Censored Planet

Censored Planet Observatory

Measuring Internet censorship globally, continuously, and remotely

Internet Measurement Village 2020

Ram Sundara Raman

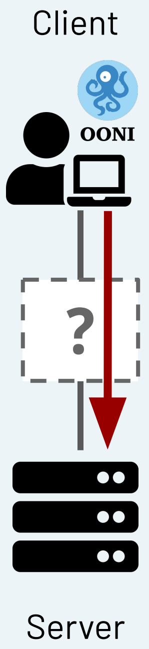
June 26, 2020

Measuring Censorship is a Complex Problem!

Internet censorship practices are diverse in their methods, targets, timing, differing by regions (even within countries or networks), as well as across time.

Direct Censorship Measurement

- Ask people on the ground, or deploy software or hardware in censored region (e.g. OONI probe, FreedomHouse)
- Use VPNs, or research networks (e.g. PlanetLab, ICLab)



Challenges with Direct Measurements

Scale

Takes tremendous effort to recruit a large number of volunteers or access points

Coverage

Hard to obtain access points that cover a majority of networks in the country

Continuity

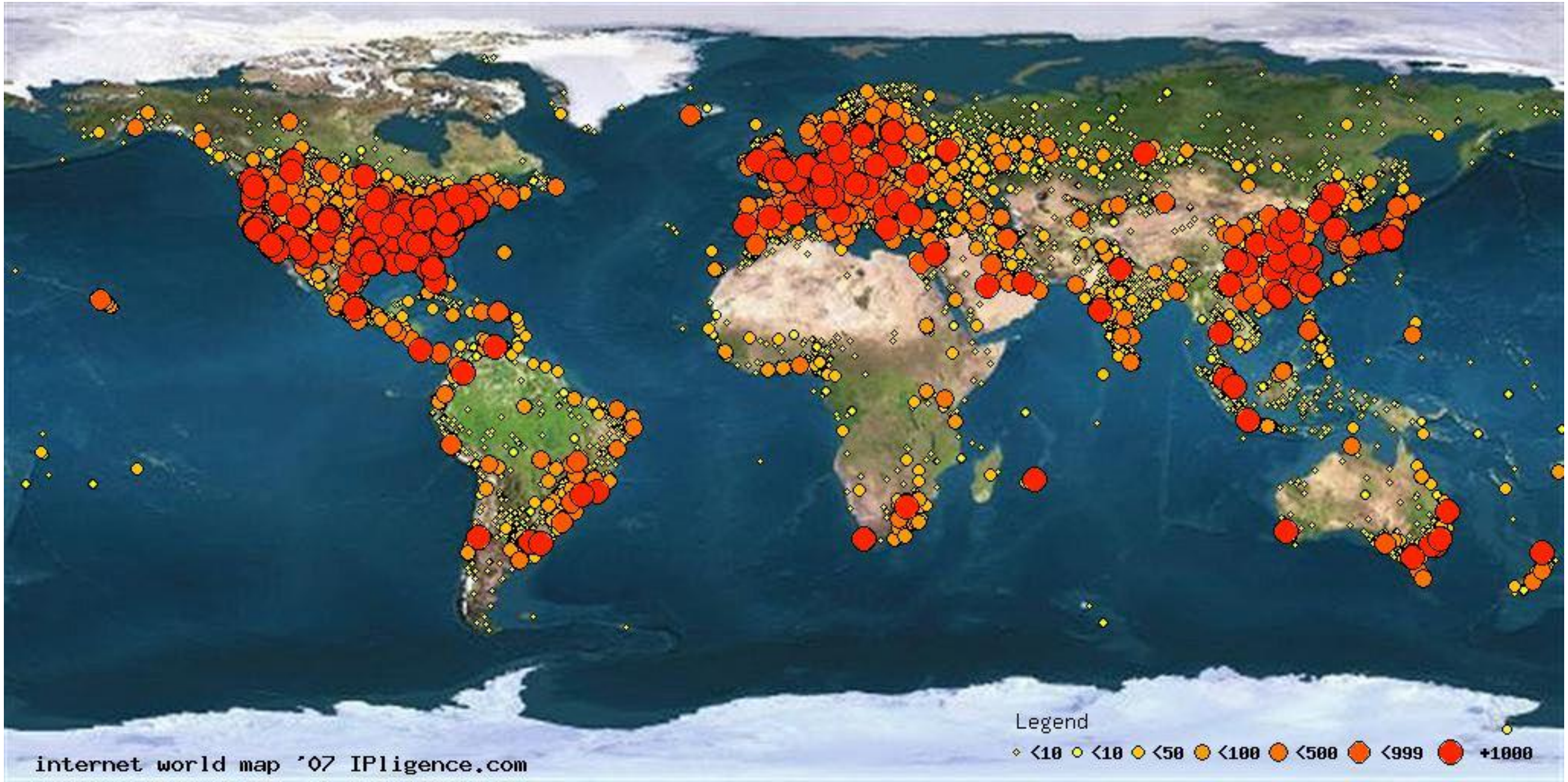
Hard to continuously and repetitively run measurements using volunteers

Synchronization

New updates and censorship measurement techniques must be pushed, and detection may be delayed

Ethics

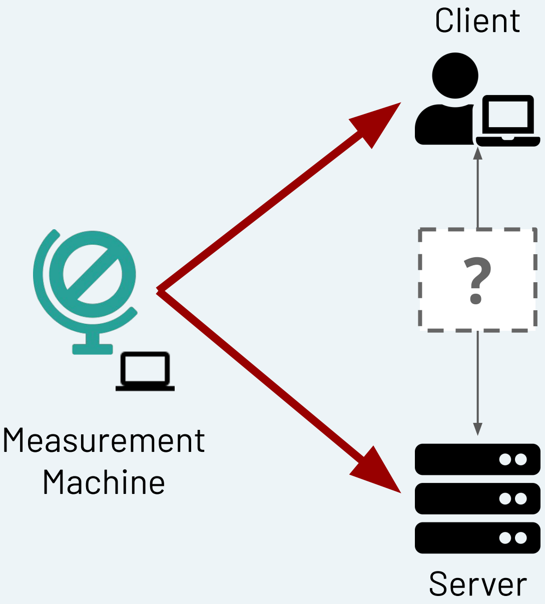
Risky to run censorship measurements unless the proper precautions are taken



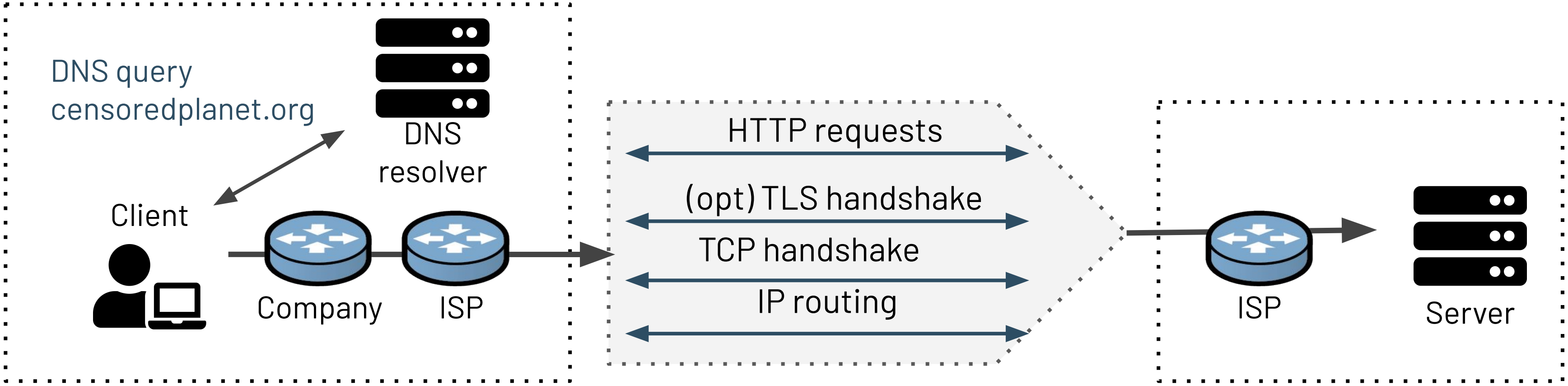
IPv4 hosts - Internet infrastructure is everywhere

Remote Censorship Measurements

Can we detect whether pairs of hosts around the world can talk to each other without controlling either endpoint?

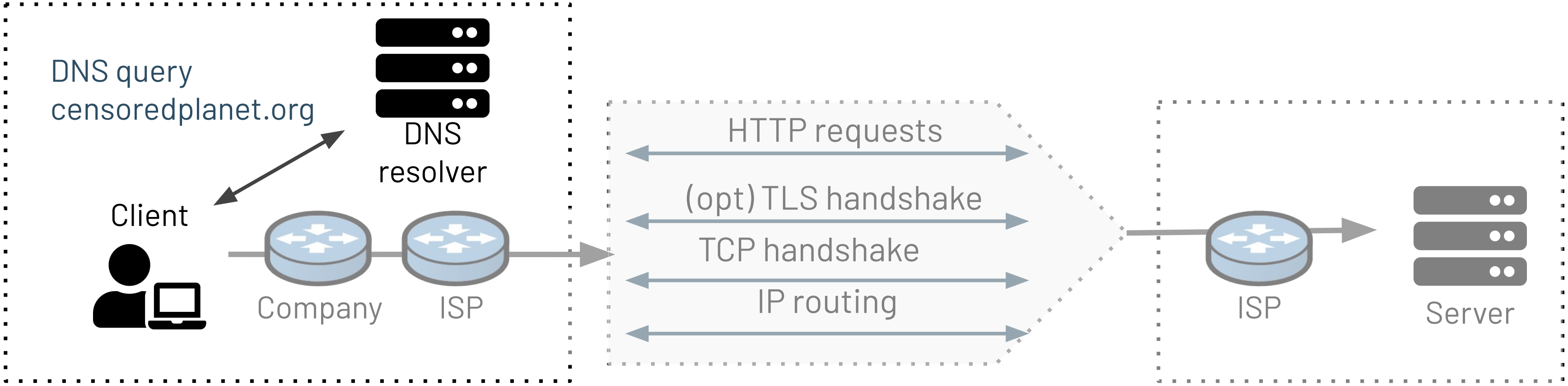


Censorship can occur at multiple protocol layers



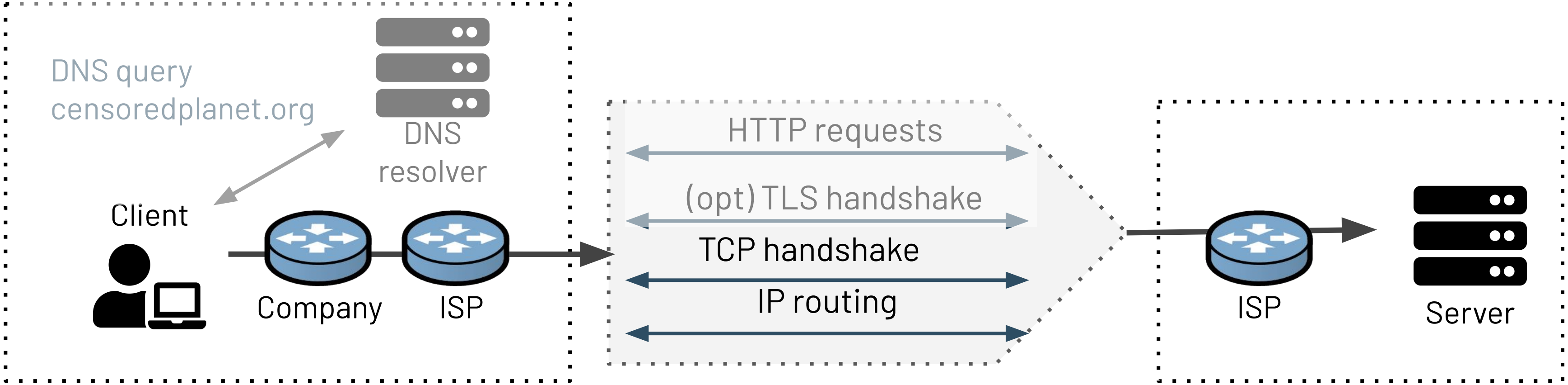
Challenge: Design methods to detect interference remotely at all network layers, without end-user participation.

