می‌خواهید هک نشوید، مراقب شماره تلفن خود باشید

هک شبکه‌های اجتماعی فقط با یک شماره موبایل!

در حالی که شبکه اجتماعی فیس‌بوک این روزها توسط بسیاری از مردم مورد استفاده قرار می‌گیرد و فارغ از بحث‌های جانبی که پیرامون آن وجود دارد، حجم بسیار بالایی از کاربران را به سمت و سوی خود جذب کرده است، اما در طرف مقابل مجرمان سایبری و هکرها را نیز به سمت خود جذب کرده است. هر چند این شرکت تلاش می‌کند تا بهترین مکانیزم‌های امنیتی را در این خصوص ارائه کند، اما واقعیت این است که هکرها نیز بی‌کار ننشسته‌اند و همواره از روش‌های ابداعی و بعضا منحصر به‌فردی در جهت دستیابی به اطلاعات کاربران استفاده می‌کنند.

در میان هک‌های مختلفی که هر روز در سراسر جهان سایت‌های اینترنتی را تهدید می‌کند، شبکه‌های اجتماعی در اولویت هستند. در این میان دسترسی به اطلاعات حساب کاربری مردم در فیس‌بوک بیش از هر سایت دیگری در اولویت کاری هکرها قرار دارد. به تازگی خبری از سوی کارشناسان امنیتی منتشر شده است که نشان هکرها به راحتی و تنها با آگاهی از شماره تلفن افراد این توانایی را دارند تا حساب کاربری مردم در این شبکه اجتماعی را هک کرده و به آن دسترسی پیدا کنند. تنها پیش شرط موفقیت این روش داشتن مهارتی در زمینه هک است.

مطلب پیشنهادی

حمله‌ای هدفمند
در پس پرده حملات لینکدین چه اتفاقی رخ داده است؟

این حرف بدان معنا است که حساب کاربری شما نه تنها با داشتن گذرواژه قدرتمند، بلکه با بهره‌مندی از ابزارهای نظارتی و امنیتی قدرتمند باز هم در معرض هک و نفوذ قرار دارد. هکرهایی که سطح دانش و مهارت آن‌ها به اندازه‌ای باشد که بتوانند به شبکه SS7 نفوذ کنند، این توانایی را دارند تا به راحتی حساب کاربری شما در فیس‌بوک را هک کنند. تنها چیزی که هکرها به آن نیاز دارند شماره تلفن شما است. نقاط ضعفی که در SS7 وجود دارد؛ به هکرها و مجرمان سازمان‌یافته این قابلیت را می‌دهد تا به راحتی توانایی شنود پیام‌های کوتاه افراد و تماس‌هایی که افراد با اسمارت‌فون خود برقرار می‌کنند را داشته باشند. جالب‌تر آن‌که حساب‌های کاربری افراد در شبکه‌های اجتماعی که شماره تماسی در آن‌ها قرار گرفته است نیز قابل کنترل خواهد بود. SS7 (سرنام Signalling System Number 7) یک پروتکل سیگنال تلفنی است که امروزه چیزی بیش از 800 اپراتور مخابراتی در سراسر جهان از آن استفاده می‌کنند. این پروتکل به اپراتورهای جهانی اجازه می‌دهد تا داده‌های خود را با یکدیگر مبادله کرده و همچنین سرویس‌های جهانی نظیر رومینگ را به مشترکان خود ارائه کنند.

مشکل کار کجاست؟

مشکل موجود در شبکه SS7 که فرآیند ارسال پیام‌های کوتاه بر مبنای این پروتکل انجام می‌شود، این است که فرض را بر اعتمادسازی بر مبدا که پیام کوتاه را ارسال (و البته دریافت کرده) کرده است؛ می‌گذارد. در نتیجه هکرها این توانایی را دارند تا پروتکل SS7 را فریب داده تا پیام‌های کوتاه را برای دستگاه آن‌ها ارسال کند. در این روش تمامی آن چیزی که هکرها به آن نیاز دارند، شماره تلفن قربانی و جزییاتی در ارتباط با دستگاهی است که قربانی از آن استفاده می‌کند. سایت فوربس گزارش داده است که چندی پیش گروهی از پژوهش‌گران Positive Technologies نمونه‌ای مفهومی از این شیوه حمله را منتشر ساخته‌اند که نشان می‌دهد، هکرها چگونه موفق شده‌اند به حساب‌های کاربری مردم در تلگرام و واتس آپ نفوذ کنند. حال همین گروه ویدویی را منتشر ساخته‌اند که نشان می‌دهد هکرها با استفاده از این ترفند قادر هستند حساب کاربری فیس بوک مردم را نیز در معرض تهدید قرار دهند. در حالی که شبکه‌های سلولی از پیشرفته‌ترین تکنیک‌های رمزنگاری استفاده می‌کند، اما واقعیت این است که SS7 از مدت‌ها قبل آسیب‌پذیر بودن خود را نشان داده است. رخنه‌های موجود در طراحی SS7 اولین بار در سال 2014 خود را نشان دادند. زمانی که یک تیم از پژوهش‌گران German Security Research Labs هشدارهای جهانی را در ارتباط با آسیب‌پذیر بودن SS7 منتشر ساختند.

مهاجم چگونه نفوذ می‌کند؟

در این شیوه حمله هکرها ابتدا روی گزینه فراموش کردن گذرواژه در صفحه اصلی فیس‌بوک کلیک می‌کنند. فیس بوک در ادامه از آن‌ها آدرس ایمیل یا شماره تلفنی که منتسب به حساب کاربری است را درخواست می‌کند. هکرها شماره تلفن حقیقی فردی که صاحب حساب کاربری است را وارد می‌کنند. اما در مرحله بعد هکر جهت پیام کوتاه یک‌بار مصرفی که توسط فیس بوک ارسال می‌شود را به سمت کامپیوتر یا تلفن همراه خود تغییر داده و به این شکل به راحتی قادر است به حساب کاربری قربانی وارد شود.

جالب آن‌که کارشناسان امنیتی اعلام کرده‌اند، این شیوه حمله تنها فیس بوک را تحت الشعاع خود قرار نمی‌دهد. هر سایت یا ارائه دهنده خدمات اینترنتی یا ایمیلی همچون جی‌میل که از پیام کوتاه برای احراز هویت کاربران خود استفاده می‌کند، در برابر این حمله آسیب‌پذیری است.

راه‌کارهای جلوگیری

واقعیت این است که اپراتورهای شبکه این توانایی را ندارند تا برای این آسیب‌پذیری در کوتاه مدت وصله لازم را ارائه کنند، اما کاربران خود می‌توانند چند اقدام احتیاطی را برای پیش‌گیری از بروز این‌گونه حملات انجام دهند:

1- هیچ‌گاه شماره تلفن خود را با شبکه‌های اجتماعی مرتبط نسازید. به جای این روش سعی کنید از تکنیک بازیابی رمزعبور بر مبنای ایمیل در ارتباط با حساب‌هایی که در شبکه‌های اجتماعی دارید، استفاده کنید.

2- سعی کنید از مکانیزم احراز هویت دو عاملی استفاده کنید که از پیام‌های کوتاه برای کدهای دریافتی استفاده نمی‌کند.

3- همواره سعی کنید از برنامه‌های ارتباطی که رمزنگاری نقطه به نقطه (end-to-end) را پشتیبانی می‌کنند، استفاده کنید. در این حالت داده‌های شما تا رسیدن به مقصد در حالت رمزنگاری قرار خواهند داشت.

در پایان ضروری است به این نکته توجه داشته باشید که این شگرد حمله هیچ‌گونه ارتباطی با شبکه‌های اجتماعی نداشته و یک آسیب‌پذیری در شبکه ارتباطی است. در همین ارتباط فیس بوک گفته است: «به دلیل این‌که سوء استفاده از آسیب‌پذیری SSL جزء موارد خاص بوده و به سطح بالایی از دانش فنی نیاز دارد، در نتیجه خطر جدی کاربران را تهدید نمی‌کند. با این وجود به همه کاربران خود توصیه می‌کنیم مکانیزم احراز هویت دو عاملی با نام Login Approvals را از بخش تنظیمات امنیتی فیس‌بوک فعال سازند. در چنین حالتی مکانیزم بازیابی از طریق پیام کوتاه غیر فعال خواهد شد و اگر هکری شماره تماس شما را به دست آورد، باز هم برای دسترسی به حساب کاربری‌تان به گذرواژه شما نیاز خواهد داشت.»

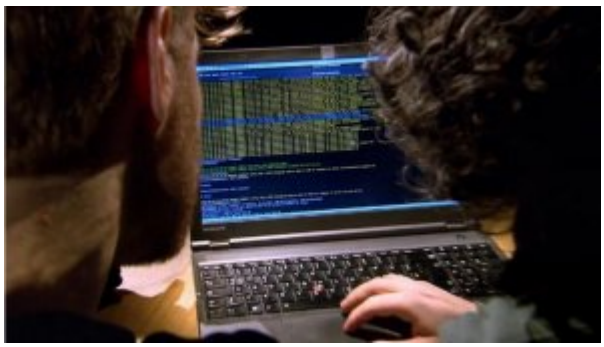
==========

شاید به این مقالات هم علاقمند باشید:

ده هزار سایت وردپرسی در معرض حملات هکری قرار گرفتند

شکاف امنیتی ۹۰ هزار دلاری که تمام سیستم‌های ویندوز را دور می‌زند!

هک‌های ترسناک باج‌افزارها رو به افزایش است



آیا قدرت و توانایی هکرها بی حد و مرز است؟

با این ابزار رایگان کشنده به شکار بدافزارها بروید + لینک دانلود

2016؛ سال اخاذی‌های آنلاین

7 روشی که هکرها می‌توانند از وای‌فای بر علیه شما استفاده کنند

بهترین ابزارهای مدیریت گذرواژه‌ها ویژه کامپیوترهای شخصی، دستگاه‌های موبایل و کامپیوترهای مک

تاریخ انتشار:
04 تیر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3583