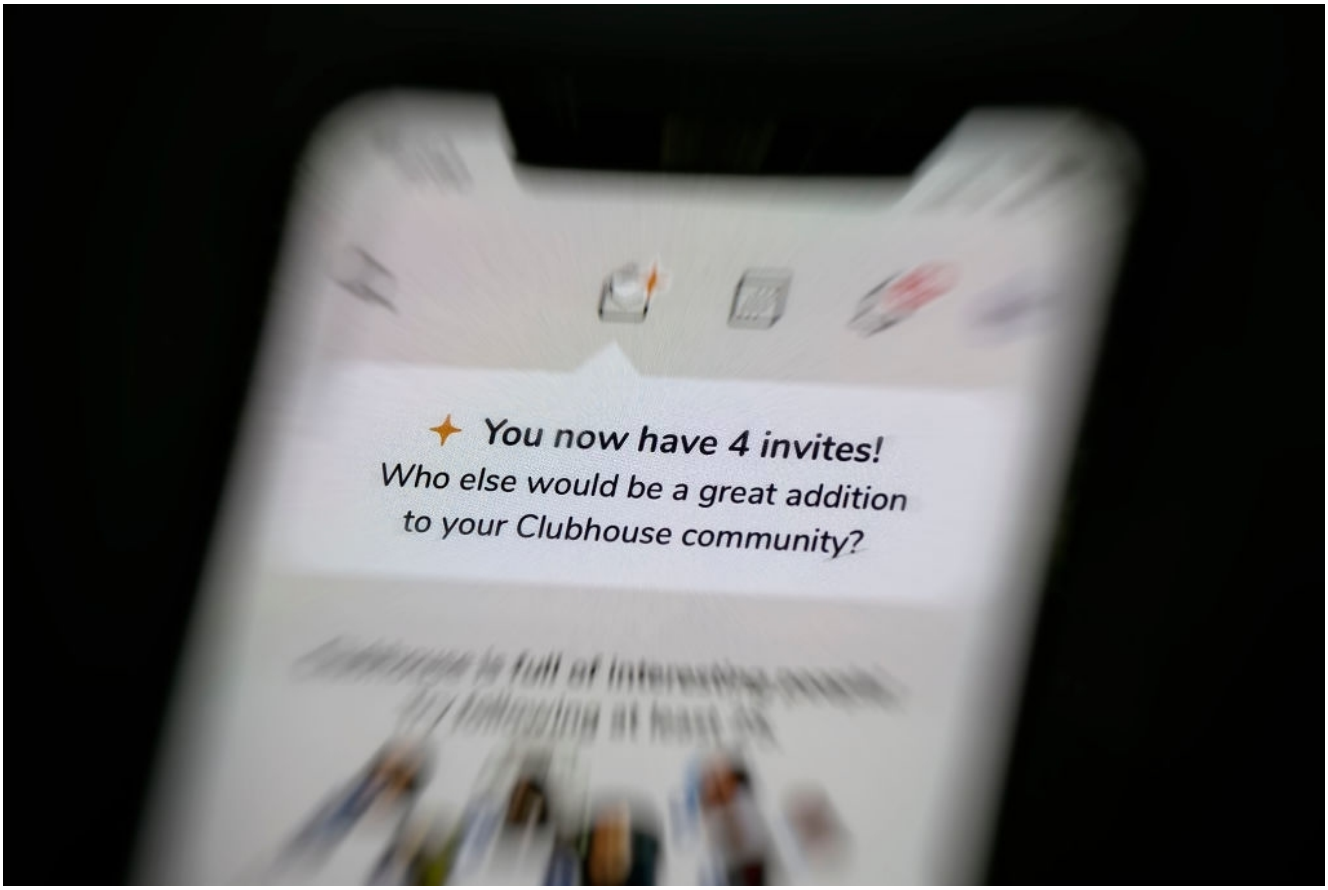
چالش‌های کلاب‌هاوس: فراموشی امنیت و حریم خصوصی زیر سایه رشد انفجاری - دیجیاتو

پیمان حسنی | یکشنبه، ۱۰ اسفند ۱۳۹۹

«کلاب‌هاوس» (Clubhouse) در ماه‌های اخیر خود را به عنوان یکی از استارتاپ‌های اخلالگر سیلیکون ولی مطرح کرده است. این شبکه اجتماعی صوتی در حال رشد است اما در همین ابتدای کار امنیت و حریم خصوصی آن زیر سوال رفته و مدیران ارشد این شرکت را برای تصحیح اشتباهات گذشته به تکاپو انداخته است.

کلاب‌هاوس که در حال حاضر در فاز بتاست و فقط برای iOS در دسترس است، چت روم‌هایی را به کاربرانش ارائه می‌کند که در واقع گروه‌های چت صوتی هستند. می‌توان این روم‌ها را به گونه‌ای تنظیم کرد که برخی کاربران سخنگو و باقی شنونده باشند. آنطور که در گزارش آمده، این پلتفرم بیش از ۱۰ میلیون کاربر داشته و ۱ میلیارد دلار ارزش گذاری شده است. فعلاً فقط بوسیله دعوتنامه می‌توان در آن عضو شد و عضویت افراد مشهوری مثل ایلان ماسک در هفته های اخیر اخیر آن را به تیتر خبرگزاری‌ها تبدیل کرده است.

این پلتفرم اخیراً با مشکلاتی مواجه شده که مورد مختلف از آسیب‌پذیری امنیتی تا ابهامات پیرامون زیرساخت را در برمی‌گیرند. تقریباً یک هفته پیش، محققان سازمان نظارتی Stanford Internet Observatory متوجه شدند که اپ این پلتفرم در حال ارسال برخی از اطلاعات کاربران به شکل رمزنگاری نشده است. این یعنی یک شرکت شخص ثالث احتمالاً می‌توانسته فعالیت‌های کاربر در اپ را رصد کند.



بدتر اینکه محققان اشاره کردند قسمتی از زیرساخت کلاب‌هاوس توسط شرکتی در شانگهای اداره می‌شود و ظاهراً داده‌های اپلیکیشن (حداقل در برخی اوقات) به سرورهایی در چین ارسال شده‌اند. این اتفاق می‌تواند کاربران را در معرض نظارت هدفمند و حتی گسترده دولت چین قرار دهد.

اوایل هفته قبل نیز خبرگزاری بلومبرگ تأیید کرد که یک سایت شخص ثالث در حال استخراج (scrape) چت‌های کلاب‌هاوس بوده است. بررسی‌های بیشتر نشان داد که فایل‌های صوتی این پلتفرم در حال روانه شدن به یک اپلیکیشن اندرویدی بوده‌اند که به کاربران این سیستم عامل اجازه می‌داده به طور بلادرنگ به چت‌ها گوش دهند.

یکی از محققان SIO توضیح می‌دهد که این وب سایت و اپ اندرویدی ظاهراً مخرب نبوده‌اند و هدفشان انتشار محتواهای کلاب‌هاوس برای تعداد بیشتری از کاربران بوده است. اما موضوع نگران کننده این است که کلاب‌هاوس به خاطر نداشتن مکانیزم‌های ضداستخراج طعمه هکرها شده بود. برای مثال، این پلتفرم تعداد روم‌هایی که یک اکانت می‌تواند در آنِ واحد از آنها استریم کند را مشخص نکرده بود، بنابراین هر کاربری می‌توانست با درست کردن یک API، تمام کانال‌های عمومی را استریم کند.

کلاب‌هاوس همچنین به دلیل اتخاذ رویکرد تهاجمی در ذخیره لیست مخاطبین کاربران زیر تیغ انتقادات رفته است. این اپ قویا تمام کاربران را تشویق به اشتراک گذاری داده‌های دفترچه یادداشت آدرس‌ها (Address book) می‌کند تا کاربران بتوانند راحت‌تر همدیگر را پیدا کنند. این اپ همچنین از کاربر می‌خواهد تا مجوز دسترسی به لیست مخاطبین برای ارسال دعوتنامه به دیگران را بدهد. چندین نفر از کاربران گفته‌اند که این اپ حین ارسال دعوتنامه، پیشنهادات را بر اساس شماره تلفن‌های موجود در لیست مخاطبین آنها و کاربران دیگر ارائه می‌کند. به عبارت دیگر، اگر شما و دوستانی که در نزدیکی شما هستند از یک پزشک، گل فروش یا داروخانه استفاده می‌کنید، تمام آن‌ها می‌توانند در لیست افراد پیشنهادی نمایش داده شوند.

کلاب‌هاوس در بیانیه‌ای به سازمان SIO وعده ارتقاء امنیت از جمله قطع ارتباط با سرورهای چین و تقویت رمزنگاری داده را داده است. این شرکت افزود که برای شفافیت بیشتر در این رابطه، با یک کمپانی امنیتی شخص ثالث همکاری می‌کند. کلاب‌هاوس در واکنش به استریم چت‌های صوتی خود روی یک وب سایت دیگر گفت که دسترسی کاربر خاطی را برای همیشه مسدود کرده و اضافه کرد که به کمک سپرهای امنیتی اضافه از رخدادن اتفاقات مشابه در آینده جلوگیری می‌کند.

با اینکه به نظر می‌رسد کلاب‌هاوس بازخورد محققان امنیتی را جدی گرفته، هنوز برنامه‌ای مشخص برای بهبود امنیت اپ خود ارائه نکرده است. محققان اضافه می‌کنند از آنجا که این اپ ظاهراً از رمزنگاری دو سویه استفاده نمی‌کند، احتمالاً هنوز تمایلی به برداشتن گام‌های جدی برای ارتقاء امنیت خود ندارد.

بد نیست به مشکلات حریم خصوصی در این اپ نیز اشاره‌ای کنیم. کاربر حین ایجاد «روم» جدید با سه گزینه روبرو می‌شود: «باز» که همه می‌توانند وارد آن شوند، «اجتماعی» فقط به فالوورها اجازه ورود می‌دهد و در نهایت «بسته» که دسترسی را منوط به دعوتنامه می‌کند. هر اتاق یا روم تنظیمات حریم خصوصی خود را دارد که پنهان هستند و کلاب‌هاوس حداقل می‌تواند آنها را آشکارتر کند.

محقق ارشد فناوری از SIO می‌گوید: «من فکر می‌کنم کلاب‌هاوس باید به کاربران این مساله را به طور کاملاً واضح بگوید که عمومی یعنی اینکه تمام کاربران می‌توانند به اتاق‌های عمومی دسترسی پیدا کنند و همه می‌توانند از حرف‌ها یادداشت برداری کنند. برای اتاق‌های خصوصی نیز آنها باید بگویند که همانند تمام مکانیزم‌های ارتباطی، افرادی که مجوز دارند می‌توانند محتواها و هویت شرکت کنندگان را ذخیره کنند، بنابراین کاربر باید سطح انتظارات را معین کرده و به شرکت کنندگان اعتماد کند.»

کلاب‌هاوس تقریباً همانند تمامی شبکه‌های اجتماعی، با مشکل سوءاستفاده دست به گریبان است. این اپ در قوانین خود نفرت پراکنی، نژادپرستی و آزاد و اذیت را ممنوع اعلام کرده و برخی قابلیت‌های مدیریت محتوا مثل مسدودسازی کاربران یا برچسب گذاری روم‌ها را ارائه می‌کند. یکی از بزرگترین قابلیت‌های کلاب‌هاوس خودش عامل سوءاستفاده است: چت‌های کاربران در این پلتفرم برای همیشه ذخیره نمی‌شوند و همین مساله سبب می‌شود تا برخی کاربران بدون در نظر گرفتن پیامدها هر چه می‌خواهند به زبان بیاورند.

یکی از محققان SIO می‌گوید کلاب‌هاوس در حال حاضر فایل‌های صوتی را در صورت شکایت کاربران از سوءاستفاده به طور موقت ذخیره می‌کند. اگر این شرکت از رمزنگاری دو سویه استفاده می‌کرد، کار به مراتب سخت تری برای مدیریت سوءاستفاده داشت چون دیگر نمی‌توانست به راحتی هویت سخنگوی فایل صوتی را تشخیص دهد.

بسیاری از شبکه‌های اجتماعی با چنین تناقضی روبرو هستند، با این وجود برخی متخصصین امنیتی معتقدند مزیت‌های رمزنگاری دوسویه به چالش‌های توسعه راهکارهای ضد سوءاستفاده فرعی می‌چربد. حتی اضافه شدن رمزنگاری دوسویه نیز ضبط نشدن مکالمه‌ها توسط کاربران را تضمین نمی‌کند و این مشکلی است که کلاب‌هاوس به سادگی قادر به حل کردن آن نخواهد بود.

دیجیاتو