نویسنده

محمد نصیری

۱,۹۱۶ ۴۲۷ ۸۶۰ ۱۲,۲۹۷

محمد نصـیری ، بنیانگذار توسینسو ، کارشناس امنیت اطلاعات و ارتباطات و کشف جرائم رایانه ای ، هکر کلاه سفید ، بیش از ۱۲ هزار ساعت سابقه تدریس در بیش از ۴۰ سازمان دولتی ، خصوصی و نظامی ، علاقه مند به یادگیری بیشتر و عاشق محیط زیست

هکرها فقط با داشتن شماره تلفن شما را هک می کنند ! SS7 چیست؟

۲۱۲۹۲ ۴

قبلاـ در خصوص جاسوسـی و انواع آن و همچنین سـرویس هـای اطلاعـاتی دنیا که به حریم [illegible] در ITPRO مطـالبی نوشـته ایم امـا اینبـار در خصوص سیسـتم عامل یا یک وب سایت خاص نمی خواهیم صـحبت کنیم ، امروز می خواهیم در خصوص امنیت سرویس های زیرساختی مخابراتی و ارتباطی صحبت کنیم که هر روزه از آنها در حال استفاده هستیم.

تصور کنید که هکرها می توانند تمامی حرکات شـما را مو به مو مشاهده کنند و تمامی تماس های تلفنی شـما را نیز شنود کنند و اینکار را صـرفا با داشتن شماره تلفن شما می توانند انجام بدهند. بله ، فقط با داشتن شماره تلفن شما و بدون نیاز به نصب کردن کوچکترین نرم افزاری بر روی تلفن گوشـی همراه شـما و جالب اینجاست بدانیـد که هیچکاری از دست شـما هم بر نمی آید چون شما مسئول برقراری این سیستم ارتباطی نیستید ! این واقعا ترسناک است.

آیا واقعا ممکن است ؟ فقط با داشتن شماره تلفن ما را هک کنند ؟

واقعا ترسـناک است ، تصور کنید که تمامی حرکات شما توسط تبهکاران سایبری بررسی و جاسوسی شود. این سئوال پیش می آید که آیا این امر ممکن است ؟ پاسخ یک کارشناس امنیت اطلاعات آلمانی که در این خصوص تحقیقاتی انجام داده است بله است ، یکی از کارشناسان زبده امنیت اطلاعات که در آزمایشگاه تحقیقاتی امنیتی برلین آلمان مشغول است در این باره می گرد که اینکار بسـیار ساده است که تنها از طریق داشتن شماره تلفن شما یک هکر می تواند به تمامی مکالمات و اطلاعاتی که شما توسط گوشی رد و بدل می کنید دسترسی پیدا کند.

حتی برای اثبات این موضوع یکی از کارمندان این مرکز تحقیقاتی با یک گوشـی Apple ساده آزمایش شد و در نهایت ۶۰ دقیقه از

مکالمات این کارمند بصورت دقیق ثبت و ضبط و جاسوسی شد. اما یکی از کارشناسان امنیتی زبده به نام کارستن نوهل آلمانی که عضو تیم هکرهای این مرکز تحقیقاتی امنیتی است در اینباره اینطور می گوید که تبهکاران سایبری در اینگونه هک در واقع دستگاه های کاربران را هک نمی کنند بلکه از ضعف امنیتی که در سیستم های ارتباطاتی و زیرساختی مخابراتی وجود دارد استفاده می کنند و اصلا کاربر سهمی نمی تواند در برقراری امنیت این مکانیزم داشته باشد .

این آسیب پذیری بسیار خطرناک امنیتی به نام Signaling system Seven یا SSY معروف است که بصورت مجازی می تواند تقریبا هرگونه تلفنی را هک کرده و از آن جاسوسی کند. این آزمایش همانطور که گفتیم بصورت کاملا عملی بر روی تلفن همراه شخص داوطلب انجام شد و بعد از استفاده شدن از SSY رسما گوشی مورد نظر تنها با داشتن یک شماره تلفن هک شده بود ! بعد از انجام شدن هک مورد ، اطلاعاتی همچون تماسهای تلفنی ، کلیه contact ها ، پیام های متنی و حتی اطلاعات GPS و محل قرارگیری فرد مورد نظر برای هکر قابل مشاهده بود. هر چند جریان به همین موارد ختم نشد و حتی امکان برقراری تماس با مخاطبین و ... نیز در این هک امکانپذیر بود.

همانطور که قبلا گفتیم این آسیب پذیری بر روی تلفن گوشی همراه شما نیست و در واقع در زیرساختارهای مخابراتی و تلفنی وجود دارد ، نصب کردن یا جلوگیری از نصب هرگونه نرم افزار بر روی گوشی نمی تواند در روند کاری این آسیب پذیری مشکلی ایجاد کند ، در واقع این شبکه Mobile است که هک می شود نه گوشی تلفن همراه شما ، قطعا شما با شنیدن این موضوع هم وحشت زده می شوید و هم خشمگین ، چراکه بدون اینکه بدانید ممکن است از تلفن همراه شما جاسوسی شده باشد. نوهل در ادامه سخنانش اعلام کرد که با این روش تقریبا همه تلفن های همراه را می توان هک کرد .

فارق از اینکه شما از چه برندی استفاده می کنید. هکر می تواند با استفاده از این روش حسابهای بانکی شما ، حسابهای ایمیلی و .. شما را هک کند زیرا اکثر مکانیزم های امنیتی Two Factor Authentication یا احراز هویت دو منظوره از تلفن همراه برای اینکار استفاده می کنند. آسیب پذیری SSY تقریبا جدید است و در آگوست ۲۰۱۵ این آسیب پذیری گزارش شده است ، جالب اینجاست بدانید که این آسیب پذیری در زیرساخت مخابراتی وجود دارد که در بیش از ۸۰۰ شرکت ارتباطی در دنیا مورد استفاده قرار می گیرد و من اصلا در جریان نیستم که سیستم مخابرات ایران و شرکت ارتباطات زیرساخت نیز آیا در دسته بندی این ۸۰۰ شرکت قرار می گیرند یا خیر ؟

نقص یا آسیب پذیری SS۷ چگونه کار می کند ؟

مکانیزم کاری این نقص امنیتی چندان پیچیده نیست ، هکر تمامی تماس های تلفنی که به تلفن مورد نظر انجام می شود را به یک دستگاه یا سیستم ضبط صدای آنلاین هدایت یا Route می کند و سپس تماس مورد نظر را به سمت کاربر تلفن همراه مسیریابی مجدد یا Re-Route می کند و به این ترتیب یکجور حمله از نوع Man In The Middle یا MITM انجام می دهد.

در صورت هک شدن به این روش هکر می تواند کوچکترین حرکت کاربر را شناسایی و با استفاده از سایر ابزارهای هکی که در اختیار دارد تمامی فعالیت های کاربر را جاسوسی کند. جالب اینجاست بدانید که نوهل اعلام کرده است که این آسیب پذیری امنیتی در سیستم های اطلاعاتی وجود داشته است و سرویس های جاسوسی و امنیتی دنیا از چنین آسیب پذیری اطلاع داشته اند و بعضا از آن استفاده نیز نی کرده اند ، قبلا در ITPRO در خصوص پروژه هایی مانند Echelon صحبت کرده ایم که تمامی دنیا توسط آمریکا شنود اطلاعاتی می شده است اما استفاده از تجهیزات مخابراتی وابسته نیز طبیعتا تبعات امنیتی به این شکل خواهد داشت.

راهکار مقابله با SS۷ چیست ؟

راهکار مقابله با IMSI چیست ؟

شما هیچککاری در خصوص این حمله نمی توانید انجام دهید و سـرویس های مخابراتی و زیرساختی بایستی برای برطرف کردن این موضوع اقدام کنند ، با توجه که در جریان زیرساخت های مخابراتی ایران و تلفن های همراه آن به شخصه نیستم امیدوارم که شرکت های اپراتور ایرانی از آن دسـته از شرکت هایی نباشند که از این آسیب پذیری استفاده می کنند. نظرات در این خصوص با رعایت احترام و ذکر دلایل فنی مجاز است. ITPRO باشید

نویسنده : محمد نصیری

منبع : ITPRO

۴ نظر

مصطفی چگنی ۴۴ ماه قبل

اره استاد این همون ss۷ معروفه جالبیش اینه که هنوز public نشده و فقط تعداد محدودی میتونن این تست نفوذ رو بزنن

من حتی db-exploite روزیر رو کردم اما چیزی نبود.

پسندها (۱)

محمد شهریارپناه ۴۴ ماه قبل

در ادامه مقاله مهنـدس نصـیری باید بگم که با اسـتفاده از این باگ هکر می تونه به راحتی و بدون نصب هیچ برنامه مخربی روی گوشـی شخص قربانی تلگرام یـا هر شـبکه ی اجتمـاعی رو به راحتی هک کنه !! ولی این تکنینک Hacking نیاز به یک دستگاهی داره به نام IMSI catcher که این دسـتگاه می یاد تمام اطلاعات و دیتای مخابراتی اعم از صدا و تصویر رو sniff می کنه و تا جایی که اطلاع دارم این دستگاه قیمت فوق العاده بالایی هم داره !!

پسندها (۳)

AZARAKHSH ۴۴ ماه قبل

ممنون مهندس واقعا عالی بود.

دوستان جهت تکمیل مقاله مهندس نصیری و تفهیم کامل این قضیه میتونید به لینک زیر مراجعه کنید.

IMSI-catcher

پسندها (۱)

ارین باقری ۴۴ ماه قبل

بین خیلی ها این ی چیزه ترسناکه.

اکثر هکر های ایرانی از ss۷ سوع استفاده میکنن.

پابلیکم نیست درسته ولی ۸۷%

پسندها (۰)

نظر شما

برای ارسال نظر باید وارد شوید.

از سرتاسر توسینسو