بیان مساله: اختلال نرم افزار از اواخر روز پنج شنبه ۱۹ فروردین ماه ۱۴۰۰ در اپراتورهای همراه اول، ایرانسل و مخابرات ایران قابل مشاهده بود. بررسی‌های اولیه نشان می‌داد روال‌های قانونی اعم‌از مصوبه کمیته تعیین مصادیق محتوای مجرمانه یا دستور مقام قضایی در این خصوص وجود ندارد. در بررسی‌های بعدی نیز صحت این موضوع به تایید رسید.

لذا این سازمان جهت رفع اختلالات پیش آمده ، مهلت ۲۴ ساعته‌ای را برای اپراتورهای مشمول این اختلالات تعیین نمود. لیکن پیگیری‌های بعمل‌آمده نشانگر آن است که اختلالات بوجودآمده رفع‌نشده است.

دراین‌خصوص و در ادامه ، روش‌های اعمال‌شده برای بوجود آمدن اختلال در اپراتورهای مختلف به‌تفصیل بیان می‌شود:

شرکت ارتباطات سیار ایران (همراه اول)

تغییر در DNS شرکت همراه اول

الف- DNS[1] های(خدمات‌دهندگان نام دامنه) شرکت همراه اول (به‌عنوان نمونه DNS سرور به آدرس ۱۰,۱۰,۸۵,۱۲۴) در پاسخ به دامنه clubhouseapi.com، آدرس ۱۰,۱۰,۳۴,۳۴ (صفحه پیوندها)را به کاربر بازمی‌گردانند(شکل۱)، که این امر موجب مسدودسازی کلاب هاوس بر روی آن اپراتور گردیده‌است.

شکل ۱: بازگرداندن آدرس ۱۰.۱۰.۳۴.۳۴

[1] Domain Name Server

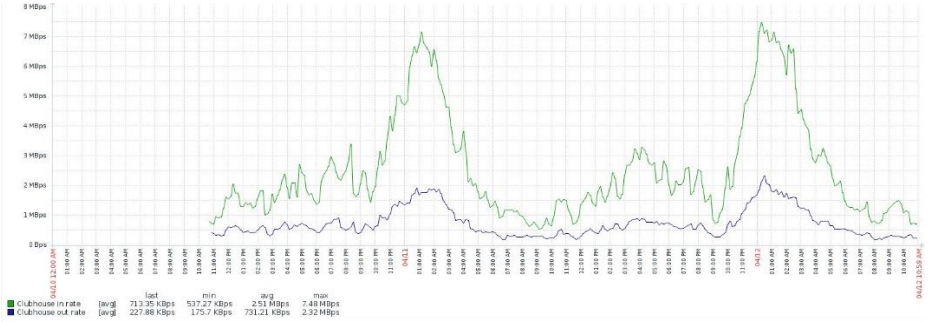
همچنین این اپراتور مسدودسازی را از دامنه ذکرشده بالا خارج و اقدام به مسدودسازی آدرس www.clubhouseapi.com نمود و در ادامه دامنه maintenance.joinclubhouse.com را نیز در DNS سرورهای خود مسدودنمود.

ب- تغییر دیگر انجام شده در روش مسدود سازی می‌باشد که به‌جای بازگرداندن آدرس پیوندها اقدام‌به عدم پاسخ به آدرس سایت مذکور نموده‌است. به‌نحوی که پاسخی برای درخواست این دامنه‌ها از سوی DNS سرورهای آن شرکت داده نمی‌شود. اما با DNSهای دیگر مانند ۸٫۸٫۸٫۸ پاسخ داده‌می‌شود و این موضوع نشان‌می‌دهد که این دامنه برروی DNS های اپراتور همراه اول مسدودشده‌است(شکل ۲).

