RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: PDAC-F02

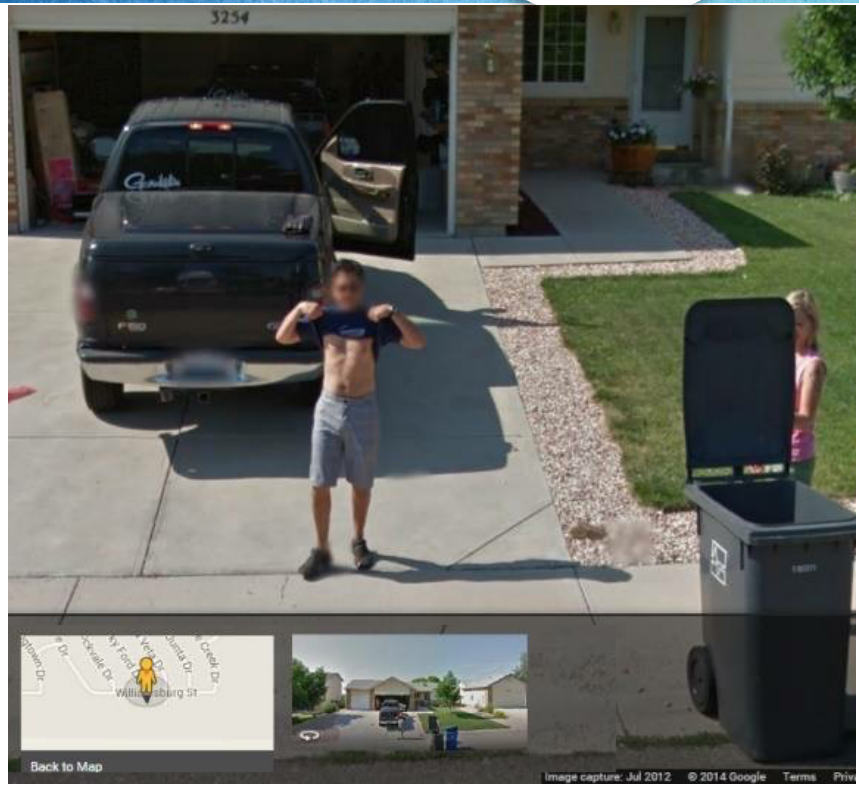
SECRETS OF THE ENCRYPTED INTERNET: WORLDWIDE CRYPTOGRAPHIC TRENDS

David Holmes

Threat Researcher
F5 Networks, Inc.
@dholmesf5

Who is that Guy?

- David Holmes
  - Childhood crypto enthusiast
  - C/C++ Programmer for 25 years
  - F5 Networks for the last 17 years
  - Today: Security Researcher
    - Python / OpenSSL / PostGreSQL
- Briefly ”internet-famous” when Google Maps car drove by me arguing at ex-wife’s house



Scanning the Internet

- Ridiculous Introduction
- Building a TLS scanner
- Key Findings
  - Protocol Selection
  - Forward Secrecy
  - Self-signed Certificates vs. Let's Encrypt
  - Strict Transport Security
  - What replaces Pinning?
- CTA: Best Practices
- Lessons Learned

Why build an SSL/TLS Scanner?

- 75% of page loads are HTTPS
- Wanted my own data
- Because it's FUN!

Building a TLS Scanner

Scanner Best Practices

- Keep scan rates as low as possible. Reduce load and impact on networks and people
- Allow opt-out for scan targets
- Coordinate with the hosting company, or anyone else who might get in the way of your scan

- **From Project Sonar Best Practices*

Mass Scanning by IP Address

- Enter Project Sonar
- Rapid7 team does Internet-wide scans
- Every host listening to port 443 twice a month
- Published via Censys
  - https://scans.io/study/sonar.ssl

Scan the Internet from your Basement

SOFTWARE

- Ubuntu
  - 14.04
- Python
  - Easy to code in
  - Beautiful
  - Multi-threaded
- MySQL
  - Decent Python Integration, free

