بسمه تعالی

تنظیم وای‌فای به IMSI Catcher برای ردیابی تلفن همراه کاربران در هر کجا

تنظیم وای‌فای به IMSI Catcher برای ردیابی تلفن همراه کاربران در هر کجا

Wi-Fi can be turned into IMSI Catcher to Track Cell Phone Users Everywhere

پنج‌شنبه ۳ نوامبر ۲۰۱۶، تهیه کننده: Swati Khandelwal

یک خطر جدید برای امنیت گوشی شما وجو دارد: گوشی شما هک و ردگیری می‌شود، بدون آنکه شما با خبر باشید.
بیاد دارید Stingrays (http://thehackernews.com/2015/04/police-spying-cell-phones.html)؟

ابزار جاسوسی تلفن همراه بحث‌برانگیز IMSI catchers، مدتی مدیدی هست که بوسیله مجریان قانون، جهت ردیابی و نظارت کاربران موبایل از طریق شبیه‌سازی یک دکل تلفن همراه و فریب دادن دستگاه‌ها که به آن متصل شوند، استفاده می‌شود. بعضی موارد حتی تماس‌ها و ترافیک اینترنت را دنبال می‌کند، متون جعلی ارسال کرده و نرم‌افزارهای جاسوسی بر روی تلفن یک قربانی نیز نصب می‌کند.
تنظیم کردن چنین دستگاه‌های نظارتی، پرهزینه هست و به یک مجموعه‌ای از اعمال نیاز دارد ولی امروزه محققان راه جدید و کم‌هزینه‌ای را پیدا کرده‌اند که همان کار را با کمک یک وای‌فای هاتاسپات (Wi-Fi hotspot) انجام دهند.

https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-7983783048239650&output=html&h=90&slotname=1876319540&adk=4188127572&adf=2806745235&w=200&lmt=1482425204&flash=24.0.0&url=http%3A%2F%2Fthehackernews.com%2F2016%2F11%2Fimsi-track-cellphone.html&wgl=1&dt=1482456204510&bpp=7&bdt=846&fdt=1482&idt=1509&shv=r20161205&cbv=r20161129&saldr=aa&prev_fmts=200x90_0ads_al&correlator=3720632664529&frm=20&ga_vid=*&ga_sid=*&ga_hid=*&ga_fc=1&pv=1&icsg=2&nhd=1&dssz=2&mdo=0&mso=0&u_tz=210&u_his=12&u_java=1&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=1&u_nmime=2&dff=times%20new%20roman&dfs=16&biw=1349&bih=599&rx=0&eae=0&fc=16&pc=1&brdim=0%2C106%2C-8%2C-8%2C1366%2C%2C1382%2C744%2C1366%2C599&vis=1&rsz=%7C%7CoeEr%7C&abl=CS&ppjl=f&pfx=0&fu=1040&bc=1&ifi=2&xpc=BF155YEPLD&p=http%3A//thehackernews.com&dtd=1529&rl_rc=true&adsense_enabled=true&ad_type=text&oe=UTF8&format=fpkc_al_lp&kw_type=radlink&hl=en&kw0=Track+Phone+Number&kw1=How+to+Track+a+Cell+Phone&kw2=GPS+Locate+Cell+Phone&okw=How+to+Track+a+Cell+Phone&rt=ChBYXHyPAAzHTQp3i93AB0qCEhIIb3cgdG8gVHJhY2sgYSBDZWxsIFBob25lIGgjHSfQVNDpP0SgBUhMI4e-b3ZOJ0QIVmZp3Ch2NWgRy

https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-7983783048239650&output=html&h=90&slotname=1876319540&adk=4188127572&adf=2806745235&w=200&lmt=1482425204&flash=24.0.0&url=http%3A%2F%2Fthehackernews.com%2F2016%2F11%2Fimsi-track-cellphone.html&wgl=1&dt=1482456204510&bpp=7&bdt=846&fdt=1482&idt=1509&shv=r20161205&cbv=r20161129&saldr=aa&prev_fmts=200x90_0ads_al&correlator=3720632664529&frm=20&ga_vid=*&ga_sid=*&ga_hid=*&ga_fc=1&pv=1&icsg=2&nhd=1&dssz=2&mdo=0&mso=0&u_tz=210&u_his=12&u_java=1&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=1&u_nmime=2&dff=times%20new%20roman&dfs=16&biw=1349&bih=599&rx=0&eae=0&fc=16&pc=1&brdim=0%2C106%2C-8%2C-8%2C1366%2C%2C1382%2C744%2C1366%2C599&vis=1&rsz=%7C%7CoeEr%7C&abl=CS&ppjl=f&pfx=0&fu=1040&bc=1&ifi=2&xpc=BF155YEPLD&p=http%3A//thehackernews.com&dtd=1529&rl_rc=true&adsense_enabled=true&ad_type=text&oe=UTF8&format=fpkc_al_lp&kw_type=radlink&hl=en&kw0=Track+Phone+Number&kw1=How+to+Track+a+Cell+Phone&kw2=GPS+Locate+Cell+Phone&okw=Track+Phone+Number&rt=ChBYXHyPAAzHRQp3i93AB0qCEhJUcmFjayBQaG9uZSBOdW1iZXIaCOiFkrsbYSudKAFSEwjh75vdk4nRAhWZmncKHY1aBHI

شبکه وای‌فای می‌تواند شماره IMSI گوشی‌های نزدیک را بگیرد و امکان ردیابی و نظارت اشخاص را فراهم کند.

IMSI یا شناسه مشتری موبایلی بین‌المللی، یک شماره منحصربفرد ۱۵ رقمی هست که برای تایید هویت اشخاص، وقتی از یک شبکه به شبکه دیگر منتقل می‌شوند، بکار می‌رود. این شماره در بخش فقط-خواندنی کارت SD و با اپراتور همراه، ذخیره می‌شود. توجه شود که این عدد با IMEI اشتباه نشود. IMSI به کاربر ولی IMEI به دستگاه مرتبط هست.

سرقت اثر انگشت خود برای ردیابی خود در هرکجا

Piers O'Hanlon و Ravishankar Borgaonkar از دانشگاه اکسفورد، در نشست کلاه قرمزان اروپا، یک نوع جدید از حمله IMSI catcher ارائه کردند که بر روی وای‌فای عمل می‌کند، و این امکان را فراهم می‌کند که هر شخصی، در حالی‌که کاربر دور زده می‌شود، شماره IMSI گوشی را در مدت چند ثانیه بدست آورد.
آن شماره IMSI، سپس جهت جاسوسی حرکت‌های کاربر استفاده می‌شود. آن چیزی که لازم هست، نحوه اتصال دستگاه‌های جدید مانند اندروید و iOS، به شبکه‌های وای‌فای هست.
(https://www.ispsystem.com/software/dcimanager?gclid=CLW_4eyUidECFXgW0wodajoM7g)

دو پروتکل متداول بعدی برای اتصال به وای‌فای پیاده‌سازی شده هست:

- پروتکل Extensible Authentication Protocol (EAP)
- پروتکل Authentication and Key Agreement (AKA)

این پروتکل‌ها، امکان اتصال گوشی به وای‌فای عمومی را فراهم می‌کنند. گوشی‌های هوشمند جدید طوری برنامه‌نویسی شده‌اند که به طورخودکار به شبکه‌های Fi-Wi مشهور، با کمک شماره IMSI برای لاگین به شبکه و بدون تعامل با کاربر، وصل می‌شوند. بنابراین هکرها با استفاده از پروتکل‌های تایید هویت وای‌فای، می‌توانند امکان برقراری یک نقطه دسترسی نادرست، که شبکه وای‌فای را پوشش می‌دهد و گوشی‌ها در محدوده‌اش را نیز فریب می‌دهد تا به آن متصل شوند.

یکبار که به نقطعه دسترسی جعلی متصل شدند، شماره IMSI آنها ربوده خواهد شد. این شماره منحصر بفرد گوشی ربوده‌شده، این امکان را فراهم می‌کند که هکر حرکت دارنده گوشی را ردیابی کند.

جلوگیری از ربودن شماره شناسه یگانه از طریق وای‌فای

محققین نوع دیگری از حمله را توصیف کردند که هکرها قادرند فراخوانی (calling) وای‌فای که بوسیله اپراتورهای موبایل فراهم شده است را بربایند (hijack). این فناوری از فراخوانی صوتی که بوسیله WhatsApp یا Skype از طریق VOIP انجام می‌شود، متفاوت هست.

در حالی‌که فراخوانی وای‌فای که بر روی دستگاه‌های iOS و اندروید پشتیبانی می‌شود، امکان آن را فراهم می‌کند که کاربران فراخوانی صوتی از طریق وای‌فای بوسیله ارتباط با Edge Packet Data Gateway (EPDG) اپراتوری که پروتکل رمزشده IPSec را استفاده می‌کند، انجام دهند.

مانند ویژگی اتصال خودکار وای‌فای، پروتکل مبادله کلید اینترنت (Internet Key Exchange: IKEv2) که برای تایید اصالت فراخوانی وای‌فای بکار می‌رود، نیز بر اساس شناسه‌ای مانند شماره IMSI هست، که با EAP-AKA مبادله می‌شود. مبادلات EAP-AKA به صورت رمز شده هست ولی مشکل این هست که بوسیله یک گواهی محافظت نشده هست.

محققین می‌گویند که این جنبه، ویژگی حمله مرد میانی (MITM) را نشان می‌دهد که این امکان را فراهم می‌کند تا هکرها ترافیک یک گوشی که سعی در فراخوانی بر روی وای‌فای دارد را قطع کنند و سریعا و در چند ثانیه شماره IMSI را استخراج کنند.

اخبار خوب این هست که شما قادرید ویژگی فراخوانی وای‌فای بر روی گوشی خود را غیرفعال کنید ولی اتصال خودکار وای‌فای فقط وقتی غیرفعال می‌شود که چنین شبکه‌ای در محدوده باشد.

محققین این موضوع را به شرکت‌های سیستم‌عامل موبایل مانند Apple، Google، Microsoft و Blackberry واپراتورهایی مانند GSMA، گزارش کردند و در حال همکاری با آنها هستند تا از محافظت شماره IMSI اطمینان حاصل کنند.

اپل به عنوان نتیجه مباحثات با محققین یک فناوری جدید در iOS10 پیاده‌سازی کرد که اجازه مبادله شبه‌نام‌ها به جای شناسه می‌دهد، که باعث کاهش آن تهدید می‌شود.

این تحقیقات نشان می‌دهد که IMSI catcher، تکنیک‌های غیرفعال را مانند فعال بکار می‌گیرد (https://www.blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf).