Android Zararlı Yazılım Analizi

written by Mert SARICA | 25 February 2012

2011 yılının son aylarında güvenlik firmaları tarafından yayınlanan mobil tehdit raporlarında Android işletim sisteminin rakiplerine göre çok daha fazla zararlı yazılım istilasına uğradığına dikkat çekiliyordu. Juniper firması tarafından yapılan araştırmaya göre 2009 ile 2010 yılları arasında akıllı telefonları hedef alan zararlı yazılımların %250 artış gösterdiği, 2011 yılının Temmuz ayı ile Kasım ayı arasında ise %472 artış gösterdiği sonucu ortaya çıkıyordu. Juniper firması tarafından yayınlanan bir başka raporda ise 2011 yılının son 7 ayında Android işletim sistemini hedef alan zararlı yazılımlardaki artışın %3,325 olduğu belirtiliyordu!

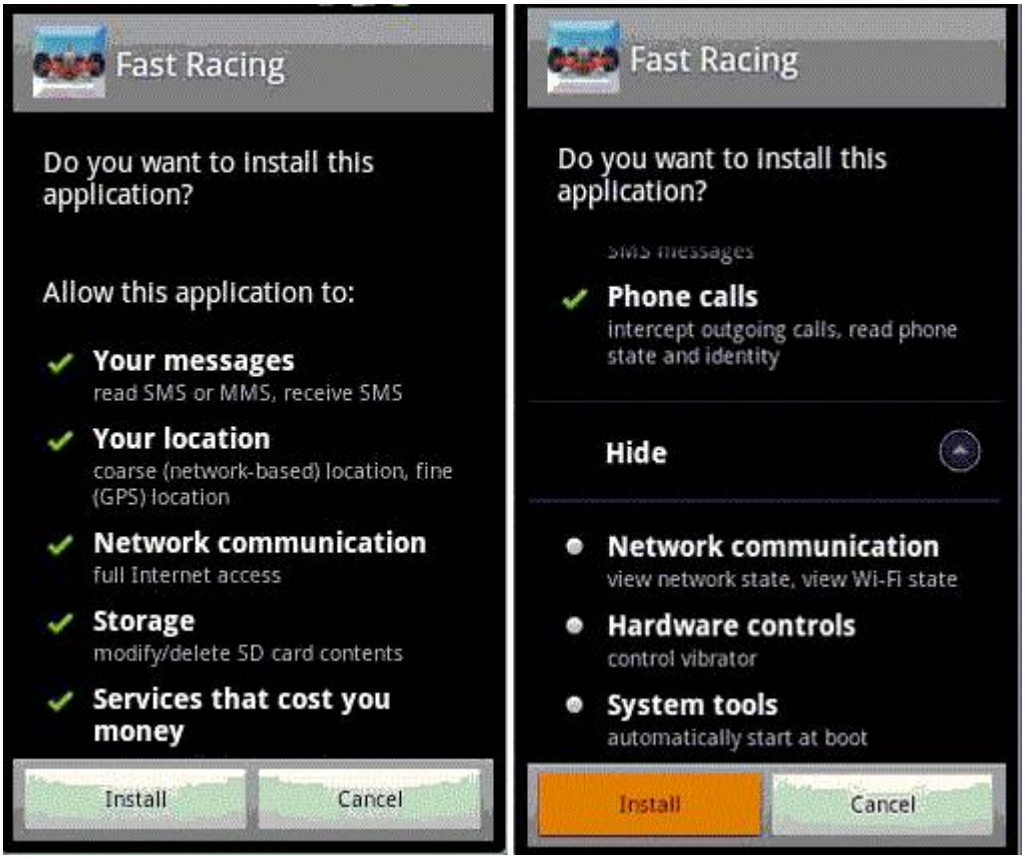
Gartner'ın yapmış olduğu bir araştırmaya göre 2011 yılının son çeyreğinde satılan her iki akıllı telefondan birinde Andoid işletim sisteminin kurulu olduğu göz önünde bulundurulduğunda art niyetli kişiler tarafından geliştirilen zararlı yazılımların Android işletim sistemini hedef almasına eminim sizde benim gibi şaşırmıyorsunuzdur.

