تولید بسته‌های امنیتی زمان و انرژی زیادی طلب می‌کند و ارائه این خدمات برای تمامی گوشی‌ها سال‌ها پس از عرضه محصول به بازار کاملا غیرمنطقی و غیراقتصادی است

قدیمی‌های ناامن

گوشی اندرویدی با سیستم‌عامل‌های به‌روز نشده امنیت شما را به خطر می‌اندازند

خشایار مریدپور
روزنامه‌نگار فناوری

افزایش خیره‌کننده قیمت گوشی‌های پرچمدار جدید مثل گلکسی S یا آیفون ۱۱ پرومکس که در گران‌ترین مدل‌ها بیش از هزار دلار قیمت دارند، باعث رونق بیش از پیش بازار گوشی‌های کارکرده و تعمیر شده قدیمی شده است. اما آیا خرید یک گوشی HTC، سامسونگ یا هوآوی مدل دو سه سال پیش با بدنه و باتری سالم، خوش‌قیمت و معمولا با امکانات مناسب ارزشش را دارد؟ در این شرایط عجیب که گوشی‌های قدیمی قیمتی معادل گوشی‌های نوی چند ماه پیش دارند، طبیعی است که بسیاری دنبال گوشی‌هایی باشند که بتوانند از پس خریدشان بربیایند. ولی آنچه بسیاری از خریداران نادیده می‌گیرند، خطرات و مشکلاتی است که استفاده از گوشی‌های کارکرده با سیستم‌عامل قدیمی می‌تواند برای امنیت و حریم خصوصی شما در دنیای دیجیتال امروز داشته باشد. در ادامه شما را با برخی از این تهدیدات آشنا می‌کنیم.

وصله‌پینه‌ها

بسته‌های امنیتی یا Patchهای به‌روزرسانی وقتی توسط سازندگان ارائه می‌شوند که هکرها در سیستم نقطه ضعفی پیدا کرده باشند. درواقع سازندگان با ارائه این وصله‌پینه‌های امنیتی به کاربران، حفره‌هایی را که می‌تواند برای ورود به سیستم و سوءاستفاده از اطلاعات آنها مورد استفاده قرار بگیرد، می‌بندند. از آنجا که مجرمان مجازی هرگز بیکار نمی‌نشینند و همواره دنبال یافتن روش‌های جدیدی برای نفوذ هستند، همه گوشی‌ها به‌مرور به‌روزرسانی‌هایی را از طرف سازندگان دریافت می‌کنند و این چرخه تا زمانی که سازنده به پشتیبانی از محصول خود متعهد باشد، ادامه پیدا می‌کند. در بیشتر مواقع شما از ارسال، دریافت و نصب این بسته‌های امنیتی اصلا خبردار نمی‌شوید، اما همین بسته‌ها، گوشی شما و سیستم‌عامل آن را به‌روز نگه می‌دارند و از شما در برابر تهدیدات پرشمار فضای مجازی محافظت می‌کنند.

وقتی چرخ از حرکت می‌ایستد

سازندگان گوشی‌های هوشمند از جمله سامسونگ، ال‌جی، هوآووی و... برای هر محصول دوره پشتیبانی محدودی درنظر می‌گیرند که دلایل مختلف اقتصادی و فنی دارد. هر گوشی جدیدی که بر بستر نسخه جدیدی از اندروید عرضه می‌شود تا مدتی نیازمند ارزیابی تهدیدات و وصله‌پینه کردن حفره‌های امنیتی خواهد بود. تولید این بسته‌های امنیتی زمان و انرژی زیادی طلب می‌کند و ارائه این خدمات برای تمامی گوشی‌ها سال‌ها پس از عرضه محصول به بازار کاملا غیرمنطقی و غیراقتصادی است. به‌علاوه زمان این دوره پشتیبانی به سازنده هم خیلی بستگی دارد؛ برای مثال گوشی‌های برند ال‌جی به‌نسبت بسیاری از برندهای دیگر به‌روزرسانی‌های بهتری را برای مدت طولانی‌تری دریافت می‌کنند، درحالی که HTC معمولا حتی زحمت ارتقاء سیستم‌عامل گوشی‌های تولید یک سال پیش را به خود نمی‌داد. در نتیجه تمام این موارد، گوگل و سازندگان گوشی‌های اندرویدی معمولا پس از یک بازه دو تا سه ساله مجبور به قطع پشتیبانی از گوشی‌های قدیمی‌تر می‌شوند تا بتوانند روند توسعه و به‌روزرسانی محصولات جدیدتر را ادامه دهند. این به آن معنی است که گوشی‌هایی که بیش از این زمان در بازار بوده‌اند، احتمالا دربرابر تهدیدهای جدید و ناشناخته آسیب‌پذیرتر از مدل‌های جدیدتر هستند.

از گوشی‌های قدیمی استفاده کنیم یا نه؟

از نظر فنی، استفاده از دستگاهی که دیگر به‌روزرسانی امنیتی دریافت نمی‌کند ایمن نیست، چراکه جزئیات جدیدترین حفره‌های امنیتی هر چند هفته یک‌بار در اختیار عموم قرار می‌گیرند. در نتیجه وقتی کاربران به استفاده از محصولی که دیگر پشتیبانی دریافت نمی‌کند، ادامه می‌دهند بیشتر در معرض آسیب‌های امنیتی قرار خواهند داشت. شاید این موضوع چندان جدی به‌نظر نیاید، اما واقعیت این است که امکان دارد چنین حفره‌هایی باعث دسترسی کامل افراد غیرمجاز به گوشی شما شده و باعث سرقت اطلاعاتی مثل ایمیل‌های شخصی و شرکتی، اطلاعات بانکی، مخاطبان، پیامک‌ها و دیگر اطلاعات شخصی و حساس شوند. اگر از گوشی‌ای استفاده می‌کنید که هکرها روش نفوذ به آن را بلدند و مثلا می‌توانند به‌سادگی از آن داده سرقت کرده یا روی آن بدافزار نصب کنند، این به آن معنی است که این نقطه ضعف دائمی همیشه با شما خواهد بود.

> از نظر فنی، استفاده از دستگاهی که دیگر به‌روزرسانی امنیتی دریافت نمی‌کند ایمن نیست، چراکه جزئیات جدیدترین حفره‌های امنیتی هر چند هفته یک‌بار در اختیار عموم قرار می‌گیرند

گوشی من هم آسیب‌پذیر است؟

فهمیدن این‌که آیا گوشی شما هنوز هم تحت پشتیبانی سازنده قرار دارد و به‌روزرسانی‌های امنیتی را دریافت می‌کند یا خیر، آن‌قدرها هم که به‌نظر می‌رسد سرراست نیست. برای شروع باید به قسمت تنظیمات گوشی بروید و به‌روزرسانی نرم‌افزاری گوشی یا Software Updates را کنترل کنید. معمولا در این قسمت می‌توانید جزئیاتی از قبیل آخرین باری که گوشی به‌روزرسانی شده و نسخه فعلی سیستم‌عامل را مشاهده کنید. اگر گوشی شما اعلام می‌کند که از آخرین نسخه استفاده می‌کند و به‌روزرسانی جدیدی برای سیستم شما موجود نیست، اما از تاریخ آخرین به‌روزرسانی چند ماه یا سال می‌گذرد، باید به فکر استفاده از یک گوشی جدید یا حداقل انتقال اطلاعات حساس خود به یک سیستم بهتر باشید. متاسفانه سازندگان به کاربران اخطاری درباره زمان پایان پشتیبانی از محصول نمی‌دهند و معمولا خودتان هستید که باید با کنترل مداوم از روند ارائه یا عدم ارائه به‌روزرسانی‌ها مطلع شوید. به‌طور کلی می‌توانید مطمئن باشید هر گوشی که بیش از دو سال عمر دارد دیگر تحت پشتیبانی سازنده نیست، هرچند ممکن است بعضی مدل‌ها حتی قبل از این مدت هم از پشتیبانی خارج شوند. از این لحاظ، اپل عملکرد بسیار بهتری دارد و با ارائه پشتیبانی از گوشی‌های ساخت تا پنج سال پیش، سطح بسیار بالاتری از امنیت و پشتیبانی را برای کاربران خود فراهم می‌کند.

چطور بفهمیم هک شده‌ایم یا نه؟

فهمیدن این موضوع اصلا ساده نیست، اما دقیق بودن و توجه به نشانه‌ها می‌تواند بسیار کارساز باشد. یکی از مهم‌ترین نشانه‌ها، پدیدار شدن نرم‌افزارهای ناشناخته‌ای است که هرگز نصب نکرده‌اید. استفاده غیرعادی از اینترنت، خالی شدن باتری و البته مشغول بودن پردازنده، همگی از نشانه‌های گوشی‌های هک شده هستند. از روش‌های مناسب برای اطمینان از امنیت گوشی‌های قدیمی می‌توانیم به دریافت و نصب آخرین نسخه از نرم‌افزارها از فروشگاه Play Store و نه هیچ فروشگاه اپلیکیشن دیگر، استفاده نکردن از نرم‌افزارهای مالی و بانکی روی گوشی‌های قدیمی و قرار ندادن اطلاعات شخصی روی آنها اشاره کنیم. راه‌حل همیشگی دیگر، رعایت جانب احتیاط و حفظ اصول امنیتی پایه در فضای دیجیتال است که ربطی به مدل و سال ساخت گوشی شما ندارد.