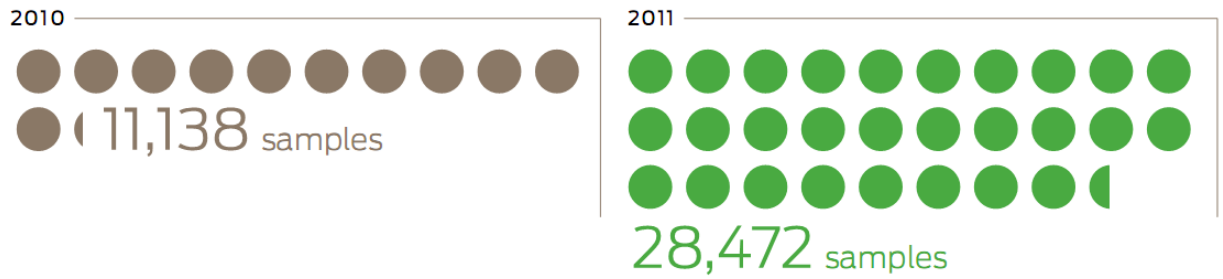
امنیت تلفن های هوشمند در حوزه بدافزار

مقدمه

رشد بدافزار در گوشی های همراه :

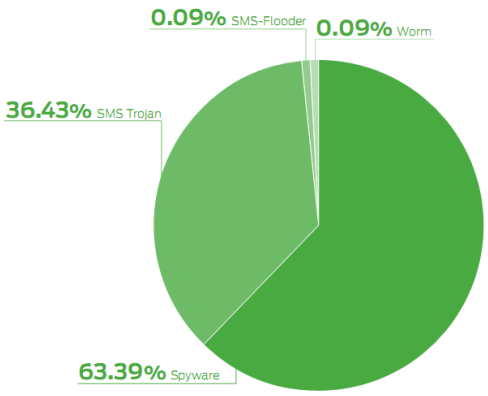
رشد سریع بدافزار در گوشی های تلفن همراه در چند سال اخیر، حاکی از میزان اهمیت تهدیدات و مخاطرات آن برای اهداف کسب وکار و همچنین کاربران خانگی است. در سال ۲۰۱۱ ، شرکت امنیتی juniper اعلام کرد که تعداد بدافزارها در انواع سیستم عامل های موبایل نسبت به چند سال گذشته، ۱۵۵درصد افزایش داشته است. افزایش نرم افزارهای مخرب در گوشی های تلفن همراه و سوء استفاده های مربوط به آنها و همچنین نحوه استفاده افراد از آنها موجب افزایش شدید تعداد بدافزارها شده است. با توجه به اینکه امروزه کاربران زیادی از گوشی های هوشمند و تبلت ها استفاده نموده و میلیون ها نرم افزار برای کاربردهای مختلفی از قبیل بازی، سرگرمی، رسانه های اجتماعی و نقل و انتقالات بانکی نصب می شوند، بسیاری از مهاجمان سایبری توجه خود را به این گونه فعالیت ها معطوف نموده اند.



شکل ۱ مقایسه ای از تعداد نمونه های بدافزار گوشی های تلفن همراه در تمام سیستم عامل ها در سال های ۲۰۱۰ و ۲۰۱۱

انواع بدافزارهای گوشی های تلفن همراه و نحوه عملکرد آنها :

اکثر نرم افزارهای مخرب گوشی‌های همراه و تبلت‌ها را می توان در دو دسته جاسوس افزارها (spyware) و تروجان های پیامک (sms trojans) طبقه بندی نمود. با اینکه طراحی این دوگونه بدافزار از پایه متفاوت است، اما کلاهبرداری مالی مهمترین انگیزه برای اینگونه حملات می باشد.



شکل ۲ دسته بندی بدافزارهای گوشی های همراه

جاسوس افزارها (Spyware):

بنابر یافته های شرکت های امنیتی در سال ۲۰۱۱، جاسوس افزارها، گونه غالب تاثیرگذار با احتساب ۶۳ درصد از نمونه های شناخته شده در گوشی های اندروید می باشد. جاسوس افزار نوعی برنامه نرم افزاری مخرب با قابلیت ضبط و انتقال اطلاعات از قبیل مختصات GPS، نوشته ها یا تاریخچه مرورگر است که بدون اطلاع کاربر، به فعالیت های خود می پردازد. اطلاعات به سرقت رفته، موجب ایجاد زمینه ای برای مهاجمان جهت سوء استفاده مالی و ضرر و زیان کاربر شده و در نهایت باعث از بین رفتن محرمانگی اطلاعات کابران می گردد.

تروجان های پیامک (SMS Trojans)

تروجان های پیامکی بنابر تحقیقات شرکت های امنیتی ، در حدود ۳۶درصد از بدافزارهای شناخته شده گوشی های همراه را تشکیل می دهند. این بدافزارها بطور مخفیانه در پس زمینه برنامه ها قرارگرفته و به ارسال پیوسته پیامک متنی به شماره های ویژه می پردازد. این شماره های ویژه غالباً مربوط به سرویس هایی است که با هماهنگی اپراتور سرویس دهنده تلفن همراه، با دریافت پیامک از کاربر، مبلغی از فرستنده پیامک کاسته و به حساب مالک شماره ویژه انتقال می دهد. هنگامی که پیامک ارسال می شود هزینه قابل برگشت نیست و گیرندگان آن نیز ممکن است ناشناس باشند. مثال هایی از این گونه پیامک ها در بخش نصب کننده های جعلی (fake installers)، آورده شده است.

مشکوک، نه مخرب !

علاوه بر برنامه های مخرب که هدف آنها به وضوح سرقت اطلاعات یا کلاهبرداری مالی از قربانیان می باشد، شرکت های امنیتی تعداد زیادی از برنامه های مشکوکی را شناسایی کرده اند که می توانند اطلاعات غیرضروری را در اختیار شخص ثالثی قرار داده و

نگرانی های امنیتی به وجود آورند. پس از بررسی تعدادی از این گونه برنامه ها مشخص شد که اطلاعات جمع آوری شده و درخواست مجوزهای این برنامه ها بیش از حد گسترده، مشکوک و یا غیراخلاقی بودند.

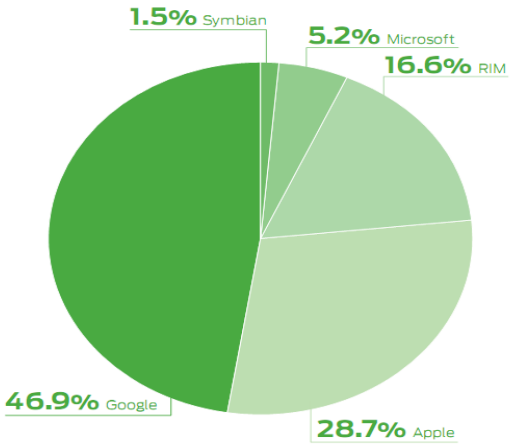
در ذیل برخی از اختیاراتی را که این برنامه ها از سیستم عامل درخواست کرده بودند و میزان خطر آنها که توسط شرکت Juniper اندازه گیری شده است ذکر می گردد:

- ۳۰ درصد از برنامه ها دارای قابلیت به دست آوردن موقعیت گوشی همراه بدون رضایت و اطلاع کاربر بوده اند .
- ۱۴/۷درصد از برنامه ها درخواست مجوز هایی را داشته که منجر به برقراری تماس های تلفنی از گوشی همراه کاربر بدون اطلاع و رضایت وی شده است .
- ۶ درصد از برنامه ها قابلیت جستجوی کلیه حساب های کاربری موجود روی گوشی های تلفن همراه از قبیل پست الکترونیکی و شناسه کاربری وب سایت شبکه های اجتماعی را درخواست کرده اند.
- ۴/۸ درصد از برنامه ها دارای قابلیت ارسال پیامک متنی بدون اطلاع و اختیار کاربر، ارسال بوده اند.

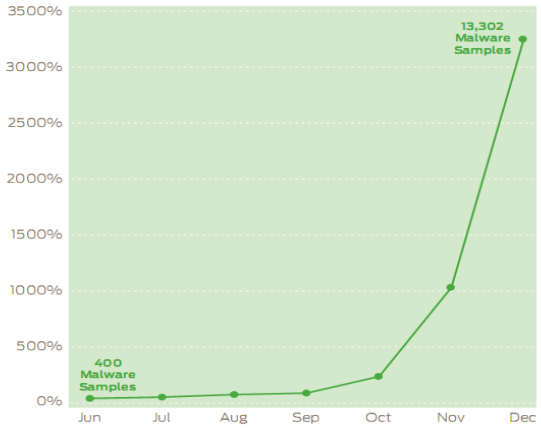
اندروید گوگل: مزایا و خطرات ناشی از محبوبیت

رشد سریع پذیرش سیستم عامل اندروید گوگل در چند سال گذشته آن را در بین سایر سیستم عامل های گوشی های همراه به قدری محبوب نموده است که از زمان انتشار آن یعنی از سال ۲۰۰۷ تا نوامبر ۲۰۱۱، توانسته حدود ۴۶/۹ درصد از بازار گوشی های تلفن همراه را به خود اختصاص دهد. به علاوه طبیعت متن باز آن استفاده از اندروید را برای توسعه دهندگان بسیار آسان و سریع نموده است.

در هفت ماهه اول سال ۲۰۱۱، تنها با احتساب نمونه های شناسایی شده، شرکت Juniper اعلام کرد که بدافزارهایی که هدف آنها سیستم عامل اندروید بوده ۳۳۲۵ درصد رشد داشته و از ۴۰۰ نمونه در ابتدای سال به ۱۳۳۰۲ نمونه در ماه هفتم رسیده است. برطبق آمار جهانی، یک رابطه مستقیم، بین محصول غالب و جرائم سایبری وجود دارد، درست مانند ویندوز مایکروسافت که در بین سیستم عامل های کامپیوتری سهم غالبی در بازار دارد و آن را به شدت مورد هدف بدافزارها قرار داده است. بطور مشابه هم اکنون همین وضعیت در گوشی های تلفن همراه مبتنی بر اندروید گوگل ایجاد شده است که در شکل زیر مشخص شده است:



شکل ۳ سهم بازار سیستم های عامل گوشی های هوشمند



شکل ۴ نمایش رشد تعدد نمونه بدافزارهای سیستم عامل اندروید

نوع دیگری از حملات مبتنی بر اندروید استفاده از مدل بازار برنامه باز (Open application marketplace) اندروید است که دسترسی مهاجمان جهت رسیدن به قربانیان بالقوه را بسیار ساده تر می کند. در حال حاضر، توسعه دهندگان می توانند برنامه خود را بدون آنکه مورد بازرسی قرار بگیرند به Official Android Market، ارسال نمایند. اگرچه گوگل در حذف برنامه های آلوده به سرعت اقدام می نماید ولیکن ممکن است که روند شناسایی اینگونه بدافزارها چند روزی طول بکشد.

