دسترسی هکرها به اطلاعات گوشی از طریق ساعت هوشمند

چگونه ساعت‌های هوشمند را امن کنیم؟

شهرت ساعت‌های هوشمند به‌سرعت در حال افزایش است؛ اما در این‌جا سؤالی مطرح می‌شود؛ آیا این پوشیدنی می‌تواند خطرات امنیتی جدی به‌همراه داشته باشد؟ در این مقاله به بررسی این موضوع می‌پردازیم.

چقدر طول می‌کشد تا شارژ باتری گوشی تمام شود؟ کدام گوشی برای من بهتر است؛ اپل یا اندروید؟ آیا می‌توانم با استفاده از آن پول غذایم را پرداخت کنم؟ در لیست پرسش و پاسخ‌های ساعت هوشمند جای نکته‌ای خالی مانده است؛ نکته‌ای که به‌شدت به چشم می‌آید: این گجت تا چه اندازه امن است؟

مطلب پیشنهادی

5 ترفند ساده برای افزایش طول عمر باتری ساعت‌های هوشمند اندرویدی

وقتی همه افراد از جمله مسئولان فناوری به تنها چیزی که فکر می‌کنند ویژگی‌های فوق‌العاده و مدت زمانی است که این ساعت‌های مچی می‌توانند شارژ نگه دارند؛ چه انتظاری می‌توان داشت که کسی بر امنیت ساعت هوشمند تأکید کند. آیا این وسایل هک‌شدنی هستند؟ آیا کسی قادر است آن‌ها را هک کند؟ آیا مستعد پذیرش بدافزارها هستند؟ اگر ساعت شما گم یا دزدیده شود ممکن است اطلاعات شخصیتان به‌راحتی فاش شود؟ آیا امکان دارد از راه دور بتوان اطلاعات آن را پاک کرد؟
شاید همه ما هرچند روز یک‌بار این‌گونه سؤالات را درباره گوشی‌های هوشمندی که در دست داریم بپرسیم؛ گوشی‌هایی که پوشیدنی‌ها می‌توانند با آن‌ها تعامل نزدیک داشته باشند. البته هنوز کسانی که از اولین خریداران این پوشیدنی بوده‌اند یا حتی رسانه‌ها که معمولاً از دامن زدن به داستان‌های هراس‌آور واهمه‌ای ندارند، به‌طور عجیبی درباره امنیت ساعت هوشمند سکوت کرده‌اند. به‌نظر می‌رسد که هر دو گروه چشم‌های خود را بر روی خطرات احتمالی بسته‌اند.

وقتی درباره امنیت ساعت هوشمند صحبت می‌شود، اولین مانعی که باید از پیش‌رو برداشته شود پذیرفتن جدی‌بودن این نگرانی است. شاید با خود بگویید گجتی که روی مچ دستتان قرار دارد صفحه‌مانیتور کوچک و احمقی است که با گوشی‌هوشمندتان در ارتباط است. این اولین چیزی است که به ذهن می‌رسد. به‌علاوه برخی می‌گویند اگر امنیت گوشی‌ای که در دست داریم در معرض خطر قرار نگیرد؛ برای ساعت هم اتفاقی نمی‌افتد.

مطلب پیشنهادی

این 19 بند زیبای جدید اپل واچ را تماشا و انتخاب کنید!

اما در دنیای واقعی داستان چیز دیگری است. این مسئله در تحقیقی که به‌تازگی محققان ترند مایکرو انجام داده‌اند کاملاً مشهود است. آن‌ها در تست‌های نفوذی که روی برخی از ساعت‌های هوشمند بنام بازار انجام دادند، متوجه شدند که امنیت این گجت‌ها از اهمیت بسیار زیادی برخوردار است. از جمله مدل‌هایی که در این تحقیق استفاده شدند می‌توان از ساعت اپل، موتورولا موتو 360 و ساعت پبل نام برد که از نظر محافظت سخت‌افزاری، ارتباطات اطلاعاتی و فضای ذخیره دیتای محلی بررسی شدند. یکی از مشاوران امنیت سایبری ترندمایکرو به‌نام «بارات‌میستری» در این‌باره می‌گوید: «کاملاً مشخص است که سازندگان و تولیدکنندگان، امنیت را فدای راحتی کرده‌اند. در تحقیقات صورت‌گرفته متوجه شدیم که تمام این ساعت‌ها اطلاعات را به‌صورت محلی ذخیره می‌کنند که اگر از محدوده گوشی که با آن در ارتباط است خارج شود؛ هکرها می‌توانند به‌راحتی به اطلاعات روی آن دسترسی داشته باشند.»

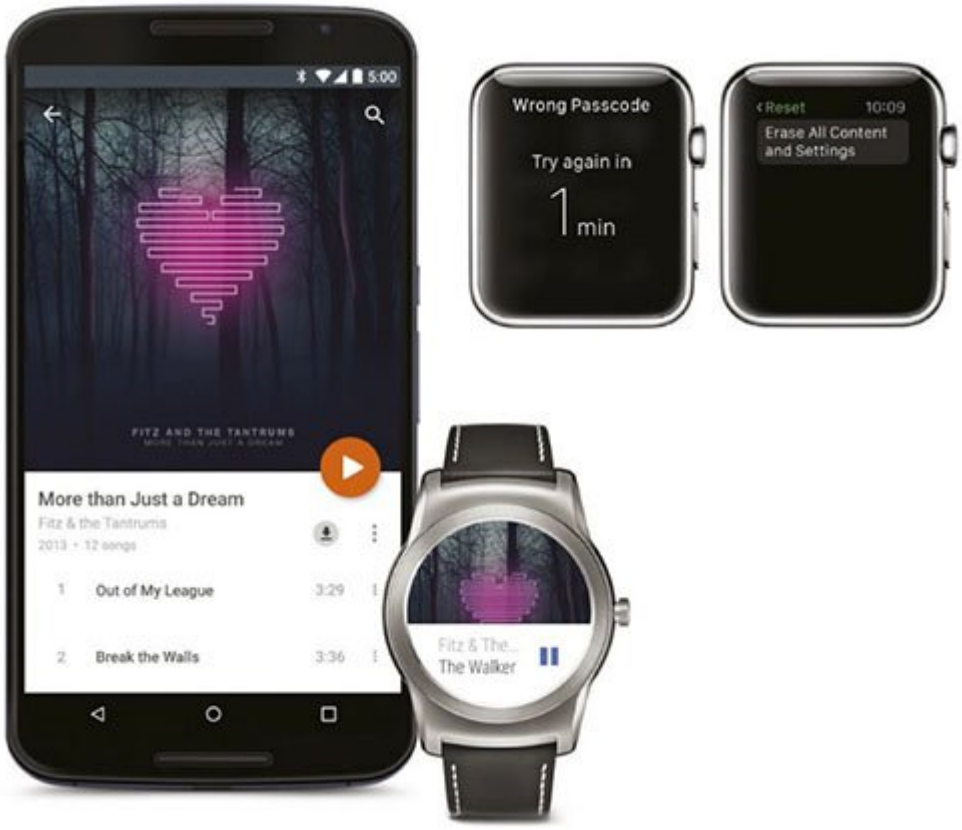
هم اپل و هم ساعت‌های اندرویدی نوتیفیکیشن‌های خوانده‌نشده را به همراه اطلاعات تناسب اندام و تقویم ذخیره می‌کنند. اپل به‌غیر از این موارد عکس؛ پس‌بوک (Passbook) و لیست مخاطبان را هم اضافه می‌کند. میستری درباره این مسئله هشدار می‌دهد و می‌گوید: «از آن‌جایی‌که اطلاعات پس‌بوک می‌تواند شامل موارد حساسی مانند بلیط پرواز باشد؛ دارندگان ساعت‌های هوشمند باید همان‌قدر که به گوشی‌های خود حساس هستند در قبال این وسیله هم حساسیت نشان دهند.»
توجه به این نکته که اطلاعات سینک شده می‌توانند از طریق اینترفیس ساعت هم قابل خواندن باشند، نگران کننده است؛ اما موضوعی که بیشتر باعث نگرانی و اضطراب می‌شود این است که ساعت اپل اطلاعات بیشتری را در مقایسه به مدل‌های اندرویدی ذخیره می‌کند. برخی عقیده دارند که ساعت‌های هوشمند فقط در محیط‌های خارج از محدوده گوشی، هوشمند هستند، اما تحقیق ترندمایکرو ثابت می‌کند که این تصور کاملاً غلط است.
به‌تازگی اچ‌پی هم تحقیقات اختصاصی خود را روی امنیت ساعت‌های هوشمند آغاز کرده و یافته‌های آن ممکن است چندان به مذاق خواننده خوش نیاید. تمام این ساعت‌ها نقاط ضعف زیادی دارند که امنیت آن‌ها را به‌خطر می‌اندازد؛ به‌طوری‌که اچ‌پی از آن‌ها به‌عنوان مزر جدید و باز برای حملات سایبری یاد می‌کند. اچ‌پی‌فورتیفای در گزارش خود از نگرانی‌هایش در این‌باره می‌گوید: «احراز هویت کاربر کافی نیست؛ اینترفیس‌های وب ناامن که به هکرها کمک می‌کند، با به‌کارگیری مکانیزم ریست‌کردن گذرواژه کاربران، حساب آن‌ها را هک کنند و اینکه رمزنگاری که روی اطلاعات ارسالی انجام می‌شود به‌شدت ضعیف و ناکارآمد است. مورد آخر برای کسانی‌که در صنعت امنیت هستند بسیار اهمیت دارد و نگرانی‌های زیادی را موجب شده است. با اینکه تمام گجت‌ها از SSL/TSL استفاده می‌کنند؛ اما نتیجه تحقیقات اچ‌پی نشان می‌دهد که ۴۰ درصد ساعت‌ها یا در برابر حملات POODLE آسیب‌پذیر هستند یا اینکه هنوز از پروتکل‌های قدیمی مانند SSL 2.0 استفاده می‌کنند.» سیمئون‌کانی مدیر استراتژی شرکت Adaptive Mobile معتقد است امکان پینگ‌کردن بدون مجوز پیغام‌های کاربران بیش از اندازه نگران کننده است. او در این‌باره می‌گوید: «یکی از اساسی‌ترین خطرات امنیتی که در ساعت‌های هوشمند دیده می‌شود همانی است که در

گوشی‌های هوشمند هم رایج است؛ اینکه کاربران را تشویق می‌کنند تا با نگاه کردن مختصر و اجمالی به نوتیفیکیشن‌ها جواب دهند. به این ترتیب هکرها می‌توانند با سودجویی از این رفتار از روش‌هایی برای تماس با کاربر استفاده کنند که اصلاً موشکافی نمی‌شوند. یعنی درست نقطه مقابل دریافت ایمیل روی پی‌سی که از همه نظر بررسی می‌شود.»

مطلب پیشنهادی

آشنایی با ترفندهای بیشتر Apple Watch
10 ترفند کمتر شناخته شده‌ای که می‌توانید با ساعت اپل انجام دهید!

او اضافه می‌کند: «هر نوع تعاملی که در آن کاربر اطلاعات کامل به‌منظور مشخص کردن دسترسی قانونی را نداده باشد یا اینکه خود دستگاه یا اکوسیستم اسکن امنیت را به‌طور خودکار قبل از ارسال آن انجام ندهد، می‌تواند آسیب‌پذیر باشد.»
نکته بعدی که با آن روبرو هستیم، ارائه فریم‌ورهای به‌روزرسانی بدون هیچ‌گونه رمزنگاری روی مکانیزم نقل‌وانتقال یا روی خود به‌روزرسانی‌هاست که می‌تواند دردسرساز شود. البته با توجه به اینکه بسیاری از به‌روزرسانی‌ها از امضای دیجیتالی برای جلوگیری از نصب مخرب‌ها استفاده می‌کنند، کمبود رمزنگاری به امکان دانلود آسان‌تر و آنالیز آن‌ها توسط خراب‌کاران کمک می‌کند. همچنین در این گزارش گفته شده که مقصر اصلی باز هم شرکت‌های سازنده و تولیدکننده هستند که به‌جای به‌کارگیری بسته‌های امنیتی مناسب، بیشتر بر طراحی و ویژگی‌های سخت‌افزاری ساعت‌ها تمرکز می‌کنند.
کن‌مانرو؛ شریک ارشد شرکای پن‌تست که یکی از حرفه‌ای‌ها در زمینه تست نفوذ است در این‌باره می‌گوید: «قسمتی از مشکلات امنیتی مرتبط با ساعت‌های هوشمند به تحول آن‌ها برمی‌گردد؛ تحولی که کمک کرده است سیستم‌های عامل به‌صورت مستقل به اینترنت وصل شوند. ما باید منتظر حملات هدفمند بیشتری باشیم. اپلیکیشن‌های ساعت هوشمند به‌گونه‌ای طراحی شده‌اند که به هر اجازه دسترسی، پاسخ مثبت می‌دهند؛ بنابراین اگر بدافزاری بتواند آپلود شود یا اینکه یک اپ مخرب روی ساعت نصب شود، قادر است به اطلاعات زیادی دسترسی داشته باشد. (شکل 1) آیا تهدید بدافزار بیشتر از آنکه متوجه ساعت باشد، به گوشی مربوط نمی‌شود؟ آیا مدرکی دال بر اینکه ساعت‌های هوشمند هدف حمله نویسندگان بدافزار قرار گرفته‌اند، وجود دارد؟» جمال‌هریس؛ مشاور امنیت اطلاعات MWR Labs می‌گوید: «در حال حاضر حملات زیادی روی ساعت‌های هوشمند صورت نمی‌گیرد؛ اما زمانی‌که کاربران شروع به استفاده از سیستم‌های پرداخت موبایلی کنند، این‌گونه حملات بیشتر می‌شود.»



1 □□□

هریس اضافه می‌کند که هم گوگل و هم اپل تلاش‌های زیادی برای مقابله با این حملات انجام داده‌اند تا از پخش بدافزار از ساعت به سمت گوشی جلوگیری کنند. اما اپلیکیشن‌ها می‌توانند به‌صورت مخفیانه روی برخی از ساعت‌های هوشمند نصب شوند و در برابر نرم‌افزارهایی که روی گوشی نصب و در حال اجرا است، رفتار متفاوتی داشته باشند و در نتیجه چالش آنالیز آن‌ها را برای کارشناسان مسائل امنیتی افزایش می‌دهد.
اما تنها دلیلی که باعث شده این ساعت‌ها از گزند حملات در امان بمانند، این است که برخلاف پیش‌بینی‌ها این گجت‌ها هنوز تبدیل به پدیده نشده‌اند. از نظر نرم‌افزار نیز هرچه سیستم‌عامل کوچک‌تر باشد؛ هدف از جذابیت کمتری برخوردار است. اما در مقابل، گوشی‌های هوشمند در مقایسه با ساعت‌های هوشمند عمومیت بیشتری دارند؛ اطلاعات حساسی که روی آن‌ها ذخیره می‌شود بیشتر است؛ قدرت پردازشی آن‌ها برای شروع حمله بهتر است و تماس مسقیم با شبکه‌های خارجی دارند.
کریس کامئو، مدیر NTT Com Security می‌گوید: «چرا باید فرد خود را برای هک کردن ساعت هوشمند به زحمت بیندازد؟ زیرا هم این کار نسبت به گوشی سخت‌تر است و هم اطلاعاتی که از آن به‌دست می‌آید بسیار ناچیز و کم‌اهمیت است. تنها چیزی که می‌توانم به آن فکر کنم آسیب‌پذیری ساعت هوشمند است که به‌شدت ساده و آسان است؛ اما چنین مشکلاتی می‌توانند به‌سرعت رفع شود.»

حریم خصوصی در معرض نمایش

اگر بدافزار برای اطلاعات شما تهدید به‌حساب نمی‌آید؛ پس برای خود شما تهدید است. لحظه‌ای به این مسئله فکر کنید که چه کسی جز شما از متن‌ها و ایمیل‌هایی که روی دستتان نمایش داده می‌شود باخبر است؟ کدهای احراز هویت، دو عاملی که به‌صورت اخطار روی صفحه ظاهر می‌شوند، چه نقشی می‌توانند داشته باشند؟ آیا به اشتراک‌گذاری غیرعمدی اطلاعات که به آن گشت وگذار شانه‌ای هم گفته می‌شود؛ می‌تواند تهدیدی جدی برای حریم خصوصی کاربر باشد؟ کریس‌کامئو معتقد است این مسئله که ساعت هوشمند همیشه روشن است، به‌خودی‌خود خطر بیشتری را در مقایسه با گوشی متوجه آن می‌کند. ساعت همیشه روی مچ بسته شده است؛ اما گوشی می‌تواند در جیب یا کیف قرار داشته باشد. بسیاری از این اطلاعات می‌تواند باعث شرمندگی و خجالت‌زدگی کاربر شود. استفاده از کدهای دوعاملی بدون PIN، گذرواژه یا مجوز هیچ فایده‌ای ندارد.
اما بارات میستری نظری خلاف کامئو دارد. او از زاویه حفظ حریم اطلاعات به این مسئله نگاه می‌کند و هشدار می‌دهد که هنوز کنترل روی این دستگاه‌ها بسیار خام و ناپخته است؛ بنابراین خطر اشتراک‌گذاری اطلاعات به‌صورت

غیرعمد به‌شدت افزایش می‌یابد. اگر کاربری فراموش کند دستگاه خود را قفل کند؛ این احتمال وجود دارد که دیگران بتوانند نوتیفیکیشن‌های روی صفحه را ببینند.
در واقع، زمانی‌که بحث مراقبت و محافظت از حریم شخصی پیش می‌آید، قفل کردن صفحه بهترین گزینه است. برای مثال، پوشیدنی اندروید با همان قفل صفحه‌ای عرضه می‌شود که در لالی‌پاپ گوشی‌های هوشمند آن وجود دارد. جمال‌هریس در این‌باره می‌گوید: «قفل‌کردن گوشی می‌تواند مانع خواندن پیغام‌ها توسط فرد حمله کننده شود. با وجود این، اگر قفلی روی ساعت گذاشته نشود؛ حتی یک نظر اجمالی می‌تواند اطلاعات بسیار حساسی را فاش کند.»

[illegible]

اما حفاظت از اطلاعات چگونه می‌تواند آسیب‌پذیر باشد؟ سینک‌کردن اطلاعات بین بلوتوث و وای‌فای هم می‌تواند ریسک دیگری باشد. سیمئون کانی می‌گوید: «این مسئله نیز می‌تواند روش دیگری برای حمله فراهم کند. اما بحث فاصله در این مورد دخیل است، چون هر دو ویژگی برد محدودی دارند و نمی‌توانند از یک حد بیشتری کارایی داشته باشند.» حالا می‌رسیم به ایردراپ اپل. هم‌اکنون مشخص شده که این سرویس اپل برای ارسال محتوای ناخواسته به کاربران استفاده می‌شود. اگر ایردراپ بتواند راه خود را به ساعت هوشمند باز کند، می‌تواند با ارسال تقاضای به‌ظاهر واقعی برای پین‌کد؛ گذرواژه یا مجوزهای لازم پیغام‌های آلوده و مخرب خود را ارسال کند.»
شاید بزرگ‌ترین خطر حریم شخصی، دزدی باشد. از آنجا که ساعت دور مچ بسته می‌شود احتمال گم‌کردن آن در مقایسه با گوشی کمتر است. اما اگر بند آن پاره شود یا اینکه فراموش کنید هنگام خارج شدن از مکان‌های عمومی مانند هتل که احتمال باز کردن ساعت از دست زیاد می‌شود، آن را بردارید خطر حتماً شما را تهدید می‌کند. اسکات لستر، محقق ارشد در امنیت اطلاعات محتوا می‌گوید: «برای کاربران اپل گزینه مرا پیدا کن وجود ندارد، اما یکی از ویژگی‌هایی که روی آن گذاشته شده این است که اگر ۱۰ بار پشت‌سرهم تلاش ناموفق برای وارد شدن به گوشی رخ دهد، اطلاعات آن به‌طور خودکار پاک می‌شود. در مورد پوشیدنی اندرویدی؛ کاربران می‌توانند وسایلی را که مستقیماً به وای‌فای متصل می‌شوند از کار بیندازند؛ هرچند که راهی برای پاک کردن اطلاعات روی آن وجود ندارد.»

حمله اپی

و سرانجام به اپ‌ها و گاردهای امنی می‌رسیم که در قالب طراحی اپ درست شده‌اند تا بتوانند جلوی حملات را بگیرند. مارک جیمز، متخصص امنیت در شرکت ایست (East)، متقاعد شده است که بدون شک اپ‌ها، بزرگ‌ترین شکستی‌ای هستند که در این بازار دیده خواهند شد.
به گفته MWR Labs، توسعه‌دهندگان اغلب درباره تغییراتی که در گوشی‌های هوشمند داده شده تا بتوانند به‌راحتی با ساعت‌های مربوطه در ارتباط باشند آگاهی ندارند. جمال‌هریس در توضیح این مطلب می‌گوید: «در پوشیدنی اندرویدی، توسعه‌دهندگان ملزم به ساخت و تعبیه سرویسی در اپ خود هستند تا بتواند بستر لازم را برای برقراری ارتباط و تبادل اطلاعات بین اندروید و پوشیدنی اندروید فراهم کند. از نظر تئوری، این سرویس فقط می‌تواند توسط پوشیدنی اندروید استفاده شود اما در تحقیقات ما مشخص شد که امکان ارتباط این سرویس با پوشیدنی روت‌شده نیز وجود دارد.» (شکل 2)

2 □□□

با توجه به اینکه ضعف یکی، می‌تواند روی دیگری نیز تأثیرگذار باشد؛ نکته مهم اینکه نیاز است چک‌های امنیتی نظیر شناسایی روت روی اپ‌هایی که برای پوشیدنی‌ها و سیستم‌عامل اندروید نوشته می‌شود،انجام گیرد. جمال اضافه می‌کند: «در مورد ساعت اپل، MWR توسعه‌دهندگانی را دیده که از روی عمد، موارد امنیتی را روی اپلیکیشن‌های iOS ضعیف می‌کنند تا به این ترتیب اطلاعات حساس‌وحیاتی به ساعت هوشمند منتقل شود. یکی از وظایف مهم و خطیر سازندگان این‌گونه ساعت‌ها آن است که مطمئن شوند این اپ‌ها تمیز هستند و از منابع شناخته شده و معتبر گرفته شده‌اند.» در خاتمه مارک جیمز می‌گوید: «تنها راه محافظت از کاربران اطمینان حاصل کردن از طراحی اپ و دقت در ارسال و انتشار آن‌ها است.»

اما کارشناسان به کدام ساعت‌ها اعتماد دارند؟

آیا کارشناسان امنیتی یک پلتفرم ساعت هوشمند را به دیگری ترجیح می‌دهند؟ بهتر است با هم نظرات آن‌ها را بخوانیم.

بارات میستری از ترندمایکرو از اپل پشتیبانی می‌کند

محافظت فیزیکی از این دستگاه در بین تمام تولیدکنندگان آن ضعیف و کمتر از سطح انتظار است. در تحقیقاتی که روی مدل‌های مختلف داشتیم، هیچ‌کدام از آن‌ها به‌صورت پیش‌فرض از احراز هویت از طریق گذرواژه یا سایر روش‌ها استفاده نمی‌کنند. پس اگر این پوشیدنی دزدیده شد همه چیز در دسترس خواهد بود. تمام ساعت‌ها به جز ساعت اپل فاقد سیستم تایم‌اوت بودند؛ یعنی گذرواژه‌ها فقط از طریق کلیک دستی روی دکمه فعال می‌شوند که موجب می‌شوند درصد آسیب‌پذیری دستگاه بالا برود. همچنین در صورتی‌که روی ساعت اپل چندین بار تلاش نافرجام ورود داشته باشید، دستگاه به‌طور خودکار پاک می‌شود.

پل لمسوریر از کرول‌أنترک به هیچ‌کدام از این ساعت‌ها اطمینان ندارد

بدون درنظر گرفتن برند یا سیستم‌عامل، ساعت‌های هوشمند ذاتاً با مشکلات امنیتی عدیده‌ای همراه هستند.
اینترفیس آن‌ها ناامن است یا اینکه سیستم احرازهویت مناسبی ندارند.
البته تنها نکته مثبت آن است که می‌توان به‌راحتی این گجت‌ها را هک کرد ولی اطلاعات زیادی نمی‌توان از آن‌ها به‌دست آورد. فعلاً کاربران باید نگران مکان‌هایی باشند که اطلاعاتشان ذخیره و به‌اشتراک گذاشته می‌شود. چون هدف نهایی هکرها سیستم ابری است که سازندگان استفاده می‌کنند.

کریس‌کامئو از NTT Com Security از اپل پشتیبانی می‌کند

اگر به گذشته نگاه کنیم، می‌بینیم که روش اپل برای مقابله با خطرات امنیتی در گوشی‌های آی‌فون با موفقیت بیشتری همراه بوده است. پلتفرم بسته، سیستم اپل استور حفاظت شده، بستن سریع جیل‌بریک و سایر مشکلات امنیتی در کنار طراحی کلی نرم‌افزار باعث شده تا آی‌فون‌ها در برابر حملات و خطرات امنیتی مقاوم باشند. درمقابل سیستم اندروید بسیار تکه‌تکه و از هم جداست و پیوسته کردن مداوم آن کاری بس دشوار. در نتیجه بسیاری از بدافزارها روی اندروید اثر می‌گذارند، اما نمی‌توانند گزندی به iOS برسانند. دور از انتظار نیست که همین رویه ادامه داشته باشد و شاهد ساعت‌های اپل با امنیت بیشتر و پلتفرم محدودتر باشیم؛ در حالی‌که اندروید کاملاً باز است و خطرات بیشتری آن را تهدید می‌کند

تاریخ انتشار:
10 فروردین 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3150