خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۸۳

هفته نامه | سال دوم | شماره هشتاد و سوم | ۱۳ آذر ۱۳۹۵

به راحتی می‌توان به تلفن همراهِ اندرویدی دونالد ترامپ نفوذ کرد

دونالد ترامپ اذعان کرد که شبکه‌های اجتماعی نقش کلیدی در پیروزی او در انتخابات ریاست جمهوری آمریکا داشت. او گفت درست است که تاکنون فعالیت زیادی در فیس‌بوک و توییتر نداشته ولی تصمیم دارد پس از ژانویه 2017 در شبکه‌های اجتماعی فعالیت داشته باشد.

همین اظهارات است که کارشناسان امنیتی در آمریکا را نگران کرده چرا که با فعالیت دونالد ترامپ در شبکه‌های اجتماعی، او در معرض حملات زیادی قرار خواهد گرفت با توجه به این حقیقت که او از یک تلفن همراه اندرویدی نیز استفاده می‌کند.

هرچند برخی از پست‌هایی که ترامپ در طول پویش انتخاباتی خود ارسال کرده، از یک دستگاه آیفون ارسال شده، اما محققان امنیتی که فعالیت‌های او در شبکه‌های اجتماعی را تحلیل می‌کردند، متوجه شدند عمده فعالیت‌های ترامپ با یک تلفن همراه اندوریدی انجام شده است.

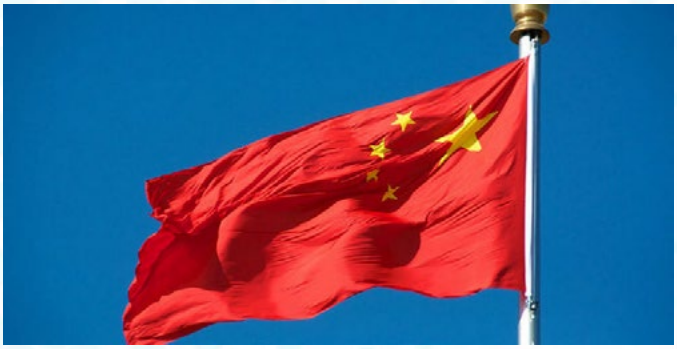
این مسئله ترامپ را در معرض خطرات زیادی قرار خواهد داد چرا که او می‌خواهد همچنان به فعالیت در شبکه‌های اجتماعی ادامه دهد و این امکان وجود دارد که پرونده‌ها یا پیوندهای مخرب برای او ارسال شوند.

مارتین الدرسون، بنیان‌گذار یک شرکت امنیتی تلفن همراه می‌گوید: «رئیس جمهور اوباما یک تلفن همراه اصلاح‌شده برای استفاده‌ی شخصی خود دارد که تنها به برقراری تماس تلفنی محدود شده است. من فکر می‌کنم رئیس‌جمهور منتخب نیز این توییت‌ها را توسط یک دستیار اختصاصی ارسال می‌کند.»

هنگامی که باراک اوباما پیروز انتخابات شد، توسط آژانس امنیت ملی آمریکا، دستگاه امن‌شده‌ی بلک‌بری برای مدت طولانی به‌عنوان دستگاه تلفن همراه او انتخاب شده بود ولی اخیراً مشاهده شده که یک نسخه‌ی امن از سامسونگ S4 برای باراک اوباما انتخاب شده است.

در مورد دونالد ترامپ، آژانس امنیت ملی آمریکا کار سختی را در پیش دارد. ترامپ اعلام کرده پس از ورود به کاخ سفید، همچنان از تلفن همراه شخصی خود استفاده خواهد کرد ولی محققان امنیتی می‌گویند این مسئله امکان‌پذیر نیست.

فیس‌بوک برای چین ابزارِ سانسور طراحی می‌کند



فیس‌بوک نرم‌افزاری را توسعه داده است که محتوای خاصی را برای کشور چین سانسور می‌کند. فیس‌بوک با این کار در تلاش است به مسدود بودن سرویس خود در این کشور پایان دهد.

