri içeriği anlatır ve örtüşebilir



Kategoriler örtüşür; sayılar başarılı saldırıları değil paylaşımları anlatır. Kaynak: Brandefense Blackhole, Türkiye etiketli paylaşımlar ve karşılaştırma sayıları, 1 Ocak-21 Kasım 2026; Kasım kısmı [S1]. Etiketli paylaşımlar olay sayısı değildir.

Dil bir ilgi işaretidir; hedefleme kararı değildir. Türkçe içerik başka ülkeyi anlatabilir. Rusça ve İngilizce listeler Türkiye'yi birkaç pazar arasında sayabilir. Etiketler birbirinden ayrı olmayabilir; toplamları ayrı grup gibi değerlendirilmemelidir.

4.4 Suç temaları ve birimler

Seçilmiş içerik temaları, görünürlüğün ne kadarının ilan edilen yetenek veya piyasa faaliyetiyle ilgili olduğunu gösteriyor [S1]. Tema etiketi satıcının iddiasını doğrulamaz. Paylaşımlar birkaç tema taşıyabilir; satırlar bu nedenle örtüşür.

İçerik teması	Türkiye etiketli paylaşım
Finans hesabı satma veya kiralama	1.969.446
Oltalamayla ilgili içerik	423.522
Finansal dolandırıcılık içeriği	70.851
Kart piyasası içeriği	70.278
Zararlı yazılımla ilgili içerik	35.631
Kimlik ve doğrulama verisi teklifleri	20.808
Veri sızıntısı ve veri tabanı iddiaları	7.056
İlk erişim teklifleri	6.833

Piyasa temaları örtüşür; başarılı saldırıları değil paylaşımları anlatır



Kategoriler örtüşür; sayılar başarılı saldırıları değil paylaşımları anlatır. Kaynak: Brandefense Blackhole, Türkiye etiketli paylaşımlar ve karşılaştırma sayıları, 1 Ocak–21 Kasım 2026; Kasım kısmı [S1]. Etiketli paylaşımlar olay sayısı değildir.

Finans hesabı satma veya kiralama teması 1.969.446 paylaşımda görülüyor. Oltalama 423.522, ilk erişim satışı ise 6.833 paylaşımda var. Bunlar farklı büyüklükte konuşma alanlarıdır. Bir saldırının aşamalarını veya suç gelirini ölçmez.

Oltalama etiketli paylaşım bir araç tanıtabilir, yardım isteyebilir veya başka satıcının mesajını tekrarlayabilir. Erişim ilanı, güncel geçerlilik kanıtı içermeyebilir. Ulusal hacim, kimlik ve dolandırıcılık ekiplerinin birlikte değerlendirme yapmasını destekler; kullanılan hesap sayısını tahmin etmez.

Tablo, kart piyasası konuşmalarını Bölüm 8'deki dar kart toplamından da ayırır. Ulusal görünümde kart dolandırıcılığı etiketli 70.278 paylaşım var. Bu sayı 70.278 kartı, başarılı tahsilatı veya etkilenen bankayı göstermez.

Yararlı ayrım, yazarın ne sunduğu veya istediğidir. Veri seti ilanı, veri talebi, kimlik bilgisi listesi, hesap temini ve DDoS duyurusu farklı doğrulama soruları gerektirir.

Tema	Kanıt örneği	Savunma sorusu
Çalışan kimliği	Eski sağlık çalışanı dosyası iddiası, B01	İş bilgileri hesap kurtarmayı kötüye kullanmaya yarar mı?
Müşteri kayıtları	Ödeme yazılımı iddiası, B02	Tedarikçi ilan edilen alanları tutuyor mu?
Taşınmaz verileri	Eski taşınmaz kaydı teklifi, B03	Varlık bilgisi kimlik doğrulamayı aşabilir mi?
Kimlik ve telefon verileri	Doğrulanmamış grup sayısı, B04	Kişisel bilgiler kimlik doğrulama sayılıyor mu?
Finans müşterisi verileri	Kripto işletmesi teklifi, B05	Kimlik ve dolandırıcılıkla mücadele sorumluları kökeni birlikte doğrulayabilir mi?
Uzaktan erişim	Hizmet sağlayıcı VPN teklifi, B06	Güncel kayıtlarda eşleşen yetkisiz erişim var mı?
Hesap temini	Banka ve borsa hesap setleri, B07	Müşteri kabulü ve ödeme kontrolleri bağlantılı kötüye kullanımı saptıyor mu?

Temalar örtüşür. Tek ilan kimlik verisi, hesap kaydı ve işlem içerebilir. Tema toplamları olay sayısına eklenemez. Bu yayım, yıl boyunca karşılaştırılabilir kategori eğilimleri ortaya koymaz.

Ek F, ayrıntılı okumadan 59 ek iddia ve piyasa teması içerir. Erişim teklifleri, tedarikçi iddiaları, arşivler ve hizmet ilanları vaka dosyalarını tamamlar. Benzer konu aynı dosya, satıcı veya kampanyayı göstermez.

4.5 Dokuz iddia dosyası

A

VAKA A

Eski çalışan verisi iddiası 2026 yılında paylaşılıyor

Kanıt kartı B01 | 4 Oca 2026 | Forum | Sağlık çalışanları

İddia doğrulanmadı

İDDİA	4 Ocak tarihli paylaşım, yaklaşık 2,7 milyon hastane çalışanı hakkında bilgi ilan etti. Paylaşan kişi, iddia edilen sızıntıyı açıkça 2025 yılına yerleştirdi [S1].
ZAMAN ÇİZELGESİ	Saklanan malzemede ertesi gün Türkçe anlatım da göründü. Benzer ifadeler iddianın yeniden dolaşımını destekler. İki paylaşanın aynı dosyaya sahip olduğunu göstermez.
BELİRLENEN	Paylaşım, alan açıklamaları ve paylaşanın belirttiği tarih elimizde. Paylaşım tarihi rapor döneminde; iddia edilen temel olayın tarihi bu dönemde değil.
ALTERNATİF	Eski derleme, yeniden paketlenmiş kayıtlar, yanlış ilan veya gerçek kamuya kapalı veri teklifi açıklayabilir. İlan tek başına bunlar arasında seçim yaptırmaz.
SINIR	Gerçeklik, kaynak sistemin sahipliği, eksiksizlik ve 2026 yılında yeni olay doğrulanmadı. İlan edilen büyüklük Brandefense ölçümü değildir.
YANIT	Sağlık ve çalışan verisi sorumluları, kurtarma veya yardım masası süreçlerinin çalışma bilgilerini kimlik kanıtı sayıp saymadığını sınamalı. Bağımsız kanaldan gelen bildirimleri iç kayıtlarla doğrulamalı.

Sonuç

Çalışma bilgilerinin hesap kurtarmaya yetki vermesini önleyin.

Kanıt kartı B01 — 4 Oca 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | İngilizce

ÖZGÜN METİN

This leak occurred in 2025.

ÇEVİRİ

Bu sızıntı 2025 yılında gerçekleşti.

Not. Hastane çalışanı veri kümesi için 2025 kaynak tarihi iddia ediliyor.

Ortaya konan
Paylaşım, iddia edilen büyüklük ve 2026 paylaşım tarihi.

Ortaya konmayan
Kaynak sistem, gerçeklik, 2026 yılında yeni bir olay veya tamamlanmış satış.

VAKA B

B

Müşteri verisi iddiası bir yazılım işletmesini adlandırıyor

Kanıt kartı B02 | 24 Oca 2026 | Forum | Müşteri hizmetleri

İddia doğrulanmadı

İDDİA	Ocak tarihli forum paylaşımı 93.000 müşteri kaydını bir ödeme yazılımı işletmesine atfetti. Ad, telefon numarası ve adres bilgilerini ilan etti [S1].
ZAMAN ÇİZELGESİ	Saklanan birkaç yanıt, iddia edilen olayı aynı biçimde anlatıyor. Tekrar görünürlüğü artırır; kaynağı veya yeni olayı bağımsız olarak doğrulamaz.
BELİRLENEN	Saklanan paylaşımda iddia edilen büyüklük ve alan türleri bulunuyor. Paket hem resmî doğrulamayı hem geniş haber kapsamını belirleyemediği için kuruluş adı verilmedi.
ALTERNATİF	Malzeme müşteriye, entegrasyona, tedarikçi dışa aktarımına veya başka kaynağa ait olabilir. Benzer alanlar tek başına etkilenen sistemi belirlemez.
SINIR	Teklif; ödeme işleme altyapısına, kart verisine veya banka ağına erişim göstermez. İlan edilen dosyanın indirildiğini veya satıldığını da göstermez.
YANIT	Satın alma ve uygulama sorumluları bu alanları tutan veri işleyenleri belirlemeli. Geniş hizmet kapatmasından önce kapsamı belirli olay kanıtı istemeli ve dışa aktarım yetkilerini gözden geçirmeli.

Sonuç

Ödeme sistemi olayı sonucu çıkarmadan veri işleyen akışını doğrulayın.

Kanıt kartı B02 24 Oca 2026

Paylaşanın takma adı verilmemiştir Forum Forum İngilizce

ÖZGÜN METİN

Full Names, Phone Numbers and Addresses.

ÇEVİRİ

Adlar ve soyadlar, telefon numaraları ve adresler.

Not. Bir ödeme yazılımı işletmesine atfedilen müşteri verileri.

Ortaya konan
93.000 kayıt iddiası ve ilan edilen veri alanları.

Ortaya konmayan
İşletmenin veya ödeme ağının anlatıldığı biçimde etkilenip etkilenmediği.

VAKA C

C

Taşınmaz kayıtları eski tarih etiketi taşıyor

Kanıt kartı B03 · 5 Şub 2026 · Forum · Taşınmaz kayıtları

İddia doğrulanmadı

İDDİA	5 Şubat tarihli teklif, 2023 etiketli taşınmaz verisi kümesini anlattı. İlan edilen sayı 97.972.190 kayıttı [S1].
ZAMAN ÇİZELGESİ	Paylaşım 2026 yılına, satıcının tarih etiketi daha eskiye ait. Bu tarihler farklı soruları yanıtlar ve ayrı tutulur.
BELİRLENEN	İlan ve başlıktaki kesin rakam elimizde. Paylaşım, bilgilerin ne zaman toplandığını veya ilk kez açıklandığını göstermez.
ALTERNATİF	Farklı dönemlerden veya kaynaklardan birleştirilen derleme, tekrarlanan kişi veya taşınmazlar içerebilir. Gerçek dosya da yanlış anlatılmış olabilir. Hiçbiri doğrulanmadı.
SINIR	Kayıtlar tekil taşınmaz sahipleri değildir. İddia, kamu sistemine güncel ayrıcalıklı erişim veya aktif sorgu hizmeti göstermez.
YANIT	Finans, taşınmaz ve müşteri hizmetleri ekipleri adres veya varlık bilgisini kimlik kanıtı kabul etmemeli. Değişiklikler ve işlemler için ayrı, güvenilir doğrulama kanalı istemeli.

Sonuç

Kimliği adres ve taşınmaz bilgisinden bağımsız doğrulayın.

Kanıt kartı B03 5 Şub 2026

Paylaşanın takma adı verilmemiştir Forum Forum İngilizce

ÖZGÜN METİN

Exact Records: 97,972,190

ÇEVİRİ

Tam kayıt sayısı: 97.972.190

Not. 2026 yılında paylaşılan, 2023 tarihli olarak sunulan taşınmaz verisi teklifi.

Ortaya konan
Taşınmaz verisi temalı ilan ve ilandaki sayı.

Ortaya konmayan
Kaynağı, güncelliği, tekil kişi sayısı veya güncel erişim.

D

VAKA D

Kimlik ve telefon teklifi doğrulanmamış kişi sayısı kullanıyor

Kanıt kartı B04 | 25 Eki 2026 | Forum | Kimlik ve iletişim

İddia doğrulanmadı

İDDİA	25 Ekim tarihli paylaşım, kimlik ve mobil telefon bilgisi ilan etti. Paylaşan kişi başlıktaki 201.593.023 rakamını kişi olarak tanımladı [S1].
ZAMAN ÇİZELGESİ	Daha eski saklanan ilanlar da büyük Türkiye temalı telefon veri kümeleri teklif etti. Benzer konular ortak dosya veya ortak kaynak göstermez.
BELİRLENEN	Başlıktaki rakam ve paylaşanın kullandığı birim gözlemlenebilir. Sayı, nüfus ölçümü veya Brandefense tahmini değildir.
ALTERNATİF	Tekrarlanan kimlikler, kişiye ait birden çok numara, birleştirilmiş eski kayıtlar veya yanlış pazarlama rakamı açıklayabilir. Hangisinin geçerli olduğu çıkarılmıyor.
SINIR	Tekil kişi toplamı, ulusal sisteme güncel erişim, eksiksizlik veya alıcı işlemi doğrulanmadı. İddianın büyüklüğü gerçekliğini çözmez.
YANIT	Gerçekçi kişisel bilgiler bilen bir arayana karşı hesap kurtarmayı sınayın. Dolandırıcılıkla mücadele ekipleri, doğru kimlik ayrıntılarının talep sahibini doğrulamadığını hizmet çalışanlarına hatırlatmalı.

Sonuç

Kişisel bilgiler bilen arayanlara karşı kurtarmayı sınayın.

Kanıt kartı B04 — 25 Eki 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | İngilizce

ÖZGÜN METİN

201,593,023 people.

ÇEVİRİ

201.593.023 kişi.

Not. İddia sahibi sayıyı kişi olarak tanımlıyor; bu birim doğrulanmadı.

Ortaya konan
Kimlik ve telefon verisi teklifindeki sayı.

Ortaya konmayan
Nüfus sayısı, tekil kişiler veya herhangi bir ulusal sisteme güncel erişim.

VAKA E

E

Finansal veri teklifi kimliklerle işlemleri karıştırıyor

Kanıt kartı B05 | 15 Kas 2026 | Forum | Finansal hizmetler

İddia doğrulanmadı

İDDİA	15 Kasım tarihli paylaşım, bir kripto varlık işletmesine atfedilen veri teklif etti. 12 Kasım görünümü, 13 tablo, yaklaşık 48 milyon satır ve 566.000 KYC kimliği iddia etti [S1].
ZAMAN ÇİZELGESİ	Görünüm tarihi satıcının açıklamasıdır. Bağımsız biçimde belirlenmiş veri alma tarihi değildir; paylaşım tarihi de güncel yetkisiz erişim kanıtı sayılmaz.
BELİRLENEN	İlan; kimlik, hesap ve işlem bilgileri dahil farklı grupları anlatıyor. Bunların toplamları birbirinin yerine geçmez.
ALTERNATİF	Eski dışa aktarım, test ortamı, birleşik kaynaklar veya uydurma ilan anlatıma benzeyebilir. Saklanan malzeme bunlardan birini doğrulamıyor.
SINIR	Doğrulama bilgisiyle ilgili alan adları, kullanılabilir sırları veya güncel hesap kontrolünü göstermez. Müşteri kaybı, bakiye, yetkisiz transfer veya tamamlanmış satış doğrulanmadı.
YANIT	Kimlik, dolandırıcılık, hukuk ve olay müdahalesi ortak bir doğrulama sorumlusu belirlemeli. Maruz kalma doğrulanırsa parolalarla birlikte oturumlar ve kurtarma yolları değerlendirilmeli; müşteriler ölçülü biçimde korunmalı.

Sonuç

Maruz kalma doğrulanırsa kimlik, oturum ve kurtarma kanıtını birlikte inceleyin.

Kanıt kartı B05 — 15 Kas 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | İngilizce

ÖZGÜN METİN

13 tables

ÇEVİRİ

13 tablo

Not. Farklı ölçü birimleri içeren kripto varlık işletmesi veri tabanı teklifi.

Ortaya konan

566k KYC kimliği, yaklaşık 48M satır ve 13 tablo iddiası taşıyan paylaşım.

Ortaya konmayan

Gerçeklik, geçerli hesap erişimi, kullanılabilir doğrulama bilgileri veya müşteri kayıpları.

VAKA F

F

VPN ilanı güncel erişim kanıtı gerektiriyor

Kanıt kartı B06 | 17 Kas 2026 | Forum | Hizmet sağlayıcılar

İddia doğrulanmadı

İDDİA	17 Kasım tarihli paylaşım, bir hizmet sağlayıcıyla ilişkili VPN erişimi teklif etti. İstenen fiyat 200 XMR idi [S1].
ZAMAN ÇİZELGESİ	İlan paylaşım tarihini ve istenen koşulları veriyor. Bağımsız doğrulanmış erişim tarihi, devir tarihi veya kalıcılık süresi vermiyor.
BELİRLENEN	İlan elimizde. İstenen para birimi ve tutar teklifin sunuluş biçimini gösterir; gerçekleşen piyasa fiyatını göstermez.
ALTERNATİF	Teklif, süresi dolmuş erişimi, sınırlı hesabı, yanlış şirket özelliklerini veya uydurma iddiayı anlatıyor olabilir. Paylaşım bunları dışlamıyor.
SINIR	Etkilenen kuruluş, geçerli kimlik bilgileri, yetki düzeyi ve müşterilere etkisi doğrulanmadı. Rapor, kuruluşu tanıtabilecek iş özelliklerini vermiyor.
YANIT	Uzaktan erişim sorumluları güvenilir yeni sinyalleri hesap geçerliliği, cihaz kimliği ve yakın tarihli oturumlarla karşılaştırmalı. Eşleşen yetkisiz faaliyeti üst incelemeye taşımalı; eşleşmeyen iddianın kapanma nedenini kaydetmeli.

Sonuç

Erişim tekliflerini aktif hesaplar ve yakın VPN oturumlarıyla karşılaştırın.

Kanıt kartı B06 — 17 Kas 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | İngilizce

ÖZGÜN METİN

price:200 xmr

ÇEVİRİ

fiyat:200 xmr

Not. Erişim teklifi doğrulama için bir ipucudur.

Ortaya konan
Hizmet sağlayıcı VPN erişimi ilanı ve istenen fiyat.

Ortaya konmayan
Kuruluşun kimliği, geçerli erişim, satış veya müşterilere etkisi.

VAKA G

Düzenleyicide tutulan belgeler, adı geçen her şirkette olay yaşandığını göstermez

İddia doğrulanmadı

Kanıt kartı B15 | 21 Kas 2026 | Mesajlaşma kanalı | Mali düzenleme

İDDİA	21 Kasım tarihli mesajlaşma paylaşımı, bir mali düzenleyici kurumun belgelerine erişim iddia etti. On binlerce kurum içi dosya ve şirket mali bildirimleri içeren büyük bir arşiv tarif etti; daha küçük bir bölümün sunulduğunu öne sürdü [S1].
KRONOLOJİ	Paylaşım, raporun kesim gününe denk geliyor. Tarihi, saldırı veya dışarı aktarım tarihini bağımsız olarak göstermez. Yeni iddia, doğrulanmış olay sayısına dönüşmeden hızla değerlendirilmelidir.
ORTAYA KONAN	Saklanan anlatım; düzenleyici kararları, denetim raporları, yazışmalar, mali raporlar ve bilgi işlem hesaplarının e-postalarını tarif ediyor. Bunlar paylaşanın tanımlarıdır. Rapor, dosyaları veya kaynaklarını doğrulamadı.
ALTERNATİF	Düzenleyicide tutulan bir arşiv, birçok kuruluşun başvurularını içerebilir. Bunların bulunması, başvuran her şirketin sistemine erişildiğini göstermez. Yeniden paketlenmiş malzeme, karışık arşiv veya yanlış tanımlar olasıdır.
SINIR	Hazırlık sırasında eşleşen resmî açıklama doğrulanamadı. Giriş yolu, güncel erişim, belgelerin gerçekliği ve etkilenen kişi kapsamı doğrulanmamıştır. Siyasi söylem ile iddia edilen hedefin ve belgelerdeki tarafların adları çıkarıldı.
YANIT	Düzenleme, hukuk ve finans hizmetleri sorumluları, güvenilir belge sinyalini kendi başvuru kayıtları ve yazışma kontrolleriyle karşılaştırmalıdır. Kaynak kanıtını koruyun. Paylaşanın andığı her firma için olay ilan etmeyin.

Sonuç

Belgenin kaynağını doğrulayın; başvuran her firmada olay olduğu sonucuna varmayın.

Kanıt kartı B15 21 Kas 2026

Paylaşanın takma adı verilmemiştir Mesajlaşma kanalı Telegram Türkçe

ÖZGÜN METİN

kurum içi dosya

Not. Düzenleyici belgesi iddiası; doğrulanmış dışarı aktarım veya adı geçen her şirkette olay göstermez.

Ortaya konan
Düzenleyici belge koleksiyonunu anlatan saklanmış paylaşım.

Ortaya konmayan
Gerçek belgeler, güncel sistem erişimi, giriş yolu veya başvuran firmalarda ayrı olaylar.

VAKA H

H ■ Pompa kontrolüne müdahale iddiası ayrı doğrulama gerektiriyor

İddia doğrulanmadı

Kanıt kartı B16 | 13 Mar 2026 | Mesajlaşma kanalı | Süreç kontrol sistemleri

İDDİA	13 Mart tarihli bir kanal paylaşımı, pompa istasyonu ve üretim tesisi kontrol paneline müdahale edildiğini öne sürdü. Olumsuz süreç davranışı ve operatör kontrolünün kaldırıldığını iddia etti [S1].
ZAMAN ÇİZGİSİ	Tarih, yayımlanmayı gösterir. Sisteme giriş, kontrol değişikliği veya fiziksel etki için bağımsız olarak belirlenmiş zaman bulunmuyor.
ORTAYA KONAN	Saklanan paylaşım birinci kişi ağzından iddia içeriyor. Paylaşımı yapan kişinin müdahaleyi gerçekleştirdiği ortaya konmadı. Ülke çerçevesi fiziksel tesisin yerini doğrulamıyor.
ALTERNATİF	Yeniden paylaşım, yanlış sunum, eski materyal veya ilgisiz test arayüzü olasılıkları sürüyor. Süreç davranışının anlatılması, müdahaleyi bağımsız olarak göstermiyor.
SINIR	Hedefin sahibi, erişim yolu, sistem değişiklikleri ve operasyonel sonuç doğrulanmadı. Siyasi söylem çıkarıldı. Üçüncü taraf kontrol sistemi denenmedi.
YANIT	İlgili varlık sahipleri, inandırıcı iddiayı yetkili uzaktan erişim kayıtları, mühendislik değişiklikleri ve operatör kanıtlarıyla karşılaştırmalı. Çelişen kanıtı koruyun. Yetkisiz değişiklik desteklenirse süreç güvenliği sorumlusunu değerlendirmeye katın.

Sonuç

Fiziksel süreç olayı açıklamadan önce yetkili mühendislik faaliyetini doğrulayın.

Kanıt kartı B16 — 13 Mar 2026

Paylaşan kişi belirlenmedi | Mesajlaşma kanalı | Telegram | İngilizce

ÖZGÜN METİN

the control panel for the pumping station and industrial facility.

ÇEVİRİ

pompa istasyonu ve üretim tesisinin kontrol paneli.

Not. Kanal anlatımı kontrol paneline müdahale iddia ediyor; müdahaleyi yapan kişi ve hedef doğrulanmadı.

Ortaya konan
Tarihli paylaşım ve iddiası.

Ortaya konmayan
Sistem erişimi, kontrol değişikliği, kesinti, fiziksel etki veya işleten kimliği.

