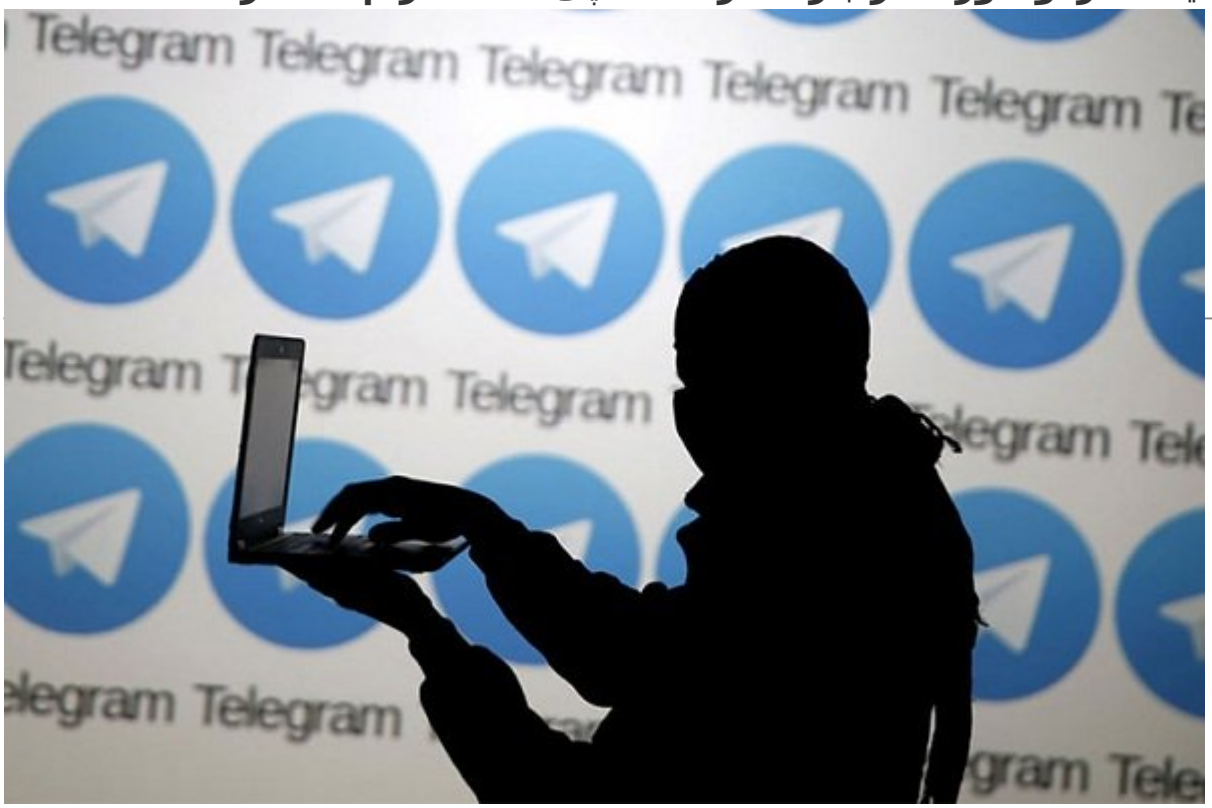
نتیجه تحقیقات رگولاتوری در باره سرقت آی‌پی‌های تلگرام منتشر شد



پس از دستور وزیر ارتباطات و فناوری اطلاعات برای پیگیری ماجرای هایجک BGP تلگرام، رگولاتوری گزارش بررسی های خود را منتشر کرد و خبر از معرفی کارشناسان شرکت مخابرات به مراجع امنیتی خبر داد.

اواسط هفته جاری موضوع هایجک شدن BGP (پروتکل مسیریابی) **تلگرام** توسط شرکت مخابرات ایران رسانه‌ای شد و وزیر ارتباطات و فناوری اطلاعات در واکنشی به این موضوع، اظهار کرد که در صورت تأیید خطا چه سهوی یا عمدی، مخابرات ایران، جریمه سنگینی خواهد شد.
وزیر ارتباطات و فناوری اطلاعات با بیان اینکه سازمان تنظیم مقررات و ارتباطات رادیویی مأمور رسیدگی به این موضوع شده است، گفت: بنابر گزارش هایی که دریافت کردم، مخابرات ایران روز هشتم مرداد ماه از ساعت 4 تا 6 بامداد درگیر تغییر توپولوژی و تجمیع شبکه استانی خود در شیراز و بوشهر بوده است.
با این حال وی قول پیگیری تا روشن شدن این موضوع را داد؛ حال سازمان تنظیم مقررات و ارتباطات رادیویی نتیجه بررسی هایش درباره اختلال در مسیریابی بین‌الملل را منتشر کرد.

