

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

■ Internet censorship all around the world ■ Russia



Touay 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.co](#)m, 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)

Slowdown of Twitter in Russia

March 10, 2021



МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)

**Роскомнадзор принял меры по защите российских граждан от влияния
противоправного контента**

10 марта 2021 года

В связи с тем, что интернет-сервисом Twitter в период с 2017 года по настоящее время не удаляется контент, склоняющий несовершеннолетних к совершению самоубийств, содержащий детскую порнографию, а также информацию об использовании наркотических средств, Роскомнадзором было направлено свыше 28 тысяч первоначальных и повторных требований об удалении противоправных ссылок и публикаций.

"

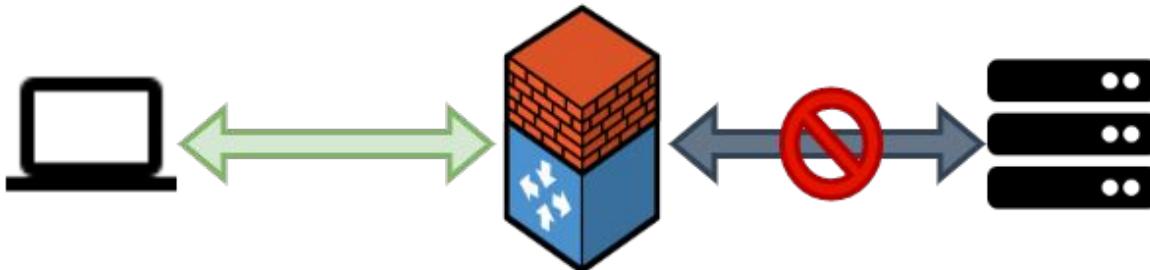
**Unlike other social networks, Twitter did not delete the illegal materials.
In order to protect Russian citizens from the influence of illegal content,
centralized response measures have been taken, namely, the slowdown of the service's
speed.**

"

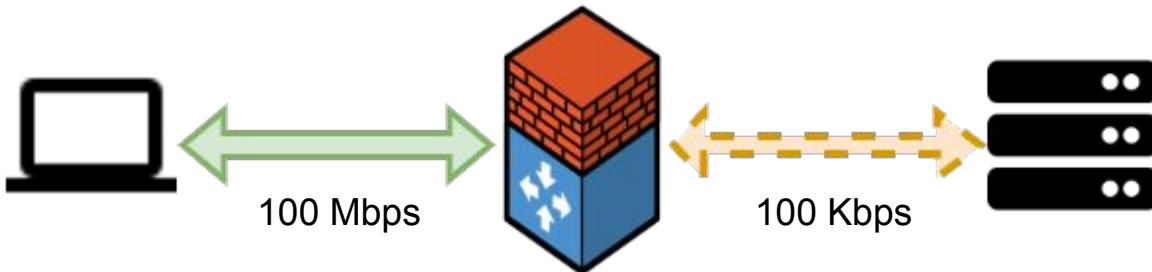


Internet Censorship

Blocking:

