بسمه تعالی

تکامل بدافزارهای موبایلی در سال ۲۰۱۹

گزارش فنی

فهرست مطالب

فهرست شکل‌ها

فهرست جداول

۱ مقدمه

امنیت تلفن همراه به‌طور فزاینده‌ای در مباحث موبایلی اهمیت پیدا کرده است. موبایل‌ها در بیشتر کاربران در کسب‌وکار نه تنها به‌عنوان ابزار ارتباطی، بلکه به‌عنوان ابزاری برای برنامه‌ریزی و مدیریت کارها استفاده می‌شوند. در شرکت‌ها، این فناوری باعث تغییرات عمیق در سازمان سیستم‌های اطلاعاتی شده و در نتیجه آن‌ها را تبدیل به منبع خطرات جدیدی کرده است.

گوشی‌های هوشمند کامپیوترهایی در مقیاس کوچک‌تر هستند. این دستگاه به حساب‌های مالی متصل بوده و به‌طور قطع در ضعیف‌ترین سطح حفاظت قرار دارد؛ که متأسفانه مجرمان سایبری از این مسئله سوءاستفاده می‌کنند. هنگامی که قابلیت دستگاه‌های تلفن همراه و خدمات آن پیشرفت می‌کنند، مجرمان سایبری را نیز به‌سوی پیشرفت بدافزارها سوق می‌دهند. از طرفی، پیشرفت‌های هوش‌مصنوعی و یادگیری‌ماشین طی چندسال اخیر، اگرچه موجب ارتقاء سطح امنیت سایبری خواهد شد اما در عین‌حال به مهاجمان نیز کمک خواهد کرد. برنامه‌های کاربردی موبایل به علت وجود آسیب‌پذیری، هدف هکرها هستند. هرگونه از این نواقص می‌توانند عواقب بسیار مشکل‌زا و وسیعی را برای شرکت‌ها و سازمان‌های مربوطه داشته باشند.

اخذ تصمیم‌های کلیدی در کسب‌وکار سازمان‌ها هر روز بیشتر و بیشتر متکی به داده‌ها می‌شود. همین مسئله انگیزه بیشتری به شیادان و خرابکاران اینترنتی خواهد داد تا با دسترسی به مجموعه‌های وسیع اطلاعات، داده‌ها را توسط باج‌افزارها[۱] دچار محدودیت کنند.

به طور کلی، در جمع بندی سال ۲۰۱۹ دو روند خاص به چشم می‌خورد:

- حملات به داده‌های شخصی کاربران مکرر اتفاق افتاد. این حملات بیشتر از طریق stalkerwareها، تبلیغ‌افزارها و سوءاستفاده از قابلیت دسترسی انجام شد.
- تشخیص تروجان‌ها در محبوب‌ترین فروشگاه‌های برنامه‌ها بیشتر شد. در سال ۲۰۱۹، نرم‌افزارهای مخربی در فروشگاه Google play یافت شد. مهاجمان با وارد کردن بدافزارها به این فروشگاه‌ها توانستند تاثیرات مخربی بر سیستم قربانیان اعمال کنند.

در این گزارش به بررسی انواع تهدیدات موبایلی اعم از بدافزارهای موبایل، تروجان‌های بانکی و تروجان‌های باج‌افزار موبایلی سال ۲۰۱۹ با استفاده از آمار و نمونه‌های آزمایشگاه Kaspersky می‌پردازیم.

---

[۱] این نوع تروجان‌ها اطلاعات موجود روی کامپیوتر را دست‌کاری کرده تا عملکرد سیستم دچار اختلال شود یا کاربران دیگر قادر به دسترسی به بخشی از اطلاعات خود نباشند. مهاجمان تنها زمانی اختلال سیستم را برطرف یا دسترسی به داده‌ها را آزاد می‌کنند که کاربران، باج طلب کرده آن‌ها را بپردازند.

۲ تهدیدات موبایلی

کاربران گوشی‌های هوشمند در معرض تهدیدهای مختلفی هستند. این تهدیدات می‌تواند استفاده از گوشی‌های هوشمند را مختل کرده و منجر به انتقال یا تغییر اطلاعات شود. علاوه بر این، از آنجا که برخی از برنامه‌ها می‌تواند حاوی بدافزار باشند، عملکرد و فعالیت‌های آن نرم‌افزار باید محدود شود (برای مثال، مسدود کردن دسترسی به محل ذخیره آدرس‌های کاربر، پیشگیری از انتقال داده‌ها در شبکه و ...).

حملات به دستگاه‌های موبایل با سه هدف عمده انجام می‌شوند:

- اطلاعات: گوشی‌های هوشمند دستگاه‌هایی برای مدیریت داده‌ها هستند؛ بنابراین داده‌های آن‌ها ممکن است داده‌هایی حساس مانند شماره کارت اعتباری، اطلاعات سیستم، اطلاعات خصوصی و logهای سیستم باشند که بسیار در معرض خطر هستند.
- هویت: گوشی‌های هوشمند به‌آسانی قابل تنظیم می‌باشند؛ به طوری که دستگاه یا محتویات آن با صاحب دستگاه در ارتباط است و هویت آن شخص را به‌عنوان صاحب دستگاه شناسایی می‌کند. به‌عنوان مثال، هر دستگاه تلفن همراه می‌تواند اطلاعات مربوط به صاحب خود را با توجه به دسترسی به آن انتقال دهد و مهاجمان می‌توانند این اطلاعات را به‌آسانی به سرقت برده و از اطلاعات شخصی صاحب خط استفاده کنند. درنهایت شخص صاحب دستگاه به عنوان مجرم شناسایی می‌شود.
- دسترسی: با حمله به یک گوشی هوشمند می‌توان دسترسی به آن را محدود کرد و کاربر را از استفاده خدمات از تلفن همراه هوشمند خود محروم کرد.

۳ حملات به داده‌های شخصی

۳-۱ stalkerwareها

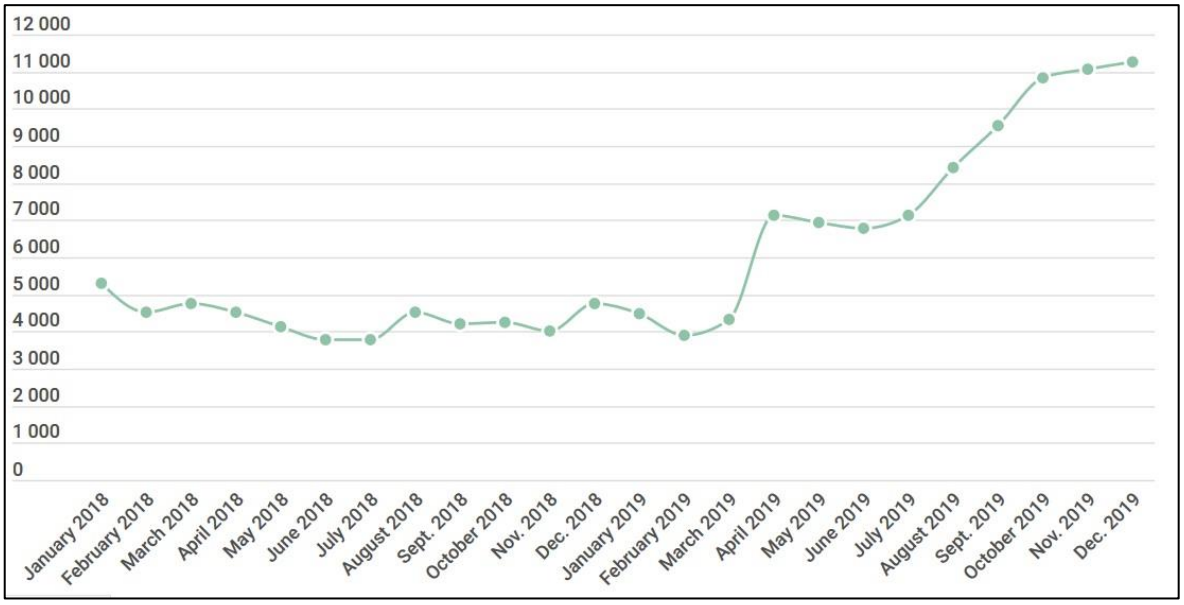
بدافزار stalkerware یکی از نرم‌افزارهای جاسوسی[۲] است که برای جاسوسی اطلاعات کودکان، همکاران یا بستگان استفاده می‌شود. این برنامه‌ها که به عنوان ابزار کنترلی والدین[۳] تبلیغ می‌شوند، دامنه کاربردهای

[۲] ماموریت این برنامه‌ها جاسوسی نحوه کاربری افراد است. برای مثال Trojan-Spy از فعالیت‌های کاربران در کامپیوتر یا اینترنت اسکرین‌شات می‌گیرد، فهرستی از برنامه‌های درحال اجرا روی سیستم تهیه می‌کند و یا تمام اطلاعاتی را که کاربران از طریق صفحه‌کلید وارد می‌کنند به ثبت می‌رساند.

[۳] parental control tools

گسترده‌تری دارند. بدافزارهای stalkerware بدون مجوز کاربر نصب می‌شوند تا مخفیانه داده‌های شخصی قربانی (تصاویر، ویدئوها، مکاتبات و داده‌های جغرافیایی) را به یک سرور فرمان ارسال کنند. این عمل باعث می‌شود داده‌های شخصی توسط اشخاص ثالث مانند توسعه‌دهندگان برنامه مورد سوءاستفاده قرار گیرد. بیشتر محصولات stalkerware رسماً با قوانین مطابقت دارند اما توزیع آن‌ها به خاطر عدم رعایت هنجارهای اخلاقی، از طریق کانال‌های قانونی مانند Google Play و App Store ممنوع است.

میزان حملات stalkerware بر داده‌های شخصی کاربران موبایلی تقریباً دو برابر شده است: از ۴۰,۳۸۶ کاربر منحصر به فرد در سال ۲۰۱۸ تا ۶۷,۵۰۰ در سال ۲۰۱۹. شکل شماره ۱ تعداد کاربران منحصر به فردی که در سال‌های ۲۰۱۸ و ۲۰۱۹ مورد حمله stalkerwareها قرار گرفته‌اند را نشان می‌دهد.



شکل شماره ۱: تعداد کاربران منحصر به فردی که در سال‌های ۲۰۱۹-۲۰۱۸ مورد حمله stalkerwareها قرار گرفته‌اند.

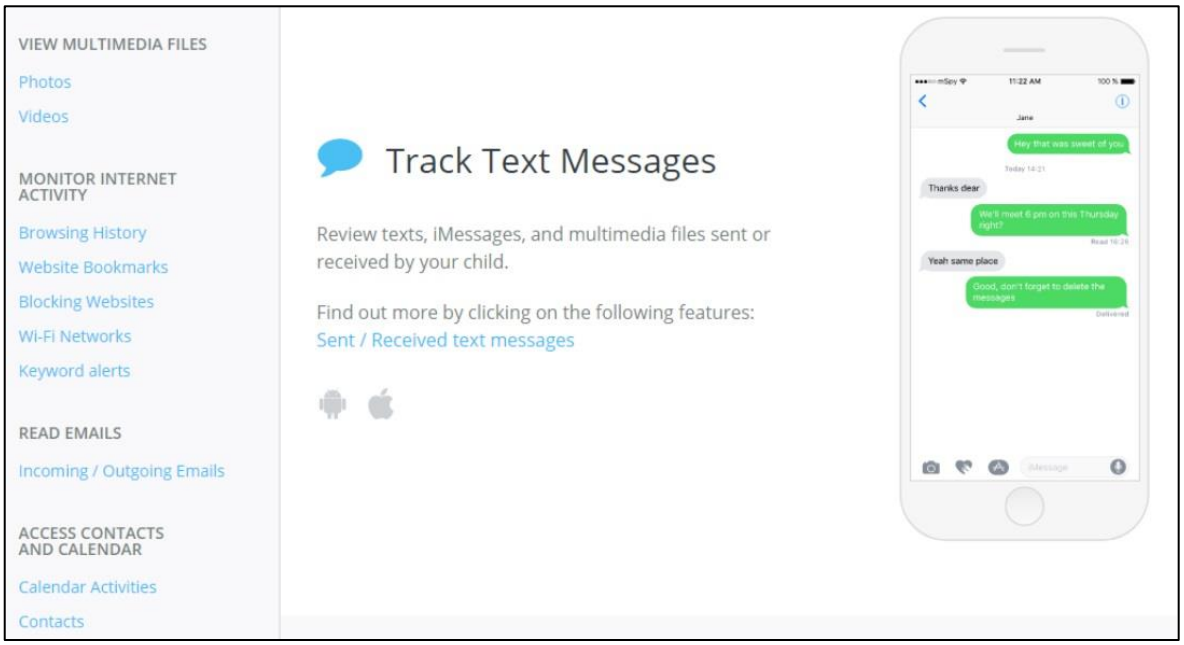
بدافزارهای Stalkerware می‌توانند به دو دسته اصلی تقسیم شوند:

- ردیاب‌ها
- برنامه‌های ردیابی تکامل‌یافته

سازنده‌های ردیاب‌ها بر دو ویژگی اصلی تمرکز دارند: ردیابی مختصات قربانی و شنود پیام‌های متنی. تا همین اواخر، بسیاری از این برنامه‌ها، در بازار رسمی Google Play اغلب به‌طور رایگان در دسترس بودند. پس از این که Google Play در سال ۲۰۱۸ سیاست‌های خود را تغییر داد، بیشتر آن‌ها از بازار حذف شدند و بیشتر توسعه‌دهندگان حمایت از محصولات خود را از دست دادند. با این حال چنین ردیاب‌هایی هنوز هم می‌توانند در سایت‌های توسعه‌دهنده و شخص ثالث آن‌ها یافت شوند.