Android işletim sistemi neden bu kadar kişi ve üretici tarafından tercih ediliyor diye soracak olursanız bunların başında açık kaynak kodlu olması, ücretsiz olması, açık markete (ücretsiz uygulamalar barındıran Android Market) sahip olması, tabii ki Linux 2.6 çekirdeğini kullanıyor olmasının çok büyük rol oynadığını söyleyebiliriz. Durum böyle olunca da bireylerden kurumlara kadar herkesin yeri geldiğinde kullandığı veya kulkanacağı uygulamanın iyi niyetinden şüphe ettiği durumlarda o uygulamayı analiz etmeye ihtiyaç duyabilir.

Analiz yöntemlerine geçmeden önce kısaca Android'in güvenlik modelinden kısaca bahsetmek istiyorum.

- Android işletim sisteminde Linux işletimin güvenlik modeli baz alınmıştır. Linux işletim sisteminde bildiğiniz üzere dosyalara verilen izinler kullanıcı bazlıdır ve bir kullanıcı başka bir kullanıcının dosyasını o kullanıcı izin vermediği sürece okuyamaz, değiştiremez ve/veya çalıştıramaz. Android işletim sisteminde de her yeni kurulan uygulamayı yeni bir kullanıcı olarak düşünebilirsiniz. Bir uygulama, diğer bir uygulamaya ait dosyalara dosya sistemi üzerinden ulaşamaz.

- Uygulamaların kurulabilmesi için mutlaka dijital sertifika ile (kendinden imzalı (s*elf–signed*) da olabilir) imzalanmış olması gerekmektedir.
- Uygulamalar çalışma esnasında kullanacakları kaynaklara, erişecekleri alanlara göre kurulum esnasında kullanıcıdan bir defaya mahsus olmak üzere izin istemek zorundadırlar. Örneğin bir uygulama, çalışabilmesi için internet bağlantısına ihtiyaç duyuyor ise kurulum esnasında bunu beyan etmek ve kullanıcıdan bu izni istemek zorundadır. İzinler, APK (Android application package) içinde yer alan AndroidManifest.xml dosyası içinde tanımlanmaktadır.



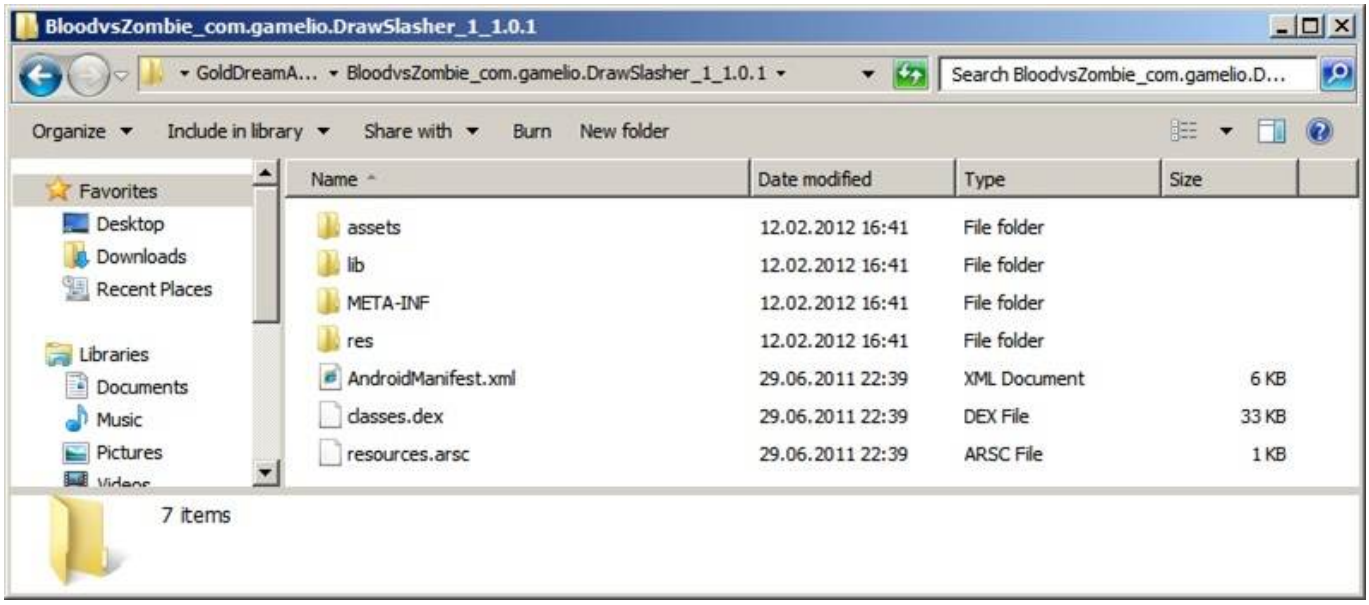
- Kurulan her bir uygulama ayrı bir Dalvik sanal makinesinde çalışmaktadır.

