گوشی اندرویدی شما در برابر حملات بدافزاری ایمن است؟

چگونه بدافزارهای اندرویدی را شناسایی و پاک‌سازی کنیم

پیشرفت‌های چند سال گذشته گوشی‌های همراه کیفیت زندگی ما را بهبود بخشیده، اما به همان نسبت مخاطرات امنیتی بالقوه‌ای را به وجود آورده است. بدافزارها می‌توانند هر سیستم‌عامل موبایلی را هدف قرار دهند، اما سهم اندروید بیشتر است، زیرا بیشتر مردم از گوشی‌های هوشمند اندرویدی استفاده می‌کنند. اخبار امنیتی حوزه فناوری‌اطلاعات نشان می‌دهند روزانه بدافزارهای مختلفی به سیستم‌عامل اندروید حمله می‌کنند. اگر کنجکاو هستید درباره مبدا بروز این حملات اطلاعاتی به‌دست آورید و بدانید چگونه باید از حریم خصوصی و دستگاه‌های اندرویدی خود محافظت کنید این مقاله اطلاعات جالبی در اختیارتان قرار می‌دهد.

آیا امکان نصب بدافزارها روی دستگاه‌های اندرویدی وجود دارد؟

برخی از کاربران معتقد هستند که تبلت‌های اندرویدی و گوشی‌های هوشمند آن‌ها در امنیت کامل قرار دارند. روزگاری که هکرها تنها به سراغ سیستم‌عامل‌های دسکتاپی می‌رفتند به پایان رسیده است. امروزه هکرها می‌توانند هر دستگاه هوشمندی از کامپیوترهای رومیزی و همراه گرفته تا تلویزیون‌ها و گوشی‌های هوشمند را قربانی حملات خود کنند. حتا گجت‌های واقعیت مجازی، پهپادها و خودروهای خودران از گزند این حملات در امان نیستند.

تاریخچه‌ای کوتاه از روند شکل‌گیری بدافزارهای اندرویدی

برای آن‌که بتوانیم شناخت درستی از خطرات امنیتی این حوزه به‌دست آوریم، ابتدا باید تاریخچه شکل‌گیری بدافزارهای اندرویدی را بررسی کنیم. گوگل در سال 2008 سیستم‌عامل اندروید را منتشر کرد، سیستم‌عاملی که امروزه 2.5 میلیارد دستگاه پذیرای آن هستند. در ابتدا هکرها علاقه چندانی به اندروید نداشتند، زیرا محبوبیت چندانی نداشت و بیشتر کاربران از کامپیوترهای ویندوزی استفاده می‌کردند. در آن روزگار هکرها روی سیستم‌عامل محبوب سیمبیان متمرکز بودند. به مرور زمان و تقریبا از سال 2010 میلادی که اندروید به سیستم‌عامل فراگیری تبدیل شد، بستری مناسب برای انتشار آلودگی‌ها به وجود آورد. منبع‌باز بودن این سیستم‌عامل در کنار فروشگاه‌های اندرویدی متفرقه‌ای که پدید آمدند، راه را برای ورود برنامه‌های مخرب به فروشگاه‌های رسمی اندروید هموار کردند. در سال 2010 میلادی اولین بدافزار اندرویدی به‌نام AndroidOS.DroidSMS.A شناسایی شد. بدافزار فوق یک برنامه کلاه‌برداری پیامکی بود که بدون اطلاع کاربر شماره تلفن همراه را در سرویس‌های پیام‌کوتاه ثبت‌نام می‌کرد. در اوایل ارائه این سرویس کاربران می‌توانستند نوع پیامکی که قرار است دریافت کنند (خبر، جوک، زنگ هفته و...) را انتخاب کرده و برای دریافت هر پیامک هزینه مربوطه را پرداخت کنند. زمانی‌که گوشی کاربر به بدافزار فوق آلوده می‌شد، به شکل خودکار به عضویت سرویس‌ها در می‌آمد و فرآیندهای تایید را پشت سر می‌گذاشت. کاربر تنها زمانی که قبض تلفن همراه خود را دریافت می‌کرد، مطلع می‌شد که عضو سرویس‌های دریافت پیام کوتاه شده است. در نیمه‌های سال 2010 میلادی بدافزار دیگری به‌نام بازی TapSnake شناسایی شد. بدافزاری که مکان موقعیت‌یاب جهانی دستگاه قربانی را از طریق پروتکل HTTP برای گوشی‌هایی که برنامه GPS Spy روی آن‌ها نصب

