سوءاستفاده جدیدAndroid RAT از تلگرام

خانواده بدافزار کاملاً جدیدی توسط محققان ESET کشف شده‌است.

محققان ESET یک خانواده جدید از ابزارهای مدیریت از راه دور اندرویدی(Android RAT) را کشف کرده‌اند که از پروتکل تلگرام برای ارسال دستور، کنترل و سرقت داده سوءاستفاده می‌کند. این خانواده کاملاً جدید بدافزار که حداقل از آگوست ۲۰۱۷ پخش شده‌است، در مارس ۲۰۱۸، کد منبع آن به صورت رایگان در تلگرام برای هک کردن کانال‌ها در دسترس قرار گرفت و در نتیجه، صدها نسخه موازی از این نرم‌افزارهای مخرب در حال گردش است.

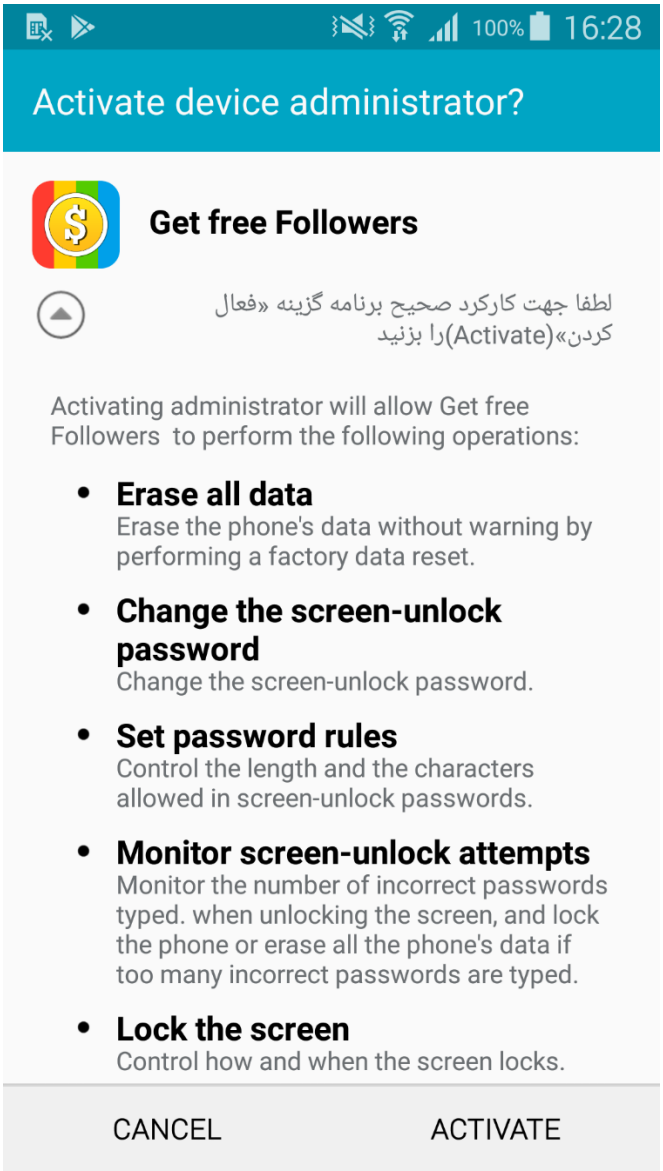
یکی از این نسخه‌ها با بقیه متفاوت است - با وجود کدمنبع رایگان آن، برای فروش در یک کانال تلگرام اختصاصی تحت نام HeroRat عرضه می‌شود. با توجه به قابلیت آن در سه مدل قیمت‌گذاری شده‌است و با یک کانال ویدیویی پشتیبانی می‌شود. این نکته که این نوع از یک سورس کد فاش شده ایجاد شده و یا اینکه یک سورس کد اصلی است و جدیداً فاش شده‌است هنوز مشخص نیست.

این بدافزار چگونه کار می‌کند؟

مهاجمان قربانیان را فریب می‌دهند تا این RAT را با انتشار فایل‌های صوتی که به ظاهر جذاب هستند دانلود کنند. این بدافزارها از طریق appهای شخص ثالث، شبکه‌های اجتماعی و برنامه‌های پیام‌رسانی گسترش می‌یابند. این بدافزار بیشتر در ایران پخش شده‌است که به عنوان برنامه‌هایی که اینترنت رایگان فراهم می‌کنند، یا بیت کوین رایگان فراهم می‌کنند یا فالورهای بیشتر در رسانه‌های اجتماعی را نوید می‌دهند، هستند. این بدافزار در Google Play دیده نشده‌است.

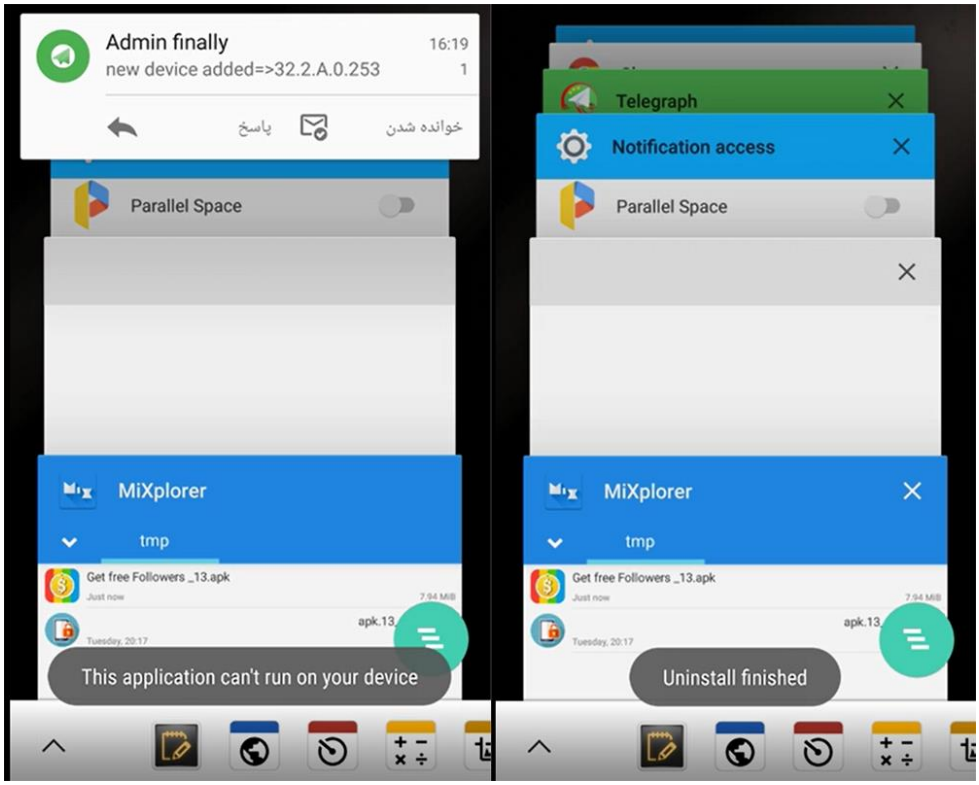
شکل ۱ برخی از تغییر قیافه‌ها مورد استفاده در انتشار RAT

این بدافزار در تمام نسخه‌های اندروید اجرا می‌شود. با این حال کاربران قربانی باید مجوزهایی از جمله فعال کردن برنامه به عنوان مدیر دستگاه را به برنامه بدهد. مهاجمان این کار را از طریق مهندسی اجتماعی انجام می‌دهند.



