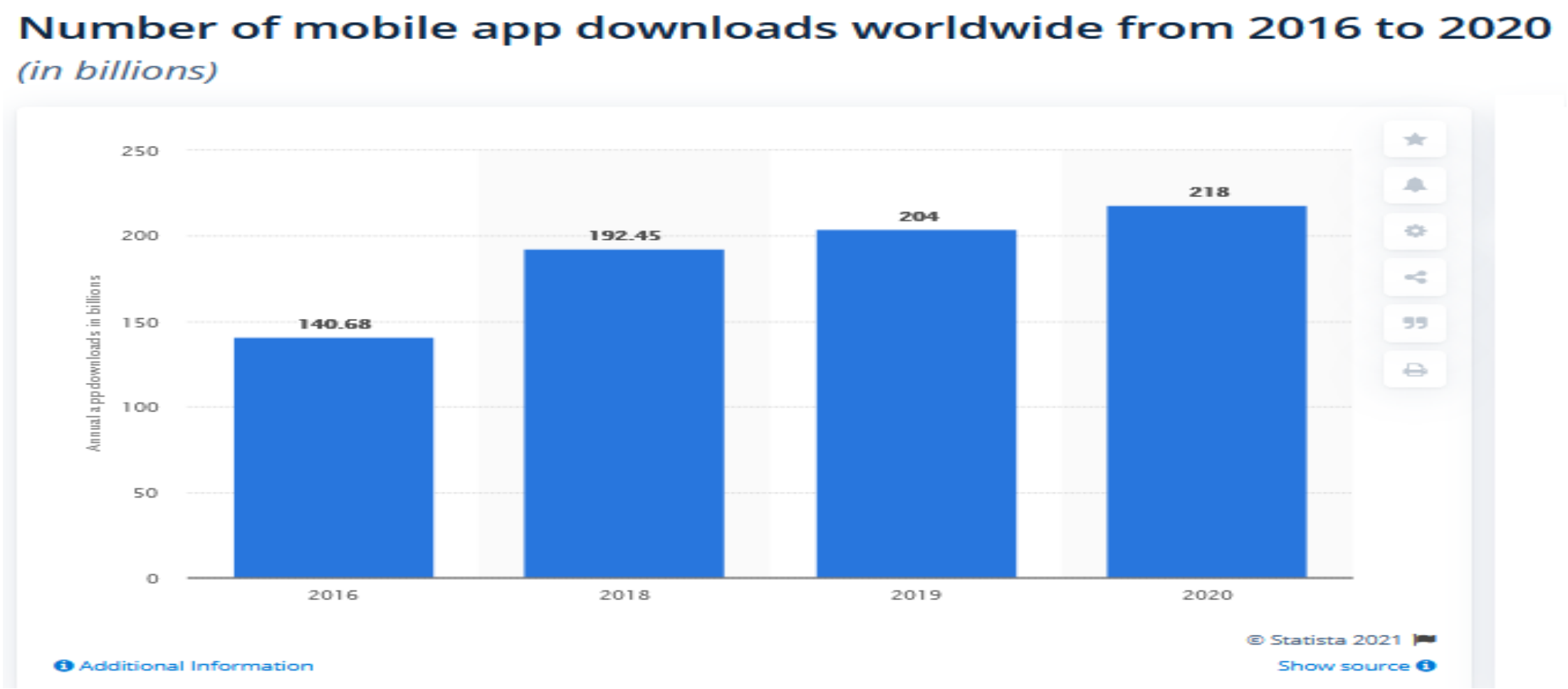
سام : سامانه امن سازی موبایل

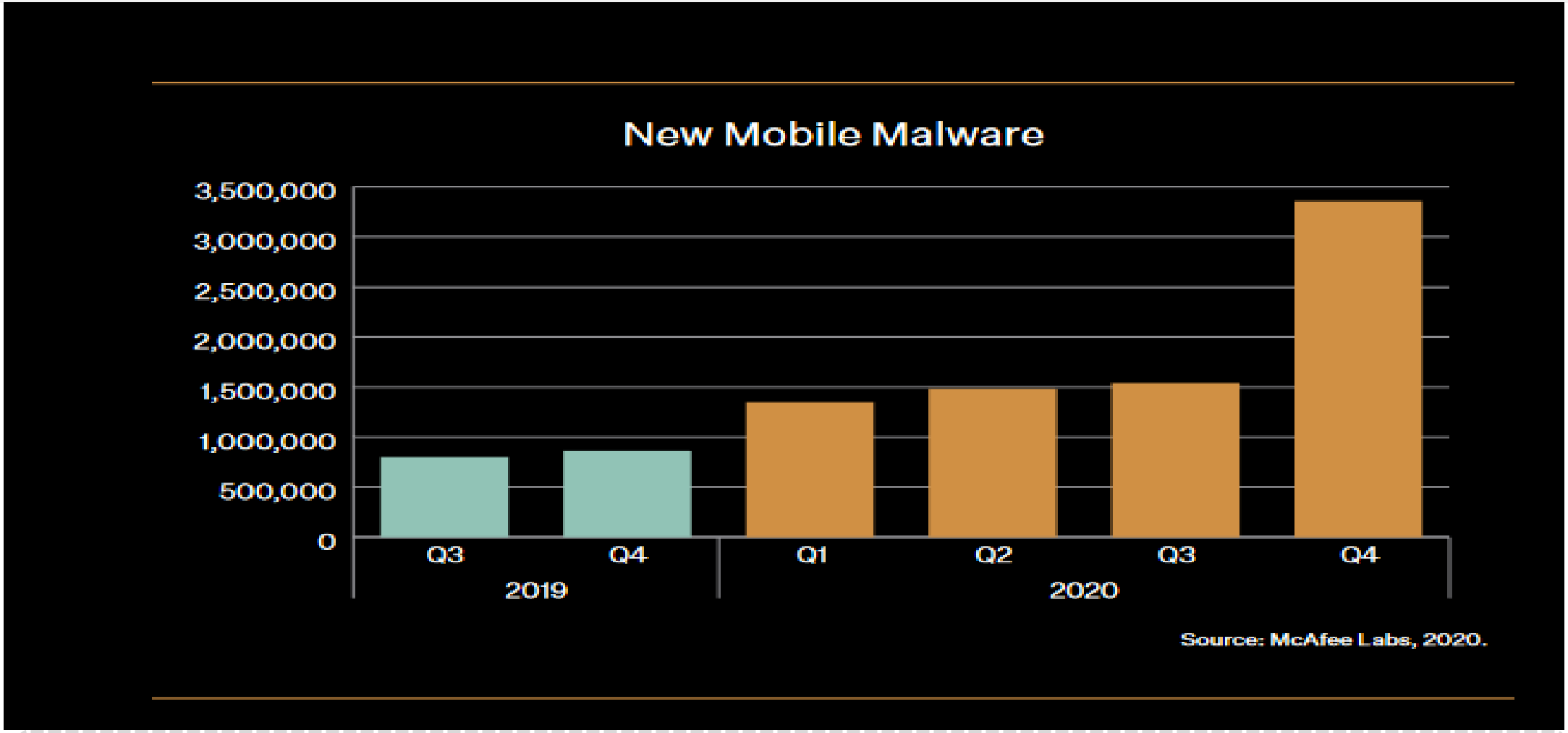
ارتباط گستر خاورمیانه

رشد روزافزون دانلود و استفاده از برنامه های کاربردی تلفن همراه



رشد روزافزون دانلود و استفاده از برنامه های کاربردی تلفن همراه

رشد بی سابقه بدافزار ها و حملات در حوزه برنامه های کاربردی تلفن همراه



گزارش کمپانی مک آفی در مورد رشد بدافزار های موبایل

سام: معرفی ویژگی ها

سامانهٔ امن سازی موبایل (سام – تحلیل ایستا)

تحلیل و کشف بد افزار مبتنی بر موتور آنتی ویروس

تحلیل اجزای نرم افزار و ریسک پذیری اجزا

تحلیل مجوز های نرم افزار و ریسک پذیری مجوزها

تحلیل و کشف بد افزار مبتنی بر تحلیل رفتار

تحلیل و کشف ریسک های امنیتی در سطح مانیفست

مهندسی معکوس جهت شناسایی آسیب پذیری ها در سطح کد منبع و کتابخانه ها

سامانهٔ امن سازی موبایل (سام – تحلیل پویا)

گزارش آسیب پذیری ها و روش های برطرف سازی

تحلیل پویا در زمان اجرای برنامه

تحلیل درسند باکس (جعبه شنی)