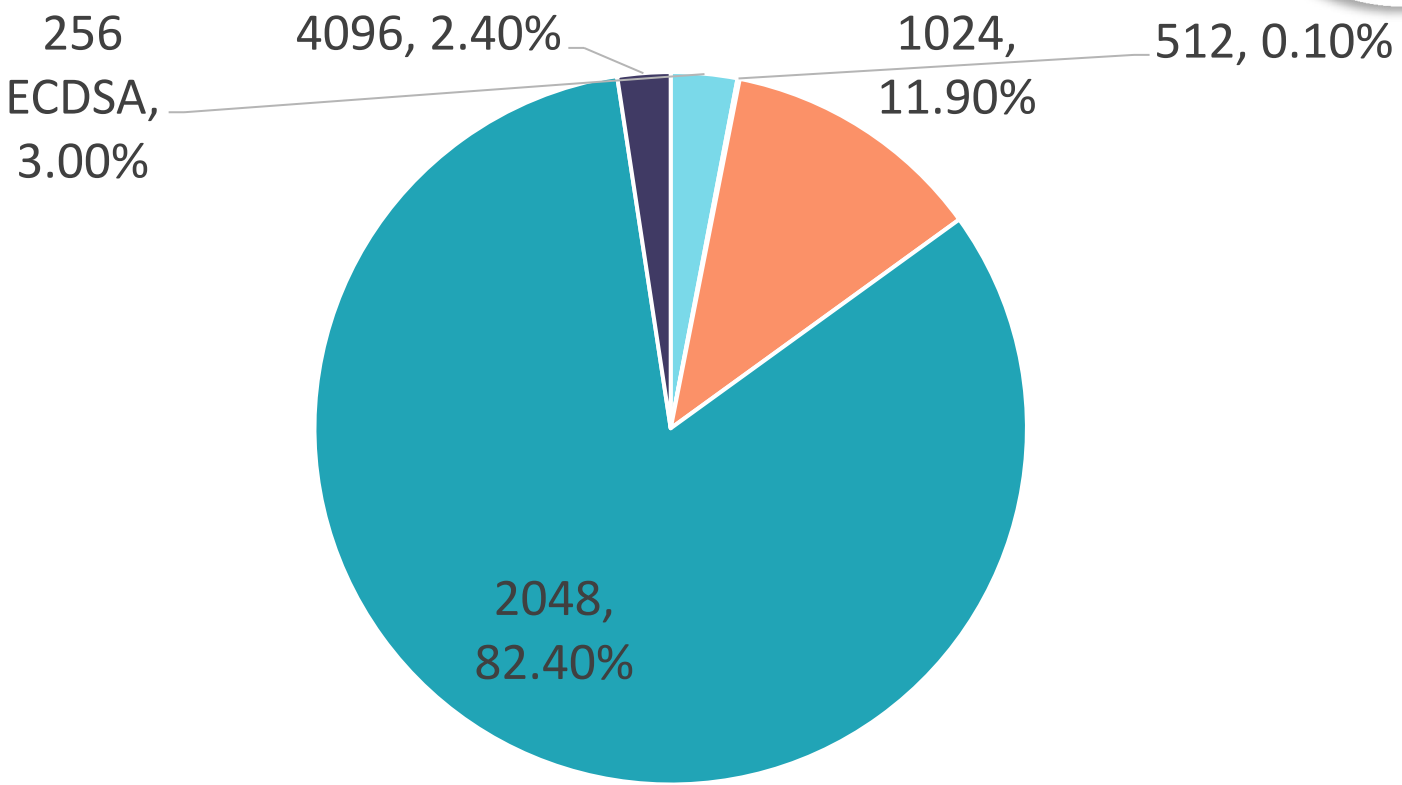
HARDWARE AND NETWORK

- 4 core stock Dell desktop PC
- 256 Gb disk space
- Comcast network
- D-Link DIR-255 Router

