SİBERKAPAN

TÜRKİYE TEHDİT RAPORU

Sayı 1 — Haziran 2026

Gözlem Dönemi

9 Haziran 2026 — 28 Haziran 2026

siberkapan.org
Türkiye'ye Özgü Siber Tehdit İstihbaratı — MISP Resmi Feed

Yönetici Özeti

9 Haziran – 28 Haziran 2026 döneminde 28.896 benzersiz tehdit IP'si tespit edildi.

Yakalanan tehditlerin %45,3'ü, küresel veritabanlarında (AbuseIPDB) henüz hiç kaydı bulunmayan IP'lerden geldi (Novel Detection).

Büyük ölçekli bir finansal altyapıda, devreye alınmasından sonraki ilk 48 saat içinde 609.000'den fazla saldırı policy seviyesinde gerçek zamanlı olarak engellendi.

Giriş

SiberKapan, 2023'te Türkiye-içi honeypot tabanlı bir feed olarak başladı; 2026'da sıfırdan yeniden inşa edilen v2 ile uluslararası MISP tehdit istihbaratı ağına resmi feed olarak kabul edildi.Artık dünyadaki güvenlik ekiplerinin tek tıkla entegre edebileceği, küresel ölçekte tanınmış bir kaynak.

Bu rapor, SiberKapan'ın honeypot, FortiGate Security Fabric entegrasyonu, fail2ban ve nginx imza motorundan topladığı verilere dayanarak Türkiye merkezli tehdit görünümünü ortaya koymayı amaçlamaktadır.

Genel Görünüm

Raporlama döneminde (9 Haziran 2026 – 28 Haziran 2026) SiberKapan, 28.896 benzersiz tehdit IP adresi tespit etti. Coğrafi dağılımda Çin (%43,0) ve Türkiye (%23,4) ilk iki sırada yer aldı, bunları ABD (%5,3), Hindistan (%4,0) ve Hollanda (%2,9) takip etti.

28.896	9-28 Haz	Çin %43,0
Benzersiz Tehdit IP	Gözlem Dönemi	En Yüksek Kaynak Ülke

Ülke	Kod	IP Sayısı	Yüzde
Çin	CN	12.430	%43,0
Türkiye	TR	6.759	%23,4
Amerika Birleşik Devletleri	US	1.537	%5,3
Hindistan	IN	1.143	%4,0
Hollanda	NL	842	%2,9
Pakistan	PK	785	%2,7

Almanya	DE	491	%1,7
Ukrayna	UA	342	%1,2
Hong Kong	HK	334	%1,2
Rusya	RU	321	%1,1

Not — Türkiye Kaynaklı Trafiğin Doğası

Türkiye kategorisindeki IP'lerin ASN/altyapı analizi, bu trafiğin üç farklı kaynaktan birinden veya birkaçının kombinasyonundan gelebileceğini gösteriyor:

(1) ele geçirilmiş ev/IoT cihazları üzerinden çalışan botnet'ler,

(2) Türkiye'de barındırılan ancak yabancı aktörler tarafından kiralanan VPS/VDS sunucuları,

(3) yerli aktörler tarafından doğrudan kullanılan altyapı.

Mevcut veri, ağırlıklı olarak Türk hosting/VPS sağlayıcılarında (tüketici ISP'lerine kıyasla) bir yoğunlaşma göstermekte olup, bu da ikinci ihtimali güçlendiriyor. Literatürde “Bulletproof Hosting” ve “Egress Node” olarak tanımlanan modellerle örtüşen bir yoğunlaşma deseni olabileceği değerlendirilmektedir — saldırganların coğrafi konum filtrelerini (Geo-IP blocking) aşmak amacıyla yerel VPS kiraladığı senaryolar bilinen bir taktiktir. Ancak bu IP'lerin büyük kısmı doğrulama süreci devam eden bir tespit kategorisinden geldiği için kesin bir sonuca varılmamıştır; bu konu ayrıca araştırılmaktadır.

Sensörlerimizin Yakaladığı: Organik Tespit

Üçüncü taraf feed'lerden ödünç alınmış bir liste değil, bu bölümdeki her satır, SiberKapan'ın kendi honeypot'larına, fail2ban entegrasyonuna ve nginx imza motoruna gerçek zamanlı çarpan trafikten geliyor.

Haziran ayı içindeki bu ~20 günlük pencerede, organik sensörler toplam 11.757 kayıt ve 1.563 benzersiz IP yakalandı. Listenin başını, hiç şaşırtmayan bir klasik çekiyor:

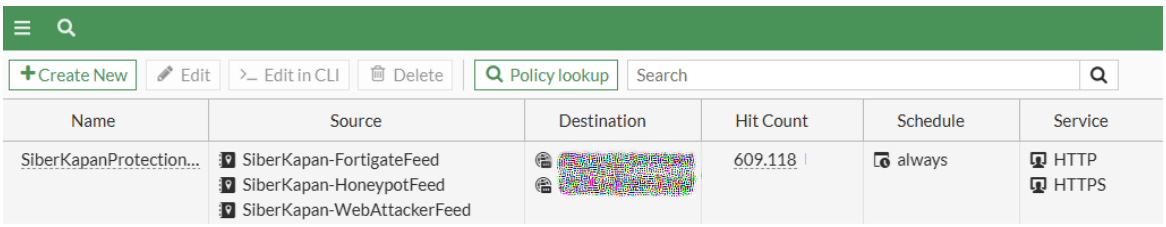
SSH brute-force (7.606 kayıt / 303 IP) internetin en eski, en sabırlı ziyaretçisi, hâlâ kapıyı çalıyor. Onu Telnet (2.152 kayıt / 471 IP) takip ediyor.Devamında Fail2ban(1470 kayıt / 515 IP),HTTP kabakuvvet (254 kayıt / 152 IP) ,RDP saldırıları (168 kayıt / 96 IP) ve en yeni tehdit istihbarat aktörümüz olan Nginx Access log paternlerinden çıkardığımız olaylar (52 kayıt / 38 IP) takip ediyor.

Saldırı Tipi	Kayıt	Benzersiz IP
SSH Brute-Force	7.606	303
Telnet	2.152	471
Fail2ban Engellemeleri	1.470	515
HTTP Honeypot	254	152
RDP	168	96
Nginx İmza Tespitleri (UA + Path)	52	38

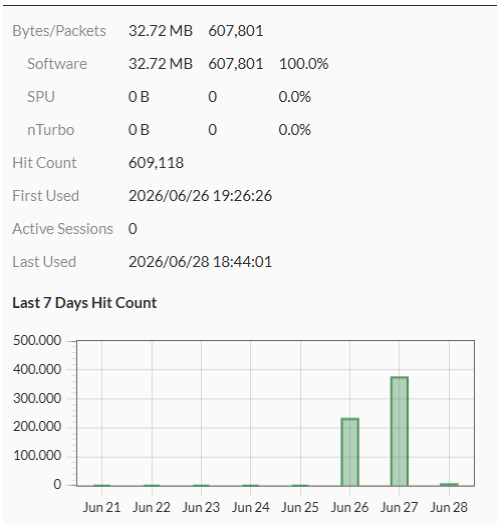
Vaka: Kritik Hacimli Bir Altyapıda Gerçek Dünya Etkisi

Teoriler güzeldir, ancak SiberKapan'ın bunu sahada da kanıtlaması gerekiyordu. Haziran ayında, Türkiye'de günlük işlem hacmi on milyonlara ulaşan bir finansal/e-fatura altyapısında SiberKapan, FortiGate üzerinde External Connector olarak devreye alındı.

Sonuç: devreye alınmasından sonraki ilk 48 saat içinde **609.118** policy seviyesinde engelleme yani SiberKapan'ın beslediği tehdit verisi, devreye girdiği ilk günlerde saldırgan trafiği gerçek zamanlı olarak durdurdu. Bu, bir laboratuvar deneyi değil; üretimde, gerçek veriyle gerçek parayla işlemlere açık çalışan bir sistemde alınan ilk somut etki ölçümü.



