GELİŞMİŞ TEHDİT ÖNLEME HİZMETİ APT

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir

Gelişmiş Tehditler

(APT- Advanced Persistent Threat)

• Gelişmiş tehditler sürekli, sosyal mühendislik gibi korsanlık tekniklerini kullanarak sistemlere erişmeye çalışır.

• Bulaştığı sistemlerde yıkıcı sonuçlar yaratmaya yetecek kadar uzun süre boyunca kalabilir.

APT Saldırıları Nasıl Bulaşır?

• Zararlı yazılım içeren web sitelerinden

• Oltalama amacıyla gönderilmiş e-mail eklerinden

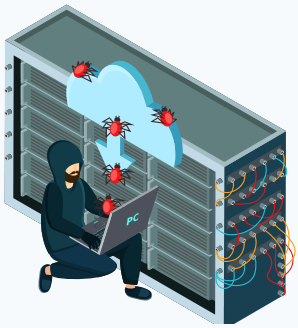
• Enfekte olmuş USB belleklerden

Ele Geçirme

Enfekte olmuş cihaz, sistemin komuta&kontrol sunucusuna bağlanarak kendi talimatlarını uygulamaya çalışır.

Yayılma

Sistemin zafiyetlerinden faydalanarak aynı ağ içindeki diğer sistemlere de fark edilmeden yayılır.



Veri Sızıntısı

İçeride yayılmış olan zararlı yazılım e-maillerden, dokümanlardan, Skype gibi anlık mesajlaşma uygulamalarından ya da web kameralardan veri sızıntısı yapabilir.

Sıfırıncı Gün Atak İstatistikleri

Günlük incelen zararlı yazılımların **%28** ila **%40'ının** sıfırıncı gün atakları olduğu tespit edilmektedir.*

Zararlı yazılımların **%94'ü** mail yolu ile bulaşmaktadır.**

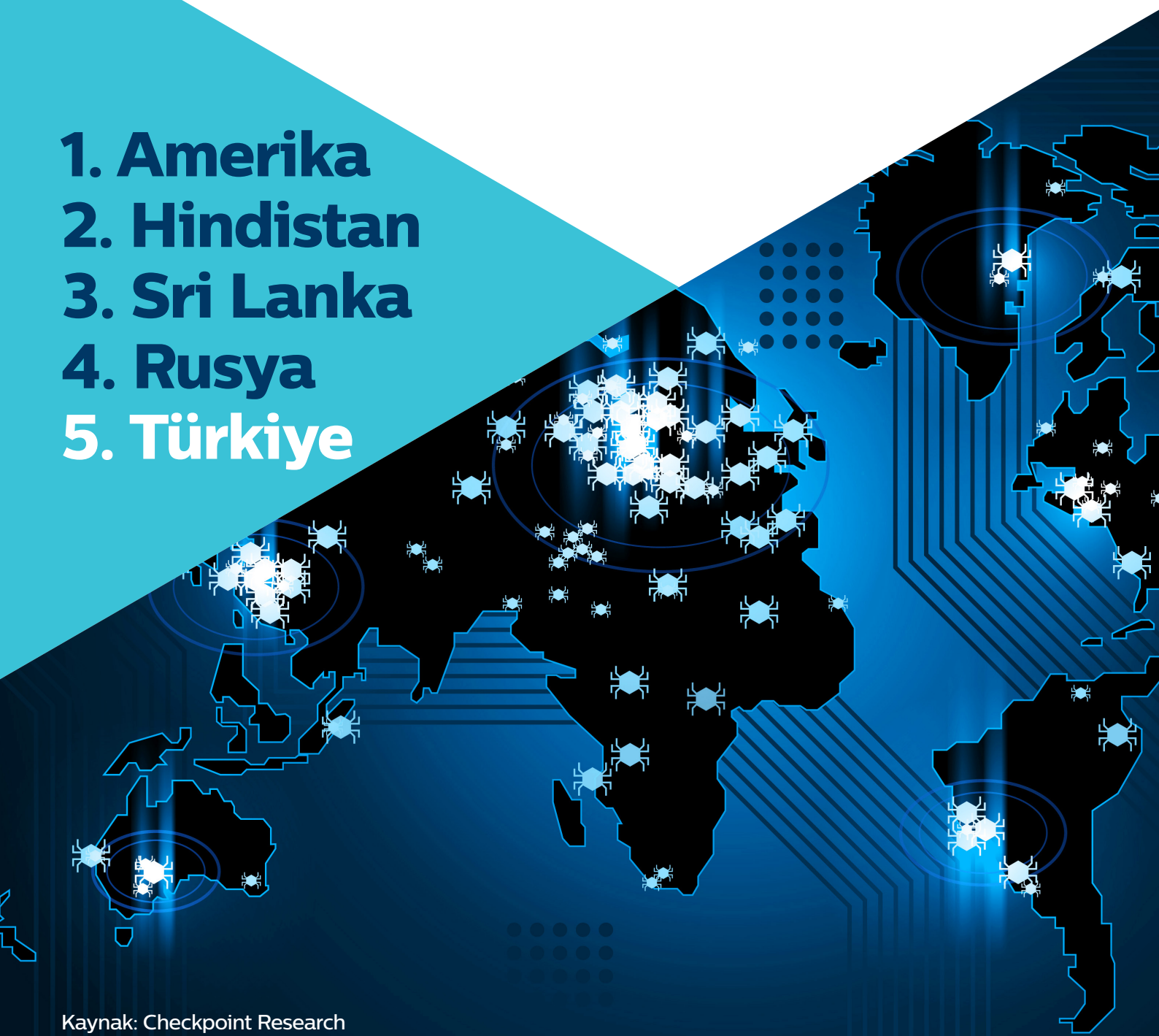
Fidye yazılımların sayısı 2020 üçüncü çeyreğinde yılın ilk yarısına kıyasla günlük ortalama **%50** artış göstermiştir.***