Peki zararlı bir yazılım, Android işletim sistemine hangi yollarla bulaşabilir ?

- Uzaktan kurulum ile: Android Market web sayfası üzerinden cep telefonunuza seçtiğiniz herhangi bir uygulamayı yükleyebilirsiniz. Art niyetli bir kişi tarafından Gmail şifrenizin çalındığını ve isterse bu şifre ile cep telefonunuza internet bankacılığına giriş yaparken kullandığınız tek kullanımlık SMS mesajlarını çalan bir truva atını yükleyebileceğini düşündüğünüzde ister istemez bu özellik sizi korkutuyor.

- Market üzerinden: Bildiğiniz üzere Android Market'e isteyen herkes (25$ ödeyerek sahip olunan bir geliştirici hesabı yeterlidir) geliştirmiş olduğu uygulamayı yükleyebilmekte ve kullanıcıların kullanımına sunabilmektedir. Durum böyle olunca da hangi uygulama güvenilir hangisi değil bunu anlamak pek mümkün olmamamaktadır. Her ne kadar Google bu duruma bir dur demek için Bouncer adında ki zararlı uygulama tarayıcı hizmetini devreye almış olsa da, Apple gibi manuel olarak kod incelemesi yapmadığı sürece zararlı yazılımlar Android Market'i istila etmeye devam edecektir.
- Android SDK ile: Android SDK, Google tarafından uygulama geliştiricileri (developer) için hazırlanmış ve bünyesinde kütüphaneleri ve hata ayıklayıcı (debugger), öykünücü (emulator) gibi çeşitli araçları barındıran bir yazılım geliştirme kitidir. Bu kit içerisinde yer alan Android Debug Bridge (adb) aracı ile öykünücüye (emulator) veya bağlı olan Android işletim sistemi kurulu cihaza uygulama yüklemek mümkündür.
- Internet üzerinden: Web sayfası üzerinden, e-posta eklentisi veya QR kodu ile internet üzerinden indirilen apk dosyası ile Android işletim sistemine uygulama yüklemek mümkündür.

APK uzantısına sahip olan Android uygulamaları zip dosya formatına sahiptir ve bu sayede APK uzantılı herhangi bir dosyanın uzantısı ZIP uzantısı olarak değiştirilerek Winzip, Winrar ve benzer dosya sıkıştırma araçları ile açılabilmektir. APK dosyasının açılması durumunda içinden çıkan classes.dex ve AndroidManifest.xml dosyaları analiz için önem taşıyan dosyalardır.



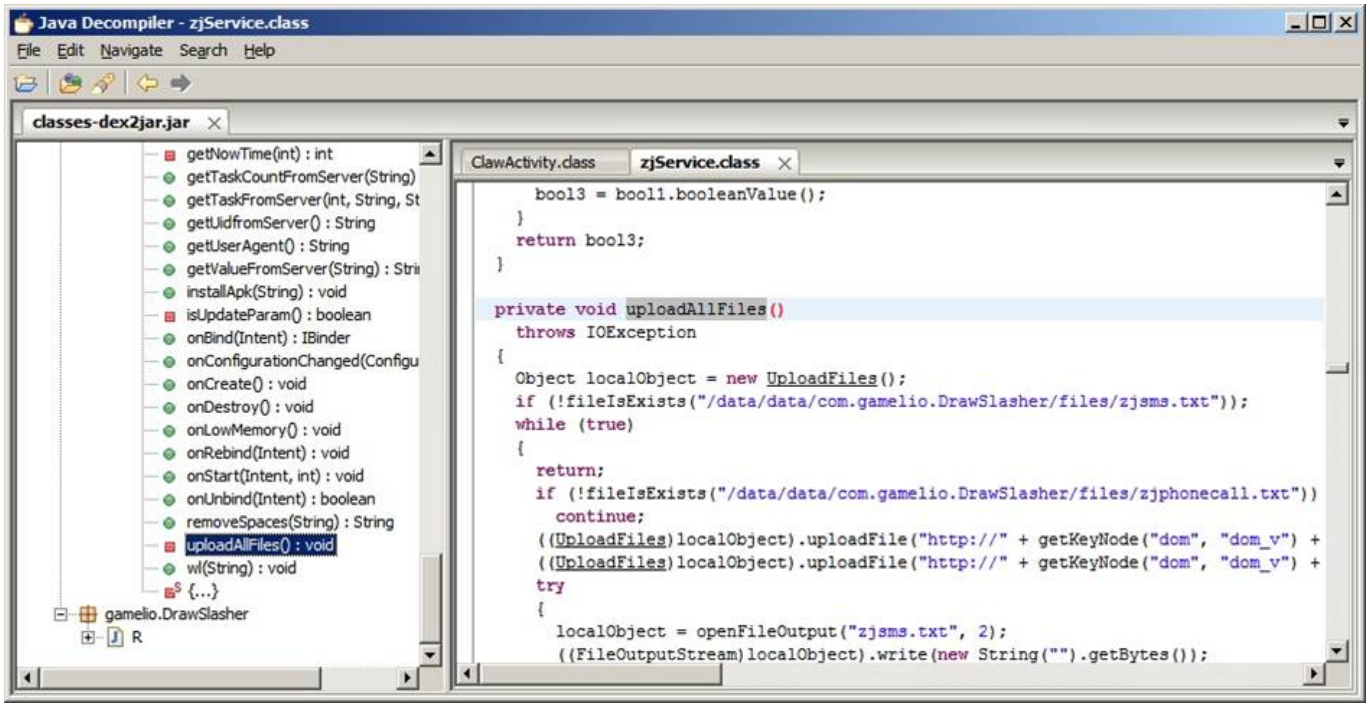
Dex uzantılı classes dosyası, Java ile kodlanmış, Java derleyicisi ile derlenmiş ve dex aracı ile Dalvik sanal makinesinde çalışacak hale

dönüştürülmüş Android uygulamasıdır. Piyasada dex dosyasını class dosyasına çeviren dex2jar gibi ücretsiz araçlar mevcuttur. Bu araçlar ile kaynak koduna çevrilen (örnek komut: d2j-dex2jar.bat