در واقع پیچیده ترین مشکل امنیتی برای گوشی های اندروید، قابلیت بارگذاری آزادانه برنامه ها توسط کلیه افراد می باشد. علیرغم اینکه این مساله انعطاف پذیری گوشی همراه را بالا می برد، برنامه های غیرقانونی و یا مخرب نیز ممکن است بارگذاری شوند. برخلاف بازار رسمی اندروید در دیگر فروشگاه های نرم افزار که عمدتاً در اروپای شرقی و چین قرار دارند تقریباً هیچ تلاشی درجهت پاکسازی بدافزارهای شناخته شده به عمل نمی آید.

پلت فرم Black berry شرکت RIM و دیگر انواع سیستم عامل ها

طبق تحقیقات به عمل آمده در شرکت های امنیتی در سال ۲۰۱۱، مشخص گردید رشد بدافزارها در سیستم عامل های بلک بری شرکت RIM، Symbian نوکیا و دیگر سیستم عامل ها روند صعودی داشته است. یکی از این بدافزارها که به خصوص بر روی سیستم عامل های بلک بری شناسایی شد تروجان Zeus بود که با به دست آوردن اطلاعات مالی کاربر اقدام به برقرای ارتباط آنلاین بانکی غیر مجاز و دسترسی به حساب اعتباری قربانیان می نمود.

بطور مشابه برای دیگر سیستم عامل ها نیز همچنان بدافزارها یک تهدید به حساب آمده و تعداد آنها در حال افزایش می باشد، هر چند که دارای نرخ رشد کمتری نسبت به بدافزارهای گوشی های اندروید هستند. به عنوان مثال شرکت Juniper ۳۸۵۱ نمونه بدافزار جدید Java ME را در سال ۲۰۱۱ جمع آوری کرده است. این مسئله بسیار جدی و مهم است زیرا برنامه های جاوا مبتنی بر ME، در بین گوشی های Symbian و ویندوز بسیار رایج می باشد.

حملات تلفن همراه و پیچیده تر شدن آسیب پذیری های آنها

علاوه بر افزایش تعداد بدافزارها، شرکت های امنیتی دریافتند که بدافزارهای پیچیده تر در سال۲۰۱۱ بطور قابل ملاحظه ای رشد یافته اند. برای مثال در ماه مارس، بدافزاری قادر بود از طریق آسیب پذیری های موجود در پلتفرم، ۸۵ درصد گوشی های همراه اندروید بویژه نسخه ۲.۲.۲ یا نسخه های قبل از این سیستم عامل را آلوده نماید. این گونه آسیب پذیری ها، به همراه بدافزارها، مهاجمان را قادر می سازد تا اختیارات سطح root را بدست آورده و بسته های اضافی را نصب کنند تا حوزه عملکرد حمله توسعه یابد. در ذیل به بررسی نمونه هایی از این حملات می پردازیم:

در ماه ژانویه GEINIMI، اولین بدافزاری بود که به صورت یک botnet از طریق بازی های نصب شده بر روی گوشی های اندروید عمل نمود. در ماه مارس بدافزار Deroid Dream برنامه های قانونی در بازار اندروید بیش از ۵۰۰۰۰ کاربر را با استفاده از آسیب پذیری های موجود در سیستم عامل اندروید، آلوده نمود. در ماه می بدافزار Deriod از دو اکسپلویت متفاوت که دسترسی کامل به گوشی های اندروید را از طریق payload های رمز شده که توسط موتور های جستجوی بدافزار هم قابل آشکارسازی نبود استفاده می کرد که در نتیجه این حمله دسترسی و کنترل کامل گوشی در اختیار مهاجمان قرار می گرفت. در ماه فوریه بدافزار ADRD به آدرس های خاصی از روی تجهیزات اندروید درخواست های جستجوی http را ارسال می نمود که باعث افزایش رتبه برخی سایتها شده بود.

آسیب پذیری های Apple iOS

با اینکه نرم افزارهای آلوده بر روی سیستم عامل iOS در بخش وسیعی به علت محدود بودن بازار نرم افزارهای کاربری و مدل نمایش سخت گیرانه اپل بسیار بسته است ولی ضرورتاً آن را نمی توان بسیار ایمن درنظر گرفت. برای نمونه، زمانیکه یک کاربر با انجام jailbreak محدودیت هایش را روی سیستم عامل از بین می برد، دستگاه بستر بسیار مناسبی برای دانلود برنامه های آلوده از منابع دیگر خواهد بود.

علاوه بر این هیچ محصول امنیتی واقعی برای پلت فرم iOS وجود ندارد چرا که شرکت اپل این امکان را برای توسعه دهندگان جهت ساخت ابزارهای امنیتی فراهم نمی کند. این ضعف حفاظتی در نرم افزار و بازار رقابتی امنیت، کاربران را با حفاظت کمی روبرو می کند در صورتی که بدافزاری بخواهد از طریق بررسی نرم افزار apple به آن نفوذ کند. در دراز مدت، این می تواند موجب ایجاد یک حس کاذب امنیت برای کاربران اپل و اثبات خطر بزرگتری از مدل باز اندروید می شود.

خطرات jailbraking :

تعداد زیادی از وب سایت ها مانند jailbreak Me وجود دارند که به کاربران این امکان را میدهد تا به آسانی با استفاده از آسیب پذیری های iOS تجهیزات اپل را jailbreak کنند که در نتیجه این اجازه به شخص حمله کننده داده می شود که نرم افزارهای مخرب را بر روی گوشی کاربران نصب نماید. به هرحال jailbreak بسیار عمومیت یافته است و سایت های سوء استفاده گری

وجود دارند که گوشی های تلفن همراه را jailbreak نموده اند و در نهایت به عنوان بخشی از کار خود بدافزاری را به جا می گذارند.

هشداری برای Application storeها

در اواخر سال ۲۰۱۱، یک محقق امنیتی به نام چارلی میلر، هنگام بررسی برنامه های اپل، تکنیکی را کشف نمود که از طریق آن امکان آپلود برنامه های غیرمجاز بر روی App Store میسر می گردید. او موفق به شناسایی آسیب پذیری درمحدودیت های code-Signing شد که جهت محدود کردن کدها توسط اپل در تجهیزات iOS استفاده می گردید و بوسیله آن اجرای برنامه ها بدون اطلاع کاربر صورت می گرفت.پس از انتشار آسیب پذیری مذکور شرکت اپل نسبت به رفع نقیصه اقدام نمود.

علیرغم آنکه توانایی مهاجمان سایبری در گسترش حملات مشابه روز به روز در حال افزایش است و طبیعت بسیار محدود پلتفرم iOS و App Store کاربران در معرض خطر جدی سایبری قرار می دهد ولی شرکت اپل از توسعه برنامه های ضد بدافزار برای دستگاه های خود جلوگیری می نماید که این مساله باعث ایجاد محدودیت هایی در بازار امنیت سیستم های عامل خواهد شد. به این ترتیب امنیت پایینی بر روی سیستم های عامل گوشی های همراه برای کاربران در مقابل شیوع بالقوه نرم افزارهای مخرب وجود خواهد داشت.

حملات مستقیم

حملات مستقیم شامل یک سیستم حمله کننده و کاربری است که اعمالی را برای سوء استفاده از سیستم های تجهیزات تلفن های همراه انجام می دهد. روش های رایج حملات مستقیم به شرح ذیل است:

- ارسال پیام یا بسته های آلوده به واسط های گوشی های تلفن همراه
- ارسال برنامه های مخرب و پیام های آلوده با پست الکترونیک، SMS و یا MMS
- حمله به برنامه ها با استفاده از محتویات مخرب یا پکت ها
- سواستفاده از آسیب پذیری های موجود یا سوء استفاده از قابلیت های مرورگر گوشی های تلفن همراه

در سال ۲۰۱۱، تحقیقات امنیتی بطور مستقیم بر روی آسیب پذیری های موجود در مرورگر دستگاه ها متمرکز شد. بطور ویژه، این تحقیقات بر روی آن دسته از آسیب پذیری ها که از طریق drive-by-download و بدون دخالت کاربران و غیره صورت می گرفتند، آغاز گردید.

تهدیدات موجود در مرورگرها

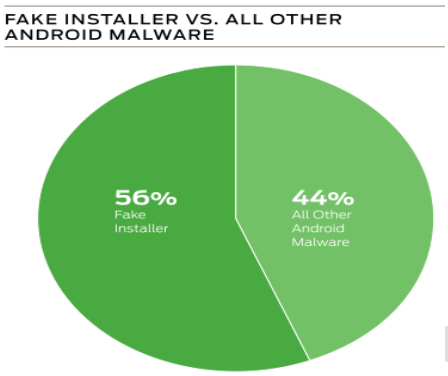
موتور وب کیت(Webkit)، که توسط مرورگرهای سیستم عامل iOS ، اندروید، بلک بری و WebOS مورد استفاده قرار می گیرد، دارای چندین آسیب پذیری شناخته شده است که مهاجمان آن را مورد هدف خود قرار می دهند. برخلاف تهدیدات مبتنی بر برنامه های کاربردی، که با دانلود برنامه های آلوده توسط کاربران منتشر می شوند، این گونه تهدیدات تنها از طریق بازدید یک وب سایت مخرب منتشر می شوند. به این صورت که با استفاده از تکنیکی به نام drive-by downloads با مشاهده یک سایت آلوده توسط کاربر، بدافزارها بطورخودکار و بدون اطلاع وی بارگذاری می شوند. بعنوان مثال، آسیب پذیری موجود در موتور وب کیت که با نام CVE-2010-1807 شناخته می شود به مهاجم این امکان را می دهد که با ایجاد یک صفحه htm خاص موجب crash کردن برنامه شده و بتواند از راه دور کد دلخواهی را اجرا نموده و یا اینکه یک حمله Denial of Service (DOS) را ترتیب دهد.

روند این گونه حملات به این صورت است که کاربر از طریق گوشی همراه خود، صفحه آلوده ای را مشاهده می نماید. مشاهده صفحه وب آلوده باعث سوء استفاده از آسیب پذیری های موجود شده و بدین طریق موجب برقراری ارتباط بین گوشی های همراه و مهاجم می گردد. سپس مهاجم دستوراتی را به منظور دریافت اطلاعات به گوشی همراه، ارسال می نماید. این دستورات از طریق آسیب پذیری موجود در برنامه های کاربری ارسال می گردند. پس از آن اطلاعات گردآوری شده توسط برنامه کاربردی، توسط مهاجم به سرقت می رود.

این تحقیقات نشان دهنده این مطلب است که در سال های آتی مهاجمان با ترکیب آسیب پذیری های موجود در برنامه ها و مرورگرها و یا سیستم های عامل ، نسبت به حملات مستقیم اقدام خواهند کرد .

عدم حفاظت مناسب در برابر تهدیدات

علی رغم رشد چشمگیر تعداد بدافزارهای گوشی های تلفن همراه و به همان نسبت پیچیده تر شدن آنها ، تاکنون حفاظت مناسبی برابر اینگونه بدافزارها ایجاد نشده است. چرا که کاربران بیش از پیش نسبت به بارگذاری برنامه های مختلف بدون در نظر گرفتن تهدیدات موجود، اقدام می نمایند. در نتیجه، برنامه های مذکور می توانند به راحتی بعنوان ابزاری به منظور سوء استفاده از کاربران مورد استفاده قرار گیرند. شرکت های امنیتی به این نتیجه رسیده اند که امروزه تحولی در حملات صورت گرفته است که باعث شده که حملات با پیچیدگی بالا به حملات سبک ، سریع و مبتنی بر نرم افزارهای کاربردی تبدیل شوند. این گونه تهدیدات معمولاً بر اساس مهندسی اجتماعی هستند مثلاً فریب کاربران برای پرداخت هزینه برای برنامه های دزدی یا رایگان. یک چنین روشهایی نیاز به مهارت های فنی کمتری داشته و نیازمند درک عمیق آسیب پذیری ها ندارد. در نتیجه، این گونه اکسپلویت ها رشد قابل ملاحظه ای داشته اند.

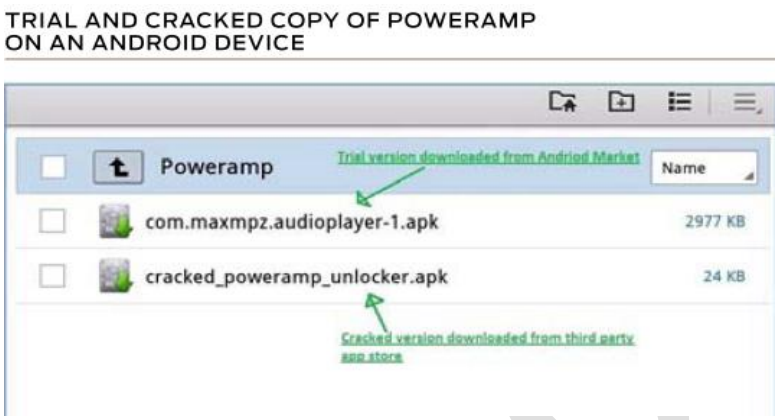


اکسپلویت های اجتماعی : نصب کننده های جعلی

در اکتبر ۲۰۱۱ ، شرکت های فعال در زمینه امنیت تلفن های همراه شروع به جمع آوری تعداد زیادی از کدهای مخرب با عنوان نصب کننده های جعلی در بازارهای متفرقه برنامه های کاربردی کردند که در آنها به جای استفاده از آسیب پذیری های فنی ، از غفلت کاربران برای حمله استفاده می شد. این گونه بدافزارها معمولاً به شکل تروجان های SMS در راستای فریب کاربران مورد استفاده قرار می گرفتند که کاربر را تشویق به ارسال پیامک ها کرده که به این ترتیب کاربران برای برنامه های جعلی و یا مجانی که در بازار شرکت Andriod وجود داشتند، متحمل هزینه می شدند. در مقایسه با دیگر انواع بدافزارهای موجود در سال ۲۰۱۱ که نیازمند سرمایه گذاری جهت گسترش و انتشار بودند این بدافزارها مورد سوء استفاده متخصصین و همچنین مهاجمان مبتدی قرار می گرفت چرا که راهی بسیار ساده تر و سریعتر برای کلاهبرداری مالی نسبت به دیگر روش ها که نیازمند کشف اطلاعات بیشتری از کاربران بودند، به حساب می آمدند. بنابراین کاربران می بایستی نسبت به درخواست های مالی که از طریق sms جهت خرید برنامه یا کالای خاصی، ارسال می شوند، احتیاط بیشتری داشته باشند. در زیر ۲ مثال از کلاهبرداری های مالی توسط بدافزارها آورده شده است.

مثال ۱ نصب کننده جعلی برنامه های سرقت شده PowerAMP

در بسیاری از مواقع مشاهده گردید که بدافزار نویسان نسبت به توزیع برنامه های کابردی پولی کرک شده و یا سرقت شده به کاربران به گونه ای اقدام می کردند که برنامه های مذکور دقیقا همانند برنامه اصلی قابل اجرا بودند با این تفاوت که هزینه های مربوط به آن برنامه به جای واریز به حساب توسعه دهندگان آنها، به حساب هکرها واریز می گردید. در این حالت کاربران پس از مشاهده برنامه جعلی و عدم تشخیص اصلیت آن، نسبت به ارسال خودکار sms های هزینه دار در جهت منافع هکرها، اقدام می نمودند. در شکل زیر برنامه جعلی powerAMP ، به فروش رسیده است:



مثال ۲ برنامه نصب کننده جعلی Opera mini web browser

بسیاری از نصب کننده های جعلی کاربران را فریب داده و آنها را تشویق به پرداخت هزینه برای نرم افزارهای مجانی می نمایند و از طریق sms سود حاصله به کلاه برداران برمی گردد. در مثالی خاص ، کاربران به خرید برنامه جعلی Opera mini web 6.5 browser ترغیب می شدند و در نهایت با ارسال سه sms هزینه دار، مبالغی به حساب هکرها واریز می گردید. در حالی که کاربران به راحتی می توانستند برنامه های کاربردی را از بازار اندروید بصورت رایگان دریافت کنند ولی به این ترتیب متحمل هزینه می شدند. جدول زیر اطلاعاتی را در مورد اجازه های درخواست شده توسط برنامه Opera mini webجعلی به همراه MD5 hash ، آورده است:

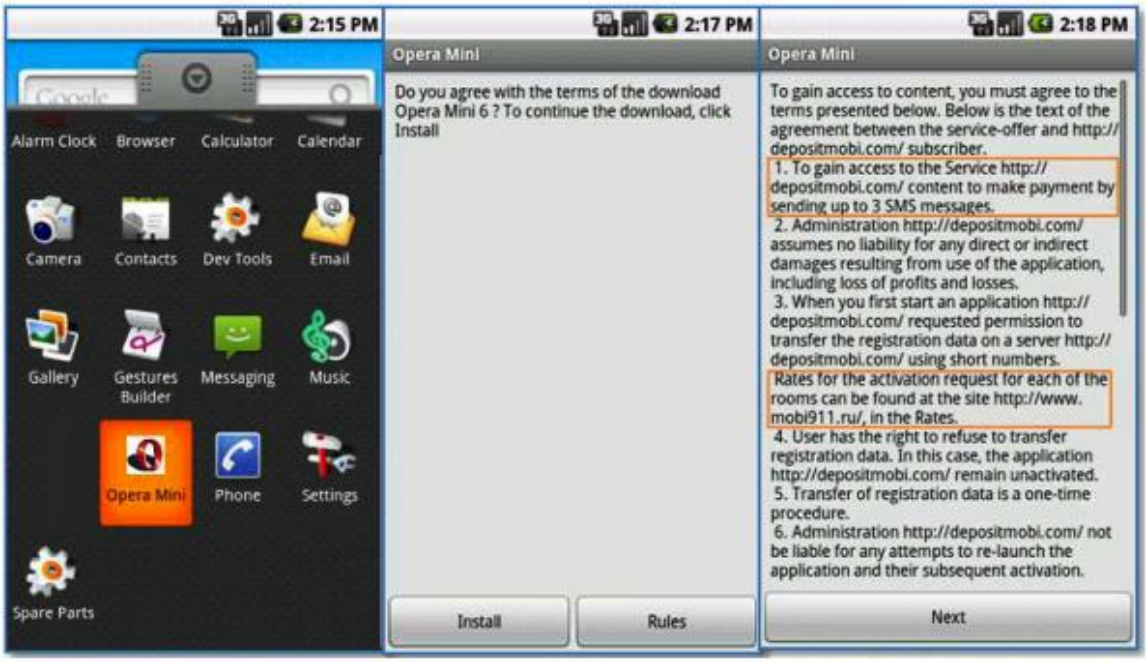
Name	Opera Mini 6.5
MD5	f0ec0e71c49083ad59e766697f39ecb4
Permission	android.permission.SEND_SMS android.permission.CALL_PHONE android.permission.RECEIVE_WAP_PUSH android.permission.READ_SMS android.permission.RECEIVE_WAP_PUSH android.permission.INTERNET

مروری بر روند آلوده سازی نرم افزارهای مخرب:

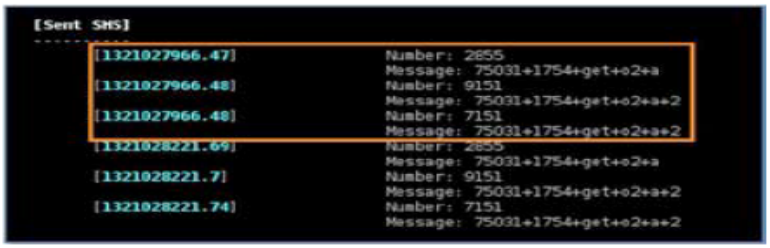
گام ۱- کاربران گوشی های اندروید یک لینک را از App Store های متفرقه از طریق ایمیل یا sms دریافت می کنند.

گام ۲- کاربران سعی می کنند از روی تجهیز اندروید وارد آن لینک شوند ولی به یک وب سایت دیگر منتقل می شوند که از طریق آن کاربران به دریافت آخرین نسخه opera mini web browser مثلاً ۶.۵ تشویق می گردند:

گام ۳- به محض اینکه کاربران به این برنامه دسترسی پیدا می کنند ، یک پیام دریافت می نمایند که بر اساس آن می بایستی جهت بارگذاری برنامه مذکور و همچنین قبول تمامی الزامات قانونی مربوطه، برروی دکمه install کلیک نمایند:



گام ۴- پس از آنکه کاربران بروی دکمه install کلیک نمایند، سه sms هزینه دار به شماره های از قبل تعیین شده ارسال می گردند. لیست زیرsms های دریافت شده را نشان می دهد:



COST PER PREMIUM SMS MESSAGE:

Premium Numbers	US $	Rubles (Russian Currency)
2855	6.65	203.2
9151	3.32	101.6
7151	1.1	33.87
Total	11.07	338.67

گام ۵- پس از ارسال sms ها، برنامه جعلی مذکور نسبت به باز کردن URL بارگذاری برنامه اصلی، اقدام می نماید. مانند کلیه کلاهبرداری های این چنینی، هیچ یک از هزینه های پرداخت شده قابل برگشت نیستند و به کاربران تحمیل خواهند شد.

هک شدن از طریق ارتباطات شبکه ای:

ارتباطات شبکه ای چنانچه به صورت مناسبی امن نشده باشند بسیار آسیب پذیر خواهند بود. اگر چه درگذشته یک چنین حملاتی نیازمند تخصص و زمان زیادی از سوی هکرها بوده است، ولیکن در حال حاضر با توجه به رواج روزافزون تبلت ها و گوشی های تلفن هوشمند، شرایط برای هکرها کاملاً عوض شده است. از آنجا که این وسایل اغلب از ارتباط Wi-Fi استفاده میکنند کاملاً ناامن بوده و به وفور توسط هکرها مورد حمله قرار گرفته اند که به دو نمونه از آن می پردازیم:

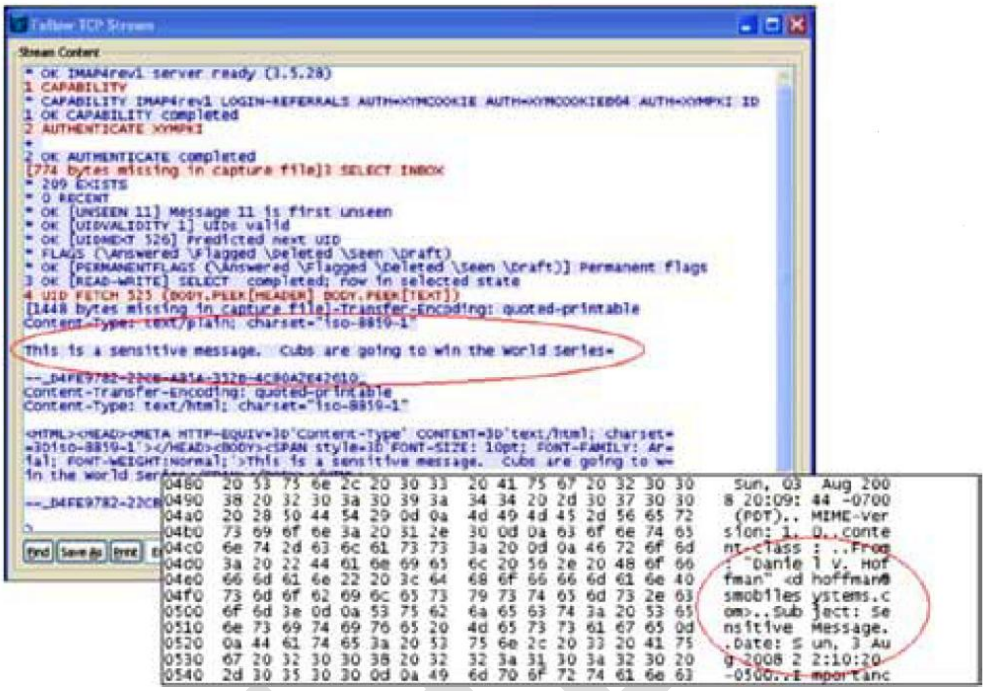
۱– هک شدن از طریق Wi-Fi

با گسترش روزافزون استفاده از ارتباط Wi-Fi در گوشی های تلفن هوشمند و تبلت ها ، تعداد Wi-Fi-hotspot ها از ۱/۳ میلیون به ۵/۸ میلیون تا قبل از سال ۲۰۱۵ خواهد رسید که نشان دهنده رشد ۳۵۰ درصدی آنهاست. Wi-Fi-hotspot ها کانال های راحتی برای هکرها جهت اکسپلویت کردن ، می باشند. با استفاده از ابزارهایی همچون FaceNiff و Firesheep به راحتی میتوان کاربران را برروی یک شبکه Wi-Fi ، شناسایی کرده و اطلاعات آنها را به سرقت برد. لذا هکرها به سهولت قادر خواهند بود که کلمات عبور کارت های اعتباری کاربران و یا دیگر اطلاعات شخصی آنها را سرقت نمایند.

۲– حملات man-in-the-middle (MITM)

شبکه های Wi-Fi مستعد حملات MITM نیز هستند. در این گونه حملات، شخص حمله کننده با استفاده از یک گوشی همراه وارد یک شبکه نا امن Wi-Fi شده و نسبت به تبادل اطلاعات در آن با دیگر کاربران اقدام می نماید. از آنجا که تعداد زیادی از گوش های تلفن همراه با امنیت پایین در این شبکه وجود دارند، هکرها به راحتی می توانند نسبت به سرقت اطلاعات حساس کاربران اقدام نمایند. همانند روش های هک کردن Wi-Fi، ابزارهای هک در MITM نیز به وفور در شبکه اینترنت، وجود دارند که از جمله میتوان به ابزارهای موجود در وب سایت ethicalhacher.net ، اشاره نمود.

در شکل زیر نرم افزار مانیتورینگ wireshark، هکرها را قادر می سازد که وارد صندوق پستی (email) کاربران تلفن همراه شده و اطلاعات حساس و ارزشمند آنها را به سرقت ببرند.



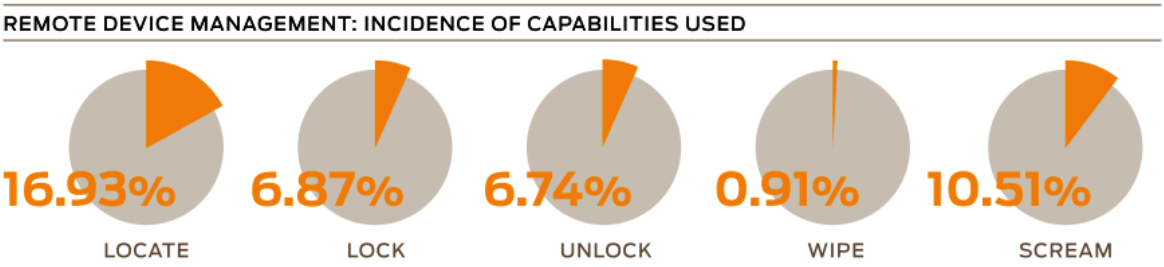
مدیریت تجهیزات گوشی های همراه :

بدافزارها و دیگر تهدیدات تکنیکی فقط یک مشکل از امنیت گوشی های تلفن همراه می باشد. علاوه بر آنها ، مدیریت گوشی های همراه در خصوص محافظت از اطلاعات حساس در هنگام گم شدن و یا به سرقت رفتن تجهیزات مذکور، نیز از اهمیت بالایی برخوردار است چرا که دزدیده شدن و گم شدن آنها ممکن است باعث ایجاد مشکلات عدیده ای مانند :

- افشاء غیر مجاز اطلاعات حساس
- خسارات ناشی از افشاء اطلاعات محرمانه پروژه های اقتصادی
- خسارات ناشی از دسترسی غیر مجاز به اطلاعات شخصی کاربران و سوء استفاده از آنها

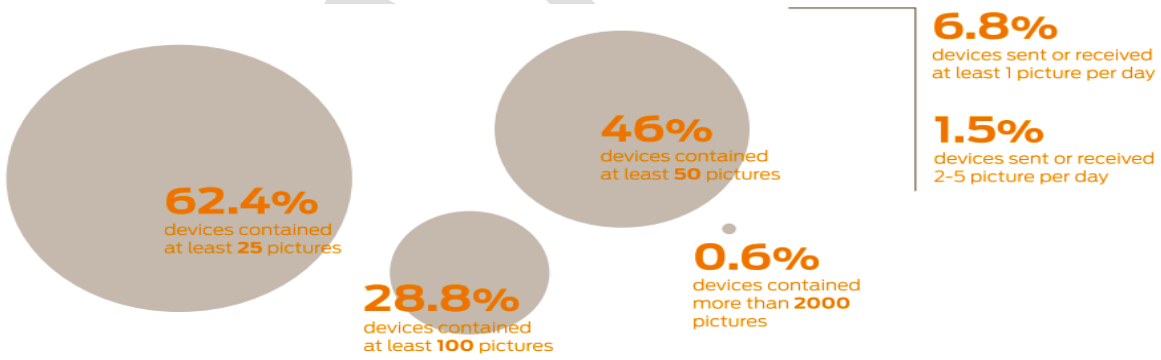
آمارها نشان می دهند که از هر ۵ کاربر که گوشی تلفن همراه آنها گم شده است، ۱ نفرشان از دستور مکان یابی (locate) استفاده نموده است، در حالیکه تنها ۰/۹۱ درصد آنها از دستور (wipe) برای پاکسازی اطلاعات حساسشان، استفاده کرده اند.

در شکل زیر میزان اقدامات انجام شده توسط کاربران در خصوص مدیریت از راه دور گوشی های تلفن همراه آورده شده است:



کنترل های والدین در خصوص حفاظت از نوجوانان در برابر تهدیدات اینترنتی:

با گسترش چشمگیر استفاده کاربران نوجوان از گوشی های هوشمند برای ارتباط با دیگر دوستان به منظور تبادل عکس و فیلم، محیط بسیار مناسبی برای سوء استفاده هکرها، ایجاد شده است. در واقع، ۵۸ درصد کاربران ۱۴ تا ۲۴ ساله، شاهد مسایل غیر اخلاقی در هنگام اتصال به شبکه اینترنت بوده اند در حالی که یک میلیون نوجوان قربانی سوء رفتارهای جنسی در دنیای مجازی بوده اند و ۱۰ درصد کاربران ۱۰ تا ۱۷ ساله عکس های غیر مجاز جنسی دریافت کرده اند که این مساله والدین را ملزم به کنترل تمامی موارد صورت گرفته بر روی گوشی های همراه فرزندانشان خصوصا ارسال و دریافت sms و مدیا، می نماید. در شکل زیر درصد تبادل عکس بین نوجوانان به نمایش در آمده است:



چشم انداز انتشار بدافزارها :

با توجه به رشد سریع تنوع بدافزارها، موارد زیر در سال ۲۰۱۲ پیش بینی می شود:

- افزایش بسیار سریعتر گسترش بدافزارها
- افزایش حملات به برنامه های مورد استفاده در گوشی های همراه
- افزایش تمرکز اهداف بدافزارها بر عملیات نقل و انتقال بانکی در راستای کلاهبرداری مالی

- افزایش حملات مستقیم از طریق drive-by-download و سوء استفاده از browser ها

راهکارهای محافظت از اطلاعات موجود بر روی گوشی های همراه:

۱- برای محافظت از اطلاعات موجود بر روی گوشی های همراه کاربران خانگی موارد زیر پیشنهاد می گردد:

- نصب آنتی ویروس معتبر به همراه دیواره آتش
- حفاظت از گذرواژه ها مانند استفاده از گذرواژه های قوی و اجرای زمان اعتبار مناسب برای آنها
- احتیاط در زمان بارگذاری برنامه ها (خصوصاً اجتناب از بارگذاری برنامه های کرک شده)
- نصب برنامه های از راه دور wipe, locate, lock, track, backup و restore برای بازیابی مجدد اطلاعات
- نصب آنتی اسپم معتبر

۲- برای محافظت از اطلاعات موجود بر روی گوشی های همراه ، موارد کنترلی زیر به والدین پیشنهاد می گردد:

- کنترل محتوای SMS ها
- کنترل محتوای ایمیل ها
- کنترل عکس های رد و بدل شده
- کنترل نرم افزارهای نصب شده
- کنترل log تماس های حاصل شده

۳- برای محافظت از اطلاعات موجود بر روی گوشی های همراه کاربران سازمان های کوچک و بزرگ موارد زیر پیشنهاد می گردد:

- برقراری یک SSL VPN برای امن سازی ارتباطات شبکه ای
- نصب آنتی ویروس و دیواره آتش معتبر
- نصب برنامه های از راه دور متمرکز wipe, locate, lock, track, backup و restore برای بازیابی مجدد اطلاعات
- کنترل نرم افزارهای نصب شده

- کنترل محتوای SMS , MMS و ایمیل های رد و بدل شده
- نصب وصله های مقابله با بدافزار به صورت روزانه
- مانیتور نمودن هر گونه تبادل اطلاعات مشکوک
- Log گرفتن از اتصالات به شبکه و تصدیق هویت کاربران

منبع: http://www.juniper.net/security