Kaynaklar:
*Fortinet Fortiguard Labs
** Verizon 2019 Data Breach Investigation Report
*** Checkpoint Research

Türkiye En Çok Atak Alan Ülkeler Arasında 5. Sırada

2020'nin ilk çeyreğinde Türkiye, %32,5'lik vaka artışı ile fidye yazılım saldırılarından en çok etkilenen 5. ülke oldu.

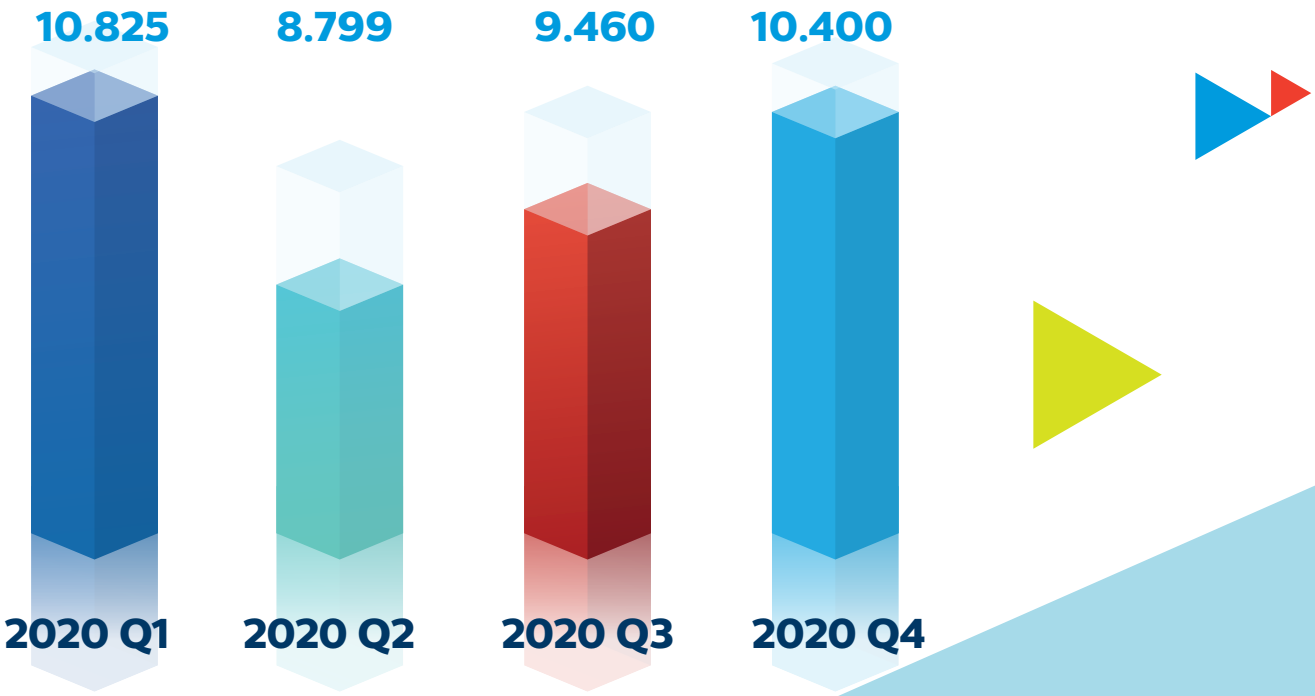
1. Amerika
2. Hindistan
3. Sri Lanka
4. Rusya
5. Türkiye