شبیه سازی حملات در زمان اجرا

تحلیل تعاملات فایل و شبکه در زمان اجرا

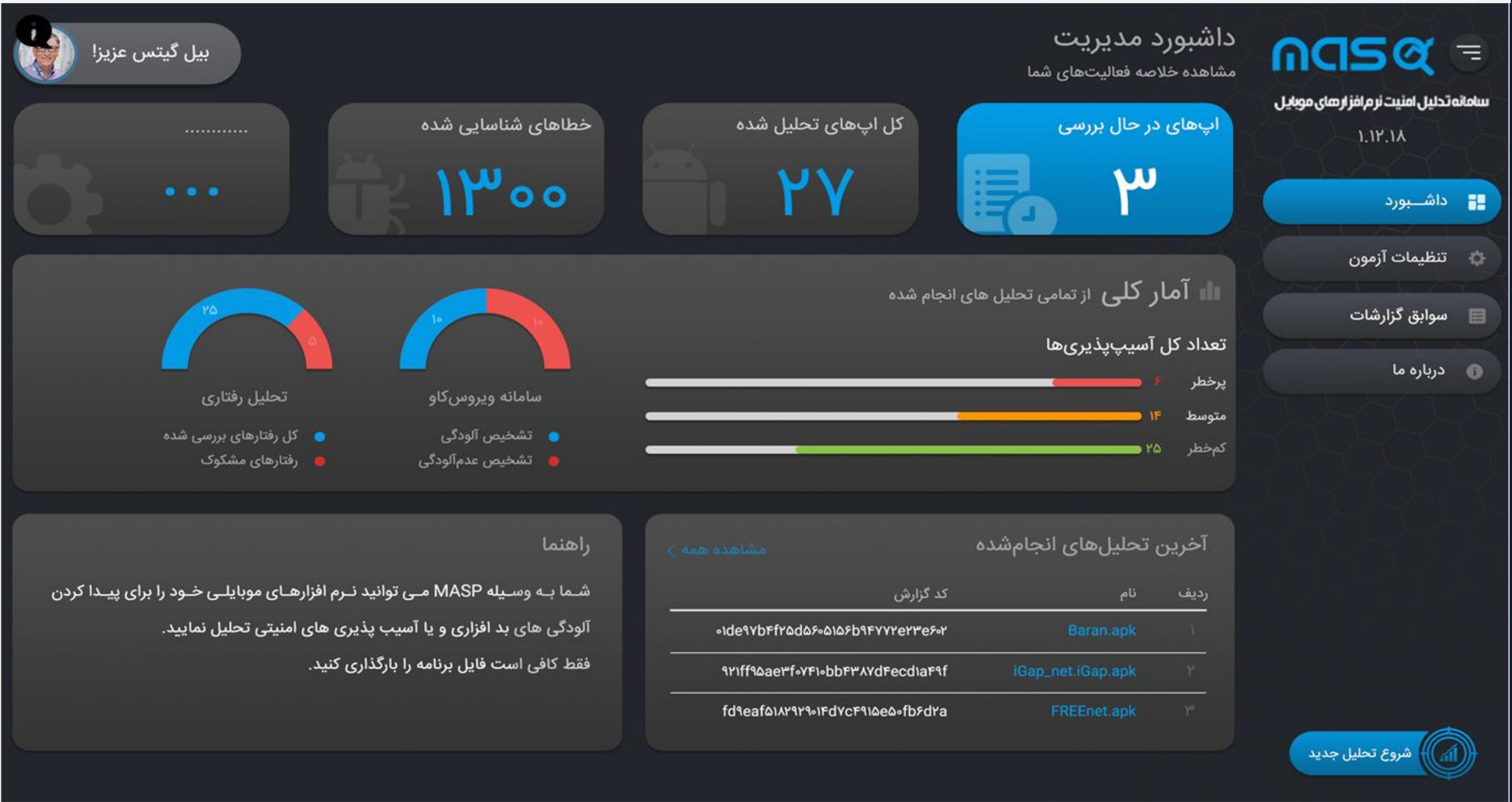
گزارش جامع تحلیل پویا

عنوان	زیر عنوانها	سام
ویروس یاب مؤثر و به روز دارد	قابلیت استفاده از چند ویروس یاب	☑
	امکان استفاده از ویروس یاب به صورت برخط	☑
	امکان استفاده از ویروس یاب به صورت محلی	☑
قابلیت شناسایی انواع بدافزار	امکان شناسایی adware	☑
	امکان شناسایی spyware	☑
	امکان شناسایی ransomeware	☑
	امکان شناسایی keylogger و rootkit	☑
	امکان شناسایی باتها و c&c	☑
	شناسایی بد افزار مبتنی بر تحلیل کد DEX	☑
	امکان شناسایی ارتباطات، دسترسی ها و رفتارهای مخرب و مشکوک	☑
قابلیت شناسایی ضعفهای ساختاری	امکان شناسایی static parameters نظیر hardcoded passwords	☑
	امکان تشخیص الگوریتمهای ضعیف امنیتی	☑
	قابلیت تبدیل کد باینری به کد زبان اصلی سطح بالا و تحلیل آن	☑
	قابلیت تحلیل کد در هم ریخته شده (obfuscated code)	☑
	قابلیت تبدیل به کدهای میانی و تحلیل آن	☑
تحلیل سایر اجزا	تحلیل کامپوننت های اصلی (Activities,Services,Recivers,Providers)	☑
	تحلیل فایل های کتابخانه ای (Library)	☑
	تحلیل مانیفست اپلیکیشن و تنظیمات عمومی و شناسایی آسیب پذیری های مانیفستی	☑
	تحلیل مجوز های اپلیکیشن و سطح ریسک انها	☑
	تحلیل ساختار و آسیب پذیری Java API	☑
تحلیل های غیر امنیتی	تحلیل جهت ارایه پیشنهاد optimization improvements به وسیله شناسایی correctness	☑
	تحلیل performance	☑
	تحلیل usability, accessibility	☑
	تحلیل Control Flow, Class /Code/Object Flow و ارایه گراف های مربوطه	☑

