

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. بررسی های اولیه نشان می داد روال های قانونی اعم از مصوبه کمیته تعیین مصادیق محتوای مجرمانه یا دستور مقام قضایی در این خصوص وجود ندارد. در بررسی های بعدی نیز صحت این موضوع به تایید رسید.

لذا این سازمان جهت رفع اختلالات پیش آمده ، مهلت ۲۴ ساعته ای را برای اپراتورهای مشمول این اختلالات تعیین نمود. لیکن پیگیری های بعمل آمده نشانگر آن است که اختلالات بوجود آمده رفع نشده است.

در این خصوص و در ادامه ، روش های اعمال شده برای بوجود آمدن اختلال در اپراتورهای مختلف به تفصیل بیان می شود:

شرکت ارتباطات سیار ایران (همراه اول)

تغییر در DNS شرکت همراه اول

الف - DNS های (خدمات دهندگان نام دامنه) شرکت همراه اول (به عنوان 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 بازمی گردانند (شکل ۱)، که این امر موجب مسدودسازی کلاب هاوس بر روی آن اپراتور گردیده است.



شکل ۱: بازگرداندن آدرس ۱۰.۱۰.۳۴.۳۴

¹ Domain Name Server

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

ب- تغییر دیگر انجام شده در روش مسدودسازی می باشد که به جای بازگرداندن آدرس پیوندها اقدام به عدم پاسخ به آدرس سایت مذکور نموده است. به نحوی که پاسخی برای درخواست این دامنه ها از سوی DNS سرورهای آن شرکت داده نمی شود. اما با DNS های دیگر مانند ۸.۸.۸.۸ پاسخ داده می شود و این موضوع نشان می دهد که این دامنه بر روی DNS های اپراتور همراه اول مسدود شده است (شکل ۲).

```

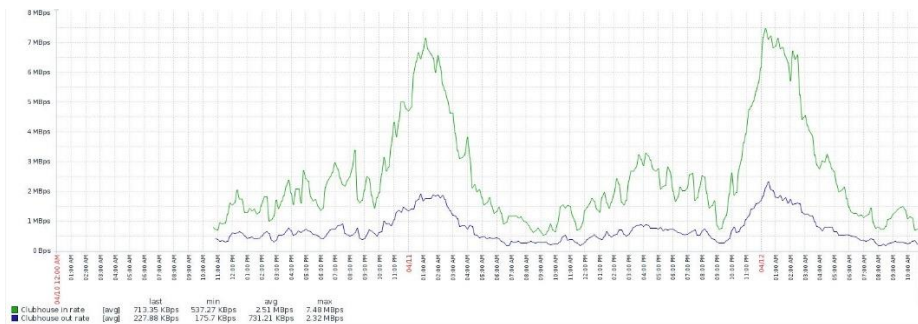
> www.clubhouseapi.com
Server: pubns3.te.epc.mci.ir
Address: 10.10.85.118
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to pubns3.te.epc.mci.ir timed-out
> server 8.8.8.8
Default Server: dns.google
Address: 8.8.8.8

> www.clubhouseapi.com
Server: dns.google
Address: 8.8.8.8
Non-authoritative answer:
Name: www.clubhouseapi.com
Addresses: 2606:4700:10::6814:e02e
           2606:4700:10::6814:e12e
           104.20.224.46
           104.20.225.46

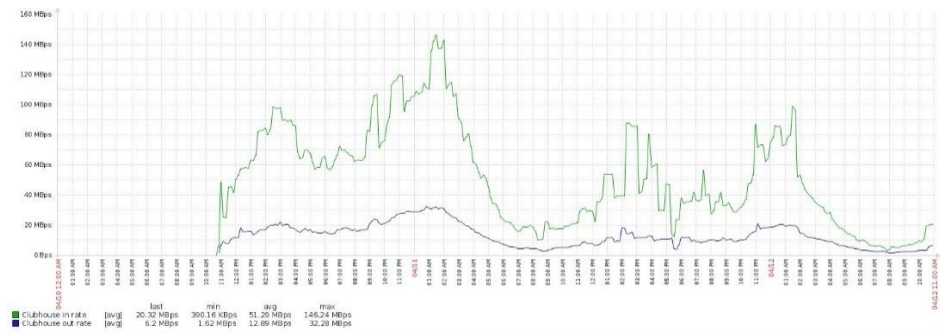
```

شکل ۲: تفاوت در بازگرداندن آدرس از دو طریق DNS شرکت همراه اول و ۸.۸.۸.۸

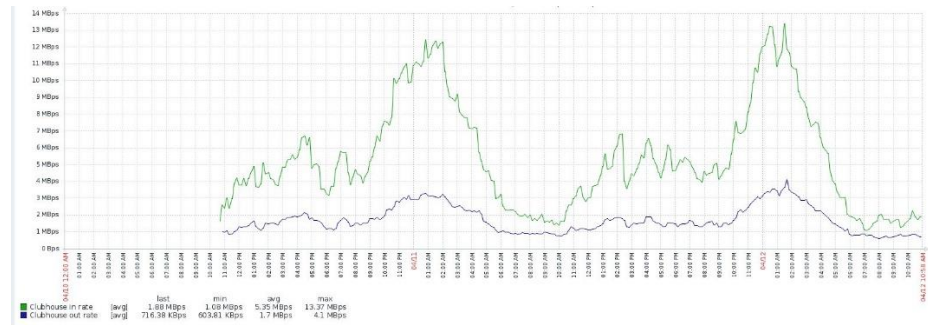
لازم به ذکر است در ابتدای اختلال با توجه به وجود DNS Cache احتمالاً ۱۰٪ کاربران با انسداد مواجه نمی شدند. در ادامه نمودارهای ترافیک این نرم افزار در بخش های مختلف کشور در سامانه های اپراتور همراه اول ارائه می شود (نمودارهای ۱-۴).



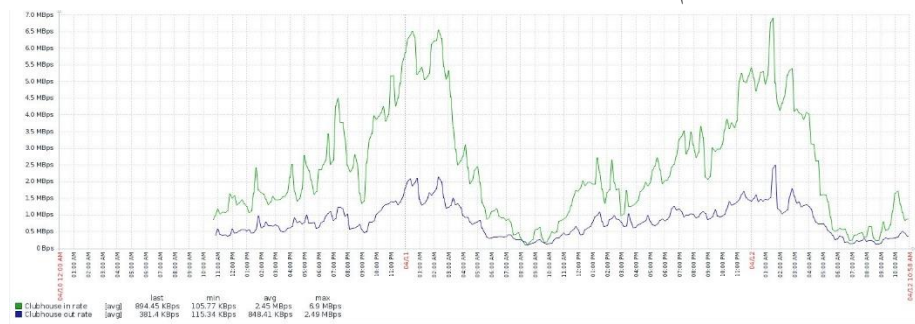
نمودار ۱: نمودار ترافیک نرم افزار کلاب هاوس در شمال غرب کشور (همراه اول)



نمودار ۲: نمودار ترافیک نرم افزار کلاب هاوس در استان های شمالی کشور (همراه اول)



نمودار ۳: نمودار ترافیک نرم افزار کلاب هاوس در استان های جنوبی کشور (همراه اول)



نمودار ۴: نمودار ترافیک نرم افزار کلاب هاوس در استان های 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 شده است بدین صورت که ابتدا IP های دامنه www.clubhouseapi.com استخراج شده است و سپس بر روی روتر آن اپراتور مسدود گردیده است (شکل ۳).

```

> www.clubhouseapi.com
Server: [10.255.255.254]
Address: 10.255.255.254

Non-authoritative answer:
Name: www.clubhouseapi.com
Addresses: 2606:4700:10:6814:e02e
          2606:4700:10:6814:e12e
          104.20.224.46
          104.20.225.46
>>>

C:\Users\ASUS>
C:\Users\ASUS>
C:\Users\ASUS>
C:\Users\ASUS>ping 104.20.224.46
Pinging 104.20.224.46 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 104.20.224.46:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ASUS>ping 104.20.225.46
Pinging 104.20.225.46 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

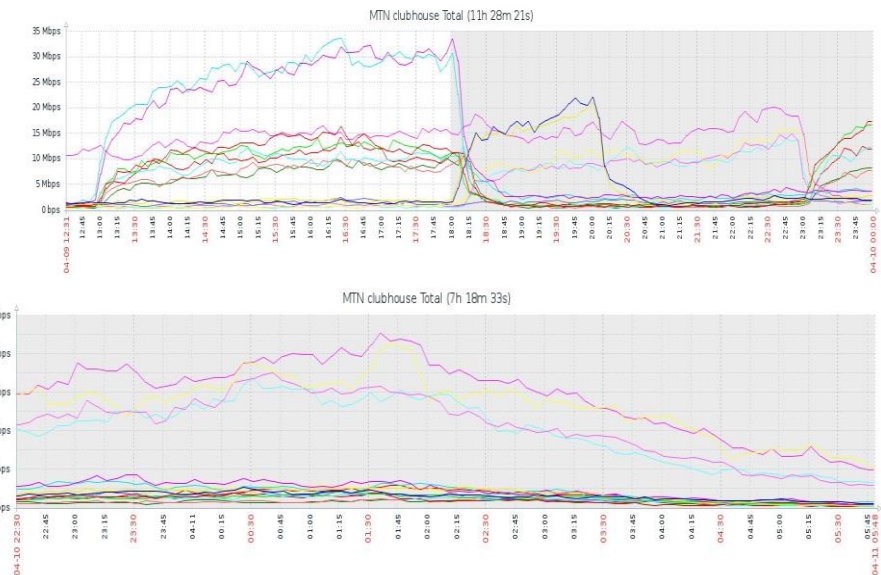
Ping statistics for 104.20.225.46:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ASUS>tracert 104.20.224.46
Tracing route to 104.20.224.46 over a maximum of 30 hops:
  0  12 ms  11 ms  5 ms  172.20.10.1
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  32 ms  53 ms  88 ms  10.218.211.65
  4  162 ms 33 ms  28 ms  10.218.212.10
  5  *      *      *      Request timed out.
  6  61 ms  44 ms  39 ms  10.218.212.65
  7  88 ms  30 ms  44 ms  10.219.103.142
  8  43 ms  43 ms  36 ms  10.220.57.142
  9  140 ms 59 ms  51 ms  10.220.58.130
 10  *      *      *      Request timed out.
 11  *      *      *      Request timed out.
 12  *      *      *      Request timed out.
 13  *      *      *      Request timed out.
 14  *      *      *      Request timed out.
 15  *      *      *      Request timed out.
 16  *      *      *      Request timed out.
 17  *      *      *      Request timed out.
 18  *      *      *      Request timed out.
 19  *      *      *      Request timed out.
 20  *      *      *      Request timed out.
 21  *      *      *      Request timed out.
 22  *      *      *      Request timed out.
 23  *      *      *      Request timed out.
 24  *      *      *      Request timed out.