Censorship can occur at multiple protocol layers



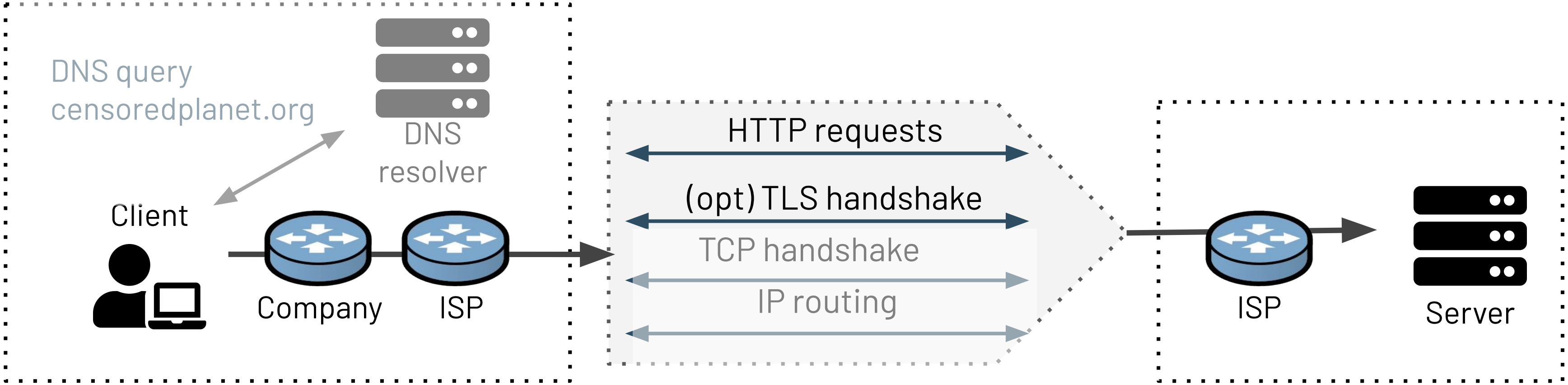
Satellite and Iris
(https://www.censoredplanet.org/projects/satellite)

Censorship can occur at multiple protocol layers



Spooky Scan and Augur
(https://www.censoredplanet.org/projects/augur)

Censorship can occur at multiple protocol layers



Quack and Hyperquack
(https://www.censoredplanet.org/projects/quack)
(https://www.censoredplanet.org/projects/hyperquack)

Remote Measurement Techniques

1

Satellite and Iris

Measure DNS manipulation using Open DNS resolvers

2

Quack and Hyperquack

Measure application-layer keyword censorship using Echo and HTTP(S) servers

3

Spooky Scan and Augur

Measure global TCP/IP blocking using IP ID side channels

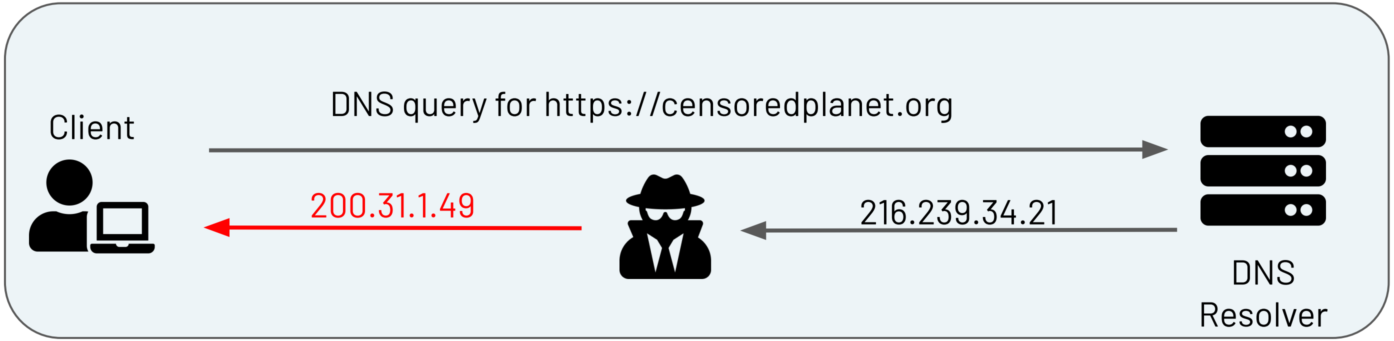
Remote Measurement Techniques

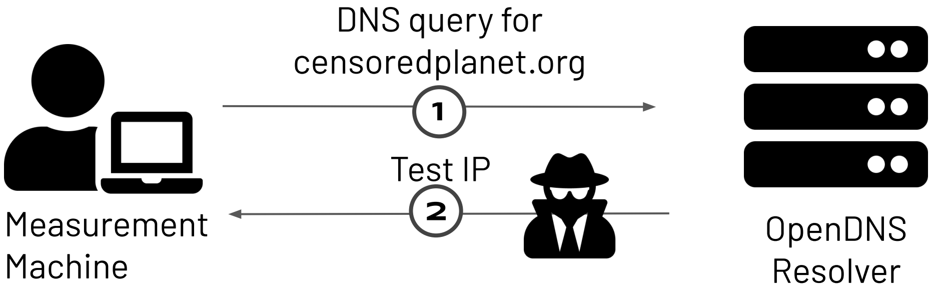
1 **Satellite and Iris**
Measure DNS manipulation using Open DNS resolvers

2 **Quack and Hyperquack**
Measure application-layer keyword censorship using Echo and HTTP(S) servers

3 **Spooky Scan and Augur**
Measure global TCP/IP blocking using IP ID side channels

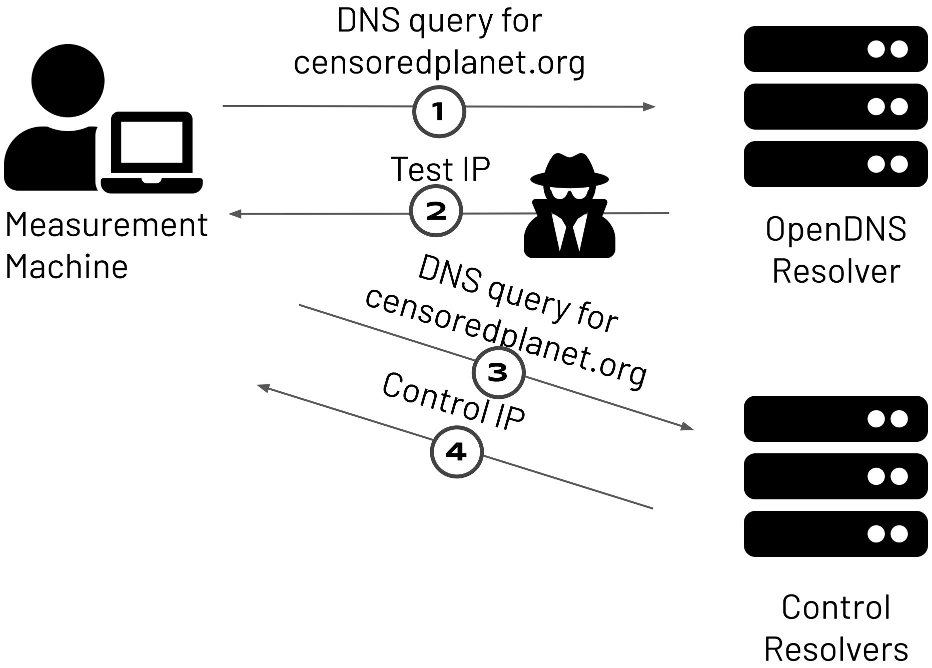
DNS Manipulation



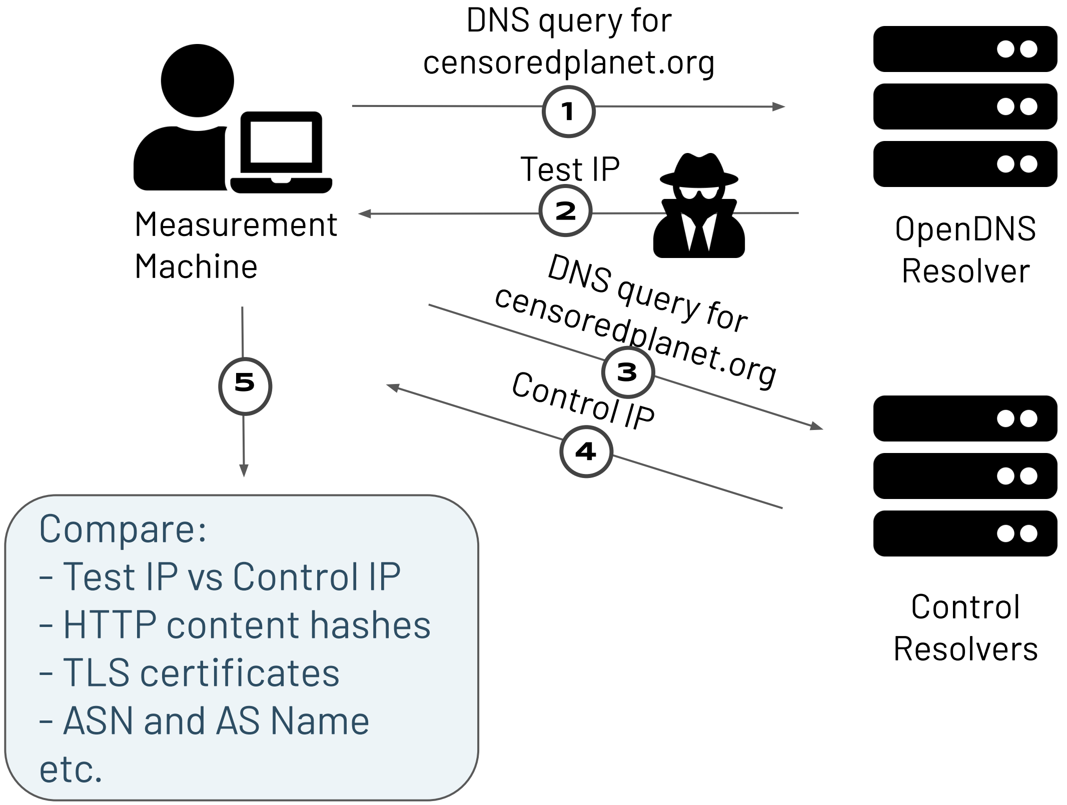


Satellite & Iris

Satellite & Iris



Satellite & Iris



DNS query for censoredplanet.org

1

Test IP

2

Measurement Machine

OpenDNS Resolver

DNS query for censoredplanet.org

3

Control IP

4

5

Control Resolvers

Compare:
- Test IP vs Control IP
- HTTP content hashes
- TLS certificates
- ASN and AS Name

etc.

