Throttling Twitter: An Emerging Censorship Technique in Russia

Diwen Xue, Reethika Ramesh, ValdikSS*, Leonid Evdokimov*, Andrey Viktorov*, Arham Jain, Eric Wustrow#, Simone Basso†, Roya Ensafi

University of Michigan, *Independent, #University of Colorado Boulder, †OONI
Slowdown of Twitter in Russia

March 10, 2021

Today Roskomnadzor began to nightmare Twitter. I'm definitely shaping abs.twimg.com 92 and pbs.twimg.com 54 ... The first one contains Twitter js bundles, the second one contains media.

Announcement from RKN on the topic: Roskomnadzor - Roskomnadzor took measures to protect Russian citizens from the influence of illegal content 132

03/10/2021 at about 10:00 Roskomnadzor began to slow down Twitter, in particular the abs.twimg.com domains 92, pbs.twimg.com 54, video.twimg.com 3, t.co 1, which are used to download images, videos and service scripts of the service.

The rate limiting was implemented incorrectly: the search for a domain was carried out by a substring, which led to a slowdown in any domains containing t.co (microso ft.com, reddit t.co m). The bug was fixed at about 11:30 am 03/11/2021 Moscow time.

Source: https://ntc.party/t/twitter/907/13 (Google Translation)
Unlike other social networks, Twitter did not delete the illegal materials. In order to protect Russian citizens from the influence of illegal content, centralized response measures have been taken, namely, the slowdown of the service's speed.

"
Internet Censorship

Blocking:

Throttling:

100 Mbps

100 Kbps
Russia’s throttling of Twitter marks the first-ever instance of a country using large-scale, targeted throttling as an emerging censorship technique.

But questions remained unanswered, such as how and where the throttling was implemented, what triggers throttling, how can it be circumvented?
Quantify Throttling Effect: Record and Replay*

Quantify Throttling Effect: Bit-inverted Replay*

Reverse Engineering the Throttler: Throttling Mechanism
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI *alone* is sufficient to trigger throttling.
  - Server certificate is not required.
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI *alone* is sufficient to trigger throttling.
- Throttling is *not* symmetric w.r.t in&outside Russia.
  - Throttling can only be triggered by connections initiated locally.
  - Challenging for researchers to study it from outside using existing remote measurement tools.
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI *alone* is sufficient to trigger throttling.
- Throttling is *not* symmetric w.r.t in&outside Russia.
- In most cases, inspection is limited to the initial packet.
  - Inspection can be extended if the initial packet is TLS/HTTP proxy/SOCKS proxy packet — possibly to target circumvention tools (e.g., GoodbyeDPI).
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI * alone is sufficient to trigger throttling.
- Throttling is *not* symmetric w.r.t in&outside Russia.
- In most cases, inspection is limited to the initial packet.
- Packets are parsed, rather than simply regex-matching domain strings.
  - Masking type or length fields leaves the connection unthrottled.
Domains Targeted

- Only t.co and twitter.com are throttled from the Alexa Top 100K.
Domains Targeted

- Only *t.co* and *twitter.com* are throttled from the Alexa Top 100K.
- Early implementation used loose string matching policy causing collateral damage to non-Twitter domains.

<table>
<thead>
<tr>
<th>Matching Rule</th>
<th>Example affected domains</th>
<th>Date Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>t.co</em></td>
<td>Reddit.com, microsoft.com</td>
<td>March 11, 2021</td>
</tr>
<tr>
<td><em>twitter.com</em></td>
<td>Throttletwitter.com</td>
<td>April 2, 2021</td>
</tr>
</tbody>
</table>
Locating the Throttler: TTL Measurement

SNI = Twitter.com
SNI = I.am.chocolate
## Locating the Throttler: TTL Measurement

<table>
<thead>
<tr>
<th>Vantage point</th>
<th>ISP Name</th>
<th>Throttling Location</th>
<th>Blocking Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OBIT</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Beeline</td>
<td>4-5</td>
<td>5-6</td>
</tr>
<tr>
<td>3</td>
<td>MTS</td>
<td>1-2</td>
<td>5-6</td>
</tr>
<tr>
<td>4</td>
<td>TELE2</td>
<td>2-3</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>Megafon</td>
<td>1-2</td>
<td>4-5</td>
</tr>
<tr>
<td>6</td>
<td>Ufanet</td>
<td>3-4</td>
<td>5-6</td>
</tr>
<tr>
<td>7</td>
<td>Ufanet</td>
<td>4-5</td>
<td>6-7</td>
</tr>
</tbody>
</table>
Longitudinal Tracking
How to circumvent the throttling?

**Client Side**
- Prepending Client Hello with other TLS records.
- Splitting Client Hello into multiple TCP packets.
- Keeping connections inactive for ~10 minutes.
- Inserting random packet with lower TTL.
- Using encrypted proxies.

**Server Side**
- Encrypt SNI!
  E.g., TLS encrypted Client Hello (ECH).
Development

“...the Twitter administration informed about fulfillment of removing content prohibited in Russia”

Throttling was lifted on landlines on May 17.

Sets a dangerous precedent - other social media sites are next in line.

Technology

Russia gives Google 24 hours to delete banned content

Wake-up call to censorship research community

- Effective and economical to implement.
- Challenging to attribute, difficult to measure.
- Current censorship detection platforms are yet not equipped to monitor throttling.
https://censoredplanet.org/throttling

Thank you
Throttling as Practiced

ISPs throttles apps in violation of net neutrality:


Iran throttles all Internet connections before election:

Source: https://www.rferl.org/a/iran-internet-disruptions-election/25028696.html

<table>
<thead>
<tr>
<th>Country</th>
<th>ISP</th>
<th>Throttled Apps</th>
<th>Rate(s)</th>
<th>Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada</td>
<td>Start Comms.</td>
<td>a, n</td>
<td>6 Mbps</td>
<td>126</td>
</tr>
<tr>
<td>Canada</td>
<td>ViaNetTV</td>
<td>n</td>
<td>1 Mbps</td>
<td>45</td>
</tr>
<tr>
<td>UAE</td>
<td>Etisalat</td>
<td>n</td>
<td>0 Mbps</td>
<td>23</td>
</tr>
<tr>
<td>US</td>
<td>Hughes Net. Sys.</td>
<td>n</td>
<td>1 Mbps</td>
<td>81</td>
</tr>
<tr>
<td>US</td>
<td>NextLink</td>
<td>n</td>
<td>4 Mbps</td>
<td>72</td>
</tr>
<tr>
<td>US</td>
<td>ViaSat</td>
<td>n</td>
<td>1 Mbps</td>
<td>112</td>
</tr>
</tbody>
</table>

IRAN

Iran Admits Throttling Internet To 'Preserve Calm' During Election

June 26, 2013 12:59 GMT   By Golnaz Esfandiari

In an unusual move, Iran’s minister for communications and information technology, Mohammad Hassan Nami, has acknowledged that the country restricted the speed of the Internet in the days leading up to the June 14 presidential election.
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI alone is sufficient to trigger throttling.
- Throttling is not symmetric w.r.t in&outside Russia.
- Inspection is symmetric w.r.t downstream and upstream traffic.
  - A Client Hello sent by the TCP server can also trigger throttling.