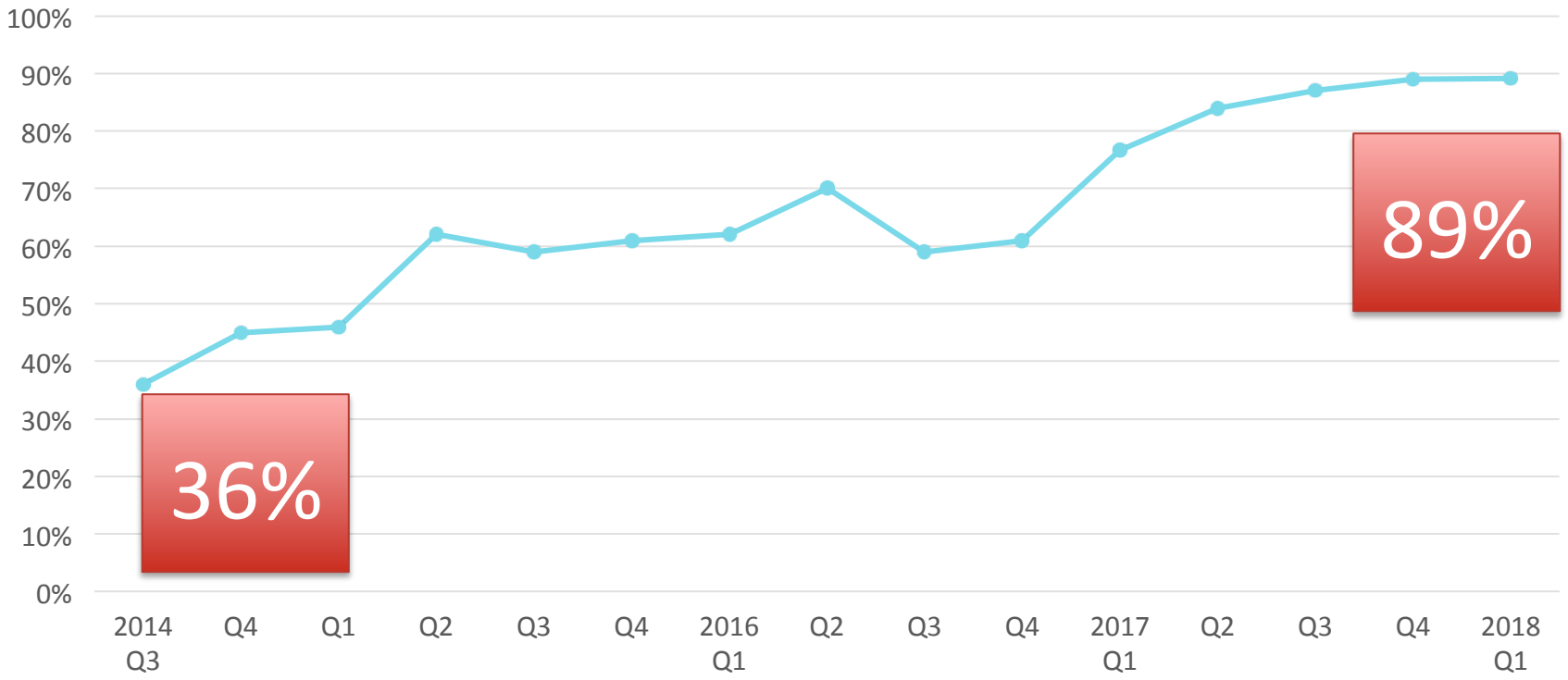
PRIMARY CRYPTOGRAPHIC STATISTICS

Baseline your TLS Security

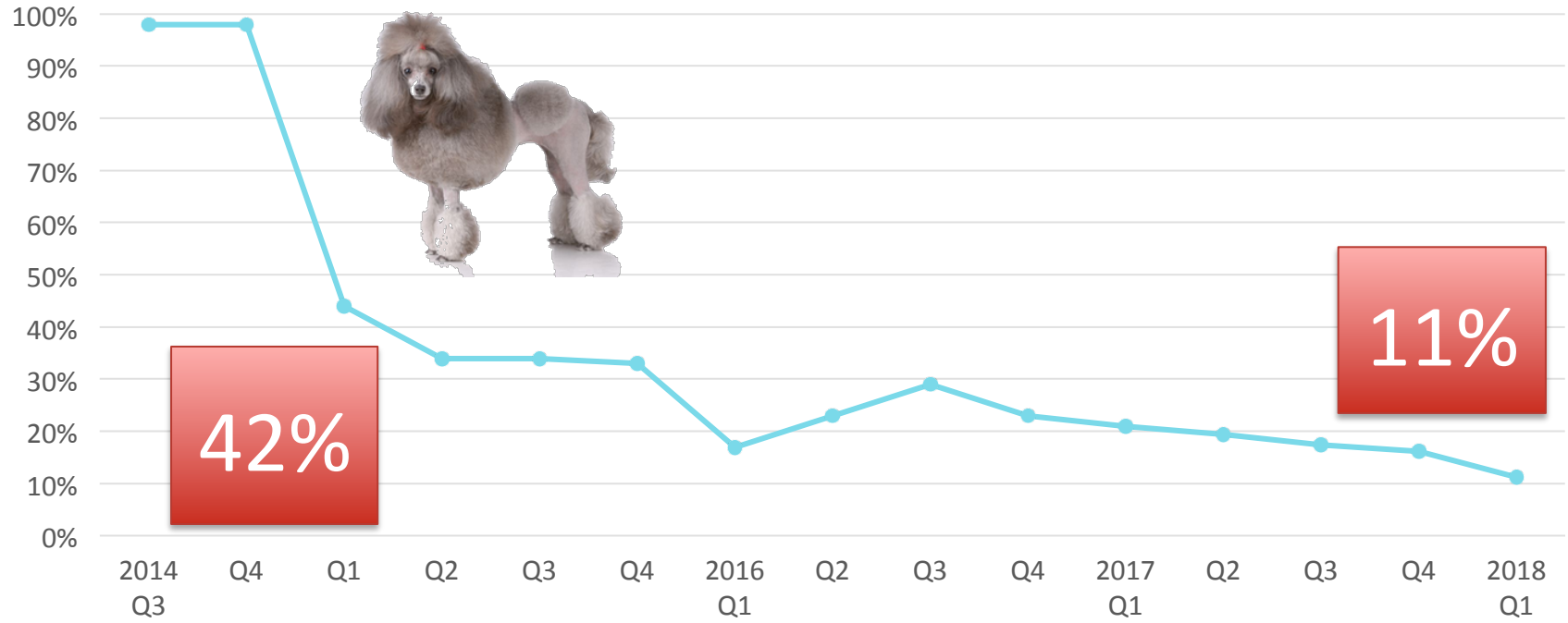
Let's start with an easy one: RSA Key Sizes



Preference for TLSv1.2+



SSLv3 Support



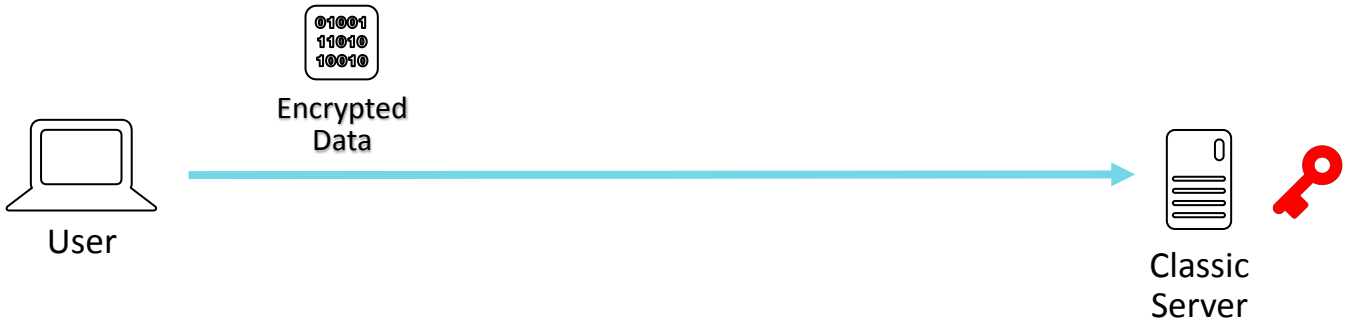
Where is TLS 1.3?

- What about TLS 1.3?
- 7% of Jan ‘18 show TLS 1.3 compatibility
  - However, nearly all of that is Cloudflare
  - Remove CF and it drops to 3400 out of sample of 672,000 (0.07%)
- TLS 1.3 = Only Forward Secret ciphers
- Adoption is slow because changes so radical
  - Nick Sullivan, Adam Langley have blog explaining compatibility problems

