رایج ترین روش های هک واتساپ

با اینکه در وب سایت AnyControl به روش‌های پیشگیری از هک پیام های واتساپ اشاره کرده بودیم، در این مطلب به تشریح روش های رایج هک واتساپ برای علاقه مندان به حفظ امنیت در این حوزه پرداخته‌ایم.

1.دزدیدن اطلاعات با روش کیو آر جک (QRLJacking)

در این حمله، مهاجم با کلون یا فیشینگ کد QR ورود به واتساپ وب، کاربر را ترغیب می‌کند تا QR جعلی را اسکن کند.

با این کار، توکن احراز هویت به سرور مهاجم ارسال می‌شود و حساب کاربر به طور کامل در اختیار هکر قرار می‌گیرد.

ابزارهای متن‌باز مانند QRLJacker یا EvilQR اجرای این روش را بسیار ساده می‌کنند.

منبع: گاردین

2. فیشینگ با کیو آر کد (QR Phishing)

هکرها QR کدهایی حاوی لینک به صفحات فیشینگ یا دانلود بدافزار ارسال می‌کنند.

کاربر پس از اسکن، به سایت مخرب منتقل شده و اطلاعات ورود خود را وارد می‌کند یا بدون اطلاع، فایل مخربی دریافت می‌کند.

منبع: INTEL741

۳ .حملات صفر- کلیک (Zero-Click Spyware)

ابزارهای جاسوسی تجاری مانند Graphite از شرکتParagon Solutions ، با بهره برداری از آسیب‌پذیری‌های zero-day و بدون نیاز به هیچ تعامل کاربر، روی دستگاه نصب می‌شوند.

این بدافزارها تمام پیام‌ها، تماس‌ها و فایل‌ها را به سرور مهاجم ارسال می‌کنند.

منبع: پیت دفندر

۴ .سوء استفاده از آسیب پذیری های برنامه (Remote Code Execution)

در نسخه‌های دسکتاپ واتساپ برای ویندوز قبل از 2.2450.6، وجود آسیب‌پذیری CVE-2025-30401 به مهاجم اجازه می‌داد، تا با فرستادن یک فایل دست‌کاری‌شده، هنگام باز کردن آن توسط کاربر، کد دلخواه اجرا کند و کنترل سیستم را به دست گیرد.

منبع: WhatsApp Security Advisories 2025

۵ .حملات از طریق تعویض سیم کارت (SIM Swap)

در این روش، مهاجم با ارائه مدارک یا فریب کارکنان اپراتور، شماره قربانی را به سیم کارت خود منتقل می کند و پیامک‌های تأییدیه (SMS) شامل کد ورود واتساپ را دریافت می‌کند.

سپس می‌تواند حساب واتساپ را به طور کامل تصاحب کند.

منبع: Security Week

۶ .نصب APK های مخرب و بد افزارهای موبایل

نسخه‌های مودشده واتساپ یا اپلیکیشن‌های جعلی که در منابع غیر رسمی منتشر می‌شوند، به تروجان ها و جاسوس افزارها آلوده هستند.

نصب این APK ها به هکر ها این امکان را می‌دهد، تمام فعالیت های واتساپ را زیر نظر بگیرند.

منبع: securelist

۷ .کمپین‌های فیشینگ هدفمند (Spear Phishing)

گروه های هکری با ارسال ایمیل یا پیام‌های هدفمند از هویت شرکت ها یا افراد معتبر، کاربران را به وارد کردن کدهای تأیید یا کلیک روی لینکهای مخرب ترغیب می‌کنند.

این روش به ویژه علیه خبرنگاران و مدیران هدفمند است.

منبع: reuters

۸ .نفوذ به گروه‌های واتساپ (Infiltration Scams)

کلاهبرداران با ورود به گروه‌های واتساپ با حساب‌های جعلی، ابتدا اعتماد اعضا را جلب می‌کنند و سپس با درخواست کد تأیید یک بارمصرف یا انتقال وجه تحت عناوین اضطراری، حساب قربانی را تصاحب یا اطلاعات مالی او را سرقت می‌کنند.

منبع: actionfraud

با مطالعه و درک این روش‌ها و رعایت نکات امنیتی مانند روزآمد نگه داشتن اپ، فعالسازی FA2، خودداری از اسکن QRناشناس و دانلود فقط از منابع رسمی، می‌توانید تا حد زیادی از هک حساب واتساپ خود پیشگیری کنید.