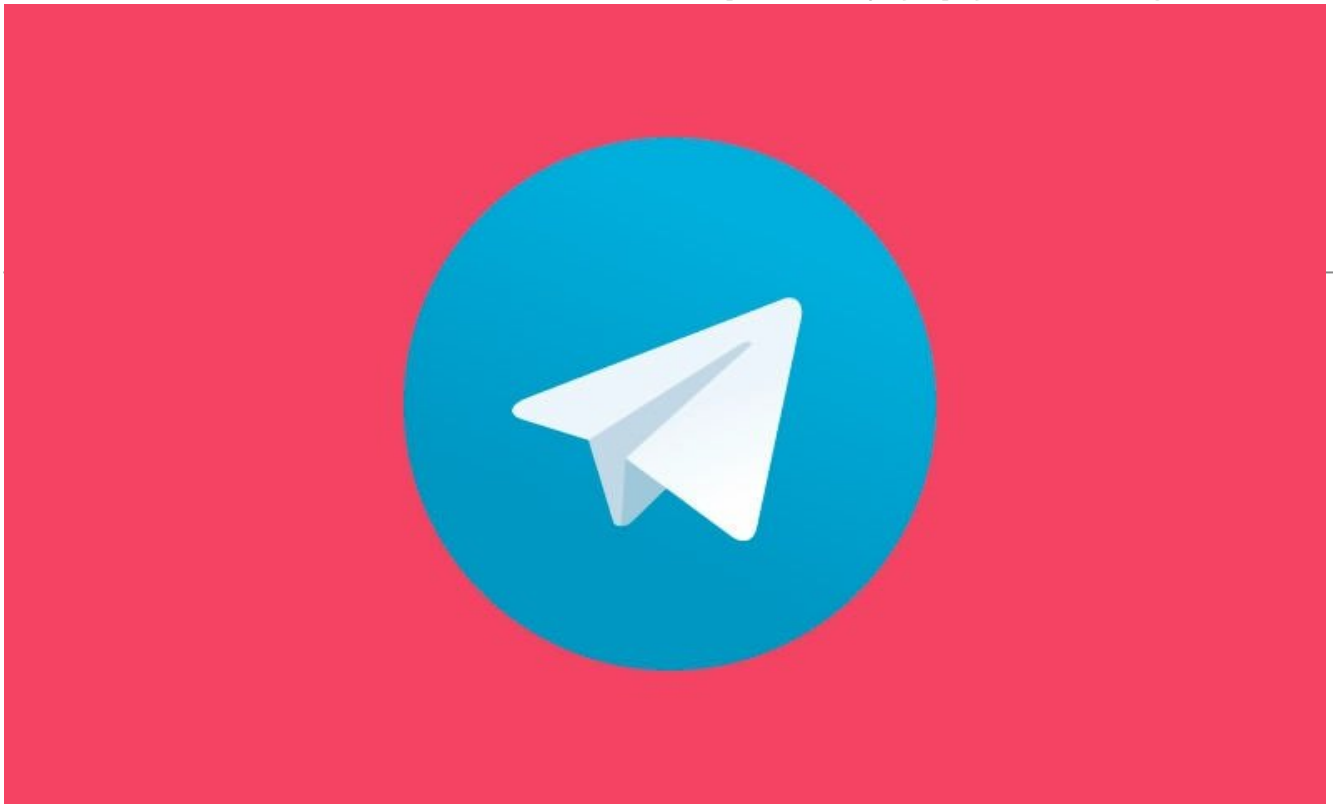
به دلیل مشکلات امنیتی

آیا باید همین الان تلگرام را پاک کنیم؟



تلگرام برنامه پیام‌رسان محبوبی است که بیش از صد میلیون کاربر دارد. شما ممکن است یکی از آن‌ها باشید. اگر این چنین است، شاید بهتر است نگاه عمیق‌تری به این برنامه بیندازید. در این مقاله حقایقی نه چندان خوشایند در ارتباط با تلگرام با شما درمیان گذاشته می‌شود. به‌طوری که شما درمی‌یابید تلگرام به عنوان یک کمپین بازاریابی تجاری آن‌گونه که تصور می‌کنید، امن نیست.

با استناد به مصاحبه‌ای که با کارشناس برجسته رمزنگاری و امنیت انجام شده است، باید به شما بگوییم طیف گسترده‌ای از مسائل امنیتی در ارتباط با این برنامه وجود دارد که آن‌را از یک نرم‌افزار پیام‌رسان مطمئن و ایمن تبدیل به یک برنامه مخاطره‌آمیز کرده است. یکی از مشکلات بزرگ تلگرام این است که این نرم‌افزار به‌طور پیش‌فرض پیام‌ها را رمزنگاری نمی‌کند. موضوعی که در بیشتر مواقع مورد حمایت پلیس فدرال قرار دارد.

[illegible]

بسیاری از کاربران تلگرام فکر می‌کنند ارتباط آن‌ها در یک وضعیت رمزنگاری شده قرار دارد، اما این گروه از کاربران به این حقیقت آگاه نیستند که برای نیل به این هدف باید به بخش تنظیمات پیشرفته تلگرام بروند و آن‌را به‌طور دستی فعال سازند. کریستفور سافویان، تکنولوژیست و تحلیل‌گر ارشد در اتحادیه آزادی‌های مدنی در ایالات متحده در این ارتباط به سایت گیزمودو گفته است: «تلگرام هر آن چیزی که ایالات متحده به آن نیاز دارد را در اختیارش قرار می‌دهد. آیا من ترجیح نمی‌دهم آن‌ها از یک روش رمزنگاری که اکنون به عنوان بهترین روش شناخته شده و توسط برنامه‌هایی همچون واتس‌آپ و سیگنال مورد استفاده قرار می‌گیرد، استفاده کنند؟ بدون شک این چنین است. حتا اگر این ویژگی به‌طور پیش‌فرض فعال نباشد، موضوع مهمی نیست.»

مطلب پیشنهادی

می‌خواهید هک نشوید، مراقب شماره تلفن خود باشید
هک شبکه‌های اجتماعی فقط با یک شماره موبایل!

هیچ‌گونه دلیلی وجود ندارد که پیام‌های شما به‌طور پیش‌فرض رمزنگاری نشده باشند. به ویژه در ارتباط با برنامه‌ای همچون تلگرام که خودش را برنامه‌ای با استانداردهای سطح بالای امنیتی معرفی می‌کند و همواره به این نکته اشاره می‌کند که از بالاترین مکانیزم‌های امنیتی استفاده می‌کند. نکته جالب توجه این است که تلگرام بر خلاف نظر بسیاری از کارشناسان امنیتی، در بخش پرسش و پاسخ‌ها (FAQ) خودش را ایمن‌تر از واتس‌آپ می‌داند. حال سوال اصلی این است، زمانی که فناوری خوبی وجود دارد و به‌طور گسترده مورد استفاده قرار می‌گیرد، چرا نباید از آن استفاده کنیم؟ ما اکنون شاهد آن هستیم که برنامه‌هایی همچون واتس‌آپ از پروتکل‌های رمزنگاری سطح بالایی استفاده می‌کنند که امروزه در دنیای فناوری مورد استفاده قرار گیرند. به‌طوری که هر پیام متنی را به‌طور پیش‌فرض رمزنگاری می‌کنند.

امنیتی که رخنه‌پذیر است!

در کنار این چنین رخنه‌ای که در تلگرام وجود دارد و هیچ‌گونه فرآیند رمزنگاری را روی چت‌ها اعمال نمی‌کند و بدون شک یک امتیاز بزرگ در اختیار هکرها و آژانس‌های دولتی قرار می‌دهد، کارشناسان اعلام کرده‌اند که فناوری رمزنگاری طراحی شده توسط خود این شرکت نیز به احتمال زیاد رخنه‌پذیر است. تلگرام روی فناوری که آن‌را رمزنگارش خودش نامیده است در حال کار است. فناوری که تعدادی از کارشناسان امنیتی مدعی شده‌اند به‌طرز عجیبی در مدت زمان فرآیند رمزنگاری پیام‌ها دارای مشکل امنیتی است. پروفسور آلن وودوارد از دانشگاه Surrey در این ارتباط گفته است: «آن‌ها از پروتکل MTProto که به‌طرز عجیبی بی ثبات است و من مشکلات امنیتی را در نمونه‌های مفهومی آن مشاهده کرده‌ام استفاده می‌کنند.» این پروتکل توسط نیکلای دورف بر مبنای الگوریتم رمزگذاری AES 256 بیتی متقارن، رمزنگاری RSA 2048 و پروتکل تبادل کلید دیفی-هلمن ساخته شده است.

وودوارد از تلگرام به دلیل عدم شفافیت و اطلاع‌رسانی در ارتباط با پروتکل رمزنگاری MTProto انتقاد کرده است. وودوارد در این ارتباط می‌گوید: «در حال حاضر ما هیچ‌گونه اطلاعی نداریم آیا تلگرام ایمن است یا خیر. این ابهامی است که ما با این سیستم ایمن داریم. رمزنگاران به‌طور معمول جزییات مربوط به الگوریتم‌هایی که طراحی کرده‌اند را منتشر می‌سازند، اما در ارتباط با تلگرام ما در تاریکی قرار داریم. شما باید تجربه کامل و قابل توجهی داشته باشید که تصمیم بگیرید خود شخصا دست به طراحی الگوریتم‌های رمزنگاری بزنید. حتا در این حالت نیز طراحی الگوریتم‌های رمزنگاری توسط خود شما کار درستی نیست. هیچ‌کس به درستی نمی‌داند آن‌ها چرا این کار را خودشان انجام داده‌اند.»

[illegible]

سافویان در این ارتباط می‌گوید: «زمانی که کارشناسان جهانی پروتکل سیگنال که از سوی شرکت Open Whisper Systems تولید شده و توسط سیگنال و حتا برنامه Allo گوگل مورد استفاده قرار می‌گیرد را ستایش می‌کنند و واتس آپ نیز از آن استفاده می‌کند، هیچ دلیلی وجود ندارد که شما تصمیم بگیرد رمزگذاری خود را بنویسید.» متیو گرین، استاد رمزنگاری در دانشگاه جان هاپکینز در این ارتباط به Daily Dot گفته است: «آن‌ها به‌طور کلی در حال ساخت یک پروتکل هستند. آن‌ها مجموعه ارزشمند و درخشانی از محاسبات پیچیده ریاضی در اختیار دارند، اما در عمل متخصصان رمزنگاری نیستند، بلکه فقط افرادی باهوش هستند که در نظر دارند پروتکل خود را طراحی کنند. این‌کار دیوانگی است. من نمی‌دانم آیا این پروتکل شکسته می‌شود یا خیر، اما یک چیز عجیب و غریب است.»

وودوارد در بخشی از صحبت‌های خود گفته است: «این برنامه دارای یک نشتی متادیتا است.» اوایل سال جاری میلادی بود که یک کارشناس امنیتی کشف کرد، یک هکر این توانایی را دارد تا تشخیص دهد، چه زمانی یک کاربر آنلاین و چه زمانی آفلاین است. در نتیجه هکر اطلاع پیدا خواهد کرد شما با چه کسی مشغول صحبت کردن هستید و چه زمانی از این برنامه استفاده می‌کنید.

[illegible]

در نهایت اگر به دنبال برنامه‌ای هستید که ارتباطات ایمن در اختیار شما قرار دهد، بهتر است از برنامه‌هایی شبیه به Signal، iMessage و WhatsApp استفاده کنید. تلگرام پتانسیل رخنه‌های بسیاری را در خود جای داده است و ممکن است یکپارچگی خود را به عنوان یک برنامه پیام‌رسان ایمن از دست بدهد.

==========

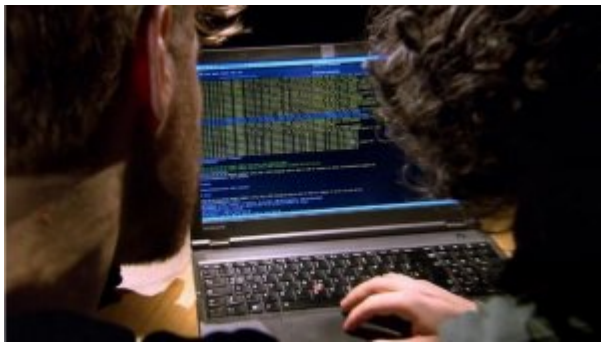
شاید به این مقالات هم علاقمند باشید:

هک شبکه‌های اجتماعی فقط با یک شماره موبایل!

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

تاریخ انتشار:
09 تیر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/3621