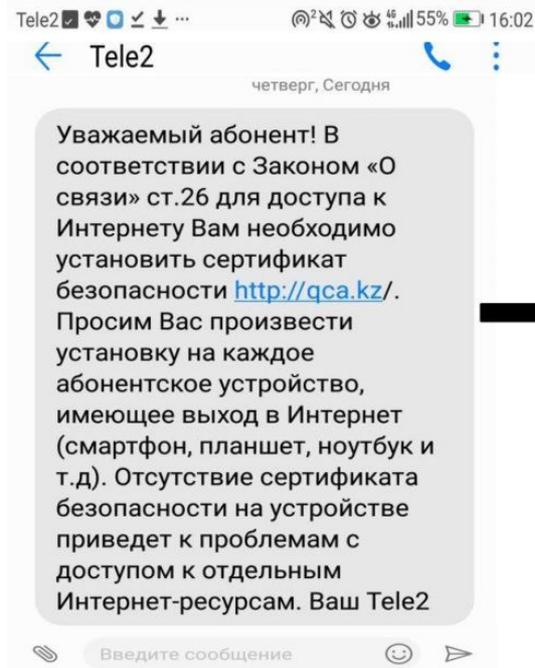


Investigating Large Scale HTTPS Interception in Kazakhstan

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/WyKj0ug.jpg>

Kazakhstan, July 17, 2019

The screenshot shows the Bugzilla interface for bug 1567114. The title is "MITM on all HTTPS traffic in Kazakhstan". The bug is marked as "Closed" and was opened and closed one year ago. The categories section shows the product is "NSS", the component is "CA Certificate Root Program", the type is "defect", the priority is "P1", and the severity is "critical". The tracking section shows the status as "RESOLVED FIXED".

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

The screenshot shows a Google Groups conversation in the "mozilla.dev.security.policy" group. The conversation title is "Nation State MITM CA's ?" with 26298 views. The first message is from Paul Wouters, asking if there is a national MITM Certificate Agency in Kazakhstan. The second message is from Kathleen Wilson, quoting Paul Wouters' question.

Conversations Search conversations within mozilla.dev.secu...
New conversation
My groups
Recent groups
All groups
Favorite groups
Starred conversations
mozilla.dev.security.policy

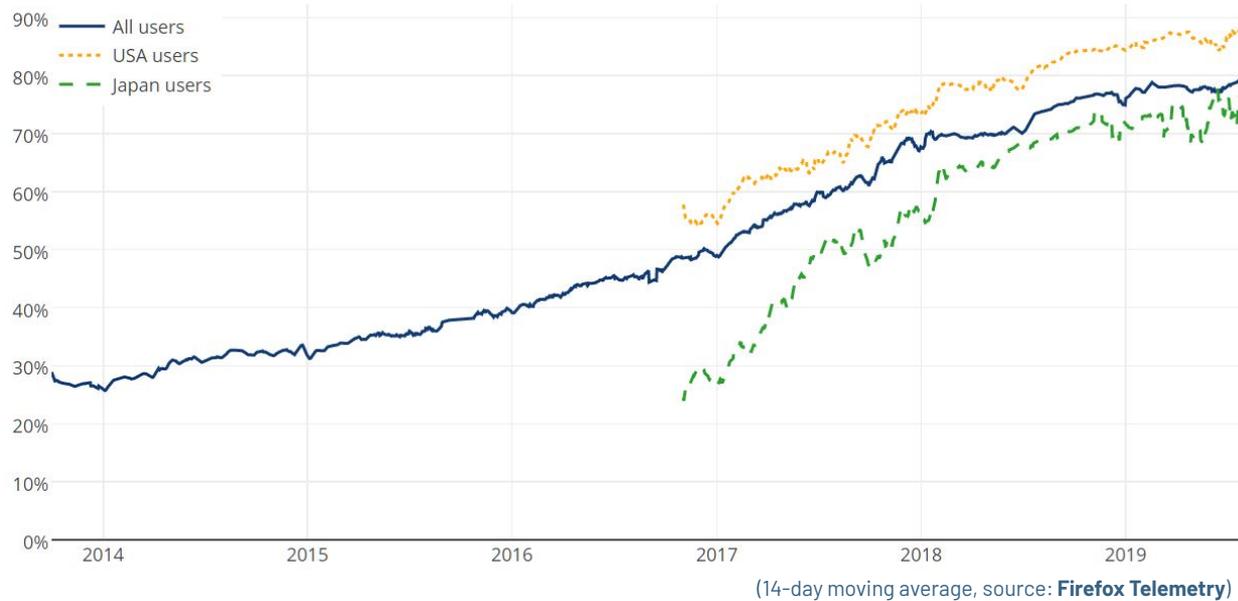
Nation State MITM CA's ? 26298 views

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

Source: <https://groups.google.com/g/mozilla.dev.security.policy/c/wnuKAhAc03E/m/cpsvHgcuDwAJ>

Increasing HTTPS adoption - A safer (and more private) Internet



DigiNotar: Iranians - The Real Target

Posted on: [September 5, 2011](#) at 4:57 am Posted in: [Bad Sites](#), [Targeted Attacks](#)

Author: [Feike Hacquebord](#) (Senior Threat Researcher)



In this blog post, we present concrete evidence that the recent compromise of Dutch certification authority *DigiNotar* was **used to spy on Iranian Internet users** on a large scale.