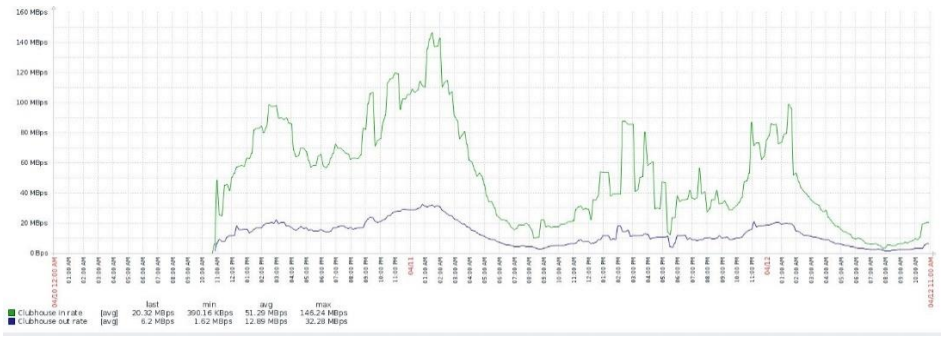
شکل۲: تفاوت در بازگرداندن آدرس از دو طریق DNS شرکت همراه اول و ۸.۸.۸.۸

لازم به‌ذکراست در ابتدای اختلال باتوجه به‌وجود DNS Cache احتمالاً ۱۰۰٪ کاربران با انسداد مواجه نمی‌شدند.

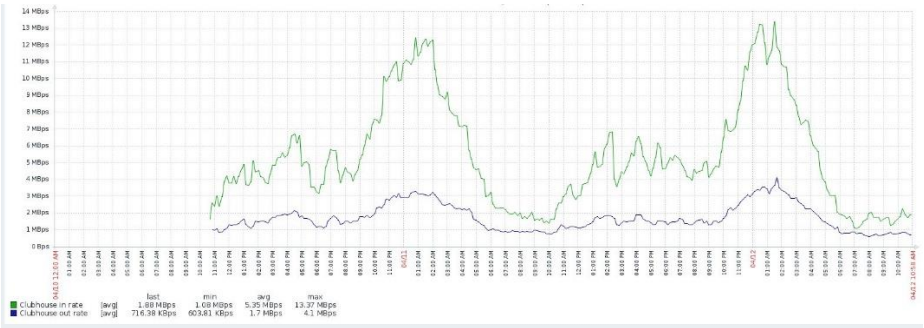
در ادامه نمودار های ترافیک این نرم‌افزار در بخش های مختلف کشور در سامانه های اپراتور همراه اول ارائه‌می‌شود(نمودارهای ۱-۴).



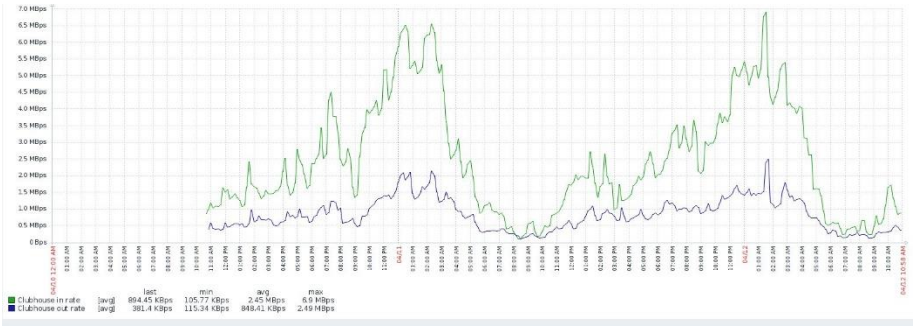
نمودار۱: نمودار ترافیک نرم‌افزار کلاب هاوس در شمال غرب کشور(همراه اول)



نمودار ۲: نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های شمالی کشور(همراه اول)



نمودار ۳: نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های جنوبی کشور(همراه اول)