گزارش سازمان تنظیم مقررات و ارتباطات رادیویی از بررسی اختلال در مسیریابی

بین الملل:

«در بررسی ابتدایی، با دستور فوریت بالای وزیر بررسیهای بیشتری با حضور متخصصان این حوزه به عمل آمد که علت مرتبط با عملیات تغییر توپولوژی و تجمیع شبکه استانی در استانهای شیراز و بوشهر توسط مخابرات ایران در ساعات 4 الی 6 بامداد تشخیص داده شده بود.
با رخ دادن BGP Hijacking، Prefix های متعددی که توسط شرکت مخابرات ایران(استان خراسان شمالی) با دستور قضایی برای فیلترینگ و جلوگیری از مسیریابی ترافیک های مربوطه، به روش Static Route به اینترفیس NULL مسیریابی شده بودند، از طریق **پروتکل BGP** در شبکه بین‌الملل منتشر می‌شوند.
شرکت مخابرات ایران در چندین نقطه با سایر اپراتورها برروی پروتکل BGP جهت انتقال ترافیک بین‌الملل (اینترنت) دارای همسایگی است و علاوه بر آن شرکت مذکور در این نقاط دارای Prefix filtering برای جلوگیری از شکل گرفتن سناریوهای BGP Hijacking بوده است.
در زمان رخداد در یکی از این چند نقطه، Prefix Filtering فی مابین با وارد کردن یک کامند غیرفعال شده است که در اثر آن مسیرهای Static از طریق پروتکل BGP به همسایه BGP انتشار مجدد یافته و متعاقباً به لینک بین‌الملل ارسال می‌شود.
این موضوع باعث اختلال در سیستم روتینگ بین‌الملل شده و باعث شد بلافاصله تمامی مسیریاب های بین‌الملل جداول مسیریابی خود را بروزنمایی کنند و ترافیک های غیر مرتبط به شبکه شرکت مخابرات ایران و به روتر استان خراسان شمالی مسیریابی شود.
با آگاهی از موضوع Prefix Filtering مربوطه مجددا توسط تیم کارشناسی بازگردانده شد و رخداد متوقف و شبکه به شرایط قبل از رخداد بازگردانده می‌شود و کل این اختلالات حدود سه دقیقه به طول انجامید.
در ادامه بررسیهای انجام شده شواهدی دال بر اراده و تصمیمی سازمان یافته به‌دست نیامد اما اقدام نادرست کارشناس مسئول محرز است، لیکن با توجه به شواهدی مبنی بر حذف مستندات سیستمی تغییرات (LOG) و اهمیت این اطلاعات در ردیابی رخداد و همچنین حساسیت موضوع و احتمال عمدی بودن و دستکاری هدفمند در فقره اخیر و وجود برخی ابعاد غیر فنی، اشخاص مرتبط به همراه مستندات توسط شرکت مخابرات ایران برای بررسی های لازم به مراجع ذی‌صلاح امنیتی معرفی شدند.
بدیهی است در آینده، نتایج بررسی ها توسط مراجع نام برده به اطلاع عموم می‌رسد.
شرکت مخابرات ایران به عنوان یکی از اپراتورهای دارنده پروانه از سازمان تنظیم مقررات و ارتباطات رادیویی نسبت به تعهدات پروانه‌ای خود مسئولیت دارد و با توجه به ابعاد اهمیت این موضوع و تأکید وزیر و همچنین با وجود عدم احراز مشکل سازمانی، این موضوع در کمیته تخلفات اپراتورهای سازمان تنظیم مقررات طرح می‌شود و نسبت به رسیدگی کامل و حسب مورد جرایم مربوطه، مطابق مفاد پروانه اپراتور، اقدام می‌شود.
سازمان تنظیم مقررات و ارتباطات رادیویی ضمن تأکید بر حفظ امنیت و صیانت از داده‌های شخصی کاربران و رعایت قوانین و پروتکلهای بین‌المللی، ضمن برخورد با این اتفاق، با جدیت بیش از پیش و با هماهنگی یکپارچه فعالان این عرصه نهایت تلاش خود را در جهت پیشگیری انجام می‌دهد.»

منبع:

tasnimnews
تاریخ انتشار:
16 مرداد 1397

نشانی منبع:
https://www.shabakeh-mag.com/news/iran/13605/%D9%86%D8%AA%DB%8C%D8%AC%D9%87-%D8%AA%D8%AD%D9%82%DB%8C%D9%82%D8%A7%D8%AA-%D8%B1%DA%AF%D9%88%D9%84%D8%A7%D8%AA%D9%88%D8%B1%DB%8C-%D8%AF%D8%B1-%D8%A8%D8%A7%D8%B1%D9%87-%D8%B3%D8%B1%D9%82%D8%AA-%D8%A2%DB%8C%E2%80%8C%D9%BE%DB%8C%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AA%D9%84%DA%AF%D8%B1%D8%A7%D9%85-%D9%85%D9%86%D8%AA%D8%B4%D8%B1-%D8%B4%D8%AF