We found that Internet users in more than 40 different networks of ISPs and universities in Iran were met with rogue SSL certificates issued by *DigiNotar*. Even worse, we found evidence that some Iranians who used software designed to circumvent traffic censorship and snooping were not protected against the massive man-in-the-middle attack.



[About](#) [Issues](#) [Our Work](#) [Take Action](#)

A Syrian Man-In-The-Middle Attack against Facebook

TECHNICAL ANALYSIS BY PETER ECKERSLEY | MAY 5, 2011

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

NOT FREE

32
/100

A. <u>Obstacles to Access</u>	10 /25
B. <u>Limits on Content</u>	11 /35
C. <u>Violations of User Rights</u>	11 /40

LAST YEAR'S SCORE & STATUS

38 /100 ● Not Free

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

Source: <https://freedomhouse.org/country/kazakhstan/freedom-net/2019>

Kazakhstan Internet Freedom

The screenshot shows the Bugzilla interface for a specific bug report. At the top left is the Bugzilla logo and a search bar. Navigation links include 'Browse', 'Advanced Search', 'New Account', 'Log In', and 'Forgot Password'. The bug report itself is titled 'Add Root Certification Authority of the Republic of Kazakhstan (root.gov.kz)' and is marked as 'Closed'. It was opened 5 years ago and closed 4 years ago. The categories section shows the product as 'NSS' and the component as 'CA Certificate Root Program'. The type is 'task', with a priority of 'Not set' and a severity of 'normal'. There are buttons for 'Copy Summary' and 'View'.

m Bugzilla Search Bugs Browse Advanced Search >> New Account Log In Forgot Password

Closed Bug 1232689 Opened 5 years ago Closed 4 years ago

Add Root Certification Authority of the Republic of Kazakhstan (root.gov.kz)

Categories

Product: NSS Component: CA Certificate Root Program Type: task Priority: Not set Severity: normal

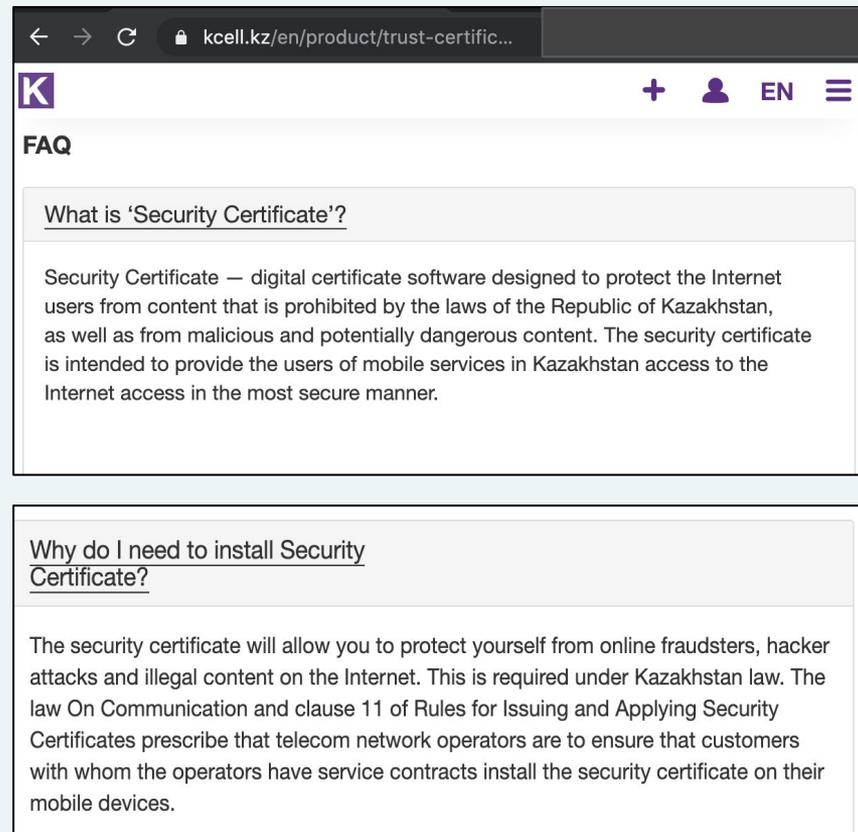
Copy Summary View

Source: https://bugzilla.mozilla.org/show_bug.cgi?id=1232689

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



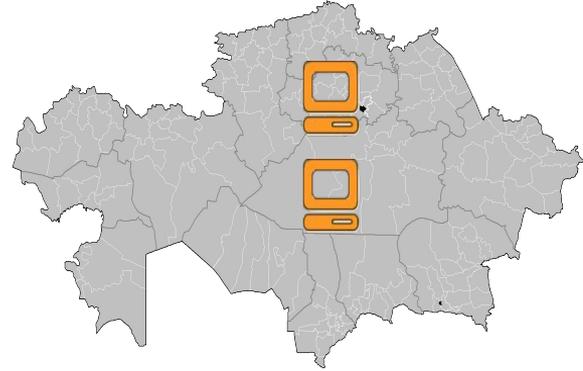
The screenshot shows a mobile browser interface with the URL `kcell.kz/en/product/trust-certific...` in the address bar. The page features a purple 'K' logo and navigation icons. The main content is under an 'FAQ' heading and includes two sections:

What is 'Security Certificate'?
Security Certificate — digital certificate software designed to protect the Internet users from content that is prohibited by the laws of the Republic of Kazakhstan, as well as from malicious and potentially dangerous content. The security certificate is intended to provide the users of mobile services in Kazakhstan access to the Internet access in the most secure manner.

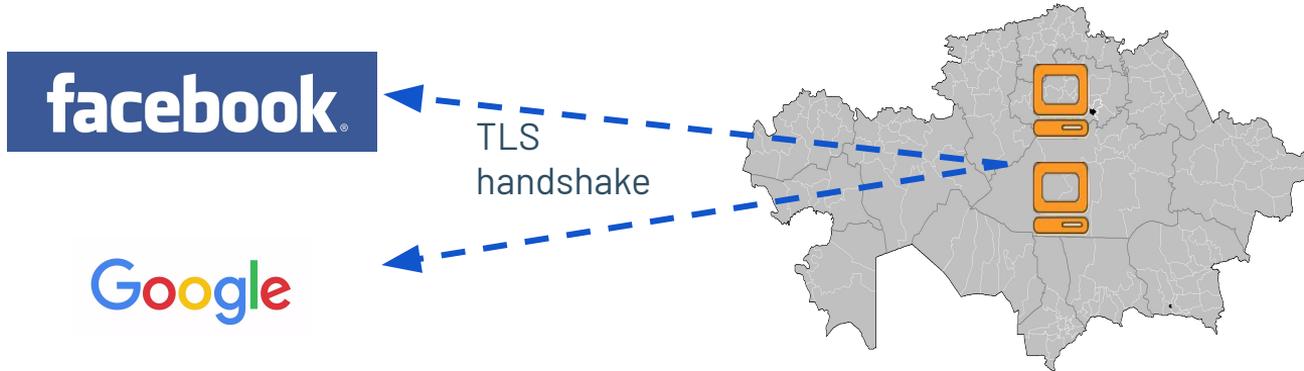
Why do I need to install Security Certificate?
The security certificate will allow you to protect yourself from online fraudsters, hacker attacks and illegal content on the Internet. This is required under Kazakhstan law. The law On Communication and clause 11 of Rules for Issuing and Applying Security Certificates prescribe that telecom network operators are to ensure that customers with whom the operators have service contracts install the security certificate on their mobile devices.

Detecting the interception

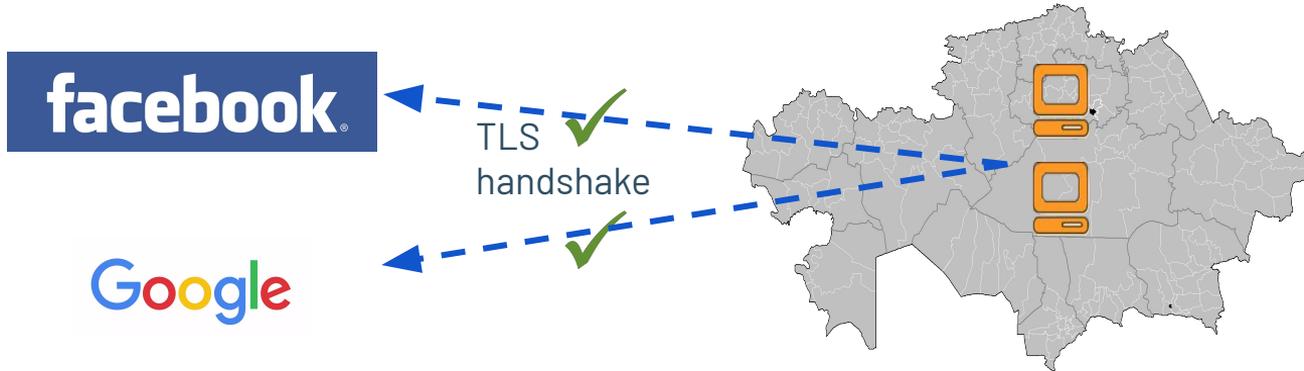
and learning what triggers it



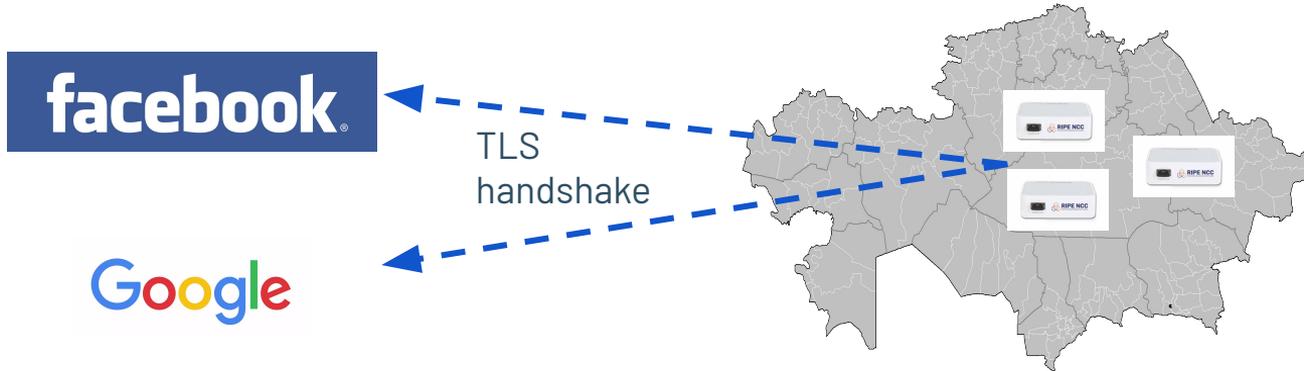
Detecting the interception - 2 VPSes



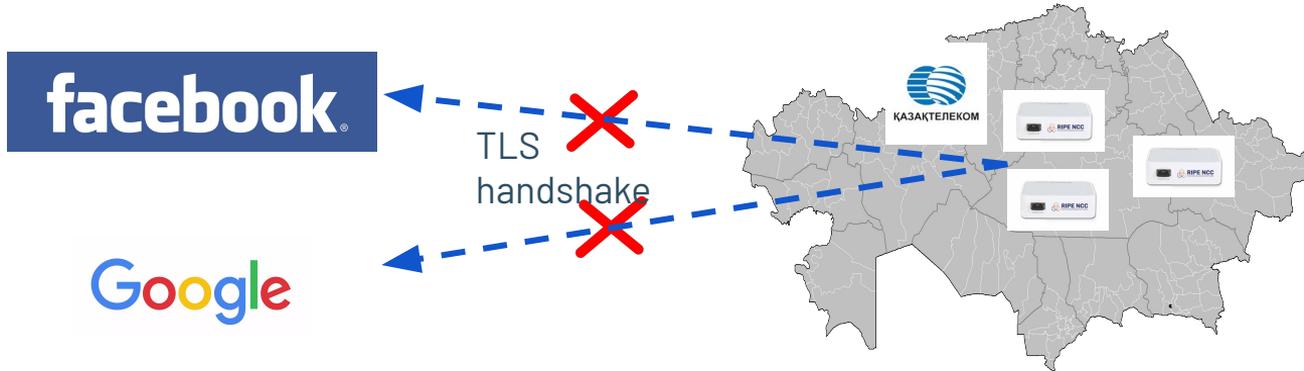
Detecting the interception - 2 VPSes



Detecting the interception - 2 VPSes - No interception

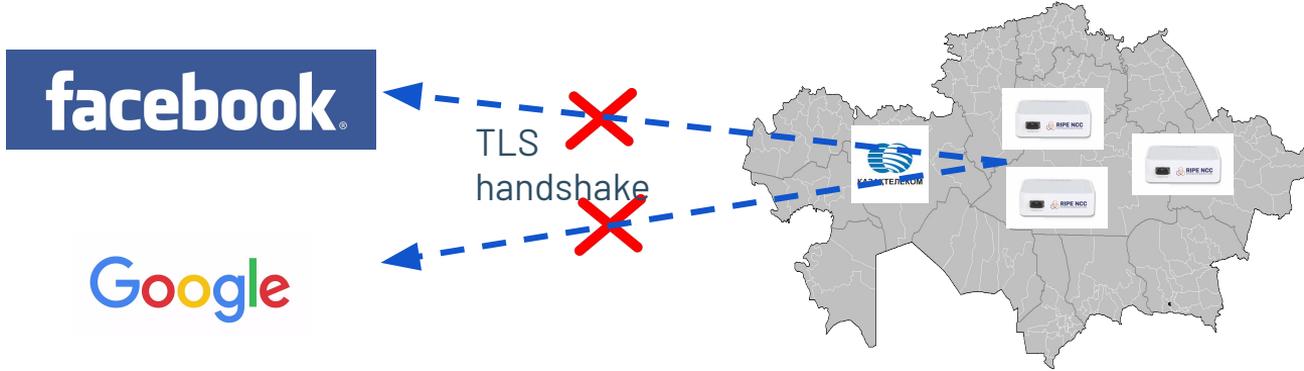


Detecting the interception - 52 RIPE Atlas



Detecting the interception - 52 RIPE Atlas - 2 RIPE Atlas probe observed interception

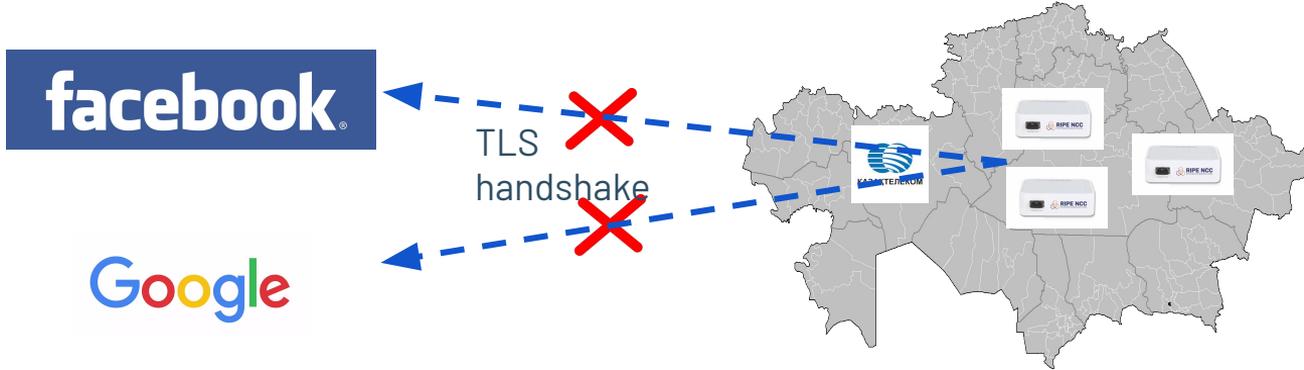
Issuer: C = KZ, CN = Security Certificate