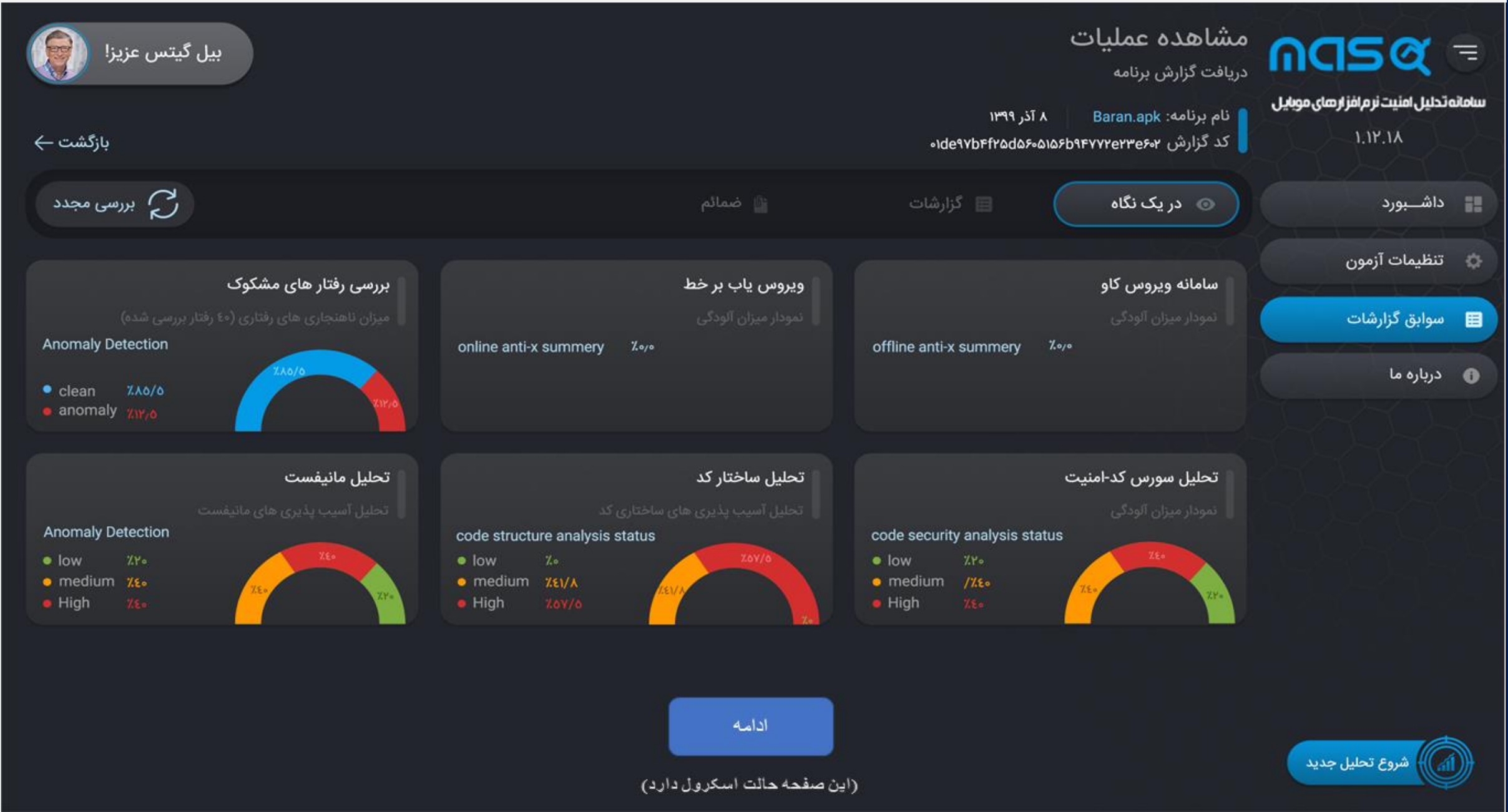
عنوان	زیر عنوانها	سام
تحلیل پویا اجزا	تحلیل و انالیز اجزای قابل پیمایش	☑
	تحلیل و انالیز اجزای کلیه اجزا	☑
ماژول نفوذ گر	جمع آوری و گزارش ریسک های قابل نفوذ	☑
	نفوذ به اکتیویتی ها	☑
	شبیه سازی حملات نفوذ به پروایدر ها و دیتابیس اپلیکیشن	☑
	حمله به سرویس های آسیب پذیر اپلیکیشن	☑
	شنود و ثبت ترافیک ورودی و خروجی اپلیکیشن بر بستر شبکه	☑
	حمله به ریسیور های آسیب پذیر	☑
	شنود / استراق سمع پیام های مبادله شده توسط intentهای اپلیکیشن	☑
ماژول تحلیل WebApi	شناسایی WebApiهای مربوط به اپلیکیشن	☑
	آنالیز امنیتی Webapi براساس استاندارد Owasp top 10 (web)	☑
ماژول نمایش و اتصال	امکان نمایش محیط تحلیل به صورت زنده توسط Vnc	☑
	امکان اتصال به محیط تحلیل و کار با محیط و اپلیکیشن مورد تحلیل به صورت زنده توسط vnc	☑
	امکان نصب و راه اندازی نرم افزار های مورد نیاز در تحلیل پویا به صورت اتوماتیک بر روی دستگاه	☑
	اتصال خودکار دستگاه به نرم افزار سیم و اماده سازی محیط تحلیل	☑
تحلیل با Agent	انجام تمامی تحلیل های پویا با agentجهت افزایش دقت	☑
	امکان تحلیل IO فایل و رمزنگاری به وسیله Agnet	☑

