صبح ساحل فناوری
سه شنبه ۲۶ شهریور ۹۸|سال سی وچهارم| شماره ۳۸۶۲
Email :Info.Sobhesahel@Gmail.Com

هنگام استفاده از درگاه‌های الکترونیکی بانکی در فضای مجازی به هشدارهای پلیس فتا توجه کنند و حتما شاخصه‌های امنیتی درگاه‌های الکترونیکی پرداخت را به دقت کنترل نمایند؛ همچنین هنگام استفاده از درگاه‌های الکترونیکی به هیچ وجه از فیلترشکن استفاده نکنند که اگر نشانی درگاه قبلا فیلترشده باشد، مشخص شود

آسیب‌پذیری مهم در سیستم عامل iOS

۷

یکی از کارشناسان امنیتی شکافی در نسخه بتا «آی.او.اس۱۳» کشف کرده که به هکر اجازه می‌دهد با برقراری تماس در اپلیکیشن فیس‌تایم به فهرست شماره تماس‌های فرد و اطلاعات همراه آن دسترسی یابد.

یک هفته قبل از آنکه iOS۱۳ عرضه شود، کارشناسان فناوری در آخرین نسخه بتای این سیستم عامل یک شکاف امنیتی کشف کرده‌اند. «جو رودریگز» یکی از محققان امنیتی شکافی در این سیستم عامل رصد کرده که به هکرها اجازه می‌دهد از طریق تماس با اپلیکیشن «فیس تایم» به فهرست شماره تماس های کاربر دسترسی یابند. به گزارش ایتنا از مهر، به گفته رودریگز هنگامیکه هکر با استفاده از فیس تایم تماس می گیرد، با استفاده از دستیار صوتی اپل (سیری) تمام شماره تماس‌های موجود در دستگاه قابل بررسی هستند. به این ترتیب علاوه بر شماره تماس، آدرس ایمیل، نام یا هرگونه اطلاعات دیگری که همراه شماره تماس ذخیره شده نیز آشکار می‌شود. این کارشناس امنیت، شکاف امنیتی را هنگام بررسی نسخه بتا iOS۱۳ در ماه جولای به اپل گزارش داد. مشابه این شکاف امنیتی در سیستم عامل iOS۱۲.۱ نیز وجود داشت. البته گزارش موجود تاکید دارد این شکاف امنیتی به تصاویر یا اطلاعات خارج از فهرست شماره تلفن های کاربر دسترسی ندارد.

مسافران بی‌خبر
کلاهبرداران فرصت‌طلب!

◆ گروه فناوری//

سودجویان با گرفتن اطلاعات مسافران، به واردات گوشی به اسم آن‌ها اقدام کردند و این موضوع واکنش‌هایی را در پی داشت و آذری جهرمی از کلاهبرداری عده‌ای که به حاجیان امسال سیم‌کارت رایگان داده‌اند و از مدارک آن‌ها سوءاستفاده و گوشی قاچاق ثبت کرده‌اند، خبر داد.

درحالی که وزیر ارتباطات اعلام کرده بود ارائه سیم‌کارت‌های رایگان به مسافران برای سوءاستفاده از مدارک آن‌ها و ثبت گوشی‌های قاچاقی نوعی دزدی است. اخیرا هم تاکید شده که خرید و فروش اطلاعات مسافران حتی با رضایت ایشان، سوءاستفاده از واردات مسافری است و شخص مسافر قانوناً مجاز نیست از طریق اطلاعات هویتی خود اقدام به ثبت تلفن همراه قاچاق کند.

به گزارش ایتنا از ایسنا، پس از اجرای طرح رجیستری، برخی از فروشندگان سودجو در بازار به افزایش قیمت گوشی با این بهانه اقدام کردند، در صورتی که مسئولان بارها اظهار کردند رجیستری هزینه‌ای ندارد و نباید باعث افزایش قیمت شود. از طرفی در یک سال گذشته، موضوع افزایش نرخ ارز نیز با توجه به ماهیت وارداتی بودن گوشی‌ها، موجب افزایش دو تا سه برابری قیمت گوشی‌ها شد.

البته گوشی‌هایی که در بازار وجود داشتند هم در مقایسه با همان گوشی‌ها در خارج از کشور، گران‌تر بودند و این موضوع باعث شد برخی به دنبال واردات گوشی مسافری باشند، زیرا به گفته‌ی آذری جهرمی، هر مسافر می‌تواند ۸۰ دلار بار مسافرتی با خود به همراه داشته باشد و مسافران می‌توانند از این معافیت گمرکی برای واردات گوشی استفاده کنند.

