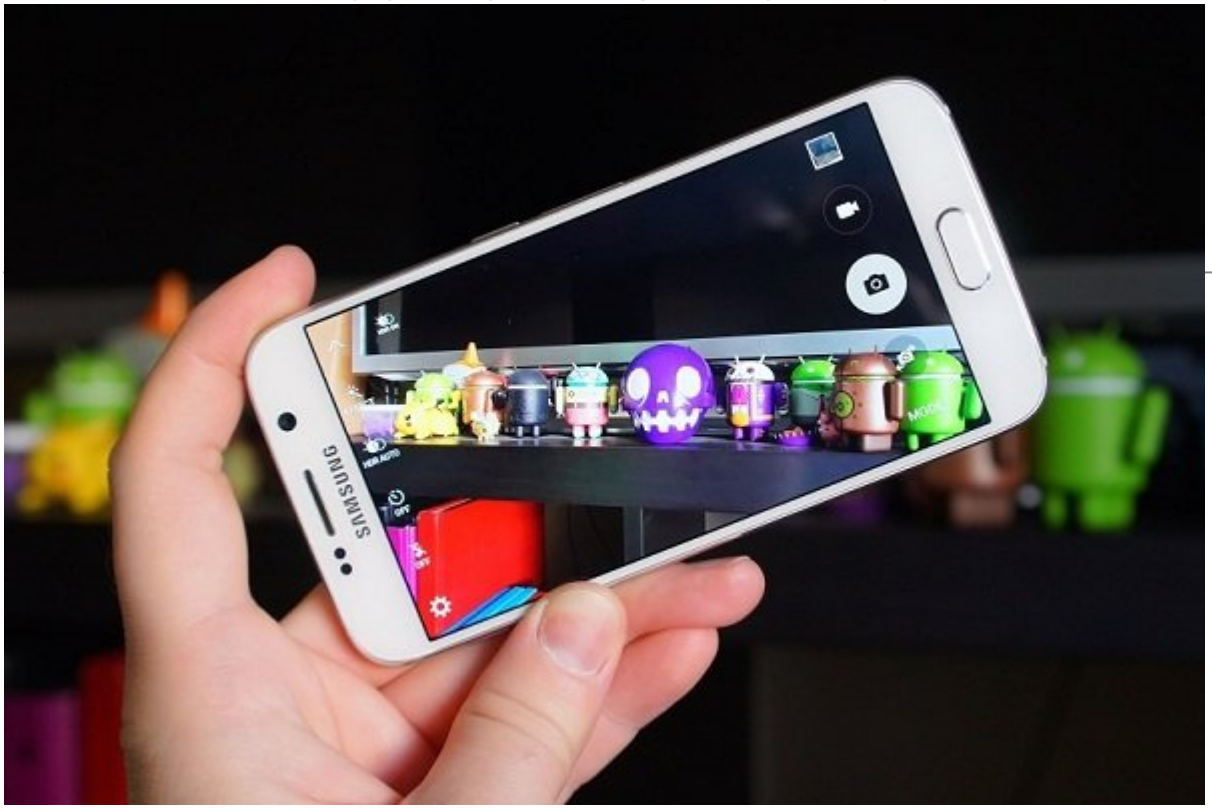
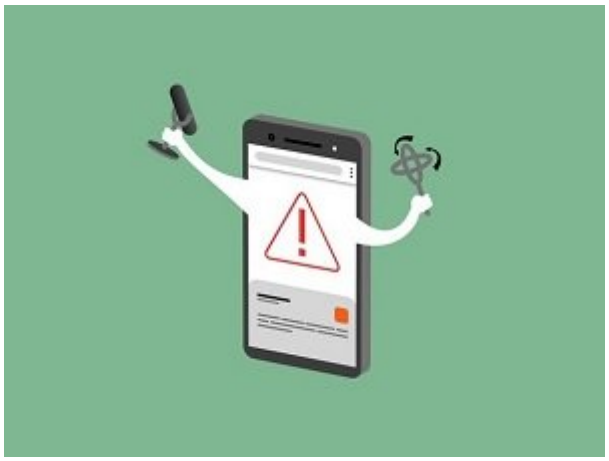
اشباح دیجیتال

استفاده مخفیانه سایت‌ها از حسگرهای گوشی همراه کاربران



در سال‌های اخیر بسیاری از کاربران به‌خوبی دریافته‌اند که چطور از خود در مقابل مهاجمان فضای مجازی محافظت کنند. آن‌ها در نصب نرم‌افزارهای تلفن همراه دقت زیادی می‌کنند، وارد هر لینکی نمی‌شوند و رمزهای عبور مناسبی برای خود انتخاب می‌کنند. بااین‌حال، پیشرفت فناوری و افزایش امکانات دستگاه‌های دیجیتال، روزنه‌های نفوذ جدیدی را به روی مهاجمان می‌گشاید و زمان می‌برد تا کاربران عادی متوجه این دریچه‌های نفوذ شوند و روش مسدود کردن آن‌ها را بیاموزند. در «دنیای موبایل» این شماره دو مثال از چنین روزنه‌های نفوذی را بررسی خواهیم کرد و این‌که چطور مهاجمان می‌توانند با دستورهای صوتی و بدون این‌که کسی متوجه شود، ده‌ها دستیار صوتی را فریب دهند یا چطور مرورگرهای گوشی همراه می‌توانند راه را برای سوءاستفاده از کاربران هموار کنند.

نرم‌افزارهای گوشی همراه برای دسترسی به حسگرهای دستگاه، معمولا از کاربر اجازه می‌گیرند و این یک الزام است. اما گروهی از محققان دریافته‌اند، مرورگرهای اینترنتی نصب‌شده روی گوشی‌ها چنین محدودیتی ندارند و این امکان را به وب‌سایت‌ها می‌دهند که بدون اجازه، بارها و بارها به اطلاعات **حسگرهای گوشی** شما دسترسی پیدا کنند. دسترسی این مرورگرها به **حسگرهای گوشی** به‌خودی‌خود موضوع خطرآفرینی نیست و مرورگرها از اطلاعات حسگرهای گوشی برای مثال برای نمایش بهتر صفحات استفاده می‌کنند و حتی استانداردهایی در این زمینه وضع‌شده است. اما محققانی از دانشگاه‌های کارولینای شمالی، پرینستون، ایلینویز و نورت‌ایسترن دریافته‌اند که این استانداردها امکان استفاده نامحدود و بی‌قیدوشرط را از **حسگرهای گوشی همراه** فراهم کرده و وب‌سایت‌ها از این موضوع بهره‌برداری می‌کنند. بررسی هزاران وب‌سایت نشان داده در ۳۶۹۵ وب‌سایت، اسکریپ‌هایی گنجانده شده که امکان دسترسی وب‌سایت به یک یا چند حسگر گوشی را فراهم می‌کند که در بین این وب‌سایت‌ها، نام‌های معروفی هم دیده می‌شود. زمانی‌که نقشه گوگل را با استفاده از مرورگر باز می‌کنید، مرورگر هشدار می‌دهد این وب‌سایت می‌خواهد به مکان شما دسترسی داشته باشد. اما در زمان استفاده از سایر حسگرها نظیر **حسگرهای حرکتی**، روشنایی یا مجاورت، چنین هشداری به کاربر داده نمی‌شود. در نتیجه، مرورگر می‌تواند به‌طور مخفیانه به این دسته از حسگرها دسترسی داشته باشد. دسترسی به اطلاعات جمع‌آوری‌شده از این حسگرها به تنهایی حریم خصوصی کاربر را تهدید نمی‌کند و این داده‌ها فقط زمانی جمع‌آوری می‌شوند که کاربر از مرورگر استفاده کند. اما به عقیده محققان، این داده‌های جمع‌آوری‌شده، به یک وب‌سایت مهاجم امکان می‌دهد که حمله‌های متنوعی را اجرا کند. برای مثال، از داده‌های جمع‌آوری شده با **حسگر** نوری گوشی متوجه شود که کاربر چه چیزی را مرور کرده یا با استفاده از داده‌های **حسگر حرکتی**، کدهایی نظیر PIN را حدس بزند.



بر اساس استانداردهای کنسرسیوم شبکه جهانی وب (World Wide Web Consortium) داده‌های این **حسگر**ها آن اندازه مهم نیستند که استفاده از آن‌ها نیازمند تأیید کاربر باشند، اما این گروه تحقیقاتی اذعان می‌کند که افشای این داده‌ها ممکن است حریم خصوصی کاربران را به خطر اندازد. این محققان بعد از بررسی ۹ مرورگر از جمله کروم، Edge، سافاری، فایرفاکس و اپرا مینی به این نتیجه رسیده‌اند که این مرورگرها دسترسی غیرمجاز سایت‌ها را به **حسگرهای حرکتی** و جهت گوشی فراهم می‌کنند. مرورگر فایرفاکس در نسخه‌های اخیر خود، اجازه دسترسی به **حسگر**های مجاورت و نوری را نیز به سایت‌ها می‌دهد. این مرورگر در نسخه ۶۰ (مه ۲۰۱۸) این دسترسی پیش‌فرض را حذف کرده است.

مطلب پیشنهادی

استخراج خودکار اطلاعات شخصی کاربران

محققان دریافته‌اند، نرم‌افزارهای مسدودکننده تبلیغات و ردیابی در مسدود کردن چنین اسکریپت‌هایی موفق نیستند. برخی از این کدهای مخفی در عمل خطرناک نبوده و در مواردی نظیر تنظیم جهت صفحه سایت یا تشخیص اشاره‌های کاربر استفاده می‌شوند. بعضی از آن‌ها حتی برای تولید اعداد تصادفی به‌کار می‌روند. اما برخی از این کدها به‌منظور کمک به ردیابی، تجزیه‌وتحلیل و شناخت رفتار کاربران استفاده می‌شوند. این محققان اعلام کرده‌اند، انتظار نداشته‌اند این تعداد از سایت‌ها و دامنه‌های اینترنتی را بیابند که مشغول استفاده مخفیانه از داده‌های **حسگر** گوشی کاربران هستند.

محققان در بررسی‌های خود با اسکریپ‌هایی هم مواجه شده‌اند که هنوز درنیافته‌اند به چه دلیلی این داده‌ها را جمع‌آوری می‌کنند. علاوه بر این، در نرم‌افزارهای تبلیغاتی سایت‌هایی نظیر وایرد، سی‌ان‌ان، لس‌آنجلس‌تایمز و سی‌نت نیز احتمالا اسکریپ‌هایی با هدف جمع‌آوری داده **حسگر**های گوشی کاربران گنجانده شده است. این محققان معتقدند، جمع‌آوری اطلاعات توسط سایت‌ها در بسیاری از موارد قانونی است، اما این‌که این کار بدون اجازه کاربران انجام می‌شود و کاربر حق انتخاب ندارد، قابل‌تأمل است.

تاریخ انتشار:

14 آذر 1397

نشانی منبع:
https://www.shabakeh-mag.com/security/14202/%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%D8%AE%D9%81%DB%8C%D8%A7%D9%86%D9%87-

%D8%B3%D8%A7%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7-%D8%A7%D8%B2-
%D8%AD%D8%B3%DA%AF%D8%B1%D9%87%D8%A7%DB%8C-
%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