



Araştırma dosyaları

Çalışmalar

E-kütüphane

Hakkında

TR

EN



DOSYA İNCELEME

Dosyayı açın. Kaydı inceleyin.

Bir dosya seçin. Kimlik, yapı, bulgu, açık gösterge ve ilişki kayıtları gerçek dosya baytlarından aynı çalışma alanında üretilir.

01 Dosya incele

02 Metin, log veya e-posta başlığı

DOSYA KABULÜ

Dosyayı buraya bırakın

Görsel, PDF, Office, e-posta, PCAP, APK, OCI, arşiv, script ve binary.

[Dosya seç](#)

veya sürükleyip bırakın, En fazla 64 MB. Dosya bellekte tutulur ve sayfa yenilendiğinde silinir.

İŞLEM SINIRLARI

Analiz yeri **Bu tarayıcı sekmesi**

Yerel rapor dosyayı sekmeden çıkarmaz.

Sunucuya gönderim **Yalnızca açık onayla**

Uygun türlerde isteğe bağlı derin analiz siz başlatana kadar dosyayı göndermez.

Dosya boyutu **64 MB yerel, 25 MiB derin**

Sınır üstündeki dosyalar reddedilir.

Çalıştırma

Dosya ve belge incelemesi nasıl kuruldu

Bir dosyayı çalıştırmadan ve hiçbir yere yüklemeyen, tarayıcıda inceliyorum. Kimliğini, yapısını ve içinde açıkça yazan göstergeleri çıkarıyor, her bulguyu dosyadaki kaynağına bağlıyorum. Sonuç bir karar değil, kontrol edilebilir bir kayıt.

1 Bu inceleme ne için var

Şüpheli bir ek geldiğinde ilk refleks onu bir çevrim içi tarayıcıya yüklemek. Ama bu, dosyayı başkasına vermek demek. İçinde müşteri verisi ya da iç yazışma olabilir. Ben ilk bakışın cihazdan hiç çıkmamasını istedim.

Bu yüzden yerel inceleme tamamen tarayıcı sekmesinde çalışıyor. Dosya okunur, ayrıştırılır, rapor üretilir ve sayfa yenilenince her şey kaybolur.

1. Sınırdaki kontrol Boyut, biçim ve okunabilir yapı. Sınırı aşan dosya açık bir hatayla durur.	2. Arka planda oku Baytlar ayrı bir tarayıcı Worker'ında okunur. Ekran kilitlenmez.	3. Kimlik ve tür SHA-256 ve görünen yapı. Dosya adına güvenilirmez.	4. Yapı ve göstergeler Desteklenen alanlar ve dosyada açıkça yazan URL, alan adı, IP, e-posta, hash ve CVE.	5. Kanıt paketi Rapor, manifest, gösterge kayıtları ve grafik. İncelenen dosya pakette yok.
---	---	---	---	---

Birkaç kelime

Statik inceleme	Dosyayı çalıştırmadan, yalnızca baytlarına bakarak yapılan inceleme.
SHA-256	Dosyanın parmak izi. Aynı dosya her zaman aynı değeri verir.
Magic bytes	Dosyanın başındaki, gerçek türünü gösteren birkaç bayt. Uzantı yalan söyleyebilir, bunlar daha zor.
Açık gösterge (IOC)	Dosyanın içinde düz metin olarak geçen adres, alan adı, IP, e-posta, hash ya da CVE.
Tarayıcı Worker'ı	Sayfanın ana ekranından ayrı çalışan bir iş parçası. Ağır işi o yapar.

2 Nerede ne çalışır

Analiz yeri	Bu tarayıcı sekmesi. Dosya sekmeden çıkmaz.
Motor	Ayrı bir tarayıcı Worker'ı. Bir inceleme en fazla 60 saniye sürebilir.
Boyut	Yerel incelemede en fazla 64 MB.
Ağ	Yok. İtibar sorgusu ya da dış servis çağrısı yapılmaz.
Kalıcı kayıt	Yok. Rapor sayfa yenilenince kaybolur, indirmedeğin sürece hiçbir yerde durmaz.
Girdi	Görsel, PDF, Office, e-posta, PCAP, APK, OCI, arşiv, script ve binary dosyalar. Ayrıca yapılandırılmış metin, log ya da e-posta başlığı.

Bir sunucuya gönderim yalnızca isteğe bağlı derin analizde, uygun dosya türlerinde ve senin açık onayınla olur. O adımın kendi kılavuzu var, HB-30 Deep Analysis.

3 Dosyayı açmak

Sayfa kabul ekranıyla açılır. Üstte iki yol var. Dosya incele ya da metin, log veya e-posta başlığı yapıştır. Yapıştırılan metin e-postaya benziyorsa e-posta olarak incelenir. Dosyayı seçer ya da bırakırsın; sitede hazır bir örnek dosya yok. Yanında, başlamadan önce okunacak kurallar durur.

