MOBİL ZARARLI ANALİZİNE GİRİŞ

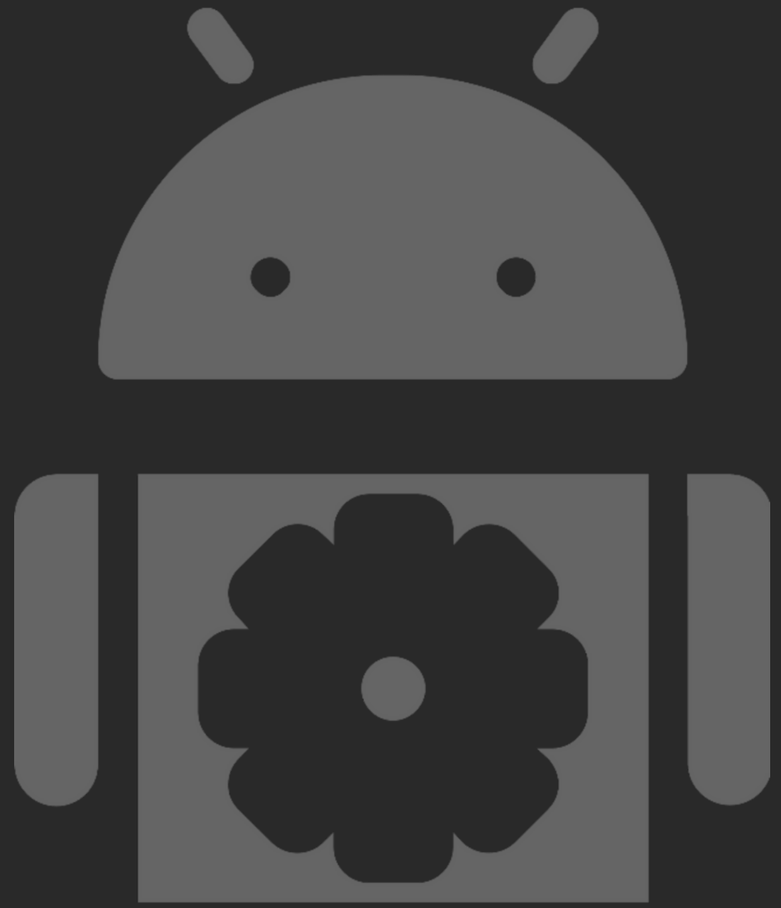
Ömer Faruk Atlıoğlu & Günsu Bilge Dal

Android Mimarisi, Joker, Anubis ve Daha Fazlası...

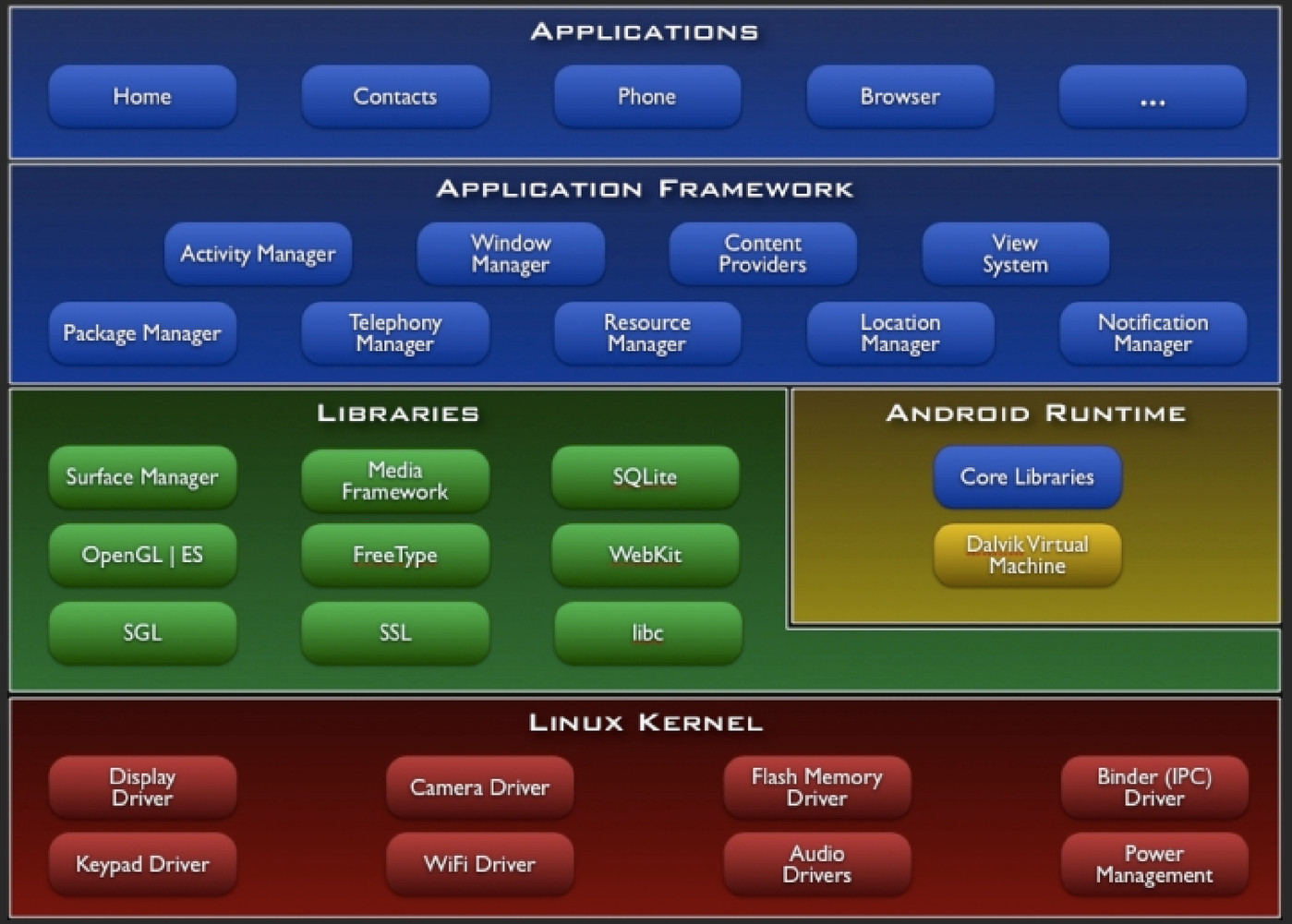
instagram: @macsecommunity
twitter: @macsecommunity
linkedin: .../company/macsecommunity/

MACSEC

Android Nedir?



Android Mimarisi

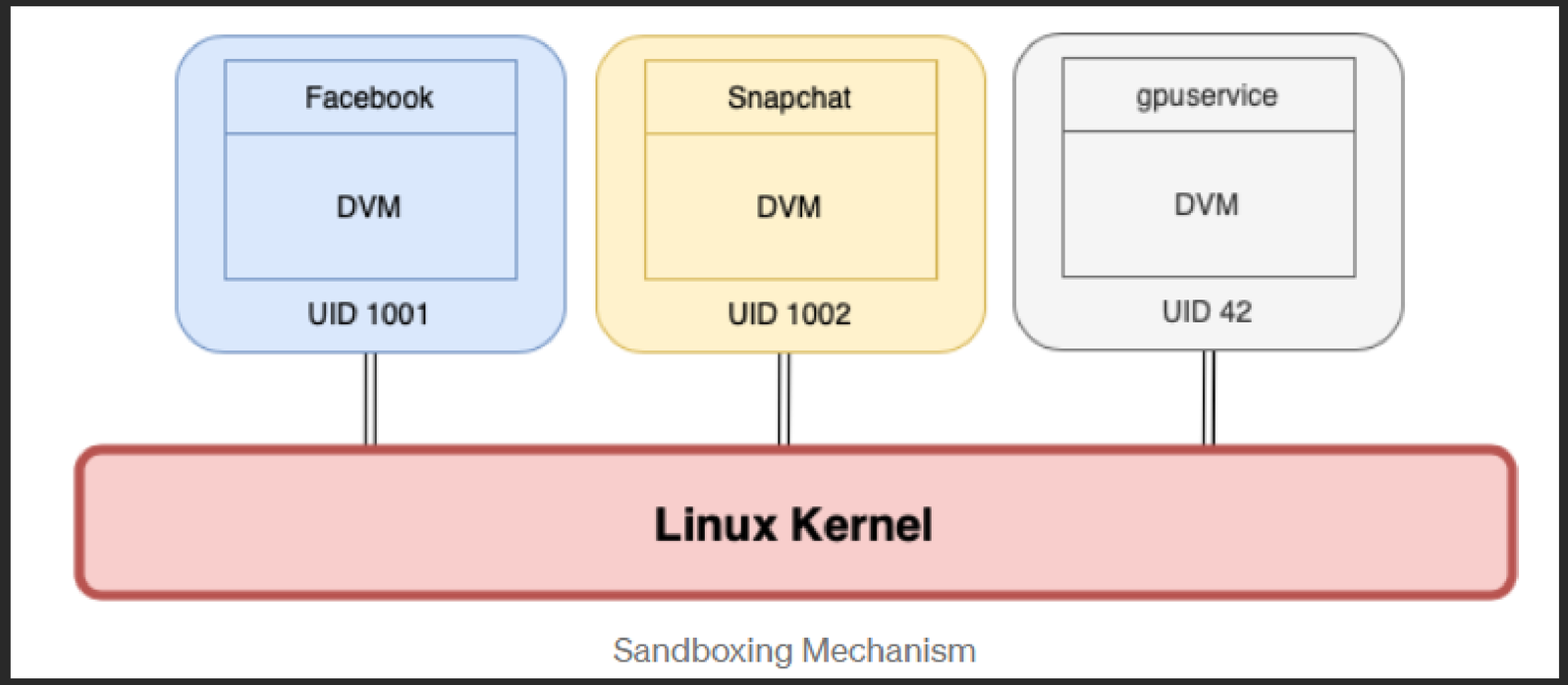


Güvenlik Özelinde Android

1- İşletim Sistemi Güvenliği
- process isolation
- user-based permission model
- inter-process communication (IPC)

2- Uygulama Güvenliği
- izinler
- veri depolama
- app signing (code signing)

Sandboxing & Rooting



Sandboxing Mechanism

Verified Boot

Çalıştırılan işletim sisteminin orijinal olup olmadığını anlamaya yarayan bir süreçtir.

Permissions (AppSec)

- Install-time
- Runtime

Veri Depolama

- Internal
- External
- Content Providers

Inter-process Communication (IPC)

Interprocess Communication (IPC), Android'de processlerin diğer processler tarafından sunulan hizmetlere erişmesine ve bunlarla etkileşime girmesine izin veren bir mekanizmadır.

Code Signing

ilgili uygulamanın kim tarafından geliştirildiğini gösteren bir mekanizmadır.

Bir Android Uygulamasının Hayat Döngüsü

Android işletim sisteminin hayat döngüsü:
https://medium.com/@voodoomio/what-the-zygote-76f852d887d9
https://www.sibervatan.org/makale/android-sistem-ve-zygote-proses/45

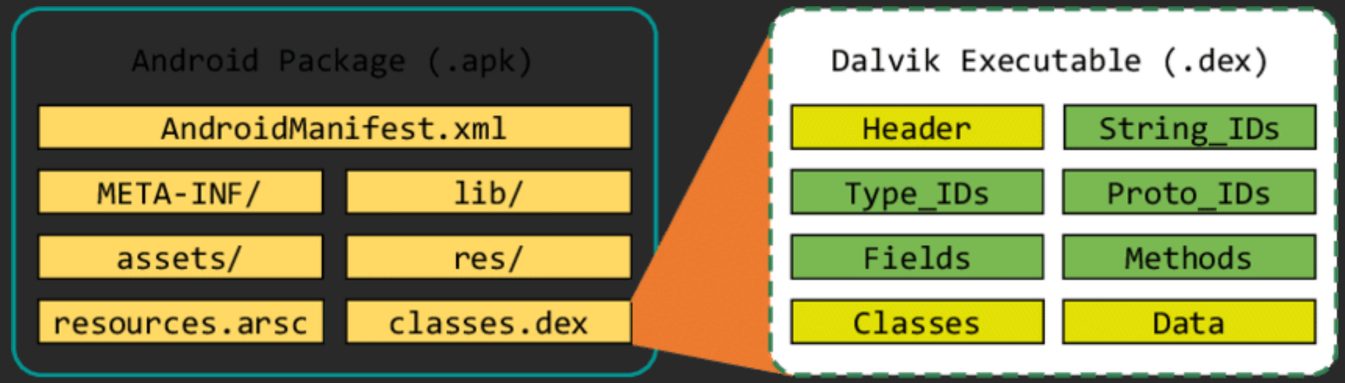
APK nedir?

"Android Package" sözcüklerinin kısaltması olan .apk uzantısı, Android işletim sistemi tarafından kullanılan dosya formatıdır. Java ya da Kotlin ile yazılır.

AppCode

classes.dex !

dex dosya biçiminde derlenmiş sınıfları içerir. Uygulamanın java kodlarının derlenmiş halidir.



libs/

dex dosya biçiminde derlenmiş sınıfları içerir. C/C++ ile derlenmişlerdir.

Resources

res/

Uygulamada kullanılacak resim, ses, video gibi kaynak dosyaları bu klasörde bulunur. Platform tarafından tanınan kaynaklar tutulur.

resources.arsc

XML dosyalarının derlenip bir araya getirildiği dosyadır. Stiller, renkler, dizeler gibi

Other Files

assets/

Kaynak dosyalar bu dosyada bulunur. Android tarafından tanınmayan veriler tutulur.

META-INF/

Sertifikalar ve imzalar bulunur. Bu dosya JAR içeriği hakkında meta verileri içermektedir.

AndroidManifest.xml!

Uygulamanın erişmek istediği izinler burada yer almaktadır. Statik analiz için önemli bir dosyadır. Uygulamayla ilgili ana bilgi verir.

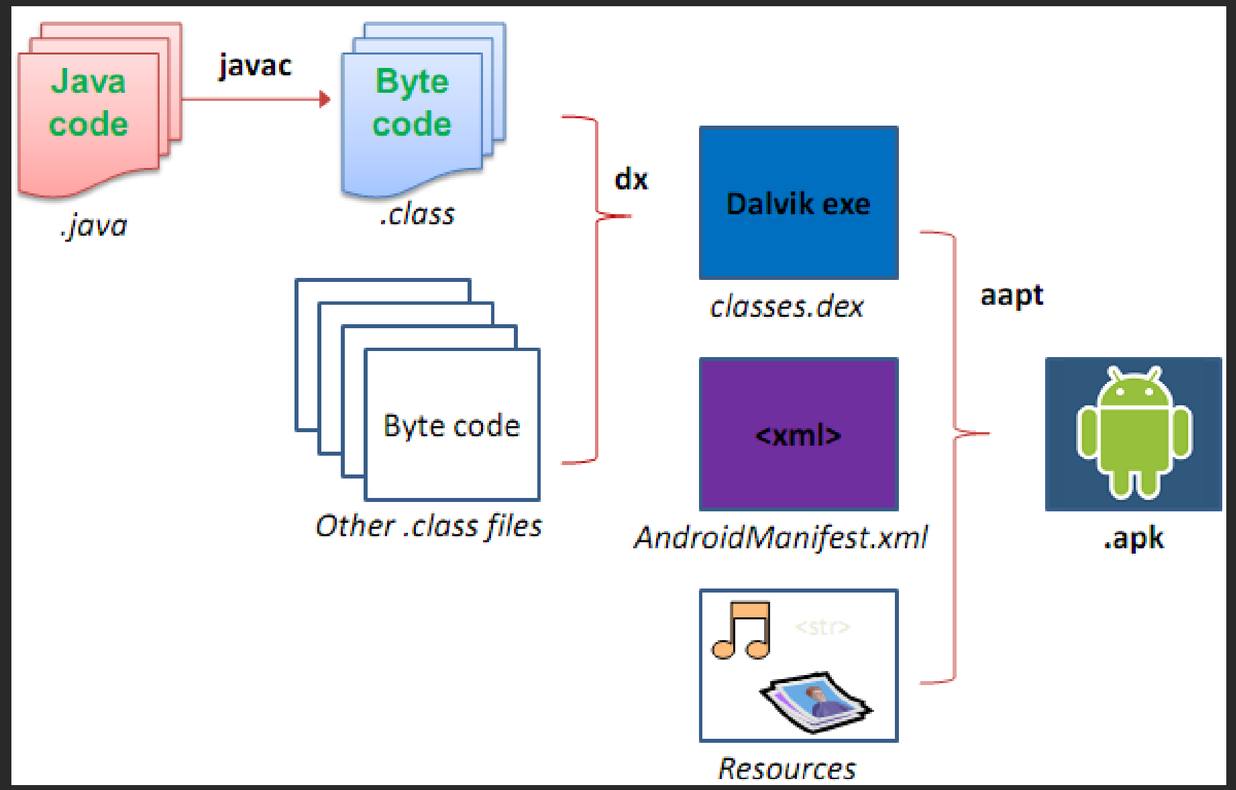
AAB Nedir?

Android application bundle olarak adlanıdırlan paket sistemidir.

AAB'nin APK'dan farkı nedir?

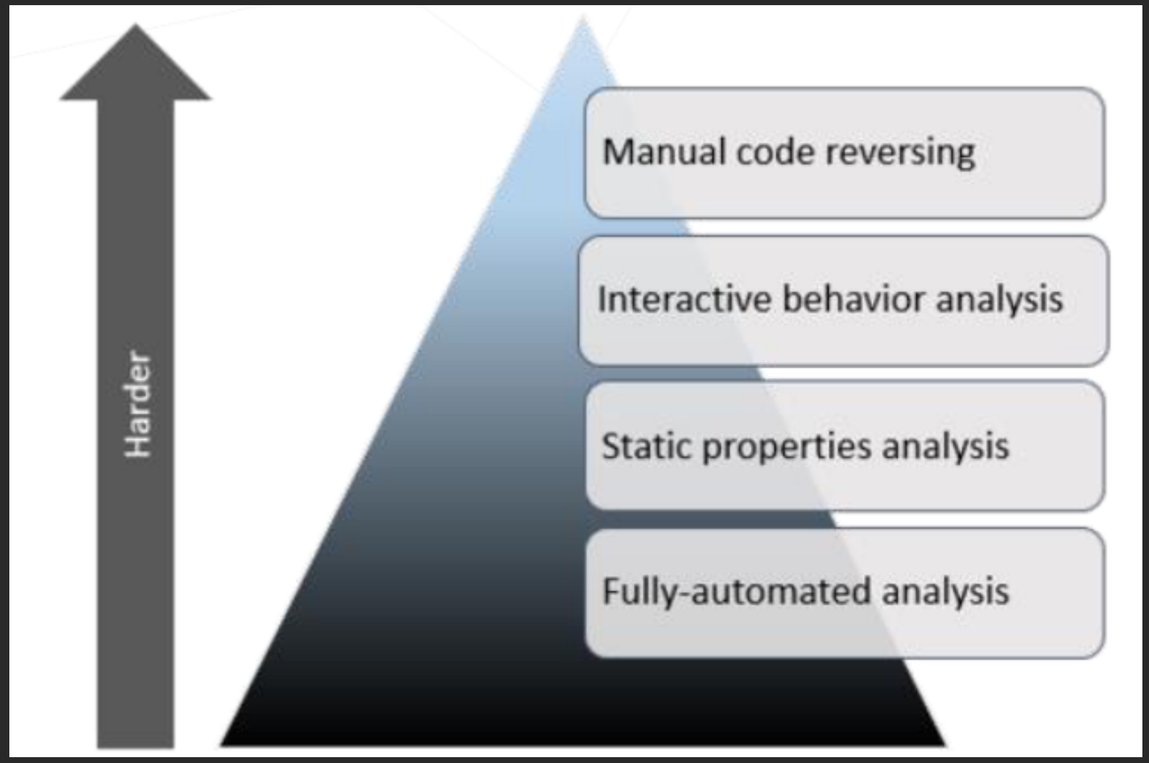
AAB'de APK'ya göre daha temiz bir filtreleme bulunmaktadır. Boyut olarak APK'dan ciddi oranlarda daha az yer kaplamaktadır.

Bir APK dosyası nasıl oluşturulur?



(Mobil) Zararlı Yazılım Analizi Nedir?

Zararlı yazılım analizi şüpheli bir uygulama veya URLnin davranışının ve amacının anlaşılması hedefine sahip bir süreçtir. Baştan sona her aşama birbiriyle etkileşimlidir.

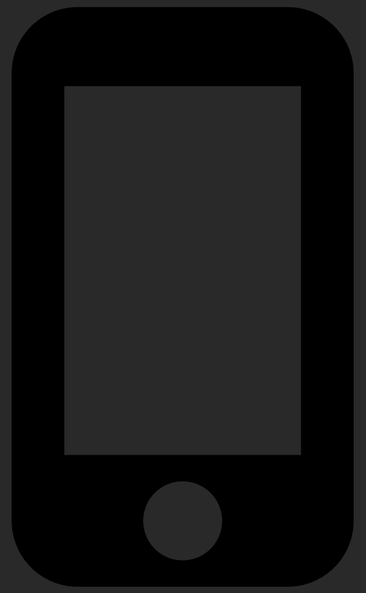


Zararlı Yazılım Türleri

- Virus
- Trojan
- Worm
- Stealer
- Ransomware
- Dropper
- Adware
- Clipper
- Rootkit
- Boot Sector/MBR
- Backdoor
- Spyware
- CryptoMiner
- Botnet

En Sık Karşılaşılan Mobil Zararlı Türleri

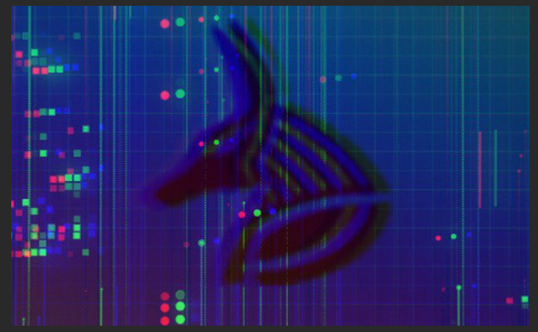
adware, backdoor, file infector, PUA, ransomware, riskware, scareware, spyware, trojan, trojan-sms, trojan-spy, trojan-banker, trojan-dropper.



Popüler Mobil Zararlı Yazılım Aileleri

Anubis

- Trojan
- Bankacılık Overlay Saldırısı
- SMS dinleme / çağrı yönlendirme



Cerberus

- Trojan
- Bankacılık Overlay Saldırısı
- SMS dinleme / çağrı yönlendirme

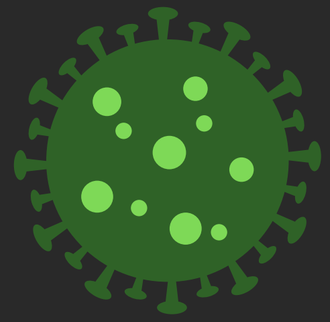
Popüler Mobil Zararlı Yazılım Aileleri

Pegasus

- Spyware
- Zero-click on iOS
- 2016

FluBot

- Bankacılık zararlı yazılımı
- Overlay Saldırısı
- Kriptopara dünyası



Popüler Mobil Zararlı Yazılım Aileleri

Joker

- Fleeceware
- Persistency by hiding
- Spyware
- 2017

https://beepeer.co › joker-virusu-androide-geri-dondu

Joker Android'e Geri Döndü: Banka Hesaplarınıza Sahip Çıkın!

25 Ağu 2021 — Başlangıçta, bu **aileden 'Joker'** veya başka tür bir Kötü Amaçlı **Yazılım** bulaşmış uygulamalar SMS yoluyla dolandırıcılık faaliyetlerinde ...

https://haberciniz.com.tr › Teknoloji

Joker virüsü yeniden hortladı! Bu 8 uygulamayı hemen silin ...

17 Kas 2021 — Bu kötü amaçlı **yazılım** 'casus **yazılım** / trojan' olarak sınıflandırılır ve “Bread” olarak adlandırılan kötü amaçlı **yazılım ailesine** aittir.

https://www.donanimhaber.com › joker-virusu-geri-do...

Joker virüsü geri döndü: Banka hesaplarınızı boşaltabilir

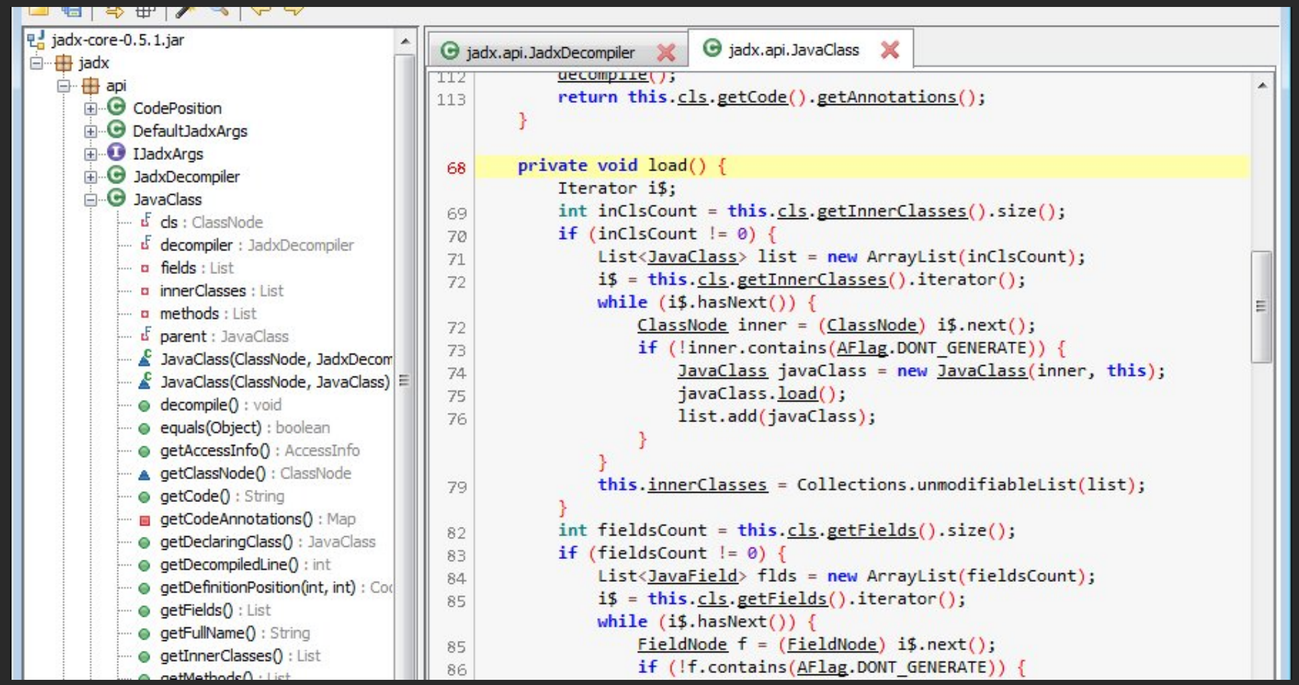
26 Ağu 2021 — **Joker** virüsü, Google Play'den temizlendikten bir buçuk yıl sonra, ... vermek olan Bread olarak bilinen bir kötü amaçlı **yazılım ailesine** ait.

Zararlı Analiz Çeşitleri

Statik Analiz

Statik analiz, zararlı yazılım çalıştırılmadan gerçekleştirilen analiz türüdür. Mobil zararlıların statik analizi kapsamında uygulamanın aldığı izinler, kaynak kodu gibi bilgiler incelenir ve zararlının çalışma yöntemi anlaşılmaya çalışılınır.

