Large-scale censorship and surveillance events

Enabled by

Client → Advanced network technology → Server

- Kazakhstan spies on citizens’ HTTPS traffic; browser-makers fight back
- Russia is restricting social media. Here’s what we know
- Sanctions and censorship are making the Internet in Iran less accessible, analysts say
Citizen Lab Identified an "Alternative Lifestyles" blocklist curated by Netsweeper was used by several countries such as UAE to block LGBTQ content.

After advocacy based on Citizen Lab’s findings, Netsweeper claims they have removed the option to block based on this category.

Canadian Internet Filtering Company Says It’s Stopped 'Alternative Lifestyles' Censorship

The UAE was found to be blocking LGBTQ content using a pre-set category in Netsweeper's software. Amid pressure from rights groups, the company says it's disabled that category.

By Jordan Pearson
Jan 21 2019, 12:25pm  Share  Tweet  Snap
What and When?

- Censorship Measurement Platforms

Censored Planet

OONI

Iodo
Who, Where and How?

- Specific censorship systems
  - Great Firewall of China
  - Iran’s national firewall
  - Russia’s TSPU system
Challenges and Gaps

1. Opaque nature of censorship
2. Lack of transparency
3. Variety of devices and censorship techniques
4. Reliance on specific behaviors
5. Large manual effort does not scale
Need: **General-purpose, robust methods**

To study censorship devices
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
CenTrace

- Conduct in-country and remote measurements in Azerbaijan (AZ), Belarus (BY), Kazakhstan (KZ), Russia (RU)
- HTTP and TLS traceroutes
Censorship occurs when traffic enters AZ.
Censorship occurs closer to the user.
Most censorship occurs inside KZ

What are these cases?
Censorship occurs in Russian AS, even before entering KZ
CenTrace Observations

- Significant portion of remote measurements are **blocked at the endpoint**, indicate local policies
- Some devices exhibit specialized behavior such as **copying TTL values** from original packet.
- Packet drops in Azerbaijan and Kazakhstan, Resets in Belarus and Russia
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
## Commercial Network Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>AZ</th>
<th>KZ</th>
<th>RU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Cisco</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Kerio Control</td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Palo Alto</td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS Guard</td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mikrotik</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Commercial Network Devices

<table>
<thead>
<tr>
<th>Device</th>
<th>AZ</th>
<th>KZ</th>
<th>RU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>✅</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Kerio Control</td>
<td></td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td>Palo Alto</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoSGuard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mikrotik</td>
<td></td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Kaspersky</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do these devices behave the same way?
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
We built robust, reusable solutions to:

1. Locate censorship devices
   Censorship Traceroute

2. Identify device vendors
   Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   Censorship Fuzzer
CenFuzz TLS: Evasion Success Rates
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute

2. Identify device vendors
   - Banner grabs and Clustering

3. Reverse-engineer censorship triggers
   - Censorship Fuzzer
We built robust, reusable solutions to:

1. Locate censorship devices
   - Censorship Traceroute
2. Identify device vendors
   - Banner grabs and Clustering
3. Reverse-engineer censorship triggers
   - Censorship Fuzzer

Study similarities between devices
Clustering Devices

CenTrace

Banners

CenFuzz

Features

Labels - vendors
Clustering Devices

Number of devices

Cluster Id
Devices within the same country/ISP form tight clusters.
Clusters with devices from different countries have same features, indicating cross-country deployment.
Our code and data are fully open-source

https://github.com/censoredplanet/CenTrace
https://github.com/censoredplanet/CenFuzz
https://github.com/censoredplanet/CenProbe

Censored Planet report - https://censoredplanet.org/censorship-devices

Highlighting policy gaps
Assisting censorship research
What’s Next?

- Integrate CenTrace, CenFuzz into Censored Planet, OONI
- Improve ground truth
- Enforce standardized error messages and blocking mechanisms
- Encourage publication and auditing of blocklists
- Invest in privacy-preserving technologies like Zero Knowledge middleboxes
Key Takeaways

- Location of censorship is important: frequently occurs in upstream ISPs or even in other countries
- Devices can be deployed with different properties: in-path, on-path, packet drops, copy TTL values
- Banners on popular protocols and blockpages are useful for identification
- The censorship triggers and other features are device- or deployment-specific and can be used to fingerprint them
Key Takeaways

• Location of censorship is important – **frequently occurs in upstream ISPs or even in other countries**
• Devices can be deployed with different properties – **in-path, on-path, packet drops, copy TTL values**
• **Banners** on popular protocols are useful for identification
• The censorship triggers and other features are **device- or deployment-specific** and can be used to fingerprint or identify them

Thank you! Questions?

Reach out at monaw@princeton.edu or ramaks@umich.edu

https://censoredplanet.org/censorship-devices