Detection and Analysis of Censorship Devices

Megan Moore

Capstone Advisor: Professor Christina Pöpper

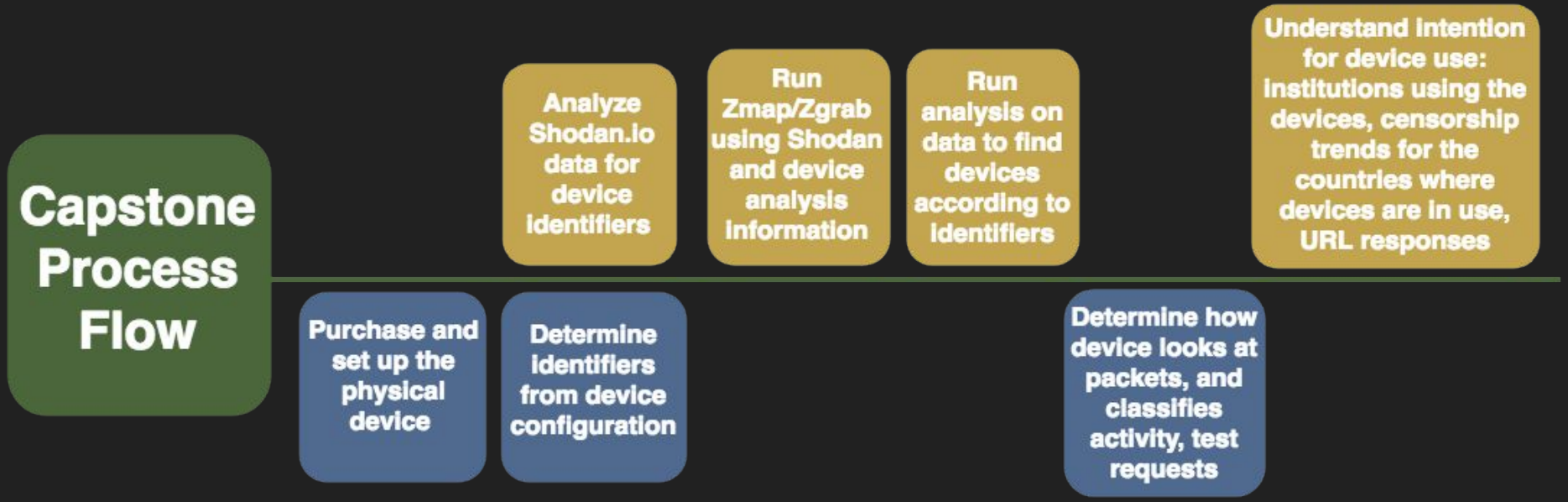
Goals

- Provide a better understanding of how the BlueCoat ProxySG works
- Understand where censorship devices are being used in the world today
- Better understand the content being censored

Previous Works

- Research looking at where devices are being used
  - Marquis-Boire et al. found Blue Coat devices in Iran, Syria and Sudan among other locations (83 total countries found with devices)
  - Marczak et al. fingerprinting and locating FinFisher devices (which are only sold to governments)
  - Dalek et al. found censorship devices in Gulf countries and confirmed that they were censoring content
- Research looking at what content is being censored
  - Xynou et al. and the Open Observatory of Network Interference investigating specific websites and topics that are being censored in a given country

Scans and Global Device Tests



Physical Device Analysis and Tests

Intentions for Device Analysis

- Understand how the device monitors and classifies packets/requests
- Collect Identifiers that will help configure scans and to locate devices in scan data

Device Analysis Findings

- Technique Classification
- Packet Viewing
- Clocking Method
- Default Settings

Classifies Content based on what kind of technique is being used (HTTP, DNS, SMTP, etc.) and depending on the technique, it will determine if that kind of activity will be monitored or not. Additionally, specific topics can be configured for blocking.

Device Analysis Findings

- Technique Classification
- Packet Viewing
- Clocking Method
- Default Settings

Similar to wireshark, the device views packets and notes the size, protocol, content, source and destination information. Additionally it can view encrypted packets

Device Analysis Findings

- Technique Classification
- Packet Viewing
- Clocking Method
- Default Settings

The default clock synchronization is done by pinging the Blue Coat servers, this indicates that there is a “phone home” done by devices, that makes the company aware of devices in use and their location.

Device Analysis Findings

- Technique Classification
- Packet Viewing
- Clocking Method
- Default Settings

The default ftp banner is set to “220 Blue Coat FTP Service” which is broadcasted on the ftp port 21. This can be used to configure a Zgrab scan

Scans

- How Zmap and Zgrab Work
- Scan Configurations
- What Data Zgrab Collects

Zmap - Internet wide scanning and surveying of the IPv4 address space (much faster than nmap)

Zgrab - More verbose and precise data gathering from devices found with Zmap

Scans

- How Zmap and Zgrab Work
- Scan Configurations
- What Data Zgrab Collects

```
zmap -p 21 -B 100M -n 1000000 --output-fields=* | ./zgrab --port 21 --ftp
--output-file=banners-test1.json
```

Port	Banner Type	Zgrab Flag Used	Identifiers
8081 & 80	server	-http="/" & -banner	'BlueCoat-Security-Appliance', 'UserGate Firewall', 'NetCache appliance', 'Traffic Inspector', 'Barracuda'
21	ftp & data	--ftp & --ftp-authtls	'220 Blue Coat FTP Service', 'NetCache', 'barracuda.barracuda'

Scan Data

- How Zmap and Zgrab Work
- Scan Configurations
- What Data Zgrab Collects

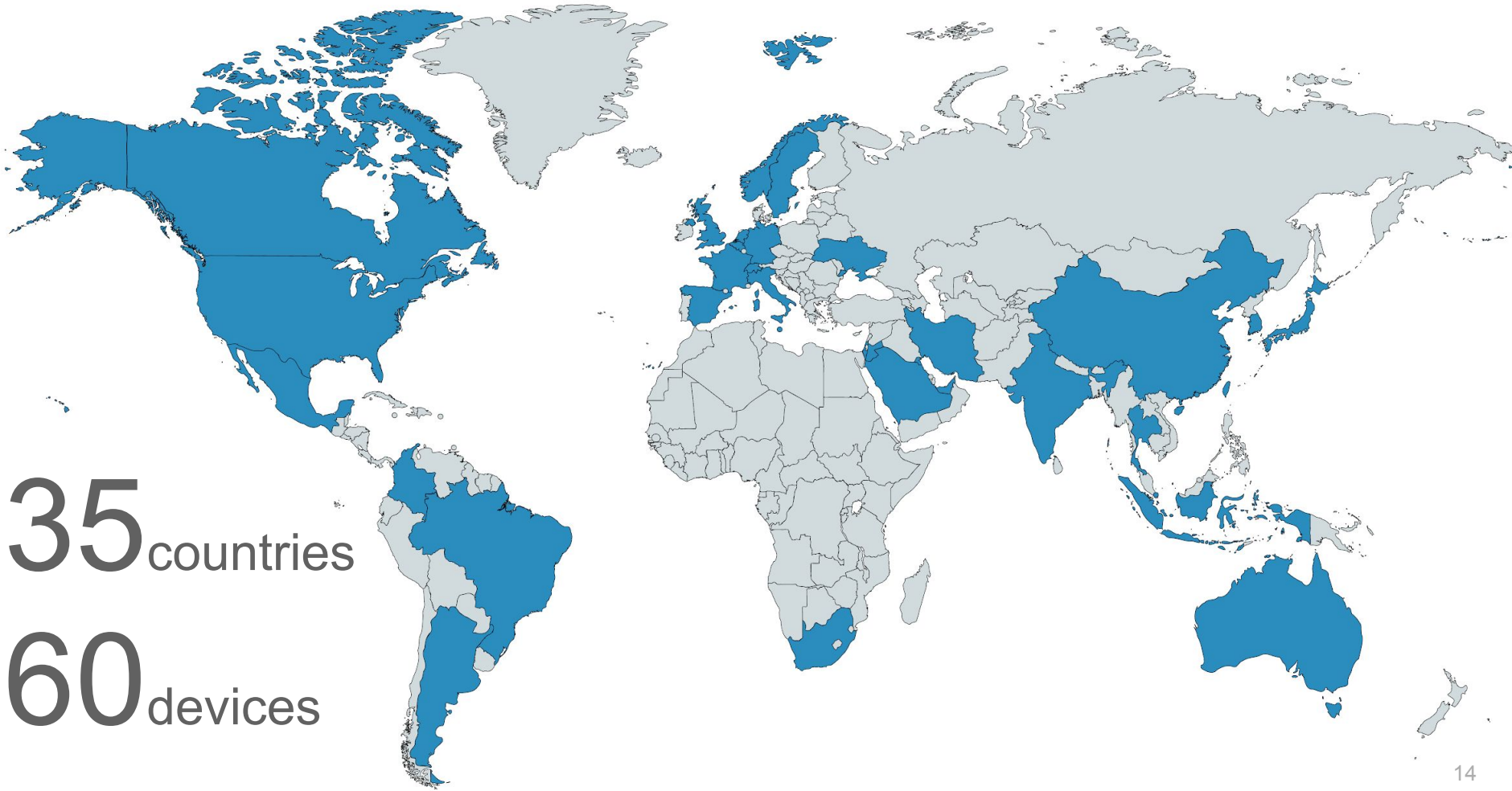
FTP Scan Response

{"ip":"80.231.198.220"', '
"domain":"3704022864"',
'"timestamp":"2018-04-12T19:30:48Z"',
'"data":{"ftp":{"banner":"220 Blue Coat FTP Service\\r\\n"',
'"auth_tls_resp":"500 Syntax error', ' command unrecognized.\\r\\n"',
'"auth_ssl_resp":"500 Syntax error', ' command unrecognized.\\r\\n"}}}