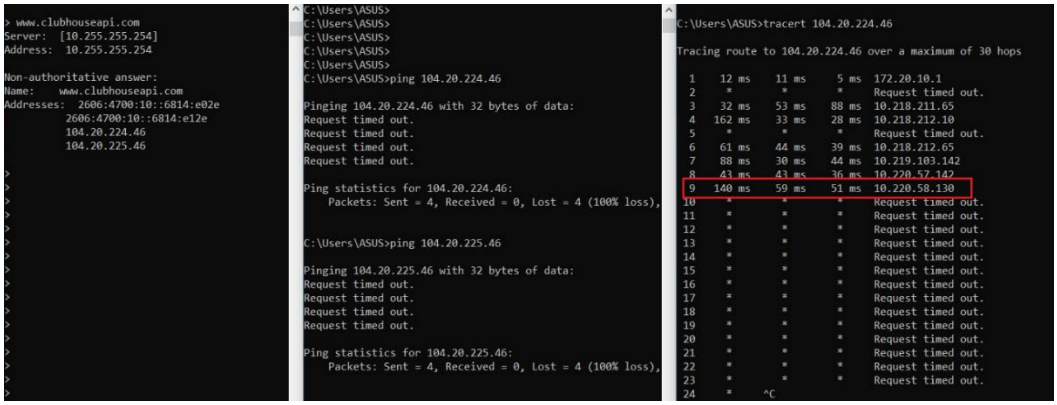


نمودار ۴: نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های شرقی کشور(همراه اول)

شرکت ارتباطات ایرانسل

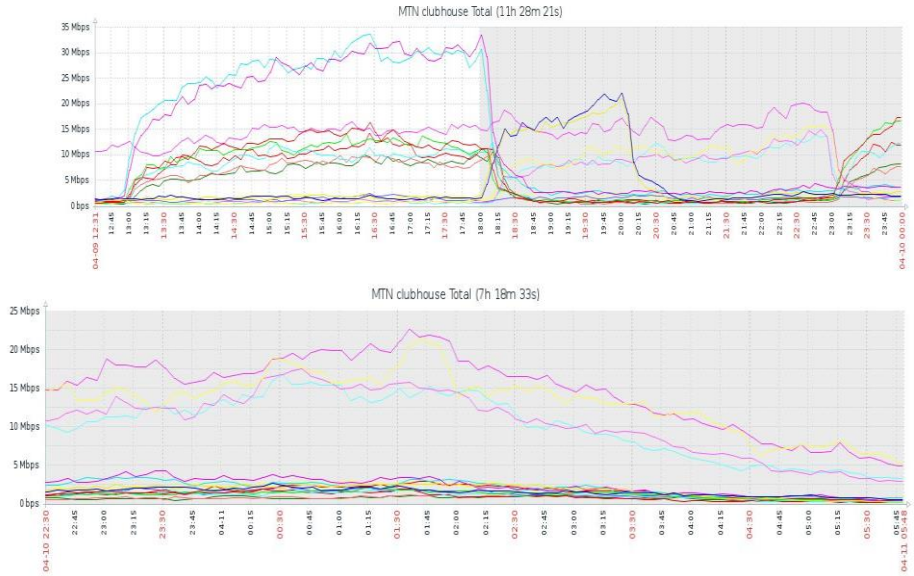
الف - تغییر در نحوه مسیریابی

در اپراتور ایرانسل مسدود سازی به صورت آی پی در برخی مناطق انجام شده‌است بدین صورت که ابتدا IP های دامنه www.clubhouseapi.com استخراج شده‌است و سپس برروی روتر آن اپراتور مسدود گردیده‌است(شکل ۳).



شکل ۳: نتیجه تغییر در مسیریابی تجهیزات شبکه

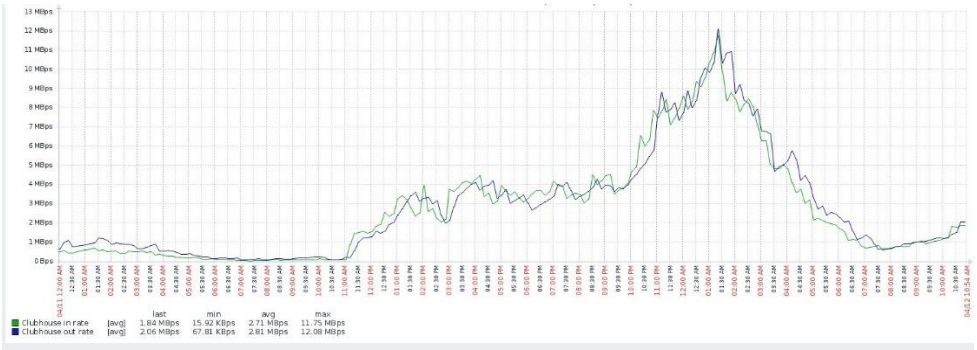
همچنین از گراف‌های زیر می‌توان زمان انسداد و نوع رفتار اپراتور در قبال انسداد را شاهد بود. در تصویر زیر مشخص است که اپراتور ایرانسل اقدام به مسدود سازی در برخی مناطق خود نموده و در برخی مناطق دیگر انسداد را حذف می‌نماید.(تاریخ گراف مربوط به روز جمعه مورخ ۲۰ فروردین ماه) واین انسداد بگونه‌ای به‌نظرمی‌رسد که کاربر احساس‌می‌کند برنامه کلاب هاس دچار اختلال می‌باشد. به‌طور مثال آن شرکت برنامه مذکور را در مرکز کشور مسدودمی‌نماید و در مناطق غربی کشور سیاستی برای آن اعمال نمی‌نماید، پس‌از مدتی این سیاست تغییرمی‌کند و برنامه در غرب کشور نیز مسدودمی‌شود و در مناطق مرکزی باز می‌شود.



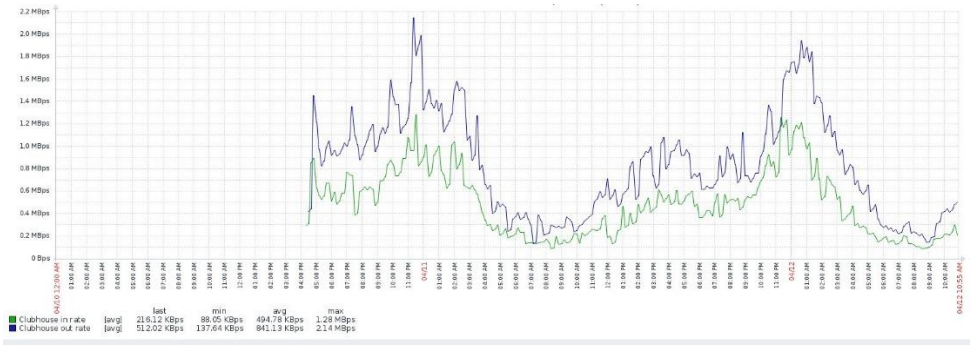
ب- حذف بسته‌ها:

بعد از برقراری ارتباط بین کاربر و سامانه مرکزی نرم‌افزار[2]، تجهیزات شبکه اپراتور با درصد بالایی بسته‌های ارتباطی را حذف‌می‌کند و این کار باعث اختلال شدید می‌شود و پیام‌رسان مکرراً جهت برقراری مجدد ارتباط، اقدام‌می‌نماید و کاربر پس‌از طی زمان انتظار طولانی به این نتیجه می‌رسد که ارتباط ممکن نیست.

در ادامه نمودارهای ترافیک این نرم‌افزار در بخش‌های مختلف کشور در سامانه‌های اپراتور ایرانسل ارائه‌می‌شود(نمودارهای ۵- ۸).

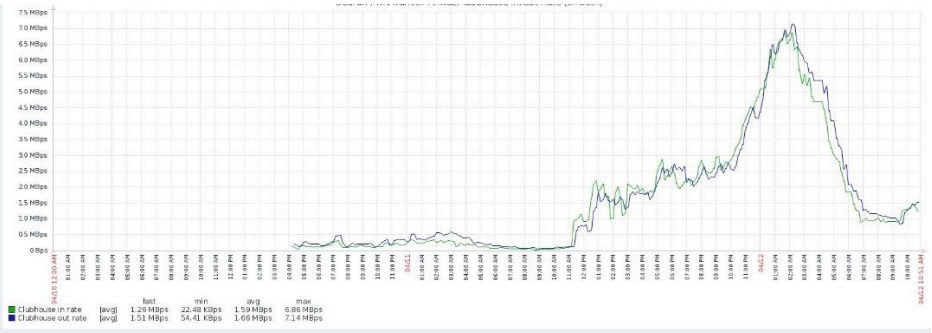


نمودار ۵: نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های غربی کشور(ایرانسل)

