انگیزه های افراد از هک واتساپ

پیش از هر چیز، انگیزه‌های هک واتساپ علی رغم تنوع تکنیک‌ها، در سه محور کلی قابل طبقه بندی هستند:

(۱) کسب منافع مالی از طریق سرقت اطلاعات اعتباری و کلاهبرداری مستقیم

(۲) نفوذ به حریم خصوصی افراد برای اهداف جاسوسی، باج‌گیری یا سوءاستفاده شخصی

(۳) نظارت و کنترل بر گروه‌های خاص مانند فرزندان یا کارکنان. در این مقاله، ضمن بررسی هر یک از این دلایل با جزئیات و مثال‌های مستند، به پیامدها و روش‌های مقابله نیز می‌پردازیم.

۱ .کسب منافع مالی

۱,۱ .سرقت اطلاعات بانکی و کارت اعتباری

یکی از رایج‌ترین انگیزه‌ها، فیشینگ یا نصب بدافزار است تا مهاجم اطلاعات بانکی و کارت اعتباری قربانی را سرقت کند. در بسیاری از حملات، لینک‌های فیشینگ یا فایل‌های آلوده از طریق واتساپ ارسال می‌شوند و کاربر با کلیک ناخواسته، کلیه اطلاعات حساس خود را در اختیار هکر قرار می‌دهد.

(indiatvnews)

۱,۲ .کلاهبرداری مستقیم و برداشت غیرمجاز

هکرها گاهی با جعل هویت بانک یا سرویس‌دهنده‌های مالی، کد تأیید یک‌بار مصرف (OTP) را درخواست کرده و پس از دریافت آن، از حساب قربانی برداشت انجام می‌دهند؛ یا با دسترسی به گفتگوهای کاربر، اطلاعات حساس مانند رمزهای عبور را استخراج می‌کنند.

(the420)

۱,۳ .فروش داده‌های کاربران در بازار سیاه

پیام‌ها، شماره تلفن‌ها، لیست مخاطبین و فایل‌های چندرسانه‌ای کاربران در بازارهای زیرزمینی به‌فروش می‌رسد؛ برخی گروه‌های تبهکار حتی پنل مدیریتی واتساپ هک‌شده را تا چند هزار دلار عرضه می‌کنند.

(lexology)

۲ .نفوذ به حریم خصوصی و جاسوسی

۲,۱ .جاسوسی شخصی و باج‌گیری

در مواردی هکرها با دسترسی به پیام‌های خصوصی و تصاویر خانوادگی، افراد را باج‌خواهی می‌کنند. نمونه‌ی برجسته، حملات «Star Blizzard» وابسته به FSB روسیه بود که با فیشینگQR ، حساب مقامات دولتی را هک کردند و تهدید به انتشار مکالمات کردند.

(theguardian)

۲,۲ .جاسوسی سازمانی و دولت‌ها

گروه‌های APT مانند APT42 وابسته به ایران، با جعل پشتیبانی فنی از شرکت‌های معتبر، پیام‌های حاوی لینک‌های مخرب ارسال کردند تا اهداف دیپلماتیک و سیاسی را رصد کنند.

(reuters)

۲,۳ .جاسوسی صنعتی

رقبا یا نفوذگران صنعتی با هک حساب مدیران و مهندسان کلیدی، به اسناد و گفتگوهای محرمانه دسترسی پیدا کرده و برای منافع تجاری خود بهره‌برداری می‌کنند.

(mcafee)

۳ .کنترل و نظارت بر گروه‌های خاص

۳,۱ .نظارت والدین بر فرزندان

برخی والدین به‌دنبال اطمینان از امنیت فرزندان زیر ۱۸ سال خود هستند. در غیاب راهکار رسمی واتساپ برای کنترل والدین، آن‌ها به نیت خیر، به هک حساب فرزند یا نصب نرم‌افزار جاسوسی روی دستگاه او دست می‌زنند.

۳,۲ .نظارت کارفرما بر کارکنان

برخی سازمان‌ها با استدلال حفظ اسرار تجاری و رعایت سیاست‌های داخلی، اقدام به رصد پیام‌های کاری می‌کنند. این امر هم از نظر قانونی و هم اخلاقی نیاز به هماهنگی با کارمندان تحت نظارت دارد.

۳,۳ .کنترل روابط عاطفی

پارتنرهایی که مشکوک به خیانت هستند ممکن است با هک واتساپ همسر یا شریک زندگی‌شان، پیام‌های خصوصی را برای حصول قطعیت بخوانند؛ پدیده‌ای که تبعات حقوقی و روانی قابل‌توجهی دارد.

پیامدها و مخاطرات

۱ .نشت داده و سرقت هویت :اطلاعات خصوصی منتشرشده می‌تواند به سرقت هویت منجر شود و قربانی را در معرض تهدیدات جدید قرار دهد.
۲ .تبعات مالی :برداشت غیرمجاز، کلاهبرداری و باج‌گیری مستقیماً از دارایی‌های قربانی می‌کاهد و جبران آن دشوار است.
۳ .آسیب روانی و اجتماعی :سوءاستفاده از تصاویر یا پیام‌های شخصی می‌تواند اعتبار فرد را خدشه‌دار و روابط خانوادگی و کاری را دچار بحران کند.
۴ .اختلال در کسب‌وکار :انتشار اسناد محرمانه یا افشای گفتگوهای استراتژیک شرکت، به رقبای تجاری امتیاز ناعادلانه می‌دهد.

با شناخت این انگیزه‌ها و رعایت نکات فوق، می‌توان تا حد زیادی از هک شدن واتساپ جلوگیری کرد و امنیت داده‌ها و حریم خصوصی را حفظ نمود.