جمعه 11 خرداد 1397 - 14:40

بد افزار HeroRat

کاربران ایرانی مراقب بدافزار HeroRat باشند

.

کاربران ایرانی مراقب بدافزار HeroRat باشند مهاجمان در حال بازاریابی و فروش جاسوس افزاری معروف به HeroRat هستند که با بهره گیری از قابلیت های پیام رسان Telegram قادر به سرقت اطلاعات از روی دستگاه های با سیستم عامل Android است. به گفته این محققان، HeroRat حداقل از آگوست سال گذشته میلادی در حال انتشار بوده است. اما در مارس 2018 کد منبع آن بر روی چند کانال هک Telegram، به صورت رایگان به اشتراک گذاشته شد. موضوعی که سبب ساخت صدها نسخه جدید از این بدافزار شده است. با این حال گردانندگان HeroRat همچنان در حال فروش این بدافزار در قالب سه مدل برنزی، نقره ای و طلایی به ترتیب با قیمت های 25، 50 و 100 دلار هستند. ضمن اینکه کد منبع آن را نیز – که به رایگان قابل دسترس است – به قیمت 650 دلار به فروش می رسانند. خریداران این بدافزار از طریق یک کانال ویدیویی قادر به دریافت خدمات پشتیبانی از گردانندگان هستند. این بدافزار از طریق بازارهای توزیع دیجیتال غیررسمی و شبکه های اجتماعی و با وعده عرضه رایگان بیت کوین، دسترسی رایگان به اینترنت یا فراهم کردن دنبال کنندگان بیشتر به طور گسترده ای در ایران در حال انتشار است. بدافزار HeroRat قابلیت اجرا شدن بر روی هر نسخه از سیستم عامل Android را داراست. با این حال نصب آن مستلزم تایید سطوح دسترسی درخواستی از سوی بدافزار توسط کاربر است. برای تشویق کاربر به موافقت با سطوح دستری درخواستی، مهاجمان از روش های مهندسی اجتماعی بهره گرفته اند. پس از نصب بدافزار، فعالیت های مخرب آن آغاز می شود. قربانی بلافاصله با پیامی روبرو می شود که در آن گفته شده که برنامک با دستگاه کاربر ناسازگار بوده و باید از روی دستگاه حذف شود. پیامی دروغین که صرفاً ترفندی برای متقاعد کردن کاربر به حذف شدن برنامک است. اما از این مرحله به بعد دستگاه قربانی در تسخیر مهاجمان قرار گرفته است. این بدافزار با فراهم آوردن یک صفحه کنترلی و با استفاده از قابلیت های Telegram، مهاجم را قادر به سرقت داده های ذخیره شده بر روی دستگاه آلوده و برقراری تماس، تصویربرداری و ضبط صدا از طریق دستگاه می کند.