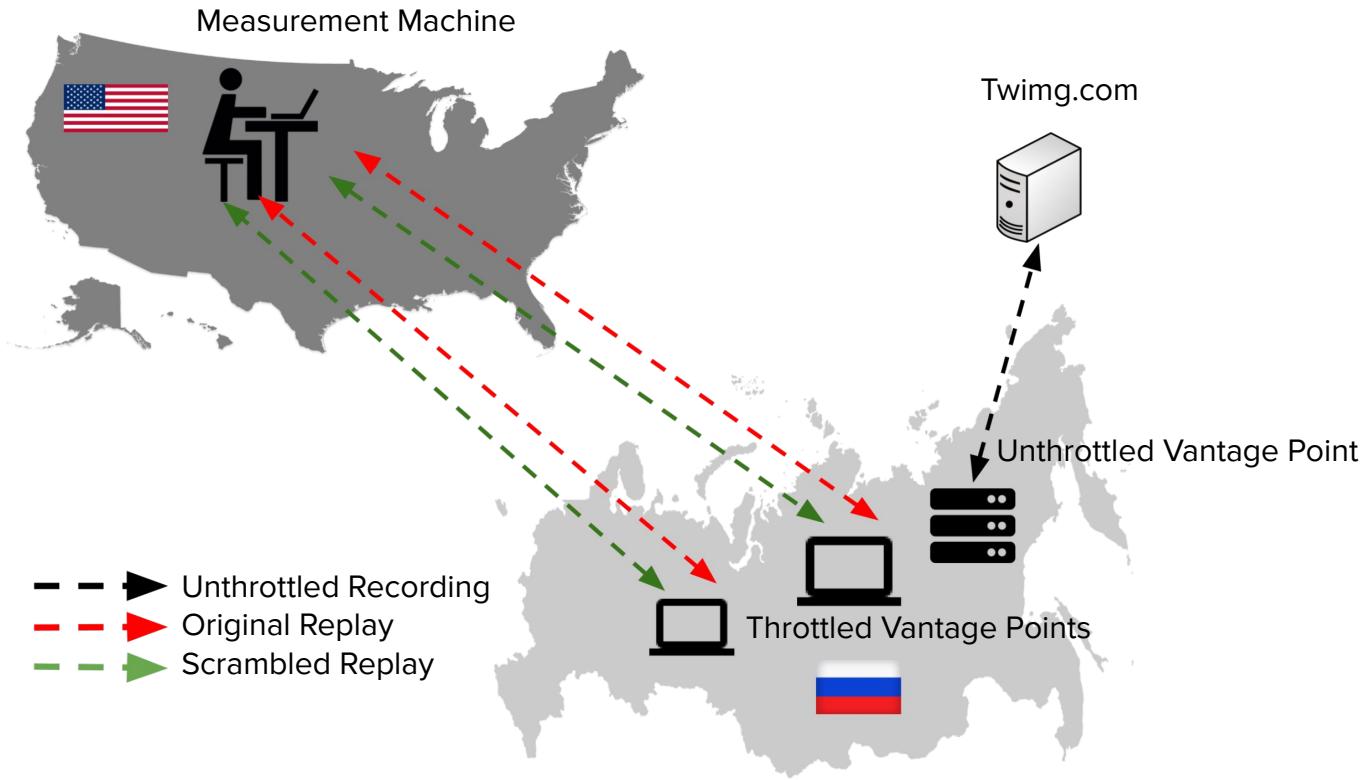


Throttling:



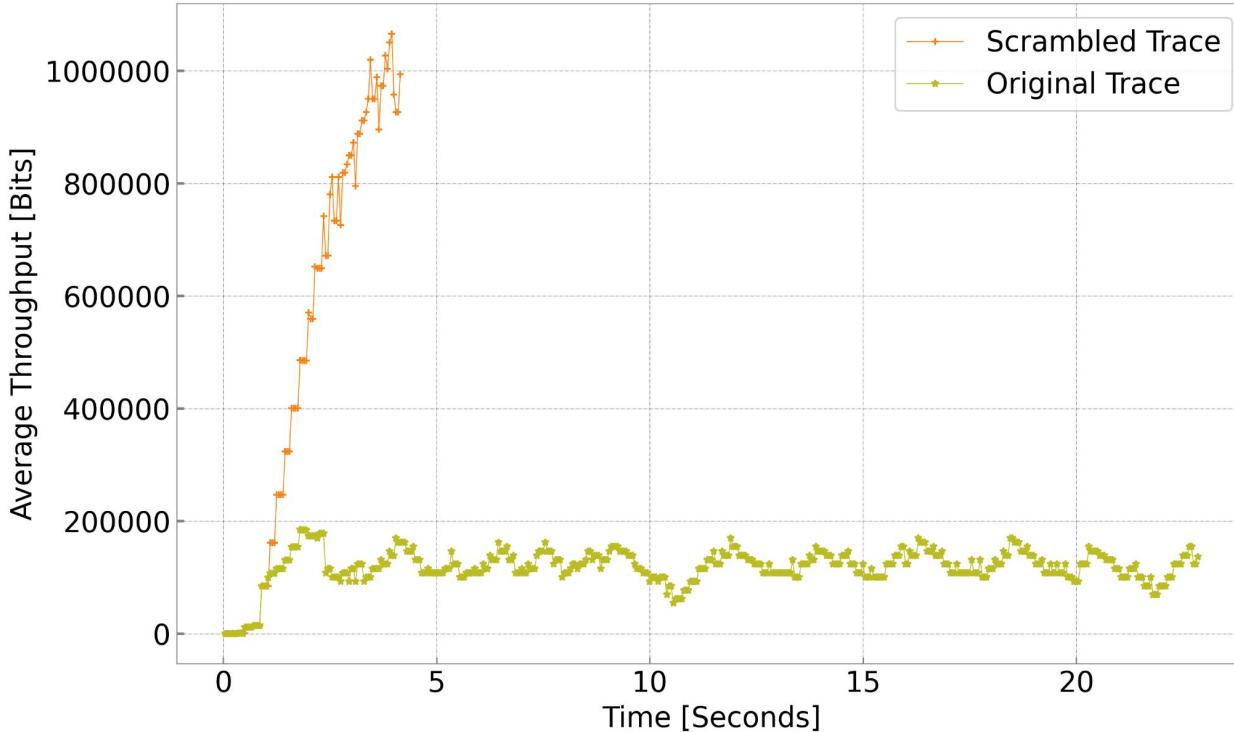
Russia's throttling of Twitter marks the first-ever instance of a country using large-scale, targeted throttling as an emerging censorship technique.

But questions remained unanswered, such as how and where the throttling was implemented, what triggers throttling, how can it be circumvented?



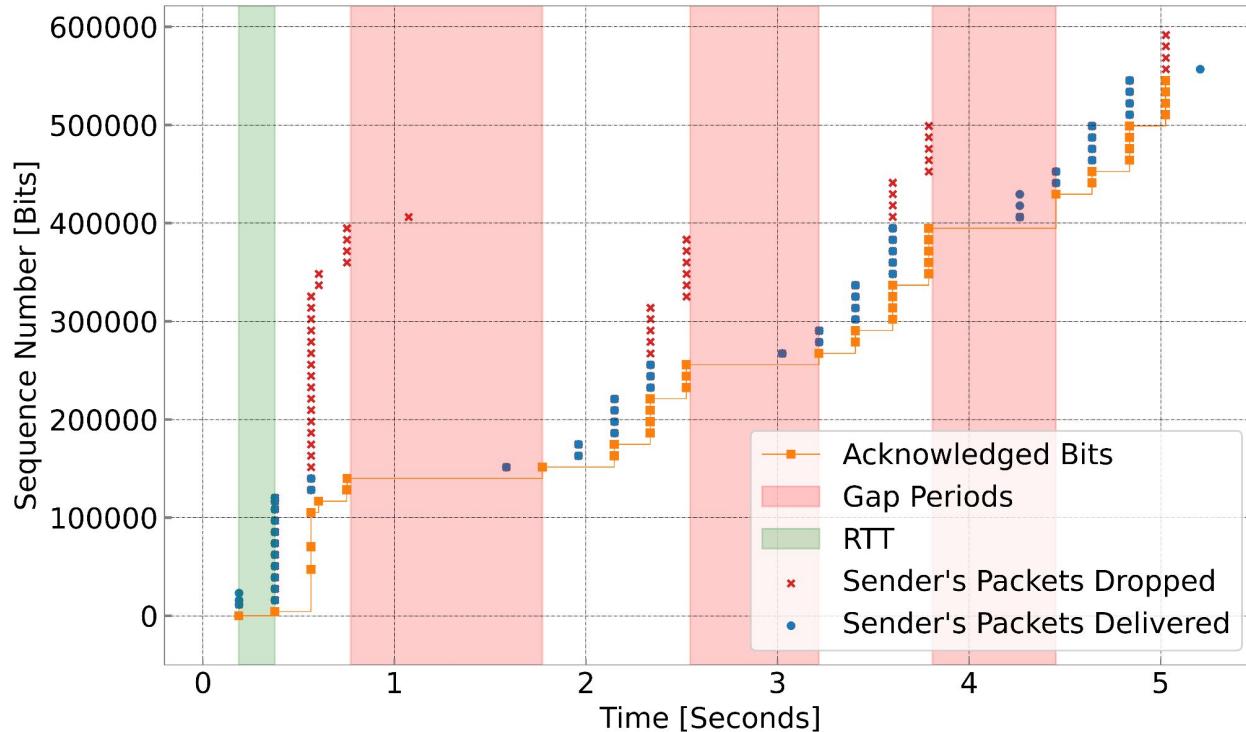
Quantify Throttling Effect: Record and Replay*

*Source: A. Kakhki, A. Razaghpanah, A. Li, H. Koo, R. Golani, D. Choffnes, P. Gill, and A. Mislove. Identifying traffic differentiation in mobile networks. In proceedings of the 2015 Internet Measurement Conference.



Quantify Throttling Effect: Bit-inverted Replay*

*Source: F. Li, A. A. Niaki, D. Choffnes, P. Gill, and A. Mislove.
A large-scale analysis of deployed traffic differentiation
practices. In Proceedings of the ACM Special Interest Group
on Data Communication.



Reverse Engineering the Throttler: Throttling Mechanism

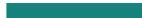
Reverse Engineering the Throttler: Throttling Trigger

- A Client Hello with a sensitive SNI alone is sufficient to trigger throttling.
 - Server certificate is not required.



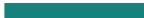
Reverse Engineering the Throttler: Throttling Trigger

- 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.



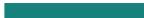
Reverse Engineering the Throttler: Throttling Trigger

- 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.



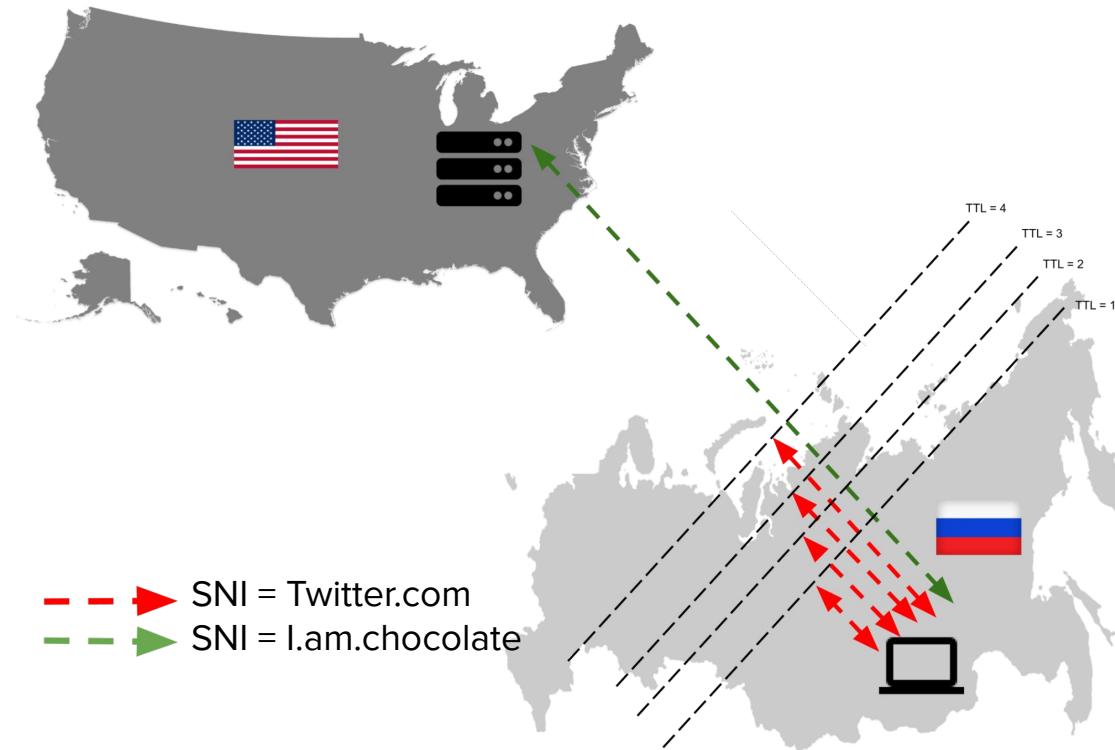
Domains Targeted

- 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.

| Matching Rule | Example affected domains | Date Fixed |
|---------------|---|----------------|
| *t.co* | Reddit. com , microsoft t.com | March 11, 2021 |
| *twitter.com | Throttletwitter.com | April 2, 2021 |



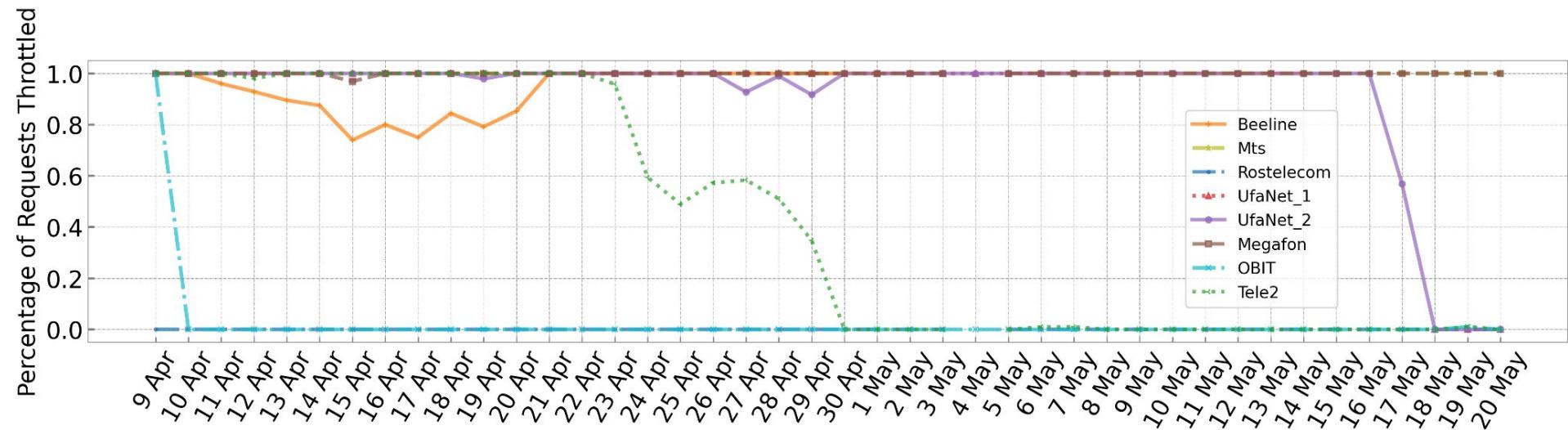
Locating the Throttler: TTL Measurement



Locating the Throttler: TTL Measurement

| Vantage point | ISP Name | Throttling Location | Blocking Location |
|---------------|----------|---------------------|-------------------|
| 1 | OBIT | N/A | N/A |
| 2 | Beeline | 4-5 | 5-6 |
| 3 | MTS | 1-2 | 5-6 |
| 4 | TELE2 | 2-3 | N/A |
| 5 | Megafon | 1-2 | 4-5 |
| 6 | Ufanet | 3-4 | 5-6 |
| 7 | Ufanet | 4-5 | 6-7 |

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).



MINISTRY OF COMMUNICATIONS AND MASS MEDIA OF THE RUSSIAN FEDERATION

FEDERAL SERVICE FOR SUPERVISION OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND MASS COMMUNICATIONS (ROSKOMNADZOR)

Twitter informed Roskomnadzor about the progress of removing prohibited materials

May 14, 2021

At the initiative of Twitter Inc., representatives of the company met with the management of Roskomnadzor on May 13. At the meeting, the Twitter administration informed about the social network's compliance with the requirements for the removal of prohibited content in Russia.

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

Reuters



Source: <https://rkn.gov.ru/news/rsoc/news73620.htm>

<https://www.reuters.com/technology/russia-gives-google-one-day-delete-banned-content-threatens-slowdown-2021-05-24/>

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.

Thank you

<https://censoredplanet.org/throttling>
