امنیت و مباحث قانونی در آندروید

نویسنده : محمد رضانیا (Aka(LinX64

آموزشکده فنی و حرفه ایی سما ، دانشگاه آزاد اسلامی ، واحد فیروزآباد ، فیروزآباد ، ایران

رایانامه : Ash.wxrz@hotmail.com

چکیده

در این مقاله، به بررسی مباحث امنیتی سیستم عامل آندروید و همچنین مباحثی از قبیل **"مباحث قانونی"** و ارائه راهکار های عملی یا کاربردی پرداخته خواهد شد که خوانندگان این مقاله پس از مطالعه کامل، قادر به جلوگیری از نفوذ به دستگاه آندرویدی خود، حفاظت اطلاعات در برابر انواع هکرها و افراد نفوذگر، رخنه های امنیتی و مواردی از قبیل جلوگیری و کشف اپلیکیشن های مخرب خواهند بود. امید است که کاربران و خوانندگان محترم از محتویات این مقاله که با زحمت و تلاش فراوان جهت انتشار انجام شده است، استفاده کافی و مفید را ببرند و از انجام اعمالی از قبیل تخریب و موارد نفوذ یا عواملی که باعث نقض قوانین پلیس سایبری و فتا می شوند، خودداری کنند.

کلمات کلیدی : آندروید، هک، امنیت، مباحث قانونی

۱- مقدمه

امروزه کمتر کسی دیده می شود که به امنیت اطلاعات و حفظ اسرار خود چه در زندگی واقعی و چه در دنیای مجازی یا فضاهای ذخیره سازی در گوشی های هوشمند یا غیره اهمیت ندهد. به همین دلیل بر آن شدیم تا مقاله ایی با عنوان **"امنیت و مباحث قانونی در آندروید"** را برای کاربران آندروید و علاقه مندان آن آماده کنیم و امیدواریم که پس از مطالعه این مقاله، کاربر یا خواننده آن بتواند از اهمیت حفظ اسرار و اطلاعات در گوشی های هوشمند آندرویدی مطلع شود و یک نمونه بارز از ابزار نفوذگران را مورد تحلیل قرار داده و در نهایت به جهت جلوگیری و آشنایی، از حملات نفوذگران و هکرها در امان بماند.

۲- مواد و روش ها

در مقاله ایی که پیش روی شما است از ابزار هایی همانند : ***ابزار های مهندسی معکوس، ابزارهای امنیت و تست نفوذ گوشی های هوشمند*** و دیگر موارد (*که در ادامه خواهید دید*) استفاده شد که در انتها یا ابتدای معرفی هر نمونه، لینکی جهت دانلود و استفاده ابزار مورد نظر قرار داده شده است. در این مقاله سعی شد به نحوی بسیار ساده و به زبان ساده تر، روش های موجود و کاملا تجربی را به زبان شیرین فارسی آورده تا کاربران و مخصوصا دانشجویان عزیز بتوانند نهایت استفاده را ببرند.

۳- آندروید چیست و چگونه بوجود آمد ؟

اندروید (از یونانی: به معنای مَرد، انسان، شبه آدم یا -رُبات (آدم آهنی)) ، به انگلیسی) : Android) یک سیستم عامل موبایل است که **گوگل** برای اسمارت فون‌ها و تبلت‌ها و هم اکنون برای تلویزیون‌ها عرضه می‌نماید و با همکاری ده‌ها شرکت بر روی دستگاه‌های مبتنی بر آندروید قرار می‌دهد. آندروید بر پایه ***هسته لینوکس*** ساخته شده است و بیشترین استفاده را در بین سیستم عامل‌های موبایل دارد.

لایسنس

اکثر قسمت‌های آندروید به صورت اوپن سورس بر اساس مجوز آپاچی نسخه ۲,۰ (Apache License 2.0) ارائه می‌گردد. با اینکه سعی می‌شود تا اکثریت قسمت‌های این سیستم عامل بر اساس همین مجوز ارائه گردد، استثناهایی نیز وجود دارد. برای مثال هسته لینوکس موجود در این سیستم عامل با پروانه عمومی همگانی گنو نسخه ۲ منتشر شده است. این بدان معناست که آندروید یک سیستم عامل اوپن سورس میباشد و به زبانی ساده تر، شما میتوانید برای خود حتی یک سیستم عامل آندروید سفارشی نیز طراحی کنید و یا توسعه بدهید!

شکل ۱-۱: تصویر از محیط Android N

هم اکنون نسخه جدید آندروید با نام Android N در نسخه Preview برای توسعه دهندگان و برنامه نویسان آماده دانلود و استفاده میباشد که سیر صعودی این برنامه در لینک[۶] قابل مشاهده میباشد.

۴- مدل امنیت[۱]

امروزه کمتر کسی مشاهده می شود که حداقل یک برنامه کاربردی را نصب نکرده باشد.در ادامه به بررسی نحوه نصب اپلیکیشن ها و پرمیشن های آنها در آندروید خواهیم پرداخت.

۱. پس از ارسال برنامه توسط اپلیکیشن هایی مانند ShareIt یا نرم افزار های مشابه و یا حتی دانلود از طریق فروشگاه های آنلاین شبیه کافه بازار یا گوگل پلی ، آندروید امضاهای برنامه نویس را چک می کند که تقلبی نباشد و به بررسی اینکه نرم افزار مخرب نباشد میپردازد.

۲. پس از بررسی و چک کردن امضا ها توسط آندروید، آندروید توسط **یک** فایل[۲] به بررسی دسترسی های مورد استفاده در اپلیکیشن میپردازد.

همچنین، دسترسی های مورد استفاده در اپلیکیشن مورد نظر قبل از دکمه نصب در *هنگام نصب* قابل مشاهده میباشد.

۳. پس از پروسه بالا، آندروید چک می کند که **اگر** دسترسی های مورد نظر با نظر کاربر نصب کننده مطابقت دارد، برنامه می تواند بروی دستگاه نصب شود.

این سه موارد، پروسه کلی نحوه نصب یک نرم افزار یا اپلیکیشن را بروی آندروید شرح می دهد.

پی نوشت : هر اپلیکیشن آندرویدی باید دارای فایل AndroidManifest باشد که این فایل با پسوند xml حاوی مشخصات و دسترسی های اپلیکیشن مورد نظر است.

۵- اجزای برنامه[۳]

سیستم عامل آندروید تقریبا به ۵ بخش و ۴ لایه اصلی

[۱] Security Model

[۲] AndroidManifest.xml

[۳] App Components

تقسیم میشود و از بخش های مهم می توان به :

- کرنل لینوکس

این سیستم عامل بر پایه هسته لینوکس توسعه یافته و عملکرد هایی مانند عملکرد سیستم های اولیه از جمله مدیریت فرآیند [1]، مدیریت حافظه [2] مدیریت دستگاه مانند ؛ دوربین ، کیبورد و صفحه نمایش را دارا میباشد.

- کتابخانه ها

در این میان ، موتور جستجوی قدرتمندی با موتور WebKit طراحی شده که متن باز است. همچنین از دیتابیس SQLite استفاده شده که عملکرد خوبی در اشتراک گذاری فایل ها و کتابخانه ها را دارد که با قدرت هر چه تمام تر شما میتوانید براحتی یک موسیقی گوش فرا دهید.

- Android Runtime

سومین بخش از این مجموعه، Dalvik Virtual Machine نام دارد که یک نوع ماشین مجازی با زبان جاوا است که برای آندروید طراحی و توسعه داده شده است.

- Application Framework

چهارمین بخش ، بخش The Application Framework Layer است که لایه چارچوب برنامه ها در Android را فراهم میکند که قادر به خدمات دهی به برنامه های کاربردی است. لذا، توسعه دهندگان نیز میتوانند با استفاده از این بخش ، برنامه های خودشان را بنویسند و تست نهایی را انجام دهند.

- برنامه ها

تمامی برنامه های این سیستم عامل را میتوانید در این بخش مشاهده کنید. برای مثال، مرورگر ها، کتاب ها، بازی های سرگرمی و غیره.

[1] Process Management

[2] Memory Management

۶- امنیت برنامه

به هر برنامه در آندروید ، یک مشخصه یا آیدی تعلق میگیرد که توسط مشخصه خود اجرا می شوند و همچنین به هر اپلیکیشن، یک پروسه اختصاص داده شده و با پروسه خود اجرا می شوند. هر اپلیکیشن آندرویدی پس از نصب در مسیر زیر با نام پکیج آن اپلیکیشن حاوی فایل های دیتابیس ذخیره می شوند :

<data/data/<package-name/

جهت اطلاعات بیشتر:

Application Fundamentals

۷- Android Debug Bridge

این نرم افزار یا Script به شما توسط یک محیط ترمینال چه در سیستم عامل لینوکس و چه در ویندوز اجازه و دسترسی مدیریت فایلها، حذف، اضافه و اجرای کامند های لینوکس بروی سیستم عامل آندروید را می دهد که در ادامه با این نرم افزار و کارکرد آن آشنا خواهید شد.

نحوه نصب یا استفاده از این نرم افزار بسیار ساده است و پس از ورود به این لینک و استخراج محتویات آن(Adb Kits) در یک مسیر و با رفتن به مسیر مورد نظر با CMD ویندوز میتوانید از این ابزار پرکاربرد استفاده کنید.

(بر عهده کاربر- خواننده مقاله)

نحوه استفاده نیز بسیار ساده میباشد. با دستور : cd وارد محل قرار گیری ابزار شوید و با دستور زیر میتوانید در آخر دیوایس ها و دستگاه های متصل به - دستگاه را مشاهده نمایید :

adb devices

نکته : لازم به ذکر است ؛ در صورتیکه شما برنامه نویسی آندروید انجام می دهید و Android Sdk را از قبل دانلود کرده اید ، در مسیری همانند مسیر پیشفرض زیر نیز میتوانید ابزار Adb را مشاهده و استفاده نمایید :

C:\Program Files (x86)\Android\android-sdk\platform-tools

۸- شروعی بر مباحث قانونی در آندروید

در این قسمت، به بررسی دستورات و محیط های عملیاتی و آزمایشگاهی این مبحث خواهیم پرداخت.

پیشنیاز ها :

- آشنایی با محیط لینوکس و دستورات آن
- آشنایی با محیط هایی همانند Terminal در لینوکس و CMD در ویندوز

و بقیه موارد که در صورت نیاز بصورت مختصر به آنها خواهیم پرداخت.

همانطور که در صفحات قبل گفته شد ، آندروید از پایگاه داده SQLite استفاده می کند. این بدان معنا است که برای مثال پیام های مسنجر ها و پیام رسانی هایی همانند WhatsApp در دیتابیس Local (داخلی) نیز ذخیره می شوند و این امر باعث افزایش سرعت در خواندن اطلاعات و بدون نیاز بودن به دانلود مجدد از سرور میباشد.

این مورد بدان معناست که :

در امر برنامه نویسی ، همواره امنیت و سرعت حرف اول را می زده اند !

این موارد گاها باعث ایجاد رخنه ها و نفوذ Rat هاو تروجان هایی می شوند که قادر به نفوذ به فایلها و اطلاعات شما میباشند. برای مثال، بزارید به بررسی دیتابیس WhatsApp بپردازیم.

پس از ورود به مسیر زیر :

data/data/com.whatsapp/

میتوانید وارد پوشه Databases شوید و فایل MsgStore.db را باز کرده یا منتقل کنید به ابزاری با واسط گرافیکی جهت مشاهده محتویات فایل.

در نهایت، محتویات پس از Import در نرم افزاری شبیه SQLiteBrowser را میتوان با یک سری جدول هایی از جمله Messages مشاهده نمود.

یک دیتابیس با جدول ها و کالومن های مشخص را میبینیم اما، فرضا قصد داریم با استفاده از این دیتابیس پیام های ارسالی یا گروه های عضو شده یا موارد غیره توسط کاربر مورد استفاده را بدست آوریم. برای این هدف باید به سراغ تب و جدول زیر :

Browse - TableName > Chat_List

رفته و در نهایت، گروه های عضو شده قابل مشاهده هستند. همچنین، اطلاعات بیشتر از جمله پیام های ارسال شده در جدول messages قابل مشاهده هستند.

این بدان معنا است که اگر دستگاه شما از قبل روت[۲]شده باشد و دستگاه شما بدست فرد مخربی افتاده باشد ، اطلاعات ذخیره شده از جمله پیام های ارسالی مانند پیام های استخراجی توضیحات قبل میتواند براحتی افشا شود و خطرناک باشد.

در توضیحات قبل فقط در رابطه با پیام های یک شبکه اجتماعی صحبت شد و اما مهم تر از پیام های ارسالی در شبکه اجتماعی، اطلاعات دیگر مانند **اطلاعات کارت بانکی، مخاطب های ذخیره شده، علاقه مندی های وب** و همچنین سایت های مرور شده و ذخیره شده و تمامی اطلاعات مهم دیگر ممکن است قابل افشا شدن باشد.

۹- روت کردن چیست و ضرر ها و مزایای آن

به طور خلاصه، روت کردن پروسه ای است که به کاربر آندروید اجازه می دهد تا کنترل همه جانبه دستگاه خود را در اختیار بگیرد. روت کردن در واقع شبیه پروسه جیل بریک (Jail Break) کردن یک دستگاه اپل است. وقتی توانستید آندروید خود را روت کنید، می توانید تنظیمات اپلیکیشن ها و سیستم آندروید

[۱] به ابزار های جاسوسی که کاربر اطلاعی از نصب بودن آنها ندارد گفته می شود.

[۲] دسترسی کاربر ریشه یا کاربری که دسترسی تمام به سیستم عامل دارد.

خود را تغییر دهید، اپلیکیشن های ویژه ای را نصب کنید و بسیاری امور دیگر. روت کردن یک دستگاه آندرویدی از دستگاهی به دستگاه دیگر تفاوت دارد اما به نظر می رسد که با گذر زمان ساده شده باشد.

در حال حاضر بسیاری از مدل های گوشی های آندروید قابل روت کردن هستند.

۱۰- چرا روت کنیم؟

دلایل بسیاری وجود دارد تا شما تصمیم بگیرید دستگاه خود را روت کنید. یکی از مهم ترین مزایای آن، توانایی حذف کردن هر نرم افزار و بازی ناخواسته ای است که شرکت ها روی گوشی ها به طور پیش فرض نصب می کنند. این مورد به افزایش حافظه گوشی نیز کمک می کند.

مزیت دیگر روت کردن، امکان به روز کردن آندروید بسیار زود تر از زمانی که شرکت ها تصمیم به این کار می گیرند.[۱] اگر گوشی شما روت نشده باشد، ممکن است هفته ها و ماه ها طول بکشد تا نسخه دستگاه شما به روز شود. دلایل دیگر برای روت کردن شامل پشتیبان گیری کامل از گوشی، ویژگی های وصل کردن دستگاه ها به هم و نیز افزایش طول عمر باتری می شود.

۱۱- خطرات این کار چیست؟

اولین نتیجه روت کردن این است که گارانتی دستگاه شما از بین خواهد رفت. اما از این مهم تر این است که اگر در این کار دقت نکنید گوشی خود را نابود خواهید کرد! باید پیش از آن جانب احتیاط را نگه دارید و در زمان روت کردن توجه لازم و کافی را به کاری که انجام می دهید، داشته باشید.

۱۲- نگرانی های امنیتی

روت کردن در کل محدودیت های امنیتی را که آندروید در نظر گرفته است را از بین می برد. این به این معنا است که کرم های امنیتی، نرم افزارهای سرقت اطلاعات و تروجان ها، آندروید روت شده را راحت تر می توانند مورد حمله قرار دهند. البته اگر آندروید مورد نظر به برنامه های آنتی ویروس مجهز نباشد و اقدامات امنیتی صورت نگرفته باشد.

۱۳- مباحث قانونی و راه های جلوگیری از افشای اطلاعات (دید کلی)

قبل از اینکه بخواهیم به مباحث قانونی و نحوه جلوگیری از افشاء اطلاعات بپردازیم ، باید اطلاعات پایه ایی از آندروید به عنوان مثال پوشه ها و فایلهای مهم داشته باشیم. در آندروید، به دایرکتوری ها و پوشه های مهم میتوان به : data/data/

که در آن، دیتا ها و دیتابیس های نرم افزار های نصب شده موجود میباشد، اشاره کرد.

به عنوان مثالی دیگر، در آندروید یک مرورگر وب بصورت پیشفرض نصب میباشد که آدرس مهم آن بصورت زیر است :

data/data/com.android.browser/

که پوشه دیتابیس شامل فایلهای مهم و اطلاعات ذخیره شده شما یا حتی سایت های باز شده و مرور شده در آن ذخیره شده است.

همچنین، در ادامه مسیر ها و فایل های مهم میتوان

به موارد زیر اشاره کرد :

- Shared_prefs

shared preference از XML

- Lib

Custom library files required by app [۲]

- Files

فایلهای ذخیره شده توسط برنامه نویس

- Cache

[۱] Installing custom roms

[۲] فایل های کتابخانه های Custom که مورد نیاز توسط اپلیکیشن است.

فایلهای کش[1]شده توسط اپلیکیشن

- Databases

دیتابیس های SQLite

همچنین، فایلها و موارد بخصوصی نیز هستند که میتوان به :

Dmesg

و یا دستور زیر که باعث ایجاد لاگ و ایجاد فایل می شود اشاره کرد :

dmesg > dmesg.log

۱۴- Android Forensic[2]

آندروید سیستم عاملی بود که سریعا از اکتبر ۲۰۰۸ توسط اولین دستگاه هوشمند خود جزو محبوب ترین ها در سال ۲۰۱۱ پیوست و همچنان این آمار رو به رشد است.

از مهم ترین قابلیت های این سیستم عامل میتوان به **متن باز بودن** آن اشاره کرد.

و اما در رابطه با مباحث قانونی؛ بطور کلی؛

Forensics چیست؟

این علم یکی از علوم جالب در زمینه کامپیوتر "علم پزشکی قانونی کامپیوتر" می باشد که با این عنوان شناخته می شود که البته توسط شرکت هایی مانند :

EC-Council

با برگزاری دوره های بخصوصی در این رابطه در حال جذب و آموزش علاقه مندان در این زمینه است. همچنین نام این مدرک را ، CHFI قرار داده اند که در این مقاله در رابطه با این مبحث در آندروید بحث خواهیم کرد.

درحال حاظر، گروه یا شرکتی تحت عنوان : Infosecinstitute

در این زمینه بسیار فعال است و تاکنون مطالب مفیدی ارائه داده است که ابزارهای مختلفی جهت استخراج اطلاعات یا مباحث قانونی نیز در این زمینه نوشته شده و موجود میباشد. از جمله این ابزارها میتوان به Android-Forensic اشاره کرد که کاملا متن باز بوده و شما نیز میتوانید در توسعه آن سهمی داشته باشید.

همچنین، در رابطه با ابزارهای این مجموعه میتوان به ابزار کامل Andriller اشاره کرد. امکانات این ابزار در نوع خود بی نظیر است و از امکانات مختصر آن نیز میتوان به : استخراج اتوماتیک اطلاعات و دیکود کردن اطلاعات، استخراج اطلاعات بدون نیاز به روت بودن دستگاه، Parse کردن اطلاعات و دیکودینگ جهت ساختار پوشه ها و غیره اشاره کرد.

در ادامه به بررسی و با نحوه کارکرد این ابزار آشنا خواهید شد و خواهید دید که چگونه می توان الگو یک دستگاه آندرویدی را بدست آورد.

برای مثال ، با استفاده از نرم افزار معرفی شده، قصد داریم الگو یک دستگاه را با استفاده از فایل :

gesture.key

بدست آورده و در نهایت قفل دستگاه را کشف کرده و به الگوء آن پی ببریم.

در این مسیر می توان به فایل مورد نظر دسترسی پیدا کرد : data/system/gesture.key/

و یا اگر از Adb استفاده میکنید، تنها کافیست با دستور زیر فایل را pull کرده و در نهایت عملیات کرک یا Decode و بدست آوردن الگو را انجام دهید.

adb pull /data/system/gesture.key

پس از شناسایی و انتخاب مسیر فایلهای ذخیره شده ، بروی دکمه go کلیک کرده و سپس اگر دستگاه شناسایی شده باشد فایلهای مهم در مسیر تعیین شده از قبل ذخیره خواهد شد. اما، فقط با فایل gesture.key کار داریم پس باید به تب LookScreens بروید و گزینه اول : Decode Gesture Pattern را انتخاب کرده و مسیر

[1] Cache

[2] مباحث قانونی

الگو را مشخص کرده و در نهایت الگو نمایش داده خواهد شد.

که در نهایت، شما به عنوان یک محقق[1]به سادگی میتوانید اطلاعات مهم را با استفاده از نرم افزار هایی مانند مثال قبل بدست آورید.

۱۵- Android Reverse Engineering[2]

در این قسمت، با مهندسی معکوس اپلیکیشن های آندرویدی آشنا خواهید شد و خواهید دید که چگونه یک اپلیکیشن مخرب خود را بجای یک اپلیکیشن دیگر جا میزند و براحتی از دستگاه شما دسترسی میگیرد.

پیشنیاز ها :

- دانستن اطلاعات کافی از برنامه نویسی آندروید به زبان جاوا و آشنایی با محیط های برنامه نویسی از جمله، Android Studio , Eclipse.
- آشنایی با دسترسی ها در آندروید
- آشنایی کافی با فایل AndroidManifest.xml

معرفی

برای شروع، لازم به ذکر است که تاکنون هیچگونه ویروسی برای آندروید ساخته نشده اما بدافزار ها و اپلیکیشن های مخرب قادر به خرابکاری و سو استفاده از کاربران آندروید میباشند.

متاسفانه، بسیاری از فعالان تعمیرات نرم افزار، بخصوص در این برهه زمانی، **ویروس** را با **بدافزار** اشتباه میگیرند و باعث سردرگمی تمامی کاربران شده اند. اپلیکیشنی که در این قسمت با آن آشنا خواهید شد، نام آن Dendroid است. این اپلیکیشن **یکی از بهترین و کاملترین تروجان های آندروید** میباشد که تاکنون ساخته شده است و توسط یک پنل از سوی هکر و فرد خرابکار که با استفاده از زبان PHP نوشته شده است و مدیریت می شود.

این اپلیکیشن بروی آندروید به عنوان های مختلف و **با آیکون های** مختلف میتواند نصب شود بدون اینکه کاربر حتی توجه ایی به محتویات و دسترسی های استفاده شده در اپلیکیشن کند.

از قابلیت های مهم این اپلیکیشن مخرب میتوان به :

- دسترسی کامل و مدیریت تمام دستگاه آندرویدی
- مدیریت تماس ها
- مدیریت فایلها
- آپلود و دانلود فایلهای حافظه دستگاه آندرویدی

و بقیه موارد اشاره کرد. البته لیست کامل امکانات را میتوانید در این لینک معرفی شده مشاهده و بررسی کنید.

۱۶- بررسی یک اپلیکیشن و انجام مهندسی معکوس بر روی آن

در این قسمت، با مهندسی معکوس یک اپلیکیشن آندرویدی آشنا می شوید و خواهید آموخت که چگونه میتوان تشخیص داد که آیا فایل مورد نظر مخرب است یا خیر.

بطور کلی چندین روش و ترفند وجود دارد که از سریعترین آنها میتوان به سایت DecompileAndroid.com اشاره کرد. تنها کافیست فایل APK مورد نظر را به آپلودر معرفی کرده و صبر کنید تا لینک دانلود ظاهر شود و پس از دانلود با محتویاتی شبیه محتویات زیر مواجه خواهید شد :

- Src
- Res

که دایرکتوری اول، کدهای جاوا مورد استفاده در اپلیکیشن آندرویدی را نمایش می دهد و دایرکتوری دوم، کدهای Layout و Res ها و Values های استفاده شده در اپلیکیشن.

البته ممکن است نتوانید کدهای جاوا را به سادگی بخوانید که در اینگونه موارد، استفاده از روش بعد را پیشنهاد میکنیم.

[1] Investigator

[2] مهندسی معکوس اپلیکیشن های آندرویدی

۱۷- Decompiling an Apk file

با استفاده از این روش میتوانید کدهای جاوا نوشته شده در یک اپلیکیشن آندرویدی را خوانده و براحتی متوجه شوید که در اپلیکیشن چه اتفاق هایی رخ می دهد.

برای شروع، به سه نرم افزار احتیاج پیدا خواهید کرد :

- Dex2Jar
- ApkTool
- JD-GUI

جهت استفاده از اولین نرم افزار، پسوند فایل APK مورد نظر را از .apk به .zip تغییر داده و محتویات فایل را در یک پوشه ایی استخراج کنید.

پس از آن، برای استخراج و مشاهده کدهای جاوا، باید فایل Classes.dex را به مکانی که نرم افزار Dex2Jar دانلود و استخراج شده منتقل کنید و با نگه داشتن SHIFT + RIGHT CLICK گزینه Open command window here را انتخاب کرده و در نهایت، دستور زیر را وارد کنید تا فایل Dex را به فایل Jar تبدیل کند.

```
d2j-dex2jar.bat classes.dex
```

در نهایت، خواهید دید که فایلی با نام classes-dex2jar ایجاد شده و با فرمت یا پسوند Jar میباشد و سپس با معرفی فایل با استفاده از گزینه File در نرم افزار Jd-GUI میتوان تمامی محتویات و کدهای کلاس های نوشته شده به زبان جاوا اپلیکیشن آندرویدی مورد نظر را خوانده و متوجه شوید که آیا کدهای استفاده شده مخرب است یا خیر.

جهت شناسایی و متوجه شدن به اینکه اپلیکیشن مورد نظر مخرب است یا خیر، اگر از قبل دانش برنامه نویسی یا تجربه ایی در این کار داشته باشید، خواهید دید برای مثال کلاس هایی از جمله کلاس های ارسال SMS و دریافت SMS برای مثال ربطی به اپلیکیشن مورد نظر ندارد و همچنین در فایل AndroidManifest.xml ببینید که دسترسی ها بی مورد اضافه شده که مورد قبول نیست و باعث سو استفاده می شود، آن اپلیکیشن را بهتر است به یک اسکنر معرفی کنید تا ببینید شک شما درست بوده است یا خیر.

از این قبیل اپلیکیشن ها در محیط اینترنت فراوان شده و از آنجایی که برنامه نویسی آندروید نیز با توجه به منابع فراوان و فعلی در محیط اینترنت بسیار فراوان شده است، ممکن است هرکسی به فکر سوء استفاده کردن از دستگاه آندرویدی شما بیفتد که بهتر است مواردی که در صفحات قبل مقاله گفته شد را رعایت کنید و بی مورد به اپلیکیشن های مختلف دسترسی Root (کاربر ریشه) را ندهید تا احیانا اپلیکیشن مورد نظر کنترل کامل را بدست بگیرد.

۱۸- سناریو نفوذ و ارائه راهکارهای جلوگیری

در این قسمت به بررسی اینکه چگونه یک فایل مخرب به دستگاه شما انتقال پیدا می کند میپردازیم و همچنین خواهید دید که چگونه میتوان دسترسی های آنها را قطع کرده و در آخر آنها را حذف کنید.

همانطور که از قبل هم میدانستید، جهت دانلود یک اپلیکیشن یا فرضاً بدنبال یک اپلیکیشن رایگان هستید که بروی گوشی خودتان نصب کنید و واضح است که با لینک های مختلف میتوانید آن اپلیکیشن مورد نظر را پیدا کنید و در نهایت نصب.