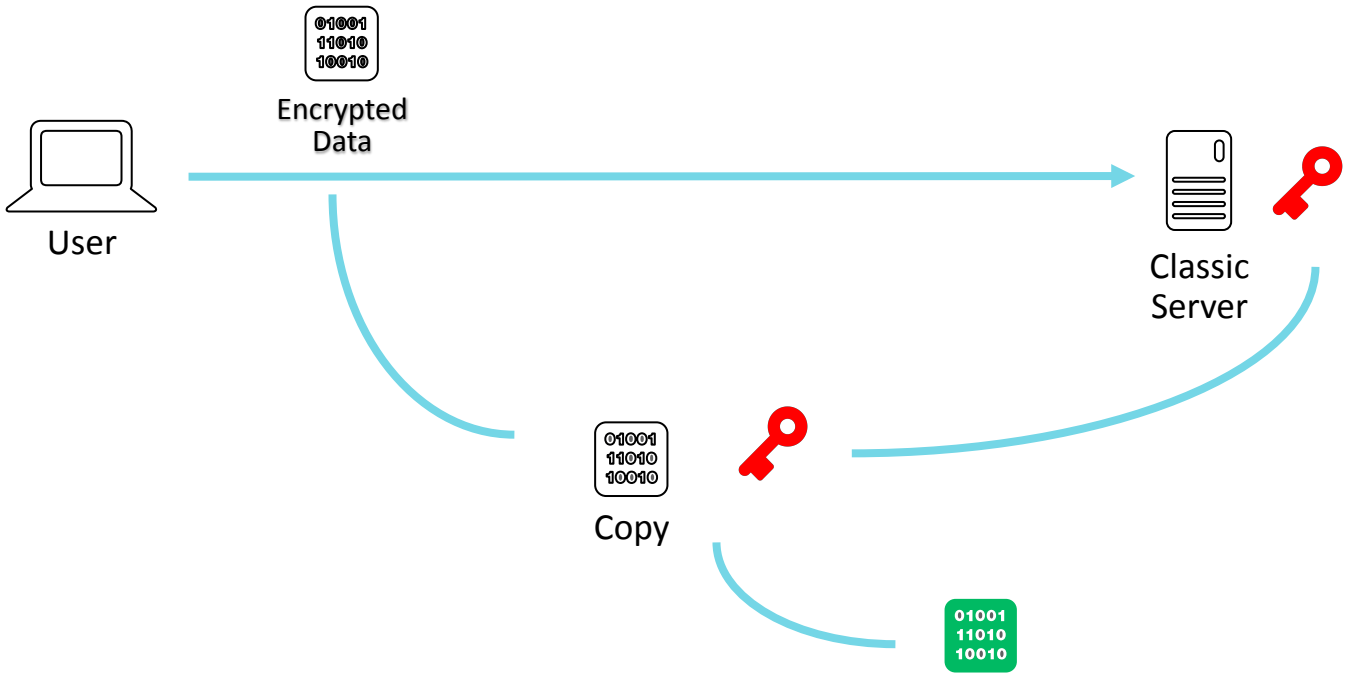
FORWARD SECRECY

Keep your secrets secret, forever

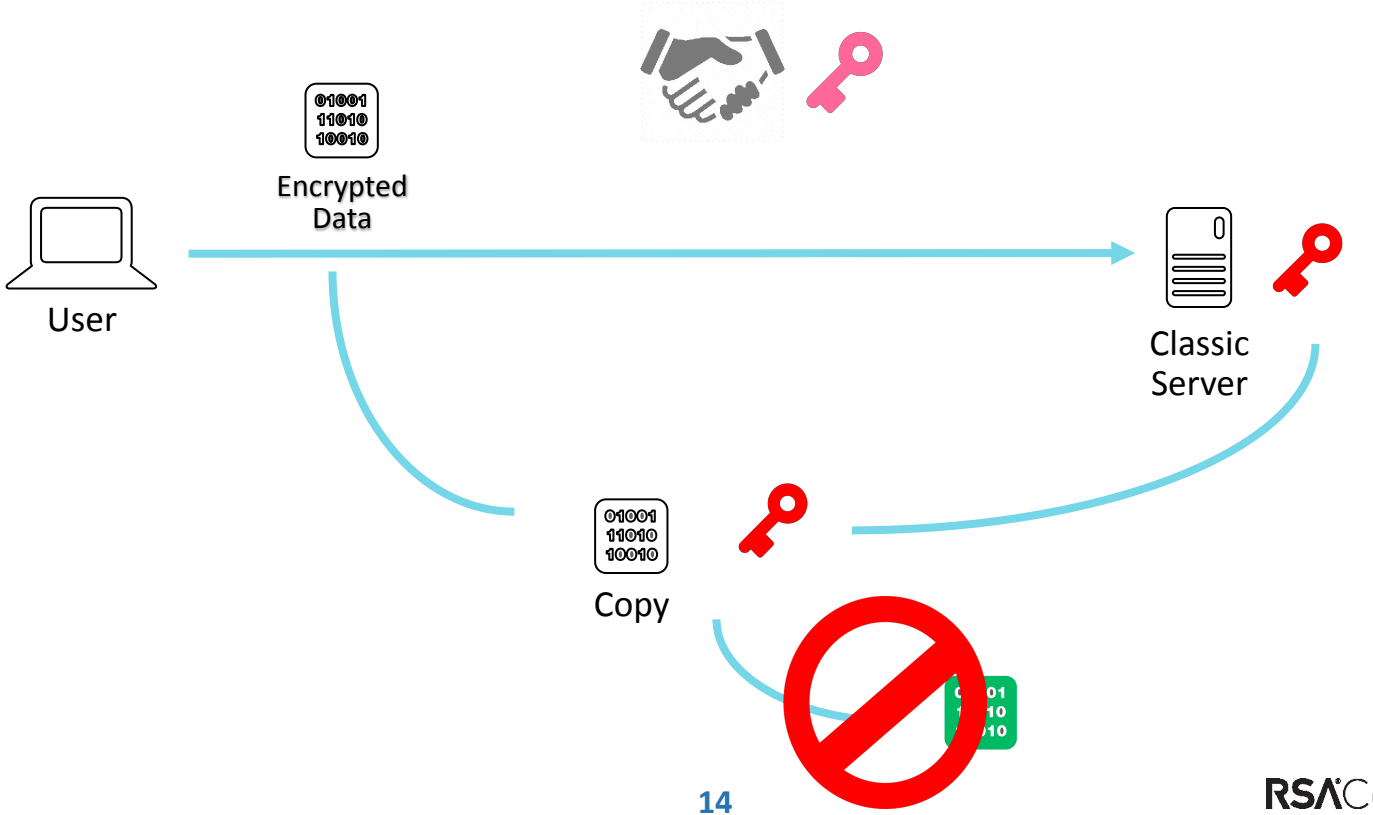
Problem: Recorded Ciphertext



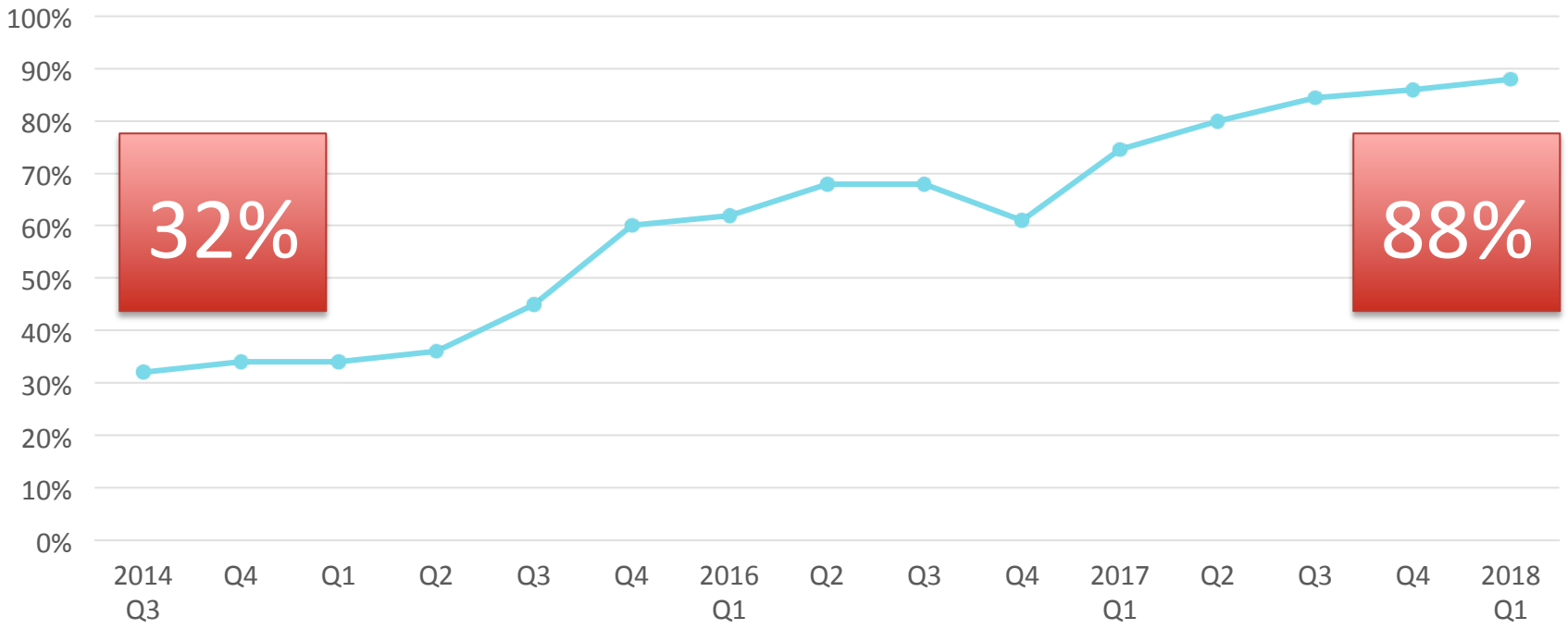
Problem: Anyone with the key can decrypt



(Perfect) Forward Secrecy – Ephemeral Key



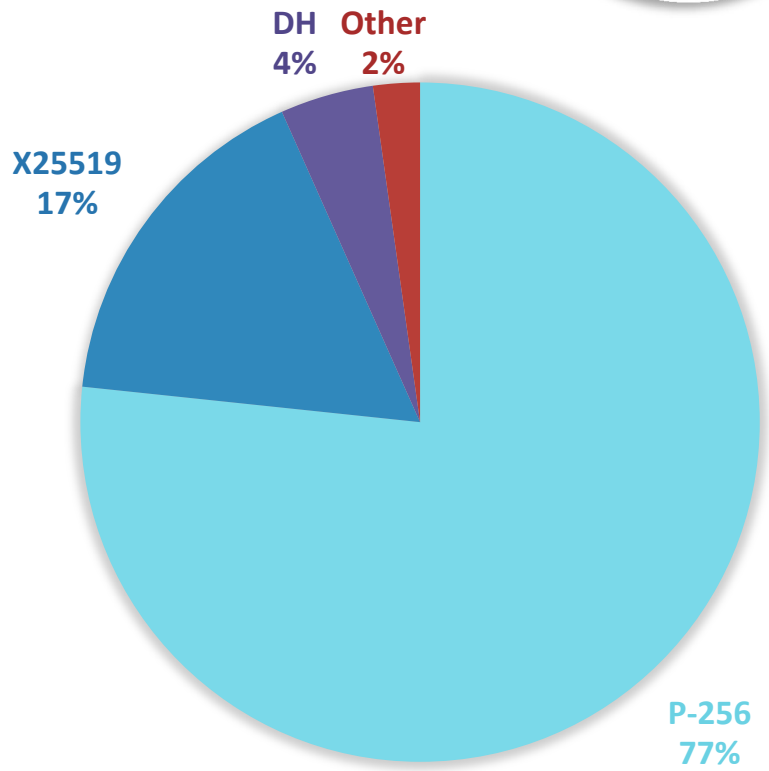
Forward Secrecy Adoption



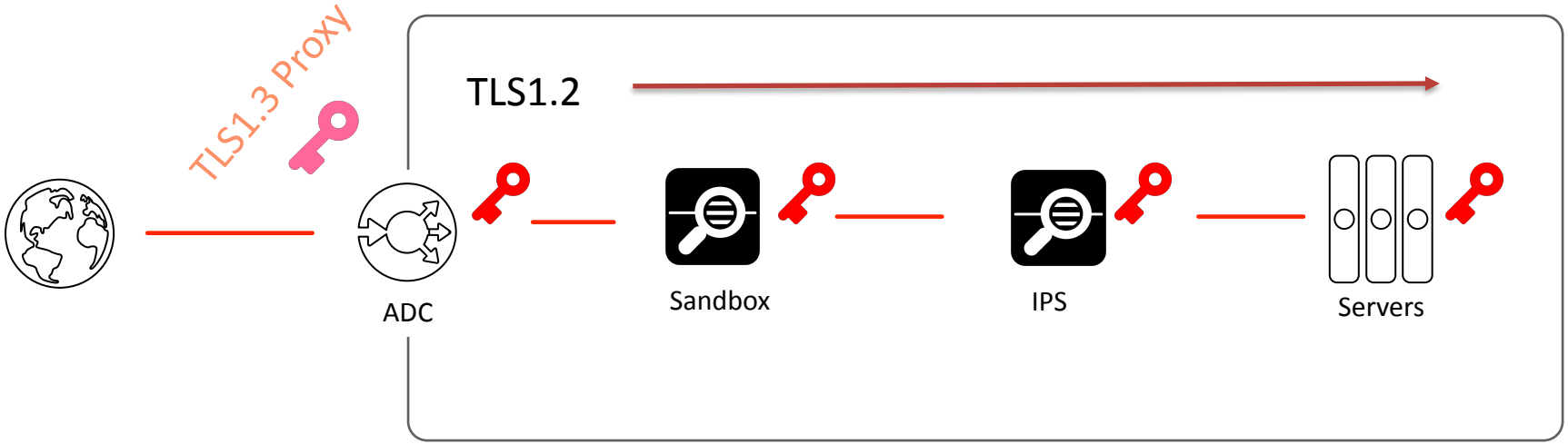
Forward Secret Types

Top 10 Ciphers – (EC)DHE = Forward Secret

1. ECDHE-RSA-AES256-GCM-SHA384
2. ECDHE-RSA-AES128-GCM-SHA256
3. ECDHE-RSA-AES256-SHA384
4. ~~AES256-SHA~~
5. ECDHE-ECDSA-AES256-GCM-SHA384
6. ~~AES256-GCM-SHA384~~
7. DHE-RSA-AES256-SHA
8. ECDHE-RSA-AES256-SHA
9. ~~AES128-SHA~~
10. DHE-RSA-AES256-GCM-SHA384



Fitting Forward Secrecy into a network



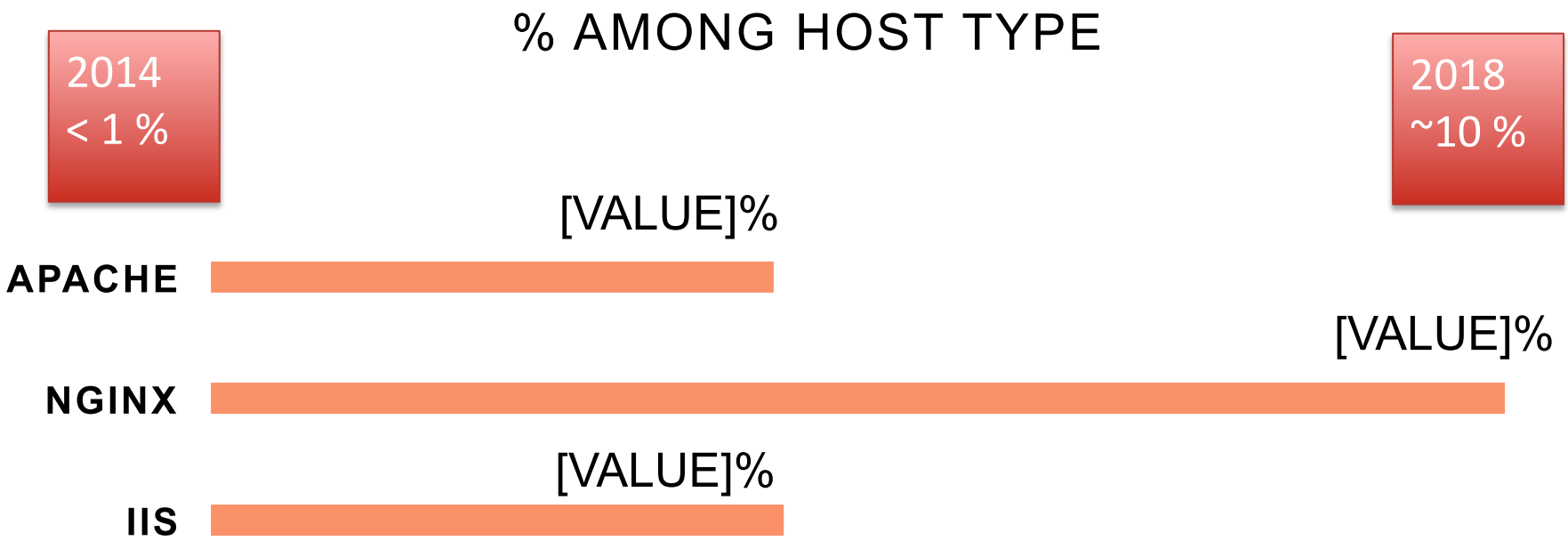
HSTS, LET'S ENCRYPT, AND LET'S NOT PIN

Maximize your TLS Security Posture

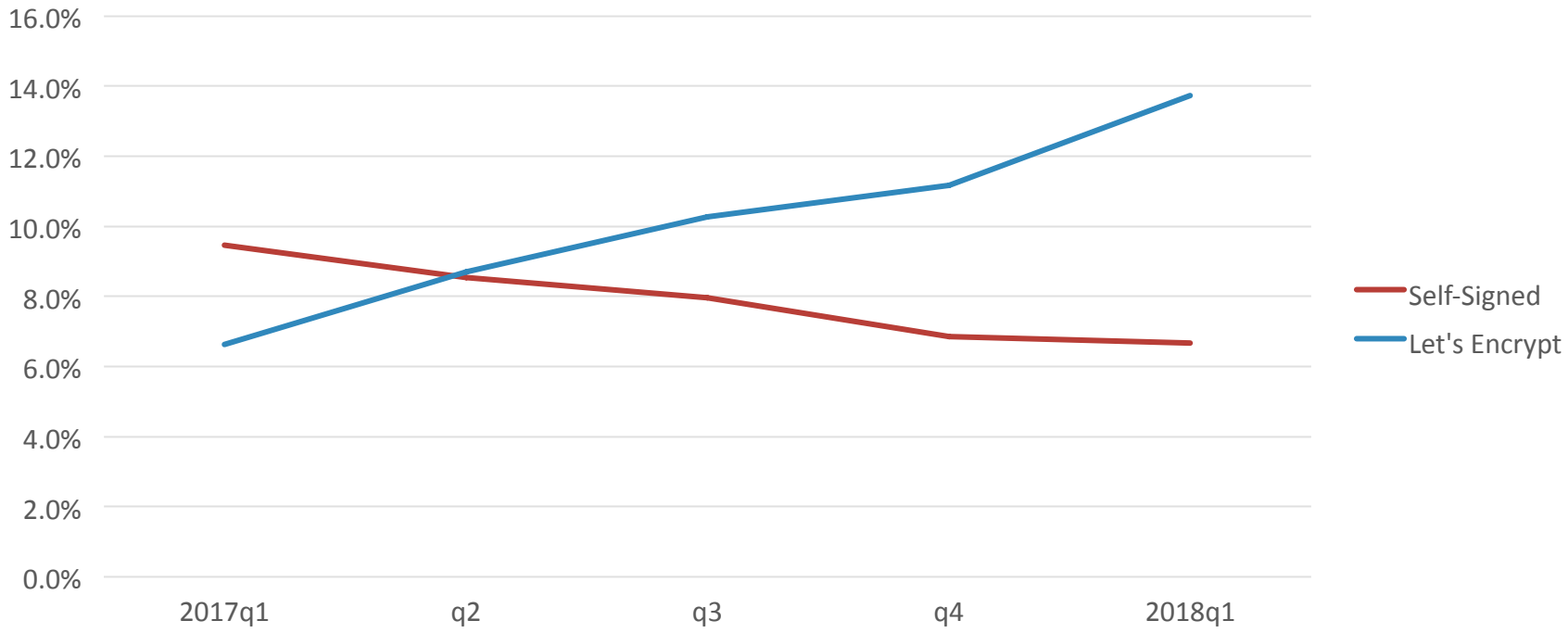
HTTP Strict Transport Security

2014
< 1 %

2018
~10 %



Self-Signed vs. Let's Encrypt



Certificate Pinning is Dead! Except for apps

Ryan Sleevi
@sleevi_

Following

Replying to @mnot

But pinning is terrible - and harms the ecosystem more than helps, as we've seen. It was a bad thing to standardize 😔

10:12 PM - 23 Aug 2017

4 Retweets **24** Likes

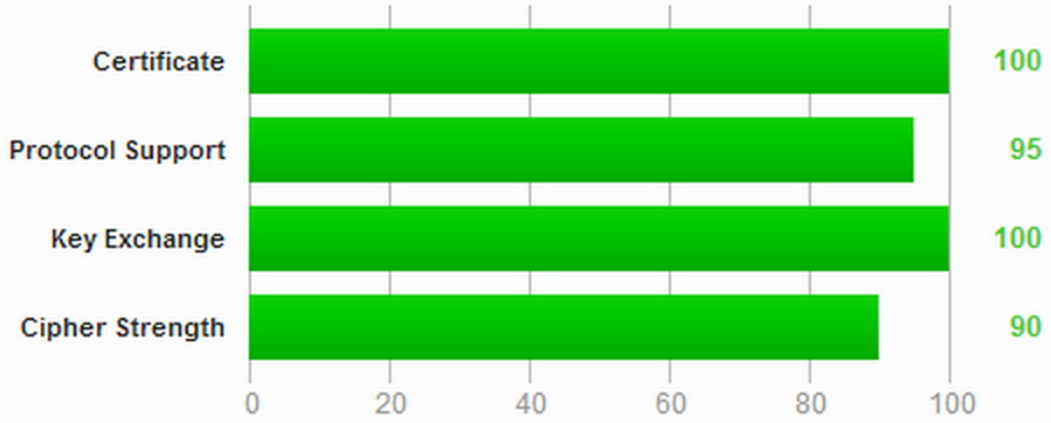
CALL TO ACTION

how to improve your TLS security

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server is not vulnerable to the Heartbleed attack. (Experimental)

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Qualys SSL Labs Server Test

Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: www.f5.com Submit

Do not show the results on the boards

Recently Seen

Recent Best

livetest.montagetalent.com	A+
ikm22.usoncology.com	A

Recent Worst

A
A
A-
A-
A-
B
B
B
B
B
B
B
B
B
B
B
B
C
F
F
F

Apply!

- Go back to work and see what your Qualys Grade is
  - I've found this OpenSSL string pretty helpful for getting an A+
  - '!DHE+AES-GCM:!DHE+AES:!DHE+3DES:ECDHE+AES-GCM:ECDHE+AES:RSA+AES-GCM:RSA+AES:!ECDHE+3DES:!RSA+3DES:-MD5:-SSLv3:-RC4'
  - Don't forget you have to enable HSTS or you only get A
- Go check out hardenize – in beta so maybe it's still free!

@dholmesf5


EDIT & SEND

Hardenize

HOME FEATURES DASHBOARDS BLOG ABOUT

We'll help you to deploy the security standards you need

With so many security features to deploy and services to configure, most organizations struggle to understand where they are, security-wise, and where they need to be. Things break. Our continuous monitoring service keeps an eye on your properties and enables you to have exactly the security you want.

Try our public report against your domain name:

e.g., www.hardenize.com RUN

feistyduck.c

14 Mar 2017 12:52 UTC

Domain

- ✔ Name servers
- ✖ DNSSEC
- ✖ CAA

Email

SECURE TRANSPORT (SMTP)

- ✔ TLS

Apply (more)!

- It's 2018: Encrypt Everything! HTTPS Everywhere
- Stop using self-signed certs: see Let's Encrypt at the very least.
- Forget pinning, see new "Expect-CT" header
- Turn on OCSP Stapling, (and see OCSP Multi-Stapling)!
- Go search censys.io for your org's certificates.
  - (or ones that were mis-issued).
- If you want to build a scanner, contact me
  - Source here: https://github.com/capmblade/dwh-tls-scan.git

Resources

Improve SSL/TLS Posture

- Hardenize!
- Qualys SSL Scanner
- Certificate Transparency
- SSL/TLS Best Practices
- SecurityHeaders.io

Scanning Resources

- 2017 TLS Telemetry Report (this data!)
- My Scanner on github
- Censys.io
- Project Sonar SSL/TLS Hosts
- Zmap Scanning Best Practices

MORE SCANNER CONSTRUCTION NOTES

(time permitting)

Towards a Complete View of the Certificate Ecosystem

Benjamin VanderSloot[†] Johanna Amann[‡] Matthew Bernhard[†]
Zakir Durumeric[†‡] Michael Bailey[§] J. Alex Halderman[‡]

[†]University of Michigan [‡]International Computer Science Inst. [§]Univ. of Illinois Urbana-Champaign
{benvds, matber, zakir, jhalderm}@umich.edu, johanna@icir.org, mdbailey@illinois.edu

ABSTRACT

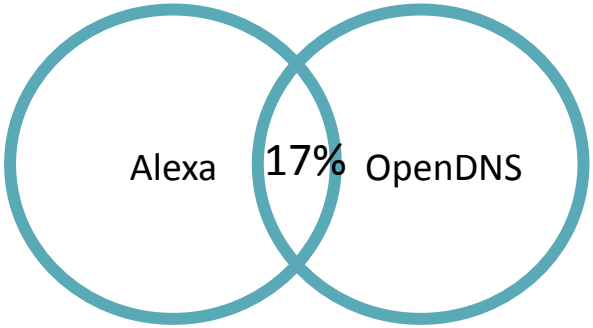
The HTTPS certificate ecosystem has been of great interest to the measurement and security communities. Without any ground truth, researchers have attempted to study this PKI from a variety of fragmented perspectives, including passively monitored networks, scans of the popular domains or the IPv4 address space, search engines such as Censys, and Certificate Transparency (CT) logs. In this work, we comparatively analyze all these perspectives. We find that aggregated CT logs and Censys snapshots have many properties that complement each other, and that together they encompass over 99% of all certificates found by any of these

tem. Instead, researchers have attempted to gain visibility into it using various fragmentary perspectives—such as scanning the IPv4 address space [12], querying popular Alexa domains, passively monitoring network traffic [3], and querying Certificate Transparency (CT) logs [20, 21]. Each methodology provides an imperfect view of the world, yet there has been little work to analyze how they differ or how they might be combined to piece together a more comprehensive picture.

Consider, for example, the different perspectives provided by CT logs and the Censys search engine [8], two widely used sources of certificate data. CT is designed to enable auditing of trusted certificates by recording them in publicly

Better Source Data?

- To get around the ServerNameIndicator problem, need hostnames.
- Amazon still published Alexa Top 1M. Accuracy in question.
- OpenDNS publishes their own Top 1M. Includes all 'bot' traffic tho.
- Whatever, just combine them. About 670,000 listen on port 443.

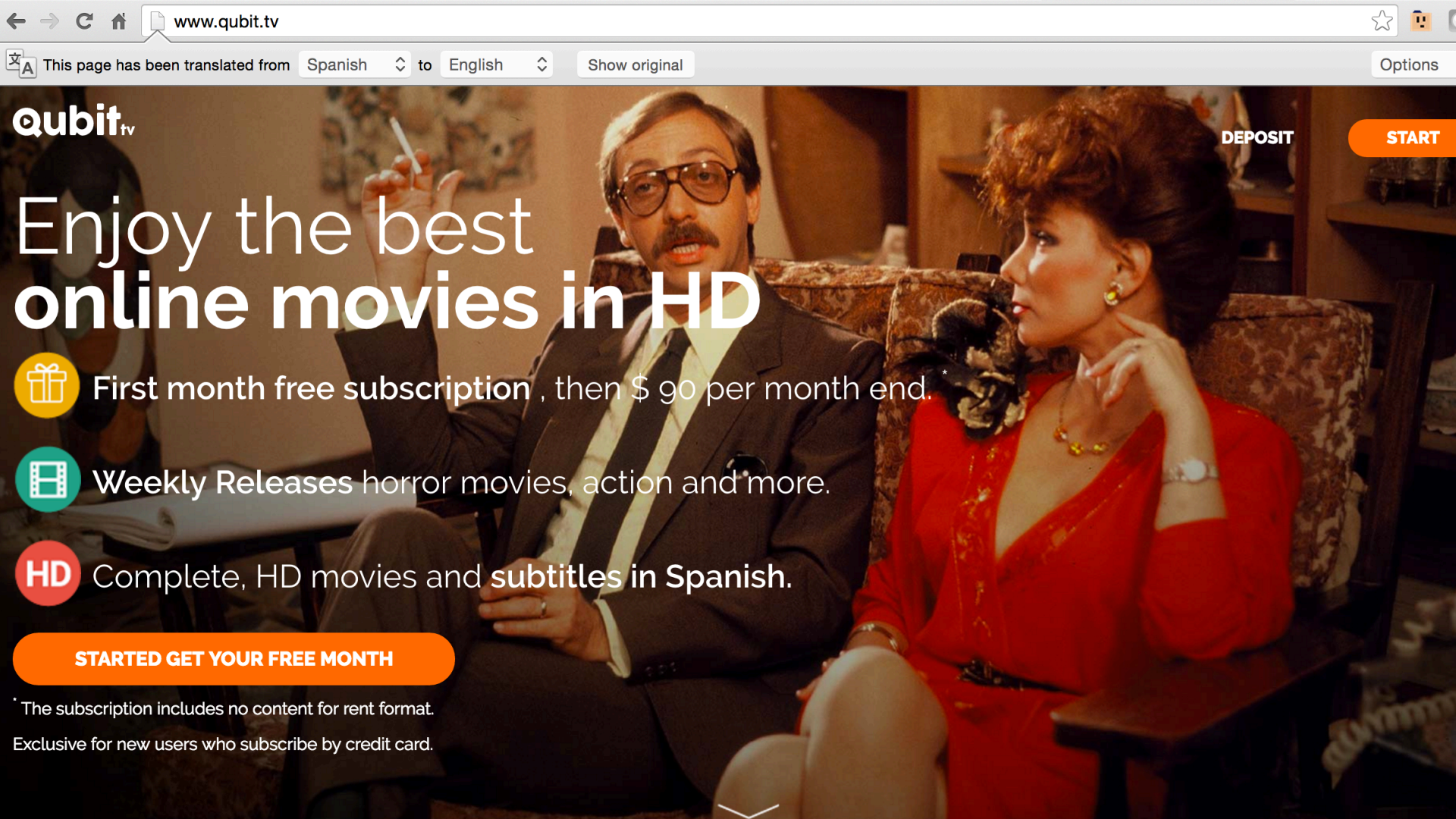


Moved from my basement to AWS

- AWS graciously allows me to do this scan
  - Request permission before each.
  - Provide instance IDs
  - Parallelize scan for faster
- One Database, multiple scanning nodes
  - Nodes divide work by alexa rank, how cute is that.
  - Be sure you resolve hostnames to addresses before starting.
  - Otherwise you'll get round-robined.
- Replace MySQL with PostGreSQL

Akamai Anomaly?


```
+----------+---------------------+
| COUNT(1) | ssl_server_string   |
+----------+---------------------+
|  1263256 | AkamaiGHost         |
|        1 | Akamai/Time Server  |
+----------+---------------------+
 2 rows in set (1 min 47.28 sec)
```


www.qubit.tv
This page has been translated from Spanish to English
Show original
Options
Qubit tv
DEPOSIT
START
Enjoy the best
online movies in HD
First month free subscription , then $ 90 per month end.*
Weekly Releases horror movies, action and more.
HD
Complete, HD movies and subtitles in Spanish.
STARTED GET YOUR FREE MONTH
* The subscription includes no content for rent format.
Exclusive for new users who subscribe by credit card.

Your Amazon EC2 Abuse Report [15802925499]

Amazon EC2 Abuse

Sent: Monday, June 13, 2016 at 7:19 AM

To: ***AWS-274-MarketingSolutions**

Hello,

You have outstanding reports against your EC2 instance(s) and we are notifying you that we have investigated and observed abusive activity. We last contacted you about this on [2016/06/10] and have not received a reply. Details of the implicated instance(s) are below:

Reported activity: Port Scanning
Instance ID: i-89a2bc4c

Please review these reports and respond with details of the action(s) you have taken to stop the abusive activity. If you do not consider the activity detailed in these reports to be abusive, please let us know why. The original reports are included at the end of this email for your convenience.

Please note that your reply is required within [24/48] hours. According to the terms of the AWS Customer Agreement (http://aws.amazon.com/agreement/), if your instances continue to violate AWS's Acceptable Use Policy (http://aws.amazon.com/aup/), we may take action against your resources or account to stop the abusive activity, including suspension or termination of your AWS account.

THANK YOU RSA 2018!