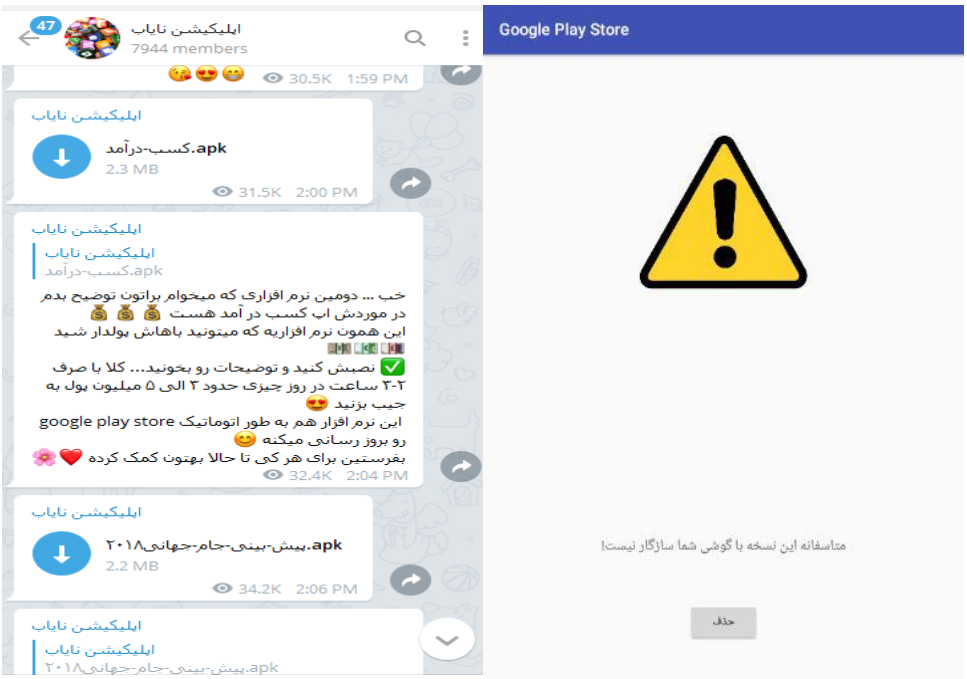
بدافزار موبایلی کسب درآمد

برنامه موبایلی **کسب درآمد** یکی از برنامه‌های اندرویدی می‌باشد که در کانال‌های تلگرامی و سایت‌های غیرمعتبر انتشار یافته و با استفاده از لوگو و آرم برنامه Google Play Store در سیستم نصب می‌گردد. این برنامه هیچ عملکردی نداشته و در بررسی‌ها مشاهده می‌گردد که فقط برای ارتباط با پلت‌فرم‌های پوش‌نوتیفیکیشن می‌باشد. برنامه‌های دیگری نیز با این برنامه از یک منبع انتشار یافته و همه این برنامه‌ها از آیکون برنامه‌های قانونی و سیستمی استفاده کرده و در سیستم عملکردهای منفی دارند.



شکل ۱ - محیط برنامه و تبلیغ برنامه در کانال‌های تلگرامی

شناسایی در آنتی ویروس‌ها

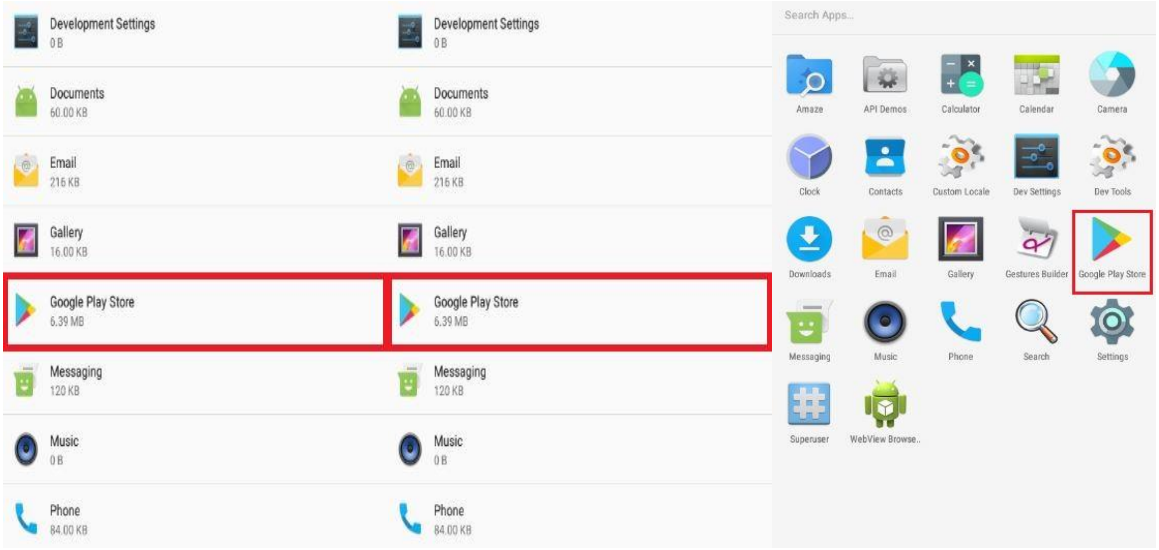
وضعیت تشخیص این فایل توسط آنتی‌ویروس‌های مشهور همراه با علت تشخیص به‌عنوان بدافزار در شکل شماره ۲ قابل مشاهده می‌باشد.

