DMARC and Email Authentication Update

Steven M Jones

Senior Systems Engineer, LinkedIn

Executive Director, DMARC.org

JPAAWG Meeting

Tokyo, Japan

November 8th, 2018

Topics

- Standards and Protocols Update
- Government Policy Update
- Use and Adoption Update

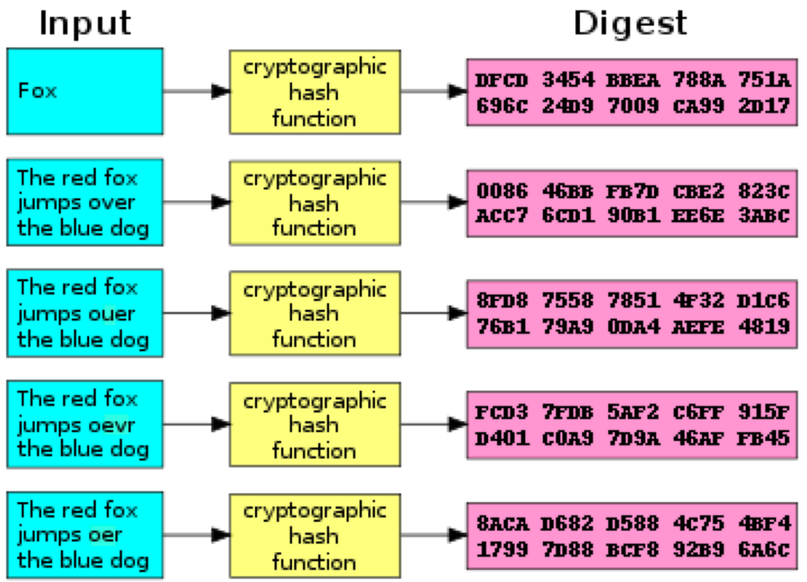
Standards and Protocols

Standards and Protocols Update

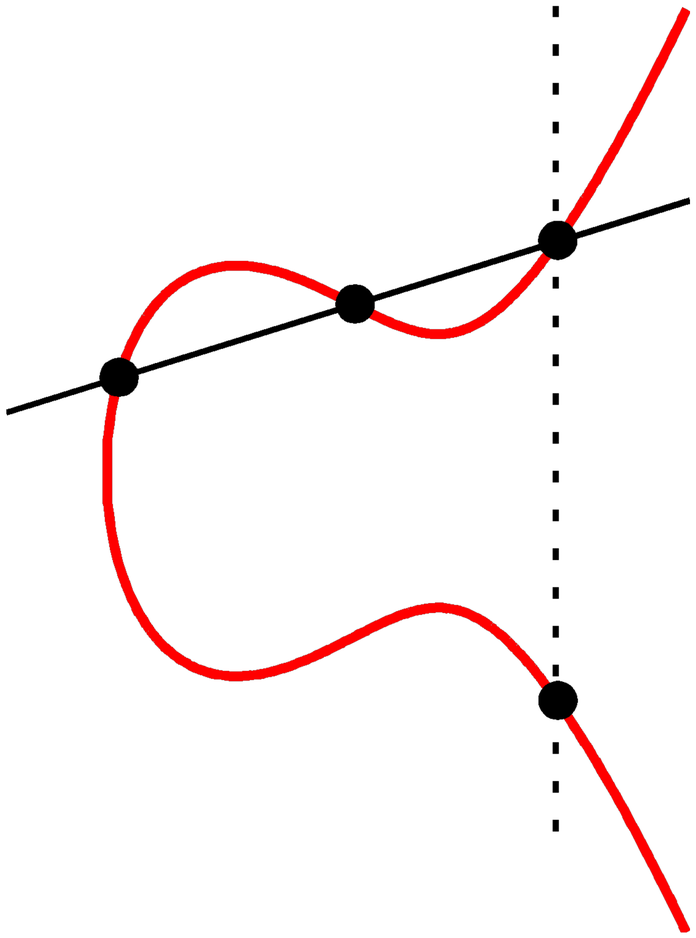
- New cryptographic guidelines for DKIM
- Developments with the ARC protocol
- DMARC, Organizational Domains, and Registrars

Changes in DKIM Cryptography (RFC 8301)

- RFC 4871(2007) allowed SHA-1 and SHA-256 hashes
- SHA-1 hash is deprecated (RFC 6194) and must not be used
- Minimum RSA key length increased to 1,024 bits
- Receivers must support key lengths of 1,024 – 4,096 bits; larger keys optional



Changes in DKIM Cryptography (RFC 8463)



- RSA algorithm is being deprecated under RFC 8017
- Elliptic Curve signing algorithm standardized under RFC 8031
- DKIM may now use PureEdDSA variant Ed25519
- Smaller keys for equivalent strength

Comparing DKIM Keys

- DKIM key record for 2,048 bit RSA key

```
test._domainkey.football.example.com. IN TXT (
    "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDkHlOQoBTzWR”
    "iGs5V6NpP3idY6Wk08a5qhdR6wy5bdOKb2jLQiY/J16JYi0Qvx/byYzCNb3W91y3FutAC”
    "DfzwQ/BC/e/8uBsCR+yz1Lxj+PL6lHvqMKrM3rG4hstT5QjvHO9PzoxZyVYLzBfO2EeC3”
    "Ip3G+2kryOTIKT+l/K4w3QIDAQAB” )
```

