Dosya ve belge sandbox

Tek dosyadan kimlik, yapı, gömülü bağlantı ve IOC raporu üretir.

İŞLEME SINIRI
Cihazında, tarayıcıda işlenir

SİTENİN AMACI

Bu site, bir soruyu güvenli ve tekrar edilebilir bir araştırma sürecine çevirmek için var. Araç sonucu tek başına hüküm değildir; kaynak ve insan kontrolü her zaman görünür kalır.

NEDEN YAPTIM?

Bilinmeyen bir dosyayı önce çalıştırmadan tanımak, açık göstergeleri ayırmak ve tekrar incelenebilir bir kayıt bırakmak için bu yerel masayı yaptım.

KÜÇÜK MİMARİ

Girdiden saklanabilir çıktıya dört parça

01 Girdi
PDF, Office, e-posta veya APK dosyası

→

02 Yerel yöntem
Dosya yapısını sınırlar içinde oku

→

03 İnsan kontrolü
Sonucu kaynağa dönerek kontrol et

→

04 Çıktı
İnceleme raporu ve ilişki grafiği

Dosya ve belge sandbox

ADIM ADIM KULLANIM

Adım 1

Malzemeyi hazırla

Başlangıçta gereken şey: PDF, Office, e-posta veya APK dosyası

Adım 2

Dosya yapısını sınırlar içinde oku

Tek dosyadan kimlik, yapı, gömülü bağlantı ve IOC raporu üretir.

Adım 3

Sonucu kaynağa dönerek kontrol et

Bulunan URL, hash veya string değerini dosya içindeki konumuyla birlikte incele. Tek bir stringi zararlılık kanıtı sayma.

Adım 4

Kaydı indir ve sakla

İnceleme sonunda saklanacak şey: İnceleme raporu ve ilişki grafiği

DÜRÜST SINIR

Dosya çalıştırılmaz. Yerel statik rapor davranış analizi, antivirüs kararı veya temiz dosya garantisi değildir.