Satellite Scale, Coverage and Ethics

- More than 8.2 million OpenDNS resolvers in 232 countries
- To reduce risk, we want to choose infrastructural resolvers
- We use resolvers with a valid PTR record beginning with the subdomain ns[0-9]* or nameserver[0-9]* → Likely to be part of big organizations
- 30k resolvers in ~4,500 ASes in 175 countries
- Stable DNS resolvers allow us to repetitively run measurements over time

Remote Measurement Techniques

1

Satellite and Iris

Measure DNS manipulation using Open DNS resolvers

2

Quack and Hyperquack

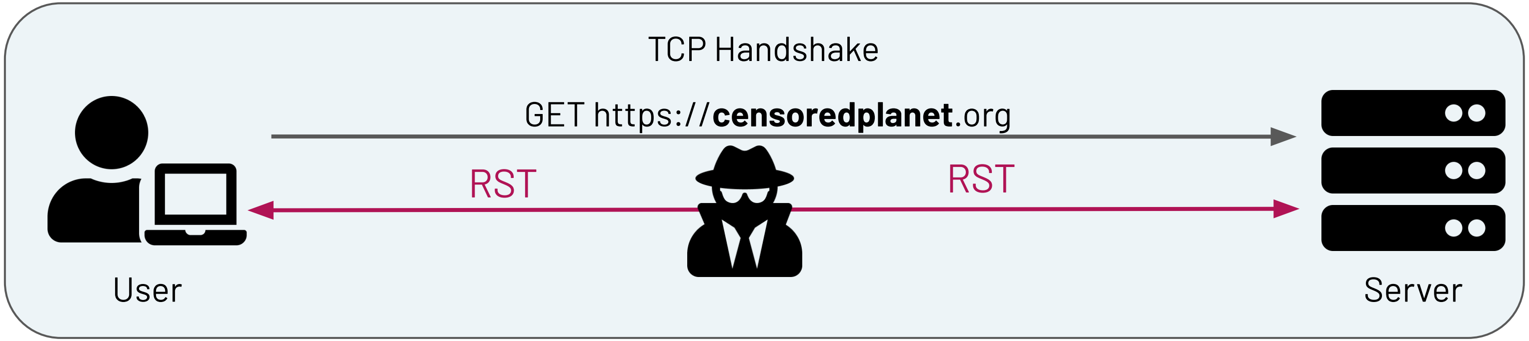
Measure application-layer keyword censorship using Echo and HTTP(S) servers

3

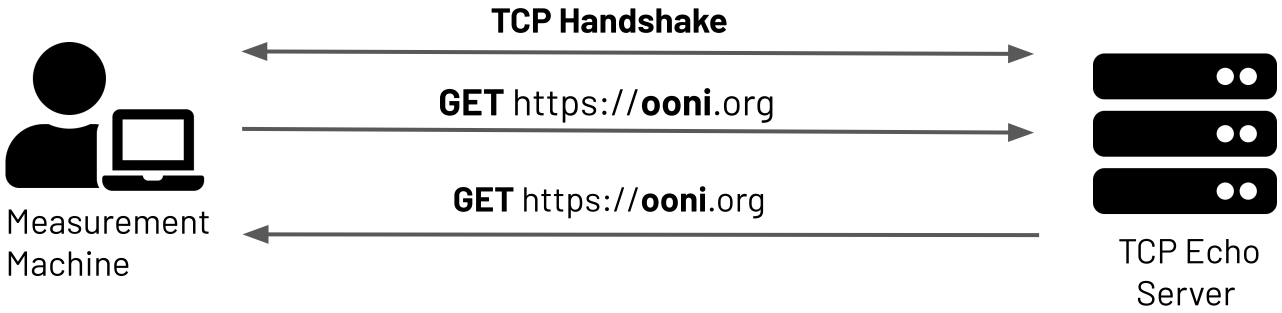
Spooky Scan and Augur

Measure global TCP/IP blocking using IP ID side channels

Application-layer keyword blocking

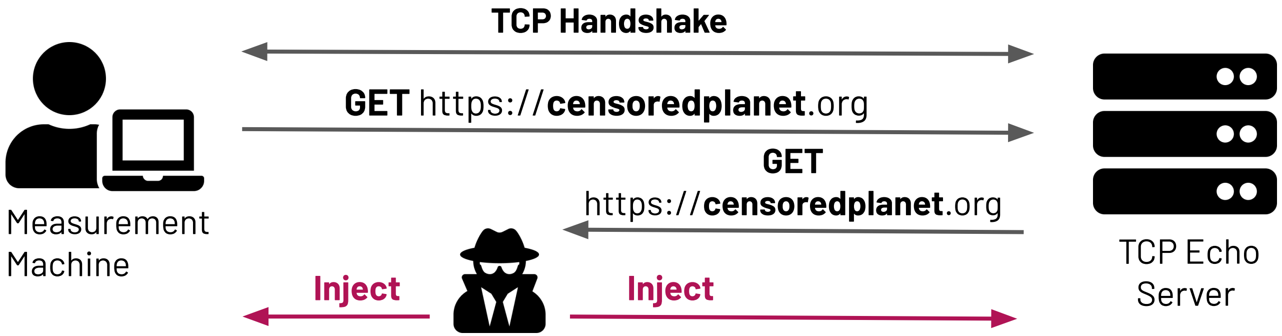


Quack



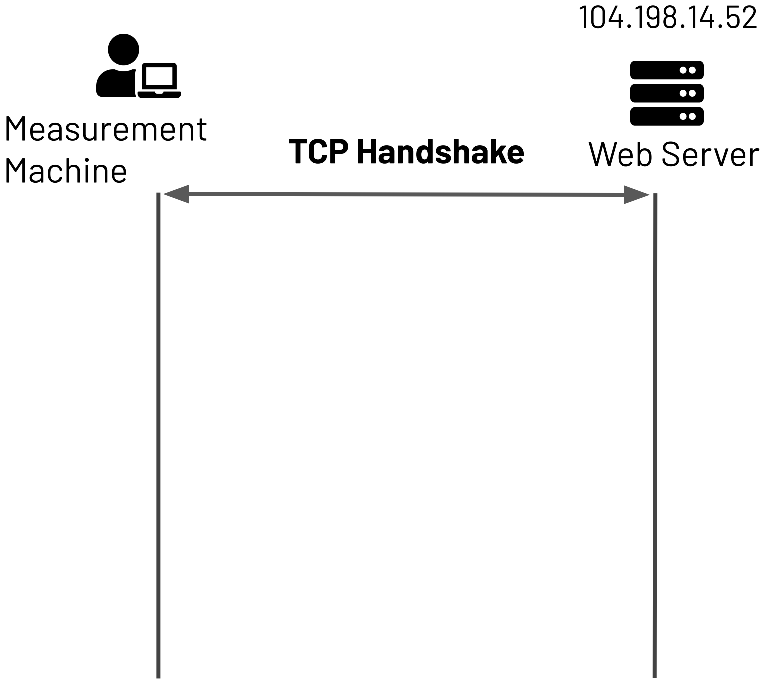
An Echo service simply sends back to the originating source any data it receives.

Quack

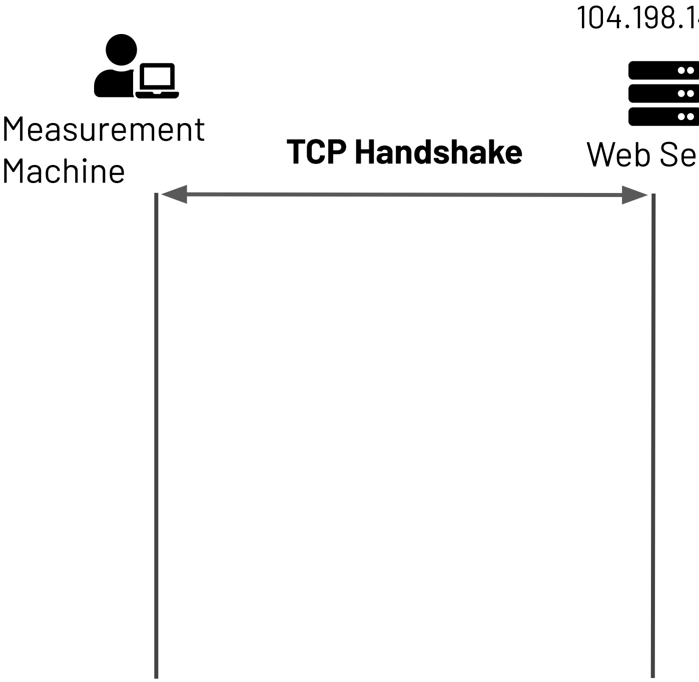

TCP Handshake
GET https://censoredplanet.org
GET https://censoredplanet.org
Measurement Machine
Inject
Inject
TCP Echo Server

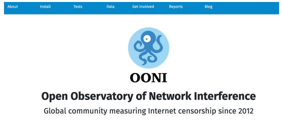
33,000 usable Echo Servers in ~2,800 ASes in 166 countries

Hyperquack



Hyperquack



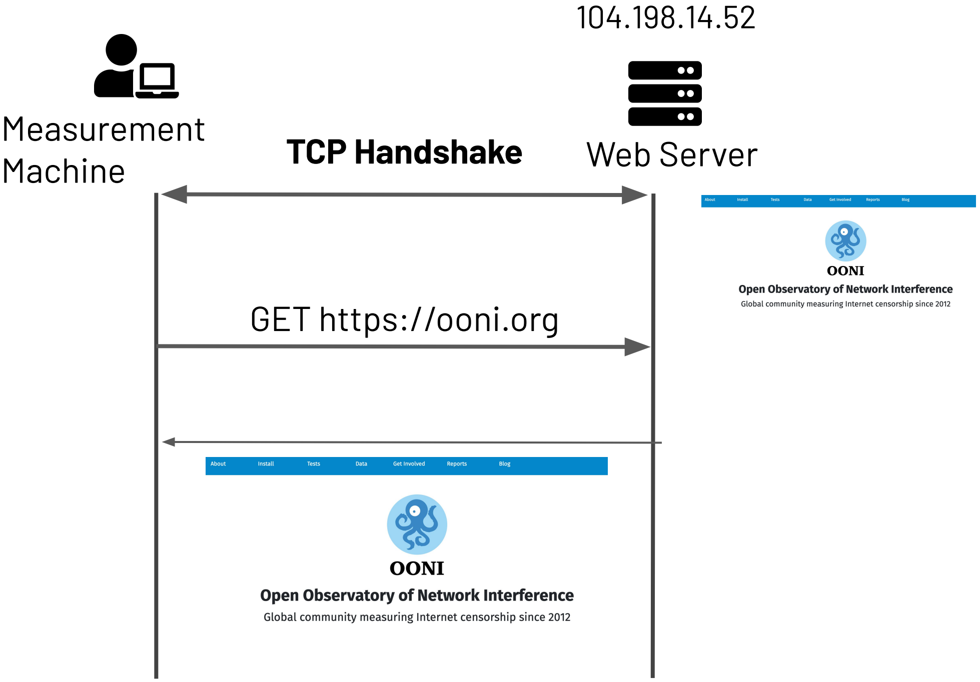


OONI

Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

Hyperquack



104.198.14.52

Measurement Machine

TCP Handshake

Web Server

GET https://ooni.org

About Install Tests Data Get Involved Reports Blog

OONI

Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

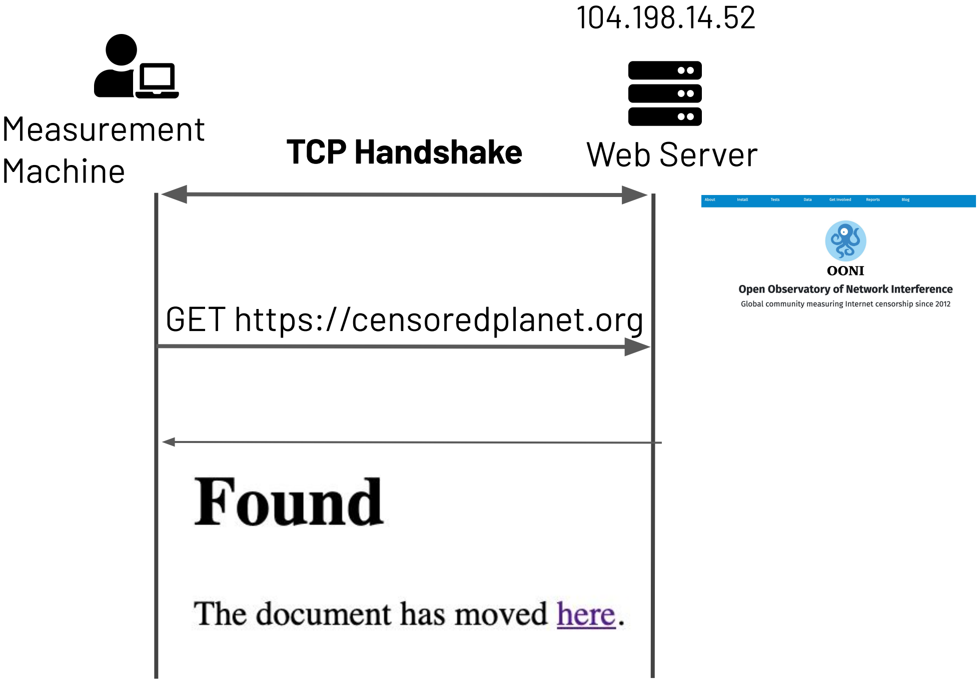
About Install Tests Data Get Involved Reports Blog

OONI

Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

Hyperquack



OONI

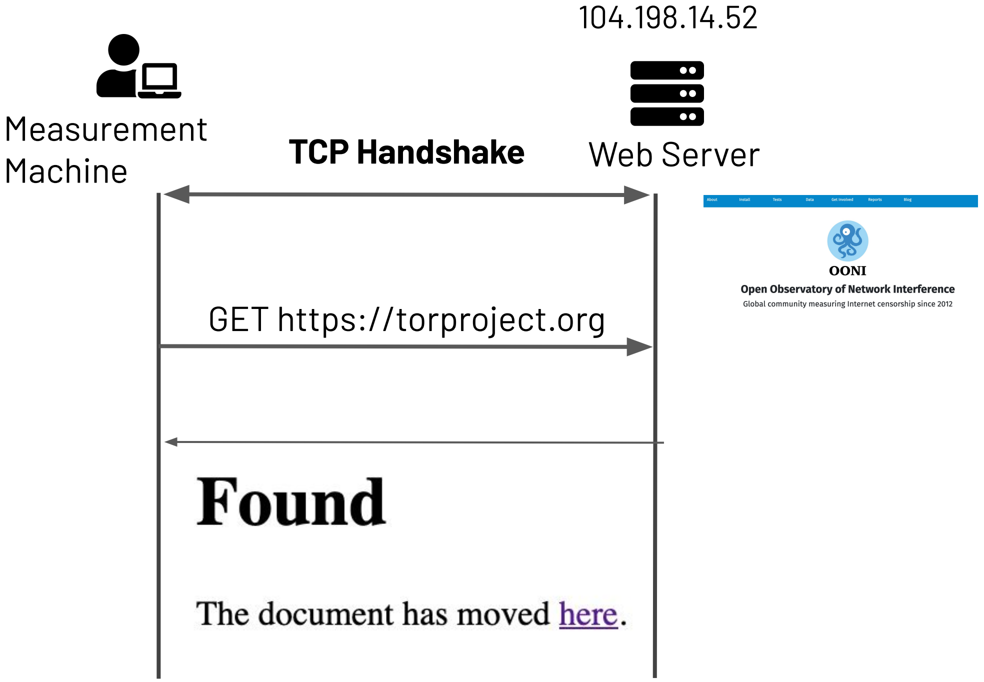
Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

Found

The document has moved here.

Hyperquack



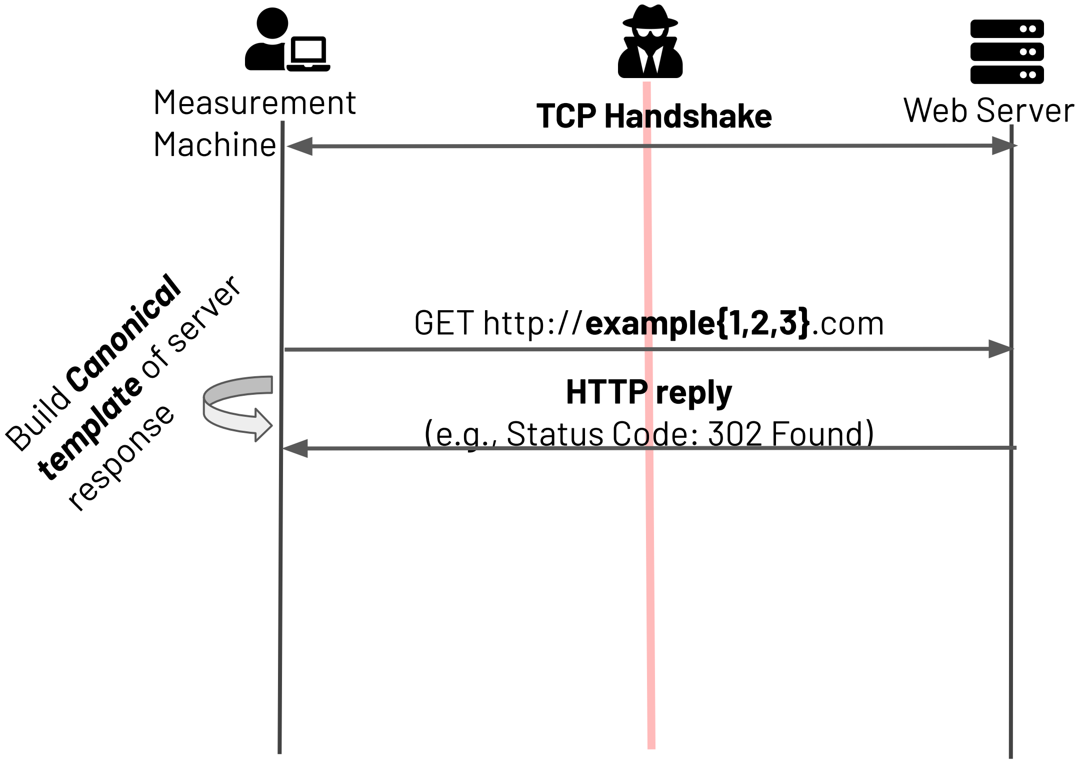
Open Observatory of Network Interference

Global community measuring Internet censorship since 2012

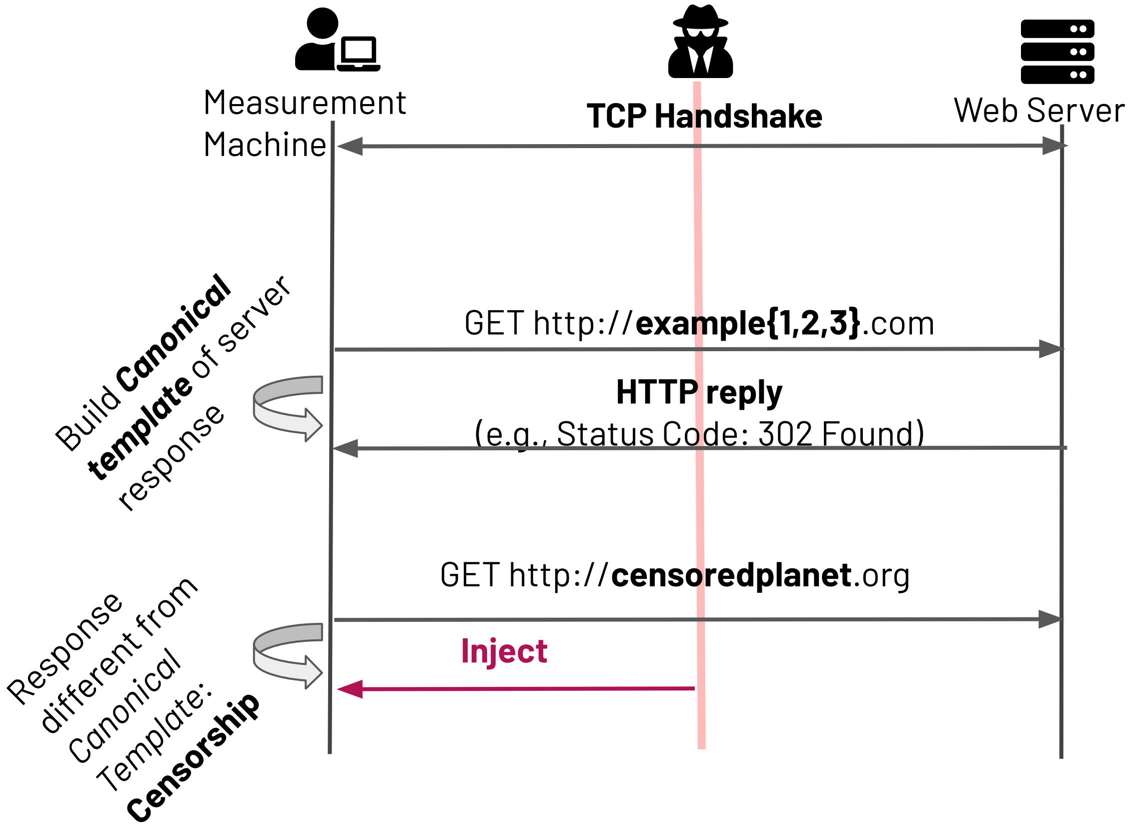
Found

The document has moved here.

Hyperquack


Measurement Machine
TCP Handshake
Web Server
GET http://**example{1,2,3}**.com
HTTP reply
(e.g., Status Code: 302 Found)
Build **Canonical template** of server response

Hyperquack



Measurement Machine
TCP Handshake
Web Server
GET http://**example{1,2,3}**.com
HTTP reply
(e.g., Status Code: 302 Found)
Build **Canonical template** of server response
GET http://**censoredplanet**.org
Inject
Response different from Canonical Template: **Censorship**

Hyperquack Scale, Coverage and Ethics

- More than 50 million web servers (all around the world)
- To reduce risk, we want to choose **infrastructural** vantage points
- Use web servers that produce a valid EV certificate, as they are more likely to be organizational
- After filtering for capacity, we regularly use 30k web servers in ~3,800 ASes in 191 countries

Remote Measurement Techniques

1

Satellite and Iris

Measure DNS manipulation using Open DNS resolvers

2

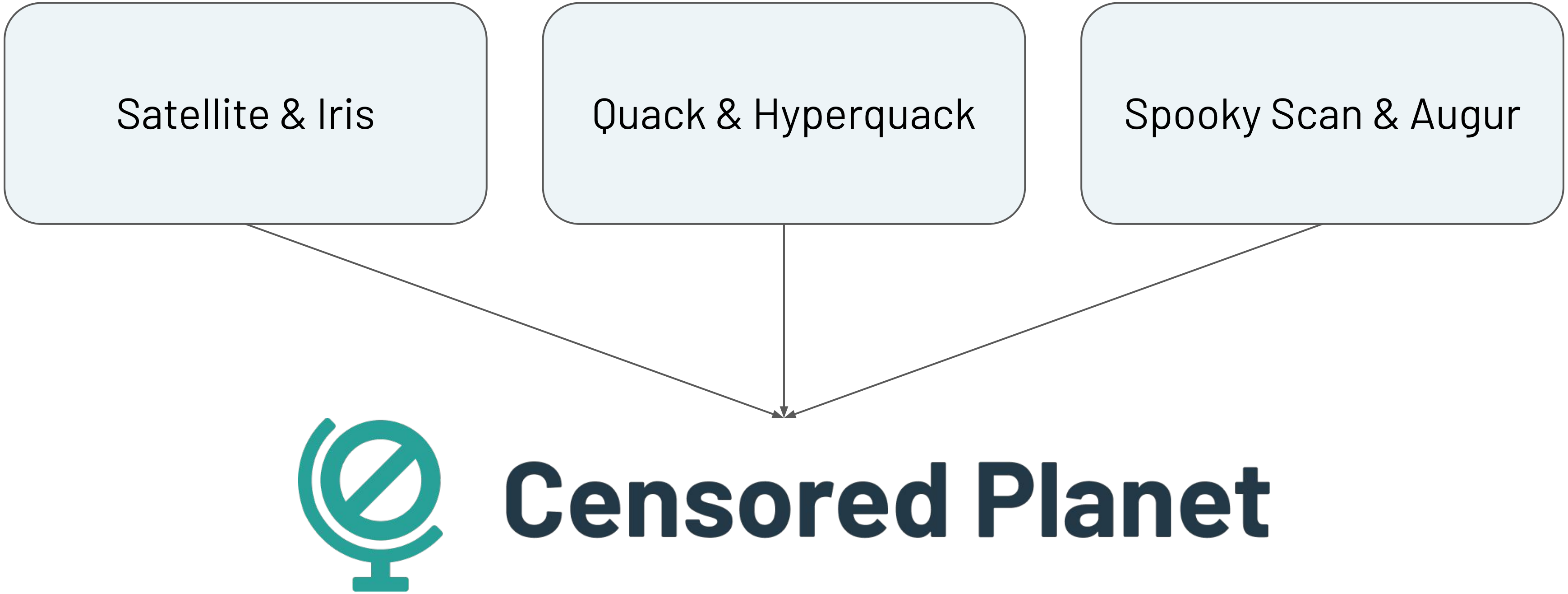
Quack and Hyperquack

Measure application-layer keyword censorship using Echo and HTTP(S) servers

3

Spooky Scan and Augur

Measure global TCP/IP blocking using IP ID side channels



Satellite & Iris

Quack & Hyperquack

Spooky Scan & Augur

Censored Planet

Censored Planet Observatory

The Censored Planet Observatory uses remote measurement tools to scalably, ethically and continuously measure different kinds of global Internet censorship

Censored Planet Observatory

- Launched in August 2018 and running continuously since
- Continuous baseline of reachability data for **2000 sensitive domains and IP addresses (From Alexa and Citizen Lab) each week**
- More than **95,000 vantage points** in **221 countries and territories** (updated every week)
- Rapid focus capabilities to analyze censorship events in detail

25 billion

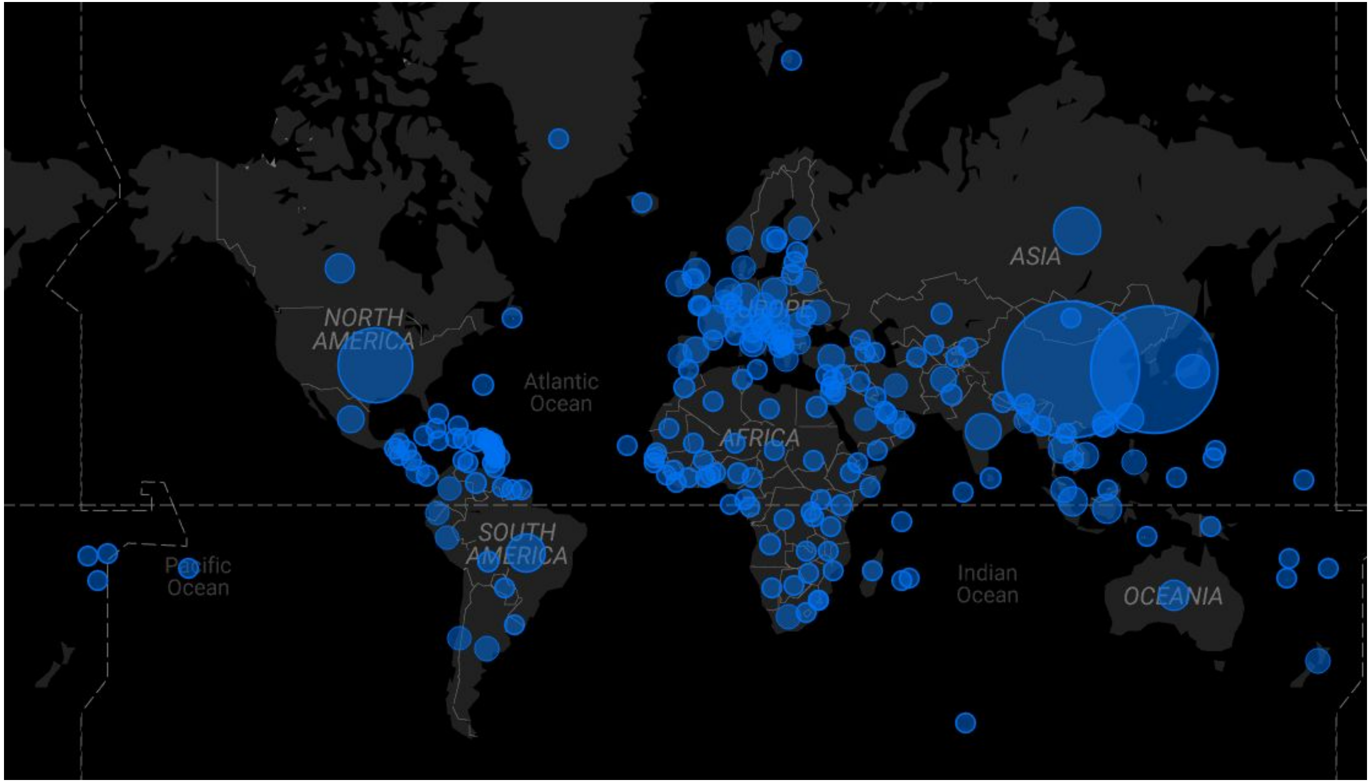
Measurements over 22 Months

221 countries

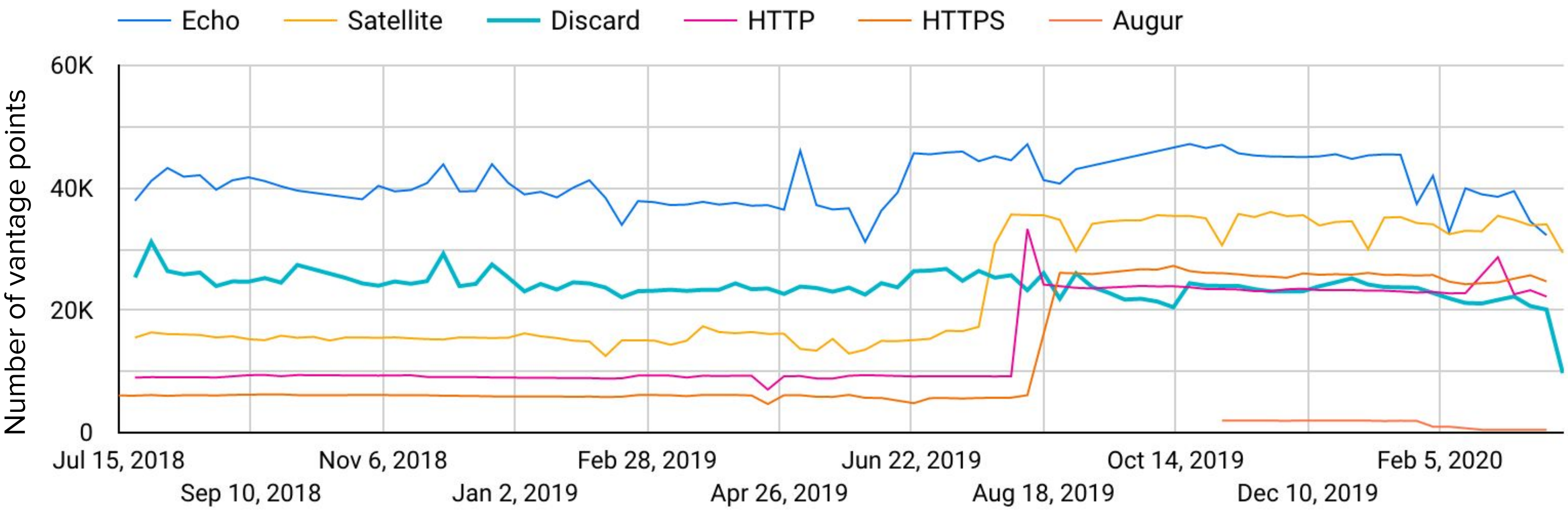
42%-360% increase compared to OONI, ICLab

8 ASes (median)/country

Median increase of 4-7 ASes per country



Vantage Points in March 2020 (Scale 1 - 29,617)

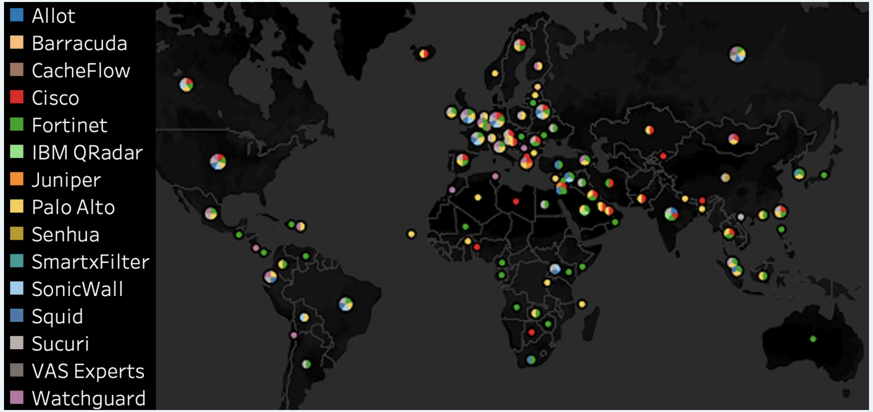


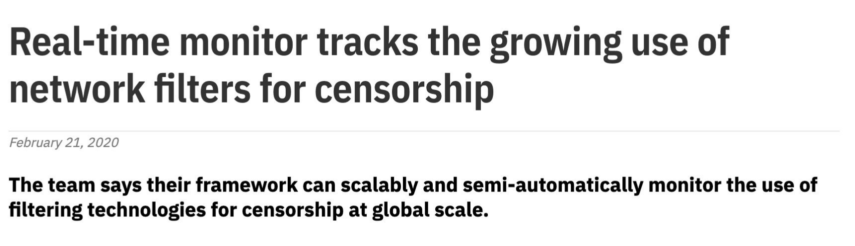
Vantage Points over time

Identifying Network Censorship Devices

Censored Planet data identified the deployments of many network censorship devices

Publication - Measuring the Deployment of Network Censorship Filters at Global Scale; R. Sundara Raman, A. Stoll, J. Dalek, R. Ramesh, W. Scott, and R. Ensafi; Network and Distributed System Security Symposium (NDSS), 2020





Real-time monitor tracks the growing use of network filters for censorship

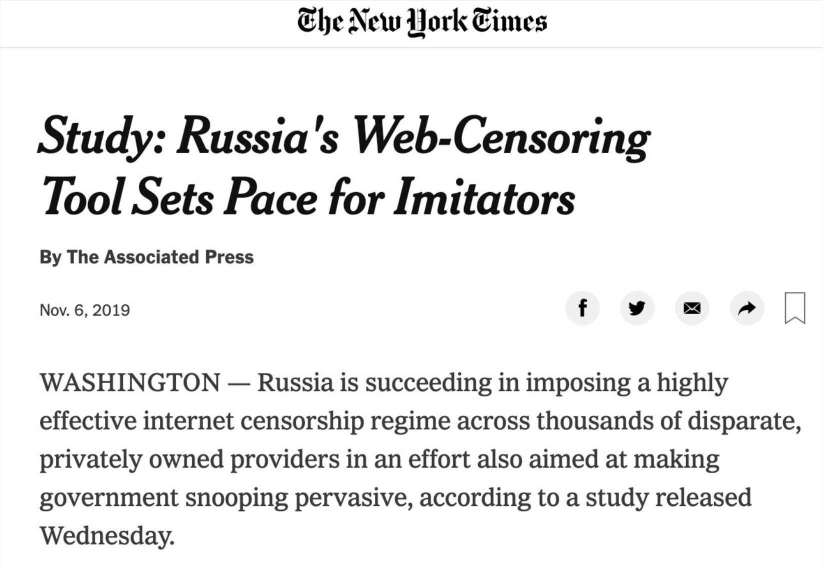
February 21, 2020

The team says their framework can scalably and semi-automatically monitor the use of filtering technologies for censorship at global scale.

Investigating Russia’s Censorship Model

Censored Planet helped investigate large-scale ISP specific blocking of online resources in Russia’s authoritative blocklist.

Publication - Decentralized Control: A Case Study of Russia; R. Ramesh, R. Sundara Raman, M. Bernhard, V. Ongkowijaya, L. Evdokimov, A. Edmundson, S. Sprecher, M. Ikram, and R. Ensafi; Network and Distributed System Security Symposium (NDSS), 2020



The New York Times

Study: Russia's Web-Censoring Tool Sets Pace for Imitators

By The Associated Press

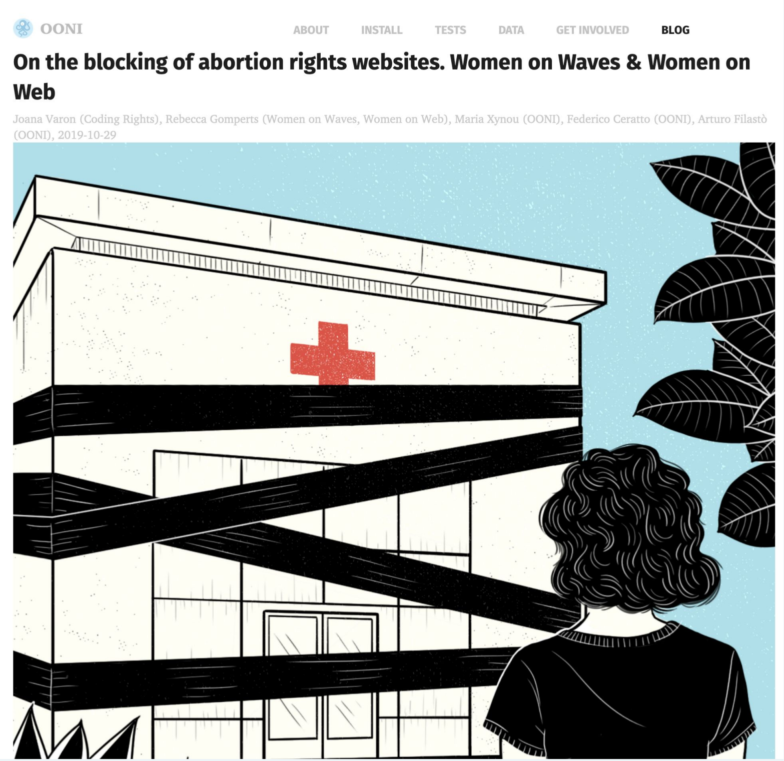
Nov. 6, 2019

WASHINGTON — Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive, according to a study released Wednesday.

Complementing Direct Measurements

Censored Planet can complement in-depth direct measurements by providing higher scale. Censored Planet data confirmed OONI's observation about the blocking of abortion rights websites.

Report - https://ooni.org/post/2019-blocking-abortion-rights-websites-women-on-waves-web/



On the blocking of abortion rights websites. Women on Waves & Women on Web

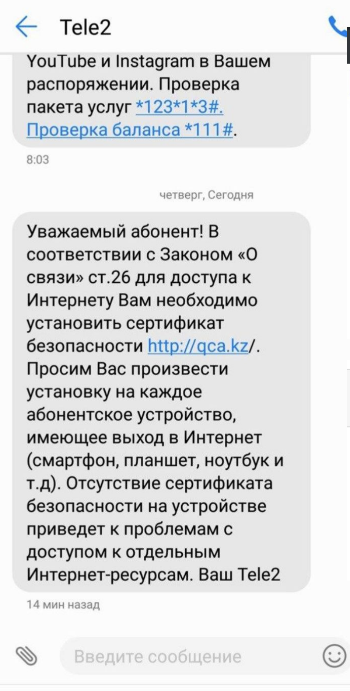
Joana Varon (Coding Rights), Rebecca Gomperts (Women on Waves, Women on Web), Maria Xynou (OONI), Federico Ceratto (OONI), Arturo Filastò (OONI), 2019-10-29

Censored Planet's Rapid Focus

Kazakhstan's HTTPS interception
https://censoredplanet.org/kazakhstan

Kazakhstan's National TLS Interception

- **July 17, 2019**: Government started intercepting large fraction of HTTPS traffic within its borders.
- Local ISPs told to instruct users to install a government-issued certificate on all devices and in every browser.



Tele2

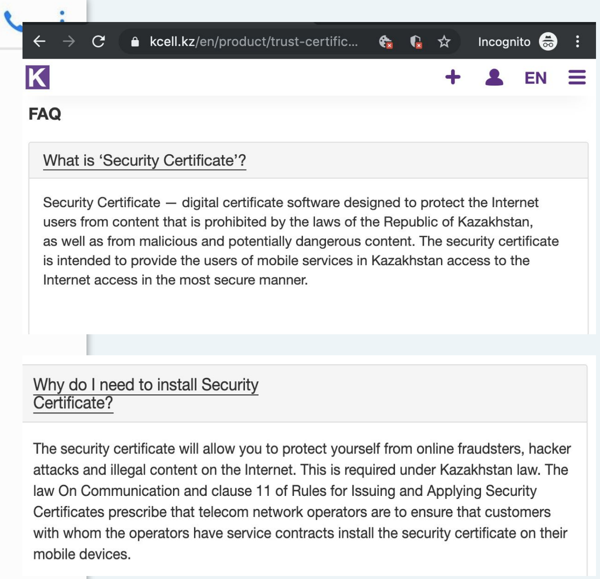
YouTube и Instagram в Вашем распоряжении. Проверка пакета услуг *123*1*3#. Проверка баланса *111#.