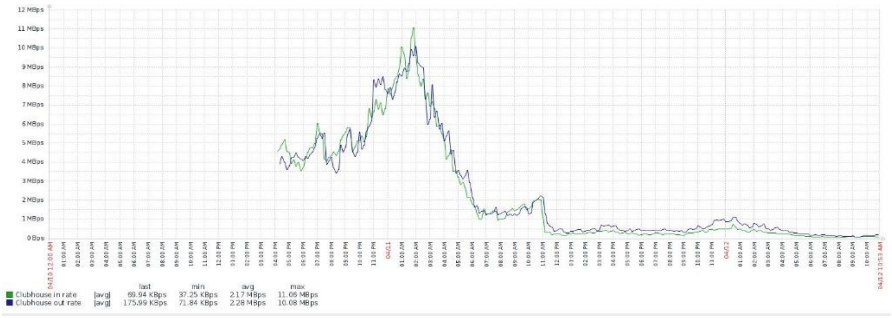


نمودار ۶: نمودار ترافیک نرم‌افزار کلاب هاوس در شمال کشور(ایرانسل)

[2] three way hand shaking& client hello



نمودار ۷ نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های شرقی کشور(ایرانسل)

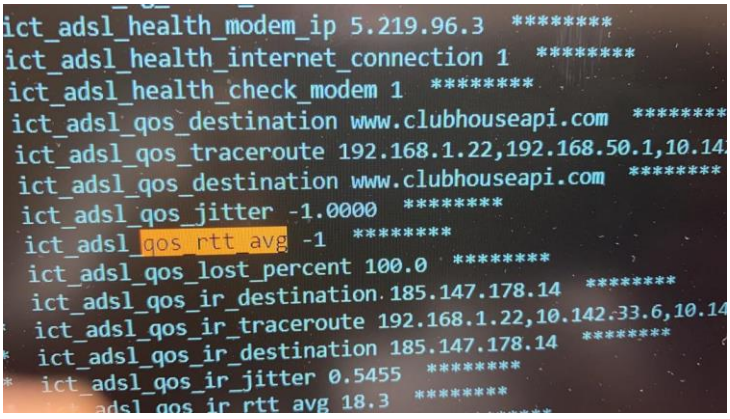


نمودار ۸: نمودار ترافیک نرم‌افزار کلاب هاوس در استان‌های جنوبی کشور (ایرانسل)

شرکت مخابرات ایران

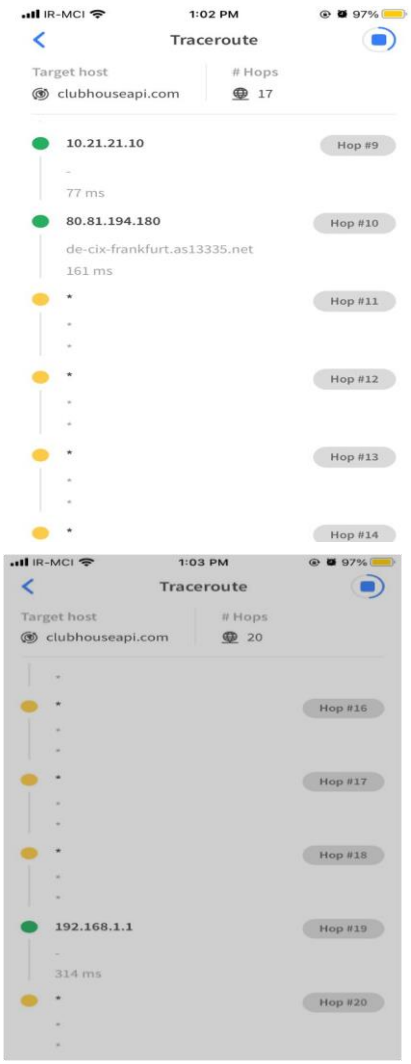
تغییر در نحوه مسیریابی شرکت مخابرات ایران

در این اپراتور مسدودسازی به‌صورت آدرس آی پی نیز انجام‌شده‌است بدین‌صورت که ابتدا IPهای دامنه www.clubhouseapi.com استخراج شده‌است و سپس برروی روتر آن اپراتور مسدودگردیده‌است(شکل ۴).



شکل۴ نتیجه تغییر در مسیریابی تجهیزات شبکه

این انسداد بگونه‌ای به‌نظرمی‌رسد که کاربر احساس‌می‌کند برنامه کلاب هاس دچار اختلال می‌باشد(شکل ۵).



شکل۵: عدم امکان دسترسی به آدرس ازطریق شبکه شرکت مخابرات ایران