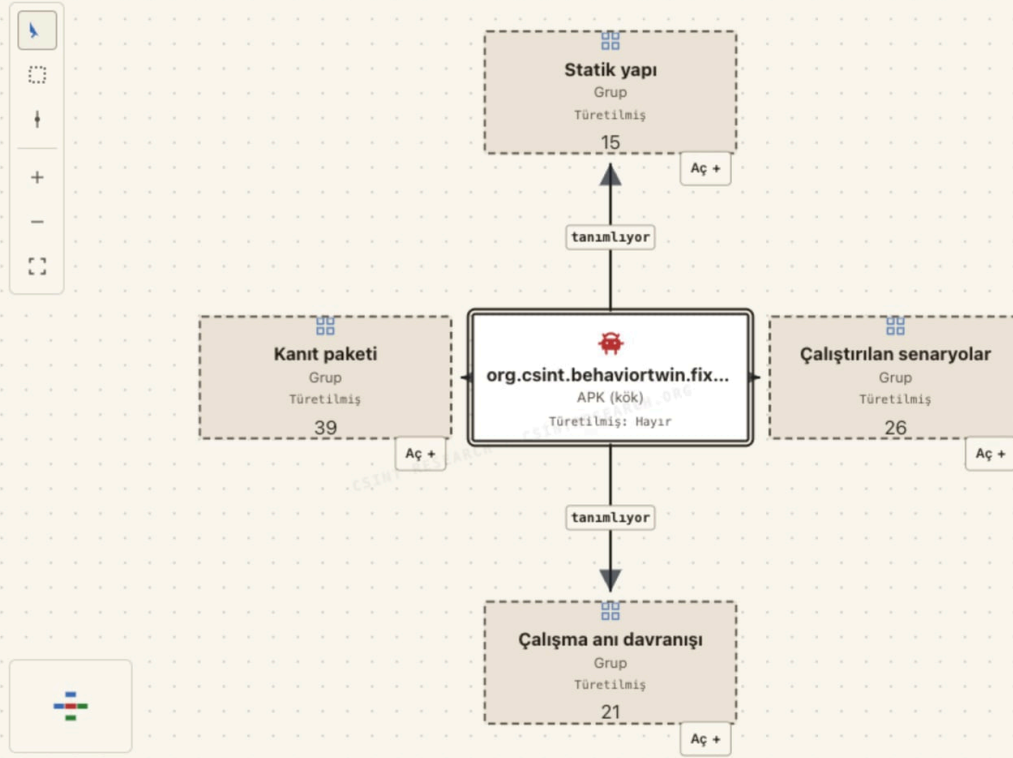




Mobile Behavior Diff ile imzalı bir Android laboratuvar kaydını okumak

Bir Android uygulamasını kendi laboratuvarımda, kontrollü bir emülatörde çalıştırıyorum. Bu sayfa o çalışmadan çıkan imzalı kanıt paketini açar, doğrular ve ne gözlendiğini gösterir.

1 Bu sayfa ne işe yarar

Bir uygulamanın yeni sürümü çıktığında aynı ekranlardan geçen bir kullanıcı için neyin değiştiğini bilmek istiyorum. Ekran görüntüsü bunu söylemez. Bu yüzden aynı yolculuğu laboratuvarımda tekrar tekrar oynatıyorum ve her olayı kaydediyorum.

Bu sayfa uygulamayı çalıştırmaz. APK dosyası da buraya gelmez. Sayfa yalnızca laboratuvarın ürettiği *.evidence.zip* paketini senin tarayıcında açar, imzasını ve dosyalarını kontrol eder, sonra sonucu gösterir.

Sayfada hazır örnek yok. Bir laboratuvar paketi açılana kadar ekran bilerek boş kalır. Sahte ya da temsili sonuç göstermez.

Birkaç kelime

APK	Android uygulamasının kurulum dosyası.
Emülatör	Bilgisayarda çalışan sanal Android telefon. Laboratuvar gerçek bir telefona dokunmaz.
SHA-256	Bir dosyanın parmak izi. Dosyada tek bayt değişse parmak izi de değişir.
Ed25519 imzası	Paketin içeriğinin imzalandıktan sonra değişmediğini gösteren dijital imza.
Frida	Çalışan uygulamanın hangi fonksiyonları çağırdığını kaydeden araç. Burada yalnız izleme modunda kullanılır, hiçbir değeri değiştirmez.
Kontrol ve treatment	Aynı yolculuğun iki koşusu. Kontrol karşılaştırmanın temelidir, treatment değişen koşuldur (örneğin bir izin kapalı ya da yeni sürüm).