Kaynak: Checkpoint Research

Türk Telekom APT Atak İstatistikleri

Türk Telekom APT servisinde 2020 yılı içinde tespit edilen zararlı dosya sayılarının çeyrek bazlı dağılımı

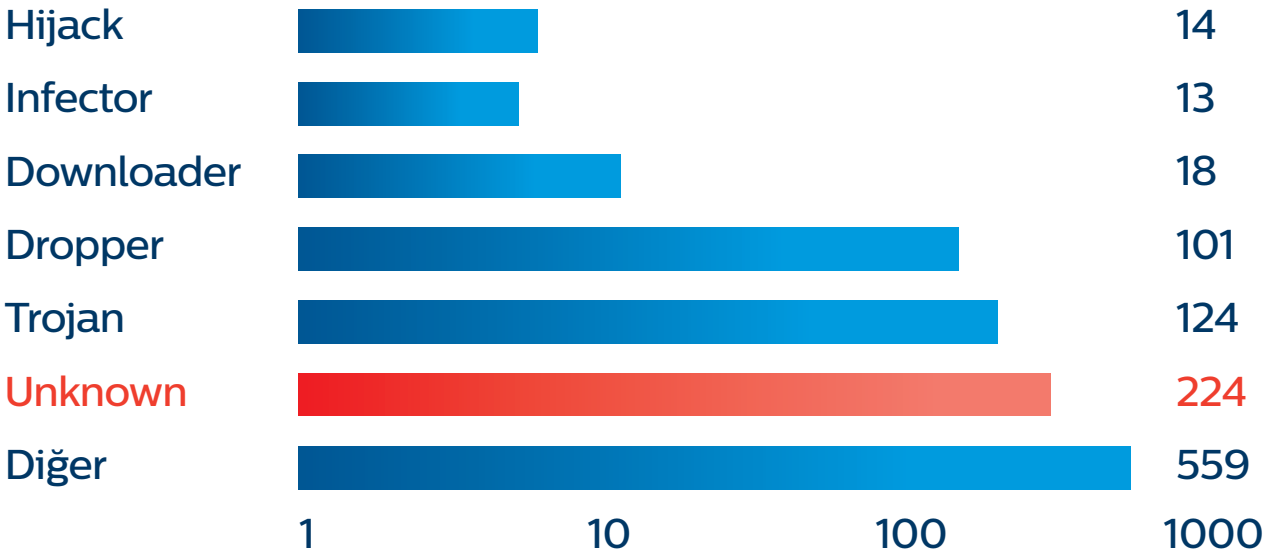


Üretici Yedekli Altyapı ile yüksek dosya tarama kapasitesi

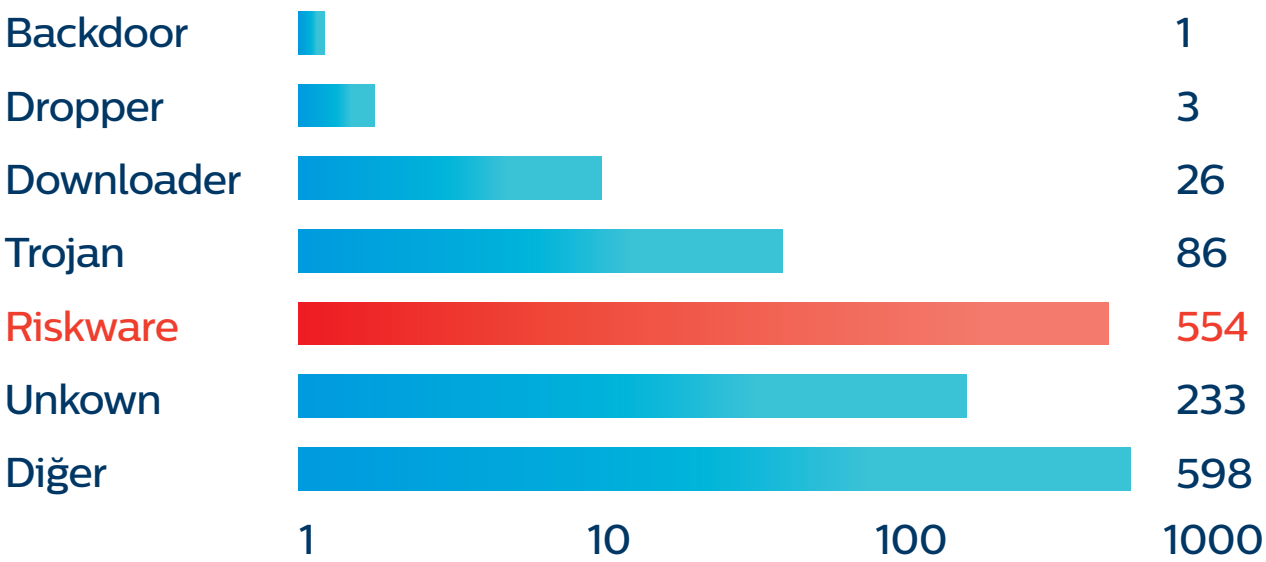
paloalto NETWORKS	FORTINET
12.000 dosya / saat	**15.000** dosya / saat

Kritiklik Seviyelerine Göre Kategori Bazlı Tehdit Sayıları

Yüksek Riskli



Düşük / Orta Riskli



*2020 yılında Türk Telekom servislerinde incelenen zararlı yazılım verileridir.