سام: نمای محصول

داشبورد مصول



داشبورد محصول



ارتباط گستر خاور میانه

تحلیل بد افزار (موتور ویروس یاب محلی)

تحلیل بد افزار

تحلیل بدافزار - محلی | تحلیل بدافزار - بر خط | تحلیل بد افزار - رفتاری | تحلیل بد افزار - اجز شناسی | تحلیل آدرس های اینترنتی | آمار

نتایج تحلیل - محلی (آفلاین)

پویش مجدد

Antivirus Name	Result
DrWeb	Not Infected
F-Prot	Not Infected
ESET	a variant of Android/Exploit.Towel.A trojan
Sophos	Andr/TowRoot-A
BitDefender	Not Infected
McAfee	Not Infected
ZAV	TrojanDownloader.AndroidOS.Agent.A
AVG	Android/CVEGen.AD.CC
Comodo	Malware

تحلیل بد افزار(تحلیل ناهنجاری و رفتار مشکوک)

تحلیل بد افزار

تحلیل بدافزار - محلی | تحلیل بدافزار - بر خط | تحلیل بد افزار - رفتاری | تحلیل بد افزار - اجز شناسی | تحلیل آدرس های اینترنتی | آمار

تحلیل رفتاری های مشکوک - ریسک پذیر

نوع رفتار	فایل مشکوک
این اپلیکیشن اطلاعات حساس مربوط به شبکه وایفای نظیر نام شبکه ، آدرس ، و پسورد و غیره را بررسی و ثبت می نماید	com/fon/connectivitysdk/model/AppWifiConfiguration.java com/fon/connectivity/android/model/AppWifiConfiguration.java com/fon/connectivity/android/wifi/NetworkManagerImpl.java com/fon/wifiapp/connectivity/FonNetworkManagerImpl.java
This application reads the ISO country code equivalent for the SIM provider's country code	com/fon/analytics/common/utils/ConnectivityUtil.java com/fon/performance/utils/ConnectivityUtil.java
This application reads the Cell ID value	com/fon/analytics/qoe/models/cellular/WcdmaModel.java com/fon/analytics/qoe/models/cellular/GsmModel.java
این اپلیکیشن وضعیت سیم کارت (فعال ، غیر فعال و ..) را می خواند	com/fon/analytics/qoe/utils/CellTools.java
این اپلیکیشن از طریق ارتباطات سوکت با یک سرور راه دور ارتباط برقرار می کند	com/mixpanel/android/java_websocket/server/WebSocketServer.java com/fon/qoe/enhanced/apkb/client/TLSSocketFactory.java com/fon/connectivity/android/util/NoSSLv۳SocketFactory.java com/fon/connectivity/android/util/TLSSocketFactory.java
این اپلیکیشن اطلاعات مربوط شبکه های داده فعال را ثبت می نماید	com/appsflyer/AppsFlyerLib.java com/fon/analytics/common/utils/ConnectivityUtil.java

تحلیل آسیب پذیری ها

تحلیل آسیب پذیری ها

تحلیل مانیفست | تحلیل سورس کد - امنیت | تحلیل سورس کد - ساختار | تحلیل کتابخانه ها - Libraries | آمار