پس از اجرای آن‌ها روی دستگاه قربانی، مهاجمان و برنامه‌های شخص ثالث می‌توانند به پیام‌ها و داده‌های مربوط به موقعیت مکانی کاربر دسترسی پیدا کنند. این برنامه‌های ثالث لزوماً فقط کاربر را ردیابی نمی‌کنند، تعاملات کلاینت-سرور در بعضی سرویس‌ها، حداقل الزامات امنیتی را نادیده گرفته و به همه افراد امکان می‌دهد به داده‌های انباشته شده دسترسی پیدا کنند.

وضعیت Stalkerwareهای تکامل‌یافته متفاوت است: چنین برنامه‌هایی در Google Play وجود ندارد، اما به طور فعال توسط توسعه‌دهندگان پشتیبانی می‌شوند. هدف آن‌ها عملکردی مانند برنامه‌های تجاری با قابلیت جاسوسی گسترده است. این برنامه‌ها می‌توانند تقریباً هر داده‌ای از دستگاه‌های در معرض خطر به دست آورند: تصاویر (کلیه تصاویر ذخیره شده و تصاویر شخصی، که به طور مثال در یک مکان خاص گرفته شده است)، تماس‌هاس تلفنی، پیام‌های متنی، اطلاعات موقعیت مکانی، کلیدهای فشرده شده (keylogging)[۴] و از این قبیل. شکل شماره ۲ تصویری از سایت یک توسعه‌دهنده نرم‌افزار stalkerware به همراه قابلیت‌های این نرم‌افزار را نشان می‌دهد.



شکل شماره ۲: تصویری از سایت یک توسعه‌دهنده نرم‌افزار stalkerware

[۴] یک نرم‌افزار یا سخت‌افزار است که کلیه کلیدهای فشرده شده توسط صفحه کلید را ثبت و ضبط می‌کند و بعضاً برای یک مهاجم یا مصارف دیگر ارسال می‌کند.

بسیاری از برنامه‌ها از دسترسی root برای استخراج تاریخچه پیام‌رسانی، از فضای ذخیره سازی محافظت شده و برنامه‌های پیام‌رسانی فوری، سوءاستفاده می‌کنند. اگر این مسئله نتواند دسترسی مورد نیاز را فراهم کند، stalkerware می‌تواند از صفحه عکس بگیرد، وارد کلیدهای فشرده شده شود و حتی متن پیام‌های ارسالی و دریافتی را از پنجره خدمات متداول[۵] با استفاده از ویژگی قابلیت دسترسی استخراج کند. به طور مثال برنامه جاسوسی تجاری Monitor Minor از این روش استفاده می‌کند. شکل شماره ۳ حاوی تصویری از برنامه جاسوسی تجاری Monitor Minor است که توانایی این نرم‌افزار را برای شنود داده‌ها از شبکه‌های اجتماعی و پیام‌رسان‌ها نشان می‌دهد.

شکل شماره ۳: تصویری از برنامه جاسوسی تجاری Monitor Minor

۳-۲ تبلیغ‌افزارها

تبلیغ‌افزار یا Adware مخفف Advertisement Software یا نرم‌افزار تبلیغاتی است. هر نرم‌افزار یا برنامه‌ای که از وجود تبلیغات در کنارش استفاده کند به عنوان تبلیغ‌افزار شناخته می‌شود. آن‌ها به اشکال مختلفی فعالیت می‌کنند؛ از صفحات Popup در مرورگرهای اینترنتی تا تبلیغاتی که در محیط یک نرم‌افزار یا هنگام نصب آن نمایش داده می‌شود.

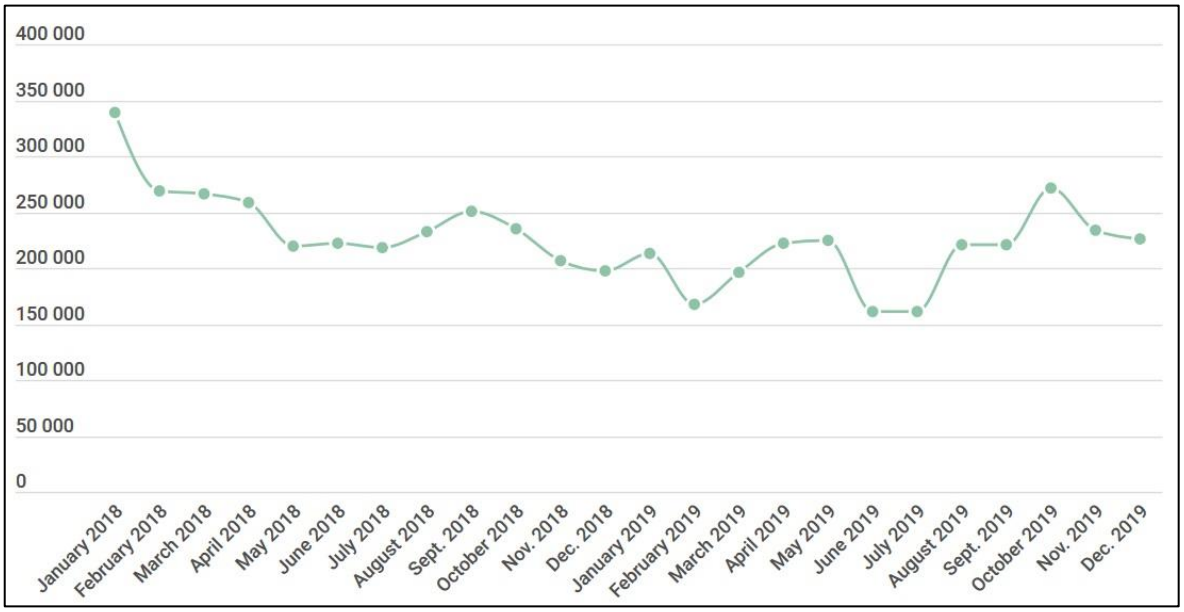
این برنامه‌ها به منظور اجرا و نمایش تبلیغات روی سیستم‌های آلوده و یا هدایت نتایج موتورهای جست‌وجو به وب‌سایت‌های تبلیغاتی طراحی شده‌اند. در بعضی مواقع تروجان‌ها مخفیانه تبلیغ‌افزارها را از یک وب‌سایت بارگیری کرده و در سیستم قربانی نصب می‌کند. از طرف دیگر، ابزارهای هکری که اغلب به عنوان Hijackers Browser نیز از آن یاد می‌شود، تبلیغ‌افزارها را با استفاده از آسیب‌پذیری مرورگر وب بارگیری می‌کنند.

عموماً تبلیغ‌افزار به هیچ وجه خودشان را در سیستم نشان نمی‌دهند. به علاوه آن‌ها به ندرت حاوی یک روش نصب مجدد هستند و تلاش برای حذف آن‌ها به طور دستی ممکن است منجر به نقص در برنامه اصلی شود.

---

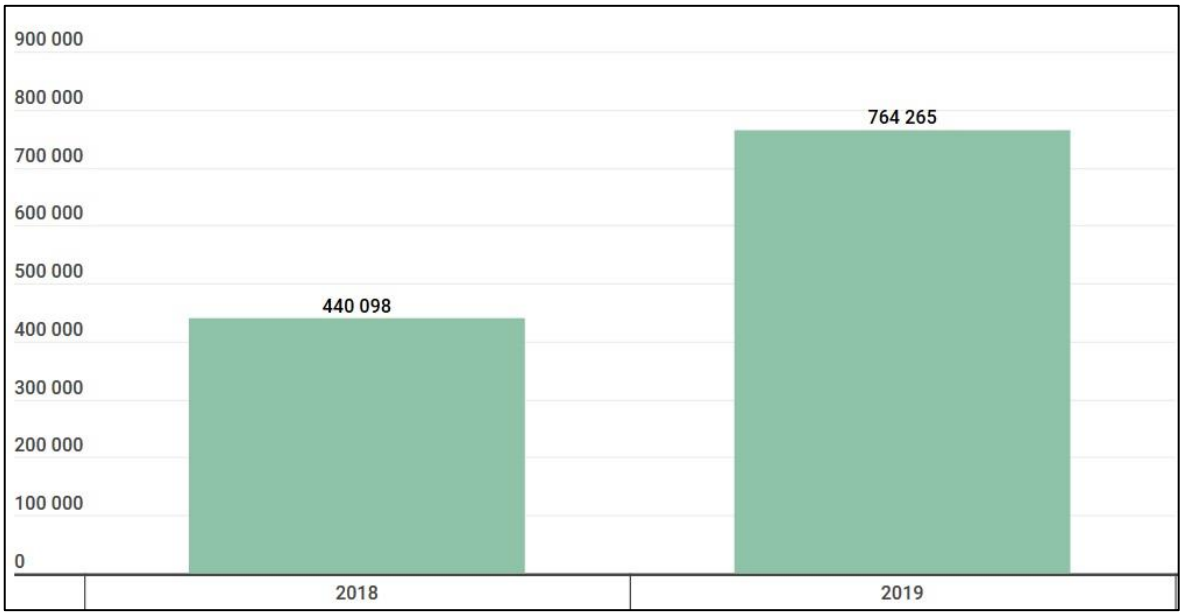
[۵] FAQ

در سال ۲۰۱۹ افزایش قابل توجهی در تعداد تهدیدات تبلیغ‌افزارها مشاهده شد،که هدف آن استخراج اطلاعات شخصی در دستگاه‌های موبایل بود. شکل شماره ۴ تعداد کاربرانی که تحت تأثیر این تهدید قرار گرفته‌اند را نشان می‌دهد.



شکل شماره ۴: تعداد کاربرانی که در سال‌های ۲۰۱۸ و ۲۰۱۹ مورد حمله تبلیغ‌افزار قرار گرفته‌اند.

همچنین، تعداد نصب تبلیغ‌افزار از سال ۲۰۱۸ تقریباً دو برابر شده است؛ در شکل شماره ۵ این تغییرات مشاهده می‌شود.



شکل شماره ۵: تعداد نصب تبلیغ‌افزار در سال‌های ۲۰۱۸ و ۲۰۱۹

این شاخص‌ها معمولا با یکدیگر ارتباط دارند، اما در مورد تبلیغ‌افزار این‌گونه نیست. این مسئله ممکن است دلایل متفاوتی داشته باشد:

- بسته‌های نصب تبلیغ‌افزار به‌طور خودکار تولید شده و تقریباً همه‌جا منتشر می‌شوند، اما به دلایلی به مخاطبان موردنظر نمی‌رسند؛ ممکن است بلافاصله بعد از تولید تشخیص داده شوند و پس از آن نتوانند منتشر شوند.
- اغلب این برنامه‌ها بخش مفیدی بجز یک ماژول تبلیغاتی ندارند؛ بنابراین قربانی بلافاصله آن‌ها را پاک می‌کند، با این فرض که آن‌ها اجازه دارند خود را از بین ببرند.

با این اوصاف، این دومین سال پیاپی است که تبلیغ‌افزارها به‌عنوان سومین تهدید برتر شناسایی شده‌اند. آمارهای KSN تایید می‌کنند که تبلیغ‌افزارها یکی از متداول‌ترین انواع تهدیدات می‌باشند: چهار جایگاه در تهدیدات برتر موبایلی بر اساس تعداد کاربرانی که در سال ۲۰۱۹ مورد حمله قرار گرفته‌اند، به کلاس‌های تبلیغ‌افزارها اختصاص داده شده‌اند که HiddenAd در آن‌ها دارای سومین جایگاه است. **Error! Reference source not found.** تعداد کاربرانی که در سال ۲۰۱۹ تحت تأثیر حمله تبلیغ‌افزارها قرار گرفته‌اند را نشان می‌دهد.

جدول شماره ۱ : تعداد کل کاربران مورد حمله این نوع بدافزار از تعداد کل کاربران تحت تأثیر حمله

ردیف	نام	میزان برحسب درصد
۱	DangerousObject.Multi.Generic	۳۵/۸۳
۲	Trojan.AndroidOS.Boogr.gsh	۸/۳۰
۳	AdWare.AndroidOS.HiddenAd.et	۴/۶۰
۴	AdWare.AndroidOS.Agent.f	۴/۰۵
۵	Trojan.AndroidOS.Hiddapp.ch	۳/۸۹
۶	DangerousObject.AndroidOS.GenericML	۳/۸۵
۷	AdWare.AndroidOS.HiddenAd.fc	۳/۷۳
۸	Trojan.AndroidOS.Hiddapp.cr	۲/۴۹
۹	AdWare.AndroidOS.MobiDash.ap	۲/۴۲
۱۰	Trojan-Dropper.AndroidOS.Necro.n	۱/۸۴

در سال ۲۰۱۹ توسعه‌دهندگان تبلیغ‌افزار علاوه بر تولید هزاران بسته مخرب تبلیغ‌افزار، محصولات خود را با افزودن تکنیک‌هایی به‌منظور دور زدن محدودیت‌های سیستم‌عامل بهبود بخشیده‌اند.

به عنوان مثال، اندروید به دلیل صرفه‌جویی در باتری محدودیت‌های خاصی را در پس زمینه عملکرد برنامه‌ها اعمال می‌کند. این مسئله روی عملکرد تهدیدات مختلف مانند تبلیغ‌افزار که در پس زمینه منتظر فرصت‌هایی مانند یک پیام از سرور فرمان و کنترل هستند، تأثیرهای منفی خواهد گذاشت. اعمال چنین محدودیت‌هایی، نمایش تبلیغات خارج از پنجره برنامه را برای تبلیغ‌افزارها غیرممکن می‌کند.

به طور مثال خانواده تبلیغ‌افزار KeepMusic راه‌حل هوشمندانه‌ای برای دور زدن این محدودیت پیدا کردند. نرم‌افزار آن‌ها، مجوزهایی مانند بدافزار درخواست نمی‌کند؛ به جای آن برنامه یک فایل MP3 که فاقد صوت است را پشت سر هم اجرا می‌کند. سیستم‌عامل تصور می‌کند که پخش‌کننده موزیک در حال اجراست، پس فرآیند پس‌زمینه KeepMusic را متوقف نمی‌کند. بنابراین این بدافزار می‌تواند درخواستی به سرور داده و آن را هر زمانی نمایش دهد.

۳-۳ سوءاستفاده از قابلیت دسترسی

در سال ۲۰۱۹ اولین نمونه از بدافزارهای مالی موبایل که دارای استقلال پیشرفته بودند، مشاهده شد (Trojan-Banker.AndroidOS.Gustuff.a). تا آن زمان از دو روش زیر برای سرقت از حساب‌های بانکی کاربران استفاده می‌شد:

- از طریق پیام کوتاه بانکی درسمت قربانی:

این روش یک سرقت مستقل است که تنها اطلاعاتی در مورد گیرنده تراکنش لازم دارد؛ این داده‌ها می‌توانند در بدنه (کد) یک ربات ذخیره شده و یا به‌عنوان فرمان، از سرور فرمان و کنترل دریافت شوند. تروجان دستگاه را آلوده کرده و یک پیام متنی حاوی درخواست انتقال با شماره تلفن ویژه‌ی بانکی ارسال می‌کند. سپس بانک به طور خودکار وجوه را از حساب دارنده دستگاه به گیرنده منتقل می‌کند. با توجه به افزایش این سرقت‌ها، محدودیت‌های مربوط به نقل و انتقالات تلفن همراه سخت‌تر شده است، بنابراین این عامل حمله از خود نسخه پشتیبان تهیه می‌کند.

- با سرقت اعتبار بانکی آنلاین:

در سال‌های اخیر بیشتر از این روش استفاده شده است. مجرمان سایبری یک پنجره فیشینگ روی سیستم قربانی نمایش می‌دهند که صفحه ورود به بانک را شبیه‌سازی کرده و خود را به جای آن جا می‌زند و به مدارک معتبر قربانی دسترسی پیدا می‌کند. در این موارد مجرمان باید با استفاده از برنامه‌ای در موبایل یا مرورگر خود، تراکنش را انجام دهند. ممکن است سیستم ضد کلاه‌برداری بانکی فعالیت غیرطبیعی‌ای را تشخیص داده و آن را مسدود کند؛ بنابراین حتی اگر دستگاه آلوده شده باشد، مهاجمان ناموفق خواهند بود.

در سال ۲۰۱۹ مهاجمان روش سومی را ایجاد کردند: سرقت با دست‌کاری برنامه‌های بانکی. در ابتدا قربانی متقاعد می‌شود که برنامه را اجرا و وارد حساب خود شود. سپس یک اعلان جعلی که ظاهراً از طرف بانک است، به سیستم قربانی فرستاده می‌شود. قربانی با ضربه زدن روی اعلان، وارد برنامه بانکی می‌شود، سپس مهاجم با استفاده از قابلیت دسترسی کنترل کامل را به‌دست گرفته و می‌توانند باعث فشردن کلیدها، پر کردن فرم‌ها و غیره شود. علاوه بر این اپراتور ربات نیازی به انجام کاری ندارد زیرا بدافزار کلیه اقدامات

موردنیاز را انجام می‌دهد. این تراکنش‌ها توسط بانک‌ها تایید شده هستند و حداکثر مبلغ تراکنش‌ها می‌تواند از حد مجاز تراکنش‌های بانکی تجاوز کند. درنتیجه مهاجمان می‌توانند از این طریق حساب‌ها را خالی کنند.

سرقت از حساب‌های بانکی تنها یکی از سوءاستفاده‌ها از قابلیت دسترسی است. درواقع هر بدافزاری با این مجوزها می‌تواند فرآیندهایی که در حال حاضر روی صفحه در حال اجرا هستند را کنترل کند، زیرا هر برنامه اندرویدی اساساً نمایانگر دکمه‌ها، فرم‌های ورود داده، نمایش اطلاعات و غیره است. پیاده‌سازی عناصر کنترلی توسعه‌دهندگان (مانند منوی کشویی که باید با سرعت مشخصی حرکت کند) نیز از دستورات قابلیت دسترسی استفاده می‌کند. بنابراین مجرمان سایبری می‌توانند آنچه خطرناک‌ترین کلاس‌های بدافزارهای تلفن همراه هستند، را ایجاد کنند: نرم‌افزارهای جاسوسی، تروجان‌های بانکی و تروجان‌های باج‌افزار.

سوءاستفاده از ویژگی‌های قابلیت دسترسی، تهدیدی جدی برای اطلاعات شخصی کاربران محسوب می‌شود. با این که قبلاً مجرمان سایبری مجبور بودند برای دزدی از اطلاعات شخصی، پنجره‌های فیشینگ را بپوشانند و درخواست مجوز دیگری از آن‌ها را بدهند، اکنون قربانیان، کلیه داده‌های لازم را به صفحه‌نمایش می‌دهند یا آن را در فرم‌هایی وارد می‌کنند که می‌توان به‌راحتی از آن خارج شد و در صورت نیاز به بدافزارها، می‌توانند بخش تنظیمات را به‌تنهایی باز کند، روی چند دکمه ضربه زده و مجوزهای لازم را به‌دست آورند.

۴ تروجان‌های موبایلی در مشهورترین فروشگاه‌های اندرویدی: Google Play

یکی از توصیه‌های کارشناسان امنیتی عدم استفاده از برنامه‌های فروشگاه‌های غیررسمی است. درواقع این کار هم نمی‌تواند محافظت صد درصد از دستگاه کاربران را فراهم آورد. باوجود تمام تلاش‌های محافظتی گوگل، همچنان نرم‌افزارهای مخرب در Play Store آن یافت می‌شود.

وارد کردن بدافزار به فروشگاه اصلی اندروید، نتایج بسیار بهتری از مهندسی اجتماعی را برای نصب برنامه از منابع شخص ثالث ارائه می‌دهد. علاوه بر این، این رویکرد به مهاجمین امکان می‌دهد اعمال زیر را انجام دهند:

- دور زدن امنیت شبکه و محافظت آنتی‌ویروس داخلی اندروید. اگر کاربر برنامه‌ای را از Google Play بارگیری کند، احتمال نصب آن بدون درخواست اضافی بسیار بالاست (به‌طور مثال برای غیرفعال کردن محافظت داخلی به بهانه فرضی). تنها چیزی که می‌تواند در آن شرایط کاربر را از آلودگی محافظت کند، یک راه‌حل امنیتی شخص ثالث است.

- غلبه بر موانع روانشناسی. فروشگاه‌های برنامه رسمی از اعتماد بسیار بیشتری نسبت به فروشگاه‌های شخص ثالث برخوردار هستند و مانند انواع فروشگاه‌های ویندوزی عمل می‌کنند که می‌تواند برای توزیع نرم‌افزار بسیار کارآمدتر باشد.
- هدف گرفتن قربانیان بدون هزینه‌های غیرضروری. برنامه Google Play می‌تواند برای جعل میزبان‌هایی استفاده شود که از برنامه‌های بانکی محبوب تقلید می‌کنند. پس از آزمایش‌های انجام شده، تعداد زیادی از برنامه‌های مخرب در Google Play تحت پوشش برنامه‌های تلفن همراه در بانک‌های برزیل کشف شد.

علاوه بر این، مجرمان سایبری چندین ترفند دیگر را برای حداکثر رساندن میزان آلودگی دستگاه به کار بردند:

- نمونه CamScanner[۶] نشان داد رفتار مجاز برنامه می‌تواند مکمل عملیات مخرب، توسط به‌روزرسانی کد خود برای مدیریت تبلیغات باشد. این مسئله می‌تواند به‌عنوان پیشرفته‌ترین عامل حمله معرفی شود و موفقیت آن وابسته به عوامل زیادی است، از جمله منبع برنامه میزبان کاربر، اعتماد توسعه‌دهندگان در کد تبلیغاتی شخص ثالث و نوع فعالیت مخرب.
- نمونه دیگر[۷] نشان می‌دهد که مهاجمان گاهی اوقات برنامه‌های نسبتاً مطلوبی را از دسته‌های محبوب کاربران در Google Play بارگذاری می‌کنند. مانند برنامه‌های ویرایش تصاویر.
- سومین نمونه یک تروجان از خانواده Joker است که نمونه‌های زیادی از آن در Google Play یافت شده و همچنان موجود است. با استفاده از تاکتیک ارسال گسترده، مهاجمان برنامه‌های مخرب را با عناوین مختلفی جا زده و آن‌ها را بارگذاری می‌کنند: از ابزارهای تعویض پس‌زمینه و راه‌حل‌های امنیتی تا بازی‌های محبوب. در بسیاری از نمونه‌ها تروجان صدها هزار بار بارگیری می‌شود. هیچ عامل حمله دیگری در این بازه زمانی کوتاه به این میزان مخاطب نخواهد رسید.

شرکت گوگل و صنعت آنتی ویروس برای مقابله با تهدیدات در سایت همکاری کرده‌اند. هدف این رویکرد جلوگیری از نفوذ بیشتر بدافزارها به فروشگاه رسمی Google Play می‌باشد.

---

[۶] این برنامه برای اسکن و مدیریت اسناد دیجیتالی استفاده می‌شود، اما بررسی‌های منفی اخیر کاربران، حاکی از وجود ویژگی‌های ناخواسته بود. پس از تجزیه و تحلیل برنامه، یک کتابخانه تبلیغ‌افزار در آن یافت شد که حاوی یک جزء Dropper مخرب است، این عنصر مخرب به عنوان Trojan-Dropper.AndroidOS.Necro.n تشخیص داده شد.

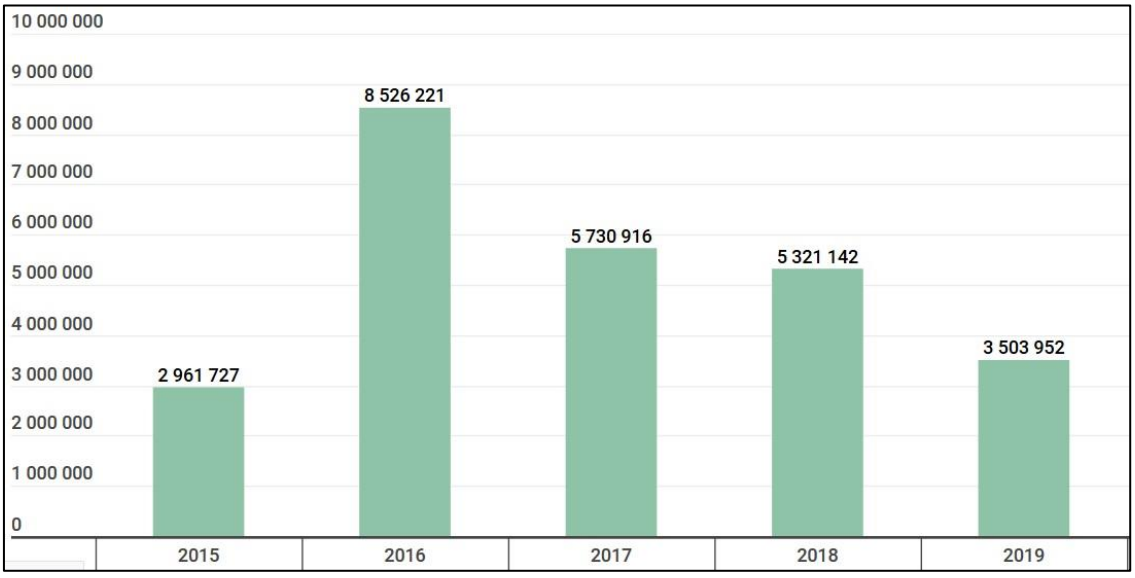
[۷] بعضی از برنامه‌های ویرایشگر تصاویر از قابلیت دسترسی سوءاستفاده می‌کنند. این برنامه‌ها دسترسی به کنترل‌های Wi-Fi را درخواست می‌کنند، که برای این نوع نرم‌افزارها بسیار غیرمعمول است، یا در هنگام اجرا، درخواست دسترسی به اعلان‌ها را دارند. سپس، در حالی که کاربر در تلاش است تا یک تصویر را (با استفاده از ابزارهای ناچیز) ویرایش کند، برنامه اطلاعات موجود در پس‌زمینه دستگاه را جمع آوری کرده و آن را به سرور ps.okyesmobi[.]com ارسال می‌کند.

۵ داده‌های آماری

در سال ۲۰۱۹ محصولات و تکنولوژی‌های موبایلی Kaspersky آمار زیر را گزارش کرده‌اند:

- ۳,۵۰۳,۹۵۲ بسته‌های نصبی مخرب
- ۶۹,۷۷۷ تروجان بانکی موبایل جدید
- ۶۸,۳۶۲ تروجان باج‌افزار موبایلی جدید

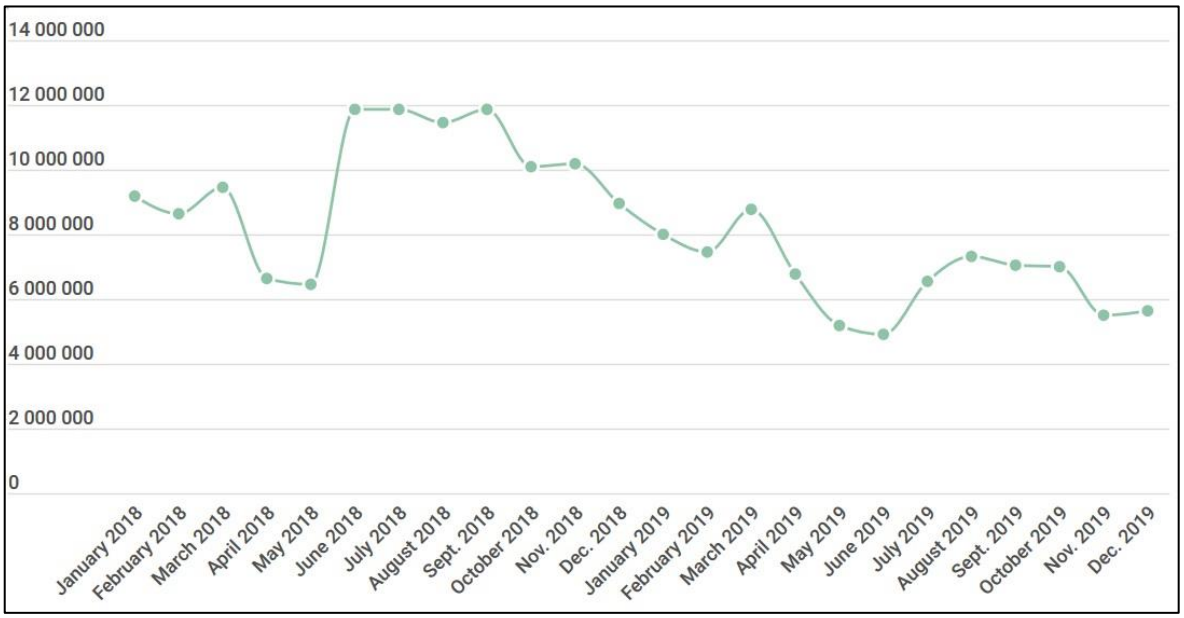
بسته‌های نصبی مخرب موبایل شناسایی شده، ۱,۸۱۷,۱۹۰ بسته کمتر از سال ۲۰۱۸ است. از سال ۲۰۱۵ تاکنون تهدیدات چندانی در زمینه موبایل تشخیص داده نشده است. شکل شماره ۶، تعداد بسته‌های نصبی موبایلی مخرب اندروید طی سال‌های ۲۰۱۹-۲۰۱۵ را نشان می‌دهد.



شکل شماره ۶: تعداد بسته‌های نصبی موبایلی مخرب اندروید در سال‌های ۲۰۱۹-۲۰۱۵

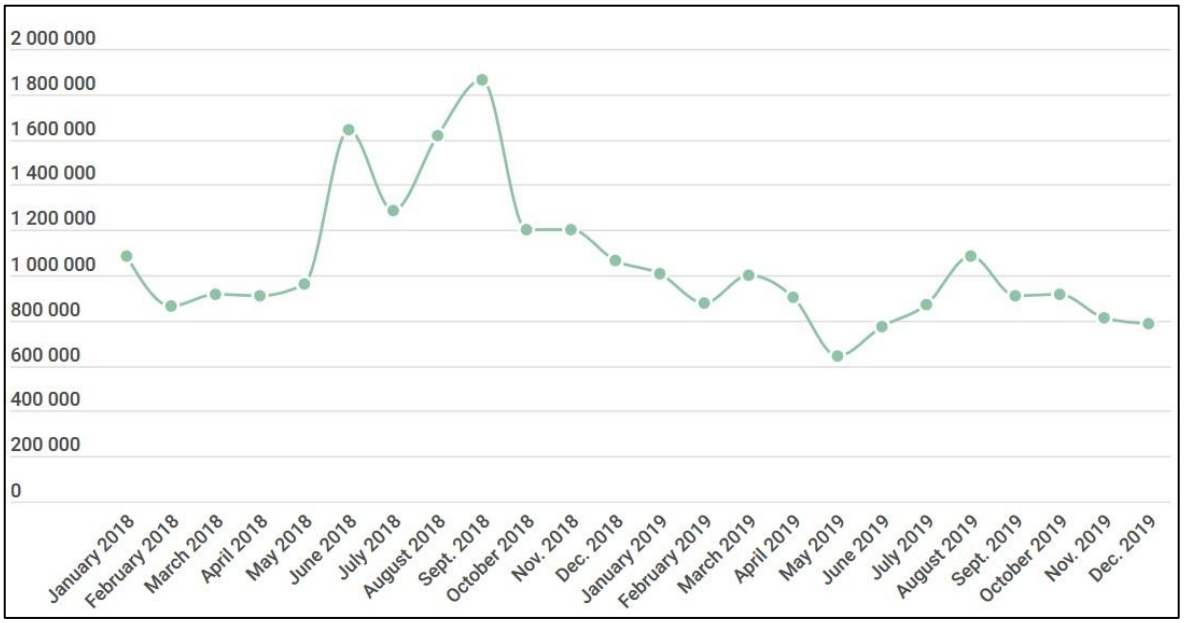
به مدت سه سال متوالی، تعداد تهدیدهای تلفن همراه توزیع‌شده با بسته‌های نصبی مخرب، کاهش کلی یافته است. این میزان تا حد زیادی وابسته به کمپین‌های خاص مجرمان سایبری است: برخی از این افراد کم‌کارتر شده‌اند، برخی دیگر کاملاً متوقف شده و مهاجمان جدید هنوز انگیزه لازم را کسب نکرده‌اند.

این وضعیت مشابه با تعداد حملات با استفاده از تهدیدات موبایلی است: که در سال ۲۰۱۸ تعداد ۱۱۶,۵ میلیون حمله و در سال ۲۰۱۹ این رقم به ۸۰ میلیون کاهش یافته است. در شکل شماره ۷ تعداد حملات ناموفق طی سال‌های ۲۰۱۸ و ۲۰۱۹ قابل مشاهده است.



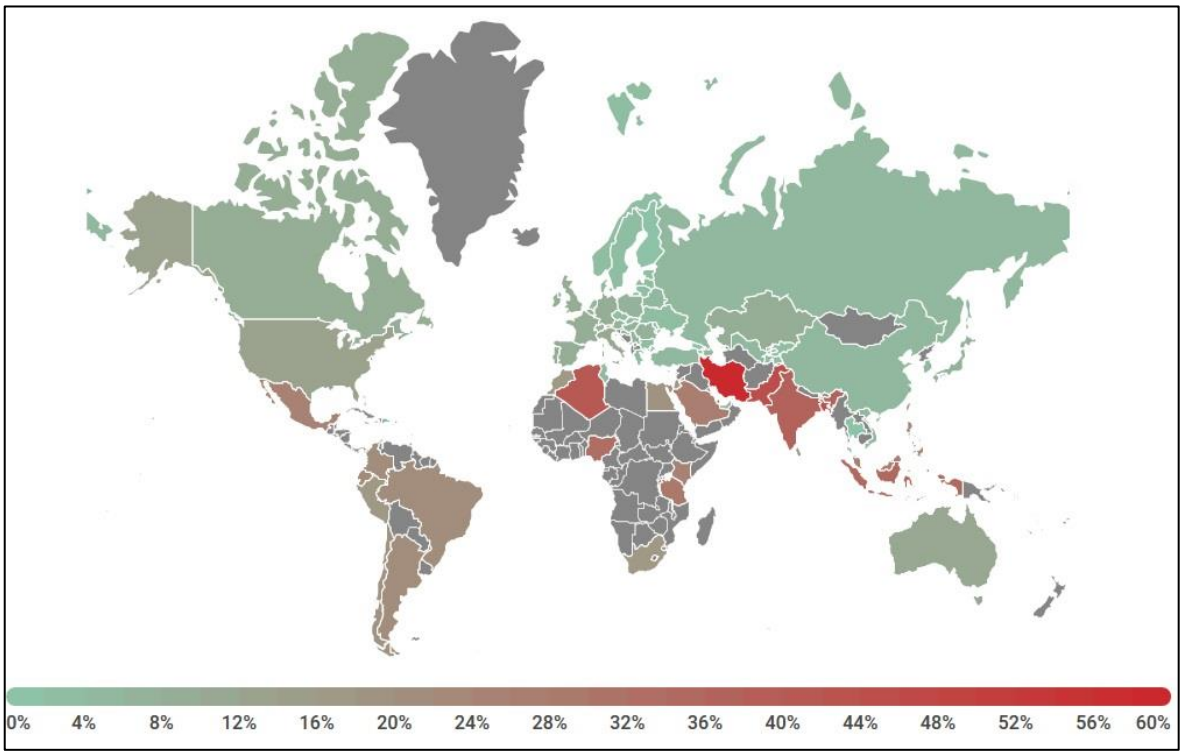
شکل شماره ۷: تعداد حملات ناموفق در سال ۲۰۱۹-۲۰۱۸

این ارقام به سال قبل از شروع تروجان بانکی همه‌گیر Asacub باز می‌گردد. از آنجا که تعداد حملات با تعداد کاربران مورد حمله ارتباط دارد، میزان کاربرانی که مورد حمله قرار گرفته‌اند مشابه با نمودار بالاست.



شکل شماره ۸ : تعداد کاربرانی که در سال ۲۰۱۹-۲۰۱۸ تحت تأثیر بدافزارهای موبایلی قرار گرفته‌اند.

در شکل شماره ۹، موقعیت مکانی کاربران تحت تأثیر حمله بدافزارهای موبایلی قابل مشاهده است.



شکل شماره ۹: موقعیت مکانی کاربران تحت تأثیر حمله در سال ۲۰۱۹

۱۰ کشور برتر با میزان کاربران تحت تأثیر حمله بدافزارهای تلفن همراه در **Error! Reference source not found.** نمایش داده شده‌اند. (کشورهایی که کمتر از ۲۵۰۰۰ کاربر فعال راه‌حل‌های امنیتی موبایل Kaspersky در دوره گزارش دارند از رتبه بندی خارج شده‌اند)

جدول شماره ۲ : میزان کاربران تحت تأثیر حمله بدافزارهای تلفن همراه

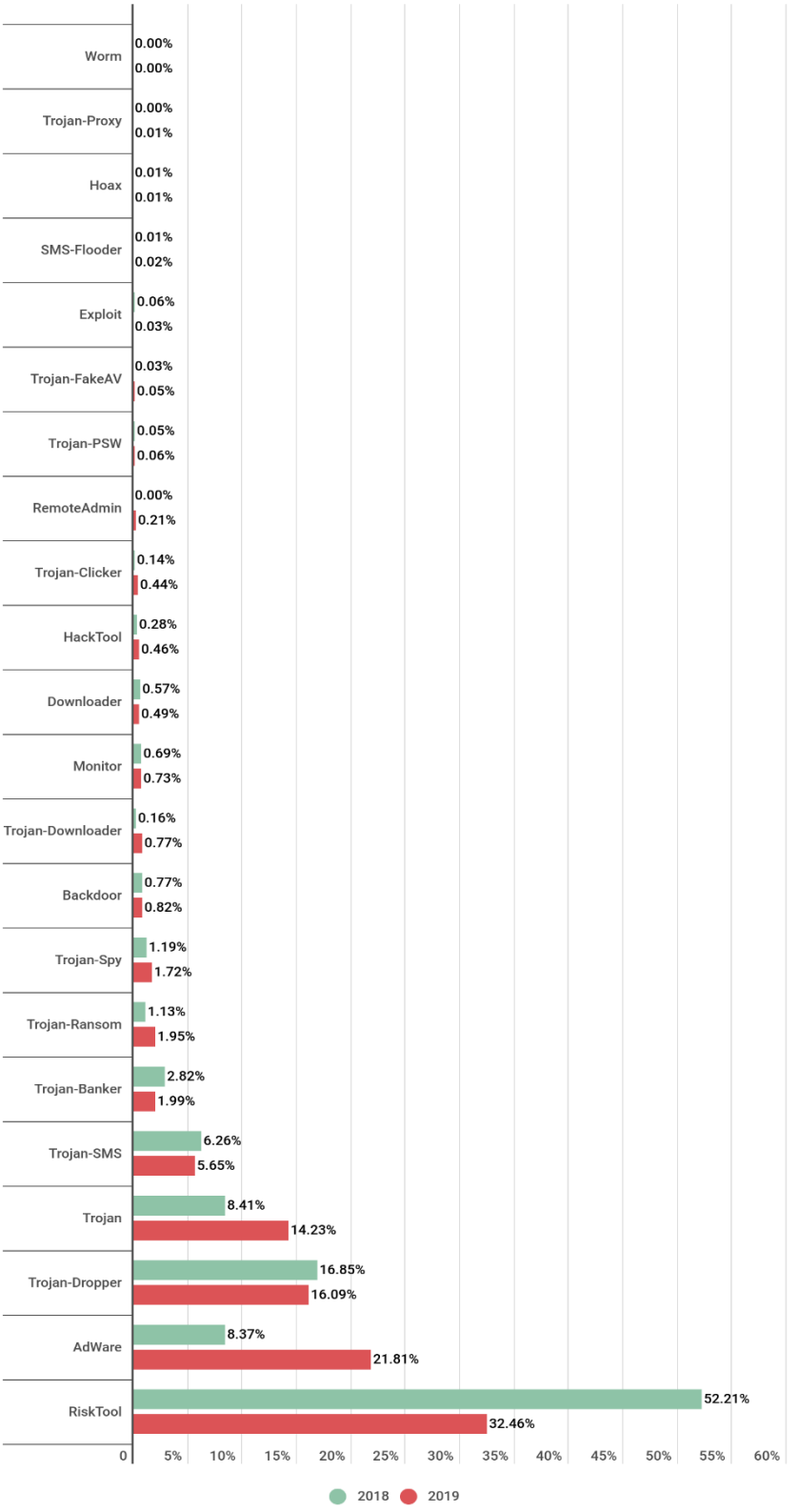
نام کشور	میزان برحسب درصد
ایران	۶۰.۶۴
پاکستان	۴۴.۴۳
بنگلادش	۴۳.۱۷
الجزایر	۴۰.۲۰
هند	۳۷.۹۸
اندونزی	۳۵.۱۲
نیجریه	۳۳.۱۶
تانزانیا	۲۸.۵۱
عربستان سعودی	۲۷.۹۴
مالزی	۲۷.۳۶

در سال ۲۰۱۹، ایران برای سومین سال متوالی در بالاترین جایگاه جدول قرار گرفت. عمده ترین تهدیدات در این کشور از طریق تبلیغ‌افزار و نرم‌افزارهای بالقوه ناخواسته ناشی می‌شود: Trojan.AndroidOS.Hiddapp.bn، AdWare.AndroidOS.Agent.fa و RiskTool.AndroidOS.Dnotua.yfe.

پاکستان با افزایش تعداد کاربرانی که توسط تبلیغ‌افزار مورد حمله قرار گرفته‌اند، از هفتمین جایگاه به دومین جایگاه تغییر پیدا کرد. بیشترین میزان با افزایش تعداد کاربران خانواده AdWare.AndroidOS.HiddenAd بوده است. بنگلادش نیز با افزایش استفاده از تبلیغ‌افزار رشد مشابهی داشته است.

۵-۱ انواع تهدیدات موبایلی

شکل شماره ۱۰ نشانگر توزیع تهدیدات موبایلی جدید طبق نوع در سال‌های ۲۰۱۸ و ۲۰۱۹ است.



شکل شماره ۱۰: توزیع تهدیدات موبایلی جدید طبق نوع در سال‌های ۲۰۱۸ و ۲۰۱۹

در سال ۲۰۱۹ میزان تهدیدات RiskTool[۸] به ٪۳۲.۴۶ کاهش یافته است؛ دلیل این کاهش ناگهانی می‌تواند خانواده تهدیدات SMSreg باشد. یک ویژگی مشخص این تهدیدات، پرداخت‌های از طریق پیام کوتاه است: به طور مثال انتقال وجه یا اشتراک در خدمات تلفن همراه. علاوه بر این کاربر صریحاً از پرداخت یا پولی که به حساب موبایل خود منتقل شده است، آگاه نیست. در سال ۲۰۱۸ تعداد ۱,۹۷۰,۷۴۲ نصب بسته‌ی SMSreg شناسایی شده و این تعداد در سال ۲۰۱۹ به میزان ۱۹۳,۰۴۳ کاهش یافته است. در عین حال، تعداد بسته‌های سایر اعضای این طبقه از تهدیدات به طرز چشمگیری افزایش یافت. در **Error! Reference source not found.** میزان بسته‌های این خانواده بدافزار از کل بسته‌های riskware تشخیص داده شده در سال ۲۰۱۹ برحسب درصد مشاهده می‌شود.

جدول شماره ۳: میزان بسته‌های این خانواده از کل بسته‌های riskware تشخیص داده شده در سال ۲۰۱۹

ردیف	نام خانواده	میزان بر حسب درصد
۱	Agent	۲۷.۴۸
۲	SMSreg	۱۶.۸۹
۳	Dnotua	۱۳.۸۳
۴	Wapron	۱۳.۷۳
۵	SmsSend	۹.۱۵
۶	Resharer	۴.۶۲
۷	SmsPay	۳.۵۵
۸	PornVideo	۲.۵۱
۹	Robtes	۱.۲۳
۱۰	Yoga	۱.۰۳

تهدیدات Skymobi و Paccy از بین ۱۰ خانواده برتر نرم‌افزارهای ناخواسته بالقوه حذف شدند؛ تعداد نصب بسته‌های این خانواده‌ها در سال ۲۰۱۹، ده برابر کاهش یافت. سازندگان آن‌ها احتمالاً توسعه و توزیع خود را به حداقل رسانده یا حتی متوقف کرده‌اند. با این حال خانواده Resharer (٪۴.۶۲) به رتبه ششم دست پیدا کرد. این خانواده، به انتشار خود از طریق ارسال اطلاعات در مورد خودش روی سایت‌های مختلف و ایمیل کردن آن‌ها به مخاطبان قربانی مشهور است.

[۸] این گروه از تهدیدات دارای چندین کارکرد هستند (مانند پنهان کردن پرونده‌ها در سیستم، مخفی کردن برنامه‌های در حال اجرا در ویندوز، خاتمه فرآیندهای فعال و غیره) که با هدف مخرب قابل استفاده هستند. آن‌ها به خودی خود مخرب نیستند. این برنامه‌ها برای کار بر روی رایانه محلی طراحی شده‌اند. اگر برنامه توسط کاربر یا مدیر سیستم نصب شده باشد، خطری ندارد.

تبلیغ‌افزارها چشمگیرترین رشد را داشته‌اند. منبع این افزایش، به علت HiddenAd (۲۶.۸۱٪) بوده است؛ تعداد نصب بسته‌های این خانواده نسبت به سال ۲۰۱۸ دو برابر شده است. **Error! Reference source not found.** میزان بسته‌های خانواده‌های مختلف تبلیغ‌افزار را نشان می‌دهد.

جدول شماره ۴: میزان بسته‌های این خانواده‌های تبلیغ‌افزار از کل بسته‌های تبلیغ‌افزار تشخیص داده شده در سال ۲۰۱۹

ردیف	نام خانواده	میزان برحسب درصد
۱	HiddenAd	۲۶.۸۱
۲	MobiDash	۲۰.۴۵
۳	Ewind	۱۶.۳۴
۴	Agent	۱۵.۲۷
۵	Dnotua	۵.۵۱
۶	Kuguo	۱.۳۶
۷	Dowgin	۱.۲۸
۸	Triada	۱.۲۰
۹	Feiad	۱.۰۱
۱۰	Frupi	۰.۹۴

رشد چشمگیری نیز در خانواده‌های MobiDash (۲۰.۴۵٪) و Ewind (۱۶.۳۴٪) مشاهده شد، همچنین خانواده Agent (۱۵.۲۷٪) که در سال ۲۰۱۸ در صدر جدول بود، به چهارمین جایگاه تنزل پیدا کرد.

در مقایسه با سال ۲۰۱۸، تعداد تهدیدات تشخیص داده شده کاهش چشمگیری پیدا کرد. یک روند نزولی برای دو سال متوالی مشاهده شده است، با این حال dropperها[۹] یکی از بی شمارترین کلاس‌های بدافزار هستند. خانواده Hqwar بیشترین میزان کاهش را داشته است: از میزان ۱۴۱,۰۰۰ بسته در سال ۲۰۱۸ به میزان ۲۲,۰۰۰ در سال ۲۰۱۹. در همان زمان، سال ۲۰۱۹ شاهد حضور خانواده Ingopack بود: ۱۱۵۶۵۴ نمونه از این dropper کشف شد.

ضمناً میزان تهدیدات تروجان توسط دو خانواده مخرب متعدد Boogr و Hiddapp افزایش یافته است. خانواده Boogr حاوی تروجان‌های متعددی است که با استفاده از تکنولوژی یادگیری ماشین (ML) کشف شده‌اند. یک ویژگی خانواده Hiddapp این است که نماد[۱۰] خود را در لیست برنامه‌های نصب شده مخفی می‌کند در حالی که در پس زمینه در حال اجراست. میزان تروجان‌های باج‌افزار موبایلی اندکی افزایش یافته

[۹] هکرها با استفاده از این تروجان‌ها می‌توانند تروجان‌ها و ویروس‌ها را روی سیستم‌های هدف نصب، یا از شناسایی بدافزارها پیش‌گیری کنند. برخی از نرم‌افزارهای ضدویروس قادر به اسکن تمام اجزای این تروجان‌ها نیستند.

[۱۰] Icon

است. سه خانواده برتر این کلاس تهدیدات همانند سال ۲۰۱۸ به ترتیب مقابل می‌باشد: Svpeng، Congur و Fusob.

۵-۲ بیست برنامه برتر بدافزار موبایل

Error! Reference source not found. میزان کل کاربران تحت تأثیر بدافزارهای موبایل را نشان می‌دهد. رتبه‌بندی بدافزارهای زیر شامل نرم‌افزارهای بالقوه ناخواسته مانند RiskTool و تبلیغ‌افزار نمی‌شود:

جدول شماره ۵ : میزان کل کاربران تحت تأثیر این حملات از تعداد کل کاربران تحت تأثیر حمله

ردیف	نام	میزان برحسب درصد
۱	DangerousObject.Multi.Generic	۴۹.۱۵
۲	Trojan.AndroidOS.Boogr.gsh	۱۰.۹۵
۳	Trojan.AndroidOS.Hiddapp.ch	۵.۱۹
۴	DangerousObject.AndroidOS.GenericML	۵.۰۸
۵	Trojan-Dropper.AndroidOS.Necro.n	۳.۴۵
۶	Trojan.AndroidOS.Hiddapp.cr	۳.۲۸
۷	Trojan-Banker.AndroidOS.Asacub.snt	۲.۳۵
۸	Trojan-Dropper.AndroidOS.Hqwar.bb	۲.۱۰
۹	Trojan-Dropper.AndroidOS.Lezok.p	۱.۷۶
۱۰	Trojan-Banker.AndroidOS.Asacub.a	۱.۶۶
۱۱	Trojan-Downloader.AndroidOS.Helper.a	۱.۶۵
۱۲	Trojan-Banker.AndroidOS.Svpeng.ak	۱.۶۰
۱۳	Trojan-Downloader.AndroidOS.Necro.b	۱.۵۹
۱۴	Trojan-Dropper.AndroidOS.Hqwar.gen	۱.۵۰
۱۵	Exploit.AndroidOS.Lotoor.be	۱.۴۶
۱۶	Trojan.AndroidOS.Hiddapp.cf	۱.۳۵
۱۷	Trojan.AndroidOS.Dvmap.a	۱.۳۳
۱۸	Trojan-Banker.AndroidOS.Agent.ep	۱.۳۱
۱۹	Trojan.AndroidOS.Agent.rt	۱.۲۸
۲۰	Trojan-Dropper.AndroidOS.Tiny.d	۱.۱۴

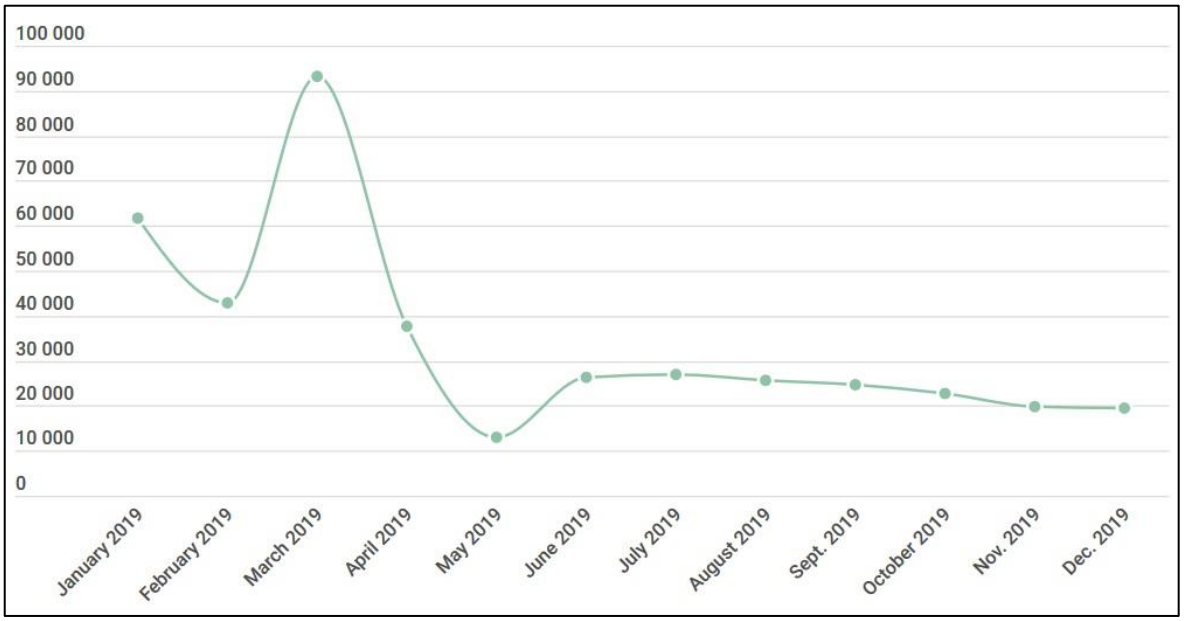
طبق جدول بالا، بیشترین میزان کاربران تحت تأثیر حمله متعلق به بدافزار DangerousObject.Multi.Generic (۴۹.۱۵٪) که از بدافزارهای شناخته شده در حوزه تکنولوژی فضای ابری است، می‌باشد. این بدافزار جدیدترین بدافزار کشف شده است؛ زیرا پایگاه‌داده‌های آنتی ویروس هنوز هیچ امضا یا ابتکاری برای تشخیص آن ندارند.

دومین جایگاه متعلق به Trojan.AndroidOS.Boogr.gsh (۱۰.۹۵٪) است که توسط سیستم‌های مبتنی بر یادگیری ماشین تشخیص داده شده است. تروجان DangerousObject.AndroidOS.GenericML (۵.۰۸٪، چهارمین جایگاه در رتبه‌بندی) مربوط به فایل‌هایی است ساختار آن‌ها با فایل‌های مخرب یکسان است.

جایگاه‌های سوم، ششم و شانزدهم مربوط به خانواده Hiddapp است که مربوط به برنامه‌هایی است که نماد خود را بلافاصله پس از شروع به کار در لیست برنامه‌ها پنهان می‌کند. عواقب بعدی چنین برنامه‌هایی ممکن است بارگیری یا نمایش تبلیغات در برنامه‌های دیگر باشد.

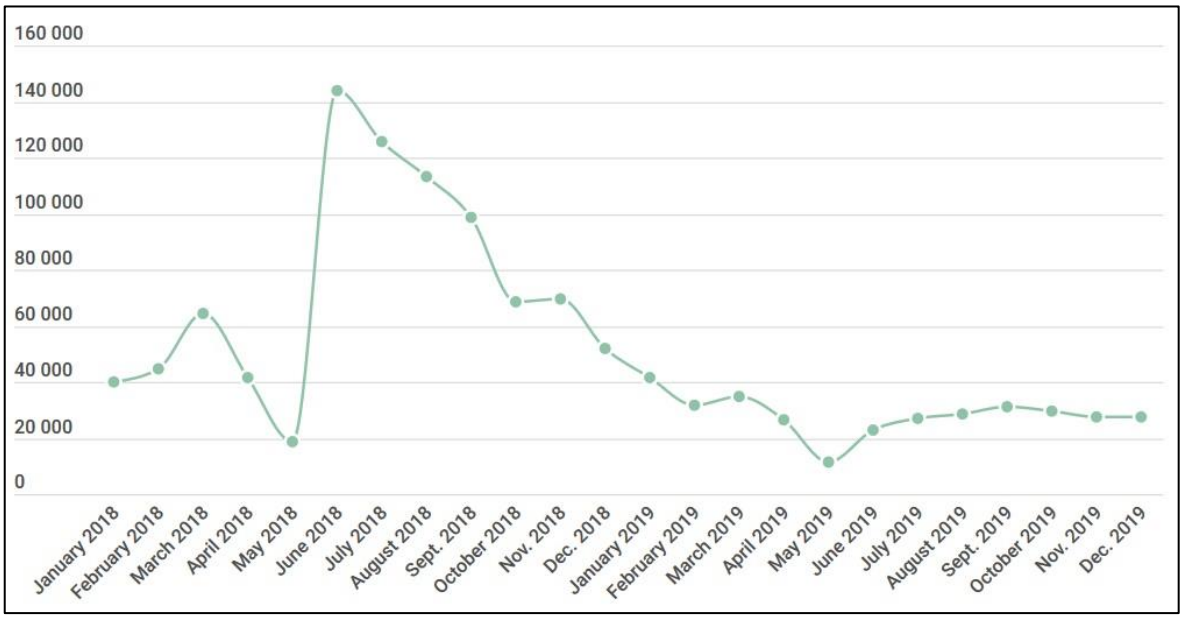
پانزدهمین و سیزدهمین جایگاه مربوط به خانواده Necro از dropperها و loaderها است. در هر دو کلاس تهدید، اعضای خانواده Necro با تعداد فایل‌های شناسایی شده، در ده جایگاه برتر قرار نگرفتند. حتی خانواده ضعیف Hwar از dropperها نسبت به خانواده Necro در مورد اشیاء تولید شده برتر است. به این ترتیب، کاربران اغلب به دلیل نفوذ خانواده در Google Play با اعضای Necro مواجه می‌شوند.

جایگاه‌های دهم و هفدهم مربوط به خانواده تروجان‌های بانکی Asacub است. در اوایل سال ۲۰۱۹، عاملان تروجان به طور فعال آن را منتشر کردند. از ابتدای ماه مارس، شاهد افت فعالیت این خانواده بوده‌ایم. شکل شماره ۱۱ تعداد کاربران منحصر به فرد تحت تأثیر حمله تروجان بانکی Asacub را نشان می‌دهد.



شکل شماره ۱۱: تعداد کاربران منحصر به فرد تحت تأثیر حمله تروجان بانکی Asacub

هشتمین و چهاردهمین جایگاه‌ها مربوط به dropperهای خانواده Hqwar است. فعالیت آن‌ها باعث شد تعداد حملات از میزان ۸۰,۰۰۰ حمله در سال ۲۰۱۸ به ۲۸,۰۰۰ حمله در سال ۲۰۱۹ برسد. با این حال، همچنان آلودگی‌های این خانواده ثبت می‌شود و ممکن است به بالاترین جایگاه برسد. شکل شماره ۱۲ نمایانگر تعداد کاربران منحصر به فرد تحت تأثیر حمله dropper موبایلی Hqwar است.



شکل شماره ۱۲: تعداد کاربران منحصر به فرد تحت تأثیر حمله dropper موبایلی Hqwar

نهمین جایگاه مربوط به یک dropper دیگر از خانواده Lezok است: Trojan-Dropper.AndroidOS.Lezok.p (۱.۷۶٪). تفاوت قابل توجه بین این تروجان و Hqwar این است که بدافزار قبل از ورود به فروشگاه به دستگاه نفوذ می‌کند. آمار KSN نشان می‌دهد که Trojan اغلب در دایرکتوری سیستم با نام PhoneServer، GeocodeService و موارد مشابه تشخیص داده شده است. **Error! Reference source not found.** مسیرهای تهدید شناسایی شده و تعداد کاربران منحصر به فرد تحت تأثیر حمله را نشان می‌دهد.

جدول شماره ۶

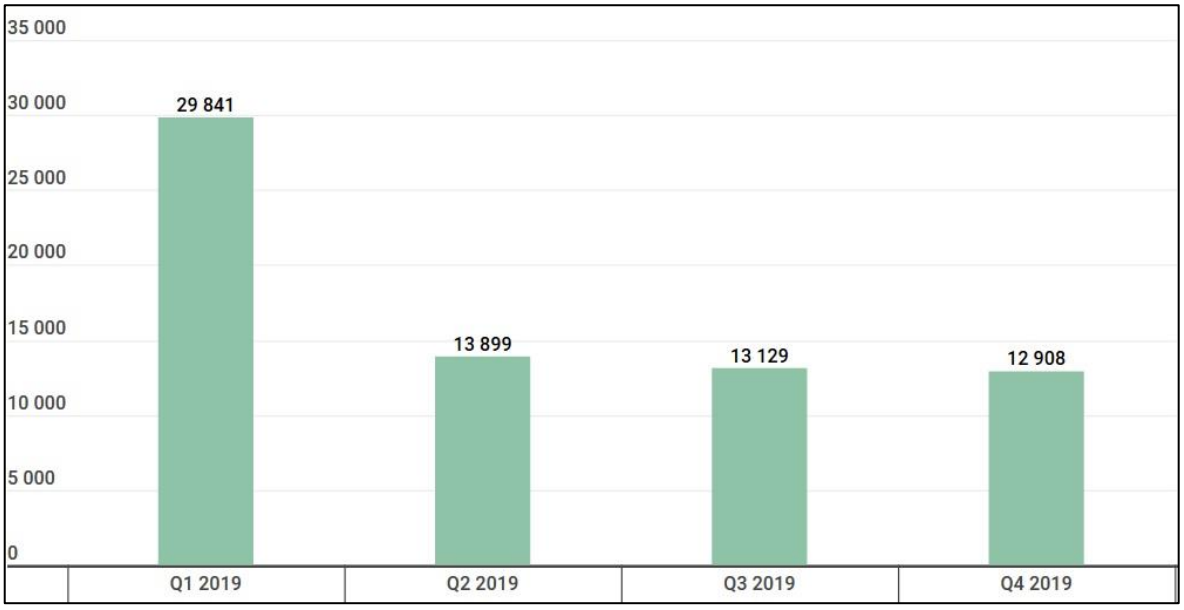
ردیف	مسیر تهدید شناسایی شده	تعداد کاربران منحصر به فرد تحت تأثیر حمله
۱	/system/priv-app/PhoneServer/	۴۹,۶۸۸
۲	/system/priv-app/GeocodeService/	۹۷۴۷
۳	/system/priv-app/Helper/	۶۷۸۴
۴	/system/priv-app/com.android.telephone/	۵۰۳۰
۵	/system/priv-app/	۱۳۹۶
۶	/system/priv-app/CallerIdSearch/	۱۳۴۳

هنگامی که دستگاه روشن می‌شود، Lezo بار آلوده خود را وارد سیستم می‌کند، حتی اگر قربانی این فایل‌ها را با استفاده از ابزارهای عادی سیستم‌عامل حذف کرده یا دستگاه خود را به تنظیمات کارخانه برگرداند. این Trojan بخشی از سیستم‌عامل کارخانه را تشکیل می‌دهد و می‌تواند فایل‌های حذف شده را بارگیری مجدد (بازگردانی) کند.

آخرین تروجان، Trojan-Downloader.AndroidOS.Helper.a (۱.۵۶٪)[۱۱] در جایگاه یازدهم است. بر خلاف تصورات، این تروجان می‌تواند حذف شود. با این وجود، سیستم آلوده شامل تروجان دیگری است که یک برنامه کمکی را نصب کرده و این برنامه نمی‌تواند به آسانی حذف شود. طبق آمارهای KSN اعضای خانواده Trojan-Downloader.AndroidOS.Triada و Trojan.AndroidOS.Dvmap می‌توانند به عنوان ناقل برنامه کمکی عمل کنند، پس ازاینکه قربانی این برنامه را حذف کرد، یکی از اعضای این خانواده مجدداً آن را نصب می‌کند.

۳-۵ تروجان‌های بانکی موبایل

در سال ۲۰۱۹ تعداد ۶۹,۷۷۷ نصب بسته تروجان بانکی[۱۲] موبایل تشخیص داده شد که این آمار نصف آمار سال قبل است. با این حال میزان تروجان‌های بانکی از بین همه تهدیدات شناسایی شده به دلیل نتیجه فعالیت رو به زوال کلاس‌ها و خانواده‌های بدافزارهای موبایلی اندکی رشد کرد. در شکل شماره ۱۳ تعداد نصب بسته‌های تروجان بانکی موبایل در سال ۲۰۱۹ مشاهده می‌شود.

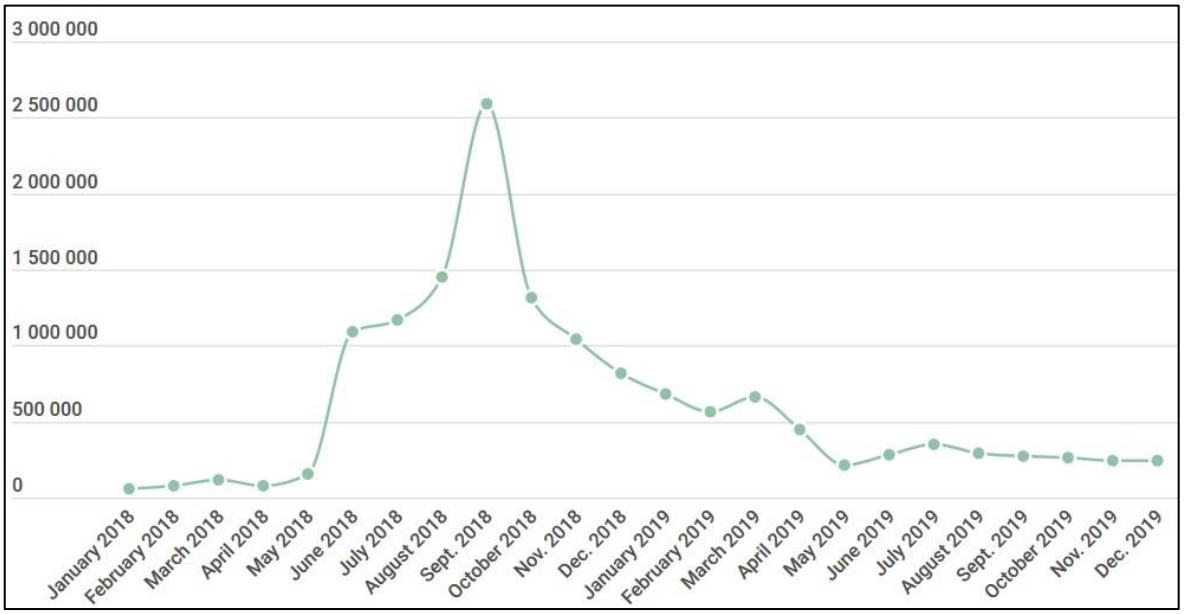


شکل شماره ۱۳: تعداد نصب بسته‌های تروجان بانکی موبایل در سال ۲۰۱۹

[۱۱] تروجان‌های Downloader، نسخه‌های جدید نرم‌افزارهای خرابکارانه از جمله تروجان‌ها و بدافزارها را روی کامپیوترهای آلوده دانلود و نصب می‌کنند.

[۱۲] تروجان‌های بانکی به گونه‌ای طراحی شده‌اند که اطلاعات حساب بانکی را در زمان اتصال به سیستم‌های بانکداری آنلاین، سیستم‌های پرداخت الکترونیکی، کارت‌های اعتباری و ... به سرقت می‌برند.

تعداد بسته‌های نصب شده تروجان‌های بانکی، مانند تعداد حملات تحت تأثیر کمپین توزیع تروجان Asacub بود، که فعالیت آن از شروع آوریل سال ۲۰۱۹ رو به زوال قرار گرفته است. در شکل شماره ۱۴ تعداد حملات تروجان بانکی موبایل در سال ۲۰۱۹ مشاهده می‌شود.



شکل شماره ۱۴: تعداد حملات تروجان بانکی موبایلی در سال‌های ۲۰۱۹-۲۰۱۸

شایان ذکر است که میانگین تعداد حملات در طول سال تقریباً ۲۷۰،۰۰۰ در ماه بوده است.

ده کشور برتر از نظر میزان کاربران تحت تأثیر حمله تروجان بانکی در **Error! Reference source not found.** مشاهده می‌شود:

جدول شماره ۷: میزان کاربران تحت تأثیر حمله تروجان‌های بانکی از کل کاربران

ردیف	نام کشور	میزان برحسب درصد
۱	روسیه	۰.۷۲
۲	آفریقای جنوبی	۰.۶۶
۳	استرالیا	۰.۵۹
۴	اسپانیا	۰.۲۹
۵	تاجیکستان	۰.۲۱
۶	ترکیه	۰.۲۰
۷	ایالات متحده آمریکا	۰.۱۸
۸	ایتالیا	۰.۱۷
۹	اوکراین	۰.۱۷
۱۰	ارمنستان	۰.۱۶

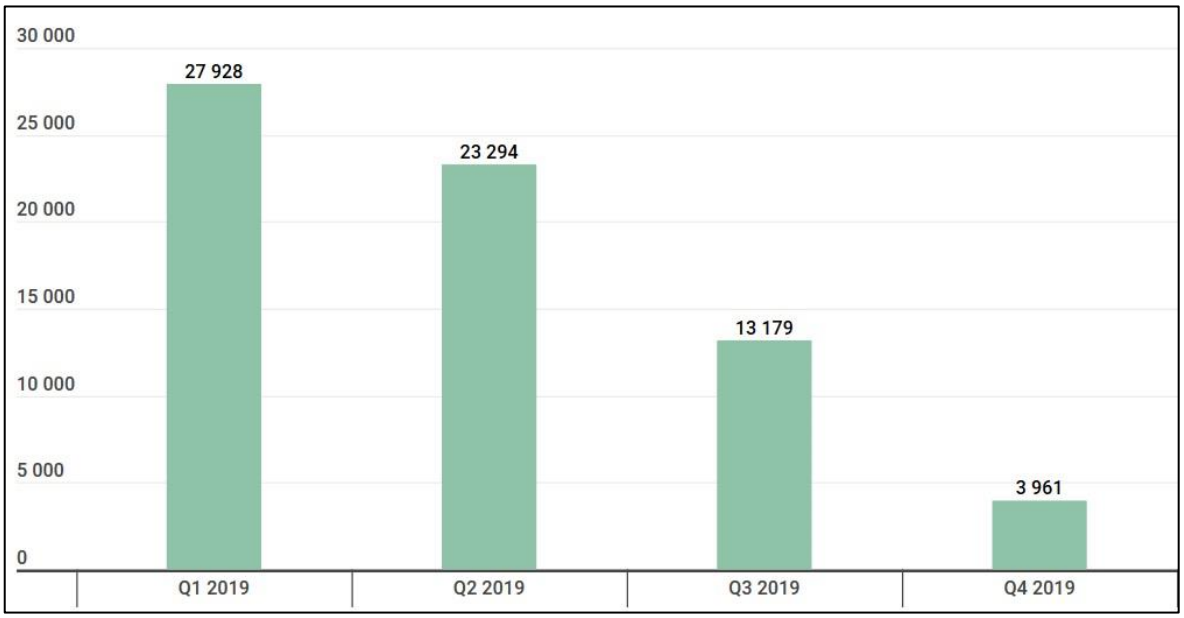
روسیه (۰.۷۲٪) برای سومین سال متوالی در بالاترین جایگاه قرار دارد: بسیاری از خانواده‌های تروجان بر سرقت اعتبار از برنامه‌های بانکی روسی متمرکز شده‌اند. این تروجان‌ها در کشورهای دیگر نیز فعالیت می‌کنند. بنابراین خانواده تروجان Asacub در کشورهای تاجیکستان، اوکراین و ارمنستان و خانواده تروجان Svpeng در روسیه و ایالات متحده تهدید محسوب می‌شوند. در آفریقای جنوبی (۰.۶۶٪) رایج‌ترین تروجان Trojan-Banker.AndroidOS.Agent.dx بود که ۹۵٪ از کل کاربران مورد حمله تهدیدات بانکی را تشکیل می‌داد. بیشترین تروجان منتشر شده در استرالیا (۰.۵۹٪) Trojan-Banker.AndroidOS.Agent.eq (۷۷٪ از کل کاربران تحت تأثیر تهدیدات بانکی) بود. در اسپانیا (۰.۲۹٪) بدافزارهای بانکی از خانواده‌های Cebruser و Trojan-Banker.AndroidOS.Agent.ep رایج بودند (به ترتیب ۴۹٪ و ۲۲٪ از کل کاربران تحت تأثیر تهدیدات بانکی). ده خانواده برتر تروجان‌های بانکی در سال ۲۰۱۹ در **Error! Reference source not found.** قابل مشاهده است.

جدول شماره ۸: میزان کاربران تحت تأثیر این خانواده از تروجان‌های بانکی از کل کاربران تحت تأثیر تروجان بانکی

ردیف	نام خانواده	میزان برحسب درصد
۱	Asacub	۴۴.۴۰
۲	Svpeng	۲۲.۴۰
۳	Agent	۱۹.۰۶
۴	Faketoken	۱۲.۰۲
۵	Hqwar	۳.۷۵
۶	Anubis	۲.۷۲
۷	Marcher	۲.۰۷
۸	Rotexy	۱.۴۶
۹	Gugi	۱.۳۴
۱۰	Regon	۱.۰۱

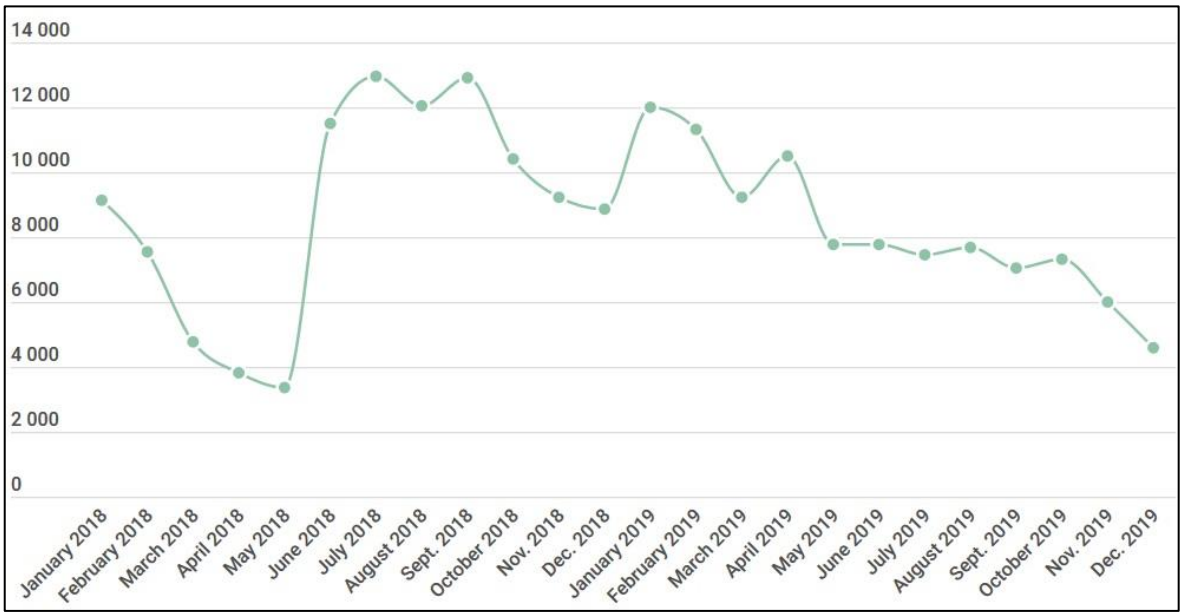
۴-۵ تروجان‌های باج‌افزار موبایل

در سال ۲۰۱۹ تعداد ۶۸,۳۶۲ نصب بسته تروجان باج‌افزار تشخیص داده شد که نسبت به سال ۲۰۱۸، ۸,۱۸۶ بسته بیشتر بود. با این حال شاهد کاهش تولید بسته‌های جدید باج‌افزار در طول سال ۲۰۱۹ بودیم. که حداقل میزان آن در دسامبر اندازه‌گیری شده است. در شکل شماره ۱۵ تعداد نصب جدید بسته‌های تروجان بانکی موبایل در سال ۲۰۱۹ مشاهده می‌شود.



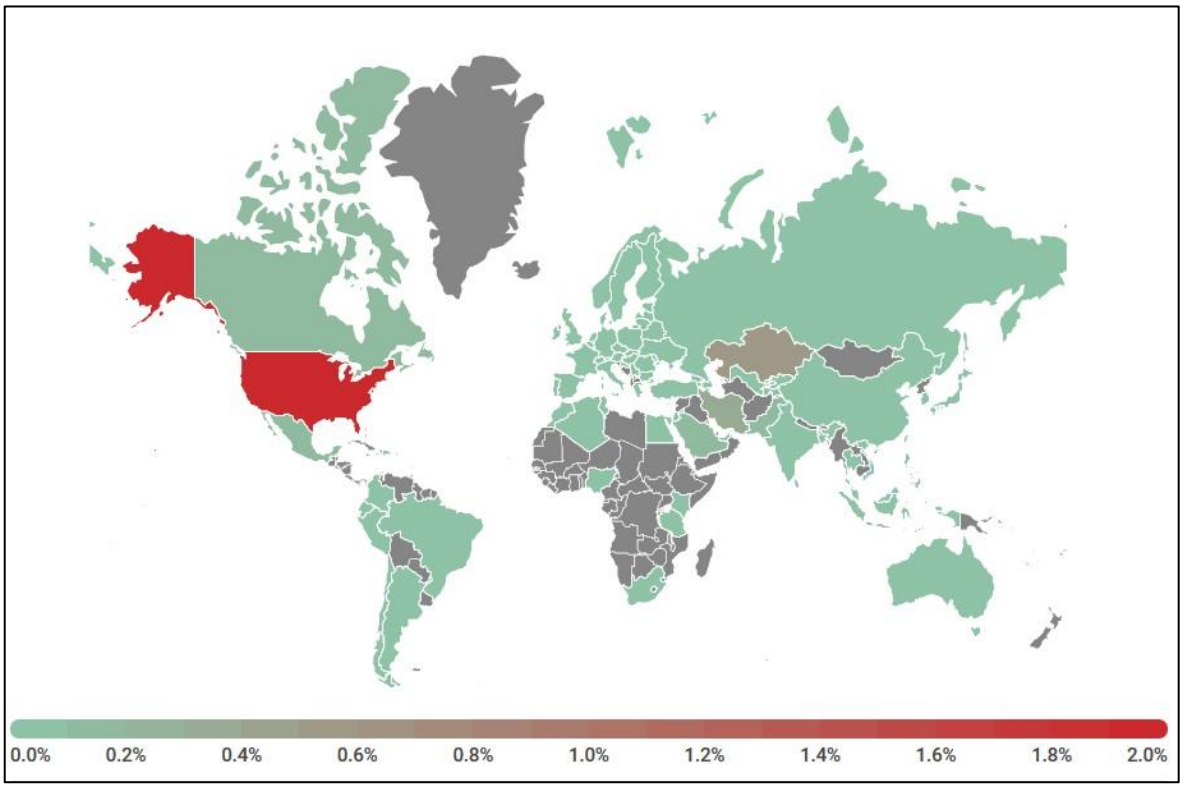
شکل شماره ۱۵: تعداد نصب جدید بسته‌های تروجان بانکی موبایل در سال ۲۰۱۹

آمار مشابهی برای کاربران تحت تأثیر حمله وجود دارد؛ که در اوایل سال ۲۰۱۹ تعداد کاربران تحت تأثیر حمله به ۱۲,۰۰۴ رسید و در پایان سال این رقم ۲.۶ برابر کاهش یافته است. این ارقام در شکل شماره ۱۶ قابل مشاهده است.



شکل شماره ۱۶: تعداد کاربران تحت تأثیر حملات تروجان باج‌افزار در سال‌های ۲۰۱۹-۲۰۱۸

شکل شماره ۱۷ پراکندگی جغرافیایی کشورهای تحت تأثیر حملات باج‌افزار را نشان می‌دهد.



شکل شماره ۱۷: کشورها با میزان کاربران تحت تأثیر حملات تروجان باج‌افزار در سال ۲۰۱۹

ده کشور برتر با میزان کاربران تحت تأثیر حملات تروجان باج‌افزار در **Error! Reference source not found.** قابل مشاهده است (کشورهایی که کمتر از ۲۵۰۰۰ کاربر فعال راه‌حل‌های موبایل Kaspersky در دوره گزارش دارند از رتبه بندی خارج شده اند).

جدول شماره ۹: درصد کاربران منحصر به فرد مورد حمله باج افزارهای تلفن همراه در کشورها از کل کاربران

ردیف	کشور	میزان برحسب درصد
۱	ایالات متحده آمریکا	۲.۰۳
۲	قزاقستان	۰.۵۶
۳	ایران	۰.۳۷
۴	مکزیک	۰.۱۱
۵	عربستان سعودی	۰.۱۰
۶	پاکستان	۰.۱۰
۷	کانادا	۰.۱۰
۸	ایتالیا	۰.۰۹
۹	اندونزی	۰.۰۸
۱۰	استرالیا	۰.۰۶

ایالات متحده (۲.۰۳٪) برای سومین سال متوالی دارای بیشترین کاربران تحت تأثیر حملات باج‌افزار است. همانند سال ۲۰۱۸، خانواده باج‌افزار Svpeng رایج‌ترین باج‌افزار شناخته شد. همچنین این باج‌افزار در کشور ایران (۰.۳۷٪) نیز به طور گسترده منتشر شده است.

موقعیت قزاقستان (۰.۵۶٪) ثابت بوده است؛ این کشور همچنان دارای دومین جایگاه بوده و رایج‌ترین باج‌افزار در آن خانواده Rkor می‌باشد.

۶ چکیده

در سال ۲۰۱۹ شاهد ظهور تهدیدات بسیار پیچیده بانکی موبایل متعددی بوده‌ایم. در واقع بدافزار می‌تواند در عملکرد عادی برنامه‌های بانکی مداخله کند. خطری که آن‌ها ایجاد می‌کنند قابل اغراق نیست، زیرا آن‌ها به قربانی زیان مستقیمی می‌رسانند. این روند در سال ۲۰۲۰ نیز ادامه داشته و شاهد تروجان‌های بانکی بیشتری با تکنولوژِی بالا خواهیم بود.

همچنین در سال ۲۰۱۹ تهدیدات stalkerware بیشتری اتفاق افتاد که هدف آن‌ها نظارت و جمع‌آوری اطلاعات از قربانی بود. در واقع، stalkerwareها با همنوعان بدافزار خود همگام بودند. در سال ۲۰۲۰ شاهد افزایش میزان این تهدیدات و کاربران تحت تأثیر این حملات خواهیم بود.

طبق آمارها، نرم افزارهای تبلیغاتی در بین جرایم سایبری محبوبیت بیشتری پیدا می‌کند. به احتمال زیاد، در آینده با اعضای جدید این کلاس از تهدیدها روبرو خواهیم شد، با بدترین حالت که شامل ماژول‌های تبلیغاتی مزاحم از پیش نصب شده بر روی دستگاه‌های قربانیان است.

۷ مراجع

[1] https://securelist.com/mobile-malware-evolution-2019/96280/

[2] https://encyclopedia.kaspersky.com/glossary/stalkerware-spouseware

[3] https://encyclopedia.kaspersky.com/glossary/adware

[4] https://securelist.com/mobile-subscriptions/91211/

[5] http://mag.onlinecode.ir/mobile-virus/

[6] https://blog.irkaspersky.com/securityarticles/539

[7] http://iedco.ir/news/10/639

[8] https://securelist.com/dropper-in-google-play/92496/