Detecting the interception - 52 RIPE Atlas - 2 RIPE Atlas probe observed interception

Issuer: C = KZ, CN = Qaznet Trust Network

Issuer: C = KZ, CN = Security Certificate



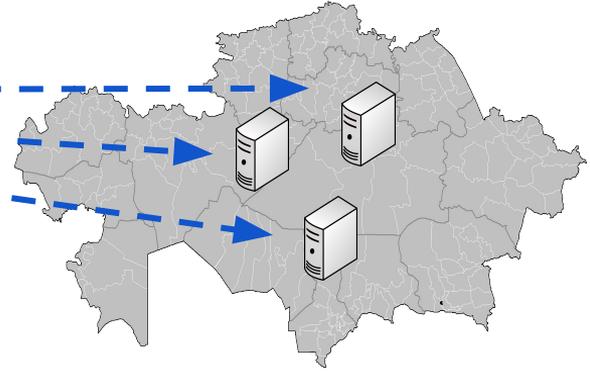
Detecting the interception - 52 RIPE Atlas - 2 RIPE Atlas probe observed interception

Detecting the interception - Hyperquack^[1,2]



Measurement
machine at UMich

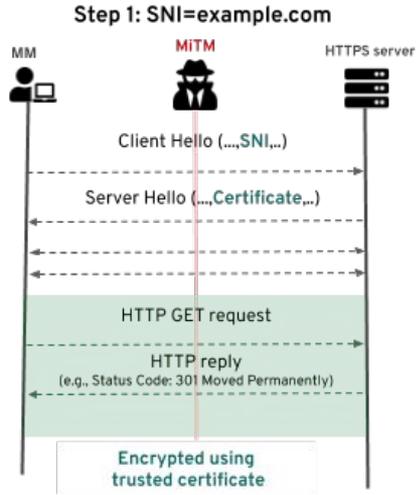
TLS handshake for
facebook.com and
google.com



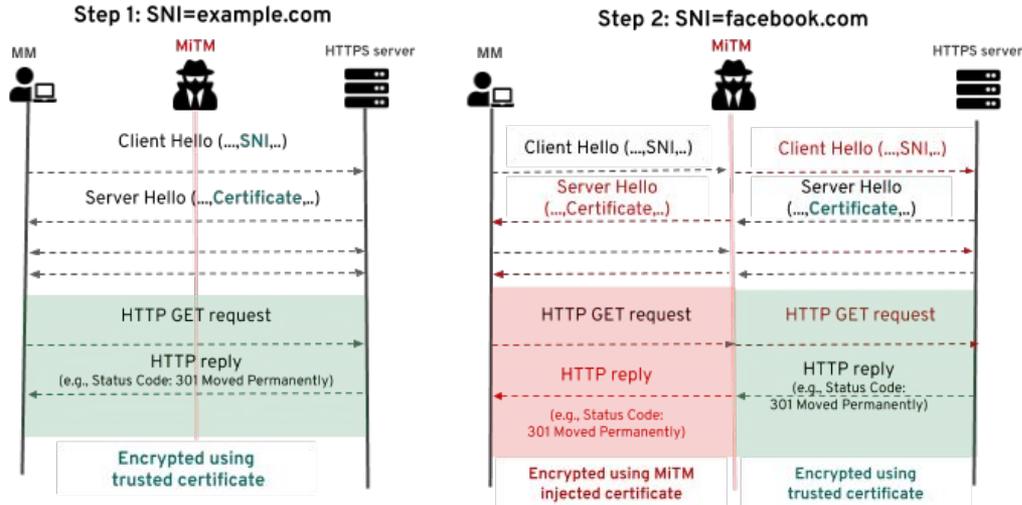
[1] Measuring the Deployment of Network Censorship Filters at Global Scale, NDSS 2020

