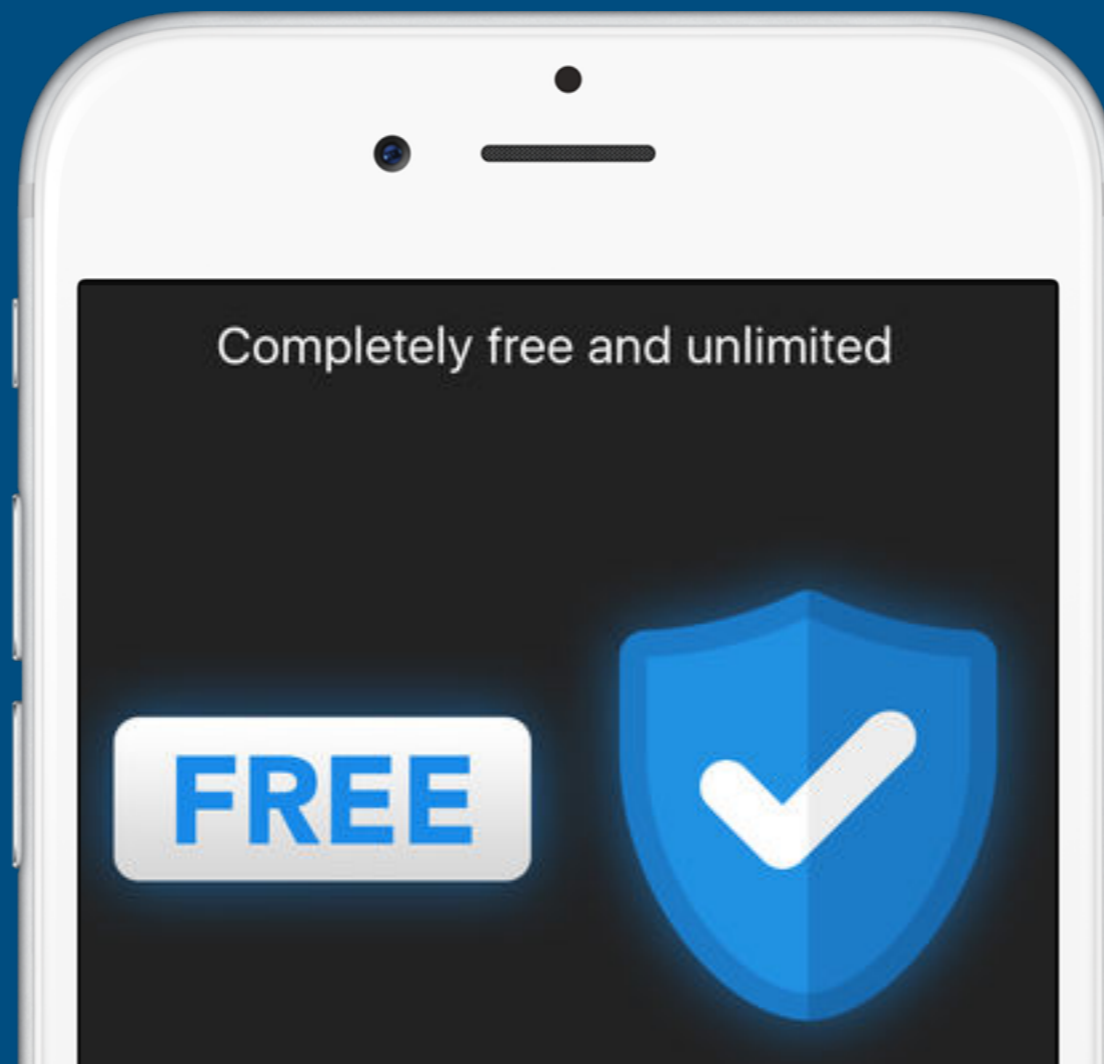


Mobile SSL Interception in the Wild

Where, how, and why?



Alban Diquet
Thomas Sileo
Data Theorem

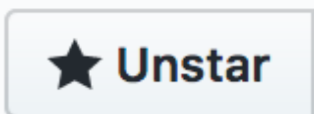
BlueHat 2017

Agenda

- Data collection methodology
- Data set and analysis of forged SSL certificates
- Results of the analysis
- Conclusion

Data Collection Methodology

TrustKit

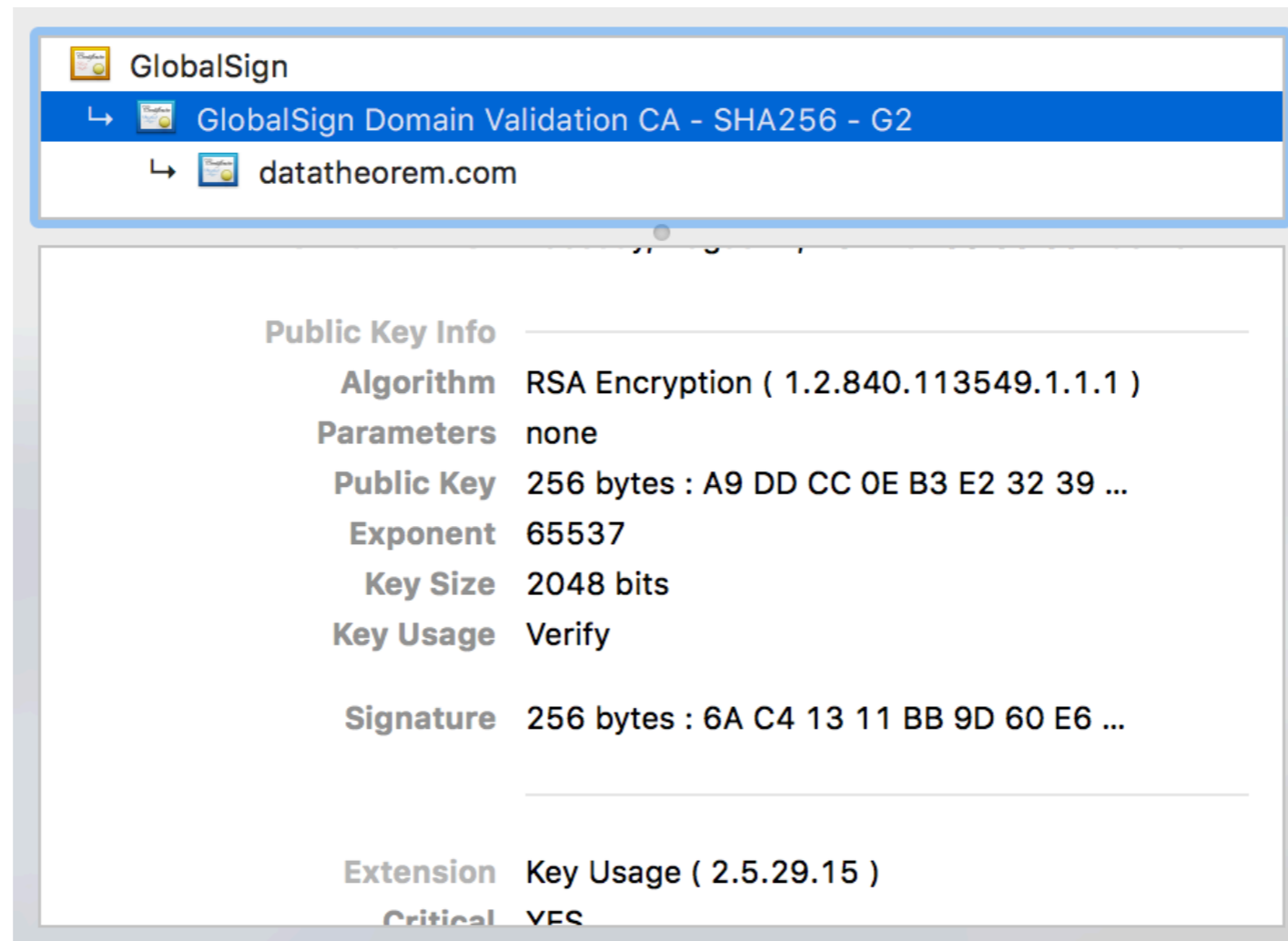
- Open-source library for SSL reporting and SSL pinning
 - Released for iOS in 2015 and for Android earlier this year
 - <https://github.com/datatheorem/TrustKit>  719
- Makes it easy to monitor and improve the security of the app's network connections

SSL Pinning

- Hardcode in the app the SSL public key(s) to be expected to be used by the app's server(s)

SSL Pinning

- Hardcode in the app the SSL public key(s) to be expected to be used by the app's server(s)

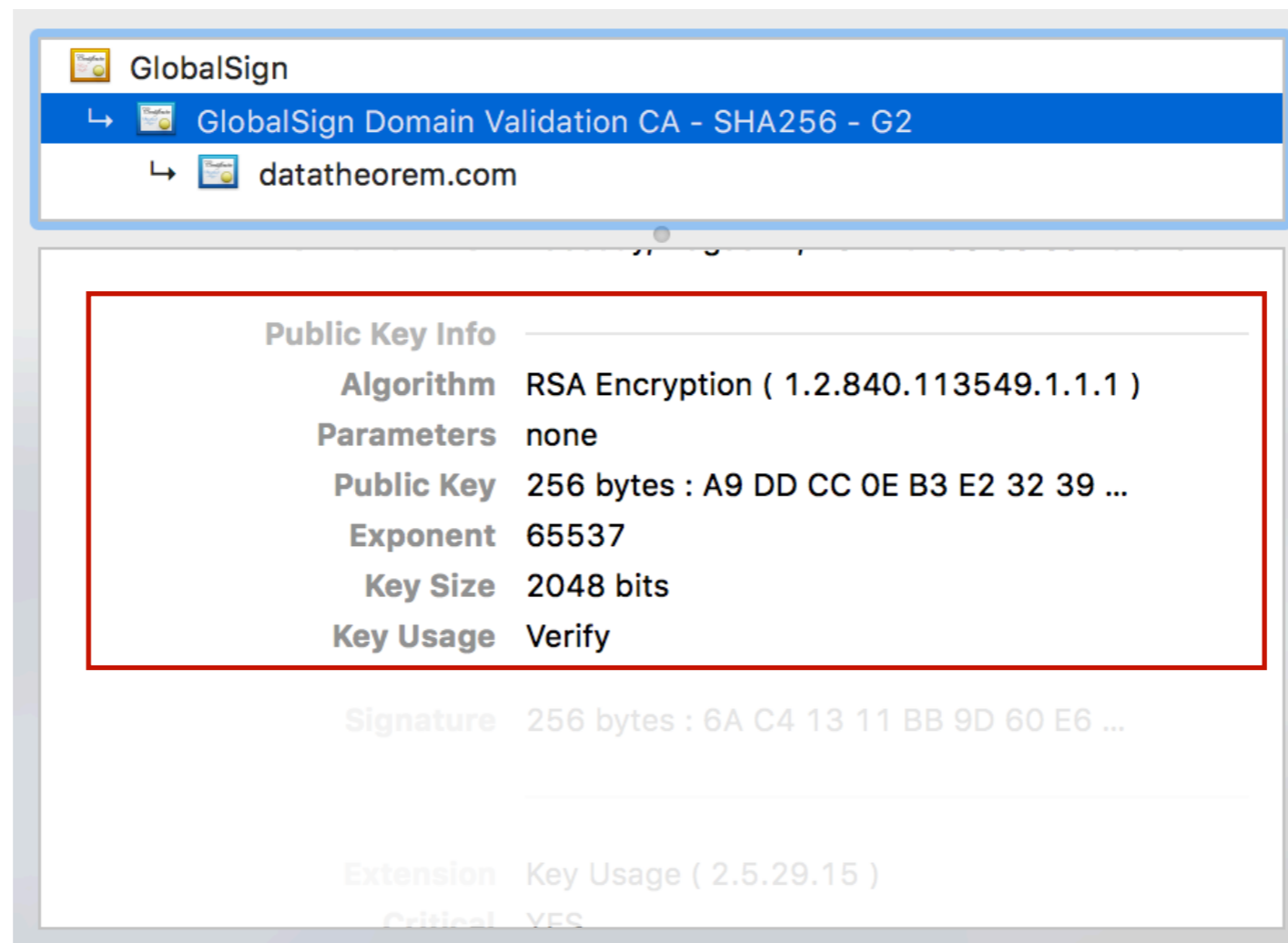


The screenshot shows a browser window with the address bar displaying "GlobalSign Domain Validation CA - SHA256 - G2" and "datatheorem.com". Below the address bar, the "Public Key Info" section is expanded, showing the following details:

Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : A9 DD CC 0E B3 E2 32 39 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 6A C4 13 11 BB 9D 60 E6 ...
Extension	Key Usage (2.5.29.15)
Critical	YES

SSL Pinning

- Hardcode in the app the SSL public key(s) to be expected to be used by the app's server(s)



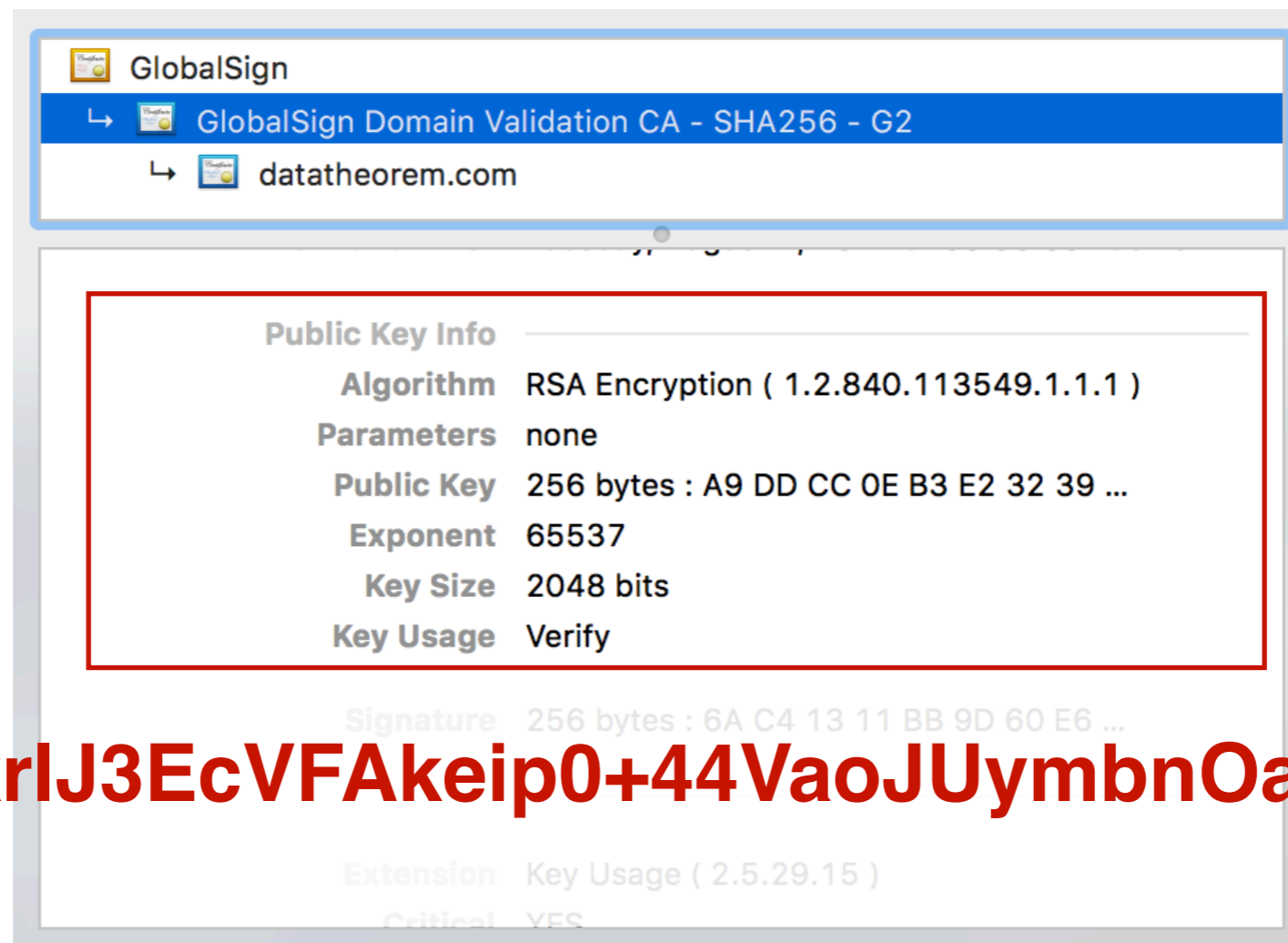
The screenshot shows a browser window with the address bar displaying "GlobalSign Domain Validation CA - SHA256 - G2" and "datatheorem.com". Below the address bar, the "Public Key Info" section is highlighted with a red border. The details listed are:

Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : A9 DD CC 0E B3 E2 32 39 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Verify

Below the highlighted section, the "Signature" field is visible with the value "256 bytes : 6A C4 13 11 BB 9D 60 E6 ...". At the bottom, the "Extension" field is visible with the value "Key Usage (2.5.29.15)" and "Critical YES".

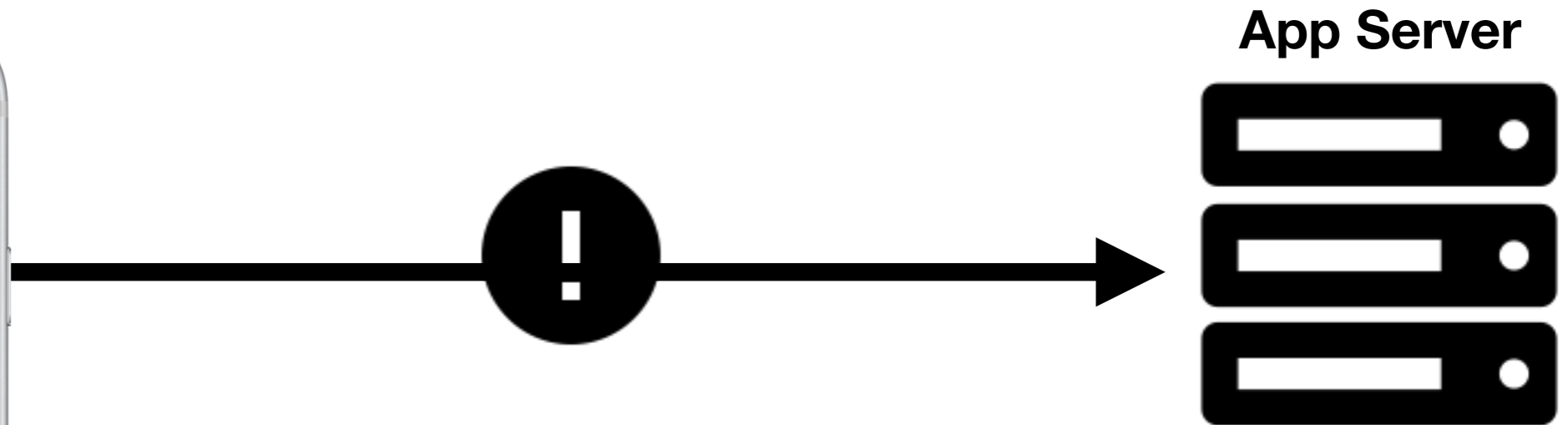
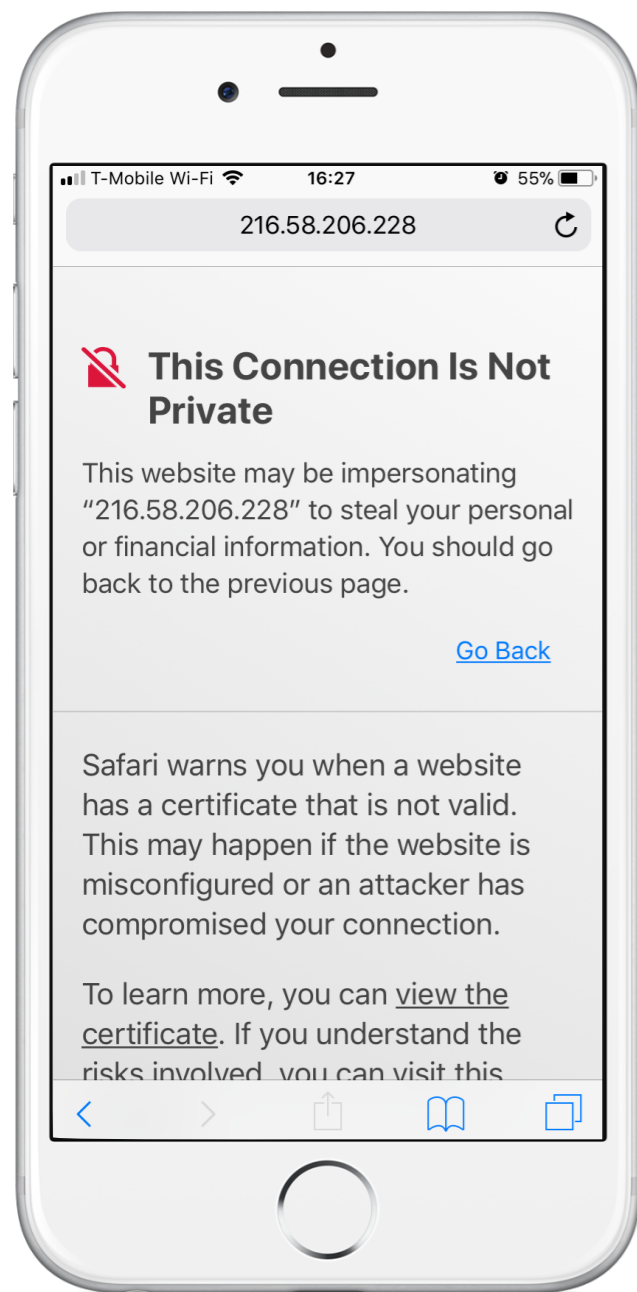
SSL Pinning

- Hardcode in the app the SSL public key(s) to be expected to be used by the app's server(s)



ICppFqbkrlJ3EcVFAkeip0+44VaoJUymbnOaEUk7tEU=

SSL Reporting



- Send a report whenever an SSL error occurred
- Default/OS SSL validation error
 - Name mismatch, expired certificate, untrusted CA, etc.
- TrustKit Pinning validation error
 - Pinned SSL key not found in the server's chain

SSL Reporting

```
{
  "app-bundle-id": "com.datatheorem.testtrustkit",
  "app-version": "1.2",
  "app-vendor-id": "599F9C00-92DC-4B5C-9464-7971F01F8370",
  "app-platform": "IOS",
  "trustkit-version": "1.5.3",
  "hostname": "www.datatheorem.com",
  "port": 443,
  "noted-hostname": "datatheorem.com",
  "include-subdomains": true,
  "enforce-pinning": true,
  "validated-certificate-chain": [
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----"
  ],
  "date-time": "2015-06-08T01:58:05Z",
  "known-pins": [
    "pin-sha256=\"rFjc3wG7lTZe43zeYTvPq8k4xdDEutCmIhI5dn4oCeE=\"",
    "pin-sha256=\"TQEtdMbmwFgYUifM4LDF+xgEtd0z69mPGmkp014d6ZY=\""
  ],
  "validation-result": 1
}
```

SSL Reporting

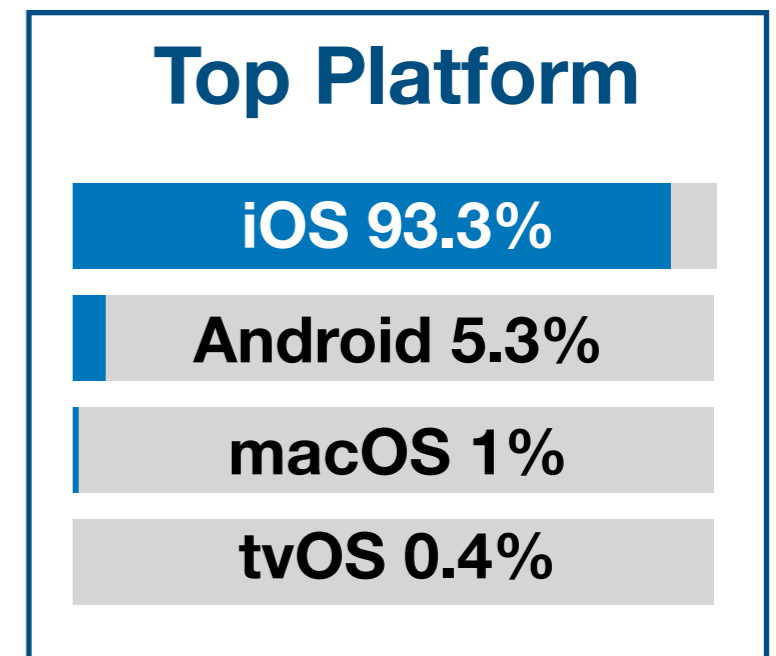
- TrustKit can be configured to send the reports to any domain
- Data Theorem hosts one for free that developers can leverage
 - Dashboard to see trends and inspect individual reports
 - Notifications for when something unexpected happens
 - Suspicious actor, spike in reports, etc.

Demo

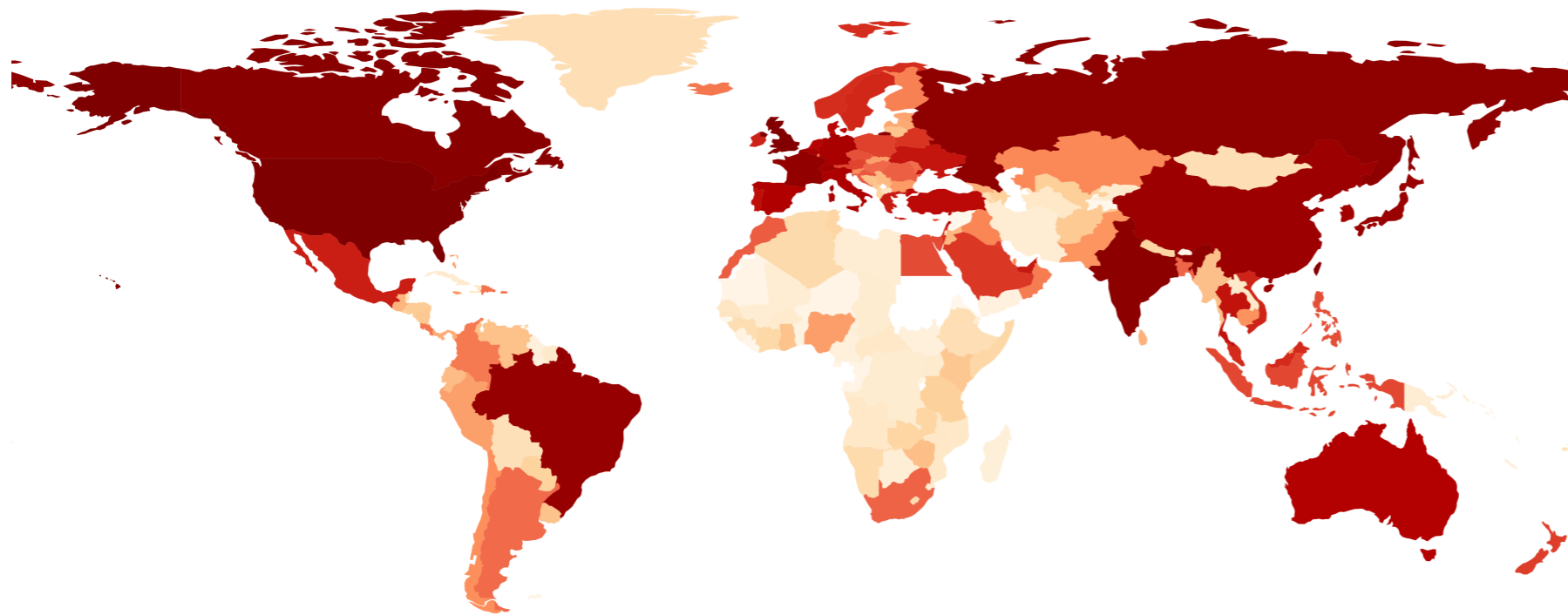
Data Set and Report Classification

The Data Set

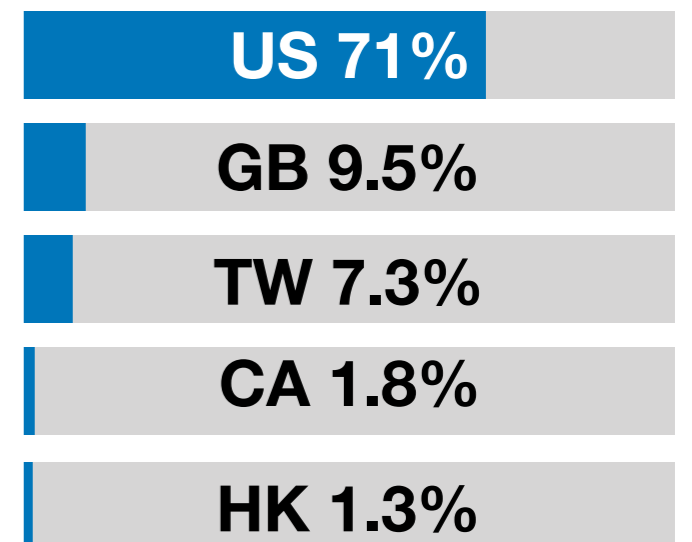
- From nearly 2 000 different apps
 - Banking
 - Shopping
 - Music/streaming
 - News



The Data Set

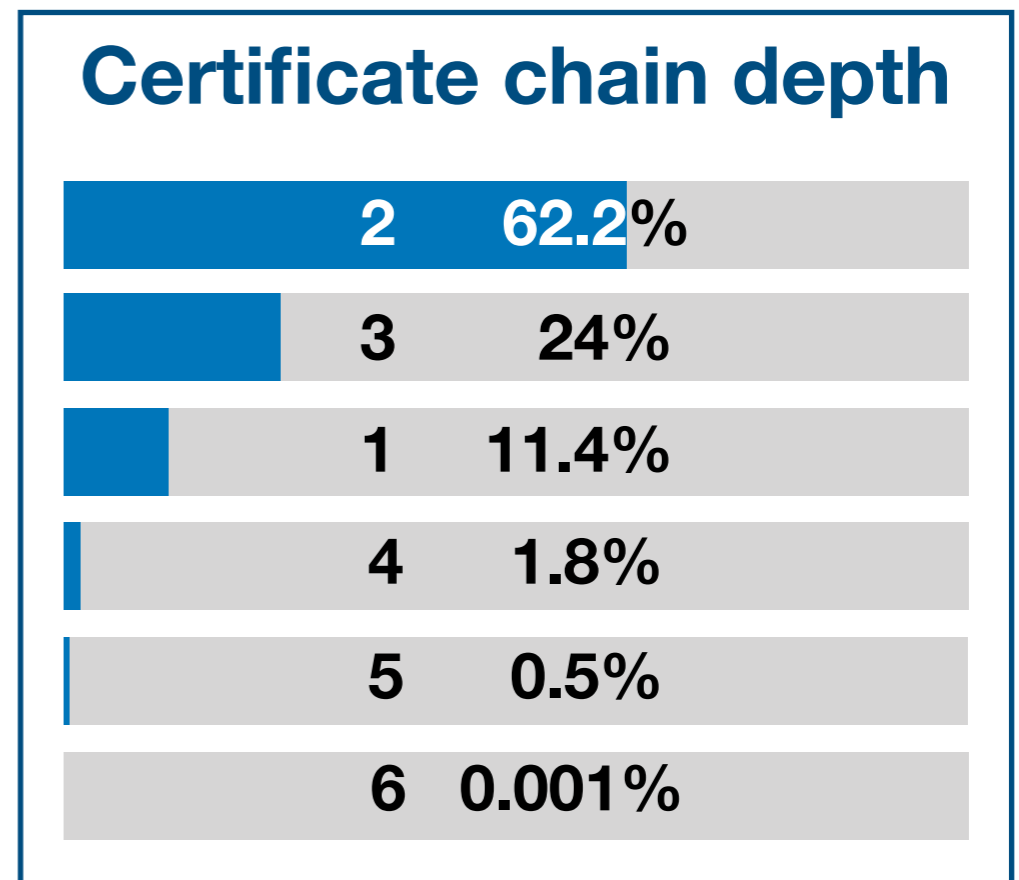


Top Countries



The Data Set

- 3.3 million unique certificate chains
- 78% of the certificates matched the hostname
 - Actual interception attempts



Report Classification

- Use different heuristics to try to find the root cause
 - By looking at the content of the report, mainly the certificate chain
- Save some metadata along with the server date
- Contact the server for the hostname that was in the report, to fetch its “real” certificate chain

Report Classification

- Perform default SSL validation on the certificate chain
- Leverage a set of rules that can target:
 - A specific certificate or a specific public key
 - Any certificate fields (Common Name, etc.)