classes.dex) class dosyası rahatlıkla analiz edilebilir.

```
C:\Users\Mert\Desktop\Netsec\dex2jar-0.0.9.7\dex2jar-0.0.9.7>d2j-dex2jar.bat spi
tmo.dex
dex2jar spitmo.dex -> spitmo-dex2jar.jar

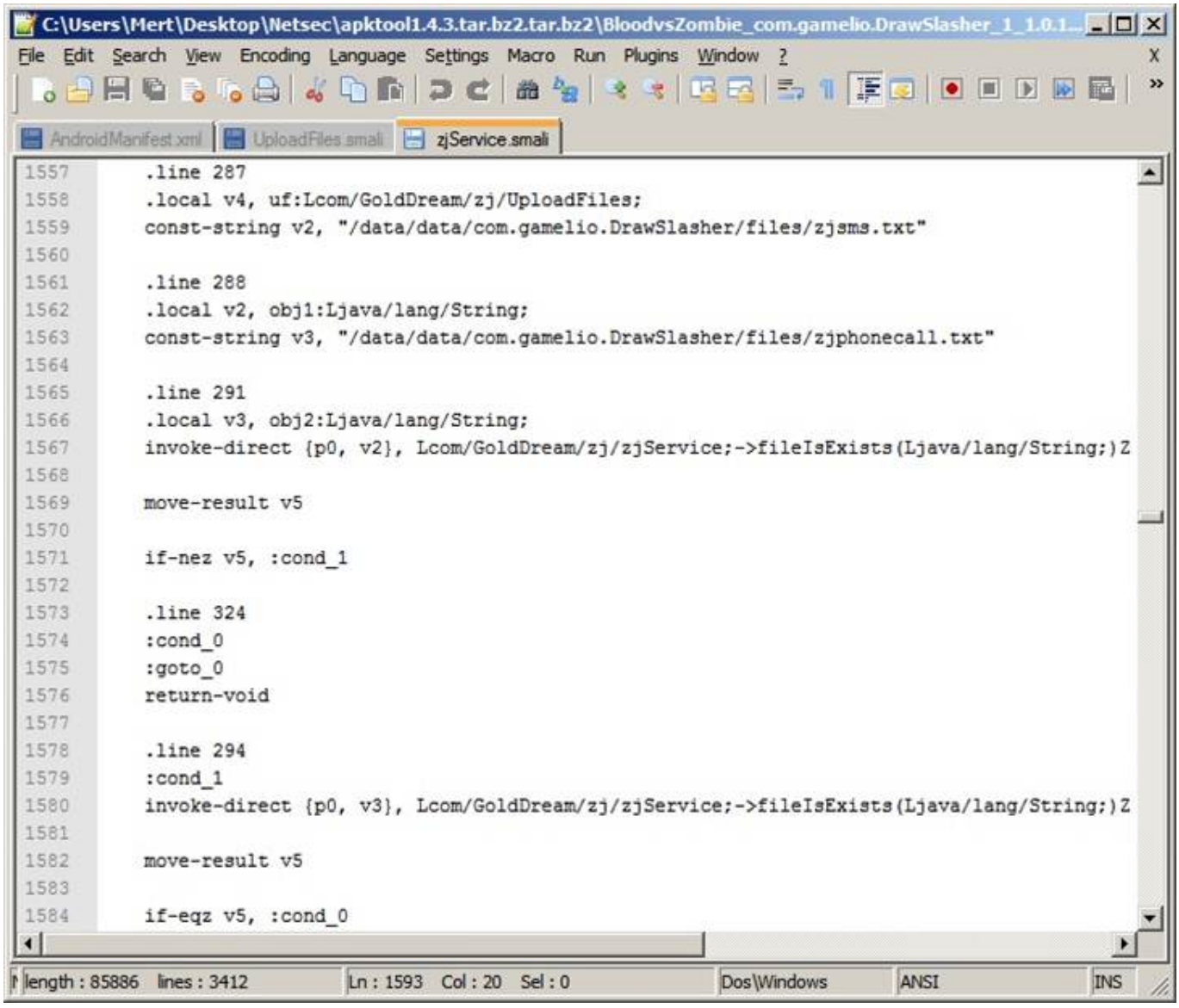
C:\Users\Mert\Desktop\Netsec\dex2jar-0.0.9.7\dex2jar-0.0.9.7>d2j-dex2jar.bat zit
mo.dex
dex2jar zitmo.dex -> zitmo-dex2jar.jar
```