شکل ۲ RAT درخواست حقوق و سطح دسترسی مدیریت (administrator) را می‌کند

پس از اینکه بدافزار بر روی دستگاه قربانی نصب و راه‌اندازی شد، یک پنجره کوچک ظاهر می‌شود که ادعا می‌کند برنامه نمی‌تواند بر روی دستگاه اجرا شود و بنابراین حذف خواهد شد. در مواردی که محققین ESET مورد تجزیه و تحلیل قرار داده‌اند، پیام حذف جعلی بسته به تنظیمات زبان دستگاه هدف می‌تواند به زبان انگلیسی یا فارسی نمایش داده‌شود. پس از اینکه حذف غیر مجاز به ظاهر کامل شد، آیکون برنامه ناپدید می‌شود. با این حال، در سمت مهاجم، یک دستگاه قربانی جدید رجیستر شده‌است.



شکل ۳ نویسنده HeroRat نصب RAT بر روی دستگاه خود نشان داده‌است (تصاویری از یک ویدیو آموزشی ارائه شده توسط نویسنده بدافزار)

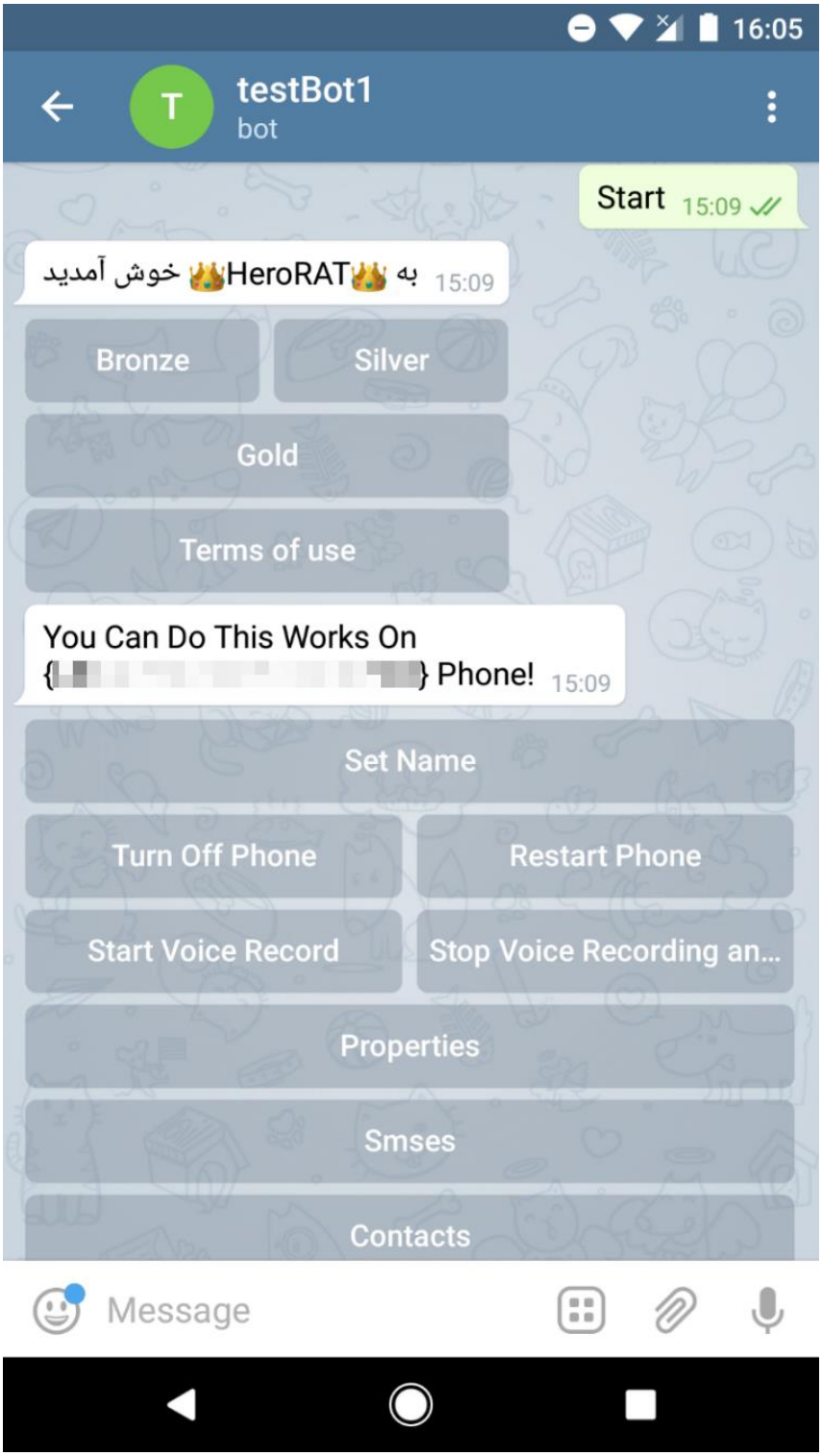
```
inf.Values.sharep.Edit().PutBoolean("ftr", false).Commit();
string[] array = new string[]
{
    "This Application Can't Run On Your Device",
    "Uninstalling...",
    "Uninstall finished"
};
if (!Locale.get_Default().get_Language().Equals("en"))
{
    array[0] = "این نرم افزار قادر به اجرا بر دستگاه شما نمیباشد";
    array[1] = "درحال حذف نصب";
    array[2] = "حذف نصب پایان یافت";
}
Toast.MakeText(this, array[0], 1).Show();
Toast.MakeText(this, array[1], 1).Show();
Toast.MakeText(this, array[2], 1).Show();
```

شکل ۴ سورس کد بدافزاری با پیام‌های پاک‌سازی جعلی در زبان انگلیسی و فارسی

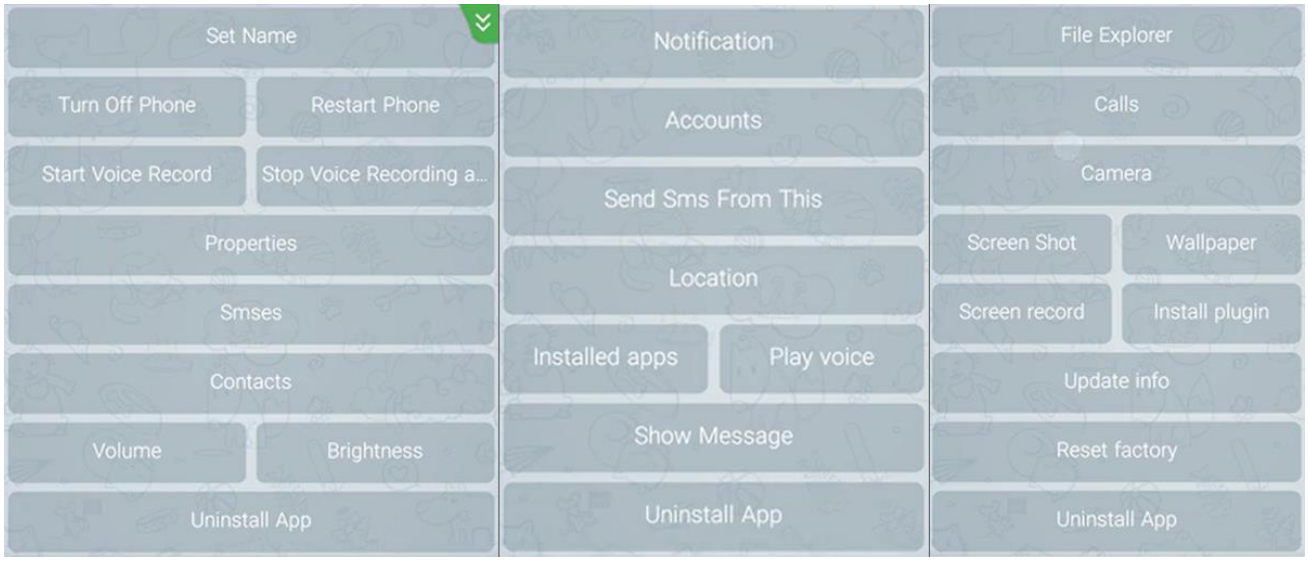
پس از دسترسی به دستگاه قربانی، مهاجم از قابلیت بات تلگرام برای کنترل لیست دستگاه‌های تازه وارد استفاده می‌کند. هر دستگاه آسیب‌دیده توسط یک ربات کنترل می شود که توسط مهاجم با استفاده از برنامه Telegram راه اندازی و اجرا شده‌است. این بدافزار دارای مجموعه گسترده‌ای از قابلیت های جاسوسی و سرقت فایل است از جمله قطع کردن پیام‌های متنی و مخاطبین، ارسال پیام متنی، برقراری تماس، ضبط صوت و تصویر، بدست آوردن محل دستگاه و کنترل تنظیمات دستگاه است. قابلیت HeroRat به سه دسته طلایی، نقره‌ای و برنزی تقسیم می‌شود که به

ترتیب برای فروش با قیمت ۲۵، ۵۰ و ۱۰۰ دلار عرضه شده‌اند. سورس کد آن هم با قیمت ۶۵۰ دلار توسط نویسنده RAT عرضه شده‌است.

قابلیت‌های بدافزار در قالب دکمه‌های قابل‌کلیک در رابط ربات تلگرام در دسترس هستند. مهاجمان می‌توانند با استفاده از دکمه‌های موجود در نسخه نرم‌افزارهای مخرب که در حال کار هستند، دستگاه های قربانی را کنترل کنند.



شکل ۵ پنل کنترلی HeroRat



شکل ۶ قابلیت HeroRat – از چپ به راست، "پنل برنز"، "پنل نقره‌ای" و "پنل طلایی" (تصاویری از یک ویدیو آموزشی ارائه شده از نویسنده بدافزار)

بر خلاف Android RAT های مورد استفاده در تلگرام که قبلا تجزیه و تحلیل شده‌اند و در استاندارد اندروید جاوا نوشته شده‌اند، این خانواده تازه کشف شده از تروجان در C# با استفاده از چارچوب Xamarin (یک ترکیب نادر برای نرم افزارهای مخرب آندروید) نوشته شده‌است.

این بدافزار از طریق پروتکل تلگرام که با زبان برنامه‌نویسی خود سازگار شده، ارتباط برقرار می‌کند. برخلاف Telegram Bot API استفاده شده توسط RAT که قبلا توضیح داده شده، این خانواده بدافزار از Telesharp یک کتابخانه برای ایجاد بات‌های تلگرام با استفاده از C# استفاده می‌کند.

دستورات ارتباطی برای سرقت اطلاعات از دستگاه‌های آسیب‌دیده هر دو به طور کامل از طریق پروتکل Telegram به کار گرفته می‌شوند (این اقدام به منظور جلوگیری از تشخیص آن بر اساس ترافیک به سرورهای آپلود معروف انجام می‌گیرد).

چگونه در امان بمانیم

با استفاده از سورس کد که اخیرا در دسترس قرار گرفته است، تحولات جدیدی می‌توانند در هر نقطه از جهان توسعه یافته و مستقر شوند. از آنجا که روش توزیع و شکل پنهان‌شدن این نرم‌افزارهای مخرب بر حسب مورد متفاوت است، بررسی دستگاه شما برای حضور هر برنامه خاص به اندازه کافی برای تشخیص اینکه آیا دستگاه شما به خطر افتاده است، کافی نیست. اگر دلیلی وجود دارد که اعتقاد دارید که دستگاه شما توسط این بدافزار به خطر افتاده است، آن را با استفاده از راه حل امنیتی قابل اعتماد تلفن همراه (مانند آنتی ویروس ESET) اسکن کنید. سیستم‌های ESET این تهدید را به عنوان Android / Spy.Agent.AMS و Android / Agent.AQO شناسایی و مسدود می‌کنند.

برای جلوگیری از قربانی شدن در برابر این بدافزار قبل از دانلود هر برنامه حتما نظرات کاربران در رابطه با آن برنامه را مطالعه کنید. همچنین به مجوزهایی که برنامه از شما می‌خواهد قبل و بعد از نصب برنامه توجه داشته باشید.