Mobil zararlı analizi kapsamında gerçekleştirilen statik analiz kaynak kod okuma, uygulama izinlerini inceleme şeklinde olabilmektedir.



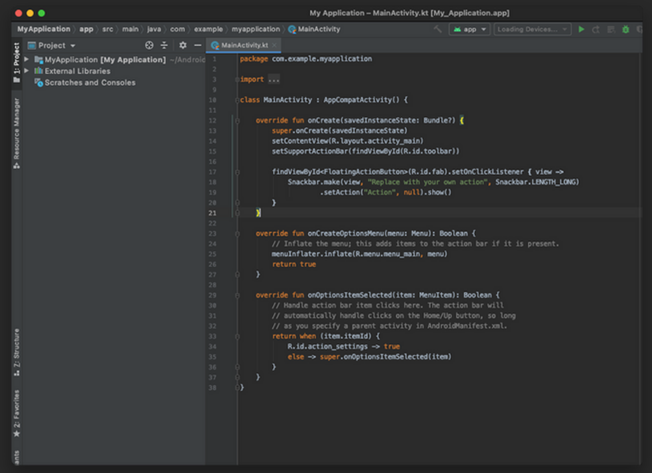
jadx, apktool, quark vb araçlar statik analiz araçlarındandır.

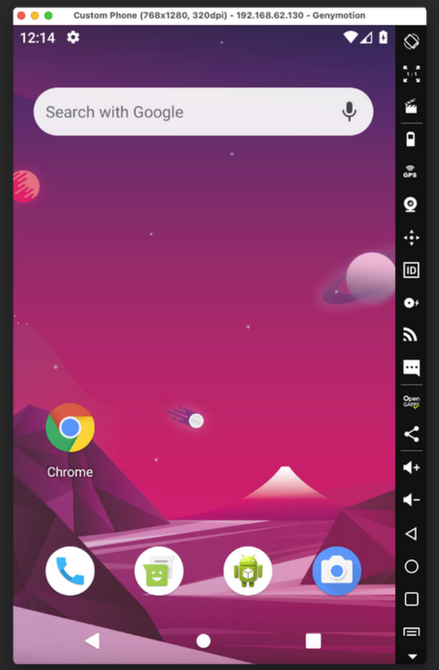
Zararlı Analiz Çeşitleri

Dinamik Analiz

Dinamik analiz, zararlı yazılımın çalıştırılması sırasında gerçekleştirilen analiz türüdür.

Mobil zararlıların dinamik analizi kapsamında uygulama emülatör ortamlarda ya da varsa burner bir araç üzerinde çalıştırılır (ortam takibi daha sağlıklı olduğu için emülator tercih edilir). Uygulamanın çalışması, oluşturduğu processler, yarattığı ağ trafiği gibi birçok dinamik bulgu elde edilerek zararlının çalışma yöntemi anlaşılır.





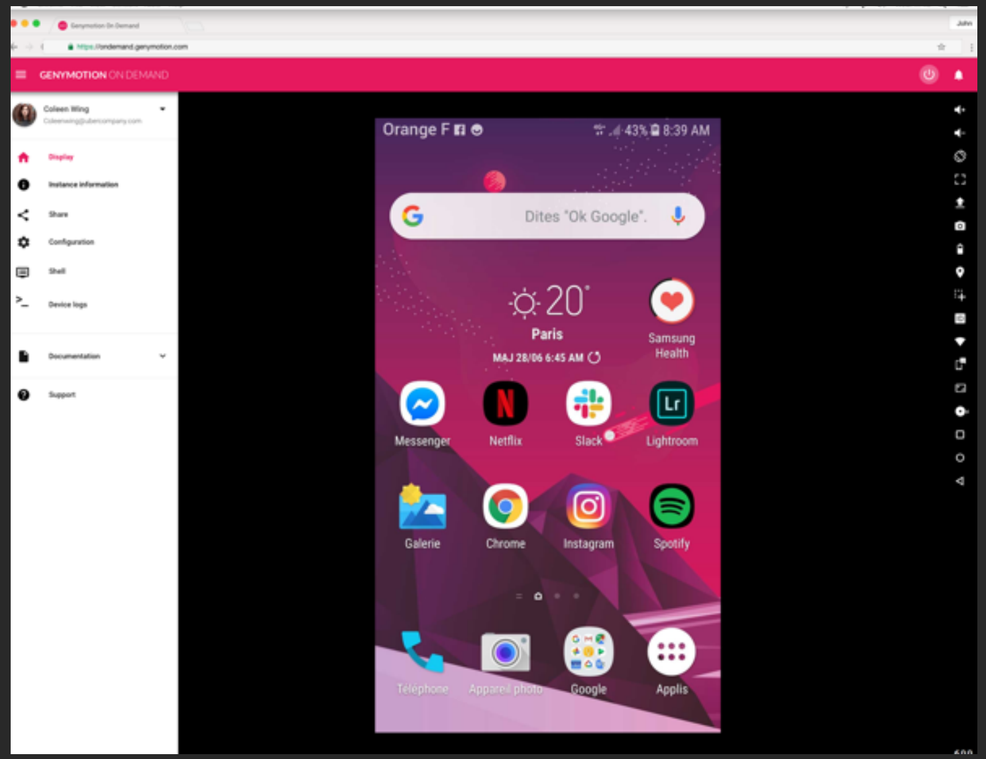
adb, Xposed, frida, Inspeckage vb. araçlar dinamik analiz araçlarındandır.