2 Paket nasıl oluşur

Sayfanın üstündeki altı adımlı satır bir sonuç değil, laboratuvarın sırasıdır. Paketi okurken neyin nereden geldiğini bilmek için bu sırayı tanımak işe yarar.



Laboratuvarın altı aşaması. Numaralar aşağıdaki açıklamalarla eşleşir.

1 APK ve parmak izi

Uygulama dosyasının SHA-256 değeri alınır. Paketteki her şey bu değere bağlanır.

- 2 Sınırlı statik okuma**
Uygulama çalışmadan önce izinleri, paket adı ve sürümü okunur.
- 3 Senaryo kuyruğu**
Senaryolar sırayla, geldiği sırada çalıştırılır. Her senaryo aynı temiz başlangıçtan başlar.
- 4 Emülatörde tekrar oynatma**
Aynı ekran yolculuğu emülatörde oynatılır. Frida bu sırada yalnızca gözlem yapar.
- 5 Olayları düzenleme**
Kayıtlar, ağ trafiği ve dosya değişiklikleri tek bir olay biçimine çevrilir.
- 6 Graf ve imzalı paket**
Olaylar bir ilişki grafiğine bağlanır. Bütün dosyalar SHA-256 ile listelenir ve liste Ed25519 ile imzalanır.

3 Paketi açmak



Paket seçme alanı. Bir paket açılana kadar sayfa bu halde kalır.

- 1 Paketi seç**
Düğmeye bas ve dosyayı seç, ya da dosyayı kutunun üstüne bırak.
- 2 Sınırı gör**
160 MB üstü dosya ya da .evidence.zip olmayan dosya hemen reddedilir.

3 Boş ekran normaldir

Bu satır, sayfanın kendi başına bir sonuç üretmediğini hatırlatır.