- DKIM key record for 256 bit Ed25519 key

```
brisbane._domainkey.football.example.com. IN TXT (
    "v=DKIM1; k=ed25519; p=11qYAYKxCrfVS/7TyWQHOg7hcvPapiMlrwIaaPcHURo=” )
```

Comparing DKIM Signatures

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=football.example.com; i=@football.example.com;
    q=dns/txt; s=test; t=1528637909; h=from : to : subject :
    date : message-id : from : subject : date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=F45dVWDfMbQDGHJFlXUNB2HKfbCeLRyhDXgFpEL8GwpsRe0IeIixNTe3
    DhCVlUrSjV4BwcVcOF6+FF3Zo9Rpo1tFOeS9mPYQTnGdaSGsgeefOsk2Jz
    dA+L10TeYt9BgDfQNZtKdN1WO//KgIqXP7OdEFE4LjFYNcUxZQ4FADY+8=
```

DKIM signature using 2,048 bit RSA

```
DKIM-Signature: v=1; a=ed25519-sha256; c=relaxed/relaxed;
    d=football.example.com; i=@football.example.com; q=dns/txt;
    s=brisbane; t=1528637909; h=from : to : subject : date :
    message-id : from : subject : date;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=/gCrinpcQOoIfuHNQIbq4pgh9kyIK3AQUdt9OdqQehSwhEIug4D11Bus
    Fa3bT3FY5OsU7ZbnKELq+eXdp1Q1Dw==
```

DKIM signature for a 256 bit Ed25519

RFC 7601bis – Authentication-Results:

- Some changes to Authentication-Results: header needed