8:03

четверг, Сегодня

Уважаемый абонент! В соответствии с Законом «О связи» ст.26 для доступа к Интернету Вам необходимо установить сертификат безопасности http://qca.kz/. Просим Вас произвести установку на каждое абонентское устройство, имеющее выход в Интернет (смартфон, планшет, ноутбук и т.д). Отсутствие сертификата безопасности на устройстве приведет к проблемам с доступом к отдельным Интернет-ресурсам. Ваш Tele2

14 мин назад



kcell.kz/en/product/trust-certific...

FAQ

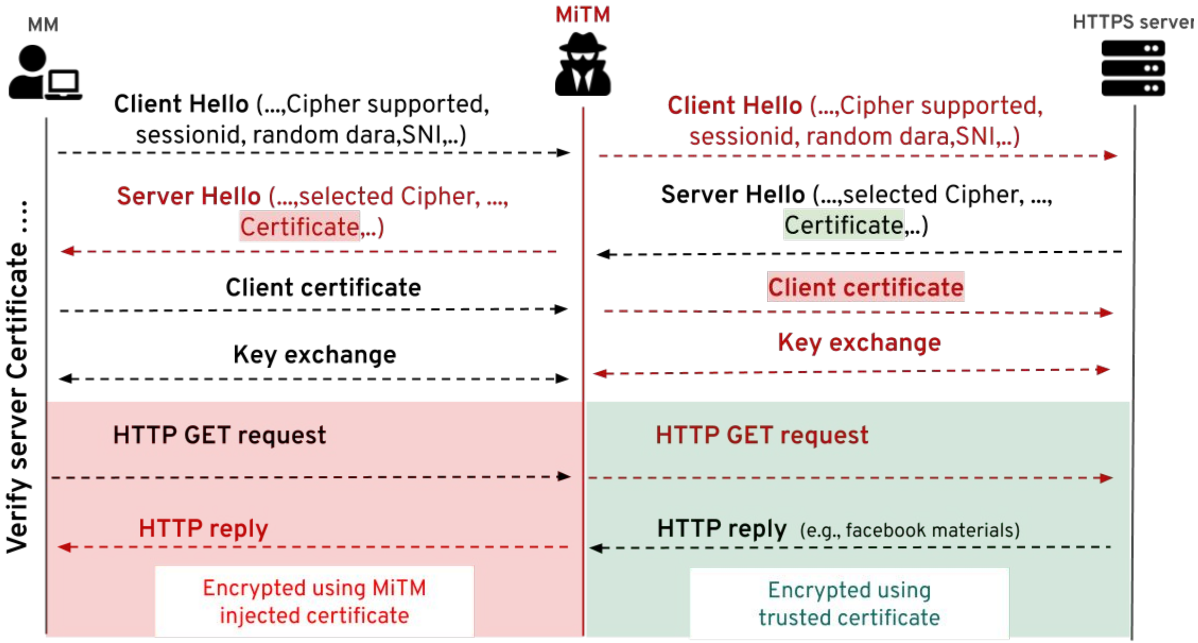
What is 'Security Certificate'?

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.

How the interception works


MM
MiTM
HTTPS server
Verify server Certificate ….
Client Hello (….,Cipher supported, sessionid, random dara,SNI,..)
Server Hello (….,selected Cipher, …., Certificate,..)
Client certificate
Key exchange
HTTP GET request
HTTP reply
Encrypted using MiTM injected certificate
Client Hello (….,Cipher supported, sessionid, random dara,SNI,..)
Server Hello (….,selected Cipher, …., Certificate,..)
Client certificate
Key exchange
HTTP GET request
HTTP reply (e.g., facebook materials)
Encrypted using trusted certificate

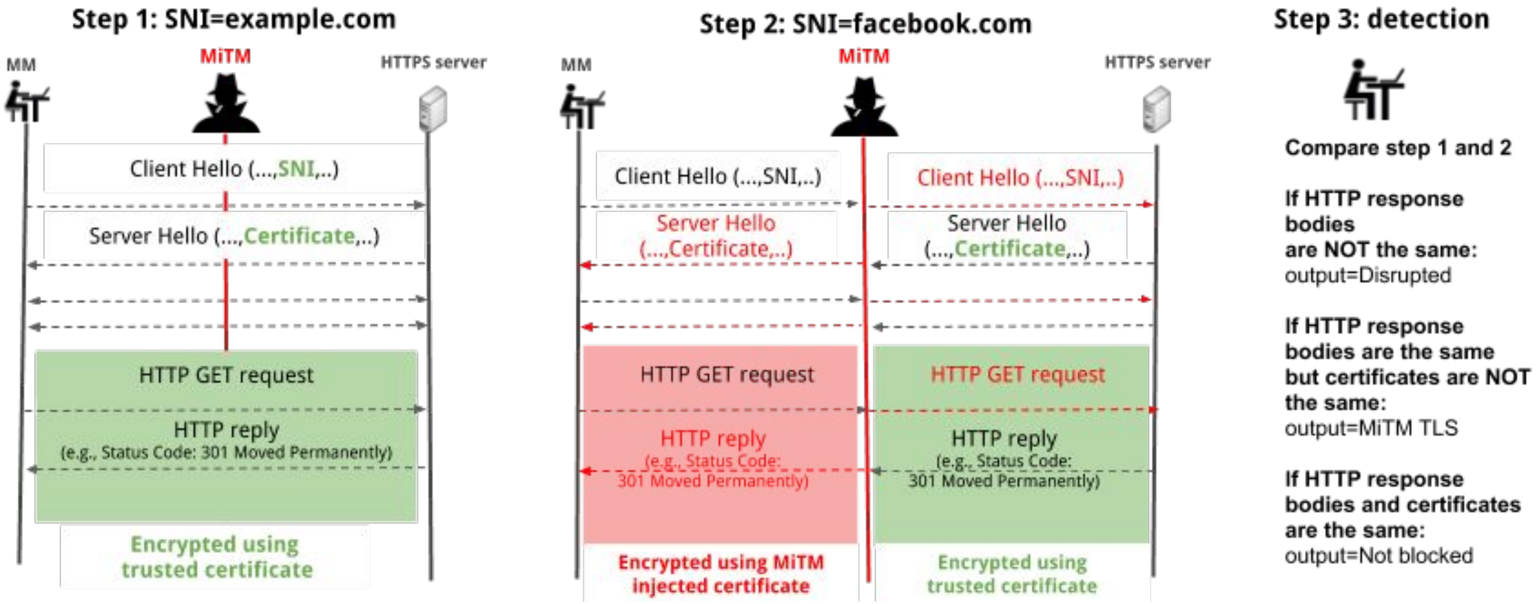
What does this mean for users?

- Complete visibility
- Traffic modification
- Selective blocking

Haven’t installed the fake cert?

- Security warnings for all website access
- Access essentially blocked if HSTS is enabled

Detecting the interception



Step 1: SNI=example.com

MM

MiTM

HTTPS server

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

MM

MiTM

HTTPS server

Client Hello (...,SNI,..)

Client Hello (...,SNI,..)

Server Hello (...,Certificate,..)

Server Hello (...,Certificate,..)

HTTP GET request

HTTP GET request

HTTP reply
(e.g., Status Code: 301 Moved Permanently)

HTTP reply
(e.g., Status Code: 301 Moved Permanently)

Encrypted using MiTM injected certificate

Encrypted using trusted certificate

Step 3: detection

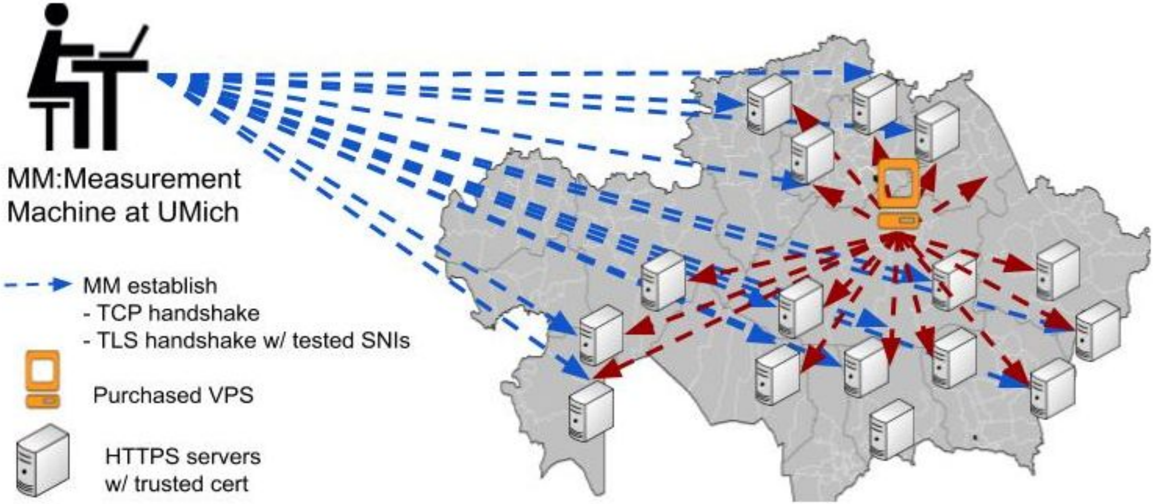
Compare step 1 and 2

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

- Hyperquack detects the use of rogue certificates
- Measurements to some VPs in Kazakhstan saw the `Qaznet Trust Network` cert

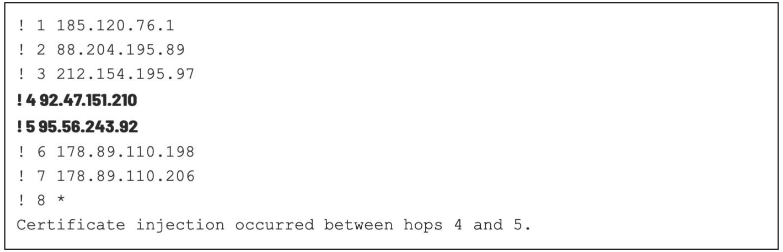


Running customized measurements

Observations

- Only 7.0 - 24% of TLS hosts tested had certificates injected → interception only happened in a fraction of the country.

- Using TTL-limited measurements, observed only certain portions of the connections, passing through AS9198 (KazakhTelecom) were affected

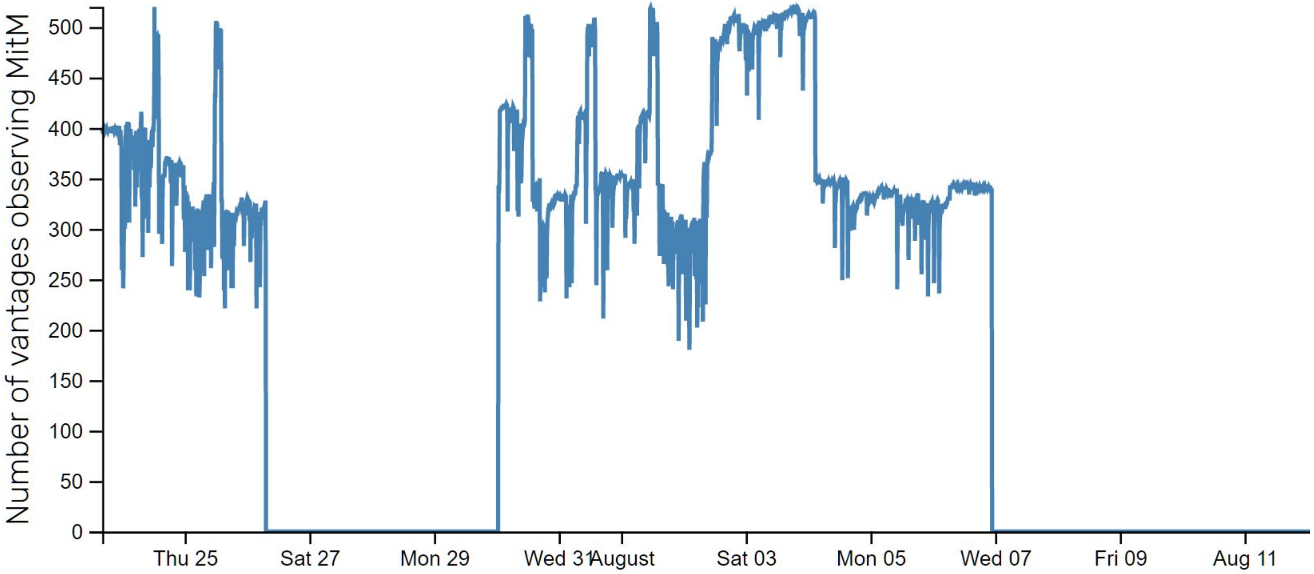


```
! 1 185.120.76.1
! 2 88.204.195.89
! 3 212.154.195.97
! 4 92.47.151.210
! 5 95.56.243.92
! 6 178.89.110.198
! 7 178.89.110.206
! 8 *
Certificate injection occurred between hops 4 and 5.
```

Observations

37 domains were affected - Mostly social media domains

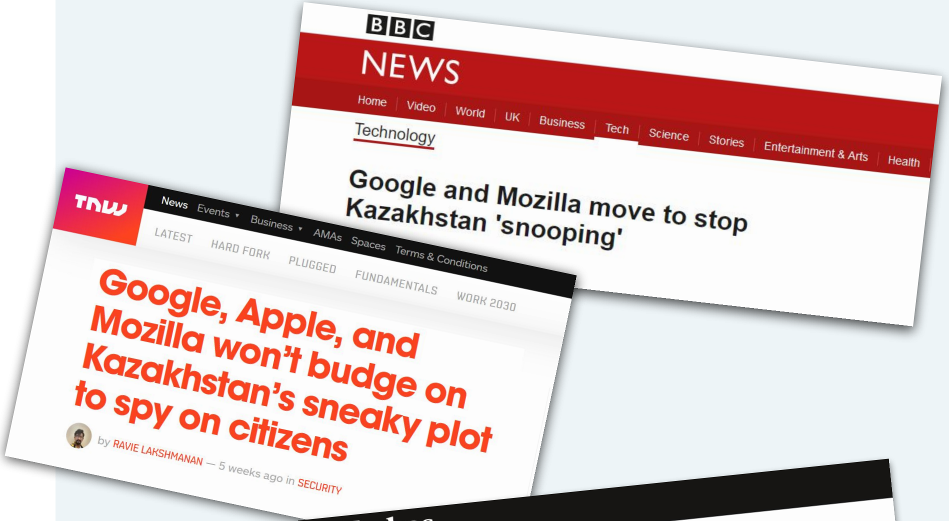
- 20 Google domains
- 7 Facebook domains
- 4 vk domains



Longitudinal Tracking

Browsers Take a Stand Against Interception

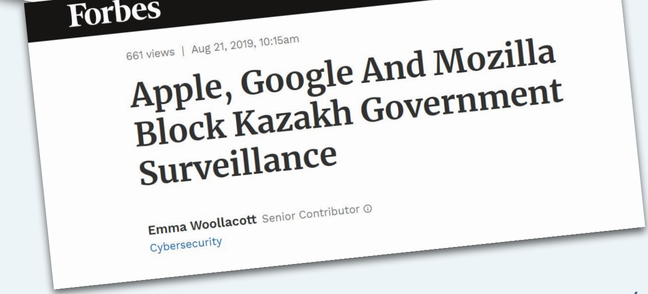
The use of ‘Qaznet Trust Network’ root CA certificate in Chrome, Firefox, and Safari is now prevented.



Google and Mozilla move to stop Kazakhstan 'snooping'

Google, Apple, and Mozilla won't budge on Kazakhstan's sneaky plot to spy on citizens

by RAVIE LAKSHMANAN — 5 weeks ago in SECURITY



661 views | Aug 21, 2019, 10:15am

Apple, Google And Mozilla Block Kazakh Government Surveillance

Emma Woollacott Senior Contributor

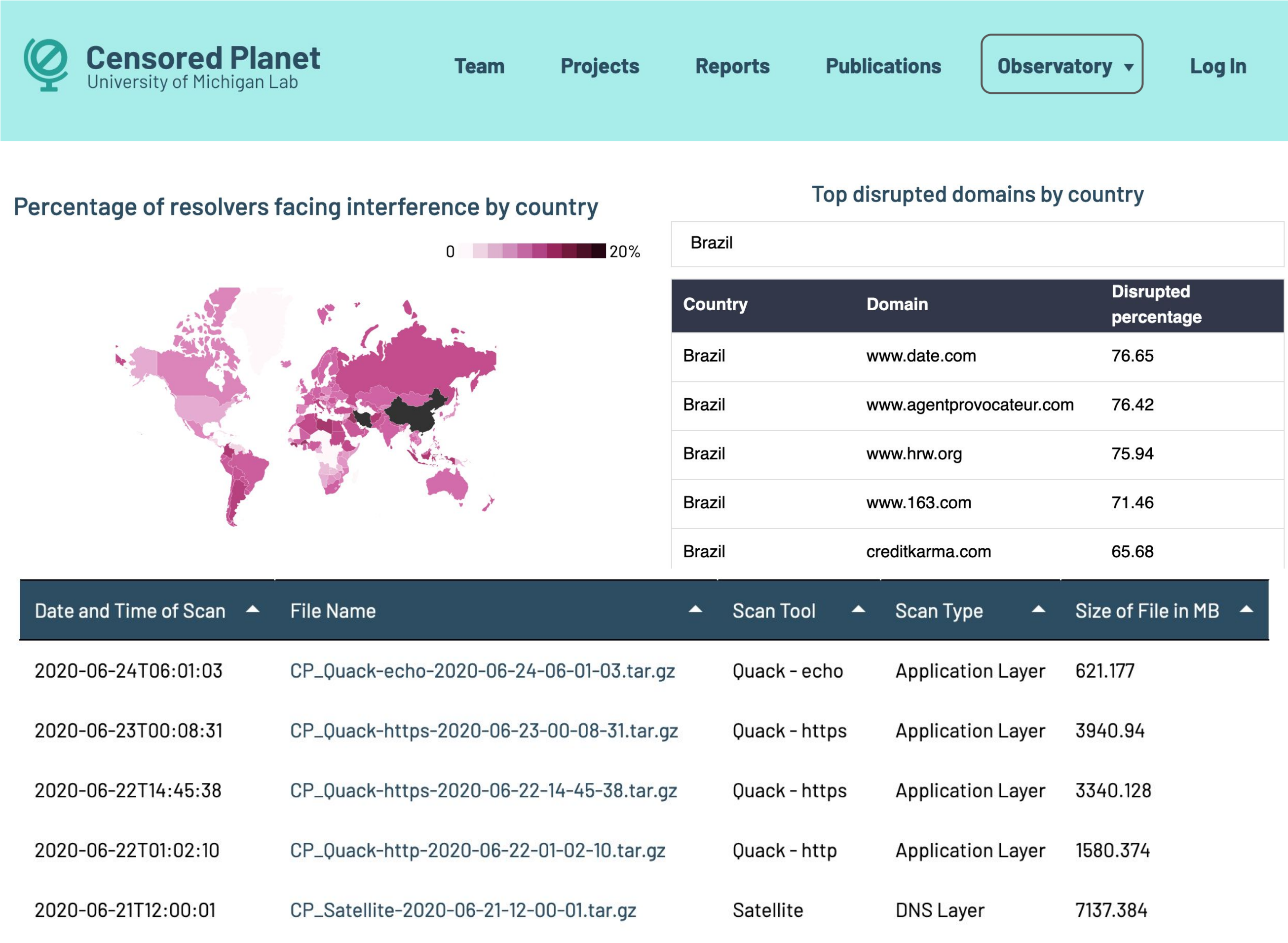
Cybersecurity

Website

https://censoredplanet.org/observatory

Please contact us at:
censoredplanet@umich.edu

Censored Planet



Percentage of resolvers facing interference by country

Top disrupted domains by country

Brazil

Country	Domain	Disrupted percentage
Brazil	www.date.com	76.65
Brazil	www.agentprovocateur.com	76.42
Brazil	www.hrw.org	75.94
Brazil	www.163.com	71.46
Brazil	creditkarma.com	65.68

Date and Time of Scan ▲	File Name ▲	Scan Tool ▲	Scan Type ▲	Size of File in MB ▲
2020-06-24T06:01:03	CP_Quack-echo-2020-06-24-06-01-03.tar.gz	Quack - echo	Application Layer	621.177
2020-06-23T00:08:31	CP_Quack-https-2020-06-23-00-08-31.tar.gz	Quack - https	Application Layer	3940.94
2020-06-22T14:45:38	CP_Quack-https-2020-06-22-14-45-38.tar.gz	Quack - https	Application Layer	3340.128
2020-06-22T01:02:10	CP_Quack-http-2020-06-22-01-02-10.tar.gz	Quack - http	Application Layer	1580.374
2020-06-21T12:00:01	CP_Satellite-2020-06-21-12-00-01.tar.gz	Satellite	DNS Layer	7137.384

Some Future Plans

- Expanding rapid focus capabilities - Ability to quickly run custom measurements working with the community
- Real-time data analysis pipeline and API for easy access into the data
- Collaborating with direct measurement platforms like OONI to combine the power of both worlds

Censored Planet

Thank you!

https://censoredplanet.org

Contact us at
censoredplanet@umich.edu