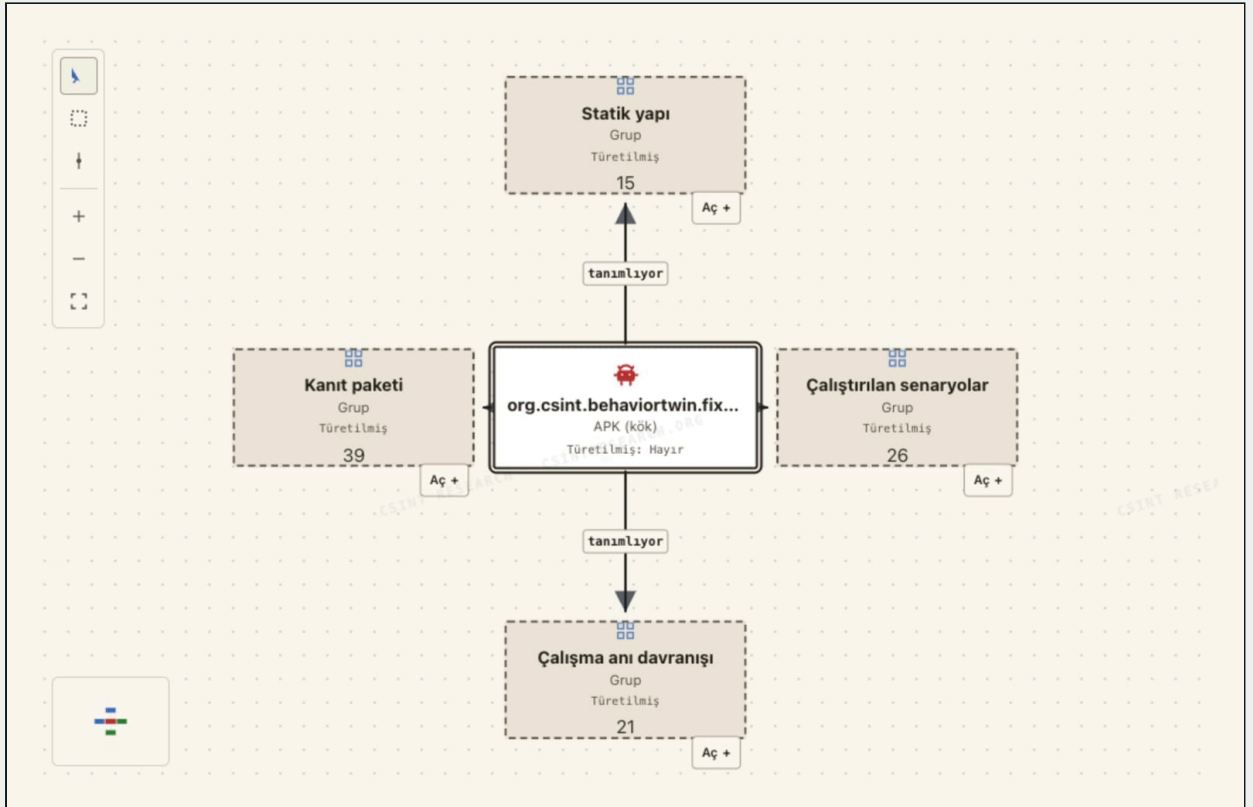
4 Doğrulamayı bekle

Tarayıcı dosya listesini, her dosyanın parmak izini, imzayı ve kayıt biçimini kontrol eder. Biri tutmazsa paket açılmaz ve hata kodu gösterilir.

Gereken	Laboratuvar aracının ürettiği bir .evidence.zip dosyası. Başka uzantı kabul edilmez.
Boyut	En fazla 160 MB.
Hesap	Gerekmez.
Veriler nerede	Paket tarayıcında açılır ve doğrulanır. Sunucuya gönderilmez.

Paket imza anahtarını kendi içinde taşır. İmza, paketin sonradan değişmediğini kanıtlar. Anahtarın kime ait olduğunu tek başına kanıtlamaz.

4 Açılınca ne görürsün



Zararsız test uygulamasının paketi açıldığında ilk görünen inceleme grafiği. Ortada APK, çevresinde dört grup ve her grubun kayıt sayısı var.

Grafiğin ortasında uygulama durur. Çevresinde statik yapı, çalıştırılan senaryolar, çalışma anındaki davranış ve kanıt paketi olmak üzere dört grup var. Bir grubun Aç düğmesi o grubun

içindeki gerçek kayıtları gösterir. Bunlar izinler, ağ adresleri, dosyalar, veritabanı tabloları, yüklenen kütüphaneler ve Frida'nın gördüğü fonksiyonlardır.

Grafiğin altında on üç görünüm var. En çok kullandıklarım şunlar.

Genel Bakış	Senaryo sayısı, olay sayısı, bulunan fark sayısı ve imzalı dosya sayısı.
Zaman Çizelgesi	Seçilen koşunun olayları sırayla. Bir olaya basınca ayrıntısı ve kanıt dosyası açılır.
Ağ Akışı	Uygulamanın bağlanmayı denediği adresler. Bağlantı, veri sızdırma demek değildir.
YIOC	Kontrol ve treatment koşuları arasındaki davranış farkları.
Notlar	Paketin kendi yorum sınırları ve hangi güvenlik katmanında çalıştığı.

Her bulgunun yanında *Ham kanıtı* aç düğmesi var. Bu düğme bulgunun dayandığı dosyayı paketin içinden açar. Bir sonuca inanmadan önce bu dosyaya bakmanı öneririm.

5 Farkı doğru okumak

YIOC görünümünde her fark bir etiket taşır. Etiket yeni görüldü (*newly-observed*), kayboldu (*disappeared*) ya da sıklığı arttı veya azaldı olur. Yanındaki iki sayı, farkın kontrol koşusunda ve treatment koşusunda kaç kez görüldüğünü gösterir. Yeni bir davranışın durumu önce *correlated* olur. Ayrı bir doğrulama koşusunda tekrar görülürse *reproduced* olur.

- ✗ Karşılaştırılan iki koşunun aynı yolculuk, aynı başlangıç ve aynı ortam olduğundan emin ol. Eşleşmeyen koşuların farkı sürüm farkı değildir.
- ✗ Bir izin listede görünüyor diye kullanıldığı anlamına gelmez. Statik kayıt ile çalışma anı kaydı ayrı tutulur.
- ✗ Şifreli trafiğin içeriği görülemiyorsa sayfa bunu tahmin etmez, görülemedi diye bırakır.

6 Neyi yapmaz

- ✗ APK çalıştırmaz ve APK yüklemes. Tarayıcıda yalnızca imzalı paketi okur.
- ✗ Laboratuvar şu an yalnızca zararsız test uygulaması için kurulu. Rastgele ya da zararlı APK'lar reddedilir.
- ✗ Sonuç yalnızca o paketteki deney için geçerlidir. Her cihazı, ağı ya da kullanıcıyı temsil etmez.
- ✗ Deneyi tarayıcıda yeniden oynatmaz ve bir uygulamanın zararlı ya da güvenli olduğuna karar vermez. Yeni koşu yalnızca yerel laboratuvar aracılığıyla yapılır.