فیس‌بوک در این ابزار پست‌های ارسالی از یک منطقه‌ی جغرافیایی خاص را که پست‌های خبری برای مردم ارسال می‌کنند، سانسور می‌کند. این غول شبکه‌ی اجتماعی در تلاش است با این‌کار استفاده از فیس‌بوک در چین را دوباره عملیاتی کند. فیس‌بوک در سال 2009 تنها یک سال پس از شروع فعالیتش در کشور چین مسدود شده است.

گزارش‌ها حاکی از آن است که فیس‌بوک برای موفقیت در چین با نبرد بزرگی مواجه است. در این کشور تنها چند هزار کاربر وجود دارد که این سرویس برای آن‌ها مسدود شده است و از آن زمان تاکنون شبکه‌های اجتماعی چینی رقابت با فیس‌بوک را شروع کرده‌اند. این رسانه‌های اجتماعی عبارتند از: Tencent QQ، WeChat و Sina Weibo.

آخرین ابزاری که فیس‌بوک توسعه داده، می‌تواند شرکت‌های شخص ثالث را قادر سازد تا خودشان به‌جای فیس‌بوک تصمیم بگیرند که چه پست‌هایی در فیدهای خبری کاربران نمایش داده شود. این ابزار همچنین آن‌ها را قادر می‌سازد بر روی محتوایی که کاربران می‌خوانند و به اشتراک می‌گذارند کنترل داشته و بتوانند بخش مورد نظر خود را سانسور کنند.

گزارش‌ها حاکی از آن است این ابزار هنوز به چین ارائه نشده است. این ابزار هنوز در مرحله‌ی آزمایش قرار دارد و به‌طور واقعی منتشر نشده است. فیس‌بوک در بیانیه‌ای گفت: «ما از قبل گفتیم که بسیار به چین علاقه‌مند هستیم و مدت زمان زیادی را برای درک و یادگیری این کشور صرف کردیم.» در ادامه‌ی این بیانیه آمده است هنوز درباره‌ی رویکرد آتی فیس‌بوک نسبت به چین تصمیم‌گیری نشده است.

درخواست‌های دولتی که اخیراً به فیس‌بوک ارسال شده، نشان می‌دهد که این وب‌گاه نسبت به سانسور محتوا خیلی بیگانه هم نیست. هرچند این شرکت تنها با حکم دادگاه به این سانسور محتوا دست زده است.

شرکت کسپرسکی از سامانه عاملِ امن خود رونمایی کرد

شرکت معروف کسپرسکی که آن را با محصولات ضدویروس می‌شناسیم، از سامانه عامل ضدنفوذ خود رونمایی کرد. طراحی این سامانه عامل 14 سال طول کشیده و بر اساس طرح اولیه‌ی لینوکس طراحی شده است.

مدیر عامل این شرکت عنوان کرد سامانه عامل کسپرسکی برای اولین بار بر روی سوئیچ لایه Kraftway 3 شروع بکار کرده است. او جزئیات بیشتری راجع‌به این سامانه عامل جدید ارائه نکرده است.

یک سوئیچ لایه 3 ابزاری بسیار سریع برای اجرای سامانه عامل کسپرسکی است که برای شبکه‌های زیرساخت و حیاتی که به امنیت بسیار بالای اطلاعات نیاز دارند و همچنین برای دستگاه‌های اینترنت اشیاء طراحی شده است.

سامانه عامل جدید کسپرسکی چه قابلیت‌های دیگری نسبت به سایر سامانه‌های عامل دارد؟

سامانه عامل کسپرسکی مبتنی بر معماری میکروهسته است که کاربران را قادر می‌سازد سامانه‌ی عامل خود را سفارشی کنند. بنابراین بسته به نیازمندی هر کاربر، سامانه عامل کسپرسکی می‌تواند با قطعه‌های مختلف سامانه عامل طراحی شود.

به گفته‌ی شرکت کسپرسکی تنها طرح اولیه از لینوکس گرفته و دیگر کوچکترین شباهتی به سامانه عامل لینوکس وجود ندارد و واسط گرافیکی کاربر نیز در آن بسیار کم است.

چه چیزی سامانه عامل کسپرسکی را ضد نفوذ می‌کند؟

این سامانه عامل در یک شرکت امنیتی طراحی شده است. این سامانه عامل می‌تواند رفتار تمامی برنامه‌های کاربردی و ماژول‌های سامانه عامل را کنترل کند. کسپرسکی ادعا می‌کند این سامانه عامل عملاً ضدنفوذ است و مهاجم برای دسترسی غیرمجاز به سامانه باید امضای دیجیتالی که از حساب‌ها محافظت می‌کند را بشکند و این کار نیاز به رایانه‌های کوانتومی دارد.

کسپرسکی در خصوص حملات منع سرویس توزیع‌شده که اخیراً بسیاری از وب‌گاه‌ها را تحت تأثیر قرار داده، صحبت کرده است. این شرکت ضمانت کرده سامانه عامل کسپرسکی از دستگاه‌هایی مانند سامانه‌های کنترل صنعتی، SCADA یا ICS و دستگاه‌های اینترنت اشیاء در برابر چنین حملاتی محافظت خواهد کرد.

بزرگ‌ترین حمله منع سرویس که ارائه‌دهنده سرویس DNS با نام Dyn را هدف قرار داده بود،

آیا مهاجمی که خطوط ریلی سان‌فرانسیسکو را هدف قرار داده بود، یک نفوذگر ایرانی است؟

مهاجمی که به خطوط ریلی سان‌فرانسیسکو حمله کرده بود، در طول یک ماه گذشته با انجام چند حمله، 100 هزار دلار بدست آورده است. وجود این نفوذگر زمانی فاش شد که خود او نیز مورد نفوذ واقع شد.

به گزارش وب‌گاه محقق امنیتی کربس، یک محقق ناشناس تصمیم گرفت رایانامه‌ای که مهاجم در پیغام باج‌خواهی خود به مدیران خطوط ریلی سان‌فرانسیسکو ارائه کرده بود را بشکند. ظاهراً این محقق توانسته است با حدسِ پاسخِ سؤال امنیتی، گذرواژه‌ی این رایانامه را بازنشانی کند. در این رایانامه پیام باج‌خواهی که به مدیران سامانه‌ی حمل‌ونقل سان‌فرانسیسکو ارسال شده و بیش از 12 کیف پول بیت‌کوین دیده می‌شود. تخمین زده می‌شود از طریق این کیف پول‌ها مهاجم توانسته است از ماه آگوست تاکنون، از شرکت‌های مختلف بیش از 140 هزار دلار باج دریافت کند.

به نظر می‌رسد این باج‌افزار شرکت‌های تولیدی و ساخت‌وساز آمریکا را هدف قرار داده بود و برای برگرداندن هر کارگزار 730 دلار (1 بیت‌کوین) درخواست می‌کرد. این نفوذگر از ابزارهای متن‌باز بر روی کارگزار اوراکل برای پویش دستگاه‌های متصل به اینترنت و آسیب‌پذیر استفاده کرده است. همچنین او به برنامه‌ی مدیریت پروژه‌ی Primavera نیز علاقه داشته است.

در گزارش ارائه‌شده در وب‌گاه کربس، ادعا شده است که برخی شرکت‌ها برای بازگرداندن اطلاعات خود، حتی مبالغ بیشتری پرداخت کرده‌اند. در مواردی مشاهده شده که قربانیان نکات امنیتی را از مهاجم درخواست کرده و در ازای آن بیت‌کوین بیشتری پرداخت کرده‌اند.

با بررسی اطلاعات موجود بر روی کارگزار و رکوردهای ثبت‌شده اعم از تاریخ و زمان ورود به سامانه، می‌توان اطلاعات جالبی از مکان جغرافیایی مهاجم پیدا کرد. به نظر می‌رسد 300 آدرس مربوط به کارگزاری که حمله از روی آن انجام شده، مربوط به ایران باشند هرچند یک حساب میزبانی دیگر نیز بر روی این کارگزار وجود دارد و شماره تماس آن +78234512271 بوده و مربوط به روسیه است. همچین ترجمه‌هایی که با مترجم گوگل انجام شده نشان می‌دهد عبارات از زبان فارسی به انگلیسی برگردانده شده است. فارسی زبان معمول در کشور ایران و بخش‌های دیگری از خاورمیانه است.