Report Classification

```
dev_tools:
  PortSwigger:
    root:
      - 'PortSwigger CA'
  Fiddler:
    root:
      - 'DO_NOT_TRUST_FiddlerRoot'
  Charles Proxy:
    root:
      - '!regex ^Charles Proxy Custom Root Certificate \.(built on .+\)$'
      - '!regex ^Charles Proxy CA \.(.+)\$'
  mitmproxy:
    root:
      - 'mitmproxy'
  [...]
```

Report Classification

```
{  
  "app-bundle-id": "com.datatheorem.corporate_proxy",  
  "hostname": "www.datatheorem.com",  
  "validated-certificate-chain": [  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----"  
  ],  
  "date-time": "2017-03-03T21:27:12Z",  
  "validation-result": 1,  
  "...": "...",  
}
```

raw report

Report Classification

```
{  
  "app-bundle-id": "com.datatheorem.corporate_proxy",  
  "hostname": "www.datatheorem.com",  
  "validated-certificate-chain": [  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----"  
  ],  
  "date-time": "2017-03-03T21:27:12Z",  
  "validation-result": 1,  
  "...": "...",  
}
```

raw report

Report Classification

```
{  
  "app-bundle-id": "com.datatheorem.corporate_proxy",  
  "hostname": "www.datatheorem.com",  
  "validated-certificate-chain": [  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----"  
  ],  
  "date-time": "2017-03-03T21:27:12Z",  
  "validation-result": 1,  
  "...": "...",  
  "...": [...],  
  "server_certificate_chain": [  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----"  
  ],  
  "received_at": "2017-03-03T21:27:25Z",  
}
```

raw report


report metadata

Report Classification

```
{  
  "app-bundle-id": "com.datatheorem.corporate_proxy",  
  "hostname": "www.datatheorem.com",  
  "validated-certificate-chain": [  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----"  
  ],  
  "date-time": "2017-03-03T21:27:12Z",  
  "validation-result": 1,  
  "...": "...",  
  "...": [...],  
  "server_certificate_chain": [  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...] \n-----END CERTIFICATE-----"  
  ],  
  "received_at": "2017-03-03T21:27:25Z",  
}
```

raw report

report metadata



Report Classification

```
{  
  "app-bundle-id": "com.datatheorem.corporate_proxy",  
  "hostname": "www.datatheorem.com",  
  "validated-certificate-chain": [  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----",  
    "-----BEGIN CERTIFICATE-----\n[...]\n-----END CERTIFICATE-----"  
  ],  
  "date-time": "2017-03-03T21:27:12Z",  
  "validation-result": 1,  
  "...": "...",  
}
```

raw report



```
{  
  "certificate_chain_infos": [  
    {"issuer":  
      {"common_name": "Fortigate CA",  
        "...": [...],  
      }  
    }  
  ]  
}
```

certificate chain info

Report Classification

```
{  
  "certificate_chain_infos": [  
    {"issuer":  
      {"common_name": "Fortigate CA",  
        "...": [...],
```

certificate chain info

```
corporate_appliance:  
  Cisco Umbrella:  
    url: 'https://umbrella.cisco.com/'  
    root:  
      - 'Cisco Umbrella Primary SubCA'  
  [...]
```

classifier ruleset

flagged for manual review

Report Classification

```
{  
  "certificate_chain_infos": [  
    {"issuer":  
      {"common_name": "Fortigate CA",  
        "...": [...],
```

certificate chain info

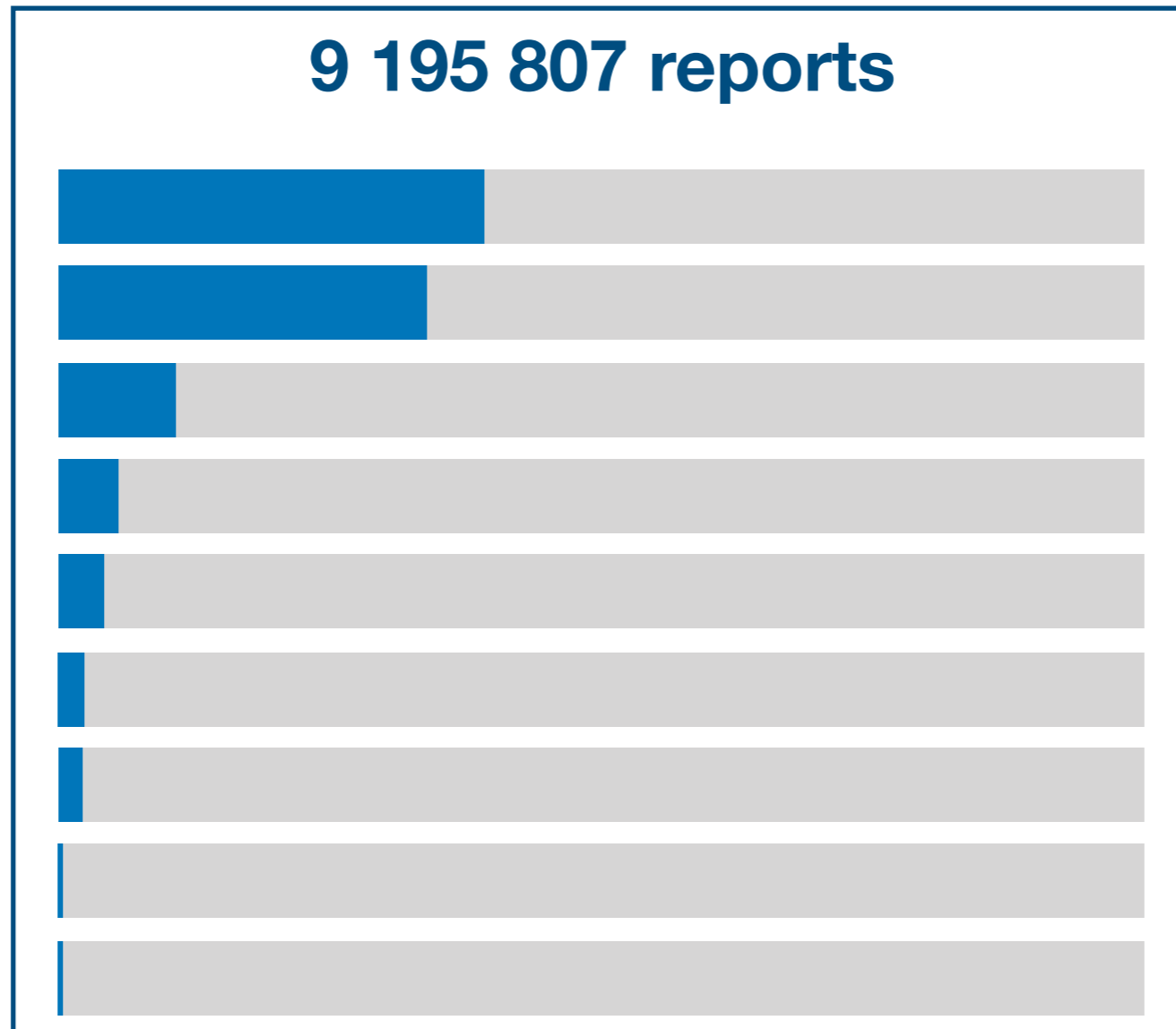
```
corporate_appliance:  
  [...]  
  Fortinet:  
    leaf:  
      - !IssuerCommonName 'FortiGate CA'  
  [...]
```

