Investigating Large Scale HTTPS Interception in Kazakhstan

Ram Sundara Raman, Leonid Evdokimov*, Eric Wurstrow#, J. Alex Halderman, Roya Ensafi

University of Michigan, *Independent, #University of Colorado Boulder
Dear subscriber!
You have to install a Security Certificate from http://qca.kz/ to access the Internet according to article no. 26 of the Law "On Communications".
We ask you to perform the installation on every subscriber's device connected to the Internet (smartphone, tablet, laptop, etc.) The lack of the Security Certificate being installed on the device will lead to problems while accessing certain Internet resources.
Yours, Tele2.

Source: https://i.imgur.com/WyKjOug.jpg
MITM on all HTTPS traffic in Kazakhstan

Categories:
- Product: NSS
- Component: CA Certificate Root Program

Type: defect
- Priority: P1
- Severity: critical

Status: RESOLVED FIXED

Source: https://bugzilla.mozilla.org/show_bug.cgi?id=1567114

Nation State MITM CA's?

Paul Wouters:
As was in the news before, Kazakhstan has issued a national MITM Certificate Agency. Is there a

Kathleen Wilson:
On 1/6/16 3:07 PM, Paul Wouters wrote: > As was in the news before, Kazakhstan has issued a
Increasing HTTPS adoption – A safer (and more private) Internet

(14-day moving average, source: Firefox Telemetry)
HTTPS presents challenges for mass surveillance and keyword-based censorship.
Advances in technology

- Sophisticated (and more accessible) middleboxes
  - SSL decryption
  - Large number of users
- Investment in Government surveillance technology
## Kazakhstan Internet Freedom

### FREEDOM ON THE NET 2019

**Kazakhstan**

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Obstacles to Access</td>
<td>10 /25</td>
</tr>
<tr>
<td>B. Limits on Content</td>
<td>11 /35</td>
</tr>
<tr>
<td>C. Violations of User Rights</td>
<td>11 /40</td>
</tr>
</tbody>
</table>

**NOT FREE**

**32 /100**

**LAST YEAR’S SCORE & STATUS**

Scores are based on a scale of 0 (least free) to 100 (most free)

Source: https://freedomhouse.org/country/kazakhstan/freedom-net/2019
Kazakhstan root CA - November 2015
Kazakhstan’s National TLS Interception

- **July 17, 2019**: Government started intercepting large fraction of HTTPS traffic within its borders.
- Facebook and Google among domains affected
Detecting the interception
and learning what triggers it
Detecting the interception – 2 VPSes
Detecting the interception – 2 VPSes
Detecting the interception - 2 VPSes - No interception
Detecting the interception - 52 RIPE Atlas
Detecting the interception – 52 RIPE Atlas – 2
RIPE Atlas probe observed interception
Detecting the interception – 52 RIPE Atlas – 2
RIPE Atlas probe observed interception

Issuer: C = KZ, CN = Security Certificate
Detecting the interception - 52 RIPE Atlas - 2
RIPE Atlas probe observed interception
Detecting the interception - Hyperquack\textsuperscript{[1,2]}

Measurement machine at UMich

TLS handshake for facebook.com and google.com

\textsuperscript{[1]} Measuring the Deployment of Network Censorship Filters at Global Scale, NDSS 2020

\textsuperscript{[2]} https://censoredplanet.org/projects/hyperquack
How Hyperquack works
How Hyperquack works

Step 1: SNI=example.com
- Client Hello (..SNI..)
- Server Hello (..Certificate..)
- HTTP GET request
- HTTP reply (e.g., Status Code 301 Moved Permanently)
- Encrypted using trusted certificate

Step 2: SNI=facebook.com
- Client Hello (..SNI..)
- Server Hello (..Certificate..)
- HTTP GET request
- HTTP reply (e.g., Status Code 301 Moved Permanently)
- Encrypted using MITM injected certificate
- Encrypted using trusted certificate
How Hyperquack works

**Step 1: SNI=example.com**
- Client Hello (…SNI…)
- Server Hello (…Certificate…)
- HTTP GET request
- HTTP reply (e.g., Status Code 301 Moved Permanently)
- Encrypted using trusted certificate

**Step 2: SNI=facebook.com**
- Client Hello (…SNI…)
- Server Hello (…Certificate…)
- HTTP GET request
- HTTP reply (e.g., Status Code 301 Moved Permanently)
- Encrypted using MITM injected certificate

**Step 3: detection**
- Compare step 1 and 2
- If HTTP response bodies are NOT the same: output=Disrupted
- If HTTP response bodies are the same but certificates are NOT the same: output=MITM TLS
- If HTTP response bodies and certificates are the same: output=Not blocked
Detecting the interception – Hyperquack – 82 VPs in 21 ASes

Measurement machine at UMich

Hyperquack measurements for ~2000 domains (Alexa Top 1000\textsuperscript{[1]} + Citizen Lab list of sensitive domains\textsuperscript{[2]})

 Servers with EV Certificates

Results from Hyperquack

- 6 of 82 (7.32%) vantage points observed the interception
- All 6 vantage points in AS 9198 (Kazakhtelecom), located in Nur-Sultan
- 27 domains, mainly social media and communications, affected
- Interception can be triggered bidirectionally
How the interception works

- Client Hello (...Cipher supported, sessionid, random data, SNI, ...)
- Server Hello (...selected Cipher, ..., Certificate, ...)
- Client certificate
- Key exchange
- HTTP GET request
- HTTP reply

Encrypted using MITM injected certificate

In the MITM scenario:
- Client Hello (...Cipher supported, sessionid, random data, SNI, ...)
- Server Hello (...selected Cipher, ..., Certificate, ...)
- Client certificate
- Key exchange
- HTTP GET request
- HTTP reply (e.g., Facebook materials)

Encrypted using trusted certificate

HTTPS server...
Conditions for triggering interception

- Traffic must pass through a particular part of AS 9198 (Kazakhtelecom)
- TLS SNI extension should contain affected domains
- Server must present a valid browser-trusted TLS certificate, but not necessarily a certificate for the domain
In-depth measurements

How and where does the interception occur?
Measurements to 6,736 TLS hosts in 85 ASes
Measurements to 6,736 TLS hosts in 85 ASes

1. Test for interception to google.com and facebook.com
2. On affected servers, test Alexa Top 10,000 domains
3. Keep measurements running
TTL-limited measurements
Results

from our in-depth measurements
Extent of the Interception

- (From University of Michigan) **459 of 6,736 (7%)** TLS hosts observed injected certificate
- (From Kazakhstan VPS) **1,598 of 6,736 (24%)** TLS hosts observed injected certificate
- Paths to all TLS hosts observing interception passed through AS 9198 (Kazakhtelecom)
<table>
<thead>
<tr>
<th>AS</th>
<th>Name</th>
<th># TLS hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>9198</td>
<td>JSC Kazakhtelecom</td>
<td>385</td>
</tr>
<tr>
<td>29555</td>
<td>Mobile Telecom-Service LLP</td>
<td>32</td>
</tr>
<tr>
<td>48502</td>
<td>ForteBank JSC</td>
<td>23</td>
</tr>
<tr>
<td>43601</td>
<td>JSC BankCenterCredit</td>
<td>9</td>
</tr>
<tr>
<td>50482</td>
<td>JSC Kazakhtelecom</td>
<td>7</td>
</tr>
<tr>
<td>60708</td>
<td>KazNIC Organization</td>
<td>2</td>
</tr>
<tr>
<td>43934</td>
<td>...Interbank Settlement Centre...</td>
<td>1</td>
</tr>
</tbody>
</table>

**ASes of hosts exhibiting interception**
Location of Interception

- Interception occurred only three or four network hops before host

- 95% of the time:
  - Hop before injection - 92.47.151.210 or 92.47.150.19
  - Hop after injection - 95.56.243.92 or 95.59.170.5

- All IPs belong to AS 9198 (Kazakhtelecom)
Custom certificate

- Same Subject and Subject Alternative Name (SAN) as the original host’s certificate
- The Public Key replaced with a host-specific RSA-2048 key (until July 19, 1024 bit), with exponent 3
- The validity period (Not Before/Not After) is the same as the original certificate’s but shifted exactly 6 hours in the past - This changed to 24 hours validity on July 30
Censor’s TLS fingerprint

- Sent RIPE Atlas measurement to our server with SNI facebook.com
- Fingerprint virtually unseen in normal Internet traffic, can be used to fingerprint and identify the MitM

<table>
<thead>
<tr>
<th>f09427b5aaf9304b</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Seen</strong></td>
</tr>
<tr>
<td>(past week)</td>
</tr>
<tr>
<td><strong>Rank</strong></td>
</tr>
<tr>
<td>(past week)</td>
</tr>
<tr>
<td><strong>TLS Version</strong></td>
</tr>
<tr>
<td><strong>Handshake Version</strong></td>
</tr>
</tbody>
</table>

Source: https://tlsfingerprint.io/id/f09427b5aaf9304b
# Domains Targeted - 37

<table>
<thead>
<tr>
<th>Company</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>allo.google.com, android.com, dns.google.com, docs.google.com,</td>
</tr>
<tr>
<td></td>
<td>encrypted.google.com, goo.gl, google.com, groups.google.com,</td>
</tr>
<tr>
<td></td>
<td>hangouts.google.com, mail.google.com, messages.android.com, news.google.com,</td>
</tr>
<tr>
<td></td>
<td>picasa.google.com, plus.google.com, sites.google.com, translate.google.com,</td>
</tr>
<tr>
<td>Facebook</td>
<td>cdninstagram.com, facebook.com, instagram.com, messenger.com,</td>
</tr>
<tr>
<td>Mail.Ru</td>
<td>mail.ru, ok.ru, tamtam.chat, vk.com, vk.me, vkuseraudio.net, vkuservideo.net</td>
</tr>
<tr>
<td>Others</td>
<td>rukoeb.com, sosalkino.tv, twitter.com</td>
</tr>
</tbody>
</table>
“Security Certificate”

But this list of domains suggests that the actual intention is instead to surveil users on social networking and communication sites.
Longitudinal tracking
Pilot testing completed...for now

“...the National Security Committee has successfully completed testing the application of the security certificate.”

“The application of the security certificate in the future will be carried out in the event of a threat to national security....

What happened to collected data??
What does this mean for users in Kazakhstan?

Installed the custom cert?
- Complete visibility
- User credentials, sensitive information
- Ability to modify traffic and selectively block

Haven’t installed the custom cert?
- Security warnings for all website access
- Access blocked if HSTS is enabled
Browsers Take a Stand Against Interception

The use of ‘Qaznet Trust Network’ root CA certificate in Chrome, Firefox, and Safari is now prevented.
Implications

- Limitations of HTTPS
  - Previous state-sponsored interception attacks required compromising a CA
- Users - Trust the certificate or be blocked
- Dangerous precedent for other countries
What to do in the future?

- Quicker response from browsers
- Non-intrusive visual indicators when custom certificates are used
- Further research into MitM defenses
- Rapid measurements to detect and study attacks
Thank you

censoredplanet.org/kazakhstan