شده بود ارسال می‌کرد. در همان سال بدافزار دیگری به‌نام DroidDream شناسایی شد. بدافزار به شکلی برنامه‌نویسی شده بود که تنها در بازه زمانی 11 شب تا 8 صبح که بیشتر کاربران خواب بوده و از دستگاه خود استفاده نمی‌کردند، فعال می‌شد. بدافزار DroidDream یک بات‌نت بود که دسترسی سطح ریشه به دستگاه‌های اندرویدی را به دست می‌آورد و اطلاعات منحصر به‌فرد گوشی‌ها را سرقت می‌کرد. بدافزار می‌توانست گونه‌های دیگری از برنامه‌های مخرب را بدون اطلاع کاربر دانلود کرده و به هکرها اجازه دهد کنترل دستگاه قربانی را به دست گیرند.

مطلب پیشنهادی

همیشه مراقب هک شدن گوشی خود باشید
از کجا بفمیم که گوشی ما هک شده است؟

بدافزارهای اندرویدی به تدریج فراگیر شدند

از سال 2010 تا به امروز هیچ‌گونه نشانه‌ای دال بر کاهش تعداد حملات بدافزاری به گوشی‌های اندرویدی مشاهده نشده است. بیشتر بدافزارهای اندرویدی و کیت‌های انتشار و ساخت بدافزارهای اندرویدی در وب‌تاریک منتشر شده و فروخته می‌شوند. به عبارت دقیق‌تر، هر کاربری می‌تواند به بازارهای وب‌تاریک وارد شده و برای آسیب‌رساندن به دیگران بدافزاری را خریداری کند. به‌طور مثال، جعبه ابزار MazelTov که نام دیگر آن سیستم دانلود APK است در سال 2015 میلادی تولید و انتشار یافت. هدف از طراحی این جعبه ابزار بارگذاری و انتشار بدافزارها روی دستگاه‌های اندرویدی است. کیت انتشار MazelTov به هکرها اجازه می‌دهد کنترل دستگاه‌های آلوده به دست گرفته، آمارهای مختلفی درباره میزان موفقیت بدافزارها به دست آورده و حتا میزان سود خود از آلوده‌سازی دستگاه‌ها را مشاهده کنند. این جعبه ابزار به ارزش 3 هزار دلار و به شکل بیت‌کوین به فروش می‌رسید.

مطلب پیشنهادی

آشنایی با معماری USSD و راهکارهایی برای بهبود مشکلات آن
USSD چیست و خطرات امنیتی آن کدامند؟

انواع بدافزارهای مطرح سیستم‌عامل اندروید

سیستم‌عامل اندروید می‌تواند به انواع مختلفی از بدافزارها آلوده شود، اما رایج‌ترین بدافزارهای این سیستم‌عامل به شرح زیر هستند:

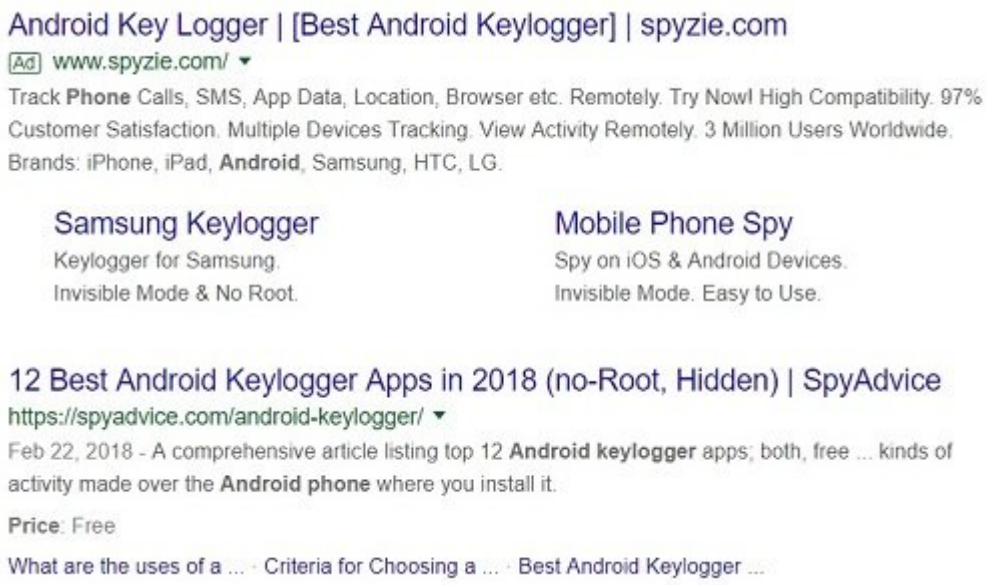
1.تروجان‌ها

تروجان، بدافزاری است که ظاهری شبیه به برنامه‌های کاربردی و نرم‌افزارهای قانونی دارد و بی خطر به نظر می‌رسد. تروجان‌ها با هدف جمع‌آوری داده‌های حساس، فعالیت‌های جاسوسی، حذف فایل‌ها، دسترسی سطح ریشه به دستگاه، بارگیری سایر بدافزارها و... استفاده می‌شوند.

2.روباینده‌گان کلیدها

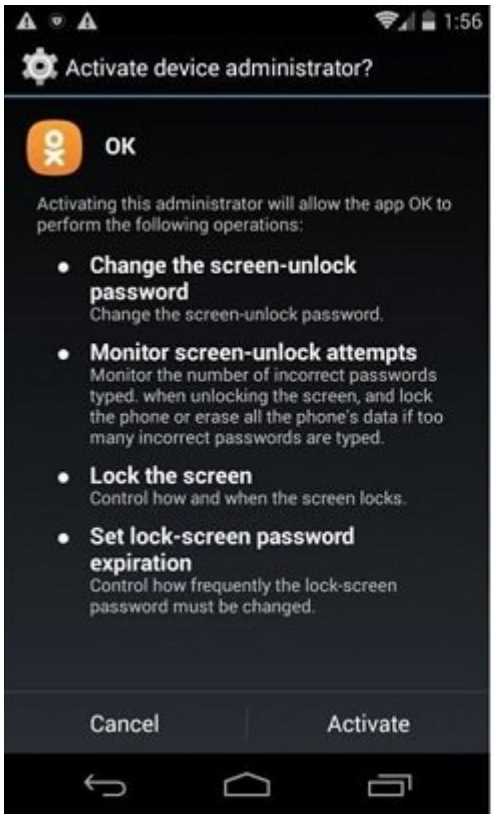
کی‌لاگرها یا به عبارت دقیق‌تر ثبت‌کننده‌های کلیدها، بدافزارهایی هستند که کلیدهای فشرده شده در صفحه‌کلید مجازی کاربر را ضبط می‌کنند. به عبارت دقیق‌تر، هر کلیدی که روی صفحه‌کلید گوشی لمس می‌شود توسط این بدافزارها جمع‌آوری می‌شود. متاسفانه بدافزارهای فوق به راحتی از طریق وب قابل دریافت هستند و حتا کاربران عادی می‌توانند با یک جست‌وجوی ساده آن‌ها را پیدا می‌کنند. بدافزارهای فوق بیشتر با عناوینی شبیه به ابزارهای کنترل والدین تبلیغ می‌شوند و حتا برخی از طراحان نرم‌افزار با شگردهای خاص آن‌ها را تبلیغ می‌کنند و به فروش

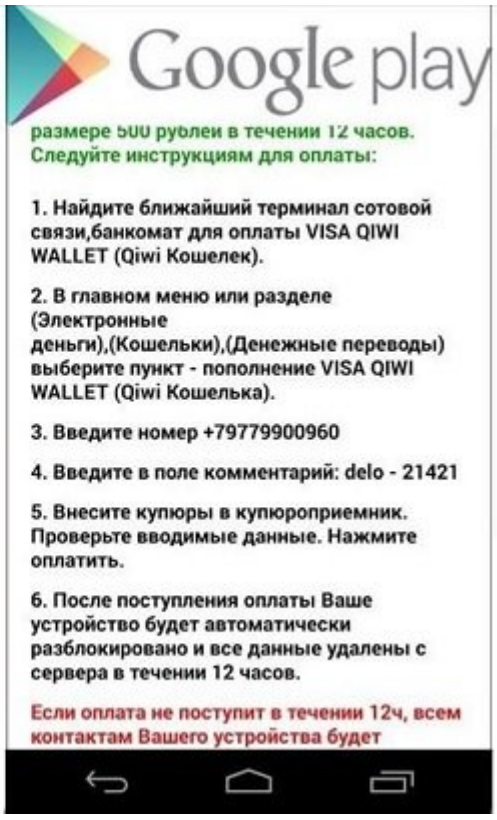
می‌رسانند.



3. باج‌افزار

این مدل بدافزارها بیشتر روی کامپیوترها پیدا می‌شوند، اما در چند سال اخیر باج‌افزارهای مخصوص گوشی‌های اندرویدی نیز انتشار پیدا کرده‌اند. بیشتر باج‌افزارهای اندرویدی فایل‌های روی گوشی‌ها را رمزنگاری می‌کنند، اما برخی از آن‌ها توانایی قفل کردن صفحه‌نمایش گوشی را دارند. در این حالت تنها یک پیام روی گوشی کاربر نشان داده می‌شود که برای رمزگشایی باید مبلغ باج مربوطه را به شکل بیت‌کوین پرداخت کند. در شکل 2 نمونه‌ای از یک حمله باج‌افزاری را مشاهده می‌کنید که مالکان گوشی‌های هوشمندی که زبان دستگاه آن‌ها روسی است را هدف قرار داده است. این پیام به کاربر اطلاع می‌دهد باید مبلغ 500 روبل را پرداخت کنند و اگر باج درخواست شده پرداخت نشود، محتوای خصوصی روی گوشی را برای مخاطبان قربانی ارسال می‌کند.





4. جاسوس‌افزار

جاسوس‌افزار گونه دیگری از بدافزارها است که برای استراق سمع از آن استفاده می‌شود. اگر کاربر پلتفرم واتس‌آپ هستید به احتمال زیاد درباره حمله جاسوس‌افزاری در واتس‌آپ مطلع هستید. حمله‌ای که از یک آسیب‌پذیری در این برنامه سوء استفاده می‌کرد. هکرها از جاسوس‌افزارها برای دسترسی به اطلاعات درون گوشی‌های هوشمند شبیه به فهرست تماس‌ها، پیام‌ها و اطلاعات حساس استفاده می‌کنند و حتا کنترل میکروفون و دوربین گوشی کاربر را به دست می‌گیرند.

5. آگهی‌افزار

اگر زمانی‌که در حال وب‌گردی هستید یا از یک برنامه کاربردی استفاده می‌کنید، تبلیغات مزاحمی روی گوشی خود به شکل تمام صفحه مشاهده می‌کنید، به احتمال زیاد گوشی شما به یک آگهی‌افزار آلوده شده است.

مطلب پیشنهادی

به حداقل رساندن خسارت از دست دادن موبایل
قبل و بعد از به سرقت رفتن گوشی موبایل چه کارهایی باید انجام داد

مهم‌ترین کمپین‌های بدافزاری اندرویدی شناسایی شده در سال 2019

هر ساله کمپین‌های بدافزاری مهمی در ارتباط با سیستم‌عامل اندروید شناسایی می‌شوند که موارد زیر جزء تاثیرگذارترین کمپین‌های 9 ماهه اخیر هستند.

Android/Filecoder.C.1

باج‌افزار FileCoder که سیستم‌عامل اندروید 5.1 به بالا را آلوده می‌کند از طریق پیام‌های متنی که لینک مخربی درون آن‌ها قرار دارد انتشار پیدا می‌کند. پیام‌ها سعی می‌کنند کاربر را متقاعد سازند تا یک برنامه کاربردی را برای شبیه‌سازی تصاویر دانلود کند. زمانی‌که برنامه بارگیری و نصب شد، تمامی فایل‌های روی گوشی رمزنگاری شده و قربانی برای دستیابی دوباره به فایل‌ها باید مبلغ 94 تا 188 دلار را پرداخت کند.

SimBad .2

کمپین فوق در فروردین‌ماه 1398 شناسایی شد و موفق شد 150 میلیون کاربر را قربانی کند. SimBad آگهی‌افزاری است که بنابر اعلام گوگل در 2019 برنامه کاربردی اندرویدی در فروشگاه رسمی گوگل شناسایی شده است. بدافزار فوق در قالب یک کیت تبلیغاتی به‌نام RXDrioder کار می‌کند و به هکرها اجازه می‌دهد تبلیغات هدفمند و مشخصی به کاربران نشان دهند. بیشتر بازی‌های سبک تیراندازی و مسابقه به آگهی‌افزار فوق آلوده بودند. آگهی‌افزار برای آن‌که شناسایی نشود، آیکون‌های برنامه‌ها را پنهان می‌کرد تا کاربر نتواند به راحتی برنامه‌ها را پاک کند. آگهی‌افزار فوق قادر بود تا آدرس اینترنتی خاصی را درون مرورگر کاربر باز کند تا آگهی‌های بیشتری نشان داده شود.

Agent Smith .3

در تیرماه سال جاری، کمپین بدافزاری دیگری به‌نام مامور اسمیت شناسایی شد. این آگهی‌افزار با گذر از سد مکانیزم‌های امنیتی موفق شد 25 میلیون دستگاه اندرویدی را آلوده کند. Agent Smith آگهی‌های مختلفی را به شکل تمام صفحه به کاربران نشان می‌داد و به ازای هر تبلیغی که کاربر مشاهده می‌کرد مبلغی را عاید هکرها می‌کرد. آگهی‌افزار می‌توانست شبکه‌های اجتماعی شبیه به واتس‌آپ را شناسایی کرده، بخشی از کدهای آن‌ها را رونویسی کرده و مانع به‌روزرسانی‌های آن‌ها شود. بدافزار داخل برنامه‌های کاربردی خاصی پنهان می‌شد و پس از نصب روی گوشی قربانی عملکرد برنامه‌های کاربردی مطرح همچون Google Updater را تقلید و روند جایگزینی کدها را آغاز می‌کرد. بدافزار فوق در 9 فروشگاه معتبر اندرویدی شناسایی شد. توسعه‌دهنده این بدافزار موفق شده

بود 11 برنامه کاربردی با کدهای یکسان را درون فروشگاه پلی‌استور منتشر کند.

4. BianLian

BianLian یک تروجان بانکی است که نسخه اولیه آن سال گذشته شناسایی شد. نسخه اولیه با عنوان برنامه‌هایی همچون محاسبه‌گر ارز، تخفیف‌یاب، پاک‌کننده دستگاه از برنامه‌های مزاحم و..... کار می‌کرد. بدافزار فوق پس از اخذ مجوز از کاربر، سرویس‌های کلیدی دستگاه قربانی را ویرایش می‌کرد و در قالب یک بدافزار روباینده کلیدها به کار خود ادامه می‌داد تا اطلاعات مربوط به کارت‌های بانکی را سرقت کند. این برنامه عملکرد کاملا عادی داشت و در صدر برنامه‌های محبوب فروشگاه گوگل قرار گرفته بود. در تیرماه نسخه جدیدی از این بدافزار به‌نام BianLian شناسایی شد. نسخه جدید می‌تواند از صفحه‌نمایش کاربر عکس گرفته و اطلاعات وارد شده که شامل گذرواژه‌ها، نام کاربری و شماره کارت‌های اعتباری است را به شکل تصویری برای هکر ارسال کند.

5. Monokle

Monokle بدافزاری در گروه جاسوس‌افزارها است که مردادماه شناسایی شد. این جاسوس‌افزار از سال 2016 تا به امروز فعال بوده و در برنامه‌های کاربردی جعلی که عملکردی شبیه به برنامه‌های محبوب اسکایپ، سیگنال و Evernote داشتند خود را پنهان می‌کرد. جاسوس‌افزار گذرواژه‌های کاربران را بازیابی می‌کرد و گوشی کاربر را به یک دستگاه شنود تبدیل می‌کرد. ضبط تماس‌ها و شنود از طریق میکروفون از دیگر فعالیت‌های مخرب این بدافزار هستند.

6. MobonoGram (Android.Fakeyouwon)

Mobonogram برنامه مخربی است که کدهای منبع باز برنامه تلگرام را استفاده می‌کرد. این برنامه کاربران کشورهایی که دسترسی به تلگرام در آن کشورها امکان‌پذیر نیست را هدف قرار می‌داد. بدافزار فوق می‌توانست هر زمان دستگاه راه‌اندازی شده یا پس از دریافت به‌روزرسانی‌ها خودش را اجرا کند. درون کدهای این برنامه ماژول‌هایی برای دسترسی به سرورهای کنترل و فرمان‌دهی قرار داشت تا آدرس‌های اینترنتی مخرب را به دست آورد. اجرای کدهای مخرب جاوااسکریپت، پنهان‌سازی منبع درخواست‌ها، کلاه‌برداری کلیکی، باز کردن وب‌سایت‌های مخرب، تخلیه سریع باتری گوش و کرش کردن گوشی بخشی از فعالیت‌های این برنامه بودند. از دی‌ماه 1397 تا خردادماه 1398 پژوهشگران 1235 آلودگی مرتبط با خانواده این بدافزار را شناسایی کردند. قبل از حذف این برنامه از فروشگاه گوگل، Mobonogram دست‌کم 5 به‌روزرسانی را منتشر کرد. لازم به توضیح است، برنامه مخرب دیگری توسط توسعه‌دهندگان این برنامه به‌نام Whatsgram طراحی و منتشر شده است.

مطلب پیشنهادی

مقابله با بدافزارهای کی‌لاگر
صفحه‌کلید خود را رمزنگاری کنید تا گرفتار کی‌لاگرها نشوید

چگونه بدافزارهای گوشی‌های اندرویدی را پیدا کنیم؟

ضدویروس‌های اندرویدی می‌توانند بدافزارها را شناسایی کنند، اگر به هر دلیلی ضدویروسی روی گوشی خود نصب نکرده‌اید یکسری علایم هشداردهنده وجود دارند که ممکن است در شناسایی بدافزارها به شما کمک کنند.

تخلیه زودهنگام شارژ باتری سریع‌تر از حالت عادی

اگر از گوشی اندرویدی به شکل عادی استفاده می‌کنید و استفاده شما بیش از حد معمول نیست، اما شارژ باتری بدون دلیل سریع تخلیه می‌شود، ممکن است گوشی به بدافزاری آلوده شده باشد. در برخی موارد برنامه‌های مخرب به سرعت باتری دستگاه را مصرف می‌کنند. برای بررسی این مشکل باید به بخش تنظیمات گوشی بروید، گزینه Battery انتخاب کنید و برنامه‌هایی که استفاده سنگینی از باتری دستگاه دارند را بررسی کنید. اطمینان حاصل کنید برنامه‌های نشان داده شده در این بخش برنامه‌های واقعی باشند و تشابه اسمی وجود نداشته باشد.

گرم شدن و کاهش عملکرد دستگاه

اگر تغییری در روند به‌کارگیری گوشی رخ نداده و استفاده شما شبیه به گذشته است، اما گوشی به سرعت گرم شده و عملکرد کندی دارد یا اجرای برنامه‌ها با مشکل روبرو می‌شود، ممکن است گوشی به بدافزاری آلوده شده باشد. برای واکاوی این مشکل باید میزان مصرف داده‌ها را بررسی کنید و ببینید چه برنامه‌هایی داده‌های بیشتری مصرف می‌کنند. به Access Settings و سپس Data بروید و تمام برنامه‌های کاربردی را بررسی کنید. اگر برنامه‌ای پیدا کردید که مصرف بیش از اندازه‌ای دارد آن‌را حذف کنید.

نمایش مکرر تبلیغات به شکل غیر عادی و تصادفی

نمایش مکرر تبلیغات حتا زمانی که کار خاصی انجام نمی‌دهید، نشانه روشنی از آلودگی به یک آگهی‌افزار است. گوشی هوشمند نباید بدون دلیل تبلیغات را نشان دهد. هیچ‌گاه روی آگهی‌ها حتا آن‌هایی که وعده‌های مختلفی می‌دهند کلیک نکنید.

نمایش پیام‌های کوتاه و تماس‌های ناشناخته

اگر پیام‌های کوتاه یا تماس‌های ناشناخته‌ای دریافت می‌کنید، ممکن است گوشی آلوده شده باشد. به‌طور مثال، ممکن است پیام عجیبی از مخاطبان خود دریافت کنید که شما را ترغیب می‌کنند روی یک پیوند مشکوک که درون پیامک قرار دارد کلیک کنید. در چنین شرایطی ممکن است بدافزاری گوشی مخاطب را آلوده کرده و چنین پیامی برای شما ارسال شده باشد. به‌طور مثال، باج‌افزار FileCoder از طریق پیام متنی کاربران را آلوده می‌کند. هیچ‌گاه به تماس‌ها یا پیام‌های ناشناخته پاسخ ندهید.

نصب برنامه‌های ناشناس روی گوشی

اگر برنامه‌های ناشناسی روی گوشی پیدا کردید که خودتان آن‌ها را نصب نکرده‌اید به سرعت آن‌ها را پاک کنید. برخی از بدافزارها شبیه به نمونه جعلی Google Updater سعی می‌کنند با تقلید عملکردهای یک برنامه واقعی با پنهان‌کاری کامل به گوشی کاربر وارد شوند.

جست‌وجو برای برنامه‌های پنهان

برخی از برنامه‌های مخرب بدون نصب هیچ آیکونی روی گوشی کاربر نصب می‌شوند. برای پیدا کردن این برنامه‌ها باید به بخش تنظیمات گوشی بروید، گزینه Applications را انتخاب کنید و جست‌وجویی در ارتباط با برنامه‌های ناخواسته انجام دهید. برنامه‌های مشکوک پیدا شده در این بخش را به سرعت پاک کنید.

مطلب پیشنهادی

درمان پس از آسیب‌دیدگی
پس از هک شدن حساب کاربری چه کارهایی باید انجام دهیم؟

چگونه مانع نصب بدافزارها روی گوشی اندرویدی شویم؟

اگر به برخی نکات امنیتی دقت کنیم، هکرها نمی‌توانند به راحتی گوشی اندرویدی ما را آلوده کنند. از جمله نکات امنیتی مهمی که باید به آن‌ها توجه داشته باشید به موارد زیر می‌توان اشاره کرد:

1.گذرواژه گوشی را به شکل پین، الگو یا فاکتورهای زیستی تنظیم کنید
اولین نکته امنیتی که باید در ارتباط با هر دستگاه اندرویدی رعایت کنید، تعیین یک گذرواژه یا یک الگوی تصویری قدرتمند است. اگر گوشی از حس‌گرهای زیستی پشتیبانی می‌کند، بهتر است از اثرانگشت برای باز کردن قفل گوشی استفاده کنید.

2. زمان خاموشی صفحه در صورت غیر فعال بودن را کمتر از 30 ثانیه تنظیم کنید

با این‌کار مطمئن می‌شوید اگر گوشی خود را در مکانی جا گذاشتید، به سرعت قفل شده و کسی به آن دسترسی نخواهد داشت.

3. گوشی را روت نکنید

کاربران سعی می‌کنند برای نصب برنامه‌های کاربردی غیر رسمی به سراغ روت کردن (از قفل خارج کردن گوشی) گوشی بروند و خودشان به‌روزرسانی‌ها را روی سیستم‌عامل نصب کنند. متاسفانه این‌کار مشکلات امنیتی متعددی به همراه دارد، تنها در صورتی این‌کار را انجام دهید که متخصص چیره‌دستی هستید.

4. تنها از فروشگاه‌های معتبر برنامه‌های کاربردی را دریافت کنید

دانلود برنامه‌ها از فروشگاه‌های متفرقه و ناشناس خطر آلودگی را دوچندان می‌کند. گوگل از مکانیزم‌های امنیتی قدرتمندی برای ارزیابی برنامه‌ها استفاده می‌کند. زمانی که برنامه‌ای از فروشگاه غیررسمی دانلود شده و نصب می‌شود در حقیقت مکانیزم‌های امنیتی گوگل را دور می‌زند.

5. برنامه‌های بدون استفاده را حذف کنید

کمی وقت صرف کرده و برنامه‌های بدون استفاده را پاک کنید. برنامه‌های بدون استفاده نه تنها رخنه‌های امنیتی به وجود می‌آورند، بلکه در بیشتر موارد با مصرف پهنای باند برای دریافت به‌روزرسانی‌های متعدد اتمام زودهنگام ترافیک اینترنتی را به همراه می‌آورند.

6. مراقب نصب برنامه‌ها باشید

در برخی موارد کاربران از فروشگاه‌های ثالث اقدام به دانلود برنامه‌های اندرویدی می‌کنند، اما در این میان برخی از فروشگاه‌ها شیطنت می‌کنند. کاربر به دنبال نصب یک برنامه کاربردی است، اما فروشگاه لینک یک برنامه دیگر را ابتدا قرار می‌دهد و لینک برنامه اصلی را پس از لینک تبلیغی قرار می‌دهد. کاربر برنامه فرعی را نصب می‌کند و زمانی‌که متوجه می‌شود اشتباه کرده به سراغ دانلود و نصب برنامه اصلی می‌رود و متاسفانه برنامه فرعی را پاک نمی‌کند.

7. به مجوزهای تخصیص داده شده دقت کنید

برخی از برنامه‌ها از کاربر درخواست می‌کنند به فهرست شماره‌ها، عکس‌ها و مخاطبان دسترسی داشته باشند، در حالی که عملکرد آن‌ها ارتباطی با این بخش‌ها ندارد. این مدل برنامه‌ها برای ردیابی فعالیت‌های کاربران ساخته شده‌اند، بهتر است به سراغ نصب چنین برنامه‌هایی نروید.

8. سیستم‌عامل را به‌روزرسانی کنید

به‌روزرسانی سیستم‌عامل و برنامه‌های کاربردی حائز اهمیت است، زیرا به‌روزرسانی‌ها برای ارائه قابلیت‌های جدید و وصله کردن رخنه‌ها عرضه می‌شوند.

9. اطلاعات گوشی را رمزنگاری کنید

رمزنگاری اطلاعات روی حافظه اصلی و کارت حافظه مانع از آن می‌شود تا اطلاعات شخصی به راحتی سرقت شوند. برای رمزنگاری باید به بخش Security گوشی بروید. دقت کنید فرآیند رمزنگاری و رمزگشایی باعث تخلیه سریع‌تر گوشی می‌شود. بهتر است زمانی‌که باتری گوشی شارژ است، این‌کار را انجام دهید.

10. اخبار امنیتی را دنبال کنید

اخبار مرتبط با انتشار بدافزارهای امنیتی را بررسی کنید تا درباره شگردهای جدید هکرها و راهکارهای مقابله با آن‌ها اطلاعات کافی کسب کنید.

11. از یک ضدویروس خوب استفاده کنید

یک ضدویروس خوب از گوشی در برابر حملات هکری محافظت می‌کند. Thor Mobile Security یکی از گزینه‌های قدرتمند است که پیش از آلوده شدن گوشی، بدافزارها را شناسایی و حذف می‌کند. این ضدویروس آدرس‌های اینترنتی را پیش از باز شدن بررسی می‌کند و اگر مورد مشکوکی پیدا کند مانع باز شدن یک سایت می‌شود.

مطلب پیشنهادی

اضافه کردن یک لایه امنیتی مضاعف
چگونه می‌توانیم یک دیوارآتش به گوشی اندرویدی خود اضافه کنیم؟

چگونه بدافزارهای روی گوشی را پاک کنیم؟

پاک کردن بدافزارها وظیفه ضدویروس‌ها است، اما برخی موارد ممکن است خود مجبور به انجام این‌کار شوید. بدون شک، بهترین راهکار برای حذف ویروس‌های گوشی اندرویدی، ریست فکتوری است، البته این‌کار تمامی اطلاعات روی گوشی و حتا اطلاعات شخصی را پاک می‌کند. در حالت کلی برای حذف بدافزارها از روی گوشی اندرویدی مراحل زیر را دنبال کنید:
1. گوشی را در وضعیت ایمن (safe mode) راه‌اندازی کنید.
2. برنامه‌های مشکوک، بدون استفاده یا قدیمی را حذف کنید.
3. ضدویروسی مطمئنی روی گوشی نصب کنید. Google Play Protect یک مکانیزم امنیتی قدرتمند است، اما هنوز هم کاستی‌هایی دارد. Google Play Protect در تیرماه سال جاری توسط آزمایشگاه AV Comparatives آزمایش شد و امتیاز 83.2 درصد و 28 تشخیص مثبت کاذب را کسب کرد. به همین دلیل بهتر است به فکر یک ضدویروس قدرتمند باشید.

تاریخ انتشار:

26 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/mobile-tricks/android-tricks/16383/%DA%86%DA%AF%D9%88%D9%86%D9%87-

%D8%A8%D8%AF%D8%A7%D9%81%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D8%B1%D8%A7-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D9%88-%D9%BE%D8%A7%DA%A9%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%DA%A9%D9%86%DB%8C%D9%85