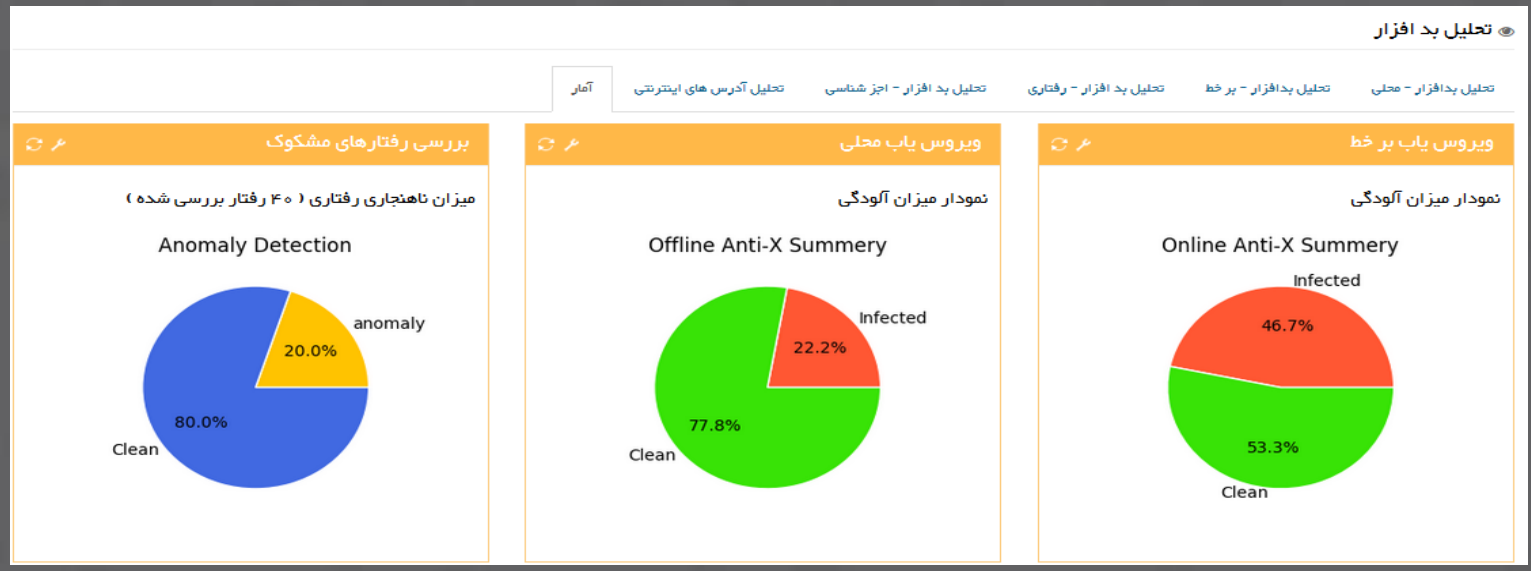
تحلیل سورس کد - امنیت

Potential Hardcoded Sensitive Data این فایل ها ممکن است حاوی اطلاعات حساس همچون رمز عبور و یا نام کاربری باشند ، لطفا با بررسی سورس کد از صحت این موضوع اطمینان حاصل کنید OWASP Top ۱۰ Mobile-۲۰۱۶ : M۱۰	خطرناک	org\owasp\goatdroid\herdfinancial\misc\Constants.java
Weak Cryptographic Hash استفاده از الگوریتم های رمزنگاری نا امن همچون Md۵,Sha۱ OWASP Top ۱۰ Mobile-۲۰۱۶ : M۵	خطرناک	org\apache\commons\codec\digest\DigestUtils.java
Write App data to External Storage این اپلیکیشن داده ها را در فضای ذخیره سازی خارجی نیز ذخیره میکند که ممکن است توسط سایر اپلیکشن ها / بد افزار ها قابل دسترس باشند OWASP Top ۱۰ Mobile-۲۰۱۴ : M۲.	خطرناک	org\owasp\goatdroid\herdfinancial\activities\ViewStatement.java
Often Misused: Authentication (DNS) استفاده از توابع مرتبط با سرویس DNS بدون هیچگونه فرایند احراز هویت ، خطر حملات جعل DNS و سرقت داده ها را به دنبال خواهد داشت OWASP Top ۱۰ Mobile-۲۰۱۶ : M۷	متوسط	com\google\common\net\HostSpecifier.java com\google\common\net\InetAddresses.java
Obsolete: Deprecated by OWASP ESAPI برخی از توابع و متد های به کار برده شده در کد از نظر کابرد و امنیت بر طبق OWASP ESAPI منسوخ شده هستند ، بهتر است با متد های امن پیشنهادی ESAPI جایگزین شوند.. OWASP Top ۱۰ Mobile-۲۰۱۶ : M۷ ESAPI Secure Coding Guideline	متوسط	com\google\common\io\FileBackedOutputStream.java net\sqlcipher\database\SQLiteDatabase.java org\owasp\goatdroid\herdfinancial\requestresponse \AuthenticatedRestClient.java org\owasp\goatdroid\herdfinancial\requestresponse\RestClient.java
Using Temp File این اپلیکشن برای نگهداری برخی از داده ها از فایل های موقت استفاده می نماید. باید با بررسی سورس کد اطمینان حاصل نمایید که این اطلاعات حساس نیستند	کم خطر / مورد توجه	com\google\common\io\FileBackedOutputStream.java net\sqlcipher\database\SQLiteDatabase.java