VAKA I

Enerji erişimi ilanı operasyonel kontrolü ortaya koymuyor

Kanıt kartı B17 | 22 Eyl 2026 | Forum | Enerji hizmetleri

İddia doğrulanmadı

İDDİA	22 Eylül tarihli forum ilanı, bir enerji hizmeti şirketine ait olduğu öne sürülen çeşitli sistemlerden veri çıkarma teklifi sunuyor. Paylaşan kişi; süren çalışma ilişkisi, birden fazla erişim noktası ve fidye yazılımı faillerini ilgilendirebilecek zayıflıklar iddia ediyor [S1].
ZAMAN ÇİZGİSİ	Tarih, yayımlanmayı gösteriyor. Veri edinme, hesaba giriş veya yetki değişikliği tarihi bağımsız olarak belirlenmedi. Süren ilişki iddiası, yetkisiz erişimin sürdüğünü ortaya koymuyor.
ORTAYA KONAN	Saklanan metin erişim teklifi içeriyor. Kısa bir kanıt etiketi, doğrulanmış gösterim sağlamıyor. Paylaşanın ilişkisi, yetkisi ve ilan ettiği ayrıcalıklar doğrulanmadı.
ALTERNATİF	Eski, üçüncü tarafa ait, yetkili veya yanlış sunulan erişim olasılıkları sürüyor. Metin, paylaşanı fidye yazılımı grubuna bağlamıyor veya işlem yapıldığını ortaya koymuyor.
SINIR	Kurumsal sisteme ilişkin iddia; elektrik sisteminin kontrolü, hizmet kesintisi veya fiziksel etki kanıtı değildir. Rapor, bu teklifi Vaka H'ye veya diğer kontrol paneli iddialarına bağlamıyor.
YANIT	İlgili hizmet sahibi, inandırıcı hesap ve tedarikçi ayrıntılarını yetkili uzaktan erişim ve bakım kayıtlarıyla karşılaştırmalı. Çelişen kanıtı koruyun. Desteklenen yetkisiz erişimi olay müdahalesine taşıyın. Etkilenen hizmet gerektiriyorsa operasyonel güvenliği ayrıca kontrol edin.

Sonuç

Operasyonel kontrol sonucu çıkarmadan hizmet erişimini ve yetkili ilişkileri doğrulayın.

Kanıt kartı B17 22 Eyl 2026

Takma ad gizlendi Forum Forum İngilizce

ÖZGÜN METİN

I have various access points and vulnerabilities.

ÇEVİRİ

Çeşitli erişim noktalarım ve zafiyetlerim var.

Not. Enerji hizmetine erişim ilanı; iddia, güncel erişimi veya operasyonel kontrolü doğrulamıyor.

Ortaya konan
Tarihli ilan ve öne sürdüğü teklif.

Ortaya konmayan
Doğrulanmış çalışma ilişkisi, yetkiler, güncel erişim, fidye yazılımı bağlantısı veya fiziksel etkiler.

4.6 Talep, eski malzeme ve hassas iddialar

B10, 2023 yılına ait malzemenin yeniden paylaşımı olduğunu açıkça söylüyor. Doğrudan bir tarihleme uyarısıdır. Yeni görünür olan konu, 2026 yılında yeni olaya kanıt eklemese de dolandırıcılık takibi gerektirebilir.

B11, bir siyasi kuruluşa atfedilen bir milyonu aşan üyelik kaydı ilan ediyor. İddia doğrulanmamıştır. Kuruluşun kimliği ve aktörün yüklü dili çıkarıldı. Kanıt, siyasi veya devlet atfı yapmadan veri doğrulama görevini destekler.

B12, 2012–2026 dönemini kapsadığı söylenen iş belgelerini ilan ediyor. Belirtilen dönem, yetkisiz erişimin tarihini göstermez. Uzun belge geçmişi ile yeni paylaşım, güncel erişim kanıtlamadan birlikte bulunabilir [S1].

Kanıt kartı B10 13 Kas 2026

Paylaşanın takma adı verilmemiştir

Forum | Forum | İngilizce

ÖZGÜN METİN

it is from 2023

ÇEVİRİ

2023 yılına ait

Not. Paylaşan kişi açıkça yeniden paylaşım yaptığını söylüyor.

Ortaya konan
Malzemeyi eski olarak tanımlayan 2026 paylaşımı.

Ortaya konmayan
2026 yılında yeni bir olay veya dosyanın gerçekliği.

Kanıt kartı B11 5 Kas 2026

Paylaşanın takma adı verilmemiştir

Forum | Forum | İngilizce

ÖZGÜN METİN

The database contains [...] member information

ÇEVİRİ

Veri tabanı [...] üye bilgisi içeriyor

Not. Bir milyonu aşan üyelik kaydına ilişkin doğrulanmamış teklif; aktör söylemi ve tanımlayıcılar çıkarıldı.

Ortaya konan
Üyelik verisi iddiası; doğrulanmış siyasi veya teknik atıf değil.

Ortaya konmayan
Gerçeklik, kaynak sistem, etkilenen kişiler veya siyasi destekçi.

Kanıt kartı B12 17 Eki 2026

Paylaşanın takma adı verilmemiştir

Forum | Forum | İngilizce

ÖZGÜN METİN

Sales documents covering 2012-2026.

ÇEVİRİ

2012-2026 dönemini kapsayan satış belgeleri.

Not. Uzun bir dönemi kapsadığı söylenen iş belgesi paylaşımı iddiası.

Ortaya konan
İş kayıtlarını ilan eden paylaşım.

Ortaya konmayan
Güncel yetkisiz erişim, eksiksizlik veya diğer tekliflerle ortak kaynak.

4.7 Olay ekibi neyi saklamalı?

Güvenilir her dış iddia için gözlem zamanını, öne sürülen sonucu, kaynak türünü ve kanıt sorumlusunu iç kayıtta tutun. Kanıtı hukuka uygun koruyun; kişisel bilgiyi en aza indirin. Doğrulama için malzeme satın almayın veya ilan edilen erişimi denemeyin.

Yararlı bir sonuç kaydı neyin değiştiğini açıklar. Doğrulama sonrası aktif hesabın kapatılması, veri işleyenin etkilenen müşteriyi belirlemesi, eski olayın zaten düzeltilmiş olması veya destekleyici kanıt eksikliği örneklerdir.

TEMEL ÇIKARIMLAR

01
Paylaşım ve temel olay tarihlerini ayrı tutun.

02
Büyük veri kümesi rakamları tekil kişileri, güncel erişimi veya kaybı göstermez.

03
Güvenilir her iddiaya doğrulama sorumlusu ve kayıtlı sonuç atayın.

BÖLÜM 05

Sektörlere göre hedefleme örnekleri

05

BU BÖLÜMÜN YANITLADIĞI SORU

Doğrulanan açıklamalar ve doğrulanmamış teklifler sektör kararlarına nasıl dönüşür?

3

ayrı tutulması gereken kanıt türü

5.1 Sektör karar tablosu 39

5.2 Fidye yazılımı ve veri aktarımı farklı sonuçlardır 40

5.3 Parola yolunun belirtildiği posta kutusu vakası 40

5.4 Tedarikçi bildirimleri tek kampanya olarak toplanamaz 41

5.5 Ek bildirimler müdahale önceliklerini netleştiriyor 41

5.6 Yanıtı da iddia kadar dikkatle okuyun 42

BÖLÜM 05

Sektörlere göre hedefleme örnekleri

KISACA

Resmî açıklamalar, genel maruz kalma rakamlarının gösteremediği somut hata yollarını ortaya koyuyor. Farklı sektörlerde fidye yazılımını, hesap kötüye kullanımını ve veri işleyen olaylarını anlatıyor. Karanlık ağ iddiaları inceleme ipucu ekliyor. Sayıları resmî bildirimlerdeki olası etki gruplarıyla karşılaştırılamaz. Her sonuç için en güçlü kanıtı kullanın; sektör sorumlusuna belirli doğrulama görevi verin.

5.1 Sektör karar tablosu

Tablo, gözlemlenen sonucu yanıta bağlar. Sektörleri sıralamaz veya etkilenen kuruluş oranı tahmin etmez.

Sektör	Kanıt	Anlamı	İlk sorumlu
Eğitim	Resmî fidye yazılımı bildirimi ve veri sorumlusunun açıklaması [S12][S13]	Kurtarma ve veri aktarımı farklı kanıt gerektirir	Altyapı ve gizlilik
Kamu hizmetleri	Parolayla posta kutusu kötüye kullanımı [S15]	Oturumları, kuralları, aktarımları ve güvenilen gönderimleri inceleyin	Kimlik ve mesajlaşma
Perakende	Tahmini müşteri etkisi içeren veri işleyen olayı [S16]	Tedarikçi bilgisi, veri sorumlusunda inceleme başlatabilir	Satın alma ve gizlilik
Finansal hizmetler	Yabancı veri işleyende oltalama; aktarım doğrulanmadı [S17]	Tedarikçi kimlik kontrollerini ve zaman çizelgesini doğrulayın	Tedarikçi riski ve kimlik
Eğitim hizmetleri	Çocuklara ilişkin kayıtları içeren fidye yazılımı bildirimi [S18]	Kurtarma ve dikkatli bildirim ortak sorumluluk gerektirir	Hizmet ve gizlilik
Gıda perakendesi	Veri işleyende kütüphane istismarını anlatan bildirim [S19]	Üçüncü taraf uygulama bağımlılıklarını inceleyin	Uygulama güvenliği
E-ticaret	Müşteri ve yönetici hesabı grupları [S20]	Kullanıcı gruplarını ve yönetici erişimini ayırın	Platform sorumlusu
Üyelik hizmetleri	Kimlik ve parola alanları içeren tedarikçi bildirimi [S21]	Kişisel bilgiler taklidi kolaylaştırabilir	Kimlik ve gizlilik
Perakende hizmetleri	Çalışan ve müşteri kategorileri içeren tedarikçi bildirimi [S22]	Olay, çalışan ve müşteri iş akışlarına yayılabilir	Hizmet sorumlusu
Yemek teslimatı	Etkilenen grubu hâlâ incelenen erişim olayı [S23]	İnceleme sonuçlanana kadar müşteri etkisini açık tutun	Olay müdahalesi
İmalat	Fidye yazılımı listelemeleri ve belge iddiaları [S1][S3]	Listelemeler süreklilik hazırlığı gerektirir; doğrulanmış sızma sayısı vermez	Operasyon ve kurtarma

Sektör	Kanıt	Anlamı	İlk sorumlu
Bankacılık	Hesap temini ve promosyon listesi teklifleri [S1]	Dolandırıcılık kontrolleri müşteri kimliği kötüye kullanımını kapsamalı	Dolandırıcılıkla mücadele ve kimlik
Enerji hizmetleri	Doğrulanmamış çoklu sistem erişimi teklifi, Vaka I [S1]	Kurumsal erişim, operasyonel kontrol veya fiziksel etki ortaya koymaz	Hizmet sahibi ve operasyonel güvenlik

5.2 Fidye yazılımı ve veri aktarımı farklı sonuçlardır

KVKK'nın 7 Ekim bildirimi, Yıldız Teknik Üniversitesinin sanallaştırma altyapısının ve üzerindeki sunucuların fidye yazılımından etkilendiğini anlattı. Yaklaşık 140.000 öğrenci ve 4.500 personelin etkilenmiş olabileceğini bildirdi. Ziyaretçi sayısı ile etkilenen kişisel veri kategorileri belirsizdi [S12].

Üniversitenin 8 Ekim açıklaması, 1 Ekim saldırısını doğruladı ve veri aktarımına ilişkin bulgu bulunmadığını söyledi [S13]. NTV, 8 Ekim tarihinde olayı haberleştirdi [S14]. Bu birleşim, vaka için paketin ad kullanma kuralını karşılar.

Soru	Resmî bildirim	Veri sorumlusunun açıklaması	Değerlendirme
Altyapı etkilendi mi?	Fidye yazılımı sanallaştırmayı ve sunucuları etkiledi [S12]	Bilgi işlem altyapısına saldırı doğrulandı [S13]	Resmen bildirilmiş olay
Olası etki grubu?	Yaklaşık öğrenci ve personel rakamları; ziyaretçiler belirsiz [S12]	Yeni grup rakamı verilmedi [S13]	Bildirimin sınırlamalarını koruyun
Veri aktarıldı mı?	Etkilenen kategoriler belirsiz [S12]	Süren incelemede aktarım bulgusu yok [S13]	Bu kaynaklarla aktarım belirlenmiş değil
Aktör ve giriş yolu?	Belirtilmedi [S12]	Belirtilmedi [S13]	Atıf veya giriş yolu sonucu yok

Operasyon yanıtı iki yoldan ilerlemelidir. Hizmetleri kurtarın ve bütünlüğü doğrulayın. Ayrı olarak günlükleri koruyun, aktarım kanıtını inceleyin ve gizlilik değerlendirmesini güncelleyin. Kurtarma duyurusu veri aktarımını yanıtlamaz; olası etki grubu da herkesin verisinin sistemden çıktığını göstermez.

5.3 Parola yolunun belirtildiği posta kutusu vakası

Belediye bildirimi, 30 Eylül tarihinde olağan dışı e-posta gönderiminin tespit edildiğini söylüyor. Erişimi önceden ele geçirilmiş parolaya bağlıyor. İki posta kutusunun içeriğinin aktarılmasını, silme kurallarını, toplu spamı ve değişen ileti ayarlarını da bildiriyor [S15].

Bu, kamu alan adını anan ilandan daha güçlü ve belirli kimlik hatası kanıtıdır. Yine de parolanın nasıl alındığını belirtmez. Eksik adıma bilgi hırsızı yazılım, oltalama kiti veya devlet bağlantılı aktör eklemeyin.

Yanıt; oturumları, kuralları, yetki devrini, dış gönderim kötüye kullanımını ve etkilenen yazışma taraflarını kapsamalıdır. Parola sıfırlamak, yetkisiz yönlendirme kuralının veya aktif oturumun kaldırıldığını tek başına göstermez. Kapanışı mesajlaşma sorumlusuyla doğrulayın.

5.4 Tedarikçi bildirimleri tek kampanya olarak toplanamaz

Bir perakende bildirimi, veri işleyen sunucusuna yetkisiz erişim sonrasında 323.052 kişinin etkilenmiş olabileceğini tahmin etti. Gıda perakendecisi bildirimi, veri işleyendeki üçüncü taraf kütüphanesinin istismarını ve 67.193 kişiyi anlattı [S16][S19]. Benzer tedarikçi dili, ortak veri işleyen veya sızma göstermez.

Bir e-ticaret bildirimi ayrıca 592 nihai müşteri ve 4 yönetim paneli kullanıcısı belirtti. Mücevher perakendecisi bildirimi 964 kişi verdi. Dernek bildirimi en fazla 9.462 üye belirtti [S20][S21][S22]. Bunlar farklı sınırlamaları olan bildirime özgü gruplardır. Ulusal tekil kişi toplamında birleştirilmezler.

Ortak savunma sorusu sözleşmesel ve operasyoneldir: Veri sorumlusu, veri işleyen olayının hangi veri, hesap ve müşteriyi kapsadığını hızla belirleyebiliyor mu? Yanıt için güncel veri haritası, çalışan iletişim yolu ve kapsamı belirli kanıtların korunması gerekir.

5.5 Ek bildirimler müdahale önceliklerini netleştiriyor

Üyelik hizmeti sunan bir oda, 2 Kasım tarihinde saptanan SQL enjeksiyonunun ardından üyelik veri tabanına erişildiğini ve verilerin dışarı aktarıldığını bildirdi. Genel muhasebe sisteminin etkilenmediğini belirtti [S45]. Bu sınır önemlidir: uygulama güvenliği ve mahremiyet ekipleri etkilenen veri tabanına ilişkin kanıtları toplarken kuruluş, komşu sistemleri ayrıca kontrol etmelidir. Tüm iş sistemlerinin etkilendiği iddiası, bildirimin kapsamını aşar.

Bir liman işletmesi, tedarikçinin yardım masasında erişim kontrolünün aşılmasını ve ardından parola değişikliklerini bildirdi. İlk etkilenen kişi sayısı 855 idi [S39]. Böbrek sağlığı hizmetleri bildirimi, çalışana yönelik sesli oltalamayı, bir hesabı, CRM sistemini ve kurum içi rehber dosyasını anlattı [S47]. Uluslararası bir ilaç işletmesinin bildirimi ise alt veri işleyende bilgi işlem çalışanı taklidiyle yapılan sesli oltalamayı anlattı [S49]. Bunlar ayrı açıklanmış yollardır. Ortak aktör ortaya koymadan, yardım masasında kimlik doğrulamanın ve devredilmiş bulut erişiminin kontrolünü destekler.

Müşteri hizmetleri bildirimleri, kişilerle tutulan görüşmeleri de ayırıyor. Teknik destek bildirimi, kişi sayısı belirsiz olan 624 sohbet kaydıyla ilgiliydi [S41]. Otomotiv bildirimi, yine kişi sayısı belirlenmemiş 8.268 sohbet kaydını kapsıyordu [S64]. Spor ürünleri perakendecisi ise 383 kişiye ilişkin 541 sohbet kaydını ayrı ayrı bildirdi [S76]. Bir görüşme birkaç kişiyi içerebilir veya aynı kişiyi tekrarlayabilir. Dönüşüm katsayısı uygulanmıyor.

Kayıtların yaşı ayrı bir konudur. E-ticaret bildirimi, 9.882 kişiye ilişkin 2022 tarihli sohbet kayıtlarını anlattı [S43]. Teslimat bildirimi, aynı yıldan 3.217 kişiye ilişkin kayıtları anlattı [S70]. Bu tarihler kayıtları nitelendirir. Sigorta şirketinin Kasım bildirimi ise yetkisiz erişimin kendisini açıkça 2022 yılına yerleştirdi [S44]. Rapor, bu sigorta bildirimini geçmiş faaliyetin açıklanması olarak ele alır; yeni bir 2026 saldırısı olarak sunmaz.

Uluslararası bildirimler başka bir sınır gerektiriyor. Lojistik grubunun bildirimi, Türkiye'de etkilenen 10.622 çalışanı belirtti [S56]. Otel grubunun bildirimi ise tamamının Türkiye'de olduğunu ortaya koymadan 9.550 müşteri bildirdi [S79]. Türk makamınca yayımlanması, yabancı veri sorumlularının her nüfusunu yalnızca Türkiye'ye ait sayıya dönüştürmez. Ek E, bu sınırlamaları ve kaynağı okunmuş diğer bildirimleri kaydeder.

5.6 Yanıtı da iddia kadar dikkatle okuyun

Memurlar.net'te yayımlanan 4 Kasım tarihli hava yolu işletmesi açıklaması, kurum içi destek sistemindeki açığın kapatıldığını belirtti. Açıklamaya göre sistemler uygulama geliştirmeye hizmet ediyordu, misafir veri tabanlarını içermiyordu ve uçuş operasyonlarında kullanılmıyordu [S80]. Bu, şirketin sistem kapsamına ilişkin ne söylediğini ortaya koyar. Rapor, ilan edilen veri miktarını, dışarı aktarımı veya iddia edilen müşteri etkisini bağımsız olarak doğrulamamıştır.

Düzenleyicinin 11 Kasım bildirimi, daha dar kapsamlı doğrulanmış bir bildirim sunuyor: hava yolu işletmesinin bilgi teknolojileri talep ve geliştirme sisteminde yönetici parolasının yetkisiz kullanımı. Faaliyet başlangıcı 12 Ekim, tespit 26 Ekim olarak veriliyor; 11.762 çalışan ve kullanıcı etkilenmiş [S90]. Parolanın nasıl alındığı belirsizdi. Çalışanlar ve sistem kullanıcıları, yolculardan farklı bir nüfustur; bildirim, ilan edilen müşteri verisi iddiasını doğrulamaz.

Soru	Kamuya yansıyan veri iddiası	Veri sorumlusunun yanıtı ve resmî bildirim	Değerlendirme
Destek sistemine erişim	Bir ilan veri sahibi olunduğunu iddia ediyor	Geliştirme sisteminde yönetici parolasıyla erişim bildirildi [S90]	Bildirim, açıklanmış bir sistem olayı ortaya koyar
Yolcu veya uçuş sistemleri	Daha geniş müşteri etkisi iddia ediliyor	Şirkete göre misafir veri tabanları ve uçuş operasyonları bu sistemlerin dışındaydı [S80]	Bağımsız doğrulanmış yolcu sistemi etkisi yok
Parolanın kaynağı	Doğrulanmış yol yok	Bildirimde belirlenmemiş [S90]	Oltalama, bilgi çalan yazılım veya içeriden kişi sonucu çıkarılmamalı

İletişim makamının 10 Haziran açıklaması, çevrim içi kamu hizmetindeki sorun için saldırı açıklamasını reddetti; yoğunluk ve teknik çalışmaları gerekçe gösterdi [S81]. Bu, kaynağa atfedilen bir anlatımdır. Ne iddia ne de yalanlama, bağımsız hizmet ve adli bilişim kanıtının yerini alır.

Bir elektronik haberleşme bildirimi özeti, faaliyet başlangıcını 10 Ocak, keşfi 26 Ocak olarak tarihlendiriyor [S83]. Bu paket için asıl bildirim okunmadı. Kişi sayısı, kaynağı okunmuş resmî kayda eklenmiyor. Önceki arşivin kapsamı eksik kalıyor.

18 Eylül tarihli ayrı bir hukuk değerlendirmesi, 16 Eylül'de yayımlanan 27 veri sorumlusu bildirimini aynı e-ticaret altyapısı sağlayıcısıyla ilişkilendiriyor. Kurumsal yazılım hizmetine ilişkin 1 ayrı bildirimi de bu gruptan ayırıyor [S93]. Bu, rapor için okunan asıl bildirimlerden ayrı bir ikincil değerlendirmedir.

Değerlendirme, ayrı olayda Türkiye'deki 424 kuruluş veya birimle ilişkili verileri bildiriyor. Kuruluşlar; kişi, hesap veya bağımsız olarak ortaya konmuş sızmalar değildir. Rapor, değerlendirmedeki birleşik kişi toplamını benimsemiyor. Veri sorumlularının kişi grupları örtüşebilir; birkaç kuruluşun toplamı da belirsizdir [S93].

Bu eski bildirim grubu, her veri sorumlusunun hizmet ilişkisini ve kanıt sınırını koruma gereğini destekliyor. Eşleşen kanıt olmadan daha sonraki tedarikçi bildirimlerine bağlanmıyor. Önceki asıl bildirimlere erişim boşlukları kapsam kaydında görünür kalıyor [S93].

TEMEL ÇIKARIMLAR

01
Hizmet kurtarmayı olası veri aktarımının incelenmesinden ayırın.

02
Parolayla posta kutusuna erişim, parolanın nasıl alındığını göstermez.

03
Benzer tedarikçi bildirimleri ortak kampanya veya ayrık ulusal toplam kanıtı değildir.

BÖLÜM 06

Haktivizm ve DDoS

06

BU BÖLÜMÜN YANITLADIĞI SORU

Duyuru ne zaman hazırlık gerektirir, ne zaman kesinti gösterir?

1

hedef seçme niyetine ilişkin saklanan duyuru

6.1 Farklı kanıt türlerinin zaman çizelgesi 45

6.2 Niyet duyurusu kesinti ölçümü değildir 45

6.3 İddiayı büyütmeden hazırlık 46

6.4 Belirsizlik sırasında iletişim 47

6.5 Sistem kontrolü iddiaları operasyonel kanıt gerektiriyor 47

BÖLÜM 06

Haktivizm ve DDoS

KISACA

Saklanan bir kanal duyurusu Türkiye'de hedef seçme niyetini anlatıyor. Daha sonraki paylaşım, araç kanalına katılım ilan ediyor. Hiçbiri tamamlanmış DDoS saldırısı göstermiyor. Bu paylaşımlarla eşleşen doğrulanmış resmî kesinti açıklaması raporda yok. Aktör, gerekçe veya etki hakkında desteklenmeyen sonuçlar üretmeden, bu malzemeyle hazırlığı ve hizmet kanıtını kontrol edin.