```

شکل ۳: نتیجه تغییر در مسیریابی تجهیزات شبکه

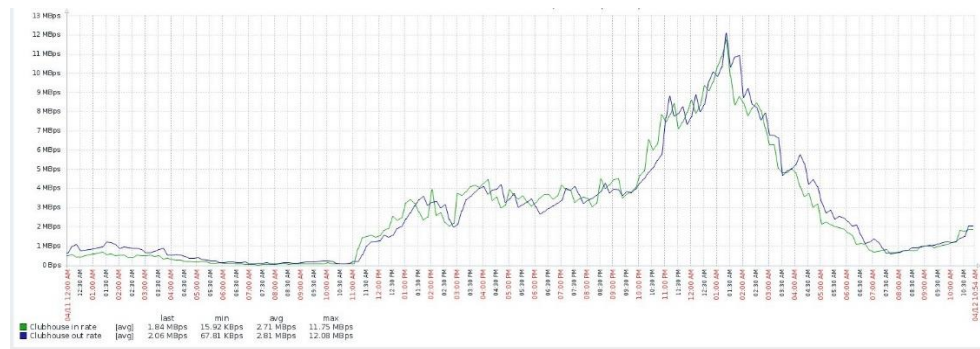
همچنین از گراف‌های زیر می‌توان زمان انسداد و نوع رفتار اپراتور در قبال انسداد را شاهد بود. در تصویر زیر مشخص است که اپراتور ایرانسل اقدام به مسدود سازی در برخی مناطق خود نموده و در برخی مناطق دیگر انسداد را حذف می‌نماید. (تاریخ گراف مربوط به روز جمعه مورخ ۲۰ فروردین ماه) و این انسداد بگونه‌ای به نظر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



ب- حذف بسته‌ها:

بعد از برقراری ارتباط بین کاربر و سامانه مرکزی نرم‌افزار^۲، تجهیزات شبکه اپراتور با در صد بالایی بسته‌های ارتباطی را حذف می‌کند و این کار باعث اختلال شدید می‌شود و پیام‌رسان مکرراً جهت برقراری مجدد ارتباط، اقدام می‌نماید و کاربر پس از 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 ارائه می‌شود (نمودارهای ۵- ۸).

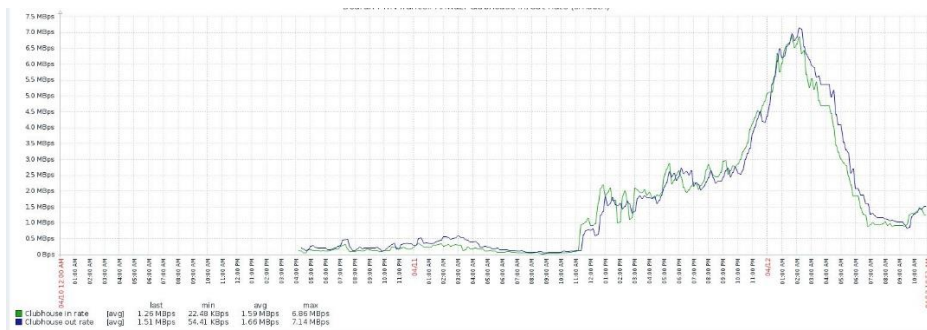


نمودار ۵: نمودار ترافیک نرم‌افزار کلاب هوس در استان‌های غربی کشور (ایرانسل)

