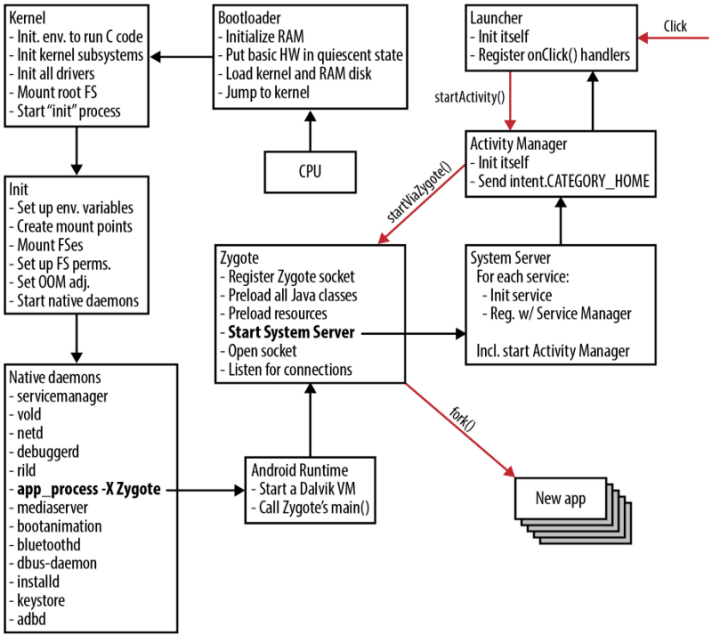
Gün 3

Not defteri:	Zararlı Yazılım Analizine Giriş		
Oluşturulan:	27.01.2020 09:47	**Güncellen...**	27.01.2020 16:35
Yazar:	Özlem Körpe		
URL:	https://github.com/gchq/CyberChef		

Android Zararlı Yazılım Analizi 101

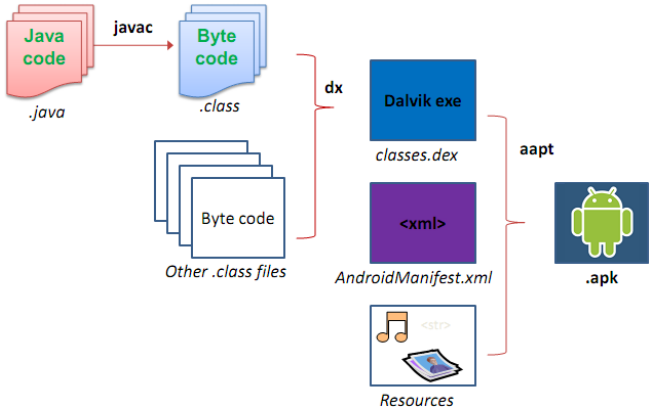
Android Boot Process



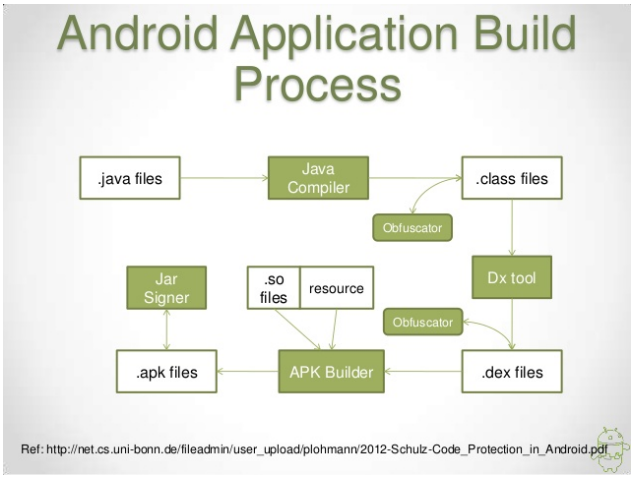
Zygote: Init processi Zygote'u başlatır. Zygote dalvik VM'i initialize eder. Sıkça kullanılan kütüphaneleri yükler.

APK (Android Application Package)

Android uygulama dosyalarıdır. Java, Kotlin, Xamarin, Unity gibi yollarla oluşturulabilir.
Android uygulamaların derlenmesi diğer Java uygulamalarından farklıdır. Fakat başlangıçta aynı şekilde başlar.