6.1 Farklı kanıt türlerinin zaman çizelgesi

Çizelge; iddiaları, resmî açıklamaları ve yayım tarihlerini özellikle ayırır. Olaylar arasında ilişki öne sürmez [S1][S12] [S13][S15][S24].

1 Eki 2026	**Üniversite olayı** Üniversite ve KVKK tarafından sonradan bildirilen olay tarihi [S12][S13]
7 Eki 2026	**Kişisel veri otoritesi** Fidye yazılımı bildirimi yayımlandı; olası etki grubu sınırlı ifadeyle verildi [S12]
8 Eki 2026	**Üniversite açıklaması** Süren incelemede veri aktarımı bulgusu bulunmadı [S13]
21 Eki 2026	**Ulusal siber otorite** PHP açıklarına ulusal yanıt duyuruldu [S24]
7 Kas 2026	**TunisianMaskers adını kullanan kanal** Türkiye'de banka veya şirket seçme niyeti; doğrulanmış saldırı değil [S1]
20 Kas 2026	**Araç kanalı paylaşımcısı** Veri ve DDoS anılan katılım ilanı; gösterilmiş hizmet sonucu yok [S1]

6.2 Niyet duyurusu kesinti ölçümü değildir

B13, TunisianMaskers adını kullanıyor ve banka veya şirket düşünüldüğünü söylüyor. Doğrulanmış hedef belirtmiyor. Dili ileriye dönük. Bu nedenle rapor, girişim veya başarılı saldırı saymadan duyuruyu kaydediyor [S1].

Ad, kanalın arkasındaki kişilerin konumunu, uyruğunu, kimliğini veya destekçisini göstermez. Burada böyle atıf yapılmıyor.

Kanıt kartı B13 7 Kas 2026

TunisianMaskers adını kullanan kanal Mesajlaşma kanalı

Telegram İngilizce ve Arapça

ÖZGÜN METİN

we think about bank or company

ÇEVİRİ

bir bankayı veya şirketi düşünüyoruz

Not. TunisianMaskers adını kullanan kanal niyet bildiriyor.

Ortaya konan

7 Kasım duyurusu.

Ortaya konmayan

Saldırı girişimi, belirli hedef, kesinti süresi veya hizmet etkisi.

Kanıt kartı B14 20 Kas 2026

Paylaşanın takma adı verilmemiştir Mesajlaşma kanalı

Telegram Türkçe

ÖZGÜN METİN

Aktif tool kanalına alım vardır

Not. Araç kanalına katılım ilanı; belirli bir kuruluşa saldırı kanıtı değil.

Ortaya konan

Veri ve DDoS sözcüklerini içeren katılım ilanı.

Ortaya konmayan

Araç kabiliyeti, kullanımı, işletenin kimliği veya B13 ile bağlantı.

Nokta	Kanal açıklaması	Resmî açıklama	Kanıt sınırı
Hedef	Türkiye'de banka veya şirket düşünülüyor, B13	Eşleşen açıklama doğrulanmadı	Kuruluş düzeyinde atıf yok
Faaliyet	DDoS başlatma niyeti	Eşleşen açıklama doğrulanmadı	Girişim belirlenmiş değil
Süre	Paylaşımda süre yer alıyor	Eşleşen açıklama doğrulanmadı	Gözlemlenmiş kesinti değil
B14 ilişkisi	Ayrı araç kanalı katılım ilanı	Eşleşen açıklama doğrulanmadı	Ortak işleten veya kampanya belirlenmedi

6.3 İddiayı büyütmeden hazırlık

Güvenilir tehdit duyurusu; azaltım bağlantılarının, kapasitenin ve hizmet izleme tabanının kontrolünü gerektirebilir. Kendiliğinden kamuya ihlal açıklaması başlatmamalıdır. Hizmet sorumluları kullanıcıya görünen erişilebilirlik ve bağımlılık durumu dahil uygulama düzeyinde kanıt istemelidir.

Site sorunu; tedarikçi kesintisi, yapılandırma değişikliği veya başka operasyon hatasından da kaynaklanabilir. Kesintiyi bir aktöre bağlamadan trafiği, uygulama sağlığını ve sağlayıcı bilgisini ilişkilendirin. Olay kaydında alternatifleri açık tutun.

6.4 Belirsizlik sırasında iletişim

Hizmet erişilebilirliği ve veri gizliliği için ayrı açıklamalar kullanın. Kamu sayfası, veri erişimi kanıtı olmadan kullanılamaz hâle gelebilir. Kamu hizmetleri çalışırken hesap veya veri kümesi iddiası inceleme gerektirebilir.

Aktör siyasi konuya atıf yaptığında, hazırlık için gerekliyse bunu iç kayıtta aktörün çerçevesi olarak tutun. Hakareti tekrarlamayın, açıklamayı benimsemeyin veya hükûmet kararını kanıtlanmış neden gibi sunmayın.

6.5 Sistem kontrolü iddiaları operasyonel kanıt gerektiriyor

Mayıs ayındaki ayrı bir paylaşım, Türkiye'de ve başka bir pazarda bankaların hedef alındığını öne sürüyor. Bağımsız olarak doğrulanmış yöntem, kesinti veya kayıp sunmuyor. Bu iddia, tamamlanmış DDoS olayı olarak sayılmıyor [S1].

F58'deki nisan tarihli telekomünikasyon iddiası ve F59'daki ekim tarihli uzaktan panel iddiası, web sitesi kesintisinden farklı doğrulama gerektiriyor. Kontrol değişikliği veya fiziksel sonuç ortaya koymuyorlar. Vaka H ile ilişki kurulmadı. İlgili sahipler uzaktan erişim ve mühendislik kayıtlarını korumalı, yetkili çalışmaları karşılaştırmalı. Kanıt yetkisiz faaliyeti destekliyorsa operasyonel güvenlik çalışanları sürece katılmalı [S1].

TEMEL ÇIKARIMLAR

01
Duyurulan niyet, saldırı girişimi göstermez.

02
Hizmet etkisini iddialardan ve iddia edilen sürelerden ayrı doğrulayın.

03
Aktörün çerçevesini ve siyasi atfı kaynağına bağlı tutun.

BÖLÜM 07

Tehdit aktörleri ve desteklenen ilişkiler

07

BU BÖLÜMÜN YANITLADIĞI SORU

Hangi aktör ilişkileri destekleniyor, atıf nerede duruyor?

3

ayrı yol: listelemeler, kampanya araştırması ve kanal iddiaları

7.1 İlişki haritası 49
7.2 Fidye yazılımı listelemeleri ve grup yoğunlaşması 50
7.3 Üretici araştırmasında yerel odaklı fidye yazılımı kampanyası 54
7.4 Ülkeye özgü sınırı koruyan casusluk araştırması 55
7.5 Kanal kimliği ve paylaşımcı etiketleri 56
7.6 FortiBleed: ülke etiketli cihazlar ve kurtarma kanıtı 57
7.7 Sanallaştırma yönetimi: ülke görünümü sınırlı bir kampanya 57

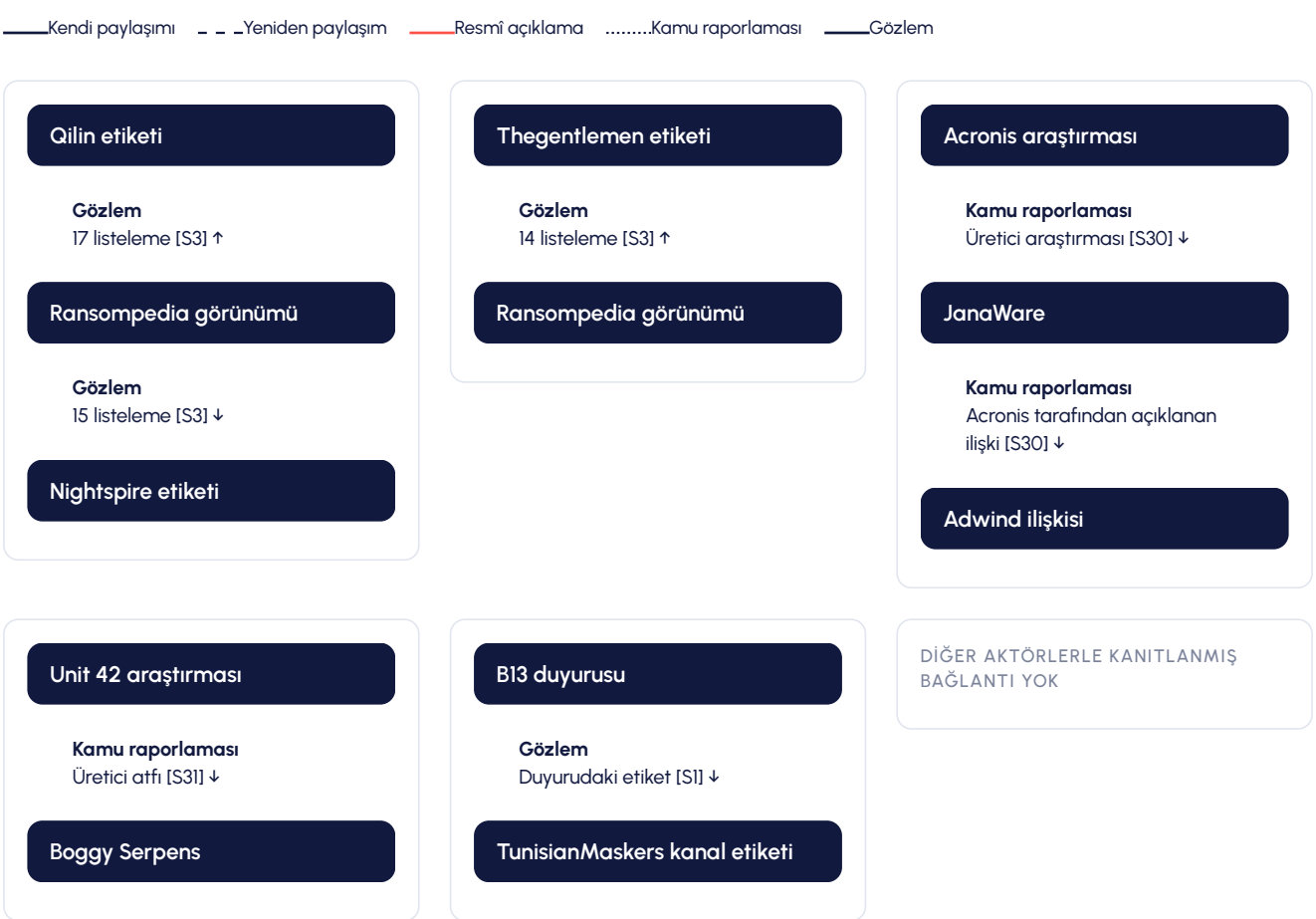
BÖLÜM 07

Tehdit aktörleri ve desteklenen ilişkiler

KISACA

Fidye yazılımı grup adları listeleme görünümünden gelir. Acronis yerel odaklı bir operasyon anlatıyor. Unit 42, Türkiye'yi daha geniş casusluk araştırmasına dahil ediyor. Ağ geçidi ve sanallaştırma araştırmaları ülke etiketli altyapı bulguları ekliyor. Kanal iddiaları ayrı tutuluyor. Bunlar ortak fail veya ulusal olay toplamı ortaya koymuyor. Kaynağa özgü ilişkileri kullanın ve inandırıcı kanıtın işaret ettiği varlıkları ve hizmetleri doğrulayın.

7.1 İlişki haritası

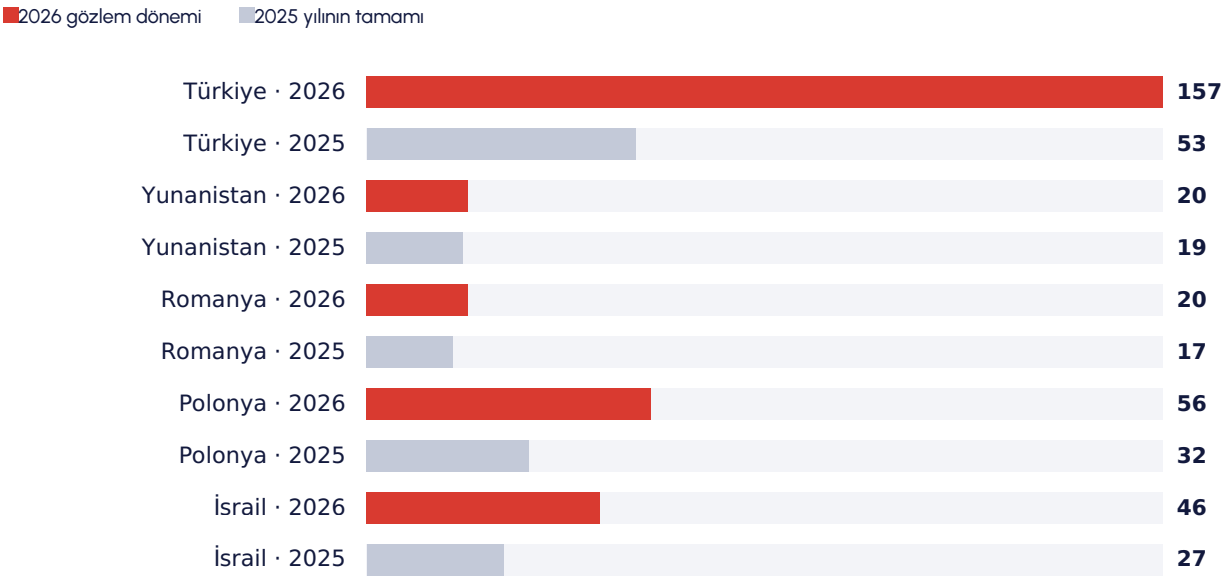


Harita suç hiyerarşisi değil, kaynaktan sonuca giden ilişkiler içerir. Ransompedia grup etiketlerini ve listeleme sayılarını destekler. Acronis, JanaWare ve Adwind ilişkisini destekler. Unit 42 kendi Boggy Serpens atfını destekler. `B13` belirli adı kullanan kanalın duyurusunu destekler `[S1][S3][S30][S31]`.

Saklanan ortak bir unsur, dokuz vaka dosyasını tek işletene bağlamıyor. Daha geniş kimlikten dolandırıcılığa uzanan zincir çizimi **analitik modeldir**. Paylaşımcılar arasında gözlemlenmiş işlemler iddia etmeden savunma bağımlılıklarını gösterir.

7.2 Fidye yazılımı listelemeleri ve grup yoğunlaşması

Bu görünümde Türkiye'nin listeleme sayısı seçilen dört ülkeden fazla



2026 dönemi ile 2025 yılının tamamı farklı süreleri kapsar. Bunlar görünürlük karşılaştırmasıdır, risk sıralaması değildir. Kaynak: Ransompedia listeleme görünümü, 1 Ocak-21 Kasım 2026 [S3]. Listelemeler iddia olarak kalır.

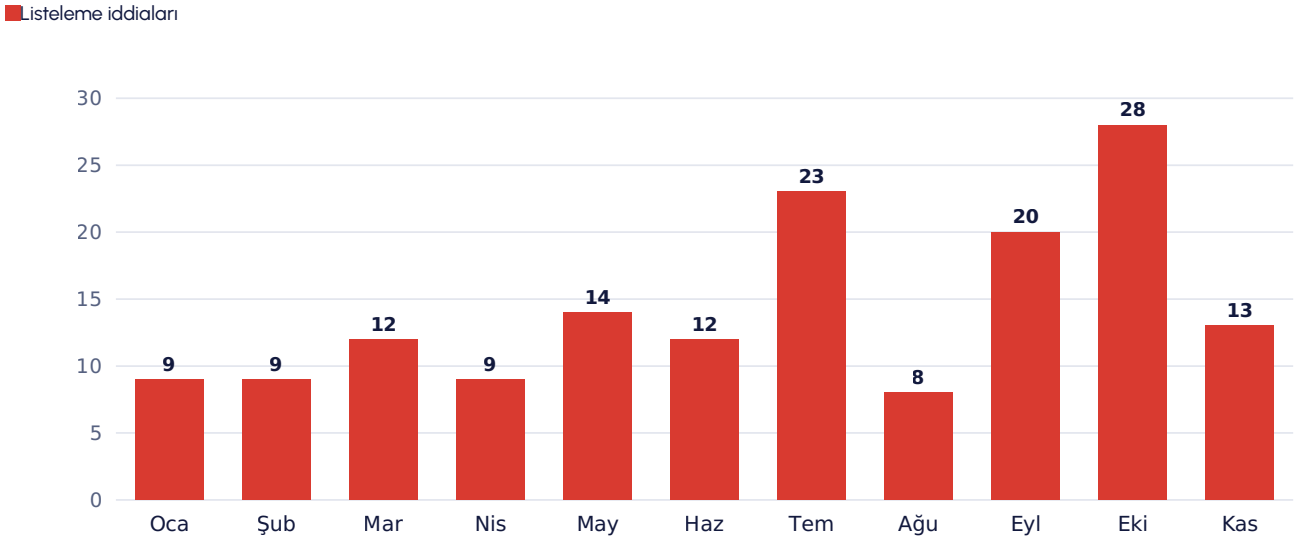
Karşılaştırma ülkeleri yalnızca bağlam sağlamak için örnek olarak seçilmiştir, bir sıralama ya da siyasi değerlendirme içermez.

Ülke	2026 dönemi	2025 tamamı
Türkiye	157	53
Yunanistan	20	19
Romanya	20	17
Polonya	56	32
İsrail	46	27

Tablo, ekonomik büyüklükleri, açıklama uygulamaları ve görünürlükleri farklı beş ülkeyi karşılaştırır. Tablodan saldırı olasılığı, hazırlık veya siyasi maruziyet sıralaması çıkmaz [S3].

Aylık görünüm, listeleme yayımlarının dağılımını gösterir. Kasım son tarihte biter; tam ay değildir.

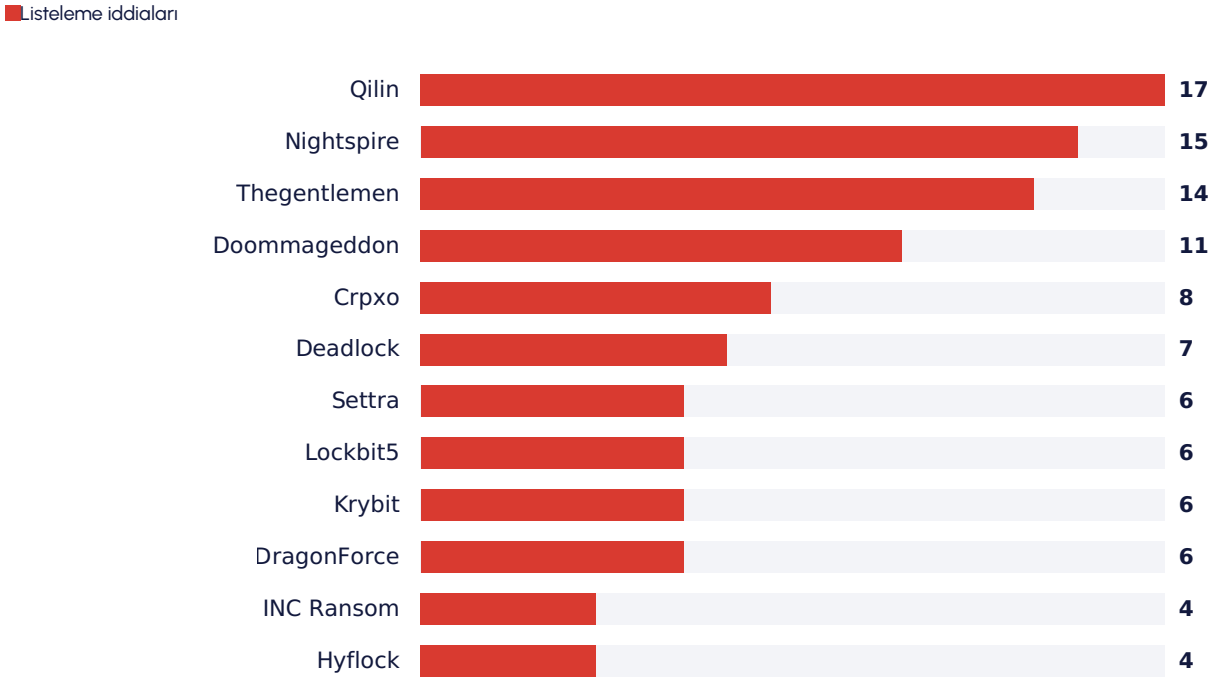
Gözlemlenen 2026 döneminde listeleme yayımları Ekim ayında en yüksek düzeyde

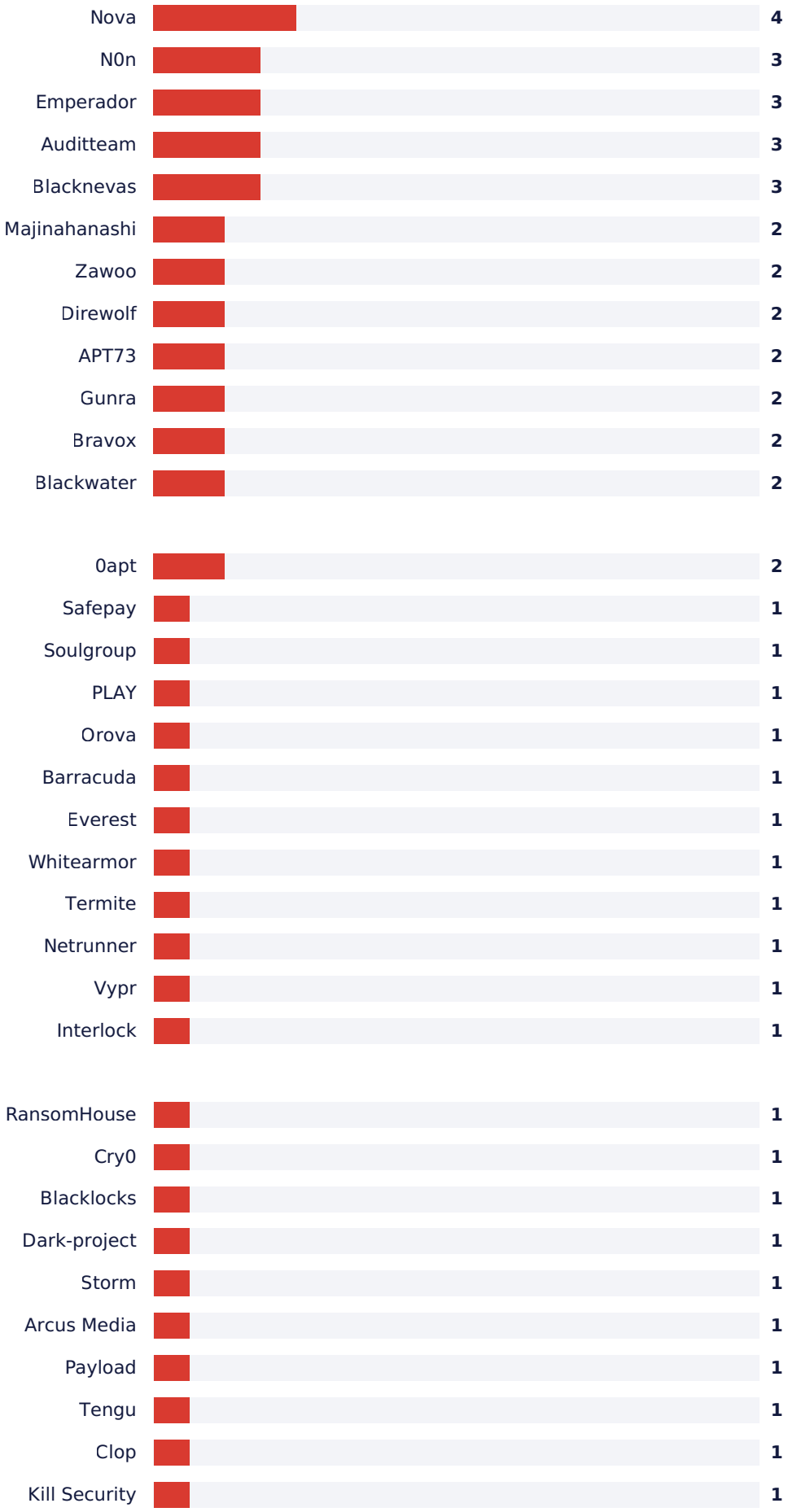


Kaynak: Ransompedia listeleme görünümü, 1 Ocak–21 Kasım 2026 [S3]. Listelemeler iddia olarak kalır.