classifier ruleset

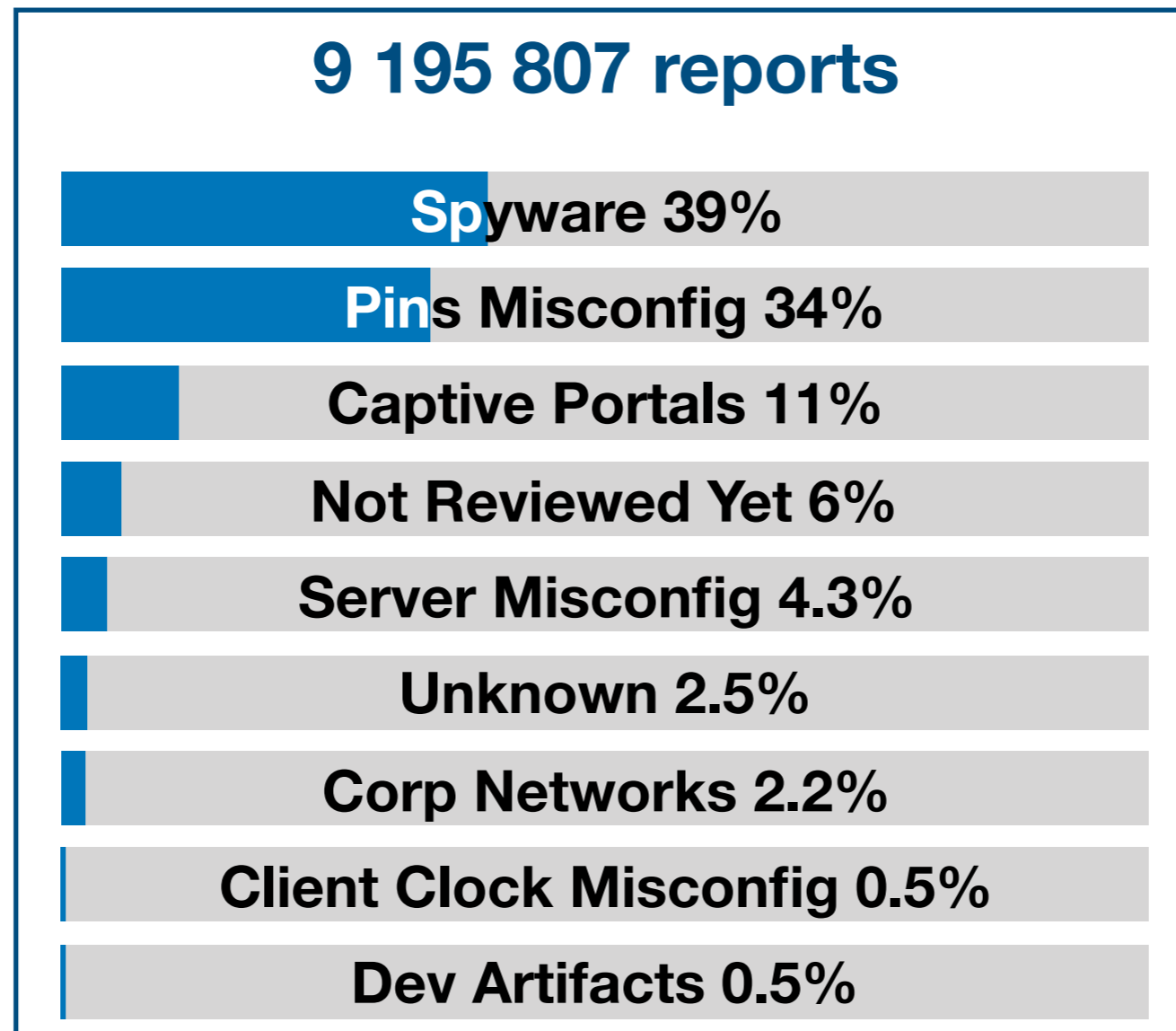
corporate_appliance / Fortinet

Results of the Analysis

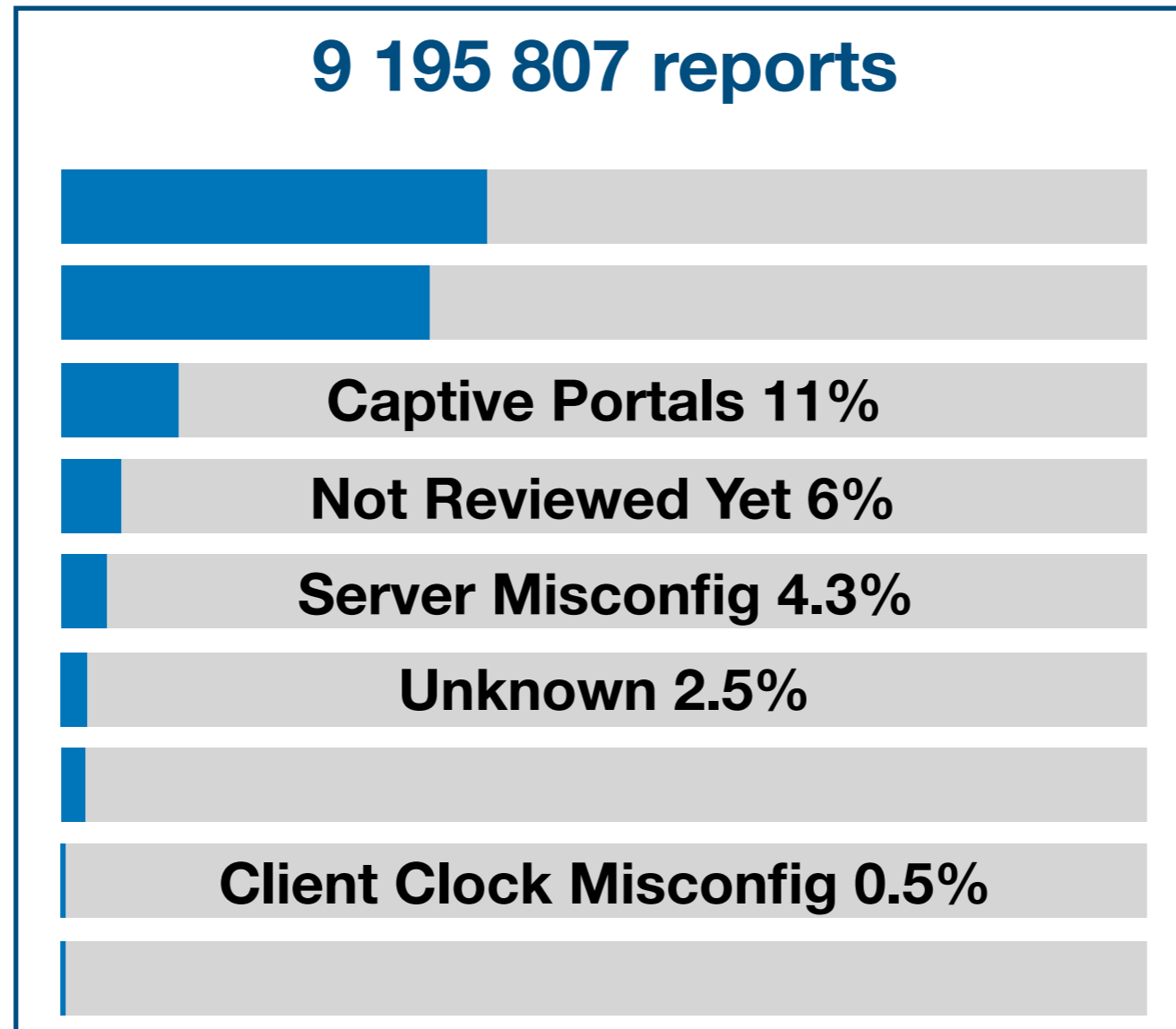
Classification Categories



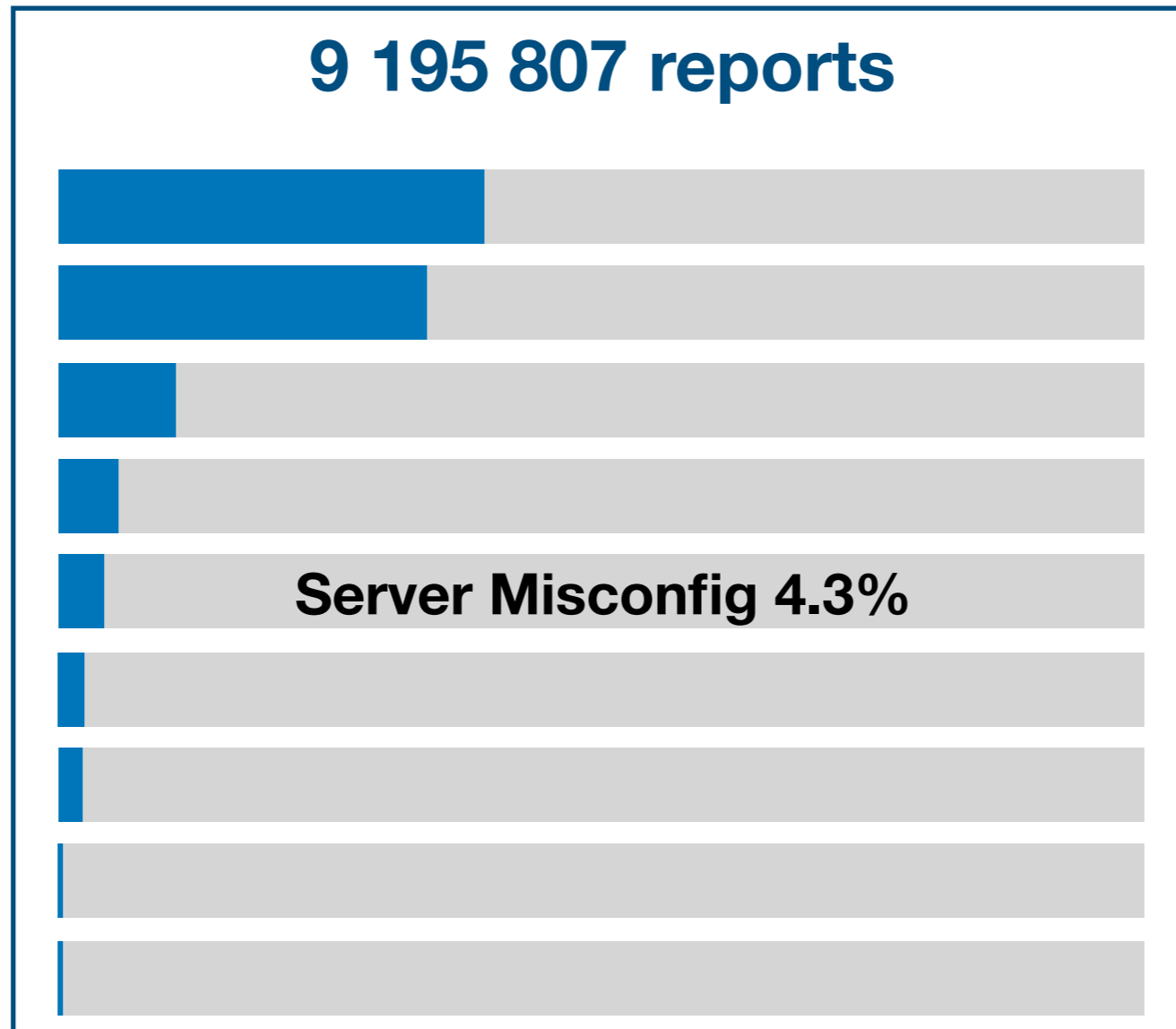
Classification Categories



Non-Mitm Categories



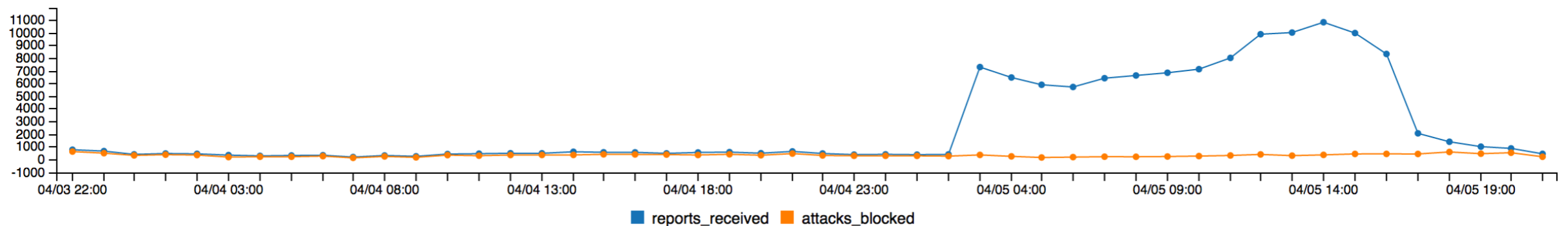
Non-Mitm Categories



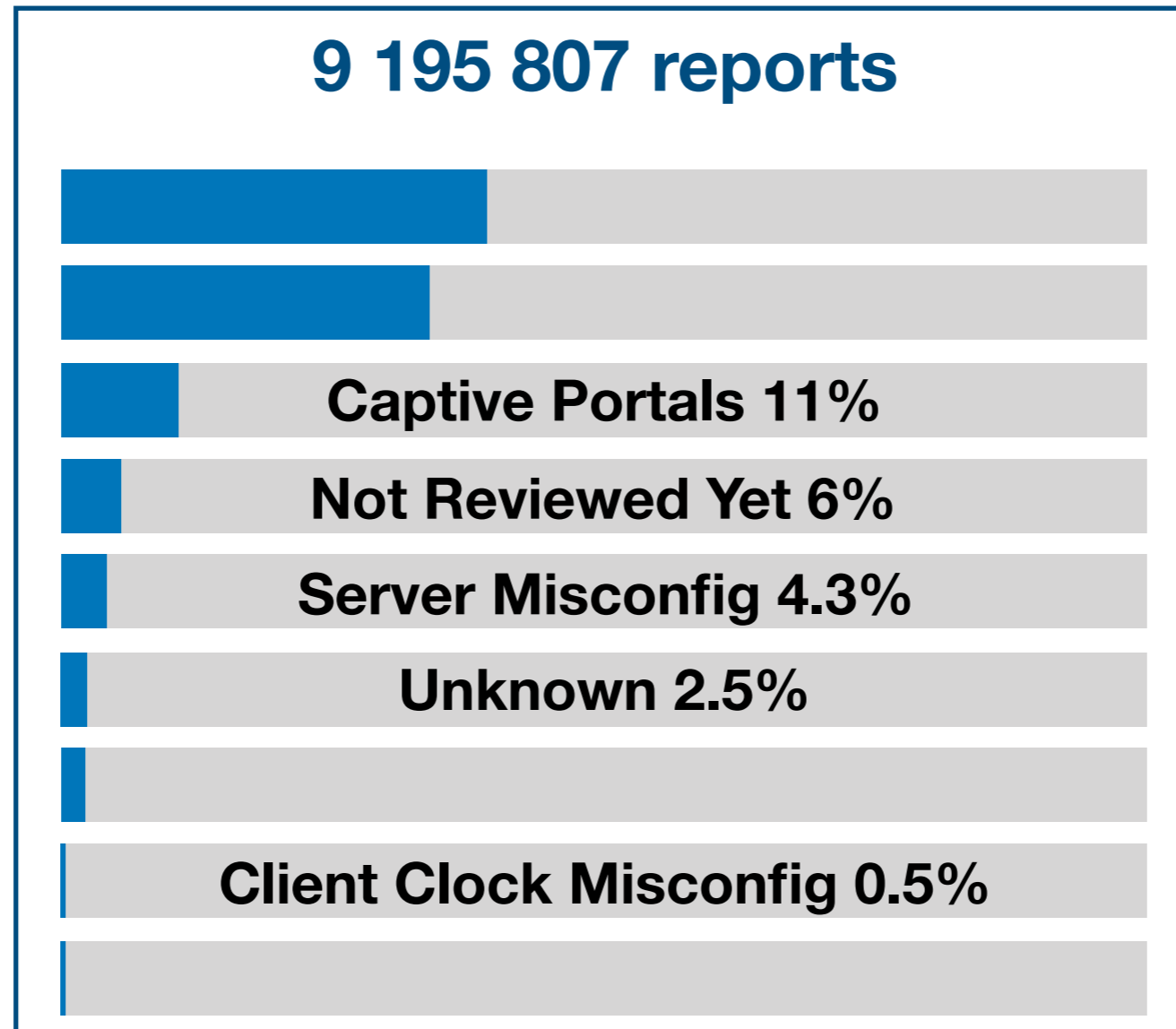
Server Misconfiguration

- Category for servers with expired SSL certificates
- Huge spike of report when a certificate deployed in production expired:

Last 48 hours 0.74 reports/sec on average with peak at 2.99 reports/sec



Non-Mitm Categories

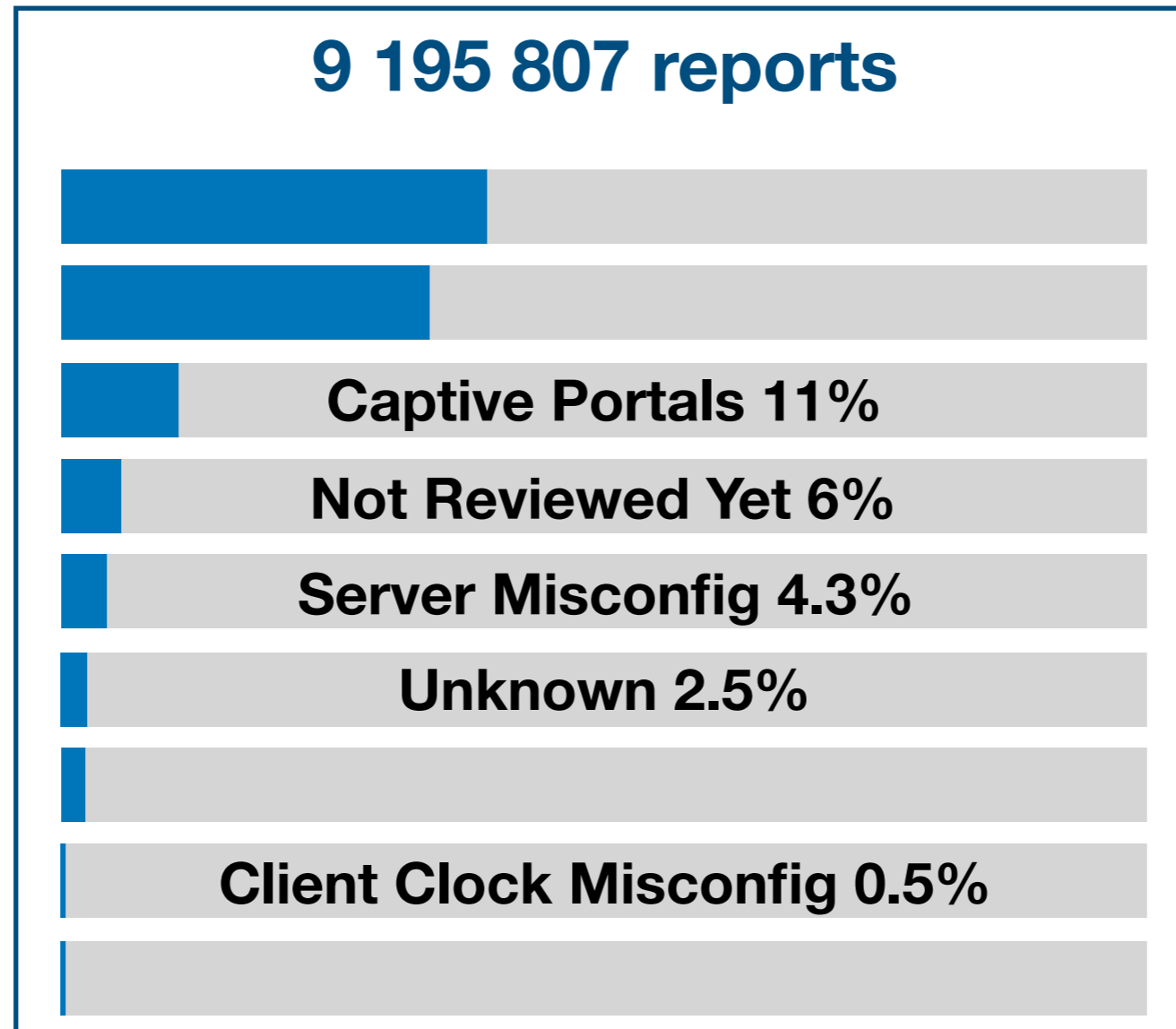


Previous Work

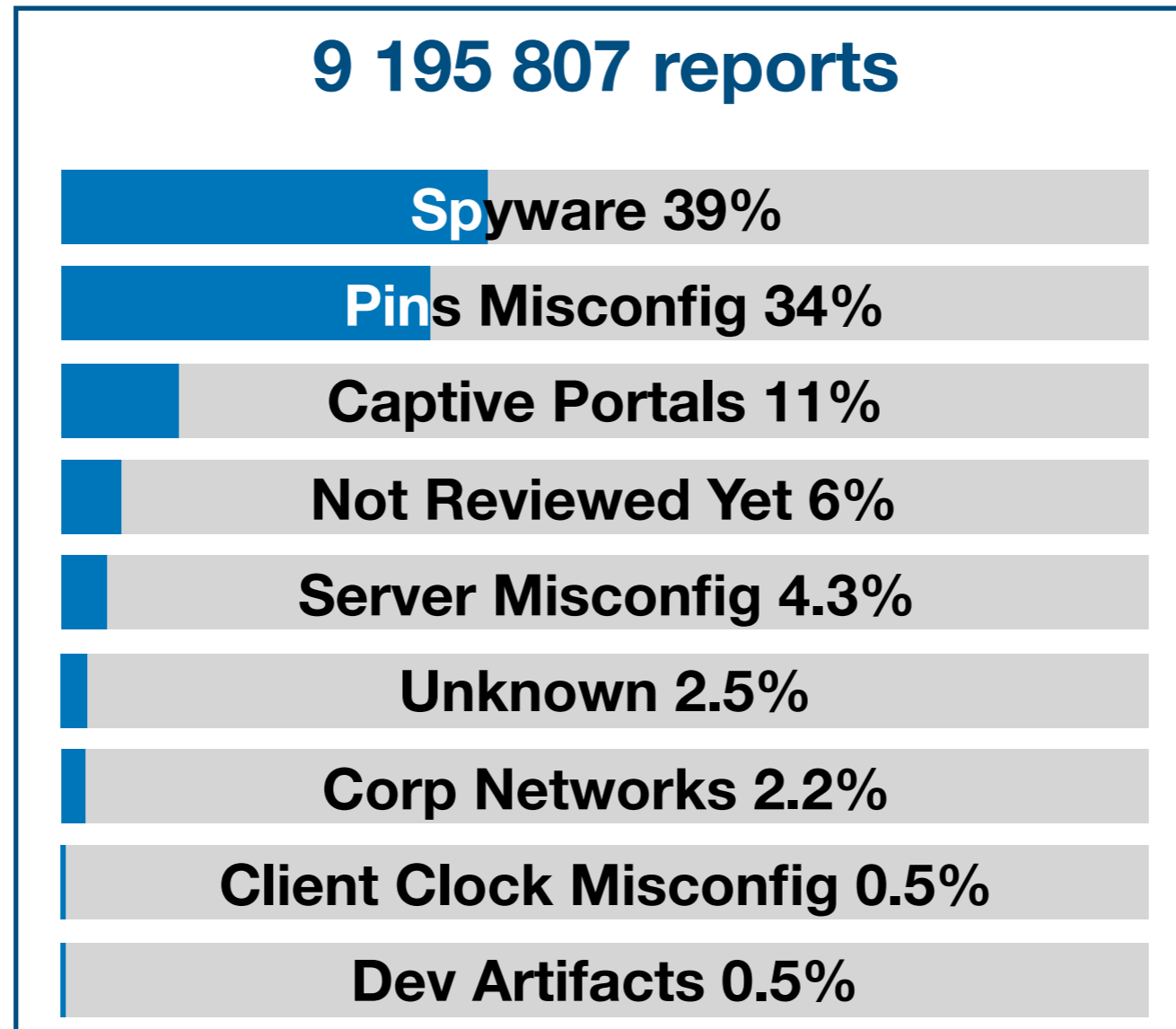
- Data from Chrome desktop for google.com:

GOOGLE.COM	Client clock misconfiguration	61%
	Captive portal	13%
	Security products	13%
	ISP misconfiguration	3%
	Fiddler Core	3%
	Anti-virus misconfiguration	3%
	Router misconfiguration	2%
	Unknown	2%

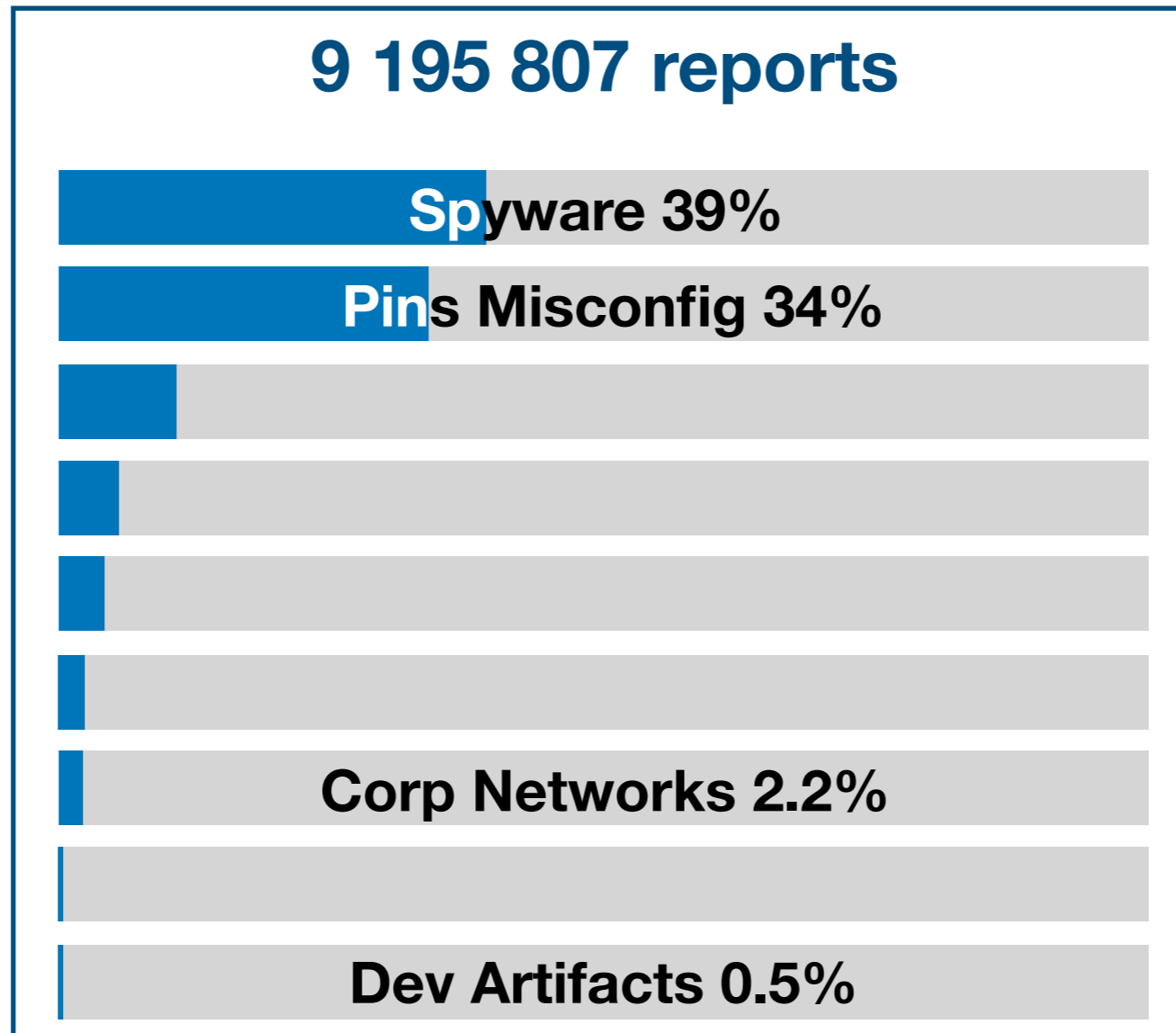
Non-Mitm Categories



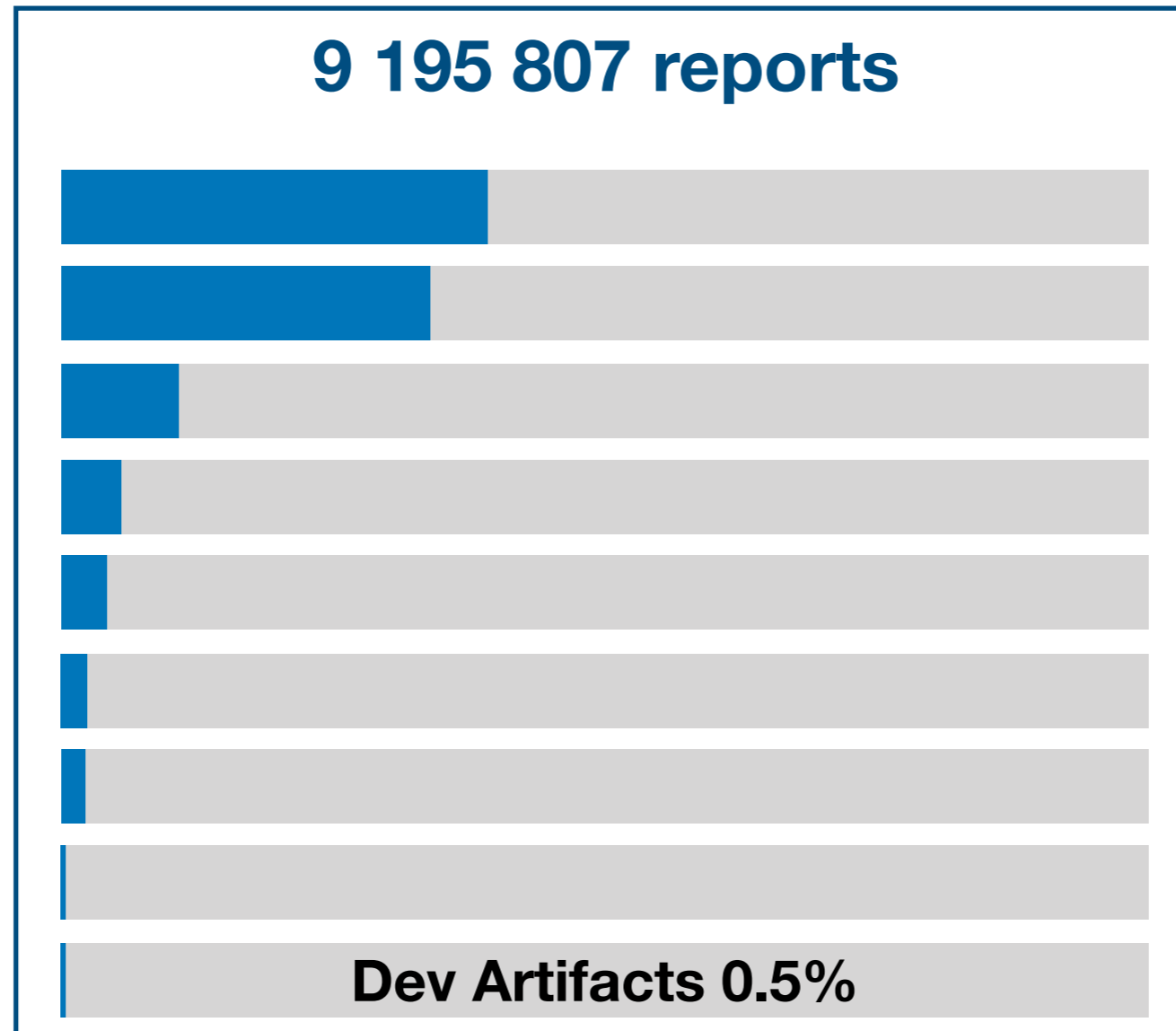
Classification Categories



Mitm Categories



Mitm Categories



Development Proxies

mitmproxy

PortSwigger

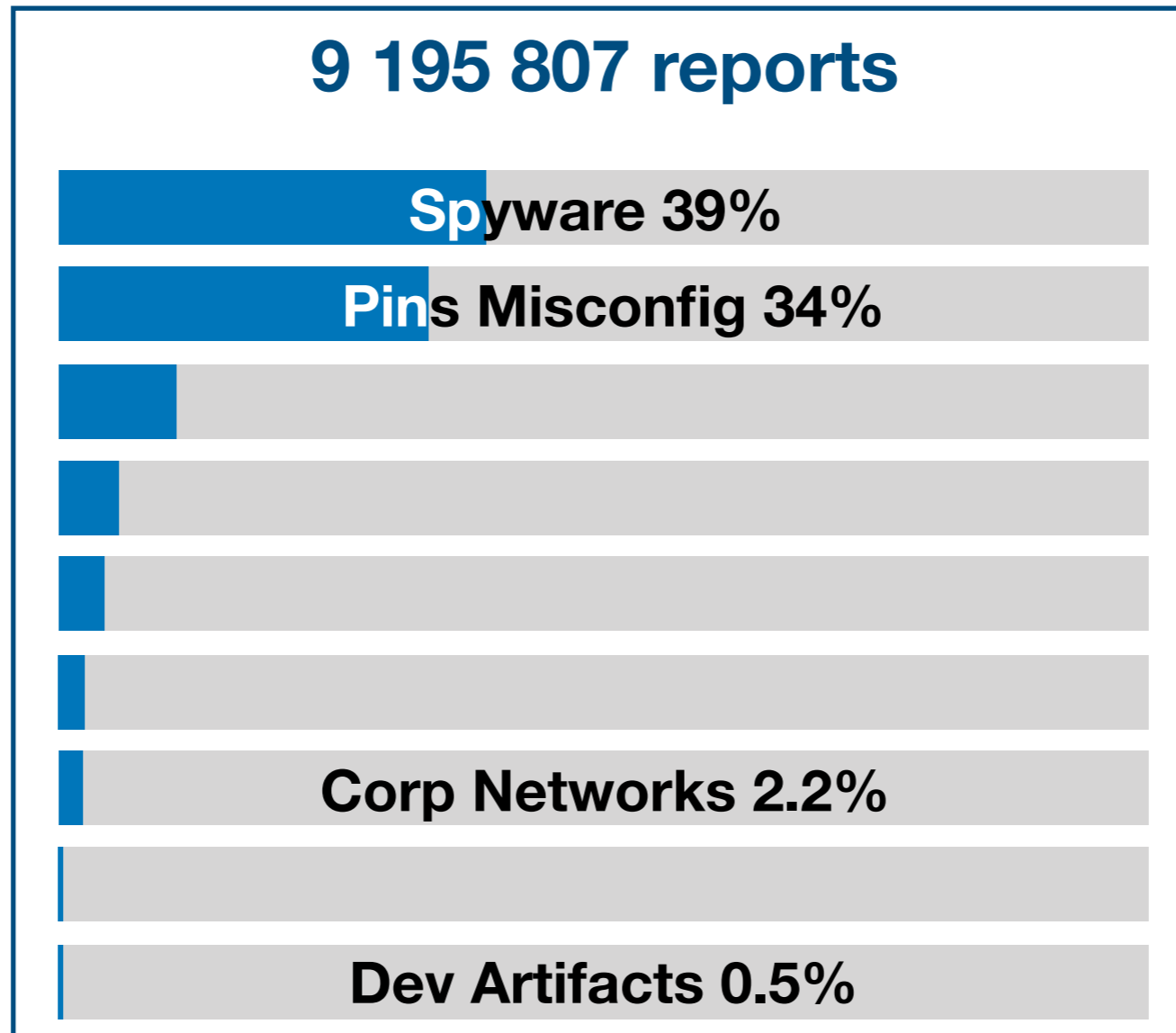
SSLsplit

Fiddler

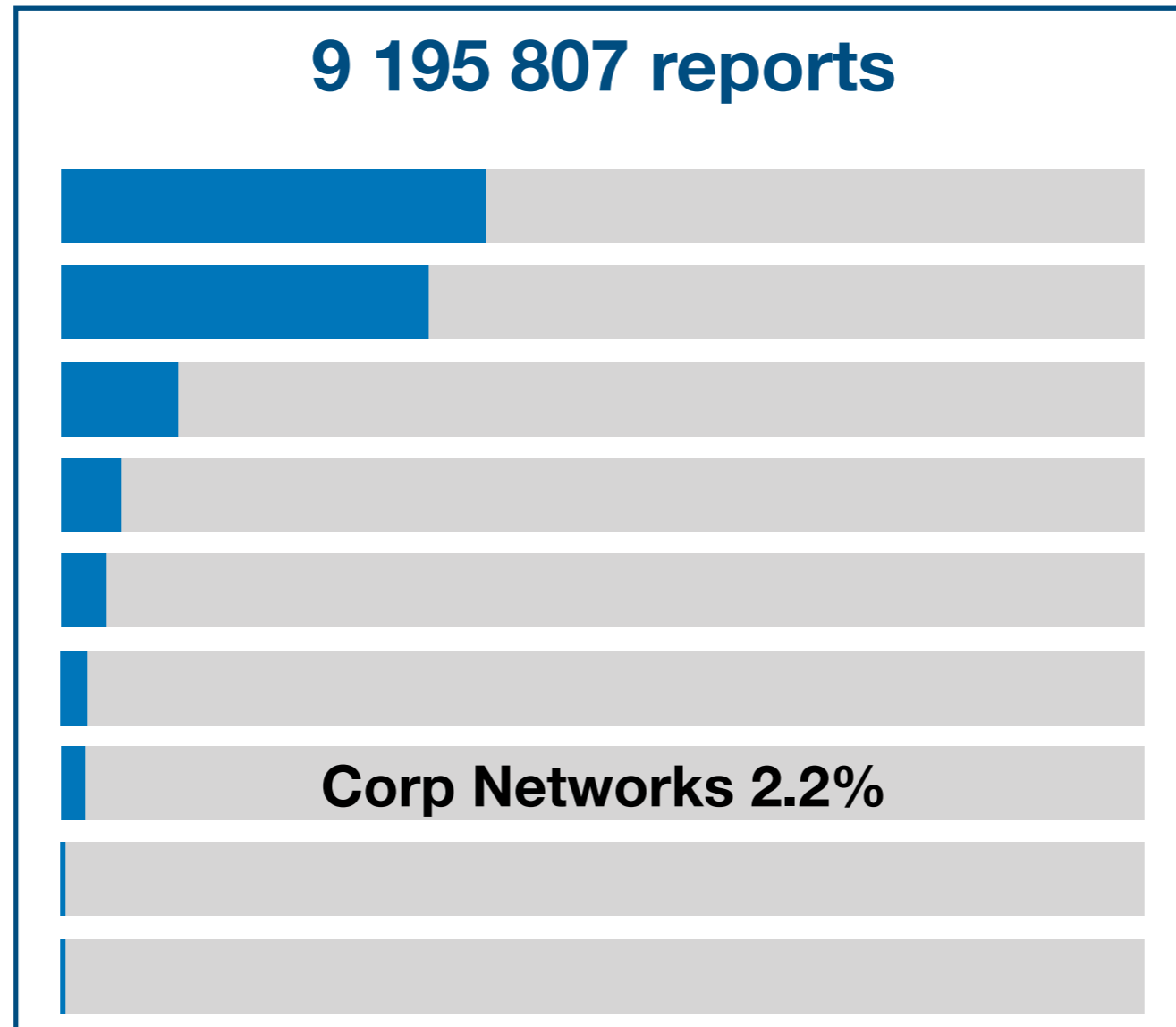
Charles Proxy

OWASP ZAP

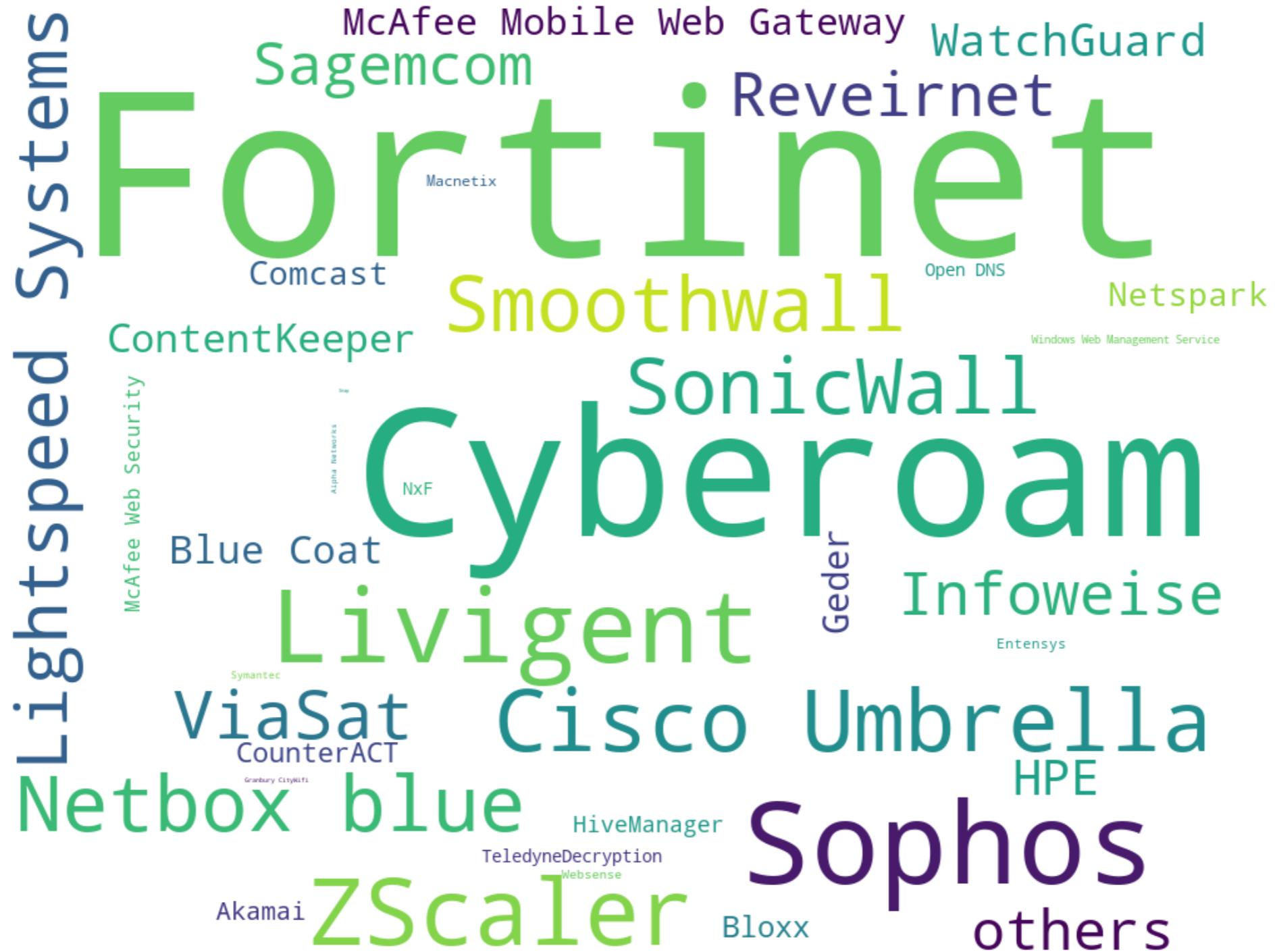
Mitm Categories



Mitm Categories

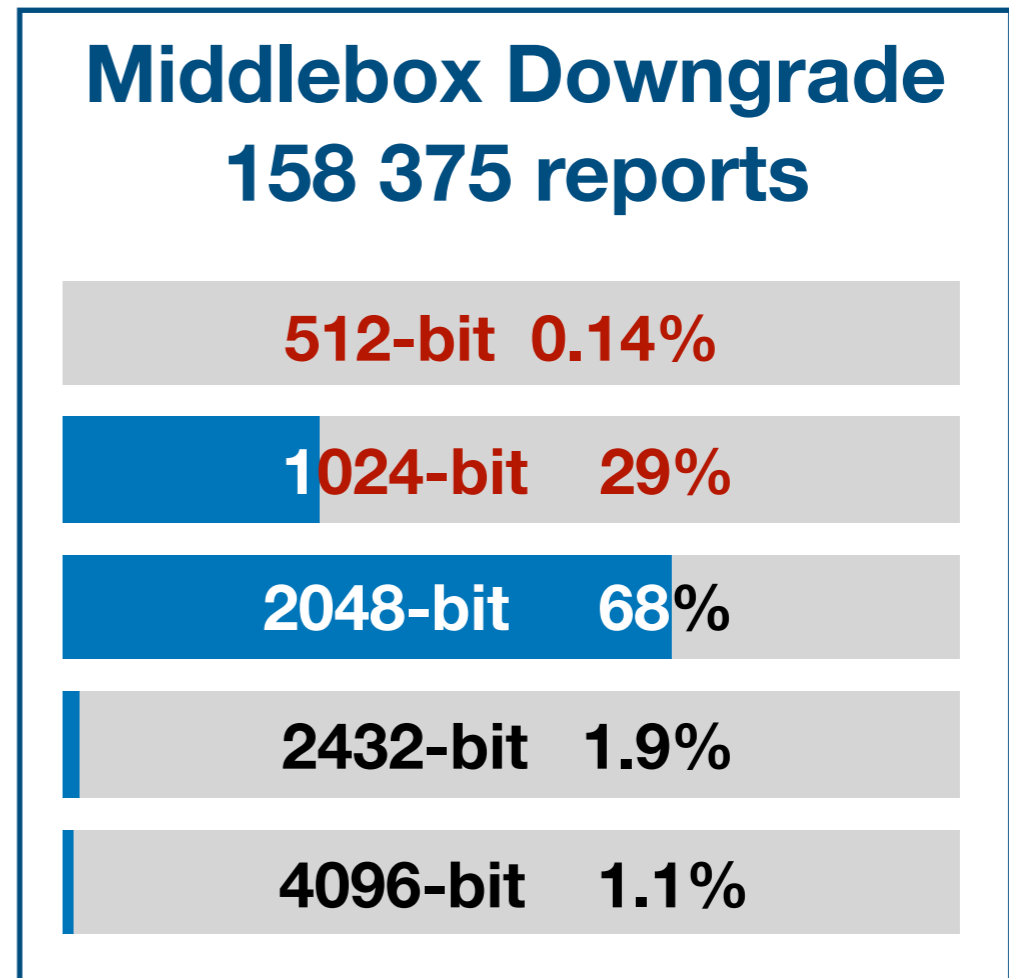


Corporate Networks

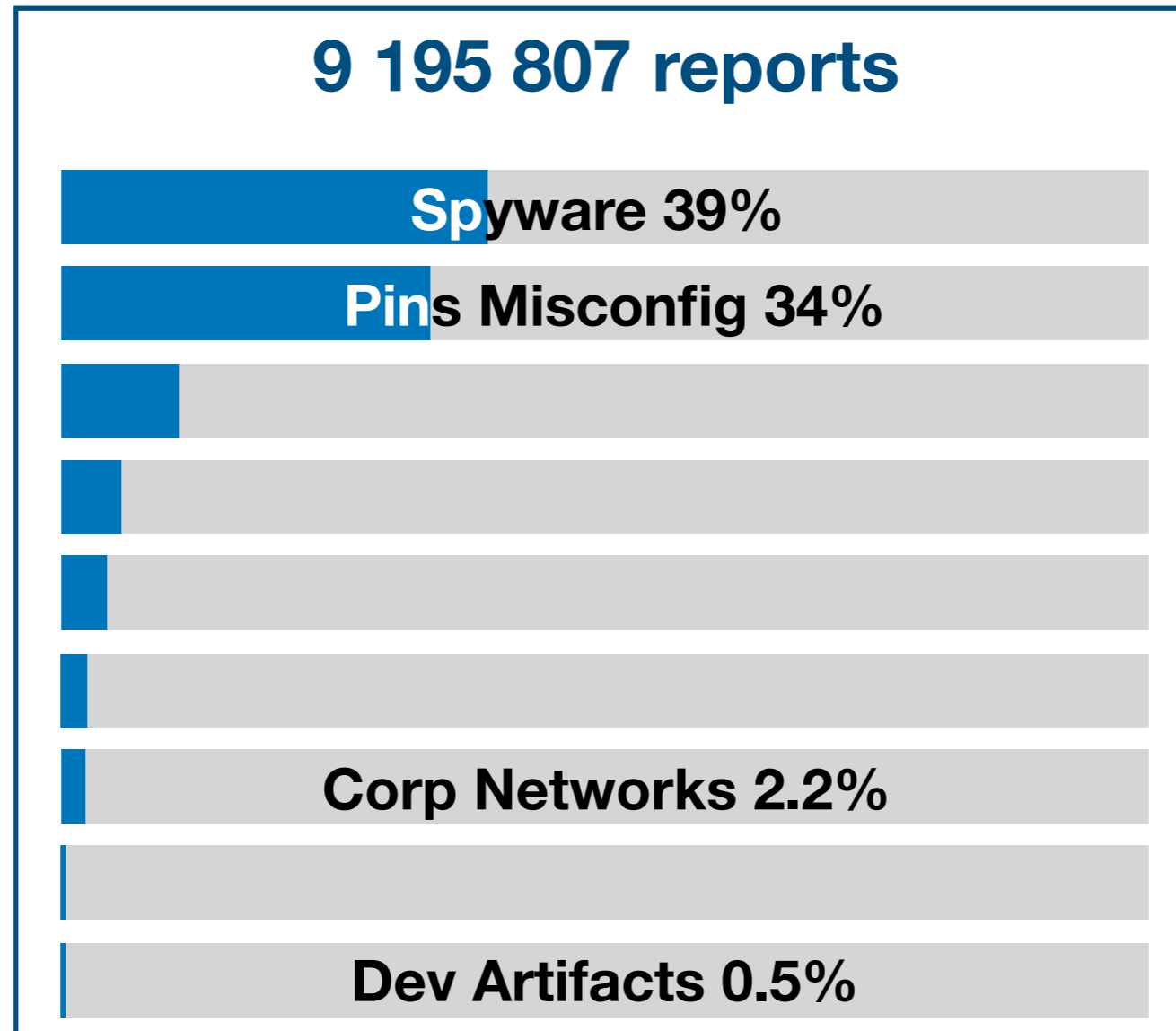


Corporate Networks

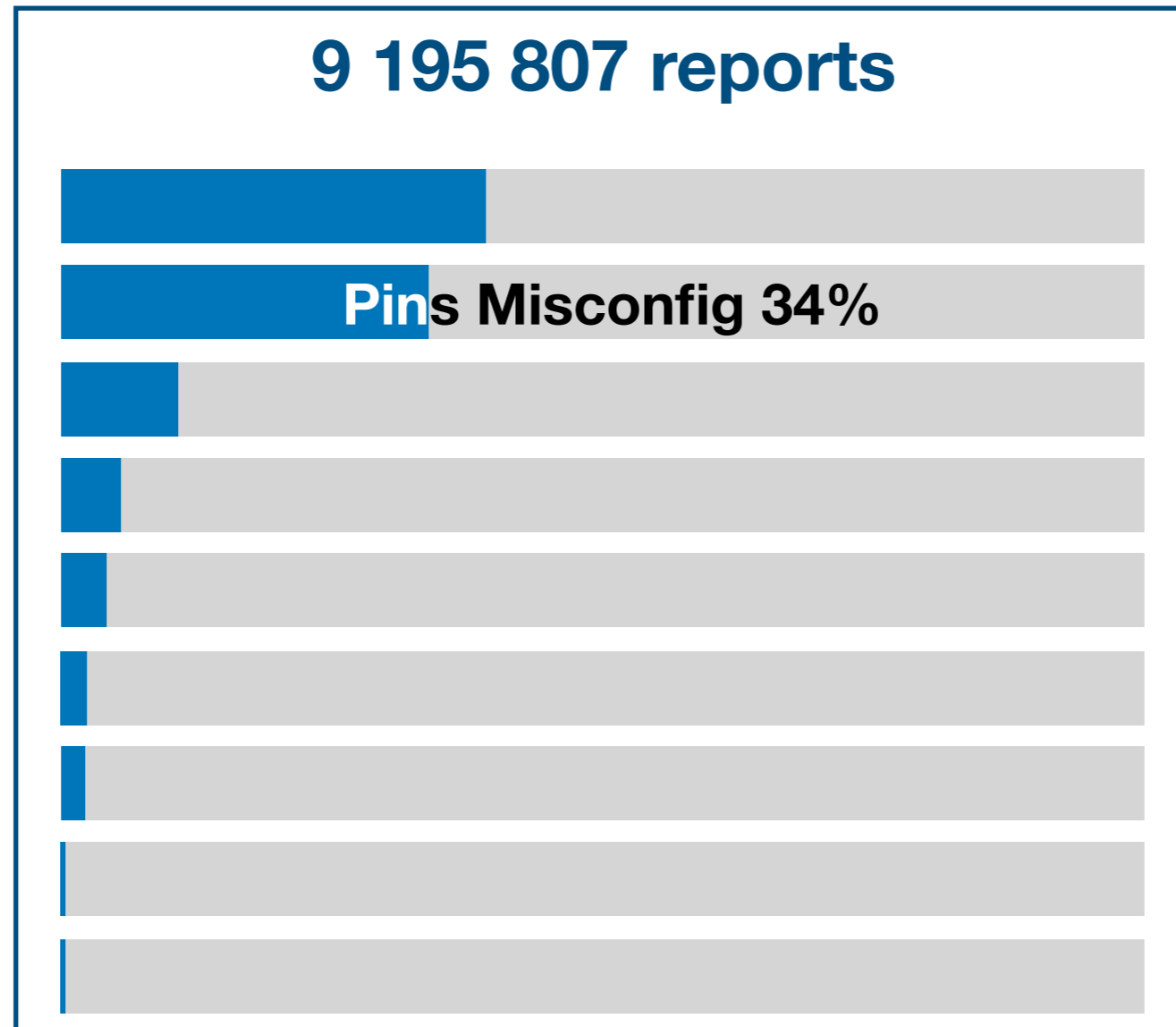
- For servers with a 2048 RSA certificate, what is the size of the middlebox's certificate?
- 29% of reports showed a downgrade to RSA 1024 or less
- TLS 1.3: big debate around encryption VS inspection



Mitm Categories



Mitm Categories



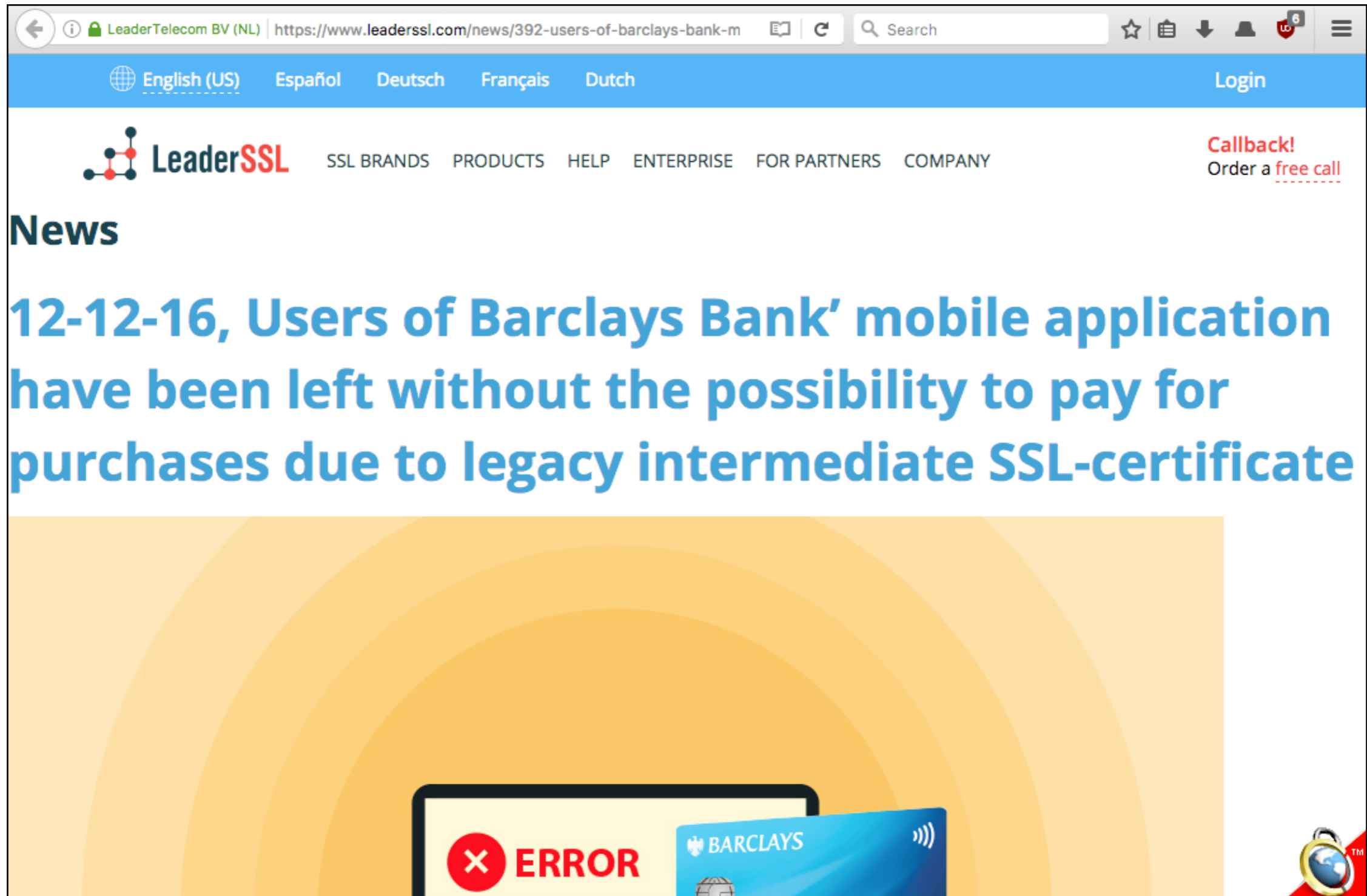
Pins Misconfiguration

- The SSL pins hardcoded in the app do not match the server's "real" certificate chain!
 - With enforce-pinning disabled:
 - The app still works but is constantly sending reports
 - With enforce-pinning enabled:
 - The app's connections will always fail

Pins Misconfiguration

- 22% of apps with misconfigured SSL pins
- Pressure on mobile developers to implement SSL pinning in their apps
 - From security teams, bug bounties, etc.
- But most apps do not need it
 - Significant logistical overhead to keep pins in the app in sync with the server SSL keys

Pins Misconfiguration



The screenshot shows a web browser window displaying a news article on the LeaderSSL website. The browser's address bar shows the URL: <https://www.leaderssl.com/news/392-users-of-barclays-bank-m>. The website's navigation bar includes language options (English (US), Español, Deutsch, Français, Dutch) and a 'Login' button. The LeaderSSL logo is visible, along with a menu of links: SSL BRANDS, PRODUCTS, HELP, ENTERPRISE, FOR PARTNERS, and COMPANY. A 'Callback!' banner offers a 'free call'. The article title is '12-12-16, Users of Barclays Bank' mobile application have been left without the possibility to pay for purchases due to legacy intermediate SSL-certificate'. Below the title is a large graphic with a yellow background and concentric circles, depicting a mobile device displaying an 'ERROR' message and a Barclays credit card.

LeaderTelecom BV (NL) | <https://www.leaderssl.com/news/392-users-of-barclays-bank-m> Search


English (US) Español Deutsch Français Dutch Login

LeaderSSL SSL BRANDS PRODUCTS HELP ENTERPRISE FOR PARTNERS COMPANY

Callback!
Order a free call

News

12-12-16, Users of Barclays Bank' mobile application have been left without the possibility to pay for purchases due to legacy intermediate SSL-certificate