  - Not necessarily for DMARC or ARC
- Clarifications for Email Address Internationalization (EAI)
- DKIM results can capture signing algorithm (`header.a`)
- DKIM results can record the selector/key used (`header.s`)

ARC Protocol

- ARC assists with authentication of indirect mailflows
- ARC Protocol in review for publication
- Some feedback from IETF leadership
- On track for publication and RFC number assignment

ARC Protocol

- Draft 18: Clarification of handling for invalid chains – lowers overhead
- Draft 19: Sample messages added, minor corrections
- Draft 20: Correct the status of the ARC header fields
- Draft 21: Clarify SMTP error codes to use when ARC fails to validate

ARC Protocol

- Additional ARC documents in IETF DMARC working group
- `ietf-draft-dmarc-arc-multi`
  - How to allow multiple signing algorithms
  - Needed to allow adoption of Elliptical Curve (Ed25519)
- `ietf-draft-dmarc-arc-usage`
  - How receivers and intermediaries can/should use ARC

ARC Protocol

- OpenARC (FOSS reference implementation) nearing v1.0
- Many packages/vendors implementing ARC
- GMail and Google Groups the largest service
- Testing exercise held in New York in October

DMARC, Top-Level Domains, and Registrars

- Allow for DMARC to be applied at ccTLD, like .uk or .jp
- Also cover intermediate domains, ex. gov.uk
- Allow TLDs to have a DMARC policy for non-existent domains, like .bank or .insurance
  - These TLDs require all registrants to publish DMARC
  - Non-existent domains leave a gap in protection
- New proposal presented at M3AAWG 44 (Brooklyn, NY)

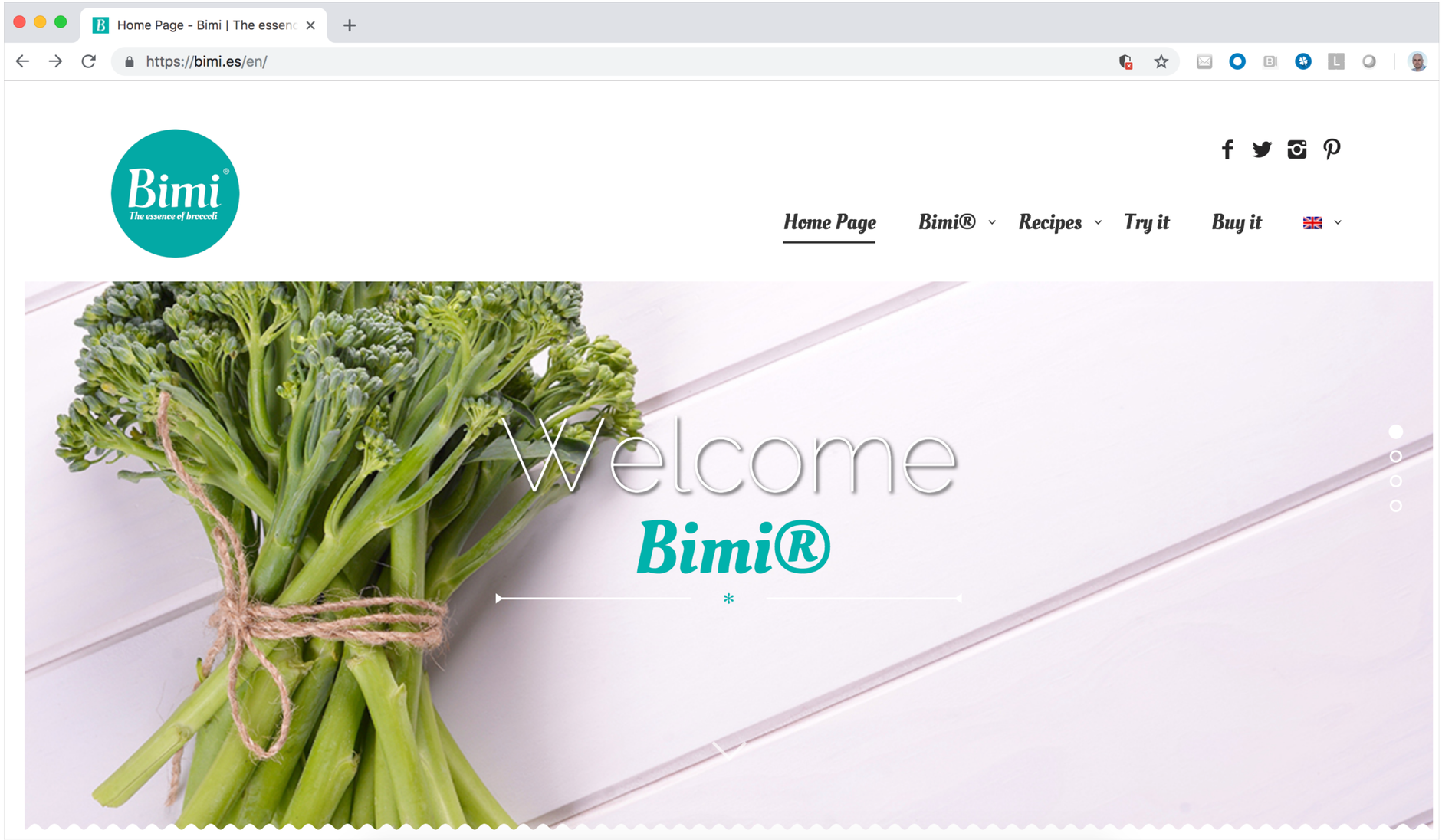
Things That Do Not (Yet?) Depend on DMARC

- Yahoo Japan displays logos with authenticated messages
  - Authentication method is DKIM
  - Relies on private registry
  - Perhaps similar to service by 1&1 / GMX.de in Germany

Things That Depend on DMARC

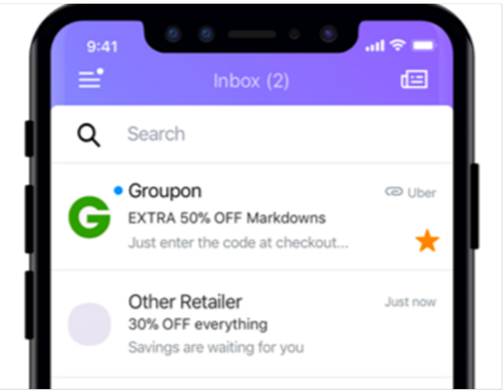
- Brand Indicators for Message Identification (BIMI)

BIMI?


Home Page - Bimi | The essenc
https://bimi.es/en/
Bimi
The essence of broccoli
Home Page
Bimi®
Recipes
Try it
Buy it
Welcome
Bimi®

BIMI

- Brand Indicators for Message Identification (BIMI)
- Email services (ex. Yahoo US) or programs (ex. Outlook) would show company logo with messages
- Relies on DMARC and third parties known as Mark Verifying Authorities (MVA)
- Trial running with Yahoo US `https://www.brandindicators.org`



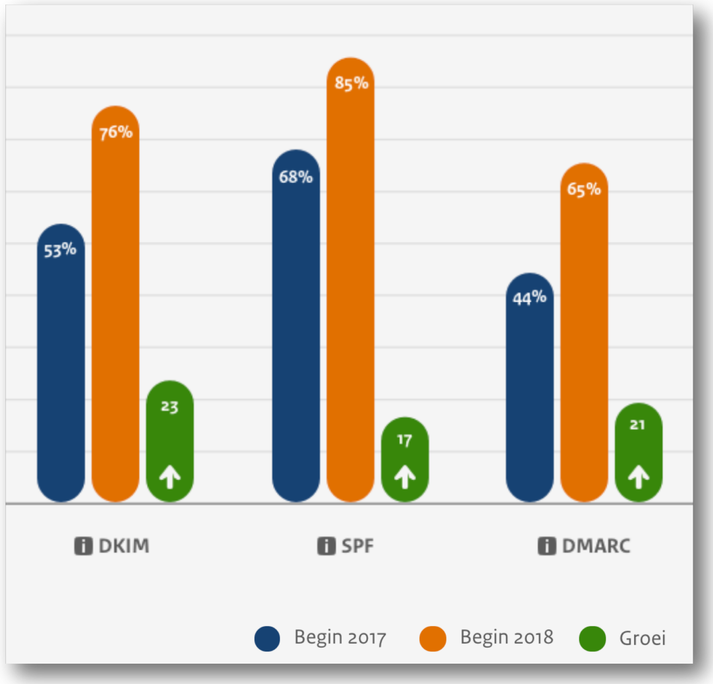