HTTP Scan Response

{"ip":"65.248.13.115"
"domain":"1930295361"
"timestamp":"2018-03-05T06:31:20Z"
"data":{"http":{"response":{"status_line":"401 Authentication Required","status_code":401
"protocol":{"name":"HTTP/1.1","major":1,"minor":1}
"headers":{"cache_control":["no-store"]
"content_type":["text/plain; charset=utf-8"]
"refresh":["0;URL=\"/Secure/Local/console/logout.htm\""]
"server":["BlueCoat-Security-Appliance"]
"set_cookie":["BCSI_MC=699777081:1; path=/"]
"www_authenticate":["Basic realm=\"172.22.0.228\""]}
"body":"Authentication required\r\n"
"body_sha256":"1399edfddf86251ee87b62dd4b23e3e2660a9c8f75d19df3499d33fc45cbff41"
"content_length":-1
"request":{"url":{"scheme":"http"
"host":"65.248.13.115:8081"
"path":"/"}
"method":"GET"
"headers":{"unknown":[{"key":"user_agent"
"value":["Mozilla/5.0 zgrab/0.x"]}
{"key":"accept","value":["*/*"]}]}
"host":"1930295361"}}}}}

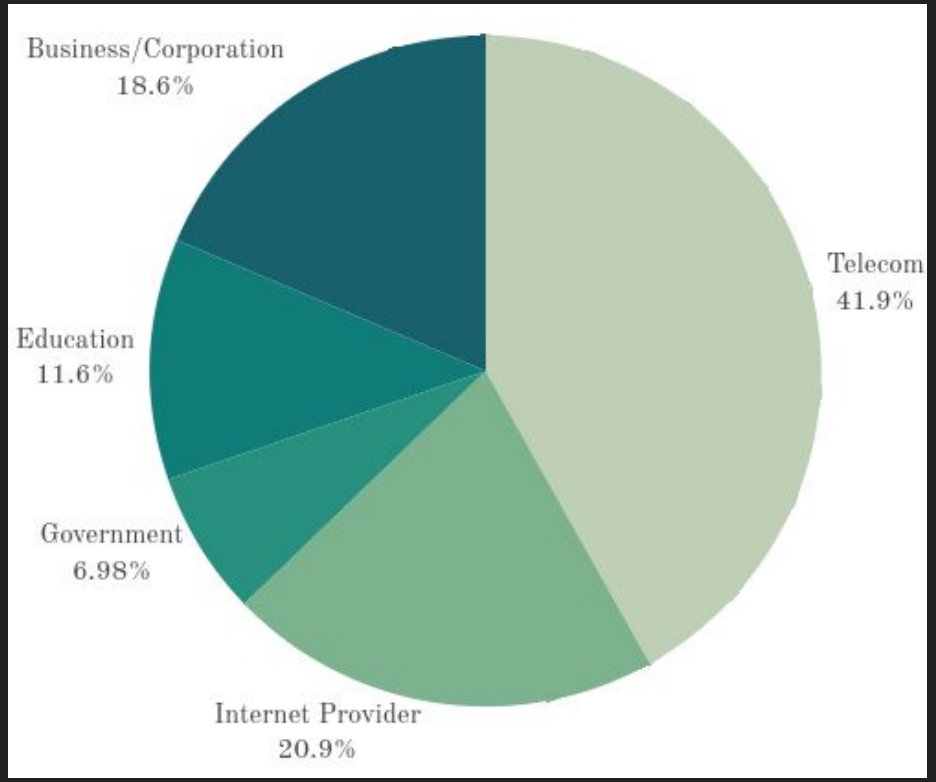
Found
Blue Coat Devices



35 countries

60 devices

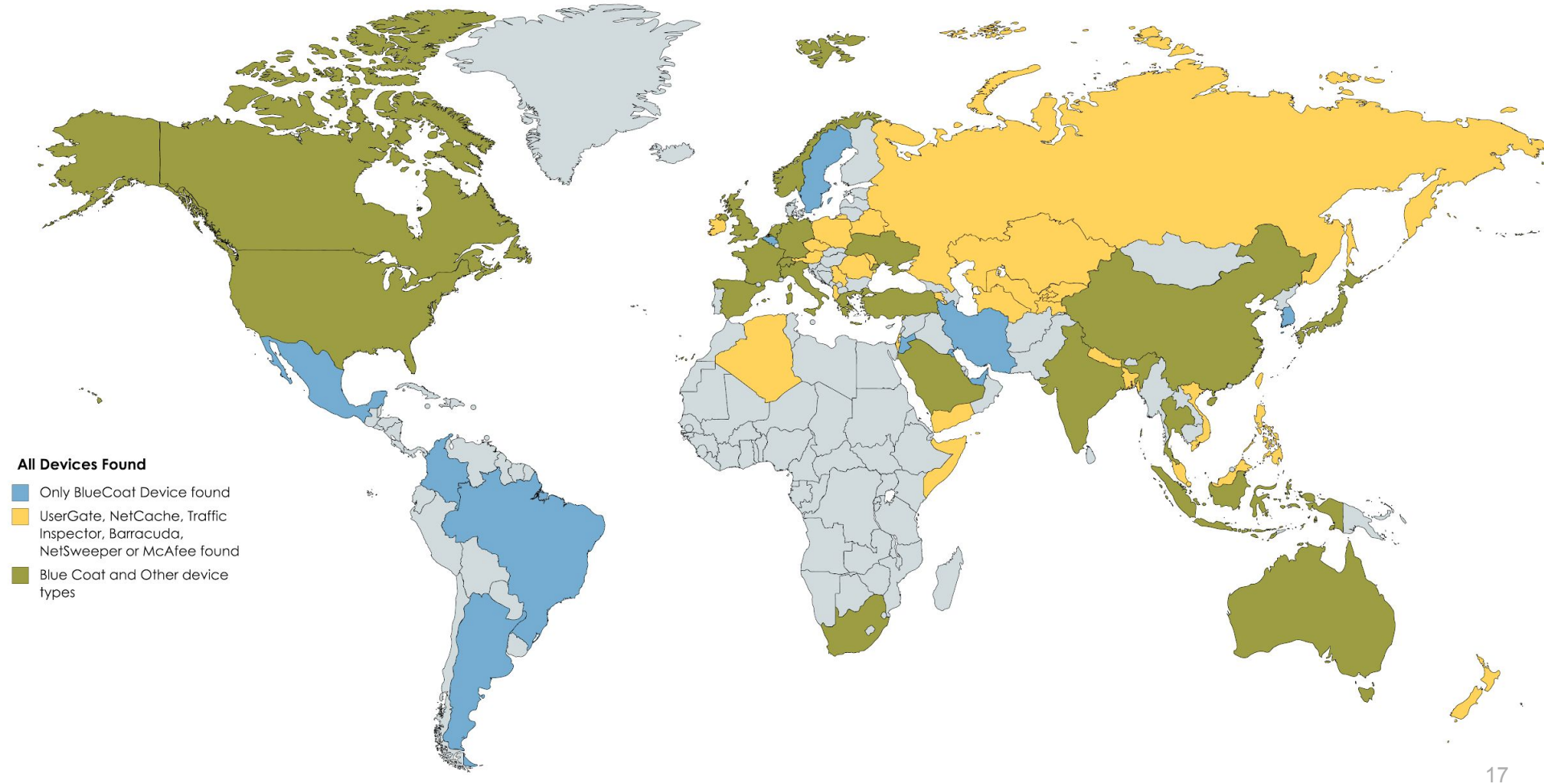
Blue Coat Institutions



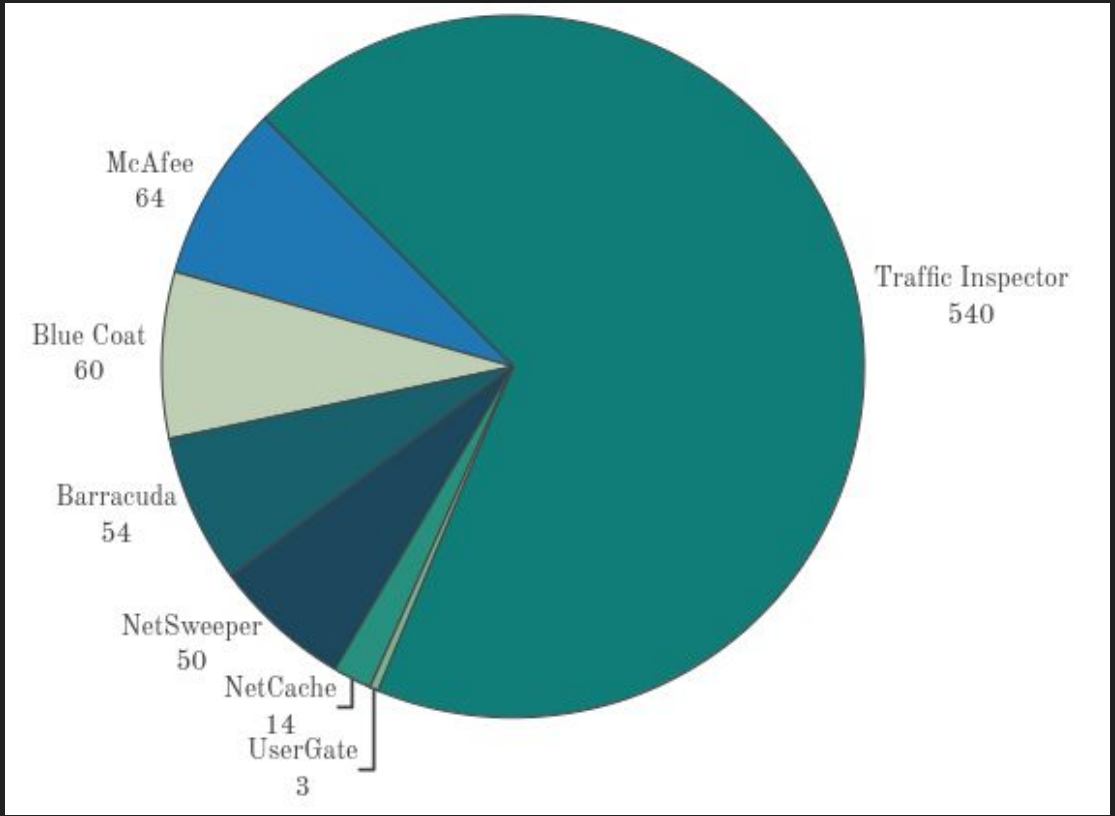
Institutions using Blue Coat include:

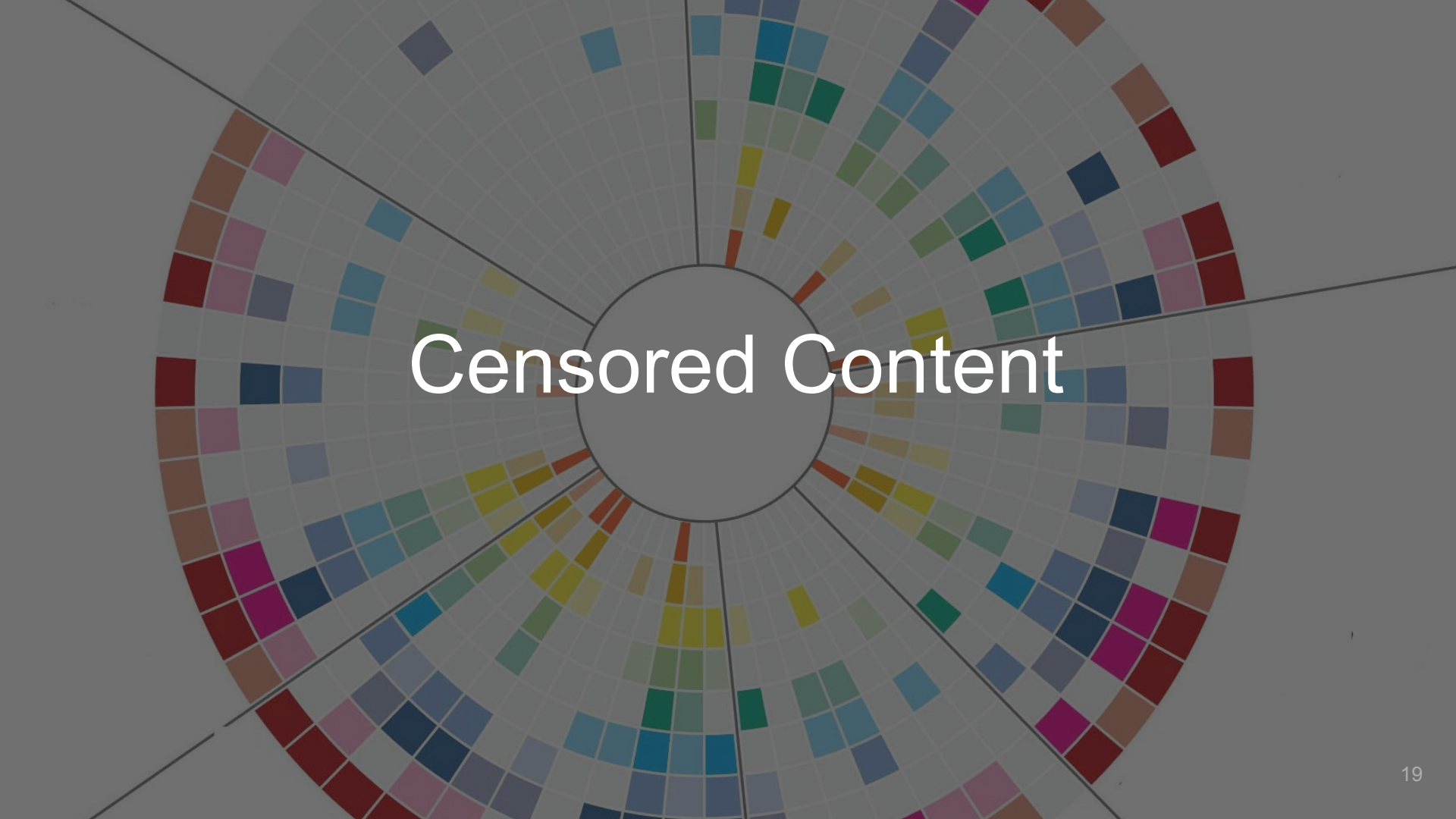
- Royal Hashemite Court - Jordan
- China Telecom - State owned
- Middle East Internet Company Ltd. - Saudi Arabia
- Indonesian Government IT provider
- Florida Public School District


All Found Devices

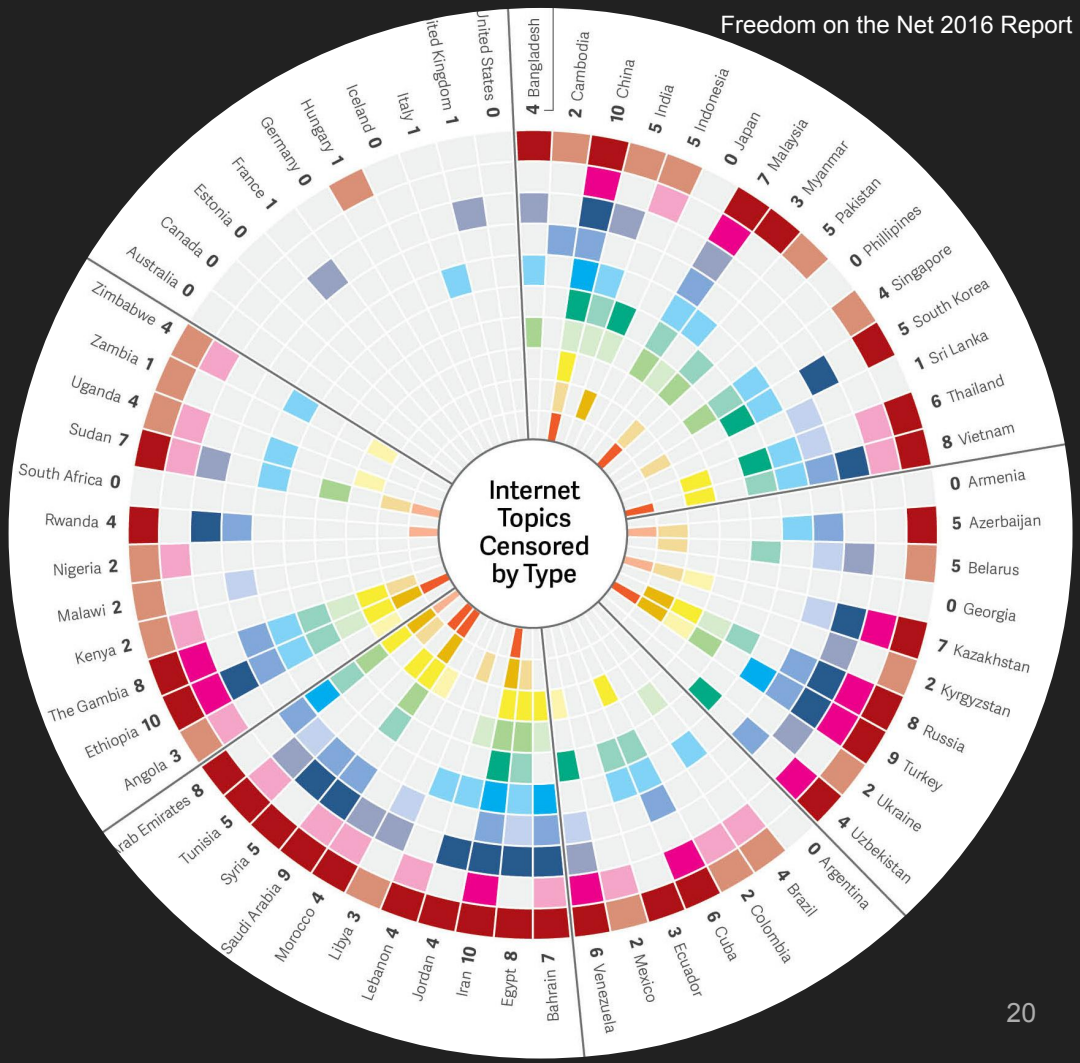


All devices found with Zgrab scan data




Censored Content

Country	# OONI blocked websites	Type of content blocked	Censorship Technique
China	Unknown	10	DNS Hijacking, TCP/IP Blocking
Iran	965	10	DNS Hijacking, Transparent HTTP Proxy
Saudi Arabia	248	9	Transparent HTTP Proxy
India	263	5	null
Indonesia	3	5	Transparent HTTP Proxy
Belgium	165	Gambling (None of the FoTN topics)	Unknown
Korea	141	5	Unknown



Conclusions

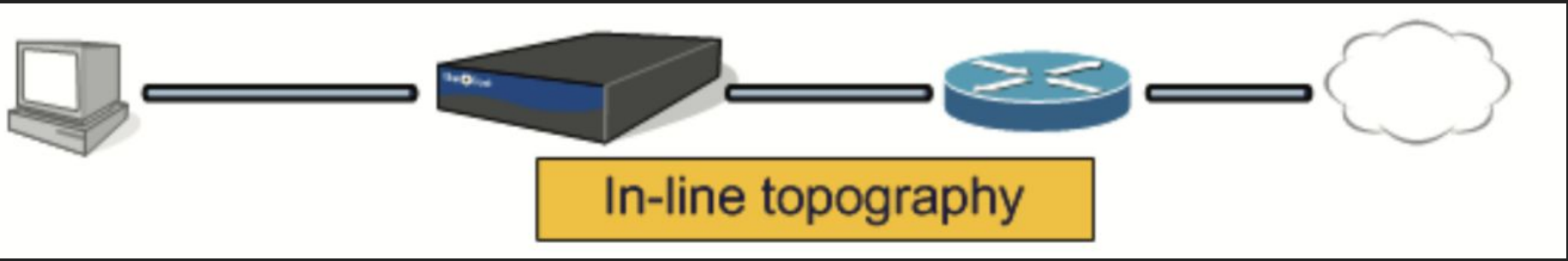
Findings

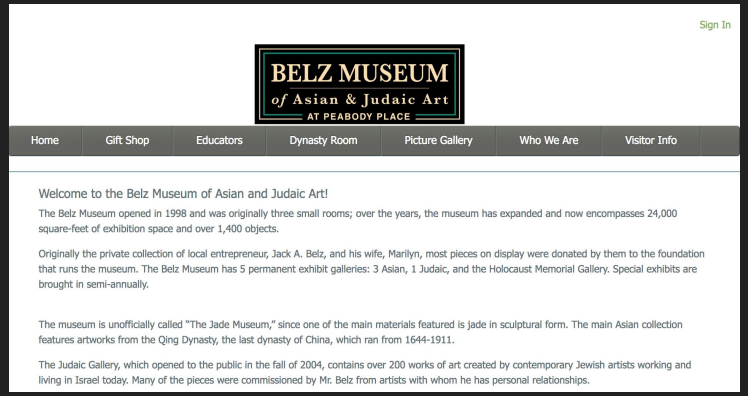
- New identifiers were found on port 21 for ftp banners
- 7 device types were found in 65 countries