Bildiğiniz veya bilmediğiniz üzere Java ile kodlanmış programlar kaynak koduna çevrilerek (decompile) analiz edilebilmektedir. Durum böyle olunca da dex formatından class formatına dönüştürülen Android uygulamasını JD-GUI ve benzer araçlar ile kaynak koduna geri çevirmek ve analiz etmek mümkündür.



Kimi zaman kaynak koduna çeviren araçlar (decompiler) hatalı çeviri yaparlar. Bu gibi durumlarda dex dosyası, apktool gibi araçlar ile tersine çevrilerek (disassembling) (örnek komut: java -jar apktool.jar d BloodvsZombie_com.gamelio.DrawSlasher_1_1.0.1.apk) analiz edilebilmektedir.

```
I: Baksmaling...
testI: Loading resource table...
I: Loaded.
I: Loading resource table from file: C:\Users\Mert\apktool\framework\1.apk
I: Loaded.
I: Decoding file-resources...
I: Decoding values*/* XMLs...
I: Done.
I: Copying assets and libs...
```

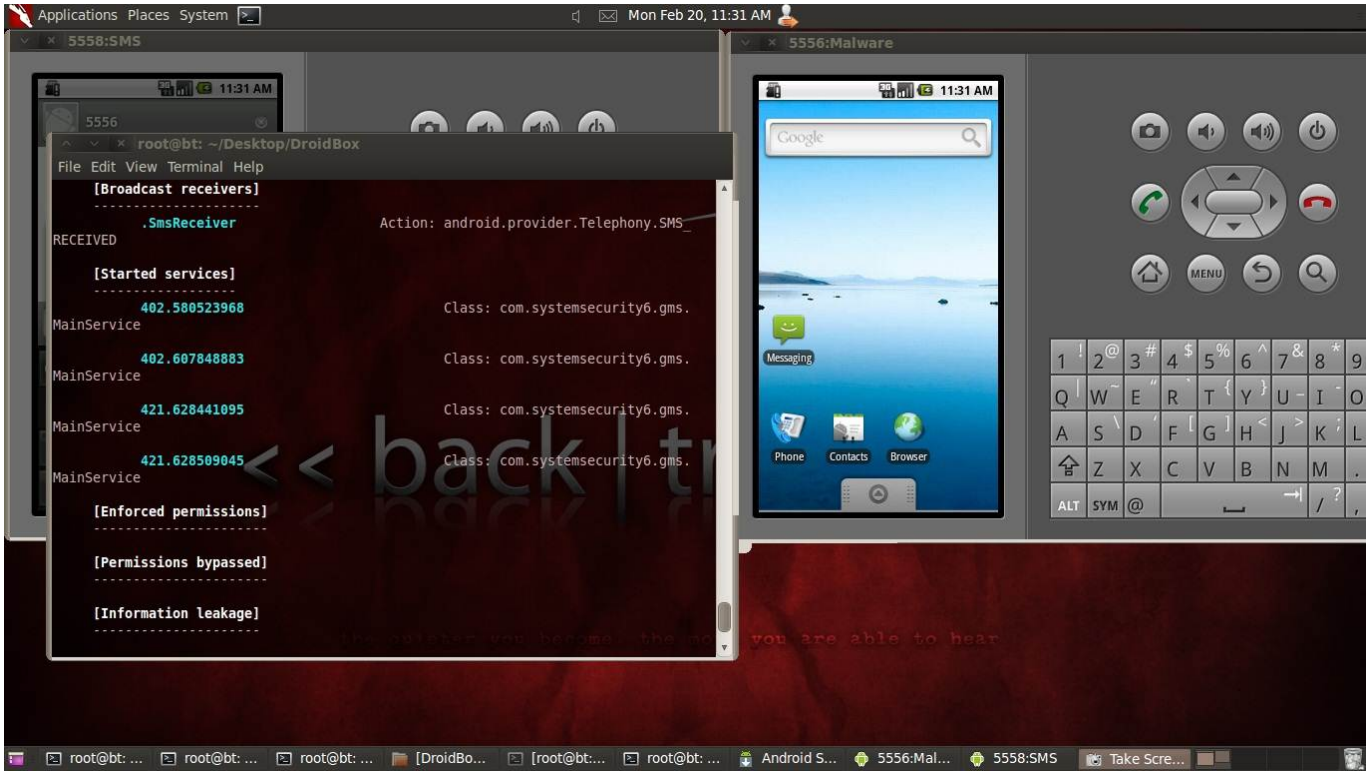


İzinlere gelecek olursak daha önce de belirttiğim gibi izinler AndroidManifest.xml dosyasında tanımlanmaktadır ancak bu dosya binary formatında olduğu için herhangi bir metin editörü ile görüntülenememektedir bu nedenle AXMLPrinter2.jar gibi araçlar ile okunaklı hale getirilmesi (örnek komut: java -jar AXMLPrinter2.jar AndroidManifest.xml) gerekmektedir. Okunaklı hale getirildikten sonra uygulamanın çalışabilmesi için ihtiyaç duyduğu izinler rahatlıkla analiz edilebilmektedir.



Statik analiz için yukarda bahsetmiş olduğum araçlara ilave olarak IDA Pro v6.1+, APKInspector, Dexdump, Smali ve Androguard araçlarından da faydalanabilirsiniz.

Dinamik analiz gerçekleştirmek için Android SDK ile birlikte gelen öykünücüden (emulator) faydalanabilirsiniz ancak zararlı yazılımın servis olarak çalışması ve/veya bazı işlemlerin gerçekleşmesi esnasında çalışma durumu söz konusu olabileceği için görsel ve/veya fonksiyonel olarak öykünücü içinde çalıştırsanız dahi size herhangi bir ipucu vermeyebilir. Bu gibi ihtimallere karşı Droidbox aracından faydalanabiliriz. Droidbox, Android uygulamalarını dinamik olarak analiz etmek için geliştirilmiş bir kum havuzu aracıdır. Gelen/giden ağ verileri takibinden, dosya okuma/yazma takibine, Giden SMS ve arama takibinden, sifreleme işlemlerinin takibine kadar sistem üzerinde gerçekleştirilen kritik işlemleri kayıt altına alarak zararlı yazılımın arka planda neler yaptığını rahatlıkla öğrenebilirsiniz.



Görüldüğü üzere Android işletim sistemini hedef alan zararlı yazılımları analiz edebilmek için statik olsun dinamik olsun faydanalabileceğimiz çok sayıda araç bulunmaktadır ve Google, Android Market'e yüklenen araçları manuel olarak kaynak kod seviyesinde analiz etmemeye devam ettiği sürece bu araçlara çok işimiz düşecektir.

Güvenliğiniz için Android işletim sisteminize mutlaka ama mutlaka bir güvenlik uygulama kurmanızı önerir, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.