Grup görünümü Türkiye listelemelerinde en sık kullanılan etiketleri gösterir. Qilin'in 17, Nightspire'ın 15 ve Thegentlemen'in 14 listelemesi, 157 toplamın 46'sını, yani %29,3'ünü oluşturur. Kalan 111 listeleme başka grup etiketleri taşır [S3].

En büyük üç grup etiketi Türkiye listelemelerinin %29,3'ünü oluşturuyor




Nova 4
N0n 3
Emperador 3
Auditteam 3
Blacknevas 3
Majinahanashi 2
Zawoo 2
Direwolf 2
APT73 2
Gunra 2
Bravox 2
Blackwater 2
0apt 2
Safepay 1
Soulgroup 1
PLAY 1
Orova 1
Barracuda 1
Everest 1
Whitearmor 1
Termite 1
Netrunner 1
Vypr 1
Interlock 1
RansomHouse 1
Cry0 1
Blacklocks 1
Dark-project 1
Storm 1
Arcus Media 1
Payload 1
Tengu 1
Clop 1
Kill Security 1

Kaynak: Ransompedia listeleme görünümü, 1 Ocak–21 Kasım 2026 [S3]. Listelemeler iddia olarak kalır.

Qilin

Fidye yazılımı listeleme etiketi | Devlet veya siyasi atıf yapılmıyor

TÜRKİYE'DE, 2026

2026
Ransompedia görünümünde 17 Türkiye listelemesi

İDDİA EDİLEN HEDEFLER

Listelemelerdeki kuruluşlar; kimlikleri verilmemiştir

KAMU KAYNAKLARINDA

[S3] Kurumun listeleme görünümü; listeleme iddia olarak kalır

DEĞERLENDİRMEMİZ

Etiket, listelemeleri karşılaştırmayı sağlar. Ortak bağlı grup, giriş yolu veya doğrulanmış mağdur sonucu göstermez.

GÜVEN
Saklanan sayı için yüksek; olay sonucu doğrulanmadı

Nightspire

Fidye yazılımı listeleme etiketi | Devlet veya siyasi atıf yapılmıyor

TÜRKİYE'DE, 2026

2026
Ransompedia görünümünde 15 Türkiye listelemesi

İDDİA EDİLEN HEDEFLER

Listelemelerdeki kuruluşlar; kimlikleri verilmemiştir

KAMU KAYNAKLARINDA

[S3] Kurumun listeleme görünümü; listeleme iddia olarak kalır

DEĞERLENDİRMEMİZ

Etiket, listelemeleri karşılaştırmayı sağlar. Ortak bağlı grup, giriş yolu veya doğrulanmış mağdur sonucu göstermez.

GÜVEN
Saklanan sayı için yüksek; olay sonucu doğrulanmadı

Thegentlemen

Fidye yazılımı listeleme etiketi | Devlet veya siyasi atıf yapılmıyor

TÜRKİYE'DE, 2026

2026
Ransompedia görünümünde 14 Türkiye listelemesi

İDDİA EDİLEN HEDEFLER

Listelemelerdeki kuruluşlar; kimlikleri verilmemiştir

KAMU KAYNAKLARINDA

[S3] Kurumun listeleme görünümü; listeleme iddia olarak kalır

DEĞERLENDİRMEMİZ

Etiket, listelemeleri karşılaştırmayı sağlar. Ortak bağlı grup, giriş yolu veya doğrulanmış mağdur sonucu göstermez.

GÜVEN
Saklanan sayı için yüksek; olay sonucu doğrulanmadı

Grup etiketleri, listelenen kuruluş için kesin zararlıyı, giriş yolunu, bağlı ekibi veya sonucu göstermez. Bir grubun farklı ülkelerde görünmesi de ülkeler arasında bağlantılı kampanya göstermez.

7.3 Üretici araştırmasında yerel odaklı fidye yazılımı kampanyası

Acronis'in 14 Nisan araştırması, değiştirilmiş Adwind Java RAT üzerinden iletilen JanaWare'i anlatıyor. Türkçe dil ve konum kontrollerini, oltalamayla gelen Java arşivlerini ve gözlemlenen 200–400 USD fidye taleplerini bildiriyor. Tarihsel değerlendirmesi en az 2020 yılına uzanıyor. Ulusal mağdur sayısı vermiyor [S30].

JanaWare

Acronis araştırmasındaki ad

Üretici araştırmasında fidye yazılımı kampanyası | Devlet atfı yapılmıyor

TÜRKİYE'DE, 2026

2026-04-14
Acronis araştırması yayımlandı

İDDİA EDİLEN HEDEFLER

Acronis'e göre Türkiye'deki kullanıcılar ve küçük kuruluşlar

KAMU KAYNAKLARINDA

[S30] Acronis, değiştirilmiş Adwind ilişkisini anlatıyor

DEĞERLENDİRMEMİZ

Ek dosya ve kurtarma planlamasında kaynak kapsamındaki örneği kullanın. Ulusal mağdur toplamı belirlenmiş değil.

GÜVEN
Üretici gözlemleri; ulusal büyüklük bilinmiyor

Savunma açısından planlama sorusu, küçük ofislerin ve tedarikçilerin beklenmeyen çalıştırılabilir eklere direnip bağımsız kurtarma yapabilmesidir. Operasyon testi, zararsız dosyalarla kontrollü tatbikat ve hizmet sorumlusu onaylı gerçek geri yüklemedir.

7.4 Ülkeye özgü sınırı koruyan casusluk araştırması

Unit 42'nin 16 Mart değerlendirmesi, Türkiye'yi Nisan 2025–Şubat 2026 dönemindeki kampanyalara dahil ediyor. MuddyWater adı da kullanılan Boggy Serpens'i İran İstihbarat ve Güvenlik Bakanlığına atfediyor [S31].

Boggy Serpens

Unit 42'ye göre MuddyWater

Üretici araştırmasındaki casusluk atfı | Atıf Unit 42'ye aittir; yazarların bağımsız atfı değildir

TÜRKİYE'DE, 2026

2026-03-16
Unit 42 değerlendirmesi yayımlandı

İDDİA EDİLEN HEDEFLER

Türkiye daha geniş kampanya coğrafyasında yer alıyor

KAMU KAYNAKLARINDA

[S31] Üretici atfı; uzaktan yönetim için geçmiş davranış, ayrı yük örneği için bellek değiştirme; Türkiye zamanlaması belirsiz

DEĞERLENDİRMEMİZ

Rapor, geniş kampanyayla doğrulanmış Türkiye olayını ayrı tutar.

GÜVEN
Kaynağın atfı; Türkiye olay tarihi belirsiz

Unit 42, yakın dönem faaliyetlerinde güvenilir hesapların kötüye kullanılmasını anlatıyor. Uzaktan yönetim örnekleri ise erken kampanyalarla ilgili bölümde yer alıyor. Bunlar geçmiş fail davranışlarıdır. Belirtilen dönemdeki zamanlamaları ve Türkiye'ye özgü kullanımları ortaya konmadı [S31]. Kampanya haritası, Türkiye için doğrulanmış 2026 olay sayısı vermez.

ÜRETİCİ ARAŞTIRMASINDA BELİRTİLEN TEKNİKLER, TAKTİKLERE GÖRE

Komuta ve kontrol	Savunmadan kaçınma
T1219 Uzaktan erişim yazılımı; geçmiş fail davranışı; dönem ve Türkiye'de kullanım ortaya konmadı [S31]	T1055.012 İşlem belleği değiştirme; üreticinin yük örneği [S31]

Unit 42 tarafından açıkça bağlanan tekniklerdir. Türkiye'deki bir mağdur için doğrulanmış teknik kümesi değildir. [S31]

Matris, her tekniğin kaynağa özgü zaman kapsamını korur. Türkiye'deki bir mağdur için doğrulanmış teknik kümesi değildir.

Taktik	Teknik	Kaynak kapsamı	Savunma kullanımı
Komuta ve kontrol	T1219, uzaktan erişim yazılımı	Geçmiş davranış; dönem ve Türkiye'de kullanım ortaya konmadı [S31]	Yetkili uzaktan yönetim kurumlarını ve kullananları inceleyin
Savunmadan kaçınma	T1055.012, işlem belleği değiştirme	Aynı araştırmadaki yük örneği [S31]	Beklenmeyen işlem davranışı için uç nokta görünürlüğünü değerlendirin

7.5 Kanal kimliği ve paylaşımcı etiketleri

TunisianMaskers adını kullanan kanal

Saklanan duyurudaki etiket

DDoS niyet duyurusu | Konum, uyruk, siyasi veya devlet atfı yapılmıyor

TÜRKİYE'DE, 2026

2026-11-07
İleriye dönük hedef seçimi duyurusu, B13

İDDİA EDİLEN HEDEFLER

Banka veya şirket düşünülüyor; doğrulanmış hedef yok

KAMU KAYNAKLARINDA

[S1] Saklanan B13 duyurusu; eşleşen resmî kesinti açıklaması doğrulanmadı

DEĞERLENDİRMEMİZ

Niyet gözlemlendi. Saldırı girişimi, hedef ve hizmet etkisi belirlenmiş değil.

GÜVEN
Duyuru için yüksek; sonuç doğrulanmadı

Veri ve erişim kartları, okuyucunun kararına katkı sağlamadan iletişim veya tanınma değeri taşıyan satıcı takma adlarını vermez. Kamu kanıt kaydı sabit kart kimliklerini tutar. Tekrarlanan ifade; ortak sahipliği, veri alımını veya tamamlanmış satışı değil, benzer ilanı destekler [S1].

Aynı ölçülülük siyasi temalı üyelik iddiası için de geçerlidir. İlan metni devlet destekçisi belirlemez ve iddia edilen mağdura siyasi etiket koymayı gerekçelendirmez.

7.6 FortiBleed: ülke etiketli cihazlar ve kurtarma kanıtı

Hudson Rock'ın haziran araştırması, 194 ülkede 73.932 güvenlik duvarı URL'si ve etkilenen 21.632 alan adı bildiriyor. Ülke tablosunda Türkiye için 3.032 cihaz yer alıyor [S94]. Bunlar kaynağa atfedilen araştırma ölçümleridir. URL, alan adı ve cihaz farklı birimlerdir. Hiçbiri seçilmiş kuruluşların veya doğrulanmış ulusal olayların sayısı değildir.

NCSC; varlık sahipliği ile ele geçirilme işaretlerinin kontrolünü, etkilenen cihazlar sıfırlanmadan yararlı kanıtların korunmasını ve erişilebilir sistemlerin incelenmesini öneriyor [S95]. Bu işlemler kurtarma kararını destekler. Şifre değişikliği, kalıcı erişimin kaldırıldığını tek başına ortaya koymaz. Kampanya ile rapordaki ayrı erişim ilanları arasında ilişki kurulmadı.

7.7 Sanallaştırma yönetimi: ülke görünümü sınırlı bir kampanya

QUIRSO'nun ağustos araştırması, 47 ülkede ele geçirilmiş 361 IP adresi bildiriyor. Türkiye'yi en büyük beş ülke grubu arasında sayıyor [S96]. Adresler benzersiz şirketler değildir. Bildirilen kalıcı uzaktan erişim, kampanya bulgusudur. Türkiye'de doğrulanmış kuruluş sayısı veya yerel fidye yazılımı sonucu sunmuyor.

İlgili CVE-2026-59310, vCenter Syslog hizmeti üzerinden kod çalıştırmayla ilgilidir. NVD kaydı etkilenen sürümleri belirtiyor [S97]. Kullanılan sürüm dalına uygun üretici düzeltmesini uygulayın ve yetkisiz kalıcı erişimi araştırın. Araştırmadaki fail atfı, bağımsız olarak kanıtlanmış kimlik olarak benimsenmiyor.

NVD ayrıca Cloud Foundation, vSphere Foundation ve Telco Cloud ürünlerini listeliyor. Bu kurulumlarda ürüne özgü üretici yanıt tablosunu kullanın [S97][S99].

Üreticinin yanıt tablosu, etkilenen sürüm dallarını ve uygun düzeltmeleri belirtiyor [S99]. İlgili daldaki önceki sürümler düzeltilmelidir. Geçici çözüm listelenmiyor. Ürün paketleri ve uzatılmış destek kapsamındaki kurulumlar için üreticinin özel yönlendirmesi izlenmeli.

Etkilenen vCenter sürüm dalı	Üreticinin düzeltilmiş sürümü veya işlemi
9.1.x.x	9.1.0.0300
9.0.x.x	9.0.2.0100
8.0	İlgili dala uygun 8.0 U3k veya 8.0 U2f
7.0	Uzatılmış destek sözleşmesi varsa üretici desteğine başvurun

İkincil kanal aktarımları, fidye yazılımı ilanlarını ve işletme tanımlarını da tekrarlıyor [S1]. Veri dışarı çıkarılmasını veya kesintiyi bağımsız olarak doğrulamıyorlar. Başka kanalda görünmeleri nedeniyle ayrı 157 ilanlık görünüme eklenmediler.

TEMEL ÇIKARIMLAR

01
Fidye yazılımı grup sayıları listeleme etiketlerini anlatır; listeleme belirsizliği korunur.

02
Kampanya genelindeki bulgular her Türk hedefin tarihini veya giriş yolunu göstermez.

03
Desteklenen ilişkilere, varsayılan suç hiyerarşisinden önce yer verin.

BÖLÜM 08

Dolandırıcılık ekonomisi

BU BÖLÜMÜN YANITLADIĞI SORU

Kimlik verileri, hesap temini ve iletişim dolandırıcılık fırsatını nasıl oluşturuyor?

15.000 TL

saklanan bir ilandaki banka hesabı teklif koşulu

8.1 Banka ve kripto varlık platformu hesabı temini 59
8.2 Ödeme kartı malzemesi: dar görünüm 60
8.3 Telefon hizmetleri ve kimlik doğrulama 60
8.4 Potansiyel müşteri listeleri ve fiyat bağlamı 61
8.5 Polis kampanyası açıklaması 62
8.6 Yazılım hizmetinde yeniden kullanılan kayıtlar 63

BÖLÜM 08

Dolandırıcılık ekonomisi

KISACA

Saklanan ilanlar kişisel bilgileri hesap teminine, telefon hizmetlerine ve müşteri listelerine bağlıyor. Tamamlanmış işlem göstermeden teklifleri ve talebi ortaya koyuyor. Resmî polis açıklaması, iddia edilen suç faaliyetine ayrı görünüm sağlıyor. Kişisel bilgileri güvenilir kimlik kanıtı saymayın; hesap açılışını işlem izlemeye bağlayın; dolandırıcılık ve güvenlik ekiplerine ortak inceleme yolu verin.

8.1 Banka ve kripto varlık platformu hesabı temini

B07, banka ve kripto varlık platformu hesap setleri istiyor. Belirtilen koşullarda banka hesabı başına 15.000 TL, platform hesabı başına 5.000 TL var. Bunlar paylaşımın teklif koşullarıdır; gözlemlenmiş ödeme veya ulusal piyasa fiyatı değildir [S1].

Kanıt kartı B07 — 18 Şub 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | Türkçe

ÖZGÜN METİN

Banka başı ödeme 15k

Not. Hesap temini ilanı; belirtilen fiyatlar teklif koşullarıdır.

Ortaya konan
Banka ve kripto varlık platformu hesap seti talebi.

Ortaya konmayan
Gerçek tedarikçi, kullanılabilir hesaplar, tamamlanmış ödeme veya banka sistemlerine yetkisiz erişim.

İlan önemlidir; çünkü hesap açmakla sonraki kullanımını kontrol etmek farklı güvenlik sorularıdır. Kimliği doğru belirlenmiş müşteri, hesabını başka tarafa kullandırmak üzere yönlendirilebilir. Ele geçirilmiş hesap da benzer işlem akışına girebilir.

Kanıt, ilan edilen hesaplarda hangi yöntemin geçerli olduğunu göstermiyor. Dolandırıcılık kontrolleri farklı yolları sınamalıdır: ilişkili hesaplar, alışılmadık alıcı değişiklikleri, hızlı para aktarımı ve tutarsız cihaz davranışı. Şüpheli örüntü inceleme gerektirir; belirli müşteriye otomatik atıf gerektirmez.

8.2 Ödeme kartı malzemesi: dar görünüm

KART RAKAMLARININ KAPSAMI

Bu rakamlar yalnızca rapor için saklanan karanlık ağ paylaşımlarında açık metin olarak görülen ödeme kartlarını kapsar. Brandefense, bu sürümün dışında kalan başka birçok yöntemle de çalıntı kart tespit eder. Rakamlar kart hırsızlığını, aktif kartları, dolandırıcılık kaybını veya Brandefense'in toplam kart kapsamını ölçmez.

Saklanan grupta 733 paylaşımda görülen, Türkiye ile ilişkili 860 tekil ödeme kartı var. Kartı çıkaran kuruluşla ilişkilendirilenler ve yalnızca ülkeyle ilişkilendirilenler aşağıda ayrı veriliyor. İlişki, kartı çıkaran bankada olay yaşandığını göstermez [S4].

Grup	Tekil kart
Kart kuruluşuyla ilişkilendirilen	578
Yalnızca ülkeyle ilişkilendirilen	282
Toplam	860

Ölçülü yanıt, kartı çıkaran kuruluşun doğrulamasıdır. Kartın aktif olup olmadığını, daha önce yenilenip yenilenmediğini ve destekleyici dolandırıcılık kanıtını kontrol edin. Kamuya açık paylaşımda görünmek, toplu yenileme kararını tek başına belirlememeli.

8.3 Telefon hizmetleri ve kimlik doğrulama

B08, mesajlaşma numarası ve eSIM hizmetleri ilan ediyor. Farklı hizmetler için 850 TL ve 100 USD dahil teklif koşulları veriyor. Mevcut abonenin numarasına erişim veya mobil operatör kontrollerinin aşılması gösterilmiyor [S1].

Kanıt kartı B08 16 Şub 2026

Paylaşanın takma adı verilmemiştir Forum Forum Türkçe

ÖZGÜN METİN

FİYAT = 850 TL

Not. Mesajlaşma numarası ve eSIM ilanı.

Ortaya konan
İlan edilen hizmet ve fiyat; satın alma yapılmadı.

Ortaya konmayan
SIM sahipliği, mevcut bir numaraya erişim veya operatör kontrollerinin aşılması.

Telefon numarası bu nedenle iletişim özelliğidir; tek başına yeterli kimlik kanıtı değildir. Kurtarma süreçleri numara değişikliklerini ve kayıtlı kanalın güvenilirliğini değerlendirmelidir. Önemli değişiklikler, yetkisiz arayanın yalnızca kişisel bilgilerle geçemeyeceği bağımsız kontrol gerektirir.

Aynı ilke KYC bilgileri için geçerlidir. Belge görüntüsüne veya doğru kimlik ayrıntılarına sahip olmak, mevcut hesabı kontrol etmekle aynı değildir. Vaka E, kimlik ve hesap malzemesinin neden birlikte değerlendirilmesi gerektiğini gösterir.

8.4 Potansiyel müşteri listeleri ve fiyat bağlamı

B09, 2.151 bankacılık promosyonu potansiyel müşteri kaydı ilan ediyor. Paylaşım, pazarlama temalı teklifi gösteriyor; banka sistemi olayını, kaynak rızasını veya güncelliği göstermiyor [S1].

Kanıt kartı B09 — 9 Eki 2026

Paylaşanın takma adı verilmemiştir | Forum | Forum | İngilizce

ÖZGÜN METİN

2.151 UNİTS

ÇEVİRİ

2.151 adet

Not. Banka promosyonu potansiyel müşteri listesi; banka sistemi olayı için kanıt değildir.

Ortaya konan
Bankacılık temasını kullanan potansiyel müşteri listesi teklifi.

Ortaya konmayan
Listenin kaynağı, rıza, güncellik veya banka sistemine erişim.

Tablo, ilan edilen ürünlerle para birimleri arasındaki farkı korur.

Kart	İlan edilen konu	Teklif koşulu	Yorum sınırı
B06	VPN erişimi	200 XMR	Gözlemlenen satış veya doğrulanmış erişim yok
B07	Banka hesabı	15.000 TL	Gözlemlenen ödeme veya kullanılabilir hesap doğrulanmadı
B07	Platform hesabı	5.000 TL	Ayrı teklif koşulu; kişi başına toplam değil
B08	Mesajlaşma numarası hizmeti	850 TL	Abone numarasına erişim belirlenmedi
B08	eSIM hizmeti	100 USD	Farklı ürün; kur dönüşümü yapılmıyor
B09	Bankacılık promosyonu listesi	Fiyat burada belirlenmedi	Kaynak veya banka sistemlerine yetkisiz erişim doğrulanmadı

İstenen fiyatı suç gelirine dönüştürmeyin. Paylaşım, pazarlığa açık tutarı, eksik paketi veya hiç sunulmamış hizmeti anlatıyor olabilir. Raporda deneme alımı veya tamamlanmış işlem kaydı yok.

8.5 Polis kampanyası açıklaması

İçişleri Bakanlığının 26 Ekim duyurusu, 35 ildeki operasyonlarda 275 şüphelinin yakalandığını bildiriyor. Farklı suç kategorileri arasında iddia edilen dolandırıcılığı, para aktarımına aracılığı ve mobil bankacılık ile oyun hesaplarına yetkisiz erişimi anlatıyor [S32].

Aynı duyuru, 1 Ocak–22 Ekim 2026 döneminde 5.062 siber suç operasyonu ve yakalanan 21.378 şüpheli bildiriyor. Bunlar resmî operasyon istatistikleridir. Siber saldırı, kanıtlanmış suç, tekil mağdur veya mahkûmiyet sayısı değildir [S32].

Duyuruda erişim kısıtlaması istatistikleri de var. Raporun savunma sonuçları için gerekli olmadığından tekrarlanmıyor. Rapor, hükûmetin erişim kararları hakkında görüş bildirmiyor.

Pratik bağ; müşteri iletişimi, kimlik kontrolleri ve işlem kontrolleri arasındadır. Dolandırıcılık bildirimi, teknik kanıtla birlikte iletişim kanalını ve hesap zaman çizelgesini korumalıdır. Güvenlik ve dolandırıcılık ekipleri, bulgularını paylaşamayan ayrı incelemeler açmamalıdır.