- Censorship reports reflected the kind of filtering and blocking that the ProxySG does
- Reports reflected controversial content being censored in these countries including political opposition, criticism of authority and LGBT issues

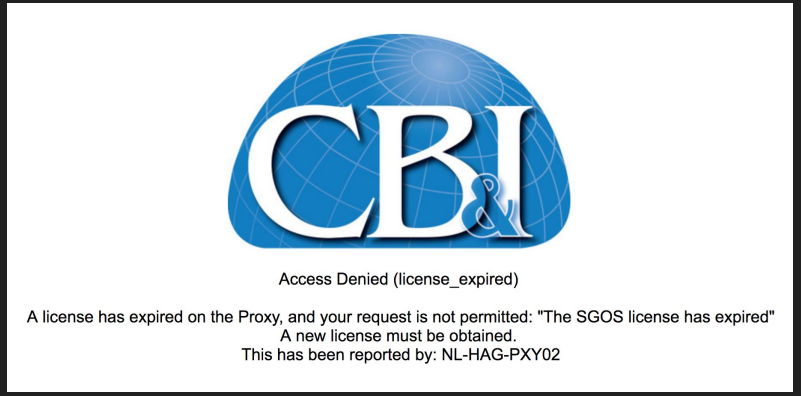
Future Questions

- What is the best way to encapsulate and manipulate packets to circumvent the censorship methods being used on the Blue Coat ProxySG?
- Are there ways to tunnel into monitored networks to test known devices when the networks are at an institutional (non-national level)?
- Can it be verified that Blue Coat has knowledge of the devices by testing if they are contacting the clock synchronization servers?

