

AĞ ANALİZ RAPORU

Cihaz gözlemleri, domain bağlamı ve inceleme bulguları

CİHAZ

Muhasebe-PC

192.0.2.15 / QUIC

SENARYO PENCERESİ

12.10.2026 / 14:00 - 14:32

DATASET 01 / OFFICE

İNCELEME ÖNCELİĞİ

92

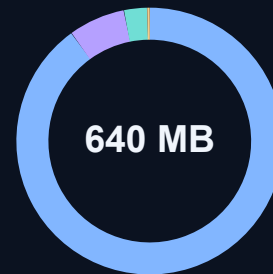
/100

YÜKSEK

DEĞERLENDİRME ÖZETİ

Tekrarlayan QUIC akışları, DNS ile ilişkilendirilen bir domain ve yüksek itibar sinyali bu senaryoda aynı cihaz üzerinde birleşiyor. Bu göstergeler bağlantının incelenmesine öncelik verir; tek başına zararlı yazılım tanısı oluşturmaz. Domain bağlamı, kaynak sinyalleri ve cihazın beklenen kullanımı birlikte değerlendirilir.

TRAFİK DAĞILIMI



- Ana domain
- Finans
- Teknoloji
- DNS

384

DNS SORGUSU

7

BAŞARISIZ SORU

4

GÖSTERİLEN DOMAIN

İNCELEME SİNYALLERİ

- 01 Tekrarlayan dış QUIC bağlantıları
- 02 DNS önbelleğiyle domain eşleşmesi
- 03 Yüksek domain itibar sinyali

ÖNERİLEN İNCELEME

Hedef domainin ve bağlantıyı başlatan uygulamanın beklenen iş akışıyla ilişkisini kontrol et. DNS eşleşmesini ve itibar kaynağını doğrula.

AĞ ANALİZ RAPORU

Cihaz gözlemleri, domain bağlamı ve inceleme bulguları

DOMAIN VE KAYNAK AYRINTILARI

Kategori, itibar ve bağlantı bağlamı ayrı değerlendirilir

Domain	Kategori	Protokol	Risk	Hacim
update-check.example	Unknown / Suspicious	QUIC	92	576 MB
binance.com	Finance	TCP / TLS	8	44 MB
resources.example	Technology	TCP / TLS	5	18 MB
resolver.internal.example	Infrastructure	DNS	1	2 MB

FALSE POSITIVE / KATEGORİ ≠ RİSK

binance.com finans kategorisinde gösterilir; bu, tek başına zararlı davranış kanıtı değildir. Eski örnekteki 72 yerine bu senaryoda 8/100 kullanıldı. Bu bir canlı itibar sorgusu veya güncel güvenlik hükmü değil, bağlamın yanlış pozitifleri nasıl azaltılabileceğini gösteren temsili bir düzeltmedir.

OSINT KAYNAKLARI / ÖRNEK KANIT YAPISI

VirusTotal v3	Motor sonuçları ve itibar etiketleri / senaryo sinyali
Safe Browsing v4	URL eşleşmesi / malware ve social engineering listeleri
WHOIS	Domain yaşı / eksik tarih bilinmiyor olarak tutulur
TLS / DNS	Issuer, tarih, self-signed metadata / IP-domain ilişkisi
GeoLite2	Country ve ASN bağlamı / tek başına risk hükmü değil

YÖNTEM VE KAPSAM

Tüm skorlar, hacimler, sorgular ve itibar sinyalleri demo için hazırlanmıştır. IP'ler documentation aralığındadır. Kategori güveni risk skoru değildir; ASN, ülke veya HTTPS tek başına karar vermez. Model çıkarımı veya API sorgusu bu PDF oluşturulurken çalıştırılmadı.