در این گونه موارد ممکن است به فایل های مخرب فکر نکنید و یک اپلیکیشن فرضا با حجم کم در حدود ۱ تا ۵ مگابایت رو دانلود کرده و حتی به حجم نیز توجه نکنید. غافل از اینکه فایل دانلود شده مخرب است یا همان فایلی بود که بدنبال آن بوده ایم. پس از نصب فایل، متوجه میشوید که اعمال مشکوکی بروی گوشی مورد نظر درحال انجام است و حتی فرض کنید گوشی شما جهت کارهای مختلف از قبل روت شده بوده است و **حتی متوجه نشوید** به اپلیکیشن مورد نظر دسترسی روت نیز بدهید!

در صورتیکه پس از اعمال بالا به اینترنت نیز متصل شوید، آن زمان است که به هکر یا فرد نفوذگر دسترسی **تام الاختیار** داده اید و هکر میتواند از تمامی امکانات گوشی هوشمند شما استفاده کند.

همانگونه که گفته شد، اپلیکیشن های مخرب میتوانند با نام های مختلف و آیکون های مختلف ظاهر و نصب شوند.

برای مثال، در Dendroid، اپلیکیشن مورد نظر با نام Flash Player و آیکون قرمز رنگ به نمایش در می آید (پس از نصب) و ممکن است شما حتی به آن برنامه بصورت برنامه ایی به عنوان باز کردن فلش پلیر در مرورگر های دیوایس از دید خود ببینید که در واقع ممکن است فایل مخرب و عامل دسترسی گرفتن فرد هکر باشد.

نتیجه‌گیری

اما شاید از خود بپرسید که راهکار های جلوگیری از این حملات چیست و چگونه میتوان از این گونه حملات جلوگیری کرد؟

در ادامه، به راه کارهای **ساده و اساسی** میپردازیم که اگر آن ها را رعایت کنید، میتوانید از اینگونه حملات جلوگیری کنید.

• **قدم اول** : همانگونه که گوگل در این رابطه گفته است، همیشه اپلیکیشن های مورد نظرتان را از مارکت های معتبر مثل Google Play Store دریافت و نصب کنید و از نصب کردن از **سورس های نامعتبر و غیر قابل** اطمینان خودداری کنید.

• **قدم دوم** : دسترسی های هنگام نصب اپلیکیشن را مورد بررسی قرار دهید. برای مثال، فرض کنید اپلیکیشنی را دانلود کرده اید که مربوط به تنظیمات دستگاه آندرویدی میباشد اما دسترسی نامرتبط در هنگام نصب دیده می شود یا دسترسی های آن بیش از حد است یا حتی ممکن است تمام دسترسی ها در آن استفاده شده باشد که در این صورت باید کنجکاوانه فایل APK را با استفاده از سایت های آنلاین آنالیز کرده و متوجه شوید که آیا فایل مخرب است یا خیر!.

سپاسگزاری

تشکر فراوان از استاد و همیار بنده در تهیه و انتشار این مقاله، سرکار خانوم کارگر – از اساتید فعال در زمینه پژوهش و عضو گروه کامپیوتر و رباتیک آموزشکده فنی و حرفه ایی سما ، دانشگاه آزاد اسلامی ، واحد فیروزآباد ، فیروزآباد ، ایران

References

Drake, J. J. (2014). *Android™ Hacker's Handbook.* Indianapolis, Indiana: John Wiley & Sons, Inc.

Gupta, A. (March 2014). *Learning Pentesting for*. Packt Publishing Ltd.

Hoog, A. (2011). *Android Forensics.* 225 Wyman Street, Waltham, MA 02451, USA.
Simson L. Garfinkel, P. (2011). *Android Forensics.*
Tamma, R. (April 2015). *Learning Android Forensics.* Packt Publishing Ltd.

---

http://developer.android.com/preview/overview.html

http://developer.android.com/guide/components/fundamentals.html

http://adbshell.com/downloads

http://resources.infosecinstitute.com/category/pen-testing-1

http://github.com/viaforensics/android-forensics

http://andriller.com

http://hackforums.net/printthread.php?tid=4555580

http://code.google.com/p/dex2jar/

http://ibotpeaches.github.io/Apktool/

http://jd.benow.ca/

http://www.virustotal.com