Ad-Aware	Android.Riskware.Agent.gGTGW	AhnLab-V3	Android-PUP/FakeApp.a4c38
Arcabit	Android.Riskware.Agent.gGTGW	Avast Mobile Security	APK:RepMetagen [Trj]
Avira	ANDROID/Hiddad.gysyp	Babable	PUP.HighConfidence
BitDefender	Android.Riskware.Agent.gGTGW	Cyren	AndroidOS/GenBl.36BECA10!Olympus
DrWeb	Android.HiddenAds.508	Emsisoft	Android.Riskware.Agent.gGTGW (B)
eScan	Android.Riskware.Agent.gGTGW	ESET-NOD32	a variant of Android/Hiddad.QL
F-Secure	Android.Riskware.Agent	Fortinet	Android/Hiddad.QL!tr
GData	Android.Riskware.Agent.gGTGW	Ikarus	Trojan.AndroidOS.Hiddad
K7GW	Trojan (005357981)	Kaspersky	HEUR:Trojan.AndroidOS.Piom.uou
MAX	malware (ai score=79)	McAfee	Artemis!1AF6CCC2B140
NANO-Antivirus	Trojan.Android.HiddenAds.felriv	Symantec	Trojan.Gen.2
TrendMicro-HouseCall	Suspicious_GEN.F47V0620	ZoneAlarm	HEUR:Trojan.AndroidOS.Piom.uou

شکل ۲ – وضعیت فایل در آنتی‌ویروس‌های مشهور

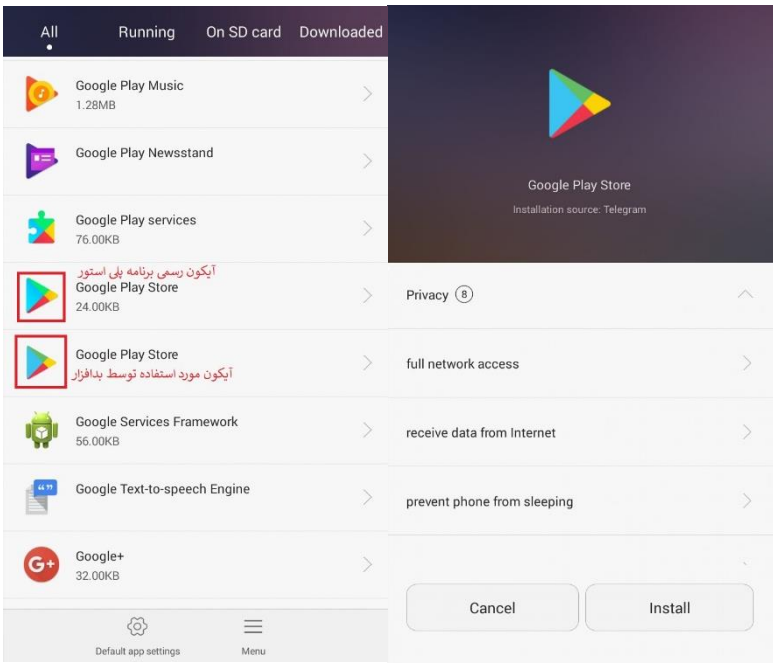
نحوه فعالیت بدافزار

این برنامه بعد از نصب توسط کاربر با آیکون برنامه Google play Store در سیستم ظاهر شده و در صورتی که کاربر برنامه را اجرا کند در صفحه‌ای برای کاربری اعلام می‌کند که برنامه با سیستم سازگار نیست و با اسفاده از دکمه‌ای اقدام به حذف برنامه کند. در صورت کلیک بر روی دکمه، پیغامی را برای کاربر (شکل ۳ سمت چپ) نشان داده و آیکون برنامه را از صفحه نمایش حذف می‌کند. در این صورت آیکون برنامه از صفحه نمایش پاک شده و مخفی می‌گردد. اما این برنامه با آیکون و نام برنامه Google Play Store در قسمت برنامه‌های نصب شده وجود داشته (شکل ۳ در قسمت مرکزی) و به فعالیت خود ادامه می‌دهد. در صورتی که کاربر به اینترنت دسترسی داشته باشد این برنامه با سرور پوش‌نوتیفیکیشن onesignal ارتباط برقرار کرده و اقدام به ارسال پیام برای کاربر در قسمت اعلانات می‌کند. این پیام‌ها می‌توانند بصورت پیام متنی، عکس و یا فیلم باشند.



شکل ۳- محیط برنامه و وجود برنامه بعدا از حذف در درون برنامه

برای تشخیص این برنامه با برنامه اصلی پلی‌استور گوگل می‌توان به آیکون این دو برنامه توجه کرد. در شکل زیر هر دو برنامه نشان داده شده است که تنها تفاوت آن‌ها در رنگ‌های سبز و زرد می‌باشد که جای آن‌ها عوض شده است و هنگام حذف بدافزار باید توجه کرد به اشتباه برنامه پلی‌استور حذف نگردد.



شکل ۴ - نصب و تفاوت آن با برنامه اصلی پلی‌استور

پاکسازی بدافزار از سیستم

برای پاکسازی و جلوگیری از ادامه فعالیت این بدافزار می‌توان بصورت زیر عمل کرد:

۱- با توجه به اینکه آیکون برنامه از صفحه نمایش حذف شده است لذا در قسمت تنظیمات از بخش مدیریت برنامه، برنامه‌ای با نام Google Play Store را یافته و حذف می‌کنیم. این برنامه از نام برنامه رسمی پلی‌استور استفاده کرده و تنها تفاوت آن‌ها در شناسایی آیکون مورد استفاده می‌باشد. که در قسمت‌های قبلی به آن اشاره شده‌است.

۲- با شماره‌گیری کد #1*800* در گوشی موبایل ، اگر سرویس‌های پیامکی فعال بودند، آن‌ها را غیرفعال می‌کنیم.

۳- در قسمت اعلانات سیستم (notification) در صورت وجود برنامه‌ای برای اعلام اعلانات، مقدار آن را غیرفعال می‌کنیم.

راه‌های مراقبت و پیشگیری

برای اینکه گوشی موبایل خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در می‌توان یک آنتی‌ویروس موبایلی قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه از منابع نامعتبر خودداری کنیم.

برنامه‌هایی که در منابع دانلود معتبر همچون Google Play عرضه می‌شوند با استفاده از محافظ‌هایی یکبار برنامه‌ها را بررسی می‌کنند. ولی بیشتر این برنامه‌ها هم امن نیستند. منابع نامتعبر شامل کانال‌های تلگرامی، مارکت‌های غیررسمی و ناشناخته شده، دریافت برنامه از یک شخص دیگر از طریق برنامه‌های اشتراک‌گذاری و غیره می‌باشد.

۳- هنگام نصب برنامه‌های موبایلی به دسترسی‌های درخواستی دقت کنیم.

یشتر برنامه‌ها برای کار خاصی طراحی شده‌اند مثلا برنامه‌ای برای تبدیل عکس به نقاشی می‌باشد ولی در صورتیکه به دسترسی‌های آن نگاه می‌کنیم امکان ارسال و دریافت پیامک هم

وجود دارد. این نوع دسترسی‌ها غیرمعقول می‌باشند. لذا هنگام نصب برنامه‌ها به دسترسی‌های درخواستی توجه کرده و در صورتیکه برنامه‌ای قبلا نصب شده باشد می‌توان در تنظیمات مربوط به برنامه، دسترسی‌های غیرعادی را غیرفعال کرد.

۴- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی گوشی موبایل را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر مانند کامپیوترهای شخصی نگهداری کنیم.

۵- عدم استفاده از نسخه‌های غیررسمی برنامه‌ها

برنامه‌هایی مانند تلگرام نسخه‌های غیررسمی زیادی مانند موبوگرام دارند که توسط توسط اشخاص دیگری توسعه داده شده‌اند و در منابع غیرمعتبر بیشتری ارائه شده‌اند. بیشتر این برنامه یک برنامه قانونی و امن نبوده و امکان آلوده‌سازی را دارند. لذا از نصب چنین برنامه‌هایی باید خودداری گردد و از نسخه‌های رسمی که توسط خود شرکت‌ها ارائه می‌گردد استفاده شوند.

۶- عدم دانلود برنامه‌هایی با عناوین گول‌زننده

برنامه‌های زیادی با استفاده از نام‌های گول زننده‌ای (مانند نمایش فیلم مستهجن) اقدام به پخش بدافزارهای خود می‌کنند لذا با توجه به محتویات بدافزاری این نوع از برنامه‌ها از دانلود و نصب خودداری کنیم.

۷- هشیار بودن در هنگام نصب برنامه‌هایی با حجم پایین

برنامه‌هایی مثل فال یا غیره که نیاز به ارائه اطلاعات برای کاربر دارند باید این اطلاعات را در درون خود ذخیره کنند لذا با این کار حجم برنامه مورد استفاده بالاتر می‌رود. برنامه‌هایی مانند فال تاروت که حجمی کمتر از یک مگابیت دارند نشان دهنده این می‌باشند که اطلاعاتی نداشته و برنامه‌های تقلبی می‌باشند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۳۱۵۰۵۷۱۸ – ۰۴۵

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی