

تهدیدات واتس‌آپ

حملات فیشینگ یکی از متداول‌ترین و آسان‌ترین روش‌های سرقت اطلاعات شخصی، مالی و حریم خصوصی کاربران در فضای مجازی است.



واتس‌آپ که یکی از بزرگترین و محبوب‌ترین اپلیکیشن‌های پیام‌رسان در جهان به شمار می‌رود، همواره یکی از پلتفرم‌های مورد استفاده هکرها و مجرمان سایبری بوده است تا با فریب دادن کاربران مبالغ هنگفت موردنظر خود را به جیب بزنند.

بارها کارشناسان فعال در حوزه امنیت سایبری در مورد روش‌ها و حقه‌های هکرها و مجرمان سایبری هشدار داده بودند و حالا نیز طبق جدیدترین گزارش‌ها به آن‌ها توصیه کرده‌اند که به هیچ عنوان به پیام‌های ناشناسی که از آن‌ها تقاضایی مبنی بر پرداخت پول و خریداری بلیت به صورت آنلاین می‌شود، پاسخ ندهند. با اینکه اپلیکیشن پیام‌رسان واتس‌آپ همچون بسیاری دیگر از نرم‌افزارهای مشابه قابل هک شدن سریع توسط هکرها و مجرمان سایبری نیست و به لطف قابلیت رمزنگاری فوق پیشرفته به کار رفته در آن همواره عنوان امن‌ترین پیام‌رسان جهان را به خود اختصاص داده است، اما به نظر می‌رسد که هکرها راه جدیدی را برای ورود به آن پیدا کرده‌اند تا بتوانند به اطلاعات شخصی و حساب کاربری قربانیان موردنظر خود دسترسی پیدا کرده و از داده‌های آن‌ها به منظور دستیابی به اهداف و انگیزه‌های خود سو استفاده کنند.

بر اساس وب‌سایت news ۱۸، به نظر می‌رسد که حملات فیشینگ از متداول‌ترین انواع حملاتی است که به کاربران واتس‌آپ می‌شود چراکه با توجه به قابلیت‌های رمزنگاری پیشرفته‌ای که در این پیام‌رسان به کار گرفته شده است، کاربران تنها خود باید راه نفوذ هکرها به اطلاعات شخصی خود را باز کنند.

واژه فیشینگ یا Phishing که مختصراً از عبارت Password Harvesting Fishing به معنای "به دست آوردن رمز عبور از طریق طعمه" به دست آمده و ساخته شده است، یکی از حملات سایبری شناخته شده مبتنی بر مهندسی اجتماعی است که با فریب دادن کاربران موردنظر اطلاعات محرمانه و خصوصی آن‌ها از جمله رمز عبور، اطلاعات حساب بانکی، اطلاعات شخصی و محتوای به اشتراک گذاشته شده آن‌ها در شبکه‌های اجتماعی را به دست می‌آورند. به گفته بسیاری از کارشناسان فعال در حوزه امنیت سایبری، این روش مورد استفاده هکرها آنقدر کامل، پیشرفته، بدون نقص و طبیعی جلوه می‌کند که کمتر کاربری به جعلی و کلاهبرداری بودن آن شک می‌کند.

در این روش خود کاربران با مراجعه و کلیک کردن بر روی لینک‌های درج شده در پلتفرم واتس‌آپ، اطلاعات مالی و شناسایی اکانت خود را در اختیار هکرها و مجرمان سایبری قرار می‌دهند و به صورت ناخودآگاه موجب خواهند شد آن‌ها به اهداف خود برسند و به حساب‌های بانکی مربوطه خود نفوذ و دسترسی پیدا کنند.

برخلاف سایر حملات سایبری که توسط هکرها و مجرمان سایبری و یا بهره‌گیری از آسیب‌پذیری‌های موجود در نرم‌افزار یا سخت‌افزار دستگاه‌های الکترونیکی مربوطه صورت می‌گیرد، حملات فیشینگ توسط خود کاربر قربانی صورت می‌پذیرد، چراکه هکرها، کاربران را فریب داده تا با دست‌خودشان اطلاعات موردنظر هکرها را تقدیم آن‌ها کنند.

حملات فیشینگ یکی از متداول‌ترین و آسان‌ترین روش‌های سرقت اطلاعات شخصی، مالی و حریم خصوصی کاربران در فضای مجازی است. پیام‌رسان واتس‌آپ که یکی از محبوب‌ترین و پرطرفدارترین اپلیکیشن‌های جهان است، از قابلیت Encryption End-to-End یا رمزنگاری پیشرفته پشتیبانی می‌کند و از

پروتکل‌های پیشرفته‌ای برای حفظ حریم شخصی کاربرانش برخوردار است.

این اپلیکیشن که برای تمامی سیستم‌های عامل اندروید، iOS و ویندوز قابل استفاده است، در سال ۲۰۱۶ میلادی لقب پرکاربردترین پیام‌رسان جهان را گرفت. شرکت فیس‌بوک

با در اختیار گرفتن و تصاحب شرکت واتس‌آپ در سال ۲۰۱۴، ۱۹ میلیارد دلار کسب کرد و از آن زمان تاکنون نیز با معرفی و افزودن قابلیت‌های جدید بدنبال جذب و حفظ طرفداران این پیام‌رسان بوده است. طبق آخرین آمارهای منتشر شده، پیام‌رسان واتس‌آپ هم‌اکنون میزبان حدود بالغ بر یک میلیارد و ۳۰۰ میلیون کاربر فعال در ماه است.