Government Policy Update

Government Policy Update

- Dutch Government
- United States Federal Government
- United Kingdom Government

Dutch Government Policy

- Early adopter of email authentication
  - DKIM required in 2015
  - DMARC required in 2017
- April 2018: Strict DMARC and SPF policies required for all agencies by the end of 2019



US Government Policy

- Department of Homeland Security
  Binding Operational Directive 18-01
  - Agencies must have DMARC “p=reject” by **Oct 16th, 2018**
  - October 2017: 18-20% have a DMARC policy
  - October 2018: 74-85% have a DMARC policy
    - 60-74% are fully compliant, with DMARC reject policy

❖ Different statistics provided by different vendor surveys

US Government Policy

- Securities and Exchange Commission investigation of Business Email Compromise (BEC)
- Nine companies studied, total losses of US$100 million
- October 16: SEC directs all companies it supervises to implement effective controls against these threats
- Effectively increasing pressure on the financial sector to implement measures like DMARC

UK Government Policy

- UK NCSC sets direction for government agencies
- Improving security from national to local gov’t agencies
- Set example for private companies to follow
- DMARC: 4.5MM messages/month blocked in first year

  `https://www.ncsc.gov.uk/information/active-cyber-defence-one-year`

- Mail Check tools released as open source

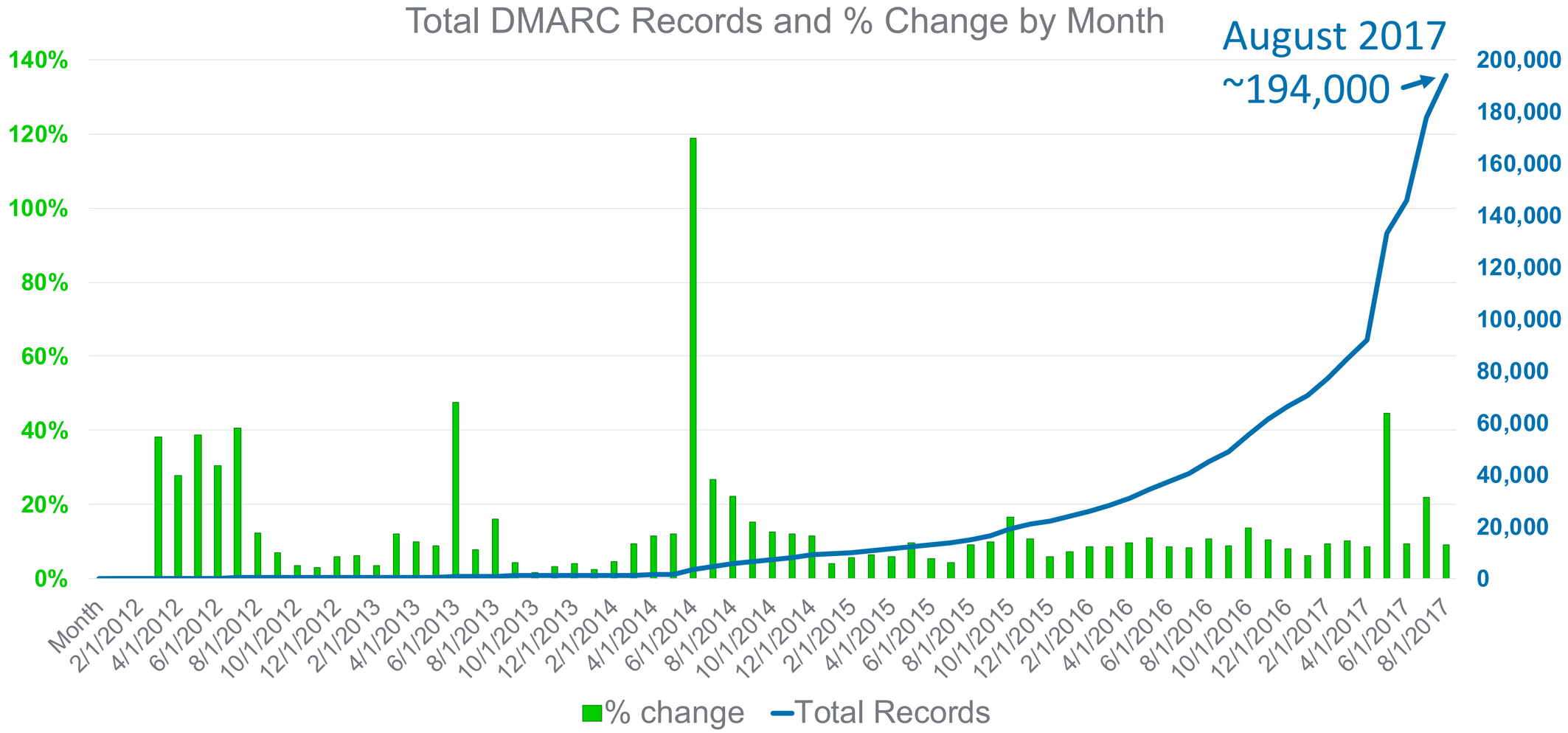
  `https://github.com/ukncsc/mail-check`

Use and Adoption Update

Use of DMARC – ROI Study

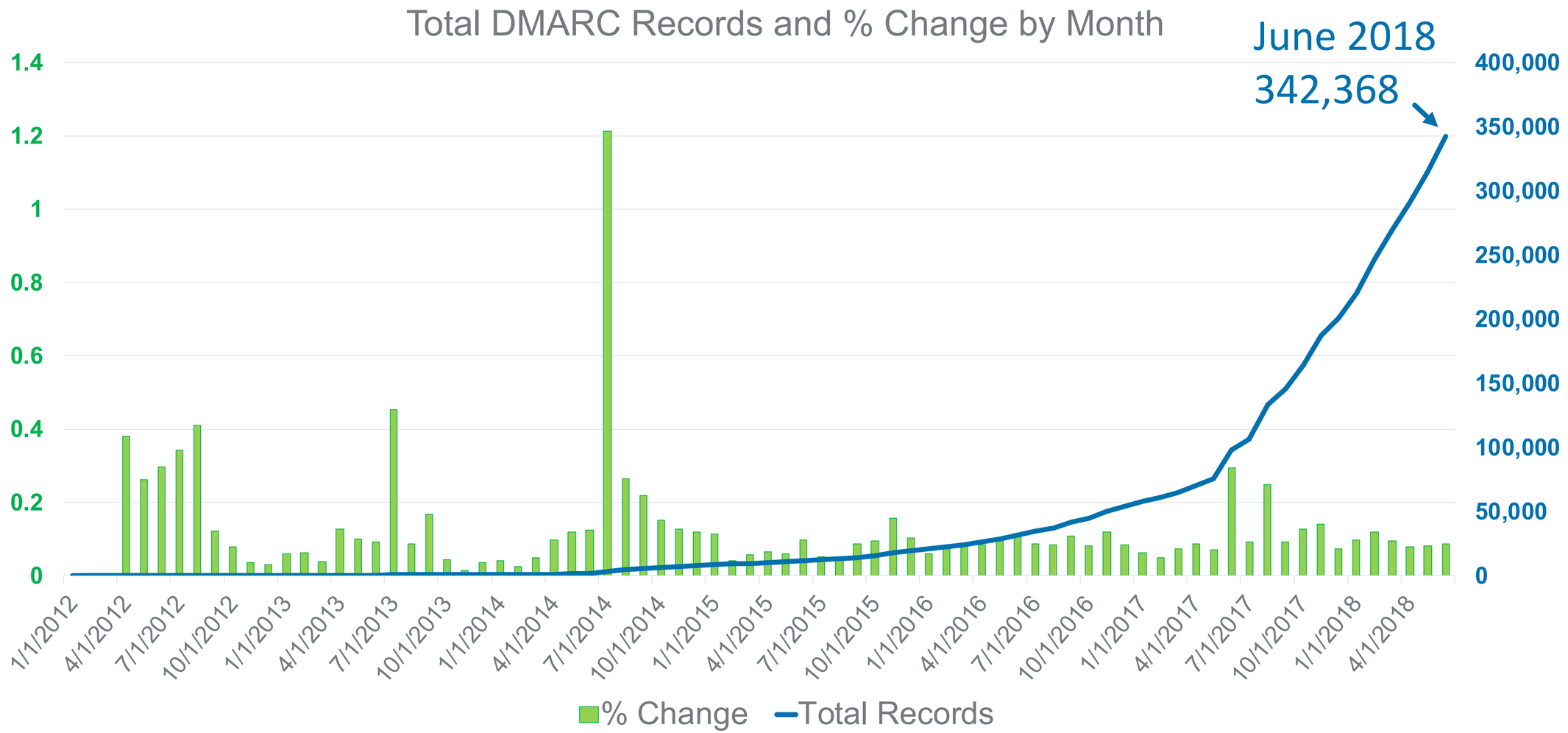
- Global Cyber Alliance study of Business Email Compromise (BEC)
- Tracking 1,046 organizations with “quarantine” or “reject” policies
- Conservative estimate that these companies avoided US$19M for the year
  - More aggressive assumptions, $66M

Growth of DMARC Adoption Globally – 3Q 2017



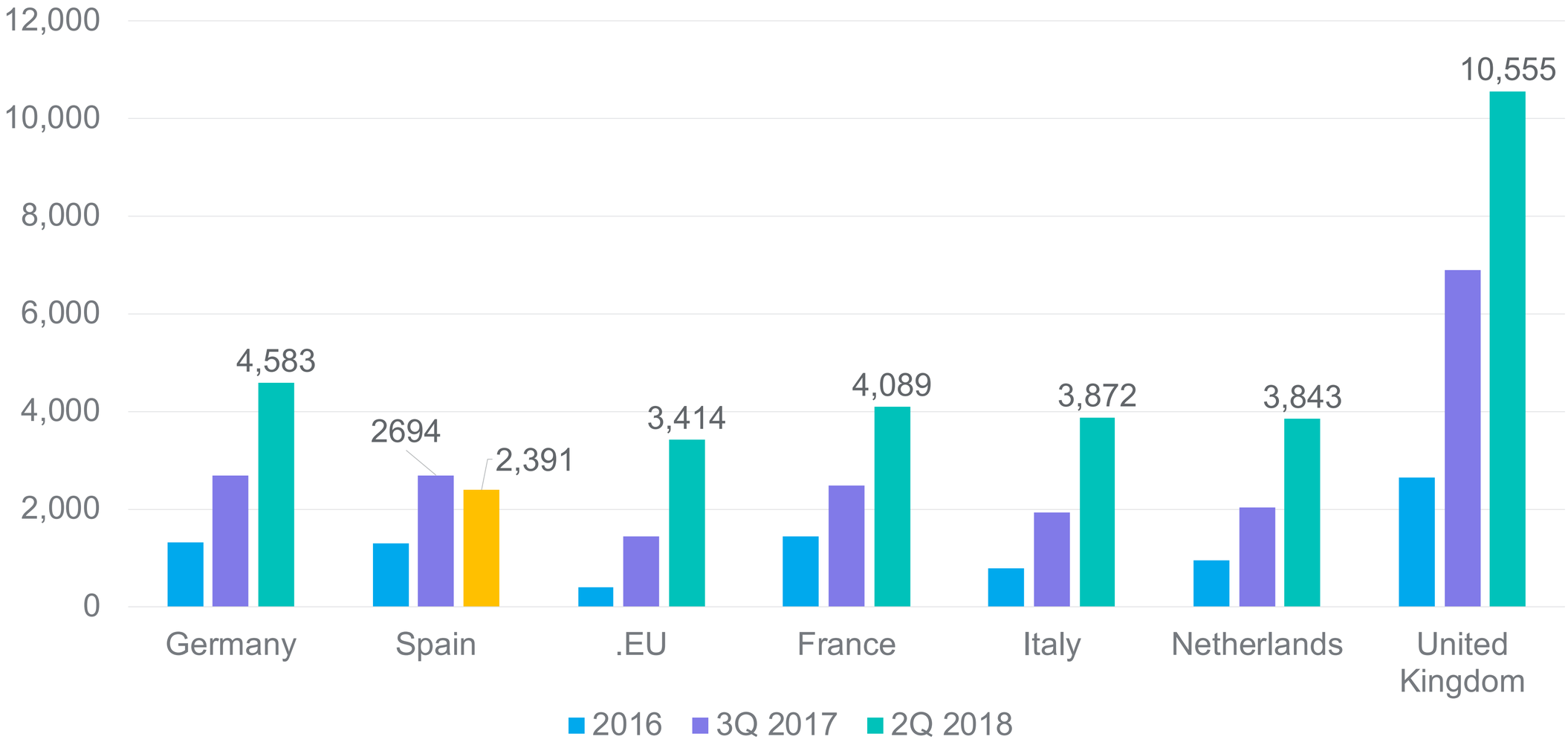
Data provided by Farsight Security

Growth of DMARC Adoption Globally – 2Q 2018



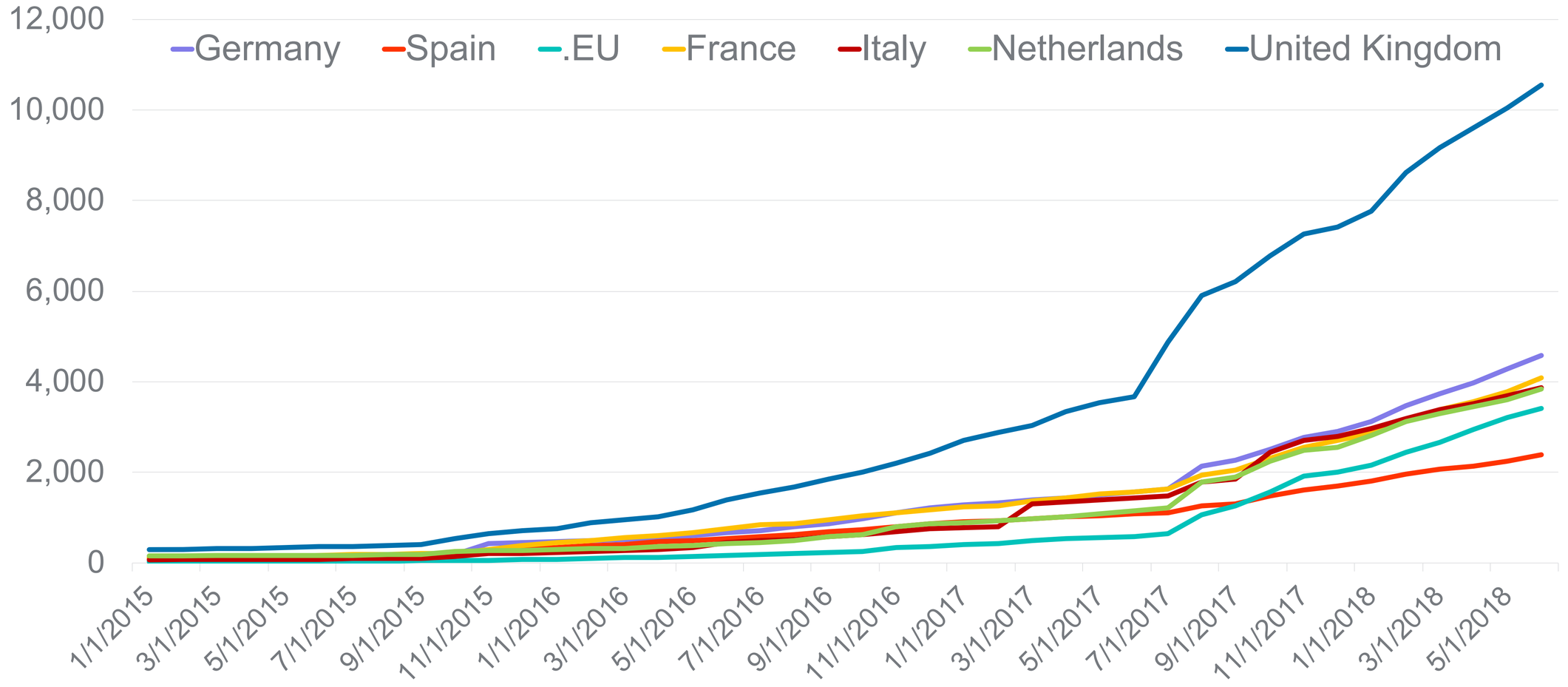
Data provided by Farsight Security

Active DMARC Records in Euro ccTLDs



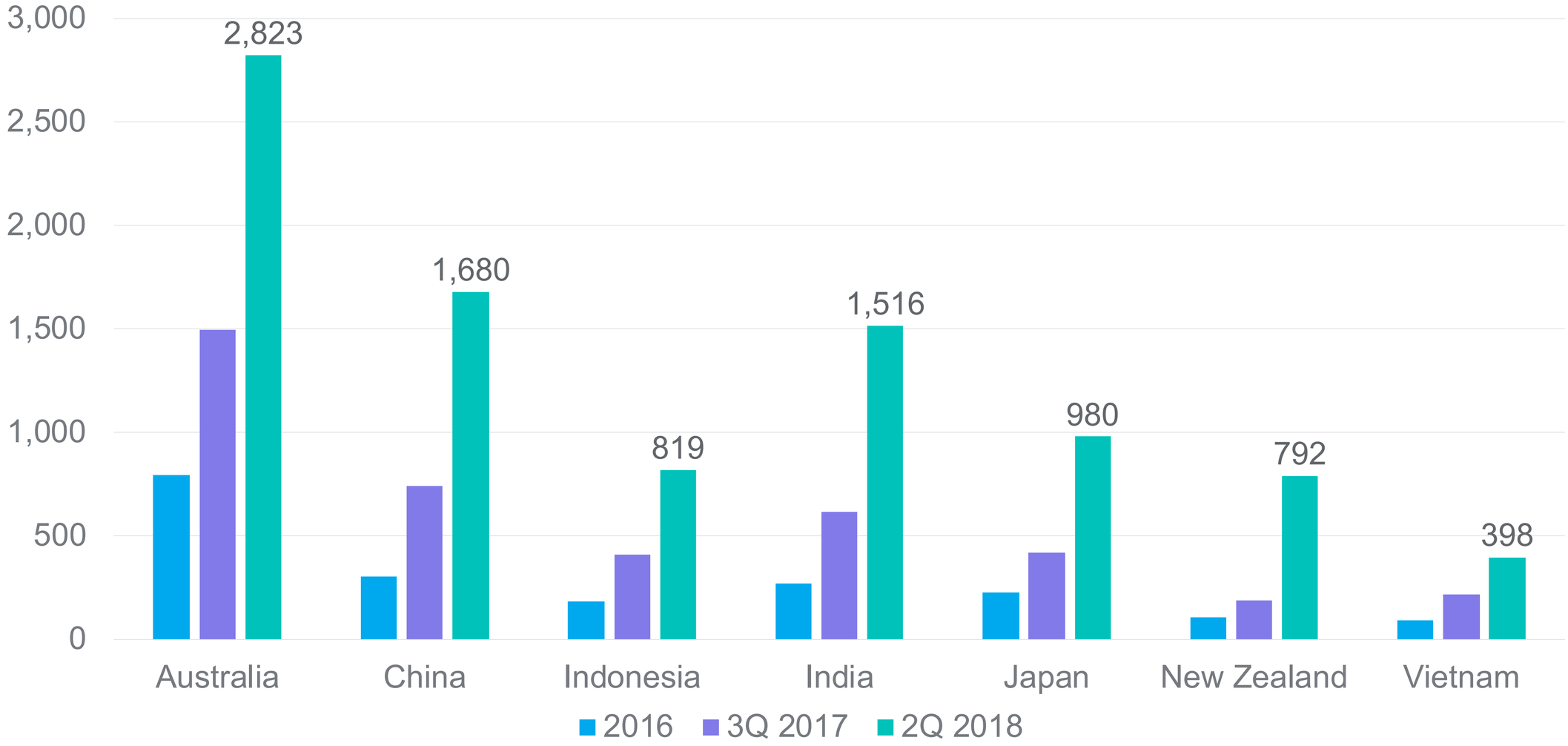
Data provided by Farsight Security

Active DMARC Records in European ccTLDs – 2Q 2018



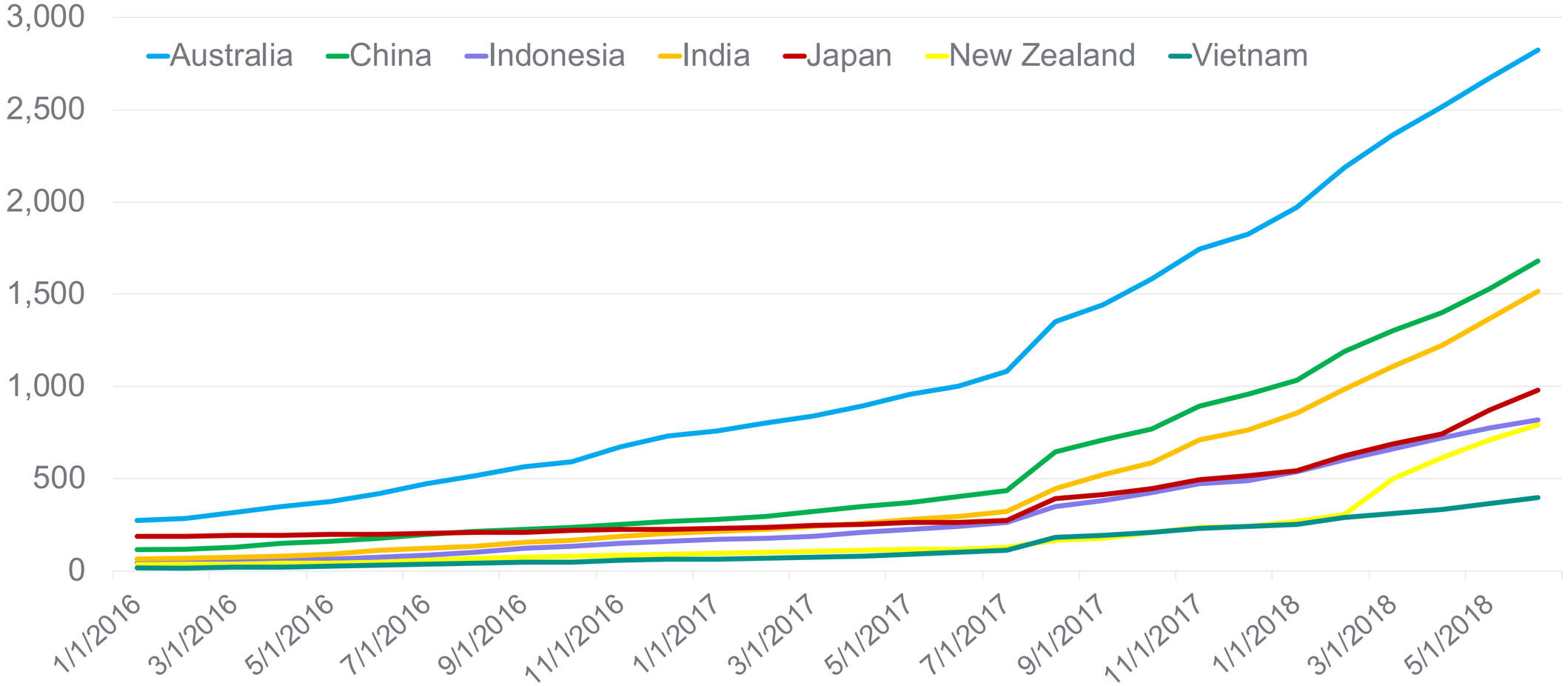
Data provided by Farsight Security

Active DMARC Records in Asia ccTLDs



Data provided by Farsight Security

Active DMARC Records in Asian ccTLDs – 2Q 2018