Emülatör Nedir?

Bilgisayarınıza, yeni bir cihaz erişimi sağlayan uygulamalardır.

Emülator sayesinde android işletim sistemini bilgisayarınıza kurabilirsiniz. Sanal bir telefon olarak karşımıza çıkacak olan emülator ile uygulama testleri, dinamik testler, yapabiliriz.

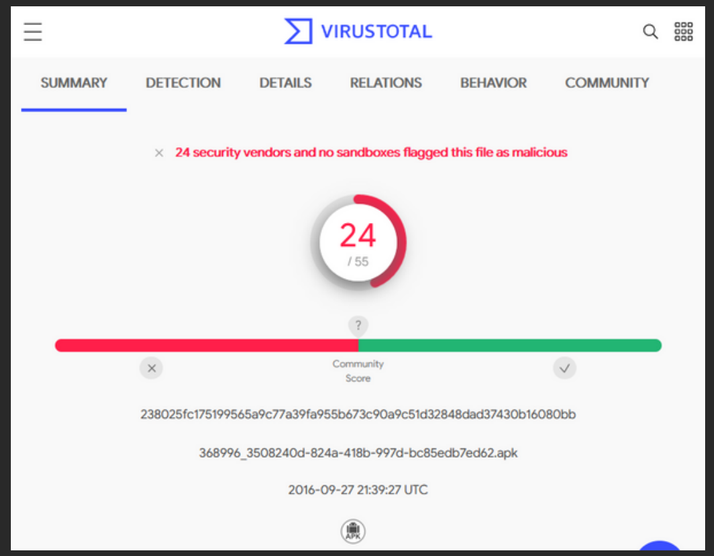
En büyük faydası ortam takibi daha kolay yapılır ve minimum maaliyet ile birden fazla cihazda deneme şansımız bulunmaktadır



genymotion, en popüler Android emülatörlerinden.

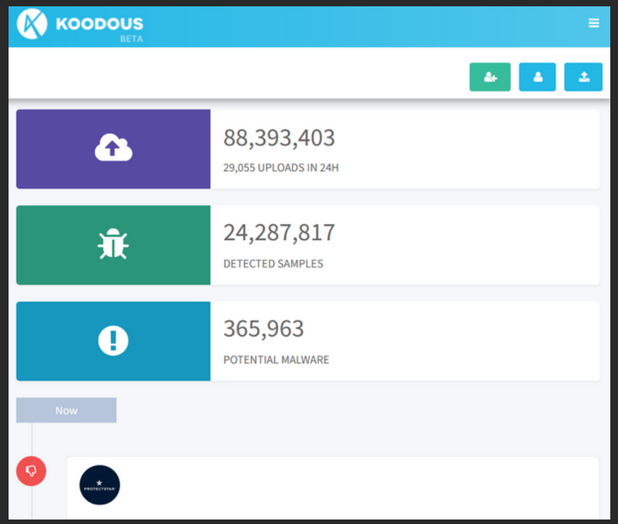
Online Platformlar

VirusTotal



BitBaan MALab

Koodous



Anti Analiz Metodları

Obfuscation:

Bu işlem, kodların anlaşılabilirliğinin daha az olması için (tersine mühendislik teşebbüslerinden korumak için) yapılmaktadır. Obfuscation işleminden sonra kodlar daha karmaşık hale gelecektir fakat cihazın kodları anlamasında herhangi bir sorun olmayacaktır.

Packing:

Packing işlemi tıpkı obfuscation gibi antivirüs ve antimalware çözümlerini atlatmak için kullanılabilen bir mekanizmadır.

Unpacking işlemi kullanılan packer bilindiğinde oldukça kolay gerçekleştirebilmektedir.

Siber uzayda yeterince önlem alınmazsa her aksiyonun bir ayak izi olduğu gibi packing işlemi de packer bilgisine ulaşılması için dosya üzerinde oldukça önemli modifikasyonlar oluşturmaktadır.

Demo'ya Geçme Vakti!

Küçük bir sample analizi :)

instagram: @macsecommunity
twitter: @macsecommunity
linkedin: .../company/macsecommunity/

MACSEC