[2] <https://censoredplanet.org/projects/hyperquack>

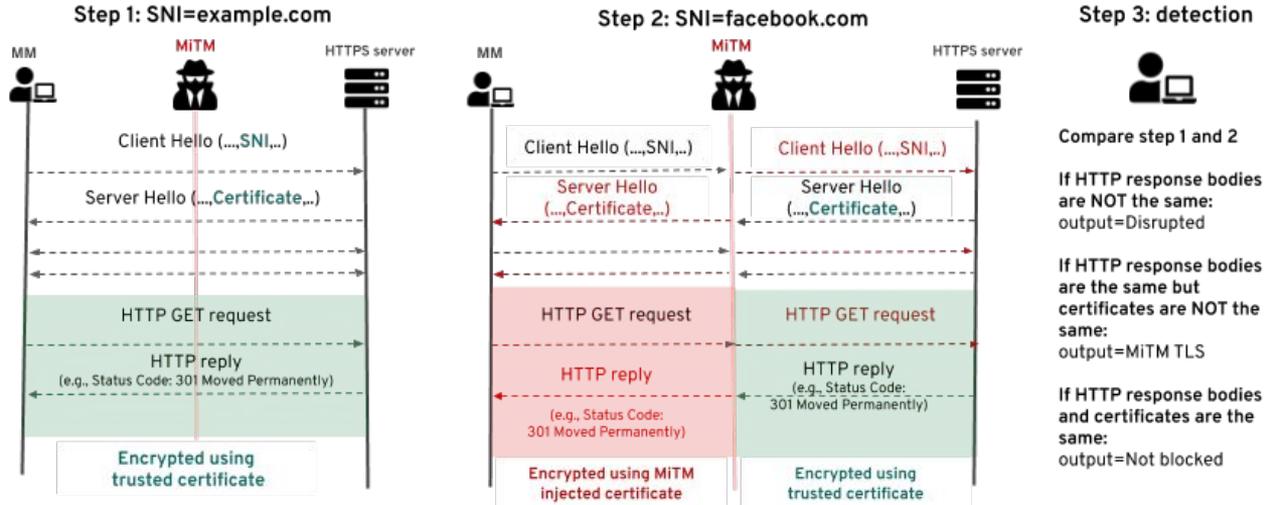
How Hyperquack works



How Hyperquack works



How Hyperquack works





Measurement machine at UMich



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

	Servers with EV Certificates
---	------------------------------

Detecting the interception - Hyperquack - 82 VPs in 21 ASes

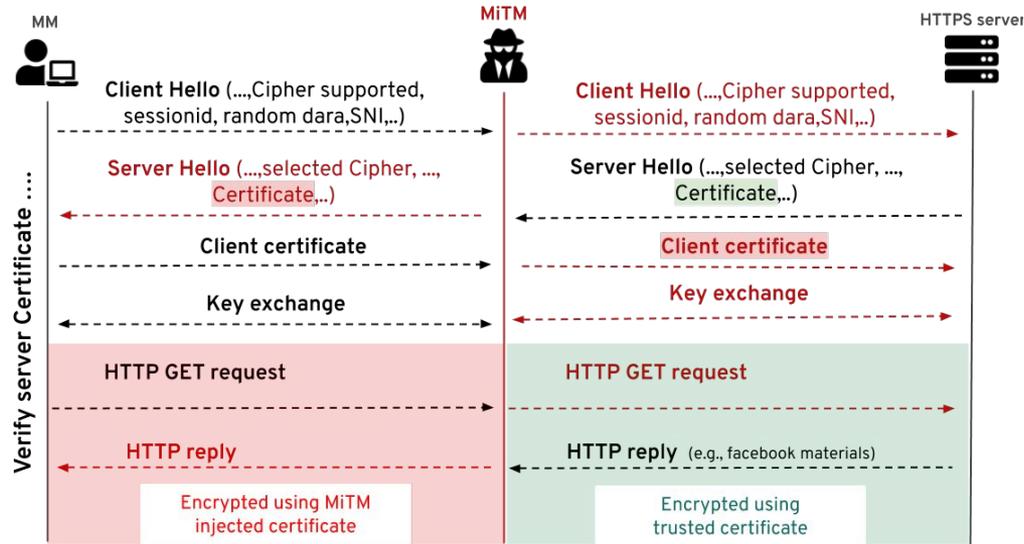
[1] <http://s3.amazonaws.com/alexa-static/top-1m.csv.zip>