Data provided by Farsight Security

Q & A

ありがとうございました

Thank you

Speaker

http://linkedin.com/in/stevenmjones

- Engineer at Sendmail, Inc.
- IT Architect for 10 years at Bank of America
  - Regular attendee at M3AAWG Meetings
  - Part of original DMARC industry group
- Executive Director of DMARC.org since 2015
- Joined LinkedIn Postmaster Team in 2017
  - LinkedIn also part of original DMARC group

References & Resources

Resources – UK Policies

February 2018: Active Cyber Defence - One Year On
https://www.ncsc.gov.uk/information/active-cyber-defence-one-year

November 2016: £1.9 billion national cyber security strategy
https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

October 2016: National Cyber Security Centre plans to create dashboard showing government department adoption of DMARC
https://www.publictechnology.net/articles/news/national-cyber-security-centre-publish-rankings-departmental-email-security

September2016: NCSC Chief outlines new, active approach
https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

June 2016: Cabinet Office requires DMARC & HTTP STS by Oct 1st
https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/

Resources – US Policies

October 2017: DHS Issues Binding Operational Directive 18 (BOD-18) re: DMARC, HTTPS
https://cyber.dhs.gov/
https://www.infosecurity-magazine.com/news/dhs-mandates-dmarc-https/

July 2017: US Senator Ron Wyden's Letter to DHS
https://www.wyden.senate.gov/download/letter-to-dhs-regarding-dmarc

March 2017: FTC - "Use Email Authentication"
https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication

April 2016: NIST Special Publication 800-177: Trustworthy Email
https://csrc.nist.gov/presentations/2016/nist-sp-800-177-trustworthy-email

Resources – Dutch and German Policies

Dutch government agencies must have strict DMARC & SPF policies by end of 2019
April 2018: https://www.forumstandaardisatie.nl/nieuws/nieuwe-adoptieafspraak-voor-informatieveiligheidstandaarden

German BSI recommends DMARC
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-098.html

eco.de / Certified Senders Alliance: DMARC is compatible with Germany's federal and state data privacy laws
https://e-mail.eco.de/wp-content/blogs.dir/26/files/eco_dmarc_legal_report.pdf

eco.de / Certified Senders Alliance: Members required to adopt strong authentication (DMARC)
https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Directive.pdf