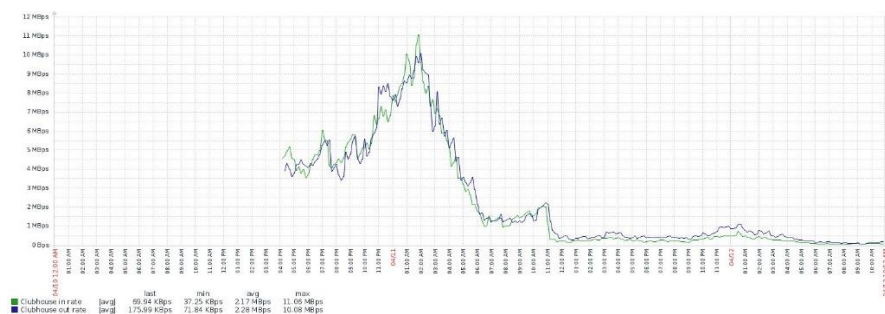


نمودار ۶: نمودار ترافیک نرم‌افزار کلاب هوس در شمال کشور (ایرانسل)

² three way hand shaking & client hello



نمودار ۷: نمودار ترافیک نرم افزار کلاب هاوس در استان های شرقی کشور (ایرانسل)



نمودار ۸: نمودار ترافیک نرم افزار کلاب هاوس در استان های جنوبی کشور (ایرانسل)

شرکت مخابرات ایران

تغییر در نحوه مسیریابی شرکت مخابرات ایران

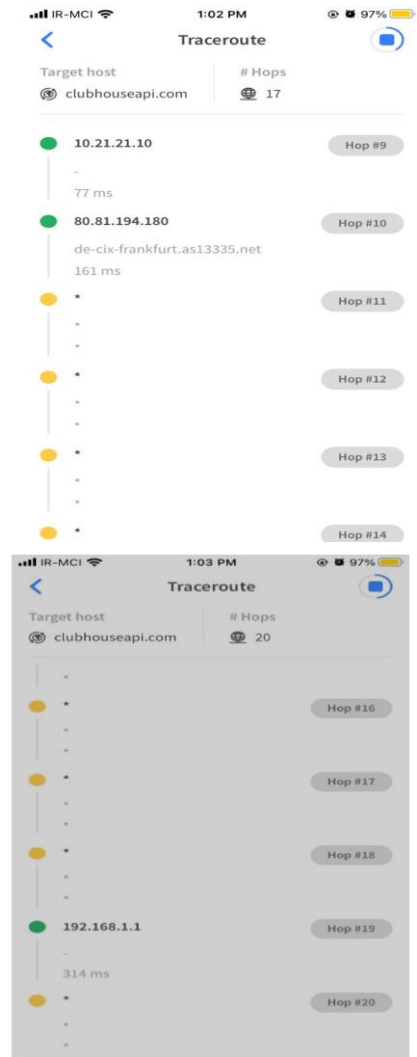
در این اپراتور مسدودسازی به صورت آدرس آی پی نیز انجام شده است بدین صورت که ابتدا IP های دامنه www.clubhouseapi.com استخراج شده است و سپس بر روی روتر آن اپراتور مسدود گردیده است (شکل ۴).

```

ict_adsl_health_modem_ip 5.219.96.3 *****
ict_adsl_health_internet_connection 1 *****
ict_adsl_health_check_modem 1 *****
ict_adsl_qos_destination www.clubhouseapi.com *****
ict_adsl_qos_traceroute 192.168.1.22,192.168.50.1,10.14.
ict_adsl_qos_destination www.clubhouseapi.com *****
ict_adsl_qos_jitter -1.0000 *****
ict_adsl_qos_rtt_avg -1 *****
ict_adsl_qos_lost_percent 100.0 *****
ict_adsl_qos_ir_destination.185.147.178.14 *****
ict_adsl_qos_ir_traceroute 192.168.1.22,10.142.33.6,10.14
ict_adsl_qos_ir_destination 185.147.178.14 *****
ict_adsl_qos_ir_jitter 0.5455 *****
ict_adsl_qos_ir_rtt_avg 18.3 *****
  
```

شکل ۴ نتیجه تغییر در مسیریابی تجهیزات شبکه

این انسداد بگونه ای به نظر می رسد که کاربر احساس می کند برنامه کلاب هاوس دچار اختلال می باشد (شکل ۵).



شکل ۵: عدم امکان دسترسی به آدرس از طریق شبکه شرکت مخابرات ایران