İŞLEM SINIRLARI

1

Analiz yeri Bu tarayıcı sekmesi
Yerel rapor dosyayı sekmeden çıkarmaz.

2

Sunucuya gönderim Yalnızca açık onayla
Uygun türlerde isteğe bağlı derin analiz siz başlatana kadar dosyayı göndermez.

Dosya boyutu 64 MB yerel, 25 MiB derin
Sınırın üstündeki dosyalar reddedilir.

Çalıştırma Kapalı
Kod, makro, script ve PDF eylemi başlatılmaz.

Ağ erişimi Yerelde yok
İtibar sorgusu veya dış servis çağrısı yapılmaz.

3

Kalıcı kayıt Yok
Rapor yenilemede kaybolur; derin analiz yüklenen geçici dosyayı iş sonunda siler.

ÜRETİLEN KAYITLAR

4

01

SHA-256 ve SHA-1 dosyanın tamamından hesaplanır.

02

Magic bytes, PE/ELF başlıkları, PDF nesneleri ve ZIP merkez dizini ayrıştırılır.

03

Sınırlı ASCII, UTF-16LE ve UTF-16BE metin taramasından yalnızca açık IOC kayıtları çıkarılır.

04

İndirilen kanıt paketi örnek dosyayı içermez.

Kabul ekranının yanındaki işlem sınırları ve üretilen kayıtlar.

1 Analiz yeri

Bu tarayıcı sekmesi. Yerel rapor dosyayı sekmeden çıkarmaz.

2 Sunucuya gönderim

Yalnızca açık onayla. Uygun türlerde derin analiz, sen başlatana kadar dosyayı göndermez.

3 Kalıcı kayıt

Yok. Rapor yenilemede kaybolur.

4 Üretilen kayıtlar

Motor tam olarak hash değerleri, ayrıştırılan başlıklar, sınırlı metin taraması ve incelenen dosyayı içermeyen bir kanıt paketi üretir.

4 Çalışma masası

Bir dosya açılınca masanın üstünde dosya kimliği, bölümler ve seçenekler durur. Sitede örnek dosya bulunmadığı için bu bölümün ekran görüntüsü yok; parçaları aşağıda yazıyorum.

Dosya kimliği	Dosya adı, tür, boyut ve SHA-256. Tıklayınca tam değer kopyalanır. Sağ üstte "Yerel rapor hazır" ve "Yerel analiz" yazar.
Bölümler	Genel bakış, bulgular ve kanıt. "Diğer" menüsünde yapı, göstergeler, grafik ve araçlar var.
Raporu indir	Tam analiz kaydını JSON olarak indirir.
Kanıt paketi	Rapor, manifest, belge metni, IOC CSV ve STIX, metin listesi ve graph.json dosyalarını tek ZIP'te toplar.

Masanın başlığında "Deep Analysis" yazar, çünkü derin analiz aynı masanın isteğe bağlı bir adımı. Yerel rapor hazır olduğunda hiçbir şey gönderilmemiştir.

5 Kanıt ve çıktı

Kanıt sekmesi bir dosya incelendikten sonra açılır ve dört şeyi gösterir.

Dört gerçek	Analiz yeri, dosya gönderimi, çalıştırma ve ağ isteği sayısı. Yerel raporda gönderim yok, çalıştırma kapalı, ağ isteği sıfır.
Sınır cümlesi	Rapor bir güvenlik kararı değildir. Teslimden önce bir insanın incelemesi gerekir.
Kanıt paketi (.zip)	Bütün çıktılar tek pakette. İncelenen dosyanın kendisi pakete eklenmez.
Açık göstergeler (.stix.json)	Yalnızca dosyada açıkça görülen değerler. Motor tahmin ya da itibar bilgisi eklemes.

6 Neden böyle kurdum ve sınırlar

Risk puanı vermiyorum. Her bulgu, onu doğuran başlığa, yola ya da metne bağlı. Hash'i dışarıya da sormuyorum, çünkü bir hash sorgusu bile ne incelediğini başkasına söyler.

- × Dosya çalıştırılmaz. Süreç, registry, bellek ve ağ davranışı gözlenmez.
- × Tek bir işaret dosyanın zararlı olduğunu kanıtlamaz. Bulgu bulunmaması da güvenli olduğu anlamına gelmez.
- × İmza kaydı gösterilir ama imza zinciri doğrulanmaz. Yüksek entropy de tek başına kötü niyet kanıtı değildir.
- × Metin taraması sınırlıdır. Tarama sınıra takılırsa rapor bunu açıkça yazar.