[2] <https://github.com/citizenlab/test-lists>

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

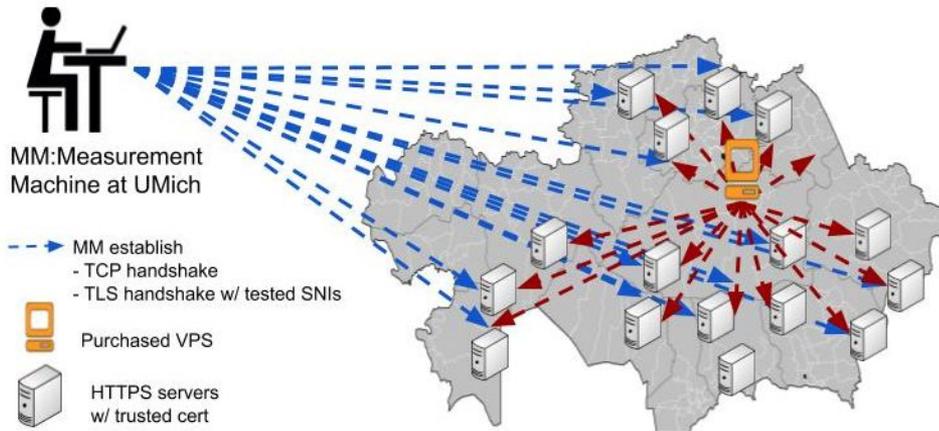


Conditions for triggering interception

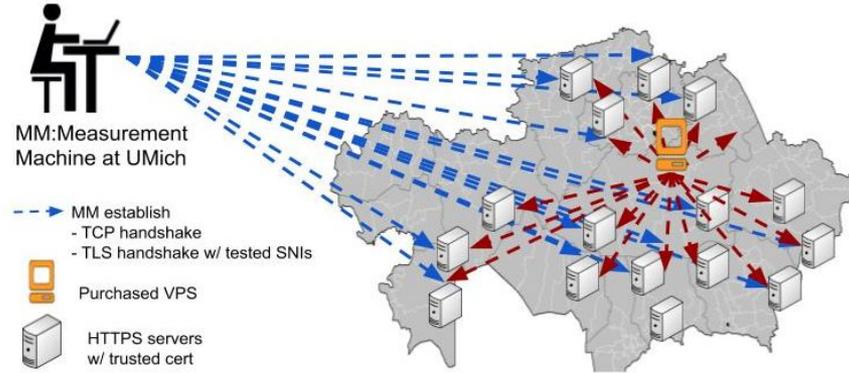
- Traffic must pass through a particular part of AS 9198 (Kazakhtelecom)
- TLS SNI extension should contain affected domains
- Server must present a valid browser-trusted TLS certificate, but not necessarily a certificate for the domain

In-depth measurements

How and where does the
interception occur?

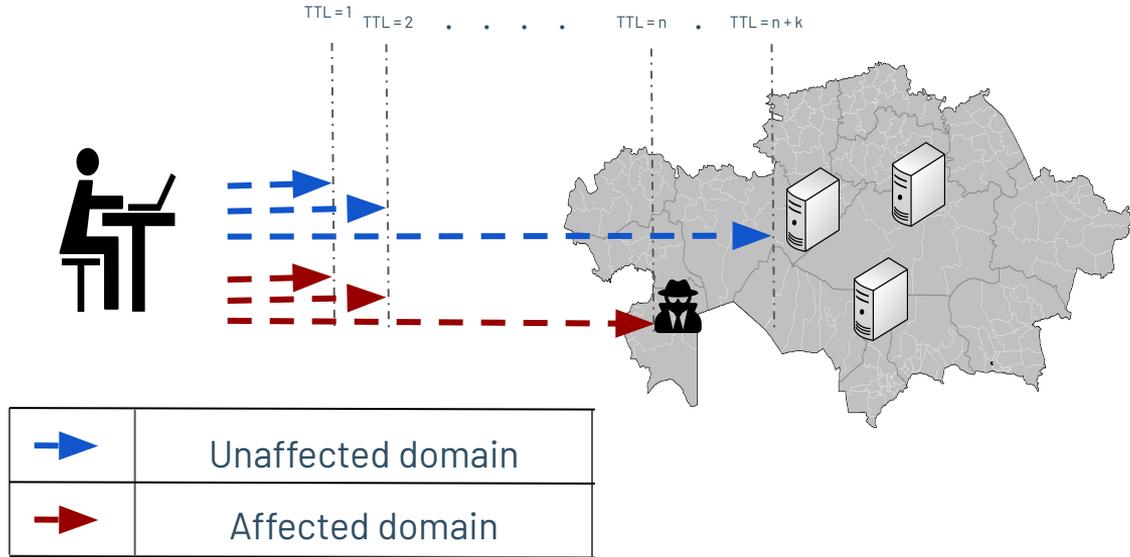


Measurements to 6,736 TLS hosts in 85 ASes



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

Measurements to 6,736 TLS hosts in 85 ASes



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)

AS	Name	# TLS hosts
9198	JSC Kazakhtelecom	385
29555	Mobile Telecom-Service LLP	32
48502	ForteBank JSC	23
43601	JSC BankCenterCredit	9
50482	JSC Kazakhtelecom	7
60708	KazNIC Organization	2
43934	...Interbank Settlement Centre...	1

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)**

```
! 1 185.120.76.1
! 2 88.204.195.89
! 3 212.154.195.97
! 4 92.47.151.210
! 5 95.56.243.92
! 6 178.89.110.198
! 7 178.89.110.206
! 8
```

Certificate injection occurred between hops 4 and 5.

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

f09427b5aaf9304b

Seen	(all time)	< 100 times (0.00%)
	(past week)	< 100 times (0.00%)

Rank	(all time)	41383 / 574811
	(past week)	-1 / 19001

TLS Version	TLS 1.0
--------------------	---------

Handshake Version	TLS 1.2
--------------------------	---------

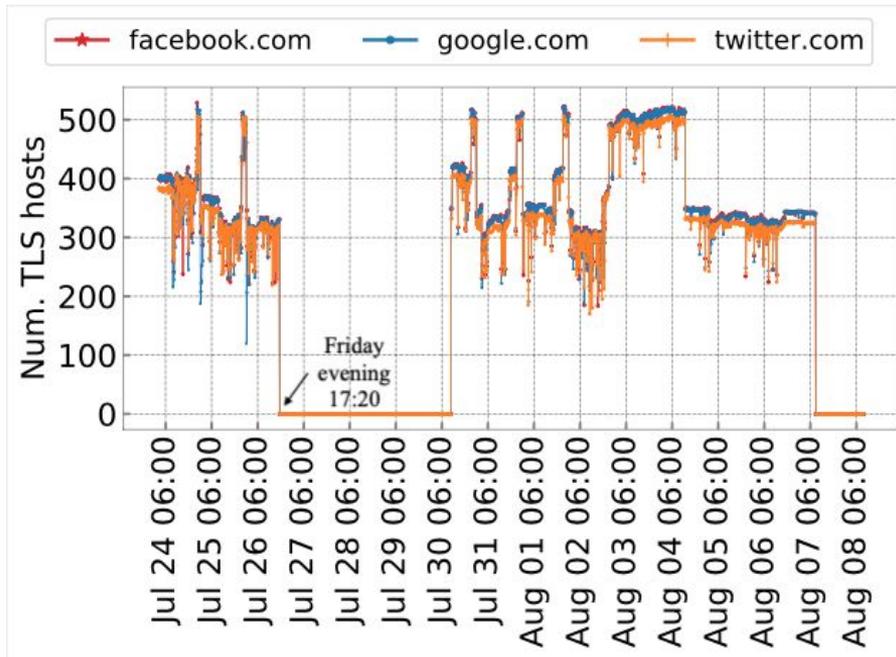
Source: <https://tlsfingerprint.io/id/f09427b5aaf9304b>