Kapanış haftası taraması, 16 Kasım tarihli bir polis duyurusu ekledi. Duyuru, 12 il merkezli operasyonlarda farklı siber suç iddiaları kapsamında 167 şüphelinin yakalandığını bildiriyor. Oltalama ve mobil bankacılık hesaplarına yetkisiz erişim de sayılan iddialar arasında. Duyuruda 32 tutuklama ve 31 adli kontrol kararı var. Bunlar süreç sayılarıdır; mahkûmiyet veya banka sistemlerine sızma sayısı değildir [S91].

14 Kasım tarihli ayrı bir duyuru, 7 ilde yatırım temalı dolandırıcılık soruşturmasını ve 12 şüphelinin yakalanmasını anlatıyor. Hesaplardaki para hareketliliği 3,2 milyar lira olarak bildiriliyor. Bu tutar doğrulanmış mağdur zararı, geri alınan para veya suç geliri değildir. Dolandırıcılıkla mücadele ekipleri, inandırıcı müşteri ihbarından işlem incelemesine ve kanıt korumaya uzanan süreci sınamalıdır [S92].

İki duyuru ayrı operasyonları anlatıyor. Şüphelilerin ve işlemlerin birbirinden tamamen ayrı olduğu ya da rapordaki hesap ilanlarıyla bağlantılı bulunduğu varsayılamaz. Duyurular, belirli bir satıcının iddia ettiği yeteneği doğrulamaz.

8.6 Yazılım hizmetinde yeniden kullanılan kayıtlar

17 Eylül tarihli bir haber, yazılım şirketi soruşturmasında 5 şüphelinin gözaltına alındığını bildiriyor. Üye olmayan kişileri de kapsayan sorgu arayüzü ile farklı kaynaklardan daha önce sızmış kayıtları anlatıyor [S98]. Bu bilgi habere atfediliyor. Pakette özgün kolluk dosyası bulunmuyor. Gözaltı, mahkûmiyet değildir. Haber, ulusal nüfus sistemine yeni bir sızmayı veya canlı sicile çalışan bağlantıyı ortaya koymuyor.

Veri zenginleştirme veya uyum yazılımı alanlar için alan etiketi, kaynağı kanıtlamaz. Tedarikçiden yetkiyi, saklama süresini, izin verilen kullanıcıları ve erişim kayıtlarını açıklamasını isteyin. Kararlaştırılan hizmet kapsamı dışındaki kişilere ilişkin açıklanamayan bilgileri araştırın. F57'deki belge ve dekont ilanları, önemli kimlik veya ödeme değişikliklerinin bağımsız doğrulanmasını da gerektiriyor [S1].

TEMEL ÇIKARIMLAR

01
Hesap temini ilanları tamamlanmış hesap devirlerinin kanıtı değildir.

02
Kart rakamları ulusal dolandırıcılık kaybını değil, dar paylaşım grubunu anlatır.

03
Kimlik, iletişim ve işlem kanıtını ortak inceleme sorumlusunda birleştirin.

BÖLÜM 09

Bankacılık ve finans incelemesi

09

BU BÖLÜMÜN YANITLADIĞI SORU

Hangi dış bankacılık sinyali kimlik, dolandırıcılıkla mücadele veya tedarikçi sorumlusuna aittir?

30

seçilmiş bankacılık ve finans alan adı

9.1 Finans portföyü ile kart çıkaran kuruluş alt kümesi farklı 65

9.2 Eşleşen kart çıkaran kuruluşların maruziyet görünümü 65

9.3 Açık metin kart gözlemleri dar kapsamlıdır 66

9.4 Tedarikçi kimliği finansal kontrol alanının parçasıdır 67

9.5 Birlikte sınanacak dört iş akışı 67

9.6 Sahte kesinlik olmadan yönetim raporlaması 67

BÖLÜM 09

Bankacılık ve finans incelemesi

KISACA

Bankacılık ve finans portföyünde en az 175.336 cihaz ve 393.538 kimlik bilgisi kaydı ilişkilendirmesi var. Seçilmiş 30 alan adının 18 tanesi güncel piyasa ilanlarıyla ilişkili. Gözlemler hesap doğrulaması gerektirir; banka altyapısına sızıldığını göstermez. Kart çıkaran kuruluşlarla eşleşen alt küme ve açık metin kart gözlemleri daha dar kapsamdadır. Hesap geçerliliği, işlem kötüye kullanımı ve veri işleme için ayrı kanıt içeren ortak kimlik, dolandırıcılıkla mücadele ve tedarikçi akışını sınayın.

9.1 Finans portföyü ile kart çıkaran kuruluş alt kümesi farklı

Seçilmiş portföyde 30 bankacılık ve finans alan adı bulunur. Maruziyet ile kart görünümü, bu portföy içindeki 14 kart çıkaran kuruluş alan adını eşleştirir. Bu, 30 değerlendirmenin tamamını kart çıkaran kuruluş yapmaz ve lisanslı bankaların eksiksiz listesini oluşturmaz [S2][S4].

Finans portföyü ölçüsü	Gözlem	Karar sınırı
Seçilmiş alan adı	30	Amaçlı portföy; bankacılık sisteminin sayımı değil
Cihaz ilişkilendirmesi, en az	175.336	Müşteri ve çalışan ilişkileri örtüşebilir
Çalışan cihazı ilişkilendirmesi	1.643	Yönetilen uç noktayı ve hesap sahipliğini doğrulayın
Kimlik bilgisi kaydı ilişkilendirmesi	393.538	Eski veya tekrarlanan kayıtlar görünür kalabilir
Güncel piyasa ilanıyla ilişkili alan adı	18	İlan; denenmiş aktif hesap değil
Belge ilişkilendirmesi	128	Hassasiyet ve yetki doğrulanmış değil

Çalışan cihazı ilişkilendirmeleri cihaz görünümünün içinde sunulur. Cihaz toplamına ayrıca eklenmez. Kimlik bilgisi ve belge kayıtlarının birimleri ayrıdır. Aynı kayıt birden fazla alan adıyla ilişkili olabilir.

Finans portföyü, 250 alan adlı ulusal portföydeki kimlik bilgisi kaydı ilişkilendirmelerinin %8,5 bölümünü içerir. Bu pay gözlemlenen maruziyet grubunu anlatır. Finansal dolandırıcılığı, aktif müşteri hesabı sayısını veya sektörün ulusal siber olaylardaki payını ölçmez.

Çok kullanılan bir müşteri hizmeti, kendi yönetilen cihazlarının dışında çok sayıda cihaz ilişkilendirmesi üretebilir. İlk iş, inandırıcı gözlemin müşteriye, çalışana, tedarikçiye veya başka bağlama ait olduğunu belirlemektir. Sorumlu ve müdahale bu ayrıma göre seçilir.

9.2 Eşleşen kart çıkaran kuruluşların maruziyet görünümü

Aşağıdaki tablo yalnızca eşleşen 14 kart çıkaran kuruluş alan adını kapsar. Daha küçük paydası korunmadan tüm finans portföyüyle karşılaştırılmamalıdır [S2][S4].

Eşleşen kart çıkaran kuruluş ölçüsü	Gözlem
Eşleşen kart çıkaran kuruluş alan adı	14
Çalışan dışı cihaz ilişkilendirmesi olan alan adı	14
Çalışan dışı cihaz ilişkilendirmesi	165.078
Çalışan cihazı ilişkilendirmesi olan alan adı	12
Çalışan cihazı ilişkilendirmesi	1.533
Güncel ilanla ilişkili alan adı	12
Açık metin kart gözlenen kart çıkaran kuruluş alan adı	12

Çalışan dışı cihaz sayısı, hizmetle ilişkili bir grupdur. Bankanın işlettiği müşteri cihazlarını, benzersiz müşterileri veya hesabı kötüye kullanıldığı doğrulanan kişileri saymaz. Aynı cihazla ilişkili materyalde birkaç banka bulunabilir.

En büyük 3 kart çıkaran kuruluş alan adı grubu, eşleşen çalışan dışı cihaz ilişkilendirmelerinin %35,9 bölümünü içerir. Yoğunlaşma, doğrulama kapasitesini kanıtın en büyük olduğu yere ayırmayı destekler. Bankaları kontrol kalitesine göre sıralamaz veya kayıtların onların sistemlerinden geldiğini göstermez.

Güncel ilanlarda kimlik operasyonları, hizmet ilgisini ve aktif hesap durumunu belirlemelidir. Uç nokta ekipleri, çalışan ilişkilendirmesinin yönetilen cihaza ait olup olmadığını ve güncelliğini ayrıca incelemelidir. Dolandırıcılıkla mücadele ekipleri, destekleyici müşteri hesabı veya işlem sinyalini araştırmalıdır.

Kanıt geliştikçe vaka bu ekipler arasında geçebilir. İlk gözlem tarihini, hesap ilişkisini ve üst inceleme gerekçesini koruyun. Birleşik tablo işi koordine eder; ilanı güncel sızmaya bağlayan eksik kanıtı sağlamaz.

9.3 Açık metin kart gözlemleri dar kapsamlıdır

KART RAKAMLARININ KAPSAMI

Bu sayılar yalnızca rapor için saklanan paylaşımlarda açık metin olarak görünen ödeme kartlarını kapsar. Brandefense, bu yayımın dışındaki başka yöntemlerle de çalıntı kartları saptar. Sayılar kart hırsızlığını, güncel geçerliliği, dolandırıcılık zararını veya Brandefense'in toplam kapsamını ölçmez.

Genişletilmiş saklanmış arşivde, 733 paylaşımda Türkiye ile ilişkili 860 benzersiz kart bulunuyor. Birbirinden ayrı gruplarda, kart çıkaran kuruluşa atfedilen 578 kart ve yalnızca ülkeyle ilişkilendirilen 282 kart var. Yalnızca ülke ilişkisi olan gözlemler, maruziyet görünümünde belirli bir bankaya atanamaz [S4].

Eşleşen kart çıkaran kuruluş görünümünde 579 kart-kuruluş ilişkilendirmesi var. En büyük 3 kuruluş sayısı bu ilişkilendirmelerin %66,3 bölümünü içerir. Kart tekrarlanan veya çelişen kuruluş bağlamı taşıyabilir. Benzersiz kart sayısında birbirinden ayrı ulusal grupların toplamı esas alınır.

Kartın görünmesi, maruziyetin kaynağını belirlemez. Müşteri cihazı, iş yeri, başka bir işlemci veya eski materyal söz konusu olabilir. Bu rapor, kart gözleminden kart çıkaran kuruluşun altyapısında olay olduğu sonucuna varmaz.

Müşteri koruması, kart çıkaran kuruluşun yetkili doğrulama ve dolandırıcılık süreçlerini izlemelidir. Hesabın aktifliğini, koruyucu işlem gereğini ve işlem kanıtının kötüye kullanımı destekleyip desteklemediğini kaydedin. Dış paylaşımın durum etiketi, kart çıkaran kuruluşun güncel kararı sayılmamalıdır.

9.4 Tedarikçi kimliği finansal kontrol alanının parçasıdır

Yatırım hizmetleri bildirimi, yabancı veri işleyenin çalışanlarına yönelik oltalamayı anlatıyor. Yetkisiz erişimin çok faktörlü tek oturum açma platformuna ulaştığını söylüyor. Veri aktarımı doğrulanmamıştı. Bildirim, ilgili bilgi türleri için sınırlar da belirtiyor [S17].

Finansal kuruluş için yararlı test, veri işleyenin olayın hangi müşteri ortamı, hesap ve veriyi kapsadığını açıklayabilmesidir. Tedarikçinin MFA bulunduğunu genel olarak söylemesi, kurtarmanın, kayıtlı cihazların ve aktif oturumların incelenip incelenmediğini yanıtlamaz.

Bildirimi bütün MFA yöntemlerinin teknik olarak aşıldığına kanıt saymayın. Belirli bir olayı anlatır; yöntem ve aktarım sorularını açık bırakır. Aynı sonucu başka yere uygulamadan kapsamı belirli kanıt isteyin.

9.5 Birlikte sınanacak dört iş akışı

Hesap kurtarma. Kamuya açık veya geçmişte açığa çıkmış kişisel bilgilerin önemli değişikliğe yetki verip vermediğini sentetik müşteri kimlikleriyle sınayın. Başarılı testte onaylı süreç, yetkisiz talebi reddeder ve nedenini kaydeder.

Yeni alıcılar ve ödeme değişiklikleri. İnandırıcı mesajla gelen acil talebi sınayın. Önceden kayıtlı, bağımsız doğrulama yolu isteyin. Çalışanın kontrolü geçersiz kılıp kılamadığını ve bu kararı kimin incelediğini kaydedin.

Tedarikçi bildirimi. Olası kimlik olayı bildiren, fakat veri aktarımı kanıtı eksik veri işleyenle başlayın. Hukuk, dolandırıcılık ve güvenlik ekipleri gerekli ilk bildirimi geciktirmeden farklı soruları koruyabiliyor mu, sınayın.

Oturumları sınırlama. Doğrulanan hesap olayı sonrasında ilgili oturumların, kurtarma yollarının, posta kurallarının ve devredilen erişimin incelendiğini gösterin. Yalnızca parola sıfırlama kaydını kapatmak yeterli tamamlanma kanıtı değildir.

9.6 Sahte kesinlik olmadan yönetim raporlaması

Yararlı yönetim panosu; doğrulamayı, sınırlamayı, kurtarmayı ve bildirimi ölçer. Sorumlu bekleyen güvenilir sinyal sayısı, sonuçlandırma süresi, kurtarma tatbikatının tamamlanması ve açık tedarikçi bağımlılıkları örnektir.

Maruziyet, kart ve fidye yazılımı popülasyonlarının etiketlerini ve tarihlerini ayrı tutun. Değişimi kendi paydalarıyla bildirin. Ardışık görünümleri ancak incelenen kapsamın karşılaştırılabilirliğini kontrol ettikten sonra karşılaştırın.

TEMEL ÇIKARIMLAR

01
Finans portföyü, eşleşen kart çıkaran kuruluş görünümü ve açık metin kart grubunun paydaları farklıdır.

02
Aktif kimlikleri, çalışan cihazlarını ve müşteri kötüye kullanımını ilgili sorumlular doğrulasın.

03
Birleşik dış sinyali doğrulanmış bankacılık olayı saymadan önce tedarikçi, oturum ve kurtarma kanıtlarını ilişkilendirin.

BÖLÜM 10

Düzenleyici ve ulusal yanıt

10

BU BÖLÜMÜN YANITLADIĞI SORU

Hangi yükümlülükler yürürlükte, hangi Kasım metinleri öneri?

72 saat

öğrenmeden sonra KVKK Kuruluna bildirim süresi

10.1 Resmî metinler ve uygulanabilirlik 69
10.2 Bildirim süreleri olay zaman çizelgesi gerektirir 70
10.3 Kanuni yaptırımlar kesin etiket gerektirir 70
10.4 Operasyonel uyum tatbikatı 71

BÖLÜM 10

Düzenleyici ve ulusal yanıt

KISACA

Kişisel veri bildirim süresiyle Siber Güvenlik Kanununun bildirim yükümlülüğü farklıdır. 7545 sayılı Kanun, kapsamdaki hizmet sağlayıcıların tespit ettiği açıkları veya siber olayları gecikmeksizin bildirmesini ister. KVKK kararı, Kurula bildirimi öğrenmeden sonra en geç 72 saat olarak yorumlar. Kasım dayanıklılık ve denetim metinleri görüşe açık taslaklardı. Hukuk ekibiyle geçerli yükümlülükleri haritalayın; bilgiler eksikken ilk bildirimi sınayın.

10.1 Resmî metinler ve uygulanabilirlik

Tablo, bu sürüm için okunan kaynakları özetler. Hukuk sorumluları, kuruluşlarına uygulanabilirliği ve güncel ikincil düzenlemeleri belirlemelidir [S8][S9][S10][S11].

Metin	Durum ve kapsam	Yükümlülük veya önem	Pratik sorumlu
6698 sayılı Kanun, madde 12 ve 2019/10 kararı	Kişisel veri ihlali bildirimi çerçevesi	Kurula gecikmeksizin, öğrenmeden sonra en geç 72 saatte bildirim; belirlenen ilgili kişilere makul en kısa sürede bildirim [S8]	Gizlilik ve hukuk
7545 sayılı Kanun, madde 2 ve 7	19 Mart 2025 tarihinden beri yürürlükte; belirtilen istisnalarla geniş siber alan kapsamı	Kapsamdakiler, tespit edilen açıkları veya siber olayları Başkanlığa gecikmeksizin bildirir [S9]	Hukuk ve olay müdahalesi
7545 sayılı Kanun, madde 8	Kanuni denetim yetkileri ve iş birliği görevleri	Hukuka uygun denetim için bildirilen sürede gerekli erişim ve altyapıyı açık tutma [S9]	Hukuk ve altyapı
7545 sayılı Kanun, madde 18	Siber güvenlik ürünleri ve şirketleri	İhracat ve kontrol değişikliği işlemleri belirtilen bildirim veya onaya tabidir [S9]	Hukuk ve kurumsal yönetim
Dayanıklılık taslağı	18 Kasım 2026 tarihinde görüşe açıldı	Kademeli siber yükümlülük ve olay ekibi sorumlulukları öneriliyor; yürürlükte görev sayılmıyor [S10]	Uyum ve güvenlik
Denetim taslağı	18 Kasım 2026 tarihinde görüşe açıldı	Denetim usulleri ve risk temelli gözetim öneriliyor; yürürlükte görev sayılmıyor [S11]	Uyum ve güvence

Siber Güvenlik Kanunundaki kapsam istisnaları, madde 2'de belirtilen istihbarat faaliyetleriyle adı verilen kanunlar kapsamındaki faaliyetlere ilişkindir. Bütün kamu kurumlarına genel muafiyet değildir. Madde 7(c)'deki tedarik hükmü özellikle kamu kurumları ve kritik altyapıları ilgilendirir [S9].

Kasım görüş duyurularının ikisi de 3 Aralık 2026 tarihine kadar görüş istiyor. Hiçbiri önerilen görevler için yürürlük tarihi vermiyor [S10][S11]. Taslakları, yürürlükte yükümlülüklerden ayrı olarak ileriye dönük uyum kaydında tutun.

10.2 Bildirim süreleri olay zaman çizelgesi gerektirir

KVKK'nın 2019/10 kararı, kanundaki en kısa sürede bildirim ifadesini Kurula bildirim için öğrenmeden itibaren 72 saat olarak yorumlar. Gerekli bilgilerin birlikte sağlanamadığı durumda aşamalı bilgiye izin verir. Haklı gecikme açıklanmalıdır [S8].

Aynı karar, ilgili kişilerin belirlenmesinden sonra makul en kısa sürede bildirim ister. Veri işleyenin veri sorumlusuna gecikmeksizin bilgi vermesini de gerektirir. Belirtilen Türkiye bağlantısı koşullarında yurt dışındaki veri sorumlusunun da bildirim sorumluluğu olabilir [S8].

Yükümlülüğü değerlendirmek için kesin kişi sayısını veya tamamlanmış adli incelemeyi beklemeyin. Tespit, iç incelemeye taşıma, öğrenme, tedarikçi bildirimi ve sonraki bulguları kaydeden zaman çizelgesi başlatın. Hukuk sorumlusu, belirli sürenin neden geçerli olduğunu kaydetmelidir.

Siber Güvenlik Kanunu ayrıca kapsamdakilerin tespit edilen açıkları veya siber olayları gecikmeksizin bildirmesini ister [S9]. Bu ifade, genel 72 saatlik siber olay süresiyle değiştirilmemelidir. Sektöre özgü görev de bulunabilir; ayrıca değerlendirilmelidir.

10.3 Kanuni yaptırımlar kesin etiket gerektirir

Aşağıdakiler güncel kanun metnindeki aralıklardır; 2026 yılında ödenecek yeniden değerlenmiş tutar hesabı değildir. Belirli kuruluşa otomatik uygulanmamalıdır [S9].

Hüküm	Davranış	Kanuni aralık	Sınırlama
Madde 16(10)	Madde 7(1)(a), (b) veya (c) görevlerini yerine getirmeme	1.000.000–10.000.000 TL	Madde 18 aralığından ayrı
Madde 16(10)	Madde 18 görevlerini yerine getirmeme	10.000.000–100.000.000 TL	Ürün ve şirket görevlerinin kendi kapsamı var
Madde 16(11)	Madde 8(4) denetim yükümlülüklerini yerine getirmeme	100.000–1.000.000 TL	Ticari şirket kuralı farklı
Madde 16(11)	Ticari şirketler için aynı denetim görevleri	Brüt satışların %5'ine kadar	Kanuni alt sınır 100.000 TL; bağımsız denetimli yıllık finansal tablo belirtiliyor

Madde 16, unsurları ve istisnaları farklı ceza hükümleri de içerir. Madde 17, idari ceza usulünü düzenler. Rapor; ilandan, listelemeden veya belirli kamu açıklamasının yokluğundan suç veya yaptırım sonucu çıkarmaz.

Güncel kanun, 31 Temmuz 2026 tarihinde yürürlüğe giren değişikliği kaydeder. Eski özetlerle güncel madde 16 metnini karşılaştırırken bu önemlidir [S9]. Belirli yaptırım vakası hakkında iddia yapılmıyor.

10.4 Operasyonel uyum tatbikatı

Eksik tedarikçi uyarısıyla başlayın: hesaba erişilmiş, bazı müşteri alanları etkilenmiş olabilir ve veri aktarımı belirsiz. Ekipten veri sorumlusunu, veri işleyeni, etkilenen hizmeti ve kanıt sorumlusunu belirlemesini isteyin.

Ardından ilk bildirim sürecini sınayın. Kuruluş bilinenleri, belirsizlikleri, sınırlamayı ve sonraki güncellemeyi açıklayabiliyor mu? Her sorunun kapanmasını beklemeden, geçerli görev için tarihli gerekçe saklayabiliyor mu?

Son olarak kamu iletişimini kanuni bildirimden ayırın. Kamu durum mesajı, düzenleyici bildirimi ve müşteri bildiriminin amacı ve alıcısı farklıdır. Her biri için kararı ve onay sorumlusunu kaydedin.

TEMEL ÇIKARIMLAR

01
KVKK süresi öğrenmeyle başlar; 7545 kapsamındaki gecikmeksizin bildirimden farklıdır.

02
Kasım görüş metinleri bu sürümde taslak olarak kalır.

03
Güncel kanunu kullanın; kanuni ceza aralıklarını ödenecek tutardan ayırın.

BÖLÜM 11

Görünüm

11

BU BÖLÜMÜN YANITLADIĞI SORU

Hangi değerlendirmeler planlamayı destekler, hangi kanıtlar bunları değiştirir?

5

değişim işaretleri belirlenmiş sınırlı değerlendirme

11.1 Temel değerlendirmeler 73

11.2 Öncelikleri değiştirecek kanıtlar 73

11.3 Koşullu planlama senaryoları 74

BÖLÜM 11

Görünüm

KISACA

En güçlü planlama işaretleri süreklilik, kimlik doğrulaması ve tedarikçi hazırlığıyla ilgilidir. Karanlık ağ faaliyeti eski kimlik bilgilerini taklit için kullanışlı tutabilir; listelemeler ve resmî açıklamalar ayrı kanıt yolları olarak kalır. Seçilmiş maruziyet portföyü kimliksiz sektör doğrulamasını destekler; ulusal yaygınlık tahmini vermez. Aşağıdaki senaryoları planlama varsayımı sayın; güncel hesap, tedarikçi veya hizmet kanıtı değiştiğinde öncelikleri değiştirin.

11.1 Temel değerlendirmeler

Güven, satırdaki belirli sonuca aittir. Aktörün her iddiasını veya gelecekteki her sonucu onaylamaz.

Değerlendirme	Güven	Dayanak ve sınır	Değişim işareti
Süreklilik planlaması öncelik gerektirir	Planlama ihtiyacı için yüksek	Listelemeler ve resmî fidye yazılımı açıklamaları; ulusal saldırı toplamı yok [S3][S12] [S18]	Tekrarlanan kurtarma başarısızlığı veya yeni doğrulanmış hizmet bağımlılığı
Kimlik doğrulama incelemesi ortak sorumluluk ister	Kontrol ihtiyacı için yüksek	Resmî posta kutusu kötüye kullanımı ve tedarikçi kimlik bildirimi [S15][S17]	Doğrulanan oturumlar, kurtarma değişiklikleri veya yetkisiz aktarımlar
Büyük veri teklifleri ön inceleme gerektirmeyi sürdürür	Orta	Tekrarlanan teklifler ve açıkça eski malzeme; satış sıklığı çıkarılmıyor [S1]	Bağımsız kaynak doğrulaması veya yeni veri sorumlusu açıklaması
Tedarikçi bildirimi yanıt hızını etkileyebilir	Orta	Birkaç bildirim veri işleyen bilgisiyle başlıyor; tek ortak kampanya belirlenmedi [S16][S20][S21]	Tedarikçinin etkilenen müşteriyi veya bağlantı sorumlusunu belirleyememesi
Maruziyet doğrulaması farklı sorumlular gerektirir	Kontrol ihtiyacı için yüksek	Seçilmiş cihaz, kimlik bilgisi ve ilan popülasyonları; sektör güvence sıralaması yok [S2]	Güncel hesap eşleşmesi, yönetilen cihaz kanıtı ve doğrulanan tedarikçi ilişkisi

11.2 Öncelikleri değiştirecek kanıtlar

Güncel hesap eşleşmesi. Aktif hesap veya yakın tarihli yetkisiz oturumla eşleşen güvenilir teklif, istihbarat ön incelemesinden olay müdahalesine geçmelidir. Eski ve düzeltilmiş hesap, otomatik yeniden sıfırlama yerine kayıtlı kapanış almalıdır.

Resmî düzeltme. Veri sorumlusu inceleme ilerledikçe etkilenen grubu veya kategorileri değiştirebilir. Yeni açıklamayı önceki hesapla uzlaştırın. Geçerliliğini yitirmiş başlık sayısını sessizce korumayın.

Tedarikçi kapsam eksikliği. Veri işleyen, etkilenen müşteri ortamını veya aktarım yolunu belirleyemiyorsa daha güçlü sınırlama ve geniş etki değerlendirmesi gerekebilir. Karar gerçek hizmeti ve sözleşme ilişkisini izlemelidir.

Doğrulanmış hizmet kesintisi. Hizmet ölçümleri ve sağlayıcı bilgisi etki gösterdiğinde DDoS duyurusu farklı önem kazanır. İddia edilen trafik, ölçülen erişilebilirlik ve iş sonucu arasındaki farkı koruyun.

Değişen maruziyet görünümü. Yeni tarihli gözlem, hesap ve hizmet bağlamı doğrulandığında öncelikleri değiştirebilir. Portföyün ve gözlem kapsamının karşılaştırılabilirliğini denetleyin. Onaylanmış başlığı değiştirmeden önce kanıtı yeniden değerlendirin.

11.3 Koşullu planlama senaryoları

Bunlar planlama varsayımlarıdır; saldırı olasılığı veya mali kayıp tahmini değildir.

Şu olursa	Planlama yanıtı	Kapanış kanıtı
Güvenilir veri iddiası veri işleyeni adlandırırsa	Gizlilik, satın alma ve olay müdahalesini toplayın	Müşteri ortamı kapsamı, alanlar ve tarihli bildirim kararı
Geçerli çalışan oturumu yetkisiz görünürse	Hesabı sınırlayın ve ilişkili erişimi değerlendirin	Oturum iptali, uç nokta incelemesi ve onaylı kurtarma
Kanal Türkiye'de DDoS hedefi duyurursa	Azaltım hazırlığını ve uygulama izlemeyi kontrol edin	İlişkilendirilmiş hizmet ve sağlayıcı kanıtı veya kayıtlı eşleşmeme sonucu
Fidye yazılımı ortak altyapı hizmetini etkilerse	Bağımsız kurtarmayı ve iş önceliklendirmesini başlatın	Sınanmış geri yükleme, bütünlük kontrolleri ve iş birimi onayı
Müşteriye doğru kimlik bilgileriyle ulaşılırsa	Bağımsız doğrulama yolunu kullanın	Dolandırıcılık değerlendirmesi ve güvenilir kanaldan teyit

TEMEL ÇIKARIMLAR

01
İddia daha çok duyulduğunda değil, güncel kanıt değiştiğinde önceliği değiştirin.

02
Gelecek senaryolarını açık kapanış kanıtlı planlama varsayımları olarak tutun.

03
Değişen maruziyet görünümü, hesap ve hizmet bağlamının yeniden incelenmesini gerektirir.

BÖLÜM 12

Eylem planı

12

BU BÖLÜMÜN YANITLADIĞI SORU

Sorumlular otuz, altmış ve doksan günde neyi tamamlamalı?

90

kurtarma ve yanıt hazırlığını göstermek için gün

12.1 Otuz, altmış ve doksan gün 76

12.2 Ulusal PHP duyurusunun teknik referansı 78

12.3 Role göre 78

12.4 Brandefense nasıl yardımcı olabilir? 78

BÖLÜM 12

Eylem planı

KISACA

Sorumluluk, kimlik sinyali doğrulaması ve bildirim hazırlığıyla başlayın. Sonra tedarikçi erişimini sınayın ve temel hizmeti geri yükleyin. Programı, iş sorumlusunun değerlendirebileceği kanıtla kapatın. Takvim önerilen plandır; kanuni süre değildir. Güvenilir sinyal güncel hesap veya hizmet kanıtıyla desteklendiğinde acil sınırlamayı daha erken başlatın.

12.1 Otuz, altmış ve doksan gün

Şeritler her görevi tamamlanma çıktısına bağlar. Takvimi gerçek hizmet önemine uyarlayın.

1Gün 1–30

Güvenilir her dış kimlik veya erişim sinyaline sorumlu atayın

SORUMLU
SOC ve kimlik

TAMAMLANMA KANITI
Doğrulama sonucu ve üst inceleme kararı içeren tarihli kayıt

Kanıt eşleştiğinde aktif hesapları ve yakın oturumları doğrulayın

SORUMLU
Kimlik ve olay müdahalesi

TAMAMLANMA KANITI
Hesap kapsamı, oturum incelemesi ve sınırlama onayı

Müşteri, çalışan ve kimlik verisi tutan veri işleyenleri envantere alın

SORUMLU
Satın alma ve gizlilik

TAMAMLANMA KANITI
Sınanmış olay bağlantılarıyla hizmet-veri işleyen haritası

KVKK süresini diğer olay görevlerinden ayırın

SORUMLU
Hukuk ve gizlilik

TAMAMLANMA KANITI
Senaryo zaman çizelgesi ve onaylı ilk bildirim yolu

Güncel ulusal siber koordinasyon kanallarını doğrulayın

SORUMLU
Olay müdahalesi

TAMAMLANMA KANITI
Bağlantı testi ve iç yönerge güncellemesi

Dışa açık PHP hizmetlerini güncel üretici rehberine göre inceleyin

SORUMLU
Uygulama ve altyapı

TAMAMLANMA KANITI
Desteklenen sürüm kanıtı ve çalışan süreçlerin yeniden başlatılması [S24][S25][S26][S27][S28][S29]

2Gün 31–60

Korunan yedek ve ayrı kurtarma erişimiyle geri yüklemeyi sınayın

SORUMLU

Altyapı ve iş sürekliliği

TAMAMLANMA KANITI

Kurtarılan hizmet, bütünlük sonucu ve iş kabulü

Aktarım kanıtı eksik veri işleyen kimlik olayı tatbikatı yapın

SORUMLU

Tedarikçi riski, gizlilik ve SOC

TAMAMLANMA KANITI

Müşteri ortamı kapsamı, bildirim kararı ve sonraki güncelleme sorumlusu

Gerçekçi kişisel bilgilere karşı müşteri kurtarmayı sınayın

SORUMLU

Dolandırıcılıkla mücadele ve müşteri operasyonları

TAMAMLANMA KANITI

Reddedilen yetkisiz kurtarma girişimi ve kontrol sonucu

Doğrulanmış kötüye kullanım sonrasında posta kurallarını, yetki devrini ve oturumları inceleyin

SORUMLU

Mesajlaşma ve kimlik

TAMAMLANMA KANITI

Etkilenen bütün kontrol alanlarını kapsayan kapanış listesi

3Gün 61–90

Belirsiz hizmet belirtileriyle izlenen DDoS duyurusu tatbikatı yapın

SORUMLU

Operasyon ve iletişim

TAMAMLANMA KANITI

İlişkilendirilmiş hizmet kanıtı ve onaylı durum açıklaması

Ayrıcalıklı tedarikçi erişimini ve erişim sonlandırmayı denetleyin

SORUMLU

Satın alma ve kimlik

TAMAMLANMA KANITI

Kaldırılan eski erişim ve onaylı istisnalar

Düzenleme taslaklarını yürürlükte saymadan inceleyin

SORUMLU

Hukuk ve uyum

TAMAMLANMA KANITI

Durum ve kaynak tarihi içeren güncel yükümlülük kaydı

Programı iş sorumlularıyla değerlendirin

SORUMLU

CISO ve yönetim

TAMAMLANMA KANITI

Açık riskler, kabul kararları ve sınanmış kurtarma kanıtı

12.2 Ulusal PHP duyurusunun teknik referansı

21 Ekim tarihli ulusal duyuru acil inceleme ve güncelleme istedi [S24]. NVD, CVE-2026-109618 ve CVE-2026-109619 kayıtlarını içerir. Üretici duyuruları aşağıdaki sürüm dalı düzeltmelerini verir [S25][S26][S27][S28].

Dal	Gösterilen etkilenen aralık	İki kayıt için asgari düzeltme
PHP 8.2	8.2.35 öncesi	8.2.35
PHP 8.3	8.3.36 öncesi	8.3.36
PHP 8.4	8.4.27 öncesi	8.4.27
PHP 8.5	8.5.12 öncesi	8.5.12

Bunlar belirtilen iki kayıt için asgari düzeltmelerdir; bu sürümlerde kalma önerisi değildir. Çalışan süreçlerin yeniden başlatılması dahil güncel, desteklenen üretici sürümlerini ve rehberini kullanın. Eski dallar desteklenen geçiş veya doğrulanmış üretici düzeltmesi gerektirir [S29]. Raporda Türkiye'deki hiçbir mağdur bu açıklarla ilişkilendirilmiyor.

12.3 Role göre

Yönetim, tatbikatta hangi hizmetin geri yüklendiğini, hangi tedarikçi bağımlılıklarının açık kaldığını ve hangi güvenilir sinyallerin sorumlu beklediğini sormalıdır. Artan paylaşım sayısı bu yanıtların yerine geçmez.

Güvenlik operasyonları, iddia, gözlem ve doğrulama alanlarını ayrı tutmalıdır. Alternatif açıklamaları kaydetmeli; kimlik, gizlilik ve iş sorumlusuyla sonucu kapatmalıdır. Gereksiz kişisel bilgiyi dağıtmadan kanıtı korumalıdır.

Altyapı ve kimlik ekipleri, sınırlamanın parolalarla birlikte oturumları ve devredilmiş erişimi kaldırdığını göstermelidir. Üretim ve kurtarma yönetiminin ayrımını sınamalı; düzeltme sonucunu gerçek hizmette doğrulamalıdır.

Dolandırıcılıkla mücadele ve müşteri operasyonları, bağımsız doğrulamayı, hesap kurtarmayı ve yeni alıcı kontrollerini sınamalıdır. Gerçekçi sentetik senaryolar kullanılmalıdır. Çalışanın başarısız kontrolü sorumlusu belirli istisna olmadan geçersiz kılamadığı gösterilmelidir.

Hukuk, gizlilik ve satın alma, olay zaman çizelgesini, veri sorumlusu-veri işleyen haritasını ve güncel görev kaydını tutmalıdır. Taslak önerileri, kanuni kurallar ve sözleşmesel bildirim taahhütleri ayrı etiket ister.

12.4 Brandefense nasıl yardımcı olabilir?

Alan adlarınızı, markalarınızı, kritik hizmetlerinizi ve güvenlik önceliklerinizi Brandefense görüşmesine getirin. Dış sinyaller, doğrulama ve yanıt sorumluluğu sorularını rapordaki vakalarla şekillendirin. Her sonucun yanında kapsamını, tarihini ve kanıt sınırını da isteyin.

Demo talep edin

TEMEL ÇIKARIMLAR

01
Her eyleme sorumlu ve incelenebilir tamamlanma kanıtı atayın.

02
Doğrulanmış güncel erişimi, plan takvimi dolmadan acil tetikleyici sayın.

03
Kurtarma, tedarikçi ve bildirim tatbikatlarını iş birimi onayıyla tamamlayın.

EKLER

Ekler

A–F

BU BÖLÜMÜN YANITLADIĞI SORU

Bu yayımı hangi gruplar ve sınırlar tanımlar?

4

ayrı birincil kanıt grubu

Ek A. Yöntem ve sınırlar 80

Ek B. Kanıt kaydı 82

Ek C. Kaynaklar 83

Ek D. Sözlük 85

Ek E. Resmî bildirim kaydı 86

Ek F. Ek iddia ve piyasa temaları 92

Ek A. Yöntem ve sınırlar

Karşılaştırma ülkeleri yalnızca bağlam sağlamak için örnek olarak seçilmiştir, bir sıralama ya da siyasi değerlendirme içermez.

A.1 Dönem ve tarihler

Paylaşım dönemi 1 Ocak–21 Kasım 2026 aralığıdır. Kasım tam ay değildir. Maruziyet gözlemleri 21 Kasım tarihlidir. Yıllık anılma bağlamı 18 Kasım'da biter. Pasif gözlemler 21 Kasım UTC'de, yerel saatte 22 Kasım'da toplandı.

Kamu kaynakları hazırlık sırasında, Türkiye yerel saatine göre 22 Kasım'da okundu. Yayım, iddia edilen edinim, sızma, tespit ve bildirim tarihleri farklı olabilir. 2026 içinde yayımlanan paylaşım, daha eski olayla ilişkili veriyi anlatabilir.

A.2 Karanlık ağ paylaşımları

Paylaşım gözlemlerini Brandefense Blackhole sağladı. Türkiye etiketli hacim 4.131.687. Ayrı incelenen gönderi arşivi 177.648 benzersiz paylaşım içerir. İncelenen ülke bağlantılı arşiv, tek tek iddiaların okunmasını destekler [S1].

Arşiv ile etiketli paylaşım görünümünün kapsamları farklıdır. Biri diğerinin alt kümesi olarak sunulmaz. Paylaşım; yanıt, tekrar, ilan veya yorum olabilir. Paylaşım sayıları benzersiz olay, veri seti, satıcı veya etkilenen kişi sayısı vermez.

Aylık ülke ve karşılaştırma satırları aynı paylaşım tarihi aralığını kullanır. Görünürlük, etiketleme ve kaynak katılımı ülkelere ve dönemlere göre değişebilir. Toplamlardan saldırı olasılığı sıralaması, ulusal yaygınlık tahmini veya nedensel eğilim çıkarılmaz.

Kısa alıntılar, gerektiğinde çıkarmalar ve koruyucu etiketler içeren gerçek parçalardır. İletişim yolları, mağdur göstergeleri ve kişisel örnek satırları yayımlanmaz. Kanıt kartlarının sabit kimlikleri, asıl kayıtları açığa çıkarmadan uzlaştırma sağlar.

A.3 Seçilmiş kuruluşlar ve pasif gözlemler

Portföy, on iki sektörde seçilmiş 250 kuruluş alan adı içerir. Seçim, belirli sektörleri ve hizmetleri kapsayacak şekilde yapıldı. Alan adları markaları, kurumsal hizmetleri ve ilişkili tüzel kişileri temsil edebilir. Portföyün bir bölümünde sahiplik ve bağımsızlık doğrulaması tamamlanmamıştır. Örneklem Türkiye'deki bütün kuruluşları temsil etmez [S2].

Yayımlanan sektör grupları 10–50 seçilmiş alan adı içerir. Pasif gözlemler, çözümlenen 239 alan adını kapsar. Eksik ve sonuçsuz gözlemler, yapılandırmanın varlığından veya yokluğundan ayrı tutulur. Başarısız gözlem, başarılı istismar göstermez.

A.4 Kuruluş maruziyeti

Atlas, seçilmiş portföy için 66/100 (C) ulusal notunu sağlar. Yalnızca bu ulusal derece yayımlanır. Kimliksiz sektör tabloları cihaz, çalışan, kimlik bilgisi, ilan ve belge gözlemlerini anlatır. Kuruluş puanlarını açıklamaz veya sektör güvenliği sıralaması sunmaz [S2].

Cihaz rakamları gözlemlenmiş ilişkilendirmeleri anlatır. Müşteri cihazları kendiliğinden kuruluşun işlettiği uç nokta sayılmaz. Kimlik bilgisi ve belge kayıtları farklı kaynaklarda veya alan adlarında tekrarlanabilir. Çalışan cihazı ilişkilendirmeleri cihaz görünümünün içinde sunulur; toplama ayrıca eklenmez.

Piyasa ilanı bir tekliftir; tamamlanan satış veya aktif hesap kanıtı değildir. Belge veya anılma kamuya açık, eski veya kötüye kullanımla ilgisiz olabilir. Benzer alan adında oltalama iddiasından önce sahiplik ve zararlı kullanım doğrulanmalıdır.

Finans portföyü seçilmiş 30 alan adı içerir. Kart çıkaran kuruluşlarla eşleşen alt küme 14 alan adını kapsar ve kendi paydasını korur. Maruziyet ile kart gözlemlerinin eşleştirilmesi ortak doğrulamayı destekler. Nedensel ilişki veya kaydın kaynak sistemini göstermez.

A.5 Kart malzemesi

Sayılar yalnızca rapor için saklanan paylaşımlarda açık metin olarak görünen ödeme kartlarını kapsar. Brandefense, bu yayımın dışındaki başka yöntemlerle de çalıntı kart saptar. Sayılar kart hırsızlığını, güncel geçerliliği, dolandırıcılık zararını veya Brandefense'in toplam kapsamını ölçmez [S4].

Birbirinden ayrı ulusal gruplarda, kart çıkaran kuruluşa atfedilen 578 ve yalnızca ülkeyle ilişkilendirilen 282 kart bulunur. Toplam 733 paylaşımda 860 karttır. Kuruluş ilişkilendirmeleri örtüşebilir. Görünüm, kart kuruluşunun altyapısında olay veya geçerli işlem yeteneği göstermez.

A.6 Fidye yazılımı

Ransompedia, Türkiye ve dört karşılaştırma ülkesi için kabul edilen listeleme görünümünü sağlar. Listelemeler, yayımlanma tarihine göre tarihlendirilir. Listelemeler iddiadır. Kuruluşlar tekrarlanabilir ve listeleme tarihi sızma tarihini göstermeyebilir [S3].

Türkiye toplamı 157 listelemedir. 2025 karşılaştırması tam yılda 53 listeleme içerir; 2026 dönemi belirtilen kapanışta biter. Eşit olmayan süre, görünürlük ve ülke sınıflandırması farkları, eşit dönemli büyüme iddiasını veya ulusal risk sıralamasını engeller.

A.7 Kamu raporları ve olay kapsamı

Resmî veri sorumlusu açıklamaları, ulusal siber duyurular, polis raporları, üretici araştırmaları ve basın haberleri farklı kanıtlar sağlar. Paket, asıl kaynağı okunmuş 57 veri sorumlusu bildirimi içerir. Operasyon duyuruları, karanlık ağ iddiaları ve listelemeler ayrı gruplardır. Benzersiz ulusal olay sayısına eklenemezler.

Bazı eski arşiv bağlantıları yönleniyor veya okunamıyor. Bu adayların kapsam kaydında açık işlemleri vardır. Eksik veya okunmamış kaynak, olay yaşanmadığının kanıtı değildir. Kapanış haftası kontrolü 15–21 Kasım aralığını kapsar ve yeni resmî operasyon materyalini ayrı kaydeder.

Dış gözlemler ve aktarılan açıklamalar kuruluşun incelemesinin yerine geçmez. Doğru kaydedilmiş ilan, gerçekte hatalı iddia içerebilir. Bu nedenle rapor, çözümlenmemiş köken ve sonuç sorularını korur.

A.8 Güven ve siyasi tarafsızlık

Yüksek güven, saklanan gözleme veya doğru aktarılan resmî açıklamaya ait olabilir. Suç ilanındaki iddiaya otomatik olarak geçmez. Orta güven sınırlı yorumu belirtir. Doğrulanmamış ifadesi destekleyici kanıtın yetersiz olduğunu söyler; uydurma olduğunu göstermez.

Rapor; hükümetler, toprak meseleleri, etnik köken, din, seçimler veya erişim kararları hakkında tutum almaz. Devlet atıfları, atıf yapılan kaynağa aittir. Aktör hakaretleri ve yüklü ifadeler çıkarılır. Türkçe yayım aynı sınırları korur.

Ek B. Kanıt kaydı

On yedi paylaşım kartı, ana bölümlerde kullanılan kanıtı tanımlar. Paylaşım tarihi, yetkisiz erişimin gerçekleştiği tarih değildir. Belirli duyuruyu anlamak için gereken kanal adı dışında paylaşanların takma adları verilmemiştir [S1].

Kart	Paylaşım	Ortam	Takma ad	Dil	Bölüm
B01	2026-01-04	forum	Verilmemiştir	English	4
B02	2026-01-24	forum	Verilmemiştir	English	4
B03	2026-02-05	forum	Verilmemiştir	English	4
B04	2026-10-25	forum	Verilmemiştir	English	4
B05	2026-11-15	forum	Verilmemiştir	English	4
B06	2026-11-17	forum	Verilmemiştir	English	4
B07	2026-02-18	forum	Verilmemiştir	Turkish	8
B08	2026-02-16	forum	Verilmemiştir	Turkish	8
B09	2026-10-09	forum	Verilmemiştir	English	8
B10	2026-11-13	forum	Verilmemiştir	English	4
B11	2026-11-05	forum	Verilmemiştir	English	4
B12	2026-10-17	forum	Verilmemiştir	English	4
B13	2026-11-07	telegram	Channel label	English and Arabic	6
B14	2026-11-20	telegram	Verilmemiştir	Turkish	6
B15	2026-11-21	telegram	Verilmemiştir	Turkish	4
B16	2026-03-13	telegram	Belirlenmedi	English	4
B17	2026-09-22	forum	Gizlendi	English	4

Ek C. Kaynaklar

Dış olgular, kaynağında okunan destekleyici ifadelerle sınırlıdır. Makale adresi verilmemiş site kökü atfı, ad kullanma kuralını karşılamayan kuruluşu korur. Tam kaynak kaydı özel çalışma alanında saklanır. Kurum araştırması kamu web sayfalarından ayrılır.

S1: Brandefense Blackhole, saklanan Türkiye bağlantılı paylaşımlar. Saklanan kurum araştırması; toplu sonuçlar bu raporda yer alır. Doğrulama tarihi 2026-11-22.

S2: Odin by Brandefense, seçilmiş kuruluşların pasif gözlemleri. Saklanan kurum araştırması; toplu sonuçlar bu raporda yer alır. Doğrulama tarihi 2026-11-22.

S3: Ransompedia, Türkiye ve karşılaştırma ülkelerinin listeleme görünümü. Saklanan kurum araştırması; toplu sonuçlar bu raporda yer alır. Doğrulama tarihi 2026-11-22.

S4: Brandefense Blackhole, ödeme kartı toplu görünümü. Saklanan kurum araştırması; toplu sonuçlar bu raporda yer alır. Doğrulama tarihi 2026-11-22.

S5: DataReportal, Digital 2027: Turkey, 5 Kasım 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S7: USOM, hizmet geçişi duyurusu. Kaynak. Doğrulama tarihi 2026-11-22.

S8: KVKK, 2019/10 sayılı ihlal bildirimi kararı. Kaynak. Doğrulama tarihi 2026-11-22.

S9: Mevzuat Bilgi Sistemi, 7545 sayılı Siber Güvenlik Kanununun güncel metni. Kaynak. Doğrulama tarihi 2026-11-22.

S10: Siber Güvenlik Başkanlığı, dayanıklılık taslağı görüş duyurusu, 18 Kasım 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S11: Siber Güvenlik Başkanlığı, denetim taslağı görüş duyurusu, 18 Kasım 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S12: KVKK, Yıldız Teknik Üniversitesi bildirimi, 7 Ekim 2026. Kaynak. Metin 2026-11-22 tarihinde kontrol edildi; canlı erişilebilirlik doğrulanamadı.

S13: Yıldız Teknik Üniversitesi, kamuoyu duyurusu, 8 Ekim 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S14: NTV, üniversite olayına ilişkin haber, 8 Ekim 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S15: KVKK, belediye e-posta hesabı olayı, 21 Ekim 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S16: KVKK, perakendeci tedarikçi olayı, 30 Eylül 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S17: KVKK, yatırım hizmetleri tedarikçisinde kimlik olayı, 30 Eylül 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S18: KVKK, eğitim vakfı fidye yazılımı bildirimi, 21 Ekim 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S19: KVKK, gıda perakendecisi tedarikçi bildirimi, 21 Ekim 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S20: KVKK, e-ticaret hizmeti bildirimi, 27 Ekim 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S21: KVKK, üyelik derneği tedarikçi bildirimi, 23 Eylül 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S22: KVKK, mücevher perakendecisi tedarikçi bildirimi, 23 Eylül 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S23: KVKK, yemek teslimatı işletmesi olayı, 7 Ekim 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S24: Siber Güvenlik Başkanlığı, ulusal PHP yanıtı, 21 Ekim 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S25: NVD, CVE-2026-109618. Kaynak. Doğrulama tarihi 2026-11-22.

S26: NVD, CVE-2026-109619. Kaynak. Doğrulama tarihi 2026-11-22.

S27: PHP güvenlik duyurusu GHSA-w8hw-w9fx-j79w. Kaynak. Doğrulama tarihi 2026-11-22.

S28: PHP güvenlik duyurusu GHSA-6wmf-4rv5-p3rp. Kaynak. Doğrulama tarihi 2026-11-22.

S29: PHP, 2026 haber arşivi ve sürüm rehberi. Kaynak. Doğrulama tarihi 2026-11-22.

S30: Acronis Threat Research Unit, JanaWare araştırması, 14 Nisan 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S31: Unit 42, Boggy Serpens Threat Assessment, 16 Mart 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S32: İçişleri Bakanlığı, siber suç operasyonu duyurusu, 26 Ekim 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S33: Siber Güvenlik Başkanlığı, olay müdahalesinde yaygın eksiklikler, Mayıs 2026. Kaynak. Doğrulama tarihi 2026-11-22.

S34: RFC Editor, RFC 7489: DMARC. Kaynak. Doğrulama tarihi 2026-11-22.

S35: RFC Editor, RFC 7208: SPF. Kaynak. Doğrulama tarihi 2026-11-22.

S36: RFC Editor, RFC 6376: DKIM. Kaynak. Doğrulama tarihi 2026-11-22.

S37: RFC Editor, RFC 4033: DNSSEC. Kaynak. Doğrulama tarihi 2026-11-22.

S38: RFC Editor, RFC 8446: TLS. Kaynak. Doğrulama tarihi 2026-11-22.

S39: KVKK, liman işletmesi bildirimi, 2026-10-27. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S40: KVKK, müşteri hizmetleri teknolojisi işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S41: KVKK, teknik destek işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S42: KVKK, müşteri hizmetleri operasyon işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S43: KVKK, e-ticaret işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S44: KVKK, sigorta şirketi bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S45: KVKK, üyelik hizmeti sunan oda bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S46: KVKK, üniversite bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S47: KVKK, böbrek sağlığı hizmetleri işletmesi bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S48: KVKK, uluslararası seyahat işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S49: KVKK, uluslararası ilaç işletmesi bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S50: KVKK, eğitim hizmetleri vakfı bildirimi, 2026-09-23. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S51: KVKK, yemek teslimatı işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S52: KVKK, otel işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S53: KVKK, inşaat işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S54: KVKK, otel işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S55: KVKK, otel işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S56: KVKK, uluslararası lojistik grubu bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S57: KVKK, yemek teslimatı işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S58: KVKK, sağlık yatırımı işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S59: KVKK, otel işletmesi bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S60: KVKK, içecek üreticisi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S61: KVKK, uluslararası hava yolu işletmesi bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S62: KVKK, giyim perakendecisi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S63: KVKK, otel işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S64: KVKK, otomotiv perakendecisi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S65: KVKK, sağlık hizmeti sağlayıcısı bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S66: KVKK, çevrim içi eğlence hizmeti bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S67: KVKK, sağlık ürünleri perakendecisi bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S68: KVKK, çevrim içi eğlence hizmeti bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S69: KVKK, gıda perakendecisi bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S70: KVKK, teslimat işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S71: KVKK, giyim perakendecisi bildirimi, 2026-09-23. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S72: KVKK, otel işletmesi bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S73: KVKK, seyahat acentesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S74: KVKK, otel işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S75: KVKK, çevrim içi perakendeci bildirimi, 2026-09-23. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S76: KVKK, spor ürünleri perakendecisi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S77: KVKK, tıbbi cihaz işletmesi bildirimi, 2026-11-04. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S78: KVKK, yemek teslimatı işletmesi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S79: KVKK, uluslararası otel grubu bildirimi, 2026-10-21. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S80: Memurlar.net, hava yolu işletmesinin açıklaması, 4 Kasım 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S81: İletişim Başkanlığı, çevrim içi kamu hizmeti açıklaması, 10 Haziran 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S83: DataGuidance, elektronik haberleşme bildirimi özeti, 5 Şubat 2026. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S85: KVKK, çevrim içi perakendeci bildirimi, 2026-09-23. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S86: KVKK, uluslararası değişim hizmetleri işletmesi bildirimi, 2026-09-30. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S87: KVKK, giyim perakendecisi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S88: KVKK, çeşitli sektörlerde faaliyet gösteren işletme grubu bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S89: KVKK, sigorta şirketi bildirimi, 2026-10-07. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S90: KVKK, hava yolu işletmesi bildirimi, 2026-11-11. Kaynak (makale adresi verilmemiştir). Doğrulama tarihi 2026-11-22.

S91: Interior Ministry, cybercrime operations in twelve provinces, 16 November 2026. Kaynak. Doğrulama: 2026-11-22.

S92: Interior Ministry, investment-themed fraud operation, 14 November 2026. Kaynak. Doğrulama: 2026-11-22.

S93: MC Legal, review of twenty-eight controller notifications, 18 September 2026. Kaynak. Doğrulama: 2026-11-22.

S94: InfoStealers (Hudson Rock), FortiBleed araştırması, 17 Haziran 2026. Kaynak. Doğrulama tarihi: 2026-11-22.

S95: UK National Cyber Security Centre, Fortinet campaign guidance, 18 June 2026. Kaynak. Doğrulama tarihi: 2026-11-22.

S96: QUIRSO, virtualisation-management exploitation research, 10 August 2026. Kaynak. Doğrulama tarihi: 2026-11-22.

S97: NVD, CVE-2026-59310 record. Kaynak. Doğrulama tarihi: 2026-11-22.

S98: Sabah, software-company investigation report, 17 September 2026. Kaynak (yazı adresi gizlendi). Doğrulama tarihi: 2026-11-22.

S99: Broadcom, vCenter security response matrix, updated 19 August 2026. Kaynak. Doğrulama tarihi: 2026-11-22.

S100: IETF, RFC 6797: HTTP Strict Transport Security (HSTS). Kaynak. Doğrulama tarihi: 2026-11-22.

Ek D. Sözlük

Terim	Yalın anlam
İddia	Paylaşım veya listelemenin öne sürdüğü, ayrıca doğrulanması gereken şey
Veri sorumlusu	Kişisel veri işlemenin amaç ve araçlarını belirleyen taraf
Veri işleyen	Veri sorumlusu adına kişisel veri işleyen taraf

Terim	Yalın anlam
SSO	Bağlantılı hizmetlere erişimde kullanılan ortak oturum açma düzeni
MFA	Birden çok kanıt türü isteyen kimlik doğrulama
KYC	Müşteri ilişkisi kurulurken veya sürdürülürken yapılan kimlik kontrolleri
Oturum	Parola değişikliğinden sonra da sürebilen doğrulanmış etkileşim
DMARC	İlgili e-posta doğrulamalarını geçemeyen iletilere ilişkin yayımlanmış alan adı politikası
SPF	Alan adının yetkili e-posta gönderim altyapısı bildirimi
DKIM	Alıcının ileti imzasını kontrol etmesini sağlayan e-posta imzalaması
DNSSEC	DNS için gerçeklik ve bütünlük kontrolünü destekleyen imzalama
TLS	Bağlantıyı koruyan, uygulama yetkilendirmesinden ayrı protokol
HSTS	HTTP Strict Transport Security: tarayıcıların sonraki bağlantılarda HTTPS kullanmasını isteyen web sitesi politikası [S100]
DDoS	Hizmet erişilebilirliğini tüketmeyi amaçlayan dağıtık trafik
SOME	Türkiye koordinasyon çerçevesindeki siber olaylara müdahale ekibi
Fidye yazılımı listelemesi	Burada iddia olarak ele alınan, kamuya açık şantaj sitesi girdisi
Analitik model	Gözlemlenmiş işlem iddia etmeden savunma bağımlılıklarını bağlayan etiketli yorum

Ek E. Resmî bildirim kaydı

Bu kayıt, önceki bölümlerde ele alınan 10 bildirime kaynağı okunmuş 47 veri sorumlusu bildirimi ekler; toplam 57 resmî bildirim yer alır. Bu bir açıklama kaydıdır, ayrı saldırı sayısı değildir. Tarih sütunu Kurul kararının tarihidir. Faaliyet, keşif ve yayım tarihleri farklı olabilir. Bazı bildirimler yabancı veri sorumlularıyla veya geçmiş faaliyetlerle ilgilidir. Burada yer almaları, Türkiye'de yeni bir saldırı gerçekleştiğini göstermez. Etkilenen kişi sayıları toplanmaz.

Önceki bildirimler üniversite, belediye posta kutusu, perakende tedarikçisi, yatırım hizmetleri tedarikçisi, eğitim vakfı, gıda perakendecisi, e-ticaret hizmeti, üyelik derneği, mücevher perakendecisi ve yemek teslimatı işletmesiyle ilgilidir [S12][S15][S16][S17][S18][S19][S20][S21][S22][S23].

Ana rapordaki yayım kuralı uyarınca adlar verilmemiştir. Kaynak kimlikleri, rol tanımlarını kimlik belirtir hâle getirmeden eşleştirmeyi sağlar. Bunlar hazırlık sırasında bulunan seçilmiş açıklamalardır; önceki arşiv dönemlerinin kapsamı hâlâ eksiktir.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S50]	2026-09-23	Eğitim hizmetleri vakfı	İnternet barındırma tedarikçisi olayı 2026-09-12 tarihinde bildirildi; 68 müşteri. Kimlik, iletişim ve parola özeti alanları bildirildi.
[S71]	2026-09-23	Giyim perakendecisi	Veri işleyenin yazılım kütüphanesinin istismarı 2026-09-10 tarihinde bildirildi; 85.722 kişi. Kimlik, iletişim ve işlem güvenliği kategorileri söz konusu.
[S75]	2026-09-23	Çevrim içi perakendeci	E-ticaret tedarikçisinin veri tabanına yetkisiz erişim 2026-09-14 tarihinde bildirildi. Tedarikçi, 473.284 nihai müşteri ve 54 yönetim paneli kullanıcısı tahmin etti; veri sorumlusu kesin kişi sayısını belirleyemedi.
[S40]	2026-10-07	Müşteri hizmetleri teknolojisi işletmesi	Fidye yazılımı 2026-09-30 tarihinde saptandı; çalışan, aday ve çağrı kaydı kategorileri söz konusu. Dışarı aktarım saptanmadı; kişi sayısı belirsiz.
[S42]	2026-10-07	Müşteri hizmetleri operasyon işletmesi	Fidye yazılımı 2026-09-30 tarihinde saptandı; çalışan, aday ve çağrı kaydı kategorileri söz konusu. Ayrı bir veri sorumlusu bildirimi; ek doğrulama olmadan ayrı bir teknik olay sayılmaz.
[S51]	2026-10-07	Yemek teslimatı işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-09-30 tarihinde bildirildi. Müşteri ve çalışan veri kategorileri söz konusu; kişi sayısı araştırılıyor.
[S53]	2026-10-07	İnşaat işletmesi	Dışarıdan erişim ve şifreleme 2026-10-03 tarihinde saptandı. Kişisel veri kapsamı ve kişi sayısı araştırılıyor.
[S57]	2026-10-07	Yemek teslimatı işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-09-30 tarihinde bildirildi. Müşteri ve çalışan kategorileri söz konusu; kişi sayısı belirsiz.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S58]	2026-10-07	Sağlık yatırımı işletmesi	Dışarıdan erişim ve şifreleme 2026-10-03 tarihinde saptandı. Kişisel veri kapsamı ve kişi sayısı araştırılıyor.
[S62]	2026-10-07	Giyim perakendecisi	Veri işleyenin yazılım kütüphanesinde zafiyet; tedarikçi bildirimi 2026-09-29 tarihinde alındı. Bildirilen alanlar arasında müşteri ve yönetim hesabı parola özetleri var; kişi sayısı belirsiz.
[S66]	2026-10-07	Çevrim içi eğlence hizmeti	Çağrı merkezi veri işleyeninde şifreleme 2026-09-30 tarihinde saptandı; ses ve çağrı detay kayıtları söz konusu. İlk incelemede dışarı aktarım bulgusu yok; yetkisiz erişim dışlanamadı; kişi sayısı belirsiz.
[S68]	2026-10-07	Çevrim içi eğlence hizmeti	Çağrı merkezi veri işleyeninde şifreleme 2026-09-30 tarihinde saptandı; ses ve çağrı detay kayıtları söz konusu. Ayrı veri sorumlusu bildirimi; doğrulanmış dışarı aktarım veya etkilenen kişi sayısı yok.
[S78]	2026-10-07	Yemek teslimatı işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-01 tarihinde bildirildi. Müşteri ve çalışanların kimlik, iletişim, konum, işlem ve finans kategorileri söz konusu; kişi sayısı belirsiz.
[S46]	2026-10-21	Üniversite	Uygulama zafiyeti; 109 kişi etkilendi. Ulusal siber merkezin bildirimi üzerine 2026-10-14 tarihinde saptandı; kimlik, iletişim ve konum kategorileri söz konusu.
[S47]	2026-10-21	Böbrek sağlığı hizmetleri işletmesi	Çalışana yönelik sesli oltalama; bir hesap, CRM sistemi ve kurum içi rehber dosyası söz konusu. Başlangıç 2026-08-04; tespit 2026-10-06. Kişi sayısı belirsiz.
[S65]	2026-10-21	Sağlık hizmeti sağlayıcısı	Fidye notu ve şifrelenmiş veri tabanı bildirildi. Sağlık, kimlik, iletişim ve finans kayıtları söz konusu olabilir; şifrelenen dosyalar ilk kişi sayısının belirlenmesini engelledi. Bildirimde tespit tarihi eksik yazılmış.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S67]	2026-10-21	Sağlık ürünleri perakendecisi	Veri işleyenin yazılım kütüphanesinin istismarı 2026-09-10 tarihinde bildirildi; 50.636 kişi. Kimlik, iletişim ve parola özeti alanları bildirildi.
[S69]	2026-10-21	Gıda perakendecisi	Veri işleyenin yazılım kütüphanesinin istismarı 2026-10-07 tarihinde bildirildi. Olası en yüksek kapsam: ayrı belirtilen 15.303 nihai müşteri ve 18 yönetim paneli hesabı sahibi.
[S72]	2026-10-21	Otel işletmesi	Kurumsal e-posta ve altyapıyı ilgilendiren hesap erişimi şüphesi; kategoriler, tarihler, dışarı aktarım ve etkilenen kişiler araştırılıyor. Olası erişim, doğrulanmış dışarı aktarım sayılmaz.
[S79]	2026-10-21	Uluslararası otel grubu	Çalışan hesabına yönelik sosyal mühendislik; erişim dönemi 2026-06-05–2026-06-06, ilk gün saptandı. 9.550 müşteri; bildirim yalnızca Türkiye'ye ait bir nüfus ortaya koymuyor.
[S39]	2026-10-27	Liman işletmesi	Tedarikçinin yardım masasında erişim kontrolünün aşılması ve parola değişiklikleri; faaliyet 2026-10-12 tarihinde başladı, 2026-10-19 tarihinde saptandı. İlk sayı: 855 kişi.
[S41]	2026-11-04	Teknik destek işletmesi	Veri işleyende tutulan sohbet içeriğine yetkisiz erişim. 624 sohbet kaydı; etkilenen kişi sayısı henüz belirlenmedi. Kayıt ve kişi farklı birimlerdir.
[S43]	2026-11-04	E-ticaret işletmesi	Veri işleyende tutulan 2022 tarihli sohbet kayıtlarına yetkisiz erişim; 9.882 kişi. Kayıtların yaşı, saldırının tarihini göstermez.
[S48]	2026-11-04	Uluslararası seyahat işletmesi	İnternet rezervasyon uygulamasında açık; en fazla 2.392 kişiye ilişkin olası erişim. Müşterilere yönelik kötü amaçlı e-postalar 2026-10-10 tarihinde, teknik bulgular 2026-10-12 tarihinde görüldü.
[S52]	2026-11-04	Otel işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-25 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S54]	2026-11-04	Otel işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-23 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S55]	2026-11-04	Otel işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-26 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S60]	2026-11-04	İçecek üreticisi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-23 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S63]	2026-11-04	Otel işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-26 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S64]	2026-11-04	Otomotiv perakendecisi	Veri işleyende tutulan sohbetlere yetkisiz erişim; 8.268 sohbet kaydı, etkilenen kişi sayısı belirsiz. Sınırlı örnekler ad, telefon, araç plakası ve randevu bilgilerini içeriyor.
[S70]	2026-11-04	Teslimat işletmesi	Veri işleyende tutulan 2022 tarihli sohbet kayıtlarına yetkisiz erişim; 3.217 kişi. Kayıtların eski tarihli olması, saldırının da eski olduğunu göstermez.
[S73]	2026-11-04	Seyahat acentesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-24 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S74]	2026-11-04	Otel işletmesi	Veri işleyen sistemlerine yetkisiz erişim 2026-10-23 tarihinde saptandı. Müşteri kimlik, iletişim ve işlem kategorileri söz konusu; kişi sayısı belirsiz.
[S76]	2026-11-04	Spor ürünleri perakendecisi	Bulut müşteri hizmetleri veri işleyeninin kayıtlarına yetkisiz erişim: 383 kişiye ilişkin 541 sohbet kaydı. Sayılar farklı birimleri anlatır.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S77]	2026-11-04	Tıbbi cihaz işletmesi	Erişim 2026-10-14 tarihinde başladı, 2026-10-23 tarihinde saptandı; bazı veriler dışarı aktarıldı. Ağırlıklı kapsam iş bağlantıları; hasta kimlikleri, cihaz bilgileri ve işitme testi verileri de bulunabilir. Kişi sayısı belirsiz.
[S44]	2026-11-11	Sigorta şirketi	Geçmiş tarihli tedarikçi bildirimi: yetkisiz erişim tarihleri 2022-01-15 ve 2022-02-14. Dönem içindeki bir açıklama olarak yer alır; 2026 için yeni olay şeklinde yorumlanmaz.
[S45]	2026-11-11	Üyelik hizmeti sunan oda	SQL enjeksiyonu 2026-11-02 tarihinde saptandı; üyelik veri tabanına erişim ve dışarı aktarım bildirildi. Veri tabanı durduruldu; genel muhasebe sisteminin etkilenmediği belirtildi. Kişi sayısı belirsiz.
[S49]	2026-11-11	Uluslararası ilaç işletmesi	Alt veri işleyende bilgi işlem çalışanı taklidiyle sesli oltalama, bulut hesaplarını etkiledi. İşleme kapsamındaki nüfus en fazla 18 kişi; fiilen etkilenenler araştırılıyor. Bazı takma adlandırılmış sağlık/genetik verileri söz konusu olabilir.
[S56]	2026-11-11	Uluslararası lojistik grubu	Çalışan anketi veri işleyicisinin analiz sistemine yetkisiz erişim 2026-11-02 tarihinde saptandı; Türkiye'deki 10.622 çalışan etkilendi.
[S59]	2026-11-11	Otel işletmesi	2026-10-27 tarihinde saptanan saldırı, sunucuyu ve misafir kablosuz ağını engelledi. Misafirlerin kişisel bilgilerinin elde edildiği bildirildi; kişi sayısı belirsiz.
[S61]	2026-11-11	Uluslararası hava yolu işletmesi	Rezervasyon veri işleyenine erişim dönemi 2023-08-10–2026-09-23; tedarikçi bildirimi 2026-11-03 tarihinde alındı. Kişi sayısı belirsiz. Türkiye'de yayımlanması, saldırının burada gerçekleştiğini göstermez.

Kaynak	Kurul kararı	Kuruluşun rolü	Bildirilen bulgu ve sınırı
[S85]	2026-09-23	Çevrim içi perakendeci	Veri işleyen bildirimi 2026-09-14 tarihinde alındı; 4.989 nihai müşteri ve 20 yönetim paneli hesabı sahibi. Kimlik, iletişim ve parola özeti alanları bildirildi.
[S86]	2026-09-30	Uluslararası değişim hizmetleri işletmesi	Başvuru yükleme alt sisteminde adres düzeyinde kimlik doğrulama yoktu; otomatik erişimle başvuru belgeleri elde edildi. Başlangıç 2026-09-04; tespit 2026-09-09; 7.591 müşteri. Yalnızca Türkiye'ye ait nüfus ortaya konmuyor.
[S87]	2026-10-07	Giyim perakendecisi	Fidye yazılımı faaliyeti 2026-09-28–2026-09-29 döneminde gerçekleşti, son tarihte saptandı. Giriş yolu, etkilenen gruplar, kategoriler ve kişi sayısı belirsiz.
[S88]	2026-10-07	Çeşitli sektörlerde faaliyet gösteren işletme grubu	Dışarıdan erişim ve şifreleme 2026-10-03 tarihinde başladı ve saptandı. Çalışan, kullanıcı ve müşteri kategorileri söz konusu; etkilenen kişi sayısı tahmin edilemedi.
[S89]	2026-10-07	Sigorta şirketi	Veri işleyen olayı 2026-09-30 tarihinde saptandı; bir günlük ses kayıtları şifrelendi. 161 çağrı kaydına erişilemedi; kişi sayısına dönüştürülmüyor.
[S90]	2026-11-11	Hava yolu işletmesi	Bilgi teknolojileri talep/geliştirme sisteminde yönetici parolasının yetkisiz kullanımı; parolanın nasıl alındığı belirsiz. Başlangıç 2026-10-12; tespit 2026-10-26; kimlik/iletişim kategorilerinde 11.762 çalışan ve kullanıcı.

Ek F. Ek iddia ve piyasa temaları

Bu temalar, dokuz ayrıntılı vakanın yanındaki diğer saklanmış anlatımları bir araya getirir. Bunlar kaynak iddiaları ve piyasa teklifleridir; ek doğrulanmış olaylar değildir. Tarihler, saklanan paylaşımları veya gözlemlenen aralıklarını belirtir. Farklı satırlar örtüşebilir; birkaç paylaşım aynı teklifi tekrarlayabilir. Özel kapsam kaydı, değerlendirilen her kalemi ve yayım kararını korur.

Kayıtta kişisel örnek satırları, iletişim yolları ve mağdurun kimliğini belirten özellikler yoktur. Yetersiz dosya adları, desteklenmemiş ikincil haberler, yabancı hedef iddiaları ve gereksiz hassas kişisel iddialar için kapsam kaydında açık dışlama gerekçeleri vardır. Bu dışlamalar, iddia edilen olayın gerçekleşmediğini göstermez.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F01	2026-01-04	Elektronik para hizmetleri	Bir paylaşım, ödeme hizmetinin arka uç kaynak kodunun yayımlandığını iddia ediyor. [S1]	Kodun elde bulunduğu, üretim ortamına erişim ve müşteri verisi etkisi doğrulanmadı.
F02	2026-01-06	Ulaşım kayıtları	Bir teklif, büyük bir ulaşım kaydı koleksiyonunu anlatıyor ve ek terminal verisi vaat ediyor. [S1]	Kaynak, birimin anlamı ve işletim sistemiyle olası ilişki belirsiz.
F03	2026-01–2026-02	Elektronik haberleşme	İlanlar, işletmeci paneli veya API erişimi sunuyor; sonraki satıcı tartışması, düzenleyici bildirimle bağlantı iddia ediyor. [S1]	Bağlantıyı satıcı ileri sürüyor. Ortak kaynak, süren erişim veya neden sırası bağımsız olarak ortaya konmadı.
F04	2026-01–2026-05	Eğitim sistemleri ve hesapları	Paylaşımlar; eğitim portalına erişim, resmî görevli hesabına sosyal mühendislik ve daha geniş üniversite erişimi iddia ediyor. [S1]	Ayrı anlatımlar, kurumsal kapsamı, ortak işleteni veya paylaşanın ileri sürdüğü giriş yolunu doğrulamıyor.
F05	2026-01-23–2026-01-24	Belediye ulaşımı	Tekrarlanan iddia, 2.255 aracı; işletim, konum ve video cihazı referans alanlarını anlatıyor. [S1]	Canlı yayına erişim veya araçların kontrolü gösterilmiyor.
F06	2026-01–2026-11	Kamu hizmeti hesapları	Paylaşımlar; kimlik bilgileri, hesap günlükleri veya tekil kamu hizmeti hesaplarına erişim sunuyor. [S1]	Hesap malzemesi, hizmet altyapısında ihlal olduğunu göstermez; bazı teklifler açıkça eski tarihlere atıf yapıyor.
F07	2026-01–2026-11	Kimlik ve sorgulama piyasaları	Teklifler; kimlik, akrabalık, adres, taşınmaz, iş ve eğitim kayıtlarını sorgulama hizmetleri veya çevrim dışı kurulumlarla birleştiriyor. [S1]	Farklı arşiv ve hizmet iddiaları, tekil kişi veya tek bir yeni saldırı toplamına dönüştürülemez.
F08	2026-01–2026-11	Geçmiş veri kümelerinin dolaşımı	Çeşitli kataloglar veya yeniden paylaşımlar, malzemelerini açıkça önceki yıllarla etiketliyor. [S1]	Rapor döneminde yayımlanması, verinin elde edilmesini yeni bir olaya dönüştürmez.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F09	2026-02-17	Sigortacılık hizmetleri	Bir satıcı, çeşitli sigorta şirketlerine ve sektör bilgi hizmetlerine ayrıcalıklı erişim iddia ediyor. [S1]	Marka listesi, doğrulanmış olay listesi değildir; kimlik bilgileri ve ayrıcalıklar doğrulanmadı.
F10	2026-01–2026-11	Hesap bilgileri ve ödeme kartları	Teklifler; kimlikle ilişkilendirilmiş hesap bilgilerini, kart malzemesini ve mobil bankacılık parola verilerini anlatıyor. [S1]	Bu iddialar, banka altyapısına saldırı veya başarılı işlem göstermez.
F11	2026-02–2026-11	Bireyler ve çevrim içi hesaplar	Hizmet menüleri; hesaba izinsiz erişim, taklit, taciz ve kişisel veri sorgulama imkânları ilan ediyor. [S1]	Yetenek ilanı, doğrulanmış mağdur, başarılı eylem veya ulusal olay sayısı sağlamaz.
F12	2026-02–2026-11	Çevrim içi perakende	Ayrı paylaşımlar; müşteri dökümü sunuyor, şantaj ileri sürüyor, veri tabanı erişimi iddia ediyor veya ödeme verisi hırsızlığı anlatıyor. [S1]	Anlatımlar tek kampanyada birleştirilmiyor. İddia edilen hukuki yazışma ve erişim doğrulanmadı.
F13	2026-02-25	Oyun ve barındırma hizmetleri	Bir DDoS satıcısı, kendi testleri sırasında oyun kesintileri ve yönlendirme etkileri iddia ediyor. [S1]	Kişinin kendi bildirdiği etkiler, bağımsız ölçülmüş kesintiler değildir; bu iddia için altyapı testi yapılmadı.
F14	2026-03–2026-04	Sabit internet müşterileri	Şikâyet yönetimi verileri ve ayrı müşteri verisi tekrarları eski tarih etiketleri taşıyor; bazı kaynak iddiaları üçüncü tarafa işaret ediyor. [S1]	Farklı ilan miktarları ve veri kümeleri, tek olay veya mobil müşteri nüfusu olarak birleştirilmiyor.
F15	2026-04–2026-11	Reklam ve nakde çevirme piyasaları	İlanlar, kartla finanse edilen reklam ve ödeme tutarını nakde çevirme hizmetleri sunuyor. [S1]	İlan edilen harcama, kontrol aşma imkânı ve gelir; doğrulanmış kayıp veya platforma saldırı kanıtı değildir.
F16	2026-04–2026-11	Pazaryeri kullanıcıları	Paylaşımlar; satıcı taklidi, kurgulanmış ücretler, görev yaparak kazanç vaatleri ve doğrulanmış hesap stoku anlatıyor. [S1]	Marka taklidi ve hesap ticareti, gerçek platformun müşteri veri tabanına erişimi göstermez.
F17	2026-04-19–2026-04-23	Paket teslimatı müşterileri	Bir veri kazıma anlatımı ve ayrı bir kod örneği, alıcı ve gönderi alanlarıyla ilgili. [S1]	Aynı etkilenen sistem, yetkilendirme hatası, toplu dışarı aktarım ve elde edilme tarihi ortaya konmadı.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F18	2026-06–2026-07	Diplomatik ve sınır ötesi belgeler	Tekrarlanan teklifler, Türkiye'deki diplomatik temsilcilik arşivini ve ayrı bir yabancı savunma bağlantılı paketi anlatıyor. [S1]	Kaynak, hassasiyet ve süren erişim iddia düzeyindedir. Ayrı paketin içeriği bir Türk kuruluşuna atfedilmemeli.
F19	2026-06-24	Ödeme terminalleri	Bir satıcı, POS veya kasa sistemleri için çok ülkeli uzaktan erişim teklifine Türkiye'yi de dahil ediyor. [S1]	Etkilenen cihaz envanteri veya kullanılabilir erişim doğrulanmadı; tekliften kart kaybı tutarı çıkarılamaz.
F20	2026-07–2026-08	Kimlik ve telefon kayıtları	Paylaşımlar, 145 milyon kimlik ve telefon kaydı ilan ediyor. [S1]	Satırlar tekil kişi değildir. Ayrı Vaka D koleksiyonuyla ilişki doğrulanmadı.
F21	2026-07–2026-08	Hastane hastaları	Teklifler; klinik, randevu ve ödeme alanları içeren 20.000 hasta kaydını anlatıyor. [S1]	Kaynak ve elde edilme tarihi doğrulanmadı; bu, Vaka A'daki eski çalışan iddiasından ayrıdır.
F22	2026-08-30	Kâr amacı gütmeyen hizmetler	Bir aracı, sistem ayrıcalığı iddiasıyla Exchange internet postası erişimi sunuyor. [S1]	İlan edilen ayrıcalık ve kuruluş özellikleri doğrulanmadı; kimliği belirten ayrıntılar olarak tekrarlanmıyor.
F23	2026-09	İletişim listeleri ve kimlik belgeleri	Teklifler, Türkiye bağlantılı iletişim kayıtlarını pazarlıyor ve çok ülkeli arşive Türk pasaportlarını dahil ediyor. [S1]	Kaynak, yaş, miktar, rıza ve ortak köken belirsiz.
F24	2026-08–2026-11	Bahis platformu müşterileri	Farklı teklifler, müşteri veri kümelerini veya çok markalı koleksiyonları anlatıyor; bir dosya açıkça tekrar olarak etiketleniyor. [S1]	Katalogdaki marka sayısı, listelenen her platformda yeni olay yaşandığını göstermez.
F25	2026-09-14	Haber medyası kayıtları	Bir paylaşım, yaklaşık bir ay önce elde edilmiş gazete veri tabanı dökümü iddia ediyor. [S1]	Anlatımda miktar, kaynak ve erişim gösterimi yok.
F26	2026-09-17	Kişisel veri platformu	Bir yazar, Türk vatandaşlarının kişisel ve psikometrik bilgilerini açığa çıkaran bir platform iddia ediyor. [S1]	Anlatım eksik. Anlam, kaynak, rıza ve gerçek kapsam belirsiz.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F27	2026-10-09	Bağışçılar ve perakende müşterileri	Bir paylaşım, işlem alanları içeren 5.945 bağışçı veya müşteri kaydı ilan ediyor. [S1]	Kayıtların bağımsız olarak belirlenmiş tekil kişiler olduğu gösterilmedi; kaynak ve elde edilme tarihi doğrulanmadı.
F28	2026-10-17	Ulaşım ve hizmet sağlayıcıları	Bir teklif, çeşitli yıllardaki müşteri, sürücü, çalışan, araç ve hizmet talebi tablolarını bir araya getiriyor. [S1]	Tablo grupları örtüşebilir; tekil kişi toplamına dönüştürülemez. B12, seçilmiş paylaşım kanıtını sağlar.
F29	2026-10-20	Araç kayıtları	Bir teklif, araç plakası kaydı koleksiyonu iddia ediyor. [S1]	Kaynak, elde edilme tarihi ve gerçeklik doğrulanmadı; örnek plakalar ve kişisel kayıtlar çıkarıldı.
F30	2026-11-02–2026-11-04	İnternete açık uygulamalar	Erişim ilanları, Türkiye alan adı kayıtlarını içeriyor; bir üniversite kaydı satıldı olarak işaretlenmiş. [S1]	Satıcının durum etiketi; aktif erişimi, işlemi veya veri kaybını doğrulamaz.
F31	2026-11-05	Üretim sektöründe uzaktan erişim	Bir aracı, üretim ortamına yüksek ayrıcalıklı VPN erişimi ilan ediyor. [S1]	Ayrıcalıklar, güncel geçerlilik ve ilan edilen iş özellikleri doğrulanmadı; bu, Vaka F'den ayrıdır.
F32	2026-11-14	Endüstriyel üretim	Bir teklif, 690 GB ve bir milyondan fazla kurumsal ağ dosyası iddia ediyor; başka bir anlatım üretim tesisi veri tabanı sunuyor. [S1]	Teklifler ilişkilendirilmiyor. Boyut, dosyaların tekilliği, kaynak ve güncel erişim doğrulanmadı.
F33	2026-11-14	Sektörler genelinde internet uygulamaları	Çok siteli liste; uygulama açıkları, yönetim erişimi ve sunucu tarafında olası dosya çalıştırma iddia ediyor. [S1]	Hedefleri doğrulamak için test yapılmadı; liste, doğrulanmış zafiyet veya olay envanteri değildir.
F34	2026-11-16	Çevrim içi topluluk	Bir paylaşan, yerel siber topluluk sitesine erişim iddia ediyor ve videoya atıf yapıyor. [S1]	Anlatım, kanıtı, kayıp kapsamını veya daha geniş altyapı etkisini ortaya koymuyor.
F35	2026-11-19	Hukuk hizmetleri belgeleri	Bir paylaşım, hukuk hizmetleri belgesi sızıntısı ileri sürüyor ve banka müşterisi ilişkileri iddia ediyor. [S1]	İddia edilen müşteri ilişkisi, müşteri bankaların sistemlerine erişimi veya belgelerin gerçekliğini göstermez.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F36	2026-05-26	Veterinerlik kayıtları	Bir paylaşım, veteriner hekimlere ilişkin kayıtlar sunuyor. [S1]	Miktar, kaynak, elde edilme tarihi ve kişi kapsamı ayrı doğrulama gerektirir.
F37	2026-10-07	İletişim izni hizmetleri	Bir paylaşım, izin yönetimi sistemiyle bağlantılı veri ifşası ileri sürüyor. [S1]	Platform ilişkisi, kişi kapsamı ve aktif erişim doğrulanmadı.
F38	2026-10-17	Finans hizmetleri arşivi	Finans veya kripto para bağlantılı arşiv teklifi; belgeleri, veri tabanı dosyalarını ve işlem kayıtlarını birleştiriyor. [S1]	Dosya, kimlik ve işlem farklı birimlerdir. Tekil müşteri toplamı veya doğrulanmış canlı erişim sağlanmıyor.
F39	2026-10-20	Telefon sorgulama derlemesi	Küresel sorgulama ilanı, büyük bir Türkiye bağlantılı alt küme iddia ediyor. [S1]	Ülke etiketli satırlar; tekil kişileri, yeni kaynağı veya ulusal sisteme saldırıyı göstermez.
F40	2026-01–2026-11	Banka, cüzdan ve pazaryeri hesapları	Tekrarlanan paylaşımlar, bazen kimlik, cihaz veya SIM malzemesiyle birlikte satılık ya da kiralık hesap sunuyor. [S1]	Tekrarlanan teklifler, tekrarlanan saldırılar değildir. Rıza, tamamlanan devirler ve işlevsel erişim doğrulanmadı.
F41	2026-03–2026-11	Restoran müşterileri	Çeşitli paylaşımlar, restoran müşterisi veya sipariş veri kümelerini anlatıyor. [S1]	Bazı anlatımlarda kaynak, ülke ilişkisi ve satırların kişi karşılığı belirsiz; ortak olay varsayılmıyor.
F42	2026-01–2026-11	Üyelik ve yönetim kayıtları	Paylaşımlar, siyasi üyelik ve yönetici kayıtları ilan ediyor. [S1]	Adlar ve yüklü söylem çıkarıldı. Kaynak, gerçeklik ve ortak veri kümesi kimliği doğrulanmadı.
F43	2026-06–2026-07	Kamu hizmeti e-postasıyla bağlantılı piyasa	Tekrarlanan çok ülkeli hizmet ilanı, yerel kullanılabilirlik ve e-postayla bağlantılı hizmetler iddia ediyor. [S1]	Çalışan resmî hesap, kurum olayı veya devlet desteği ortaya konmadı; tekrar bağımsız kanıt değildir.
F44	2026-11-19	Trafik ve bahis kayıtları	Bir satıcı, hesap envanteriyle birlikte trafik kazası raporu ve bahis veri kümeleri listeliyor. [S1]	İki veri kümesi etiketi, iki olay göstermez; kaynak ve elde bulundurma doğrulanmadı.
F45	2026-01–2026-11	Taklit araçları	İlanlar; bankacılık, alışveriş ve kamu hizmeti temalı oltalama veya taklit araçları sunuyor. [S1]	Gerçek markalar, taklit edilen taraflardır; altyapılarına saldırı veya ortak işleten ortaya konmadı.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F46	2026-01-04–2026-01-19	Sabit hat müşterileri	Yeniden paylaşılan müşteri verisi anlatıları, eski bir veri edinme öyküsünü uygulamaya yeniden erişildiği iddiasıyla birleştiriyor. [S1]	Birbiriyle çelişen kişi sayıları açıklığa kavuşmadı. Tekrarlar, yeni erişimi veya yeni bir müşteri grubunu doğrulamıyor.
F47	2026-01-04	Savunma tedarikçisi belgeleri	Bir gönderi, savunma tedarikçisine ait olduğu öne sürülen büyük bir arşivin elde bulunduğunu ve kaynağının çalışan e-postaları olduğunu iddia ediyor. [S1]	Özgünlük, edinme tarihi, çalışan hesaplarına erişim ve süren erişim doğrulanmadı. Siyasi mesajlar herhangi bir devlete atfedilmiyor.
F48	2026-01–2026-03	Belgeler, haberleşme ve nakde çevirme	Ayrı ilanlar şirket veya ikamet belgeleri arıyor; belgesiz internet telefonu veya kripto parayı nakde çevirme hizmetleri sunuyor. [S1]	Rıza, kaynak, hizmetin çalışması ve tamamlanan işlemler doğrulanmadı. İlanlar tek bir işletene bağlanmıyor.
F49	2026-01-21	Sosyal platform kullanıcıları	Bir gönderi, Türk kullanıcılara ait olduğunu öne sürdüğü bir veri kümesi sunuyor ve toplama dönemini 2022–2026 olarak tanımlıyor. [S1]	Kaynak, etkilenen kişi grubu, güncel erişim ve daha önce dolaşan arşivlerle ilişki açıklığa kavuşmadı.
F50	2026-01-22	Araç ve sigorta kayıtları	Bir ilan, sigortayla ilgili alanlar içeren 36.046 araç kaydı iddia ediyor; kaynağa ulaşılamayınca toplamanın sona erdiğini söylüyor. [S1]	Kayıtlar benzersiz araç sahiplerini göstermiyor. Kaynak, edinme tarihi, eksiksizlik ve canlı arayüz erişimi doğrulanmadı.
F51	2026-01-31–2026-02-03	Abonelik ödemelerinin kötüye kullanımı	Gönderiler, Türkiye konumu ve ödeme etiketleri kullanarak bölgesel abonelik ödeme yöntemleri tanıtıyor. [S1]	Geçerli kart, tamamlanan tahsilat, hizmet hakkı veya gerçek platforma sızma doğrulanmadı.
F52	2026-04-13	Banka ve şirket sorgulama araçları	Bir ilan, şifre veya vergi numarasıyla otomatik banka hesabı ve şirket bilgisi sorgulaması yapabildiğini iddia ediyor. [S1]	İşlevler, kaynak ve canlı hesaplara erişim doğrulanmadı. Örnek alanlar, banka altyapısına erişim kanıtı oluşturmuyor.
F53	2026-05-03	Adres kayıtları	Bir ilan, Türkiye vatandaşlarına ait 15.203.213 adres kaydı iddia ediyor ve gönderiden birkaç gün önce elde edildiğini söylüyor. [S1]	Güncellik, kaynak, rıza ve benzersiz kişi anlamı doğrulanmadı. İddia edilen satır sayısı ulusal mağdur sayısı değildir.

Referans	Paylaşım tarihleri	Rol veya konu	Saklanan anlatımdaki iddia	Kanıt sınırı
F54	2026-11-15	Ormancılık çalışanlarının kayıtları	Yeniden paylaşılan bir gönderi, ormancılık çalışanlarıyla ilişkilendirilen kimlik, telefon ve yeterlilik alanları sunuyor; iddia edilen sızıntıyı açıkça 2021 olarak etiketliyor. [S1]	2026 yılında paylaşılması, yeni veri edinildiğini göstermiyor. Özgünlük, kişi grubu ve rıza doğrulanmadı.
F55	2026-01-05–2026-01-07	Tüketici taklidi ve peşin ücret talepleri	Bir kişisel anlatı, kargo şirketi temalı bir aramayı aktarıyor. Ayrı bir kandırma metni, sözde kazanılan ödül için kayıt veya vergi ödemesi istiyor. [S1]	Tamamlanan ödeme, gerçek kurum katılımı ve ortak yazarlık doğrulanmadı.
F56	2026-02-24	Kısıtlı kayıtların kötüye kullanılması iddiası	Bir kanal, kurum içindeki kişilerin kısıtlı kişisel kayıtları paylaştığı suçlamalarını aktarıyor. [S1]	Dayanak soruşturma ve özgün haber bağımsız olarak doğrulanmadı. Aktarım; görevi kötüye kullanmayı, mahkûmiyeti veya yeni bir sisteme sızmayı ortaya koymuyor.
F57	2026-02–2026-04	Belge ve ödeme dekontu düzenleme	Karma hizmet listeleri; kimlik belgesi, ruhsat, form, diploma ve ödeme dekontu düzenleme ilanları içeriyor. [S1]	İşlevler, yetki ve tamamlanmış doğrulama atlatma işlemi doğrulanmadı. Veri tabanına kayıt ekleme iddiası, erişimin kanıtlandığı anlamına gelmiyor. Ortak fail varsayılmıyor.
F58	2026-04-23	Telekomünikasyon yönetimi	Bir kanal, bir sağlayıcının 5 birimine hizmet veren yönetim sistemini kontrol ettiğini iddia ediyor. [S1]	İddia edilen birimler, ayrı şirket veya doğrulanmış olay değildir. Erişim, kontrol değişiklikleri, failin kimliği ve hizmet etkileri doğrulanmadı.
F59	2026-10-23	Uzaktan süreç kontrol panelleri	Bir aktarım, adı belirtilmeyen bir araştırmacının 161 uzaktan kontrol sistemine eriştiğini öne sürüyor. [S1]	Özgün kanıt, sahiplik, benzersiz tesisler, yetkisiz değişiklikler ve fiziksel sonuçlar doğrulanmadı. Vaka H ile ilişki kurulmadı.

Bu rapor hakkında

Odin by Brandefense; güvenlik yönetimi, operasyon, altyapı, kimlik, dolandırıcılıkla mücadele, gizlilik ve tedarikçi riski ekipleri için bu ülke raporunu hazırladı. Saklanan kurum kanıtını kaynağından doğrulanmış bağlamla birleştirir. Mağdur göstergesi, kişi satırı, erişim yolu veya iç araştırma işleyişi açıklamaz.

Paket, serinin ayrı editörlük ve yayın iş akışı için hazırlanmıştır. Kuruluş maruziyeti rakamları ile eksik kaynak kapsamı görünür sınırlar olarak kalır. Çevrilmiş sürümün yorumunda İngilizce ana metin esas alınır.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO