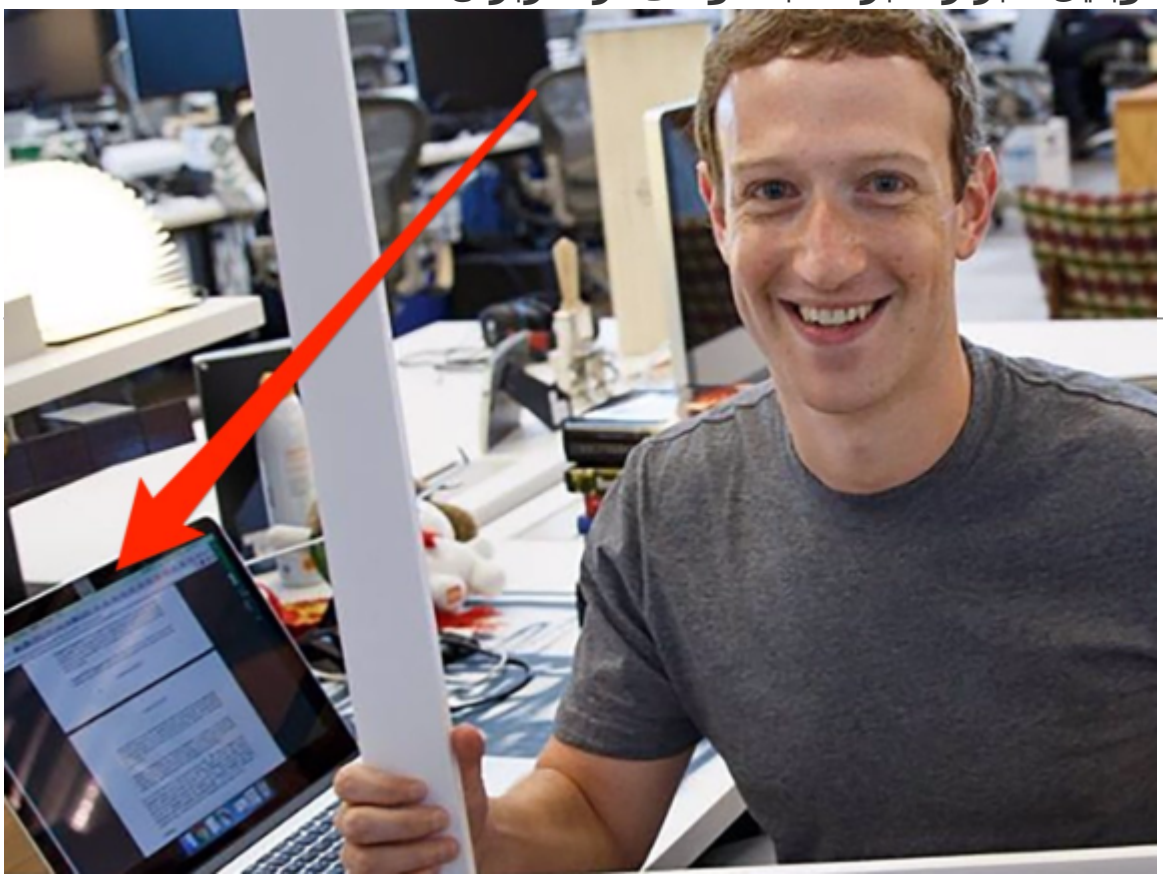
دوربین‌های موبایل؛ ابزاری برای جاسوسی از کاربران



بسیاری از مردم وقتی بطور اتفاقی متوجه شدند مارک زاکربرگ دوربین لپ‌تاپ خود را با چسب پوشانده است، فهمیدند که وب‌کم‌ها و دوربین ابزارهای همراه، ترسناک‌تر از آن چیزی هستند که به نظر می‌آیند. یک محقق حوزه امنیت اعلام کرده است نرم‌افزارهایی که بر روی گوشی‌ها و تبلت اپل نصب می‌شوند، قادرند به سادگی از کاربران خود « جاسوسی تصویری» کنند و عکس‌ها و ویدیوهای بدست آمده را به روش‌های گوناگون تجزیه و تحلیل کرده و اطلاعات مهمی را از آن‌ها استخراج کنند.

ما در زمان دانلود یا نصب یک نرم‌افزار موبایل نظیر یک پیام‌رسان یا حتی یک خبرخوان، مجموعه‌ای از اختیارات را به آن اعطا می‌کنیم که از جمله آنها، دسترسی به دوربین گوشی است. وقتی به یک نرم‌افزار اجازه دسترسی به دوربین گوشی خود را می‌دهید، آن نرم‌افزار می‌تواند به هر دو دوربین اصلی و سلفی دسترسی پیدا کند، بدون اطلاع شما عکس بگیرد یا ویدیو تهیه کند و بدون معطلی، عکس‌ها و ویدیوهای شما را روی سرور خود بارگذاری کند یا بطور زنده بر روی اینترنت پخش کند. البته این همه داستان نیست. چنین نرم‌افزارهایی امکان ردیابی و تشخیص چهره را نیز دارند بطوریکه می‌توانند ویژگی‌ها و حالات چهره کاربر خود را شناسایی کنند. بدین ترتیب نرم‌افزار مهاجم، اطلاعاتی نظیر اینکه کاربر در آن لحظه مشغول چه کاری است یا در چه محلی حضور دارد را به دست خواهد آورد. بارگذاری تصادفی تصاویر روی سرور نرم‌افزار و استفاده از الگوریتم‌های تشخیص چهره این امکان را به مهاجم می‌دهد تا تصاویر دیگری از کاربر که روی اینترنت موجود است را نیز بدست آورد و حتی مدلی سه‌بعدی از چهره وی بسازد.


HoT
08:31
Feed
Empty
Raw

با کمک فریم‌ورک Vision آی‌اواِس، با یک برنامه ساده می‌توان اطلاعات چهره کاربر را استخراج کرد.

با توجه به اینکه سخت‌افزار گوشی‌ها و تبلت‌های اپل به نسبت قدرتمند هستند، از کدک‌های پیشرفته‌ای استفاده می‌کنند و دسترسی به اینترنت پرسرعتی دارند یک کاربر عادی به سختی متوجه خواهد شد که ویدیوی وی بطور زنده روی اینترنت در حال پخش است. اگر این نظارت تصویری با نوع محتوایی که کاربر در آن لحظه استفاده می‌کند ترکیب شود، حالات روحی او نیز قابل تشخیص خواهد بود. حتی می‌توان حضور افراد دیگر را هم در محل تشخیص داد. هر برنامه‌سازی می‌تواند با استفاده از فریم‌ورک Vision نسخه iOS 11، در لحظه ویژگی‌های چهره نظیر چشم‌ها، دهان و ... را تجزیه و تحلیل کند.

نمونه‌ای از یک لنز «پوشش لنز دوربین» که در بازار موجود است.

شاید ساده‌ترین و البته بهترین روش مقابله با چنین حملاتی، پوشاندن دوربین با نوار چسب باشد! البته برای این کار محصولات ویژه‌ای هم به بازار عرضه شده است. راهکار دیگر این است که به نرم‌افزار اجازه ندهیم که به دوربین گوشی دسترسی پیدا کند. می‌توان در صورت لزوم، عکس را با نرم‌افزار پیش‌فرض گوشی گرفته و از آن عکس در نرم‌افزارهای دیگر استفاده کنیم. البته اینکار مشکل دیگری به بار می‌آورد و آن لو رفتن موقعیت مکانی شماست. زیرا وقتی با گوشی خود عکسی می‌گیریم موقعیت مکانی محل نیز در عکس ذخیره می‌شود.

منبع تصویر ابتدای مطلب : بیزینس‌اینسایدر

منبع:
وب‌سایت Felix Krause
تاریخ انتشار:
04 آبان 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/10375/%D8%AF%D9%88%D8%B1%D8%A8%DB%8C%D9%86%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D9%88%D8%A8%D8%A7%DB%8C%D9%84%D8%9B-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C-%D8%A7%D8%B2-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86