رخنه

چرا هکرها به گوشی همراه کاربران علاقه بسیاری دارند؟

برای یک لحظه تأمل کنید و به اطراف خود نگاهی بیاندازید؛ حداقل سه تا چهار گوشی هوشمند را در کنار خود مشاهده می‌کنید (البته اگر فرض کنیم خود شما تنها مالک یک گوشی هوشمند هستید!).

جای هیچ تردیدی نیست که امروزه گوشی‌های هوشمند به بخش جدایی‌ناپذیر زندگی مردم تبدیل شده‌اند. این گوشی‌ها به مالکان خود اجازه می‌دهند وظایف روزمره را به ساده‌ترین و راحت‌ترین شکل ممکن انجام دهند. در شرایطی که گوشی‌های همراه هر روزه سطح رفاهی بیشتری را برای کاربران به ارمغان می‌آورند، به همان نسبت توجه هکرها را نیز به‌سمت خود جلب می‌کنند.

مطلب پیشنهادی

استفاده از ماشین مجازی
با این ترفند ویژه می‌توانید با هر نوع باج‌افزاری مقابله کنید

سؤالی که در این بین وجود دارد این است که در حالت کلی چرا هکرها باید به گوشی‌های هوشمند کاربران علاقه‌مند شوند، در حالی که نفوذ به سامانه‌های صنعتی یا نفوذ مستقیم به شبکه‌های ارتباطی یک سازمان بزرگ ممکن است سود بیشتری را عاید آن‌ها کند؟ اولین پاسخی که به این پرسش می‌توانیم بدهیم این است که گوشی همراه شما برای هکرها حکم یک صندوقچه طلا را دارد. به‌واسطه آنکه اطلاعات بسیاری از شما روی آن وجود دارد. در چند سال اخیر کاربران به‌شکل کاملاً بی‌سابقه و ماورای تصور اطلاعات شخصی خود را روی گوشی‌های همراه ذخیره‌سازی کرده‌اند. امروزه بسیاری از برنامه‌ها به‌ویژه برنامه‌هایی که از سوی یک شرکت تولید می‌شوند با یکدیگر در ارتباط هستند و ما در اغلب موارد مجبوریم اطلاعات بسیاری را درباره خود در این برنامه‌ها ثبت کنیم. این اطلاعات ممکن است مشخصات هویتی شما یا جزئیاتی در ارتباط با حساب‌های بانکی شما باشد. زمانی که تصمیم می‌گیرید برای سفارش غذا اشتراکی را در یک رستوران ایجاد کنید، اطلاعات فردی، شماره تلفن و نشانی خود را در برنامه یا سرویس یک رستوران وارد می‌کنید تا در آینده بتوانید به‌راحتی از طریق گوشی هوشمند خود غذای مورد نظر را سفارش دهید. این ساز و کار دیگر مختص کشورهای غربی نیست و داخل کشور ما نیز در حال حاضر چنین سرویس‌هایی ارائه می‌شود. دسترسی به همین اطلاعات ناچیز نیز برای هکرها ارزشمند است.

مطلب پیشنهادی

حمله‌ای از سوی زیرنویس‌های مخرب
200 میلیون کاربر از طریق زیرنویس‌های مخرب در معرض تهدید قرار دارند

اما اطلاعات شخصی تنها دلیلی نیست که هکرها را به گوشی همراه شما علاقه‌مند می‌کند. گوشی‌های هوشمند امروزه به یکی از ابزارهای مهم سازمانی تبدیل شده‌اند و بسیاری از شرکت‌ها برای تعدادی از کارمندان خود خطوط همراه ثابت را خریداری می‌کنند و در اختیار آن‌ها قرار می‌دهند. این افراد از طریق شبکه‌هایی همچون تلگرام یا دیگر سرویس‌های آنلاین با سازمان و مدیران مطبوع خود در ارتباط هستند. در نتیجه، نفوذ به یک گوشی همراه به معنای گذر از دروازه‌ای است که دسترسی به اطلاعات حساس سازمانی را امکان‌پذیر می‌سازد.

مطلب پیشنهادی

سرمقاله شماره 177 ماهنامه شبکه
BYOD، داده‌های سازمان، ابزارهای کارکنان

نکته دیگری که باعث علاقه‌مندی هکرها به گوشی‌های هوشمند می‌شود، مسئله امنیت است. متأسفانه چند وقت پیش شاهد گسترش باج‌افزار مخربی به‌نام WannaCry بودیم. این باج‌افزار به‌راحتی سیستم‌های ویندوزی که به‌روزرسانی امنیتی مایکروسافت را دریافت نکرده بودند، قربانی خود ساخت. ظهور فناوری‌هایی نوینی همچون BYOD (سرنام Bring Your Own Device) نیز بر وخامت اوضاع افزوده است. به‌واسطه آنکه سازمان‌ها از یک استراتژی مدون برای یکپارچه کردن حفظ امنیت این دستگاه‌ها استفاده نمی‌کنند. جالب آنکه حتی مدیران ارشد و کارکنان سازمان‌ها نیز به‌خوبی از این موضوع اطلاع دارند که دستگاه‌های همراه تهدیدی جدی برای زیرساخت‌های یک شبکه به شمار می‌روند؛ با وجود این، تمهیدات لازم را برای ایمن‌سازی این دستگاه‌ها به کار نمی‌گیرند. به‌ویژه آنکه مالکان گوشی‌های همراه در بخش‌های مختلف یک سازمان مستقر هستند و ممکن است هر لحظه در معرض یک تهدید هکری قرار گیرند. در کنار اطلاعات شخصی و نبود یک مکانیسم امنیتی یکپارچه نباید از ویژگی پر کردن خودکار فرم‌های اینترنتی غافل شویم. ما همواره تمایل داریم تا اطلاعات و فایل‌های شخصی را در هر مکانی و با کمترین زحمت ممکن در اختیار داشته باشیم.

مطلب پیشنهادی

اشتباهات رایج کاربران
۷ اشتباه امنیتی مرگ‌بار که احتمالا شما هم مرتکب می‌شوید

زمانی که عضو سایت‌ها یا سرویس‌های اینترنتی می‌شویم یا در برنامه‌های مختلف اطلاعاتی را وارد می‌کنیم، تصمیم می‌گیریم گزینه پر کردن خودکار را فعال کنیم. در این حالت دیگر نیازی نداریم جزئیات و اطلاعات مربوط به احراز هویت را در هر بار ورود به یک سرویس وارد کنیم. این رویکرد در درازمدت باعث تنبل شدن ما می‌شود. زمانی که تصمیم می‌گیریم گزینه پر کردن خودکار را فعال کنیم، در واقع یک نقص داده‌ای را رقم زده و خود را به‌راحتی در معرض یک تهدید ناخواسته قرار داده‌ایم.

عامل دیگری که هکرها را به گوشی همراه ما علاقه‌مند می‌سازد، فعالیت‌های آنلاین مالی است. امروزه بسیاری از کاربران ترجیح می‌دهند به‌جای مراجعه به بانک یا دستگاه‌های خودپرداز از دستگاه‌های همراه خود برای نقل و انتقال پول استفاده کنند. البته ساز و کار مورد استفاده ما در مقایسه با نمونه‌های خارجی تفاوت‌هایی دارد، اما شکی نیست در کوتاه‌مدت نمونه‌ها و مدل‌های داخلی کیف پول گوگل یا سامانه‌های پرداختی ارائه شده از سوی اپل و سامسونگ در داخل کشور نیز پیاده‌سازی خواهند شد. در حالی که پیاده‌سازی چنین ساز و کاری خدمات بانکی را بیش از پیش راحت و به چرخه اقتصادی کشور کمک می‌کند، اما به همان نسبت علاقه هکرها به گوشی‌های همراه ما را نیز بیشتر می‌کند. سامانه‌های موقعیت‌یاب عامل مهم دیگری هستند که باعث می‌شوند هکرها به گوشی‌های ما علاقه‌مند شوند. شاید این سامانه در بعضی موارد راهگشا باشد، اما به این نکته توجه داشته باشید که هکرها به‌راحتی قادر هستند به سامانه‌های موقعیت‌یاب جهانی یک گوشی هوشمند نفوذ کنند. عامل مهم دیگری که نباید از آن غافل شویم هرزنامه‌ها هستند. امنیت و هرزنامه دو واژه جدایی‌ناپذیر هستند.

مطلب پیشنهادی

باج‌افزارهایی در کمین گوشی‌های همراه
کسپرسکی گزارش داد: رشد سه برابری حمله باج‌افزارها به گوشی‌های موبایل

دلایل متعددی وجود دارد که هکرها را مجاب می‌کند هرزنامه‌ها را برای کاربران ارسال کنند. در مقطع فعلی گوشی‌های هوشمند جزء یکی از بهترین زیرساخت‌هایی به شمار می‌روند که هکرها برای ارسال هرزنامه‌ها می‌توانند از آن‌ها استفاده کنند. درنهایت، مهم‌ترین عاملی که باعث شده است هکرها به گوشی‌های همراه کاربران علاقه‌مند شوند، به کم‌اطلاعی کاربران بازمی‌گردد. کاربران در طی این سال‌ها یاد گرفته‌اند چگونه از لپ‌تاپ‌ها و کامپیوترهای خانگی خود محافظت کنند. اما در مقابل هنوز آن گونه که باید مسئله امنیت گوشی‌های همراه را جدی نگرفته‌اند. همین موضوع باعث شده است تا از ده سال پیش تاکنون بر شدت حمله به گوشی‌های همراه افزوده شود. جالب آنکه هرچه با مباحث امنیتی بیشتر آشنا می‌شویم، با انواع مختلفی از تهدیدات امنیتی روبه‌رو می‌شویم که هیچ‌گاه تصور نمی‌کردیم در زیر انگشتان ما

قرار داشته باشند!

تاریخ انتشار:

10 تیر 1396

نشانی منبع:
https://www.shabakeh-mag.com/opinion/8374/%DA%86%D8%B1%D8%A7-%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D8%A8%D9%87-%DA%AF%D9%88%D8%B4%DB%8C-%D9%87%D9%85%D8%B1%D8%A7%D9%87-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%B9%D9%84%D8%A7%D9%82%D9%87-%D8%A8%D8%B3%DB%8C%D8%A7%D8%B1%DB%8C-%D8%AF%D8%A7%D8%B1%D9%86%D8%AF%D8%9F