سام: تحلیل آپ های الوده و آسیب پذیر

تحلیل نرم افزار مشاوره خانواده جعلی توسط ماژول تحلیل بدافزار

اجرای نرم افزار پس از نصب ، وانمود شدن به حذف آپ به دلیل خطای ناشناخته



مشاهده نمودار آلودگی تولید شده توسط ماژول تحلیل بدافزار

تحلیل نرم افزار مشاوره خانواده جعلی توسط ماژول مهندسی معکوس

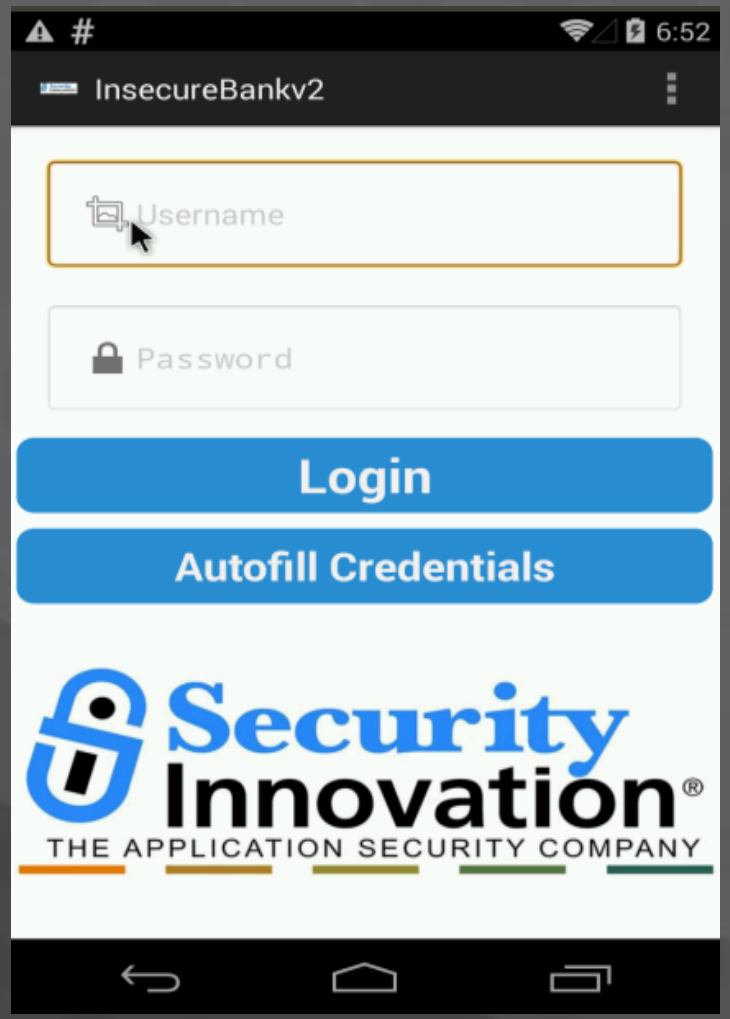
```
public CoinHiveConfig(String string2, String string3, String string4
    d.b(string2, "url");
    d.b(string3, "siteKey");
    d.b(string4, "username");
    this.url = string2;
    this.siteKey = string3;
    this.username = string4;
    this.threads = n2;
    this.throttle = f2;
    this.autoThread = b12;
    this.forceASMJ = b13;
    this.enable = b14;
}

public /* synthetic */ CoinHiveConfig(String string2, String string3
    if ((n3 & 1) != 0) {
        string2 = "file:///android_asset/coinhive.html";
    }
    if ((n3 & 2) != 0) {
        string3 = "RHDMXKDoD2aYDwX5PRM0IUfNrQMv9yCR";
    }
    if ((n3 & 4) != 0) {
```

این اپلیکیشن در کد منبع خود از کتابخانه Coinhive استفاده نموده و با سو استفاده از منابع سخت افزاری تلفن همراه کاربر اقدام به استخراج مخفیانه ارز دیجیتال برای گروه تولید کننده این بدافزار می نماید.

```
public final String generateUrl() {
    Object object = i.a;
    object = new Object[]{this.url, this.siteKey, this.username, this.threads, this.autoThread, Float.valueOf(this.throttle)};
    object = String.format("%s?site_key=%s&username=%s&threads=%d&is_auto_thread=%s&throttle=%s", Arrays.copyOf(object, object.length));
    i.a(object, "java.lang.String.format(format, *args)");
    return object;
}
```

تحلیل اینترنت بانک آسیب پذیر توسط ماژول تحلیل مانیفست



اجرای نرم افزار پس از نصب ، وانمود شدن به حذف آپ به دلیل خطای ناشناخته

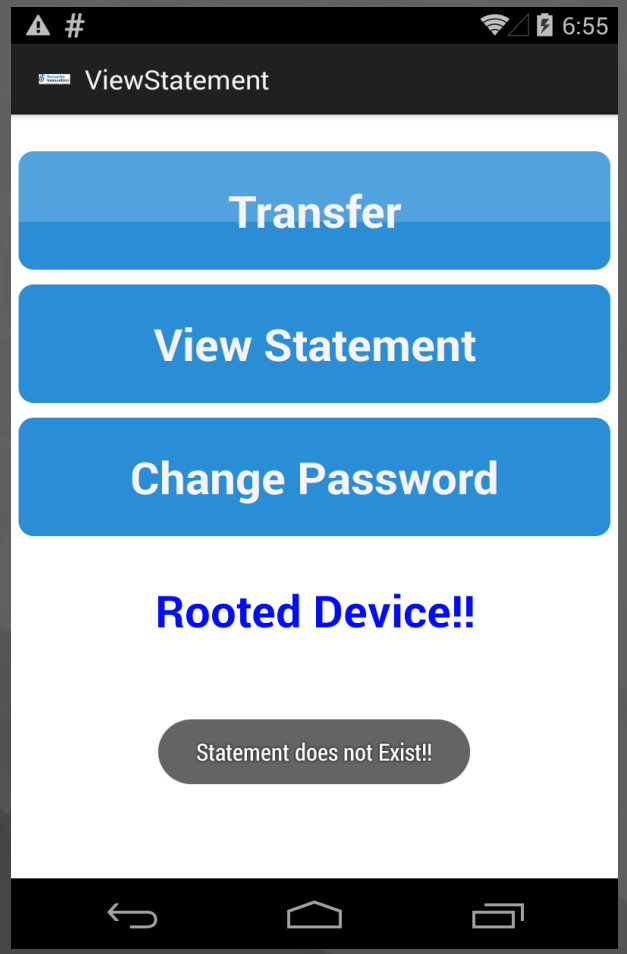
تحلیل آسیب پذیری ها

تحلیل مانیفست

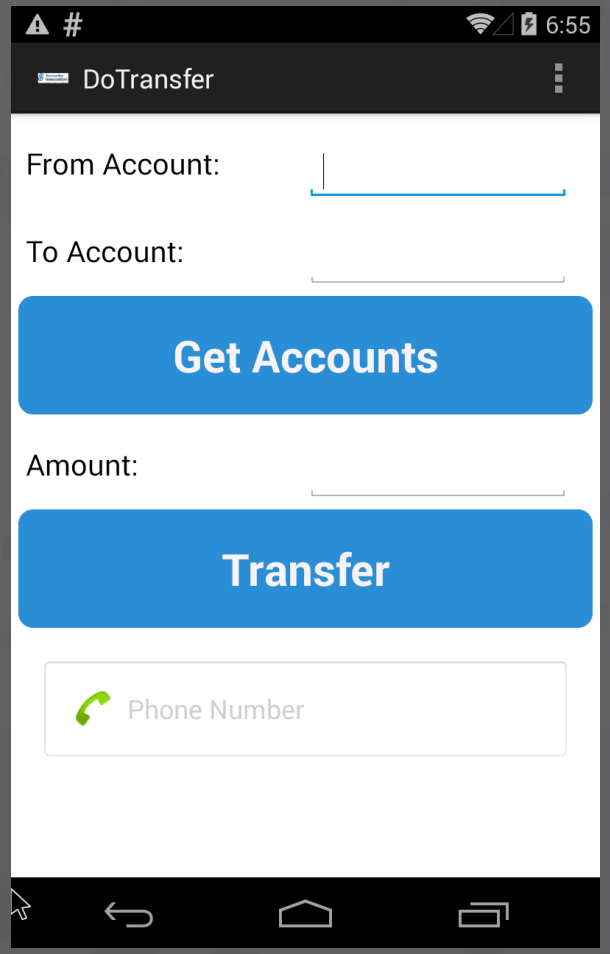
آسیب پذیری	سطح خطر	شرح
حالت پشتیبان گیری برای اپلیکشن فعال است allowBackup Flag is Set To] True[OWASP Top ۱۰ Mobile-۲۰۱۴ : M۴	متوسط	فعال بودن حالت پشتیبان گیری باعث خواهد شد تا هر فرد بتواند بدون نیاز به مجوز خاصی و با استفاده از ابزار adb از داده های برنامه نسخه پشتیبان تهیه نماید که می تواند منجر به فاش شدن غیر عمدی داده های برنامه گردد.
Activity {com.android.insecurebankv۲. .PostLogin} is not Protected Exported Flag Is Set To TRUE	پر خطر	An Activity is not Protected. این کامپوننت به صورت exported و بدون هیچ محافظت خاصی تعریف شده است. فرد مهاجم / بد افزار ها می توانند با فراخوانی مستقیم این کامپونت بدون هیچ مجوز خاص و یا به عنوان مثال بدون عبور از مرحله احراز هویت در اپلیکشن به این کامپونت دست یابند
Activity {com.android.insecurebankv۲. .DoTransfer} is not Protected Exported Flag Is Set To TRUE	پر خطر	An Activity is not Protected. این کامپوننت به صورت exported و بدون هیچ محافظت خاصی تعریف شده است. فرد مهاجم / بد افزار ها می توانند با فراخوانی مستقیم این کامپونت بدون هیچ مجوز خاص و یا به عنوان مثال بدون عبور از مرحله احراز هویت در اپلیکشن به این کامپونت دست یابند
Activity {com.android.insecurebankv۲. ViewStatement} is not Protected. Exported Flag Is Set To TRUE	پر خطر	An Activity is not Protected. این کامپوننت به صورت exported و بدون هیچ محافظت خاصی تعریف شده است. فرد مهاجم / بد افزار ها می توانند با فراخوانی مستقیم این کامپونت بدون هیچ مجوز خاص و یا به عنوان مثال بدون عبور از مرحله احراز هویت در اپلیکشن به این کامپونت دست یابند

مشاهده نمودار آلودگی تولید شده توسط ماژول تحلیل بدافزار

دسترسی به اجزای آسیب پذیر بدون احراز هویت در تحلیل پویا



دسترسی به صفحه جزییات حساب
بدون احراز هویت در تحلیل پویا



دسترسی به صفحه انتقال وجه بدون
احراز هویت در تحلیل پویا

اجرای آپ در سند باکس تحلیل پویا و
بررسی آسیب پذیری های شناخته شده
توسط ماژول تحلیل مانیفست

با سپاس


شرکت مهندسی
ارتباط گستر خاورمیانه آپادانا
امنیت در فناوری اطلاعات