Pins Misconfiguration



GeoTrust Global CA



RapidSSL SHA256 CA



*.payliquid.com



RapidSSL SHA256 CA

Intermediate certificate authority

Expires: Friday, May 20, 2022 at 16:45:51 Pacific Daylight Time

✔ This certificate is valid

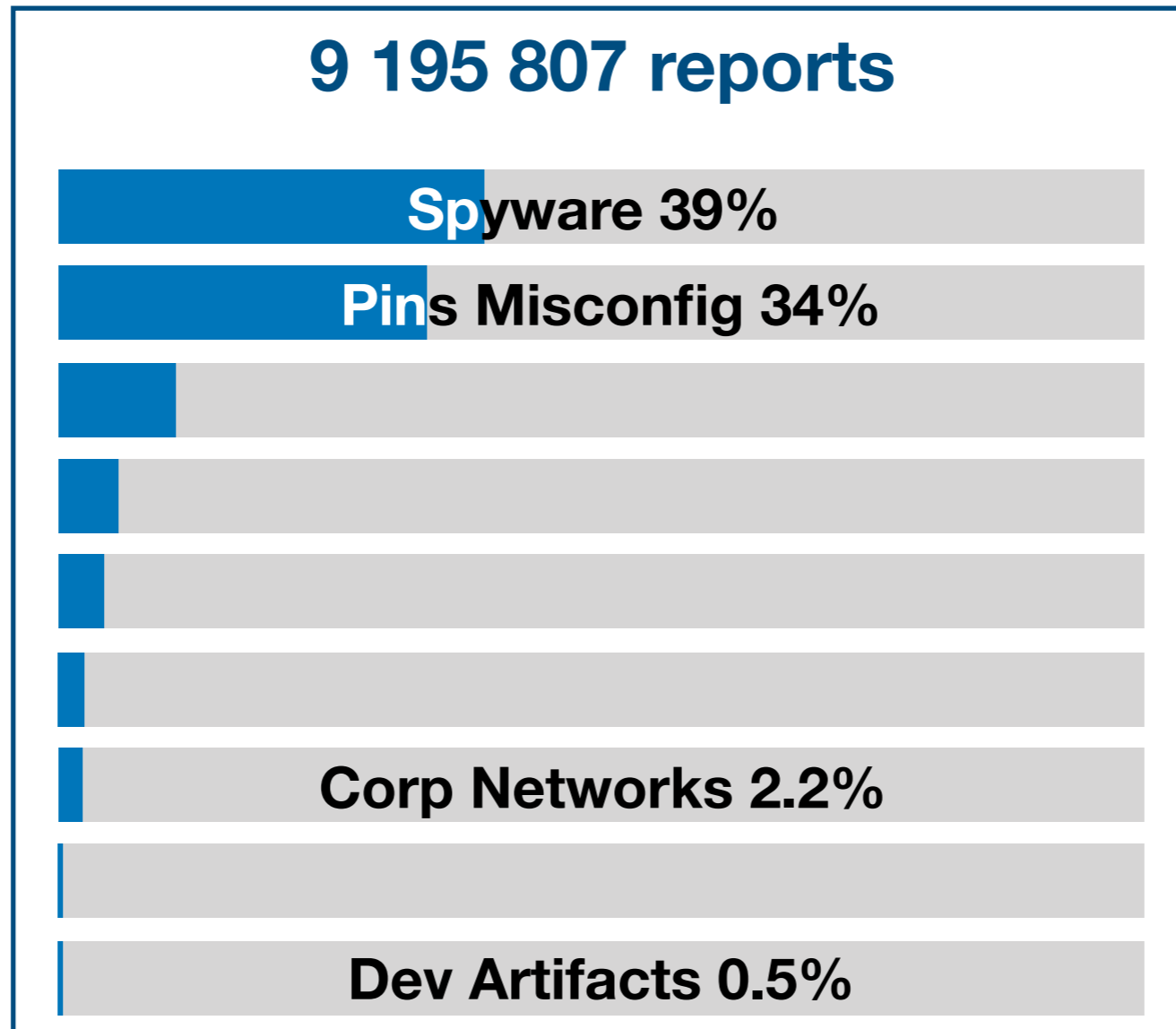


Details

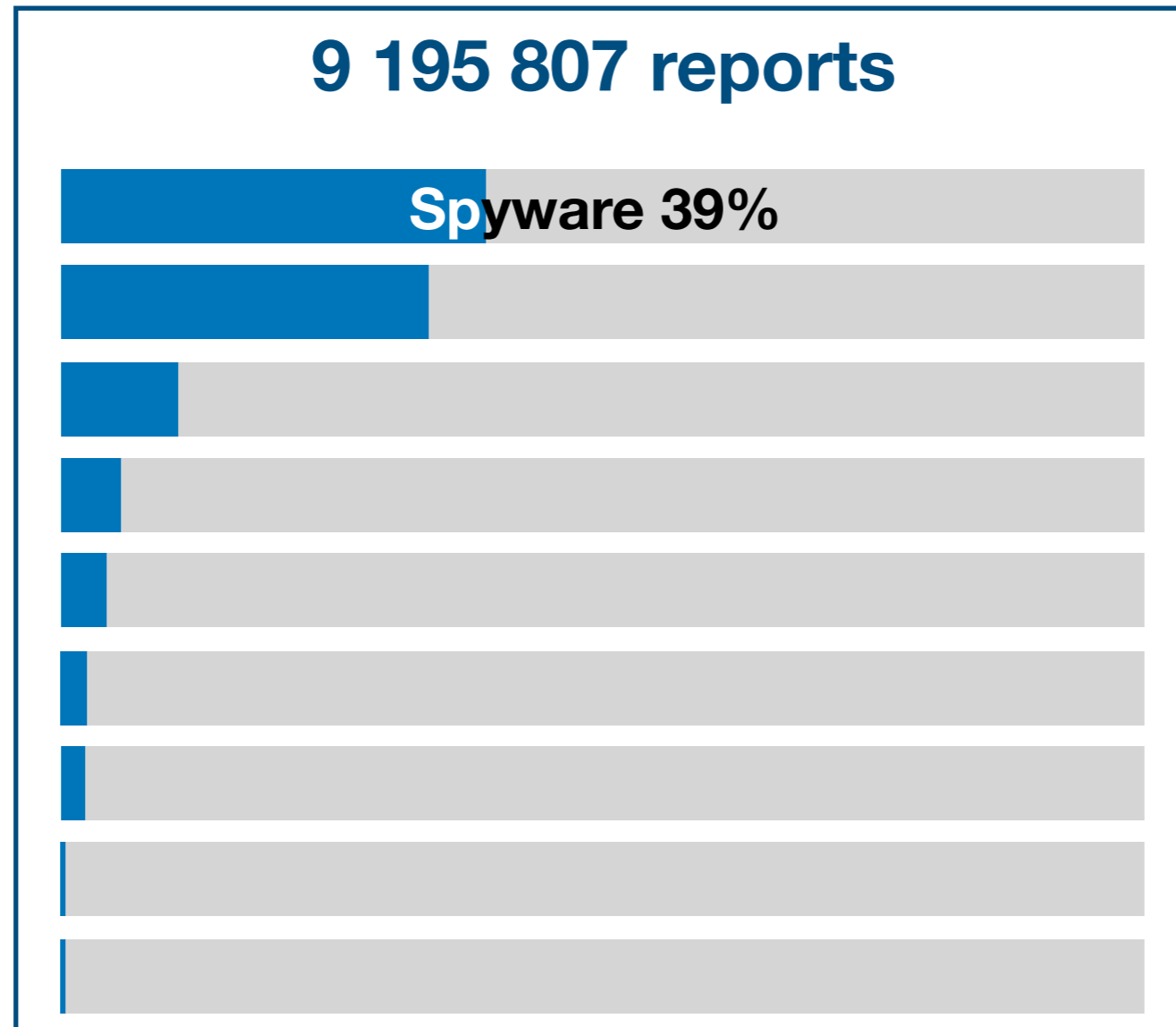
“Several thousands of customers of small and medium-sized businesses, operating mostly in the UK market, will not be able to perform any transactions from 8.30 a.m. 25/11/16 on a "Black Friday" and during the holiday shopping period.

This will affect hundreds of thousands of customer's transactions, until the application is updated, and then released again.”

Mitm Categories

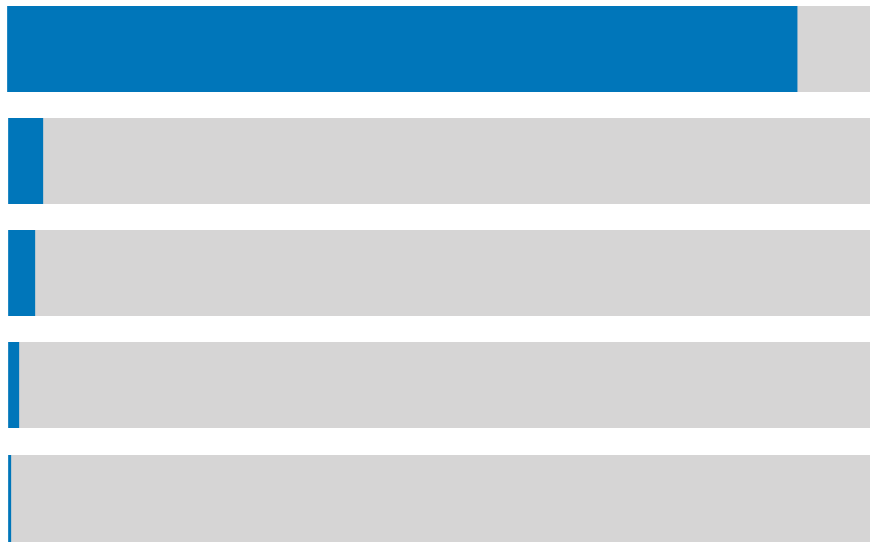


Mitm Categories



Spyware Categories

Market Intelligence
3 580 078 reports



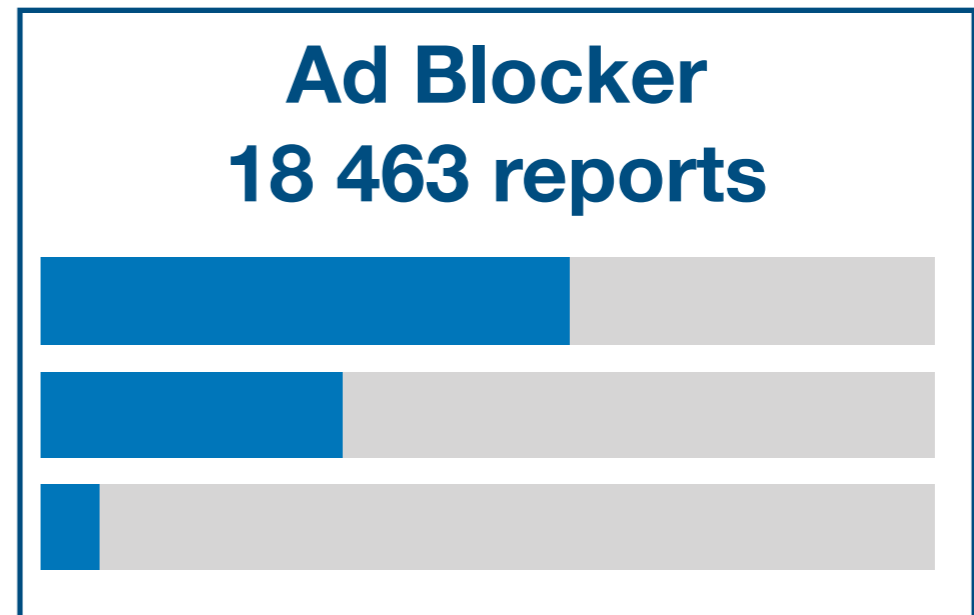
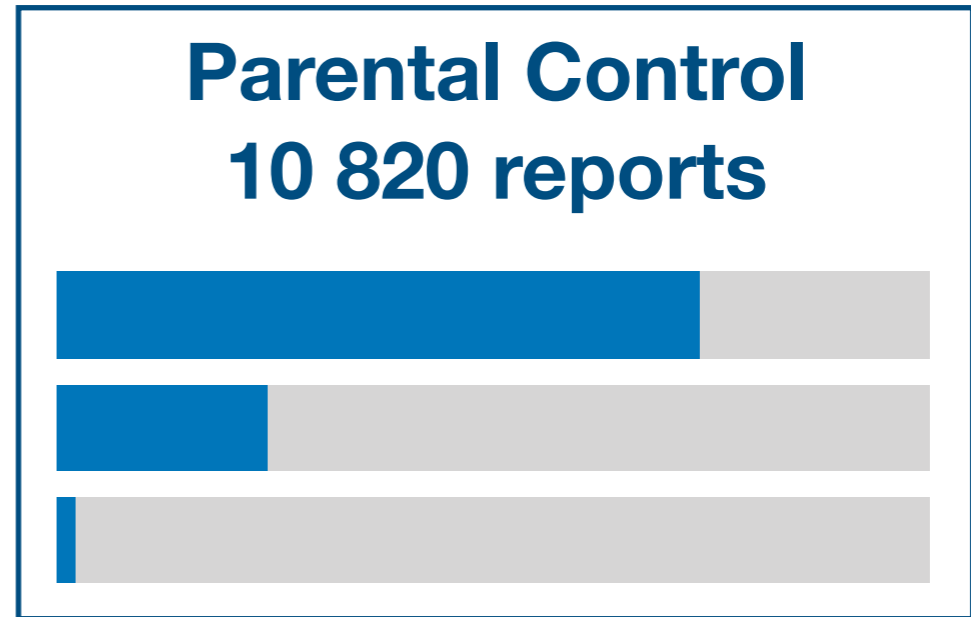
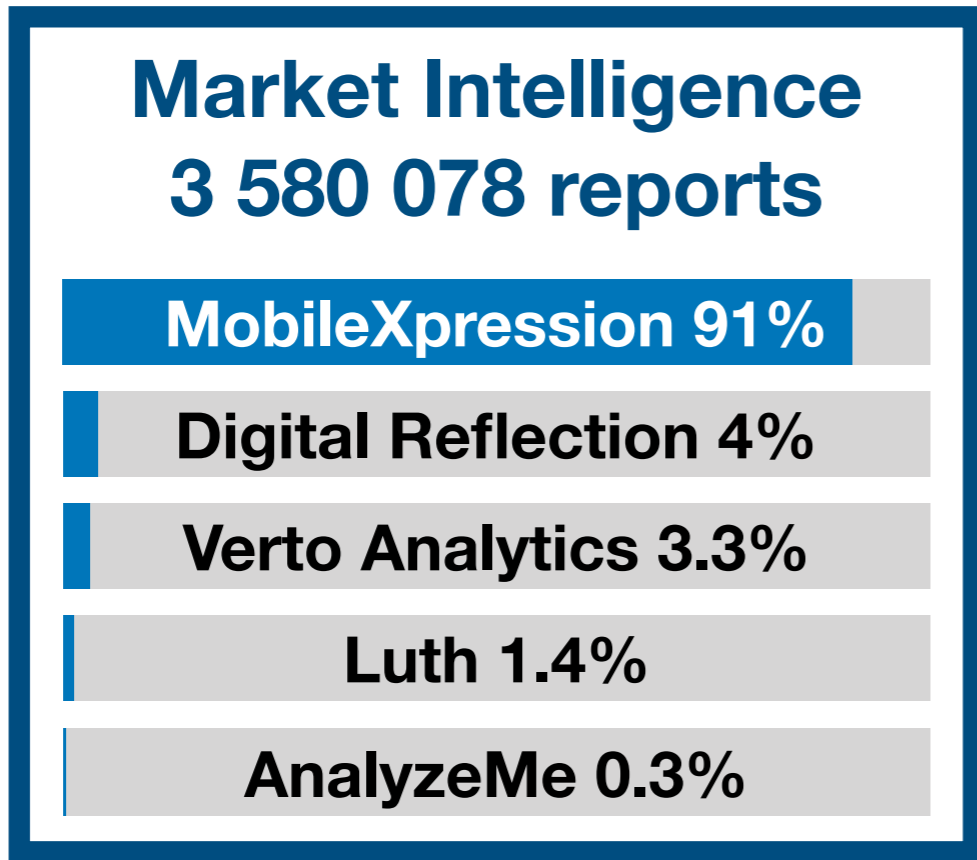
Parental Control
10 820 reports



Ad Blocker
18 463 reports



Spyware Categories



Spyware - Market Intel

- Mainly investigated MobileXpression and Digital Reflection
 - Common Name of the intercepting root/CA certificate
- Large number of reports across ~20 000 devices
 - Only seen on iOS devices

MobileXpression



If you hold the Internet in the palm of your hand, you can shape it.

Join Now!

Members' Login:

E-mail

Password

Login

[password help](#)

What We're About:

MobileXpression is an elite market research community dedicated to improving the mobile Internet. Mobile users are invited to join our panel and help shape the future of Internet you hold in the palm of your hand - simply by sharing your mobile surfing activity with us. [Click here to find out if you qualify to be a member of MobileXpression.](#)



Improving the mobile Internet and the environment.

TREES *for*
KNOWLEDGE

Demo

MobileXpression

TrustKit report 5479414662955008 [\[json\]](#) [\[pem\]](#) [\[share\]](#) [\[permalink\]](#)

2017-10-19 07:30:14 (device datetime:
2017-10-19T07:30:14Z)

7D1747F8-4D5E-42D5-AAB0-DA9708B830B5

App version 1.0

OS version 10.2.0

64.94.142.14

US / ca / los angeles

www.datatheorem.com

[cert match hostname]

[pinning enforced]

TrustKit version: 1.5.1

TSKPinValidationResultFailed

classifier version v2.3

device_spyware / MobileXpression

Cert #1

sha1-dbb96588d9a0a5470f90030054593aa177378c6c [\[search\]](#)

sni77340.cloudflaressl.com

Subject

Common Name: sni77340.cloudflaressl.com, Country: US

Cert #2

sha1-515371bea029ec427f4cfa0ec50cdc6ac2a3af3d [\[search\]](#)

MobileXpression CA

Subject

Common Name: MobileXpression CA; Organizational Unit: MobileXpression; Organization: Voice5; Street Address: 11950 Democracy Drive, Suite 600; Locality: Reston; State/Province: Virginia; Postal Code: 20190; Country: US

MobileXpression

TrustKit report 5479414662955008 [\[json\]](#) [\[pem\]](#) [\[share\]](#) [\[permalink\]](#)

2017-10-19 07:30:14 (device datetime:
2017-10-19T07:30:14Z)

7D1747F8-4D5E-42D5-AAB0-DA9708B830B5

App version 1.0

OS version 10.2.0

64.94.142.14

US / ca / los angeles

www.datatheorem.com

[cert match hostname]

[pinning enforced]

TrustKit version: 1.5.1

TSKPinValidationResultFailed

classifier version v2.3

device_spyware / MobileXpression

Cert #1

sha1-dbb96588d9a0a5470f90030054593aa177378c6c [\[search\]](#)

sni77340.cloudflaressl.com

Subject

Common Name: sni77340.cloudflaressl.com, Country: US

Cert #2

sha1-515371bea029ec427f4cfa0ec50cdc6ac2a3af3d [\[search\]](#)

MobileXpression CA

Subject

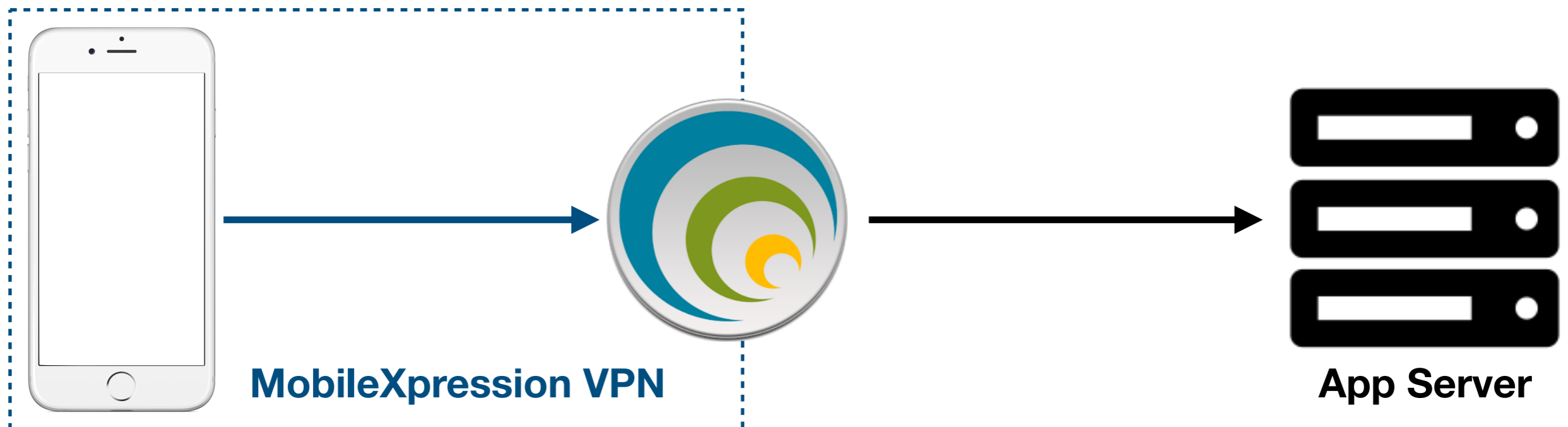
Common Name: MobileXpression CA; Organizational Unit: MobileXpression; Organization: Voice5; Street

Address: 11950 Democracy Drive, Suite 600; Locality: Reston; State/Province: Virginia; Postal Code: 20190;

Country: US

What Happened?