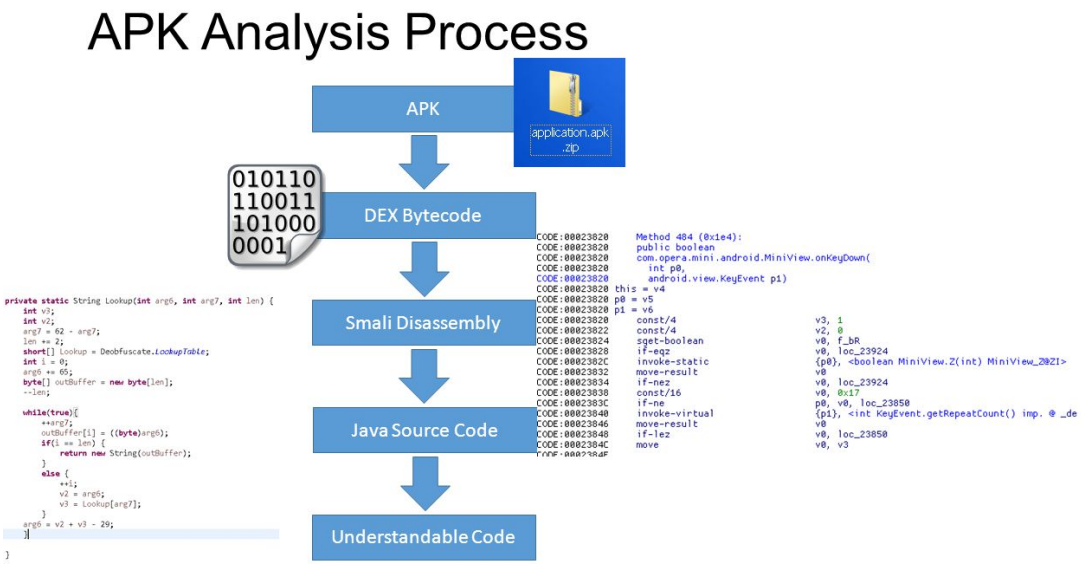


Class ve jar dostaları dx aracı ile birleştirişerek Dalvik byte-code'u içerien classes.dex dosyasını oluşturur. Classes.dex dosyası ve resource dosyaları aapt aracı ile birleşerek apk dosyası oluşturur

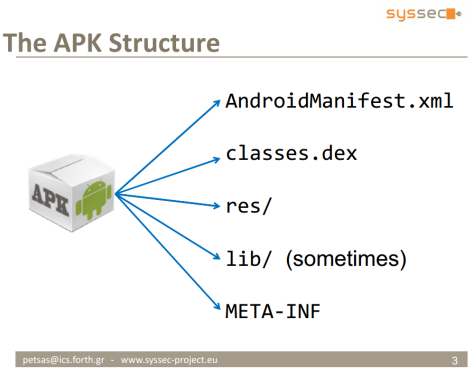


.apk file > jarsigner > zipalign > signed apk file.

APK Analysis



APK Yapısı



- **Android Manifest**: Uygulamanın kullanacağı servis ve isimlerin belirlendiği XML dosyasıdır.
- **Lib**: Javanın dışında farklı diller kullanılarak oluşturulan so dosyalarını java ile JNIBridge yardımıyla kullanılmasına olanak sağlar
- **Res**: Resources.arsc içerisinde olmayan kaynak dosyalarını bulundurur
- **Resources.arsx**: Önceden compile edilen resource dosyalarını bulundurur.
- **META-INF**: İmzda kullanılan anahtarı bulundurur.
- **Assets**:Uygulamada kullanılan binary, image ve farklı dosyaları içerir.

Android Zararlı Yazılım Analizinde Kullanılan Toollar

- jadx/jadx-gui
- apktool
- adb
- emulator : genymotion/android/virtualbox
- burp
- frida, frida-tools

Android Permissions / İzinler

READ_CALENDAR: Takvimi okuma
WRITE_CALENDAR: Takvime yazma
CAMERA: Kamera erişimi
READ_CONTACTS: Rehber kayıtlarını okuma
WRITE_CONTACTS: Rehber kayıtlarına yazma
GET_ACCOUNTS:
ACCESS_FINE_LOCATION:
ACCESS_COARSE_LOCATION:
RECORD_AUDIO: Ses kaydetme.
READ_PHONE_STATE:
READ_PHONE_NUMBERS: Telefon numaralarını okuma
CALL_PHONE: Arama yapmak.
ANSWER_PHONE_CALLS: Aramaları cevaplamak.
READ_CALL_LOG : Kaydedilen aramaların görüntülenmesi.
WRITE_CALL_LOG:
ADD_VOICEMAIL:
USE_SIP:
PROCESS_OUTGOING_CALLS:
BODY_SENSORS: Sensörlere erişim.
SEND_SMS: SMS gönderme izni
RECEIVE_SMS: SMS alma izni
READ_SMS: SMS'leri okuma izni
RECEIVE_WAP_PUSH:
RECEIVE_MMS: MMS mesajı almak.
READ_EXTERNAL_STORAGE: External hafızayı okuma.
WRITE_EXTERNAL_STORAGE: External hafızaya yazma.

ADB: Android Debug Bridge

Adb devices: Birden fazla emülatör kullanılıyorsa, emülatör bilgisi verir.
Adb shell: Emülatör içerisinden shell alınır, root komutları çalıştırılabilir.
Adb pull / push : Cihaza veri gönderip cihazdan veri almak için kullanılır.
Adb forward tcp:3333 tcp:3333 : Network trafiği için kullanılır.
Adb logcat: Uygulamanın debug aşamasında kullanılır. Log.d(tag,mesaj) şeklinde kullanılabilir. Logcat kayıtları okunabileceği için uyulamanın önemli bilgilerinin logcate basılmaması gerekmektedir. Bu yüzden proje paketlenmeden önce logcat incelenmelidir.
Adb reboot:
Adb install:
Adb uninstall:

/data/folder

/data/data/package

- app_apk
- app_files
- app_webvies
- cache
- code_cache

- shared_prefs : İçerisinde farklı isimlerde xml dosyası bulunur.

/data/app/package

- base.apk
- lib
- oat

CyberChef
CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser. These operations include simple encoding like XOR or Base64, more complex encryption like AES, DES and Blowfish, creating binary and hexdumps, compression and decompression of data, calculating hashes and checksums, IPv6 and X.509 parsing, changing character encodings, and much more.
https://github.com/gchq/CyberChef
https://gchq.github.io/CyberChef/

Play Protect
Antivirüs gibi çalışarak Google Play Store'a yüklenen uygulamaları güvenlik kontrolünden geçiren sistemdir.

Android Zararlı Yazılım Türleri

Adware
Telefonda istenmeyen reklam çıkaran uygulamalardır. Örneğin USER_PRESENT receiver'ine kurulduğunda telefon her kilit ekrandan çıkarıldığında reklam görüntülenir.

apktool d sallakazan.apk -d sall : Baksmaling aracıyla dex kodunu smaliye çeviriyor.