Türk Telekom Gelişmiş Tehdit Önleme Servisi

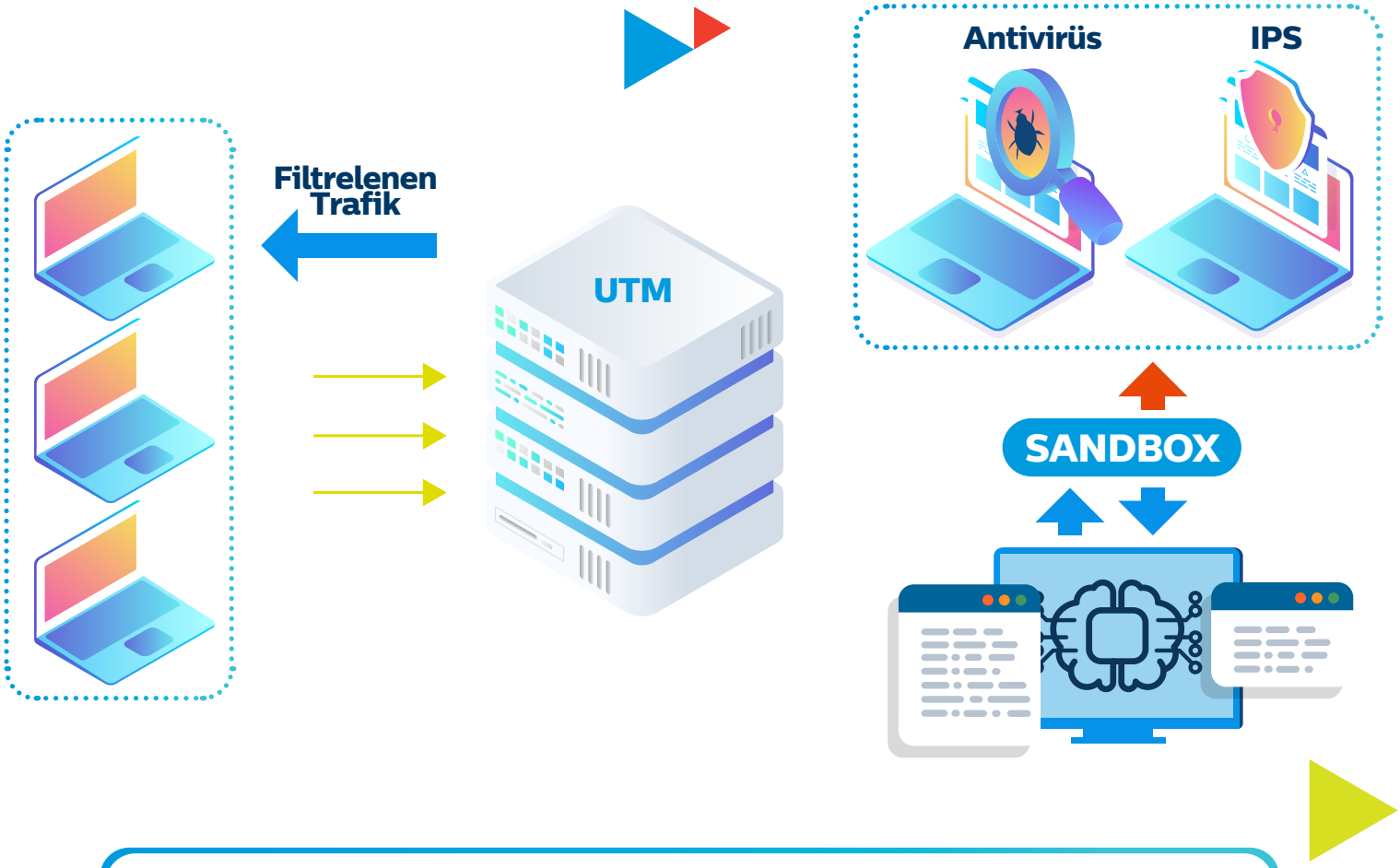
Türk Telekom'un omurgadan sunmakta olduğu APT servisi ile hızlı devreye alım ve kurulum kolaylığından yararlanarak sistemlerinizi oltalama saldırıları ve sıfırıncı gün ataklarına karşı koruma altına alabilirsiniz.

APT, Antivirüs ve IPS servisleri ile entegre çalışarak ihtiyacınız olan hızlı ve esnek çözümü sunmaktadır.

Türk Telekom uzman kadro desteği ile siber ataklar sistemlerinize ulaşmadan omurga seviyesinde engellenir.

APT servisi erişim bağımsız sunulmaktadır, farklı operatörden hizmet alan internet müşterileri de Türk Telekom APT servisinden aylık ödeme modeli ile yararlanabilir.

Türk Telekom APT Servisi Nasıl Çalışır?



Gelişmiş Tehdit Önleme
Sıfırıncı gün ataklarına karşı koruma sağlar.

İnternet üzerinden indirilen dosyaları inceler ve analiz eder.

Zararlı olduğunu tespit ettiği dosyaların indirilmesini önler.

Sandboxing (Denetleme Ortamı), siber istihbarat ve raporlama sunar.

Tüm atak vektörleri için koruma sağlanır. (E-mail, web trafiği, anlık mesajlaşma)


Türk Telekom
Değerli Hissettirir