Questions?


In-line topography


Sign In
BELZ MUSEUM
of Asian & Judaic Art
AT PEABODY PLACE
Home
Gift Shop
Educators
Dynasty Room
Picture Gallery
Who We Are
Visitor Info
Welcome to the Belz Museum of Asian and Judaic Art!
The Belz Museum opened in 1998 and was originally three small rooms; over the years, the museum has expanded and now encompasses 24,000 square-feet of exhibition space and over 1,400 objects.
Originally the private collection of local entrepreneur, Jack A. Belz, and his wife, Marilyn, most pieces on display were donated by them to the foundation that runs the museum. The Belz Museum has 5 permanent exhibit galleries: 3 Asian, 1 Judaic, and the Holocaust Memorial Gallery. Special exhibits are brought in semi-annually.
The museum is unofficially called "The Jade Museum," since one of the main materials featured is jade in sculptural form. The main Asian collection features artworks from the Qing Dynasty, the last dynasty of China, which ran from 1644-1911.
The Judaic Gallery, which opened to the public in the fall of 2004, contains over 200 works of art created by contemporary Jewish artists working and living in Israel today. Many of the pieces were commissioned by Mr. Belz from artists with whom he has personal relationships.


CB&I
Access Denied (license_expired)
A license has expired on the Proxy, and your request is not permitted: "The SGOS license has expired"
A new license must be obtained.
This has been reported by: NL-HAG-PXY02


ANTELOPE VALLEY
HOSPITAL
A facility of Antelope Valley Healthcare District
About
Services
Patients
Visitors
News & Events
Antelope Valley Healthcare District improves the quality of health in our community through research, education and innovation.


88.85.228.90
Apps
Albert
Classes
Email
LinkedIn
weSTEM
CitizenLab
GitHub
Request Error (invalid_request)
Your request could not be processed. Request could not be handled
This could be caused by a misconfiguration, or possibly a malformed request.
For assistance, contact your network support team.
Your request was categorized by Blue Coat Web Filter as 'Suspicious'.
If you wish to question or dispute this result, please click here.

Blue Coat	User Gate	NetCache	Traffic Inspector	Barracuda	McAfee	NetSweeper
Spain	Russia	Saudi Arabia	Russia	Greece	Vietnam	US
Norway		South Africa	Kazakhstan	United States	Phillippines	India
UAE		Israel	Belarus	Turkey	Indonesia	Liechtenstein
South Africa			Kyrgyzstan	Norway	Malaysia	Canada
Thailand			Tajikistan	China	US	Ireland
Netherlands			Czech Republic	France	Bangladesh	UK
Germany			Ukraine	Russia	Greece	South Africa
United States			Moldova	Kazakhstan	Turkey	Somalia
Canada			Uzbekistan	Canada	Germany	New Zealand
Hong Kong			Armenia	Spain	SIngapore	Yemen
Israel			Turkmenistan		Serbia	Indonesia
France			Germany		Romania	Australia
India					Israel	Albania
United Kingdom					Czech Republic	
China					Switzerland	
Saudi Arabia					Italy	
South Korea					Austria	
Japan					Netherlands	
Belgium					France	
Argentina					Poland	
Mexico					India	
Indonesia					Taiwan	
Singapore					Korea	
Malta					Thailand	
Australia					Nepal	
Switzerland					Australia	
Kuwait						
Iran						
Sweden						
Italy						
Taiwan						
Colombia						
Ukraine						
Jordan						
Brazil						

Country	# OONI blocked websites	Type of content blocked	Found Censorship Techniques
China	Unknown	10	DNS Hijacking, TCP/IP Blocking
Iran	965	10	DNS Hijacking, Transparent HTTP Proxy
Saudi Arabia	248	9 (not satire)	Transparent HTTP Proxy
India	263	5 (Criticism of Authority, Conflict, Satire, Social Commentary, Blasphemy)	null
Indonesia	3	5(Criticism of Authority, Corruption, Social Commentary, Blasphemy, LGBTI issues)	Transparent HTTP Proxy
Belgium	165	Gambling and Casinos (None of the FoTN topics)	Unknown
Korea	141	5 (Criticism of Authority, Conflict, Satire, Social Commentary, LGBTI issues)	Unknown