- A configuration profile was installed on the device
 - With an always-on VPN config
 - To route **all traffic** through the MobileXpression server
 - With a custom root CA added to the device's trust store
 - To allow **traffic decryption** by the MobileXpression server



MobileXpression?

“MobileXpression is a service of comScore, Inc., a global leader in measuring the digital world, providing insights into consumer behavior and attitudes.”

ComScore

- Owner of several “market research” apps
 - MobileXpression, Digital Reflection
- Promise users rewards (gif cards, etc.) for installing the app and configuration profile

ComScore

- Owner of several “market research” apps
 - MobileXpression, Digital Reflection
- Promise users rewards (gif cards, etc.) for installing the app and configuration profile

Rip off app ★
by Central Law

They spent four weeks collecting data from my phone. First week I won an amazon gift card which I never received. Then they never gave any more rewards when they say you get something each week. Contacted customer support and they never replied. I gave em a week and still nothing. They got my data for free. Don't be like me

ComScore

“This capability is based on a massive, global cross-section of approximately 2 million consumers, who have allowed comScore to collect their online browsing, hardware and application usage, and purchasing behavior.”

ComScore

- Inspect/decrypt all the users' traffic to measure app usage
- ComScore's business model as a "measurement company"

The value of everywhere.



We uniquely combine massive scale with smarter methods to turn data into value.

Our unmatched data footprint combines proprietary digital, TV and movie intelligence with vast demographic details to deliver the most precise understanding of audiences, brands and consumers everywhere. It's what makes our solutions better.

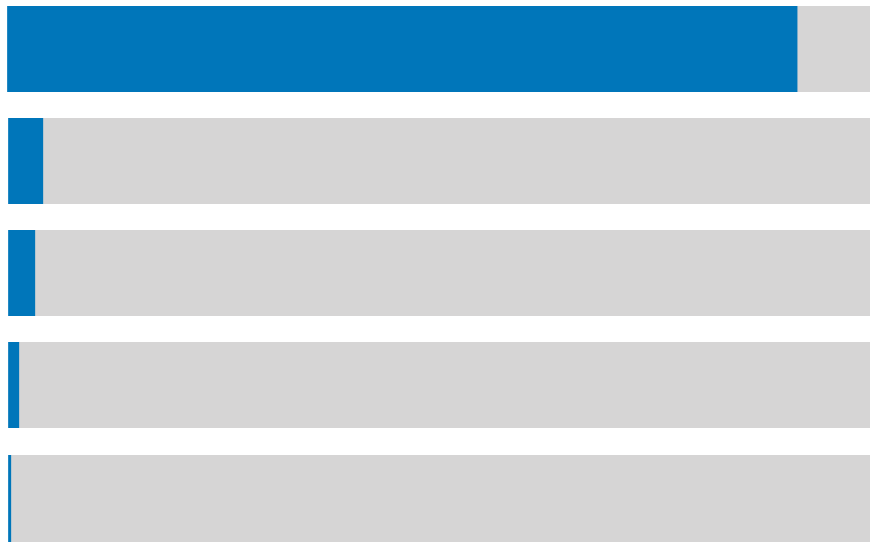
[Our solutions](#)

Spyware - Market Intel

- Configuration profiles are problematic
 - Highly technical security warnings when installing the profile
 - The profile/VPN does not get uninstalled when removing the app
 - Makes sense from a technical perspective but will confuse users
- But not an easy issue to fix
 - Corporate enrollment / MDM use case
 - A profile can be installed directly via Safari
 - Banning the spyware app from the store does not prevent it

Spyware Categories

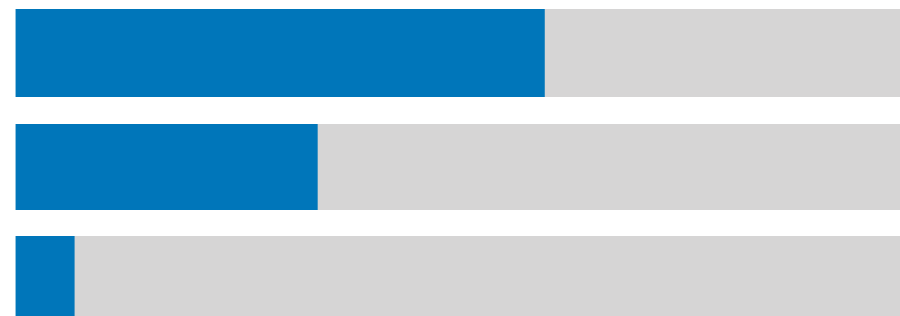
Market Intelligence
3 580 078 reports



Parental Control
10 820 reports

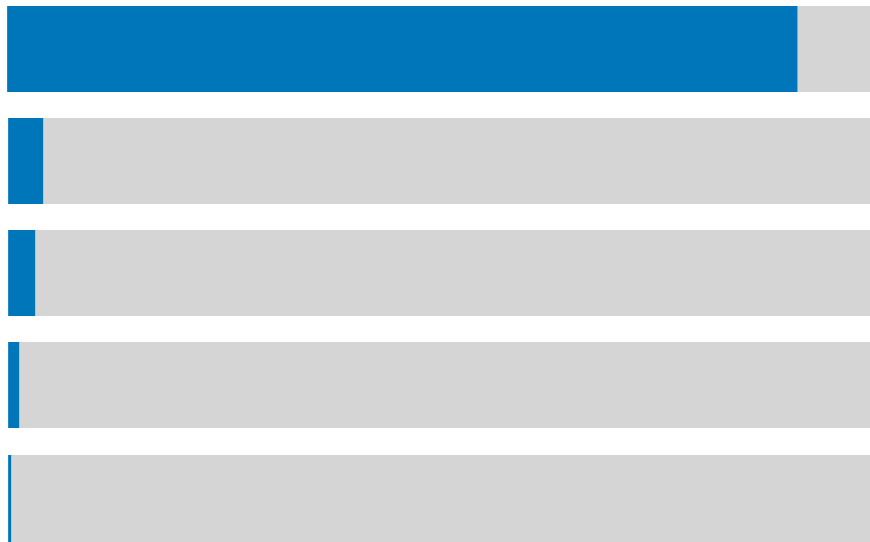


Ad Blocker
18 463 reports



Spyware Categories

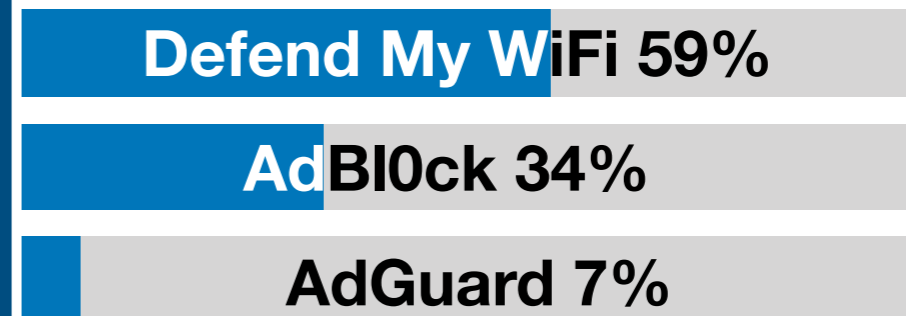
Market Intelligence
3 580 078 reports



Parental Control
10 820 reports



Ad Blocker
18 463 reports



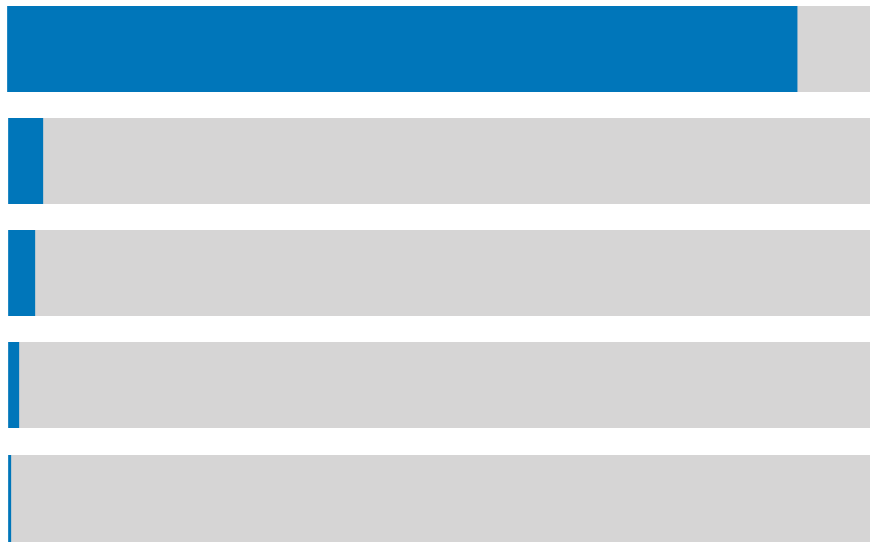
Spyware - Ad Blocker

- Similar technical implementation with a VPN and custom CA
- Defend My WiFi
 - "Automatically turns public Wi-Fi into safe and secure private WiFi"
 - Company does not exist anymore?
- Adblock Mobile
 - iOS 8: SSL mitm on ad domains only
 - iOS 9+: No more custom CA installed



Spyware Categories

Market Intelligence
3 580 078 reports



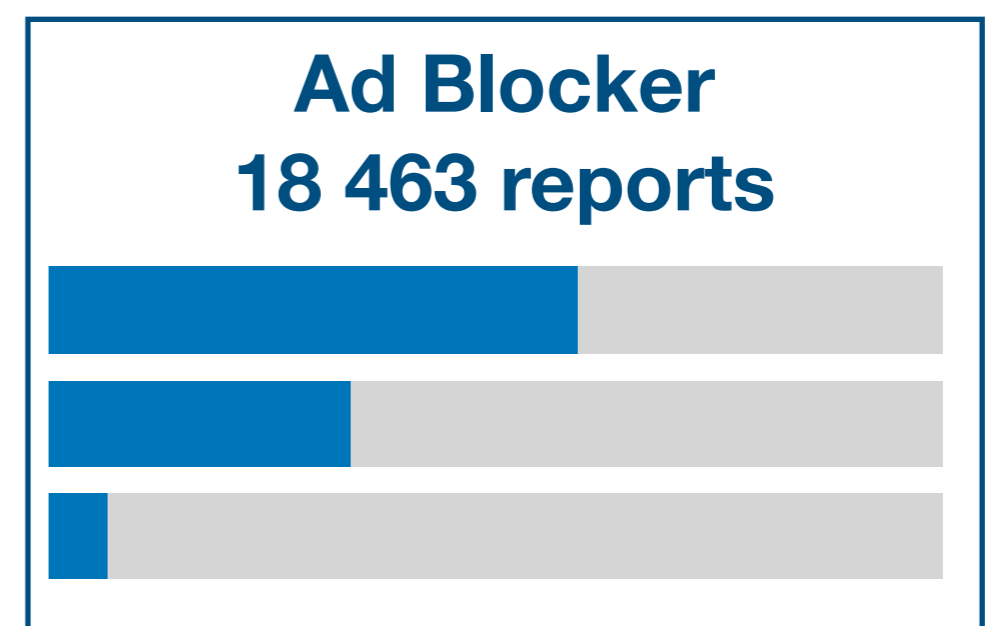
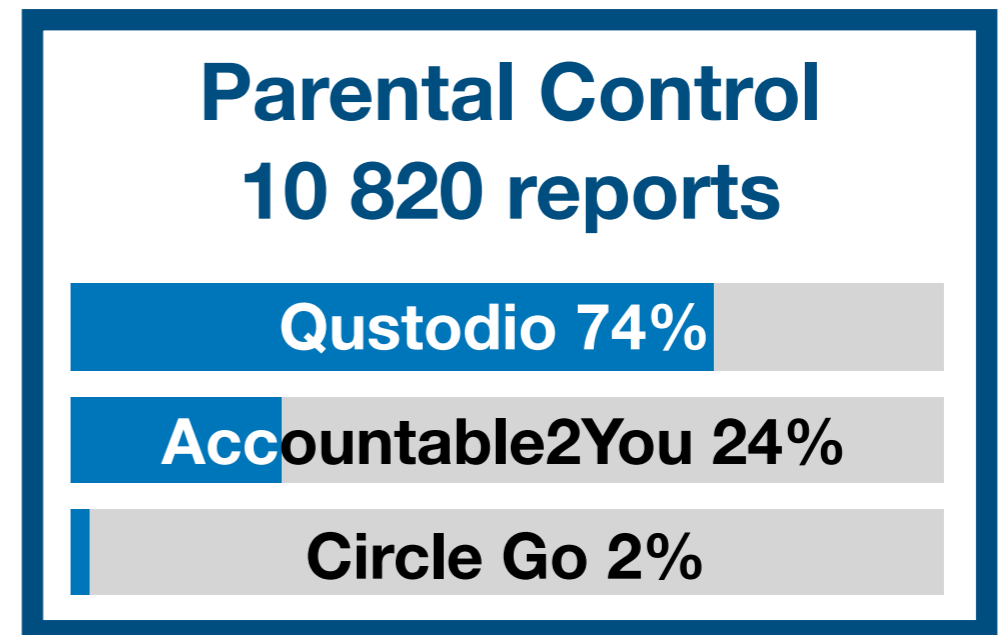
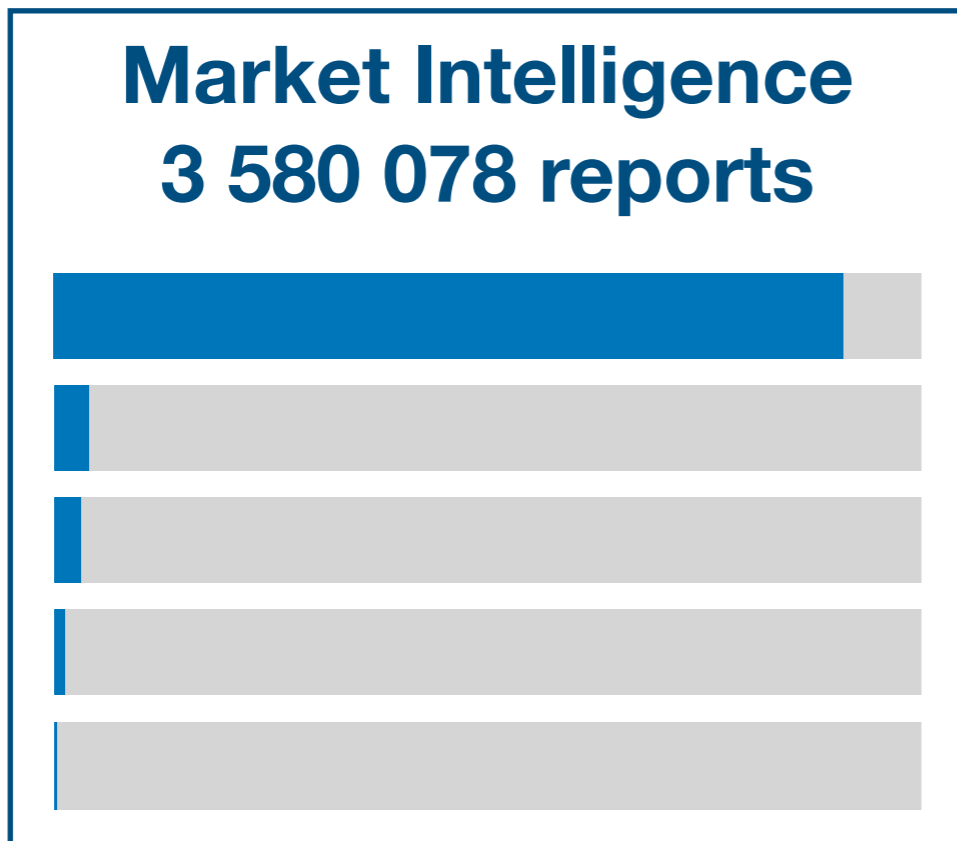
Parental Control
10 820 reports



Ad Blocker
18 463 reports



Spyware Categories



Spyware - Parental Control

- Qustodio, Accountable2You, Circle Go
- Parental control/monitoring tools

How it works...



Create an Account

Create your account from our website and select the plan that fits you best.



Install on Your Devices

Download the A2U app from your device's app store and login to your account.



Set Up Accountability Partners

Set up your partners and assign them to monitor specific device activity.

Conclusion

What did we see?

- Traffic interception does happen, and for many reasons
 - It has an impact on the security of the connection
 - Usually not malicious
 - Employers
 - Users “willingly” sharing their data for a reward
 - No visible move from Apple and Google on this

What do we do?

- Which group does your app belong to?
 - It is acceptable to expose the user's data to "lawful interception" (such as the user's employer)
 - Games, Business apps
 - The user's data is private and can never be exposed
 - Mobile banking
 - Can be technically enforced via SSL pinning

What do we do?

- More options on mobile compared to the web
- SSL reporting can help understand what is happening across your user base
- SSL pinning can be used for sensitive apps
 - Does not prevent reverse-engineering of your app
 - Significant burden and risk of catastrophic failure
 - Must be decided and planned carefully

Thanks!

@nabla_c0d3
@trucsdedev



Questions?

@nabla_c0d3
@trucsdedev