اما واردات گوشی‌های مسافری با هزینه پایین‌تر، موجب شد سودجویان که مسافر نبودند هم از این امکان فراهم‌شده که با استفاده از کارت ملی، امکان واردات یک گوشی وجود داشت، استفاده کنند.

در برهه‌ای شرایط این‌طور بود که قاچاقچی بارش را بدون ثبت سفارش به صورت قاچاق وارد کشور می‌کرد و با عنوان گوشی مسافری می‌توانست کد رجیستری بگیرد.

به همین دلیل پس از مدتی، این روند شکل صحیح‌تری به خود گرفت؛ همان‌طور که آذری‌جهرمی اظهار کرد که موضوع وصل سیستم سامانه نیروی انتظامی به گمرک مطرح است که باید اتفاق می‌افتاد. قرار بود این اتصال برای مشخص شدن دقیق واردات گوشی از طریق مسافر صورت بگیرد، نه‌این‌که به اسم بار مسافر، بتوان خارج از روال‌های مورد تأیید وزارت صنعت، معدن و تجارت، گوشی وارد کرد.

◆ **کلاهبرداری از مدارک حاجیان برای واردات گوشی‌های قاچاق**

اما موضوع واردات گوشی مسافری توسط کسانی که واقعا مسافر نبودند و از اطلاعات مسافران سوءاستفاده کردند، به اینجا ختم نشد. اگرچه با اتصال سامانه‌های نیروی انتظامی و گمرک، دیگر فقط کارت ملی برای واردات گوشی مسافری کافی نیست و مسافر واقعی می‌تواند از این امکان استفاده کند، برخی با گرفتن اطلاعات مسافران، به واردات گوشی به اسم آن‌ها اقدام کردند و این موضوع واکنش وزیر ارتباطات و فناوری اطلاعات را در پی داشت و وی از کلاهبرداری عده‌ای که به حاجیان امسال سیم‌کارت رایگان داده‌اند و از مدارک آن‌ها سوءاستفاده و گوشی قاچاق ثبت کرده‌اند، خبر داد.

این افراد با «سوءاستفاده از تسهیلات درنظر گرفته شده برای مسافران» با مراجعه مستقیم به مسافران و یا از طرق دیگری همچون آژانس‌های مسافرتی، در ازای پرداخت مبالغی، اقدام به خرید اطلاعات هویتی مسافران و زائران کرده و با استفاده از این اطلاعات اقدام به رجیستر کردن گوشی‌های قاچاق می‌کنند. در این باره دو حالت یا گوشی بدون اطلاع شخص مسافر و یا با اطلاع و رضایت شخص مسافر ثبت می‌شود.

در حالت اول که گوشی بدون اطلاع شخص مسافر ثبت می‌شود، متخلفان پس از دستیابی به اطلاعات هویتی مسافر، ابتدا بدون اطلاع مسافر اقدام به صدور سیم‌کارت بنام وی کرده و سپس با استفاده از سیم‌کارت صادرشده، کد ملی و شماره گذرنامه مسافر، اقدام به ثبت تلفن همراه مسافری می‌کند. در صورتی‌که برای مسافر سیم‌کارتی صادر شده باشد، پیامکی با سرشماره CRA.ir برای سایر خطوط وی ارسال می‌شود و این امکان برای شخص مسافر وجود دارد که با شماره‌گیری شماره ۱۹۵ و یا با مراجعه به آدرس اینترنتی cra.ir.۱۹۵ نسبت به ثبت شکایت در «سامانه ثبت و پاسخگویی به شکایات سازمان تنظیم مقررات و ارتباطات رادیویی» اقدام کند.

همچنین شخص مسافر می‌تواند با استفاده از اپلیکیشن «دولت همراه» و از بخش «تعداد خطوط مشترکین تلفن سیار» از صدور سیم‌کارت جدید بنام خود مطلع شود.

البته فرد متخلف با استفاده از سیم‌کارت صادرشده به نام مسافر قادر به انجام تخلفات متعددی است که ثبت تلفن همراه تنها یکی از این تخلفات است.

◆ **مسافرانی که به فروش اطلاعات خود راضی هستند**

در حالت دوم شخص مسافر با رضایت شخصی و در ازای دریافت مبلغی اقدام به فروش اطلاعات خود می‌کند. اما باید توجه داشت مطابق مقررات قانونی، مسافرانی که از مرزهای رسمی وارد کشور می‌شوند درصورتی که «صرفاً برای مصرف شخصی» و با هدف «غیرتجاری» تلفن همراهی «از خارج از کشور خریداری کرده و با خود وارد کرده باشند»، می‌توانند پس از ورود به کشور با مراجعه غیرحضوری به سامانه گمرک و پرداخت حقوق و عوارض گمرکی، آن را ثبت (رجیستر) و قابل استفاده کنند.

در این میان برخی افراد هم قصد دارند تا خرید و فروش اطلاعات هویتی مسافران را قانونی جلوه دهند که از جمله می‌توان به عملکرد برخی از اتحادیه‌های صنف تلفن همراه اشاره کرد که به طرق مختلف زائرانی را که به زودی قصد تشرف به زیارت عتبات عالیات را دارند، به فروش اطلاعات شخصی خود به واحدهای صنفی فروش تلفن همراه و مشارکت در این تخلف ترغیب می‌کنند.

اما باید توجه داشت همان‌طور که کانال اطلاع‌رسانی ثبت تلفن همراه (رجیستری) اعلام کرد، خرید و فروش اطلاعات مسافران حتی با رضایت ایشان، سوءاستفاده از واردات مسافری است و در صورتی‌که تلفن همراهی از خارج از کشور خریداری نشده و همراه مسافر وارد نشده باشد، شخص مسافر قانوناً مجاز نیست از طریق اطلاعات هویتی خود (شخصاً یا از طریق فروش اطلاعات خود به غیر) اقدام به ثبت تلفن همراه قاچاق کند و در صورت انجام، قطعاً مرتکب خلاف‌اظهاری به گمرک شده و مسئولیت حقوقی آن متوجه فرد مسافر خواهد بود.

واردات گوشی‌های مسافری با هزینه پایین‌تر، موجب شد سودجویان که مسافر نبودند هم از این امکان فراهم‌شده که با استفاده از کارت ملی، امکان واردات یک گوشی وجود داشت، استفاده کنند

دانستنی

هنگام استفاده از درگاه‌های الکترونیکی بانکی از فیلترشکن استفاده نکنید

◆ گروه فناوری//

هنگام استفاده از درگاه‌های الکترونیکی به هیچ وجه از فیلترشکن استفاده نکنند که اگر نشانی درگاه قبلا فیلتر شده باشد، مشخص شود.

ئیس پلیس فتا استان قم به خاطر پیشگیری از کلاهبرداری‌های مالی اینترنتی به شهروندان هشدار داد : هنگام استفاده از درگاه‌های الکترونیکی بانکی به هیچ وجه از فیلترشکن استفاده نکنید که اگر نشانی درگاه قبلا فیلترشده باشد، مشخص شود.

به گزارش ایتنا از پایگاه اطلاع‌رسانی پلیس فتا، سرهنگ علی موالی رییس پلیس فتا قم در تشریح این خبر گفت: کلاهبرداران برای اینکه بتوانند اعتماد شهروندان را جلب کنند در طراحی درگاه‌های جعلی پرداخت به جهت سرقت اطلاعات بانکی افراد از لوگو، آرم بانک‌ها و نشان اپلیکیشن هایی معتبر بانکی سوء استفاده می‌کنند.

این مقام انتظامی گفت: شهروندان توجه نمایند وجود تصاویرلوگو، آرم بانک‌ها و موسسات دولتی و اپلیکیشن‌های معتبر در درگاه‌های جعلی دلیلی بر امن بودن خدمات آن درگاه یا اپلیکیشن نیست یعنی در واقع از تصاویر برای کلاهبرداری سوء استفاده شده است.

وی به شهروندان توصیه کرد: هنگام استفاده از درگاه‌های الکترونیکی بانکی در فضای مجازی به هشدارهای پلیس فتا توجه کنند و حتما شاخصه‌های امنیتی درگاه‌های الکترونیکی پرداخت را به دقت کنترل نمایند؛ همچنین هنگام استفاده از درگاه‌های الکترونیکی به هیچ وجه از فیلترشکن استفاده نکنند که اگر نشانی درگاه قبلا فیلترشده باشد، مشخص شود.

این مقام مسئول بیان کرد : شهروندان نشانی درگاه‌های جعلی بانکی را حتما به نزدیک‌ترین پایگاه پلیس فتا خبر دهند یا در قسمت ارتباطات مردمی سایت پلیس فتا ثبت کنند تا در رصد اطلاعاتی پلیس فتا قرار گیرد.

رمزارز تلگرام آبان ماه عرضه می‌شود

◆ گروه فناوری//

به گفته سرمایه‌گذاران تلگرام، رمزارز اختصاصی این شبکه اجتماعی ۳۱ اکتبر (۹ آبان) امسال عرضه می‌شود.

به گزارش پایگاه خبری «ورج»، آخرین بار که خبری از رمزارز گرام (Gram) منتشر شد، تلگرام قصد داشت عرضه اولیه سکه (initial coin offering) خود را لغو کند، بنابراین اخبار اخیر مبنی بر انتشار این رمزارز تا حدود یک ماه آینده آن دسته از افرادی را که تلگرام و دنیای رمزارزها را از نزدیک دنبال نمی‌کنند، غافلگیر کرد.

در اسناد حقوقی که سرمایه‌گذارهای تلگرام به رسانه‌ها ارائه داده‌اند، این شرکت این بار ضرب الاجلی جدی را برای عرضه این رمزارز تعیین کرده است؛ اگر تا ۳۱ اکتبر (۹ آبان) امسال این اتفاق نیفتد، تلگرام موظف است ۱.۷ میلیارد دلار سرمایه‌ای را که برای اجرای این طرح جمع آوری شده است، بازگرداند.

کاربران می‌توانند این رمزارزها را در کیف پول دیجیتال گرام که تلگرام در نظر دارد به تمام بیش از ۲۰۰ میلیون کاربر در جهان ارائه دهد، ذخیره کنند.

تلگرام نخستین شرکتی نیست که رمزارز اختصاصی خود را ارائه می‌دهد. فیس‌بوک نیز در حال توسعه رمزارز اختصاصی لیبرا است که بنابر گزارش‌ها توسط ارزهای رایج در حساب‌های بانکی پشتیبانی می‌شود. پیش‌بینی می‌شود که این رمزارز در صورت تایید، در سه ماهه اول سال ۲۰۲۰ میلادی عرضه شود. شرکت وال‌مارت که به عنوان بزرگترین خرده فروشی جهان شناخته می‌شود نیز در اوایل اوت (مرداد) پتنت توسعه رمزارز اختصاصی خود را ثبت کرد.

بازار موبایل

ردیف	برند/ مدل	قیمت بدون گارانتی(تومان)	تاریخ بروزرسانی
۱	Samsung Galaxy S۱۰	۸,۴۵۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۲	Samsung Galaxy Note۹	۸,۲۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۳	Samsung Galaxy A۵۰	۳,۷۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۴	Samsung Galaxy Note۱۰	۱۲,۰۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۵	Apple iPhone XR	۹,۵۹۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۶	Apple iPhone XS Max	۱۳,۴۹۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۷	۸ Apple iPhone	۸,۵۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۸	Apple iPhone XS	۱۲,۷۹۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۹	۴ Huawei nova	۶,۸۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۱۰	lite Huawei P۳۰	۳,۹۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۱۱	Pro Huawei P۳۰	۱۳,۶۹۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۱۲	(Nokia X۷) ۸,۱Nokia	۶,۱۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۱۳	PureView ۹Nokia	۹,۰۵۰,۰۰۰	۱۳۹۸/۰۶/۱۱
۱۴	۷,۱Nokia	۳,۳۰۰,۰۰۰	۱۳۹۸/۰۶/۱۱

*** تمامی قیمت ها از سایت www.gsm.ir استخراج شده است**

گوگل کروم به‌روزرسانی شد

◆ گروه فناوری//

شرکت گوگل، مرورگر کروم خود را برای رفع یک نقص شدید که می‌تواند هکرها را قادر به انجام حملات اجرای کد از راه دور (RCE) کند، به‌روز رسانی کرد.

این آسیب‌پذیری که با شناسه «CVE-۲۰۱۹-۵۸۶۹» ردیابی می‌شود، یک نقص «استفاده پس از آزادسازی» (use-after-free) است که در موتور مرورگر Blink وجود دارد. Blink یک موتور مرورگر منبع‌باز است که اولین بار در سال ۲۰۱۳ و به‌طور خاص به‌عنوان بخشی از پروژه کرومیوم و با چارچوب‌های مختلف نرم‌افزاری قابل استفاده مجدد برای سیستم‌عامل اندروید، ساخته شد.

این موتور مرورگر از گوگل کروم استفاده می‌کند.

به گزارش ایتنا از مهر، موتورهای مرورگر در قلب هر مرورگر اصلی قرار دارند و نقش اصلی آن‌ها، تبدیل اسناد HTML و سایر منابع صفحه وب به نمایش‌های بصری در دستگاه‌های کاربران است.

محققان هشدار دادند که سوءاستفاده موفقیت‌آمیز از آسیب‌پذیری موجود در Blink می‌تواند به مهاجمان اجازه دهد تا کد دلخواه را در متن مرورگر اجرا کنند، اطلاعات حساس را به‌دست آورند، محدودیت‌های امنیتی را دور بزنند، اقدامات غیرمجاز را انجام دهند یا موجب شرایط انکار سرویس (DoS) شوند.

بسته به امتیازات مرتبط با برنامه، مهاجم می‌تواند برنامه‌هایی را نصب کند، داده‌ها را مشاهده یا حذف کرده و آن‌ها را تغییر دهد یا حساب‌های جدید با حقوق کامل کاربر ایجاد کند.

نقص موجود در Blink می‌تواند با ترغیب کاربر به بازدید از یک صفحه وب خاص طراحی‌شده، مورد سوءاستفاده قرار گیرد. بنابراین، مهاجمان می‌توانند از راه دور چنین صفحه وبی را راه‌اندازی کنند و از راه دور به سیستم قربانیان حمله کنند.

این نقص بر نسخه‌های گوگل کروم قبل از ۷۶.۰.۳۸۰۹.۱۳۲ تأثیر می‌گذارد. به‌گفته محققان، در حال حاضر هیچ گزارشی از سوءاستفاده گسترده از این آسیب‌پذیری گزارش نشده است؛ اما گوگل از کاربران ویندوز، مک و لینوکس خواسته است تا مرورگر کروم خود را به نسخه ۷۶.۰.۳۸۰۹.۱۳۲ به‌روز کنند.

جاسوسی با سیم‌کارت

◆ گروه فناوری//

محققان امنیتی حمله جدیدی را کشف کرده‌اند که با کمک سیم‌کارت انجام می شود و اطلاعات کاربر را رصد می‌کند.

در مواردی خاص سیم‌کارت افراد خطر امنیتی بالاتری نسبت به نرم افزار موبایل دارد. محققان شرکت AdaptiveMobile Security شکاف امنیتی جدیدی به نام Simjacker کشف کرده اند که یک شرکت نظارتی از آن برای نفوذ به دستگاه‌های افراد استفاده می کرده است. در این روش هکر با استفاده از یک موبایل هوشمند با مودم GSM یا هرگونه سرویس A۲P، یک پیامک به موبایل قربانی ارسال می کند.

به گزارش ایتنا از مهر، این پیامک حاوی دستورات جعبه ابزار سیم (SIM Tool Kit) است که S@T Browser دستگاه از آن پشتیبانی می‌کند. S@T Browser در حقیقت اپلیکیشنی است که در سیم کارت قرار دارد. استفاده از S@T Browser و دستورات جعبه ابزار سیم (SIM ToolKit) فناوری قدیمی است که هنوز برخی از شبکه‌های موبایل و سیم کارت ها از آن استفاده می کنند.

با کمک دستورات جعبه ابزار سیم می توان مرورگرها را فعال یا صوت پخش کرد. در گذشته اپراتورهای موبایل از این پروتکل ها برای ارسال پیام های تبلیغاتی یا اطلاعات صورتحساب به کاربر استفاده می‌کردند. طبق یافته محققان امنیتی هکرها با استفاده از روش Simjacker که در بالا گفته شد، اطلاعات مکانی و شماره های IMEI را به دست می‌آورند. این اطلاعات بعدا با استفاده از اس ام اس به دستگاه دیگری ارسال می شود تا ثبت شوند.

این روش بسیار مرموزانه و بی سروصدا است. هرچند در آن از پیامک استفاده می شود اما کاربر هیچ نوتیفیکیشنی دریافت نمی کند. هکرها می توانند به راحتی به اطلاعات آپدیت شده هر دستگاه دست یابند. از این روش برای دستیابی به اطلاعات آیفون، دستگاه‌های اندروید مختلف و حتی چند دستگاه اینترنت اشیا (مجهز به سیم کارت) استفاده شده است.

این شرکت نظارتی نیز اعلام کرده اکنون بیش از دو سال است که از این روش در بیش از ۳۰ کشور در خاورمیانه، شمال آفریقا، آسیا و اروپای شرقی استفاده می کند.

البته کارشناسان تخمین می زنند از این شیوه نظارتی به طور گسترده استفاده نشده است.