FortiGate Policy— SiberKapan beslemeli koruma kuralı, 609.118 hit (hedef bilgisi gizlenmiştir)



Hit Count Dağılımı — ilk kullanım 26 Haziran 19:26, 27 Haziran'da yoğunlaşıyor

Önden Görmek: Novel Detection

Bir tehdit istihbaratı platformunun asıl sınavı, bilineni tekrar etmek değil henüz kimsenin bilmediğini ilk gören olmaktır.

10.867	%45,3
Karşılaştırılan IP	Novel Detection Oranı

Bu dönemde AbuseIPDB ile karşılaştırılan 10.867 IP'nin %45,3'ü (4.926 IP), SiberKapan tarafından tespit edildiği anda AbuseIPDB'de hiçbir rapor kaydına sahip değildi.Sıfır rapor, sıfır confidence skoru. Başka bir deyişle, bu IP'ler dünyanın en büyük topluluk tabanlı tehdit veritabanında henüz tanınmamışken, SiberKapan onları zaten yakalamıştı.

Bu, şans eseri bir rakam değil, SiberKapan'ın honeypot öncelikli mimarisinin doğal bir sonucu saldırgan, büyük feed'lere rapor edilmeden önce küçük, sabırlı bir tuzağa düşüyor.

Metodoloji Notu

“Novel detection”, tarih bazlı bir kıyaslama değil, AbuseIPDB'nin ilgili IP için toplam rapor sayısının ve confidence skorunun sıfır olduğu durumlar baz alınarak hesaplanmıştır. Bu yöntem, zaman damgası temelli karşılaştırmaların taşıdığı yorum belirsizliğini ortadan kaldırmak için tercih edilmiştir.

Bu Rapor Hakkında

Bu, SiberKapan Türkiye Tehdit Raporu'nun ilk sayısıdır ve 9 Haziran 2026 – 28 Haziran 2026 veri penceresini kapsamaktadır. Bu nedenle rapor, bir trend analizi değil, bir başlangıç noktasıdır. Gelecek sayılarda dönemsel karşılaştırmalar yapılabilmesi için referans işlevi görecektir.

Şeffaflık ilkesi doğrultusunda, aşağıdaki veri kategorileri bu rapora kasıtlı olarak dahil edilmemiştir:

- **UDP Flood tespitleri:** Doğrulama süreci devam eden bir tespit kategorisi olduğu için (yanlış pozitif riski nedeniyle inceleme altında), bu rapordaki hiçbir istatistiğe dahil edilmemiştir.
- **Harici feed kaynaklı toplu veri (örn. malware_distribution):** Bu kayıtlar SiberKapan'ın kendi tespiti değil, üçüncü taraf feed'lerden alınan veridir; “organik tespit” istatistiklerinde ayrı tutulmuştur.

SiberKapan, 2023'te Türkiye-içi honeypot tabanlı bir feed olarak başladı; 2026'da sıfırdan yeniden inşa edilen v2 ile uluslararası MISP tehdit istihbaratı ağına resmi feed olarak kabul edildi. Artık dünyadaki güvenlik ekiplerinin tek tıkla entegre edebileceği, küresel ölçekte tanınmış bir kaynak haline geldi.

Önerilen Aksiyonlar

Bu raporda gözlenen saldırı kalıplarına karşı önerilen, kısa ve uygulanabilir savunma adımları:

- **SSH / Telnet:** Standart portların değiştirilmesi, Telnet'in tamamen devre dışı bırakılması ve brute-force korumasının firewall/SIEM seviyesinde aktif edilmesi önerilir.
- **FortiGate / SIEM Entegrasyonu:** SiberKapan MISP feed'inin External Connector olarak bağlanması, bilinen kötü niyetli IP'lerin gerçek zamanlı engellenmesini sağlar.
- **Web Uygulama Güvenlik Duvarı (WAF):** Nginx imza tespitlerinde görülen User-Agent ve path bazlı kalıplara karşı katı WAF kurallarının devreye alınması önerilir.
- **VPS/Hosting Sağlayıcıları:** Anormal çıkış trafiği gösteren sunucu kiralamalarının (özellikle kısa süreli, yüksek hacimli) izlenmesi, olası kötüye kullanımın erken tespitine yardımcı olabilir.