Domains Targeted - 37

Company	Domains
Google	allo.google.com, android.com, dns.google.com, docs.google.com, encrypted.google.com, goo.gl, google.com, groups.google.com, hangouts.google.com, mail.google.com, messages.android.com, news.google.com, picasa.google.com, plus.google.com, sites.google.com, translate.google.com, video.google.com, www.google.com, www.youtube.com, youtube.com
Facebook	cdninstagram.com, facebook.com, instagram.com, messenger.com, www.facebook.com, www.instagram.com, www.messenger.com
Mail.Ru	mail.ru, ok.ru, tamtam.chat, vk.com, vk.me, vkuseraudio.net, vkuservideo.net
Others	rukob.com, sosalkino.tv, twitter.com

“Security Certificate”

But this list of domains suggests that the actual intention is
instead to surveil users on social networking and
communication sites



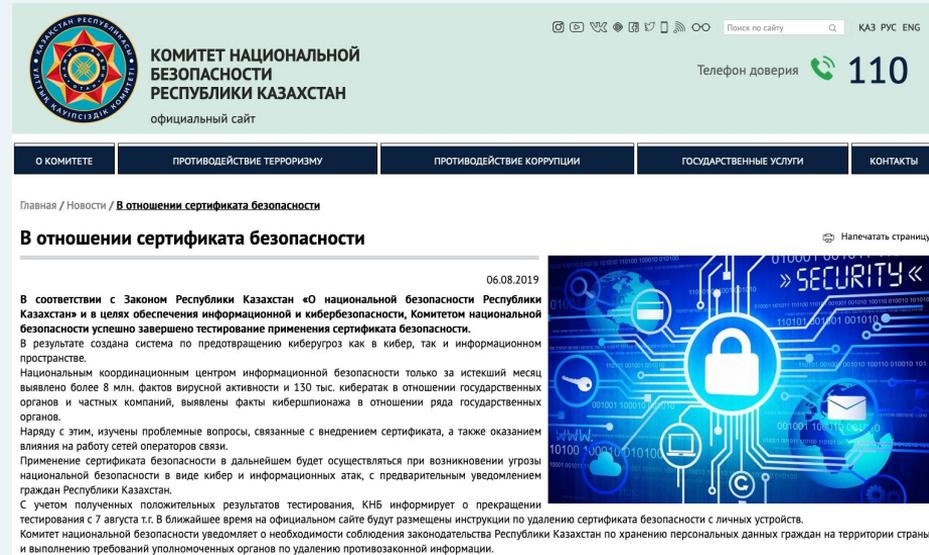
Longitudinal tracking

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??



КОМИТЕТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН
официальный сайт

Поиск по сайту KAZ РУС ENG

Телефон доверия 110

О КОМИТЕТЕ ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ ГОСУДАРСТВЕННЫЕ УСЛУГИ КОНТАКТЫ

Главная / Новости / **В отношении сертификата безопасности**

В отношении сертификата безопасности

06.08.2019

В соответствии с Законом Республики Казахстан «О национальной безопасности и кибербезопасности, Комитетом национальной безопасности успешно завершено тестирование применения сертификата безопасности. В результате создана система по предотвращению киберуязвимостей как в кибер, так и информационном пространстве.

Национальным координационным центром информационной безопасности только за истекший месяц выявлено более 8 млн. фактов вирусной активности и 130 тыс. кибератак в отношении государственных органов и частных компаний, выявлены факты кибершпионажа в отношении ряда государственных органов.

Наряду с этим, изучены проблемные вопросы, связанные с внедрением сертификата, а также оказанием влияния на работу сетей операторов связи.

Применение сертификата безопасности в дальнейшем будет осуществляться при возникновении угрозы национальной безопасности в виде кибер и информационных атак, с предварительным уведомлением граждан Республики Казахстан.

С учетом полученных положительных результатов тестирования, КНБ информирует о прекращении тестирования с 7 августа т.г. В ближайшее время на официальном сайте будут размещены инструкции по удалению сертификата безопасности с личных устройств.

Комитет национальной безопасности уведомляет о необходимости соблюдения законодательства Республики Казахстан по хранению персональных данных граждан на территории страны и выполнению требований уполномоченных органов по удалению противозаконной информации.



Source: <http://knb.gov.kz/ru/news/v-otnoshenii-sertifikata-bezopasnosti>

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
