JP AAWG Japan Anti-Abuse Working Group

Updates for DMARC and Related Technology

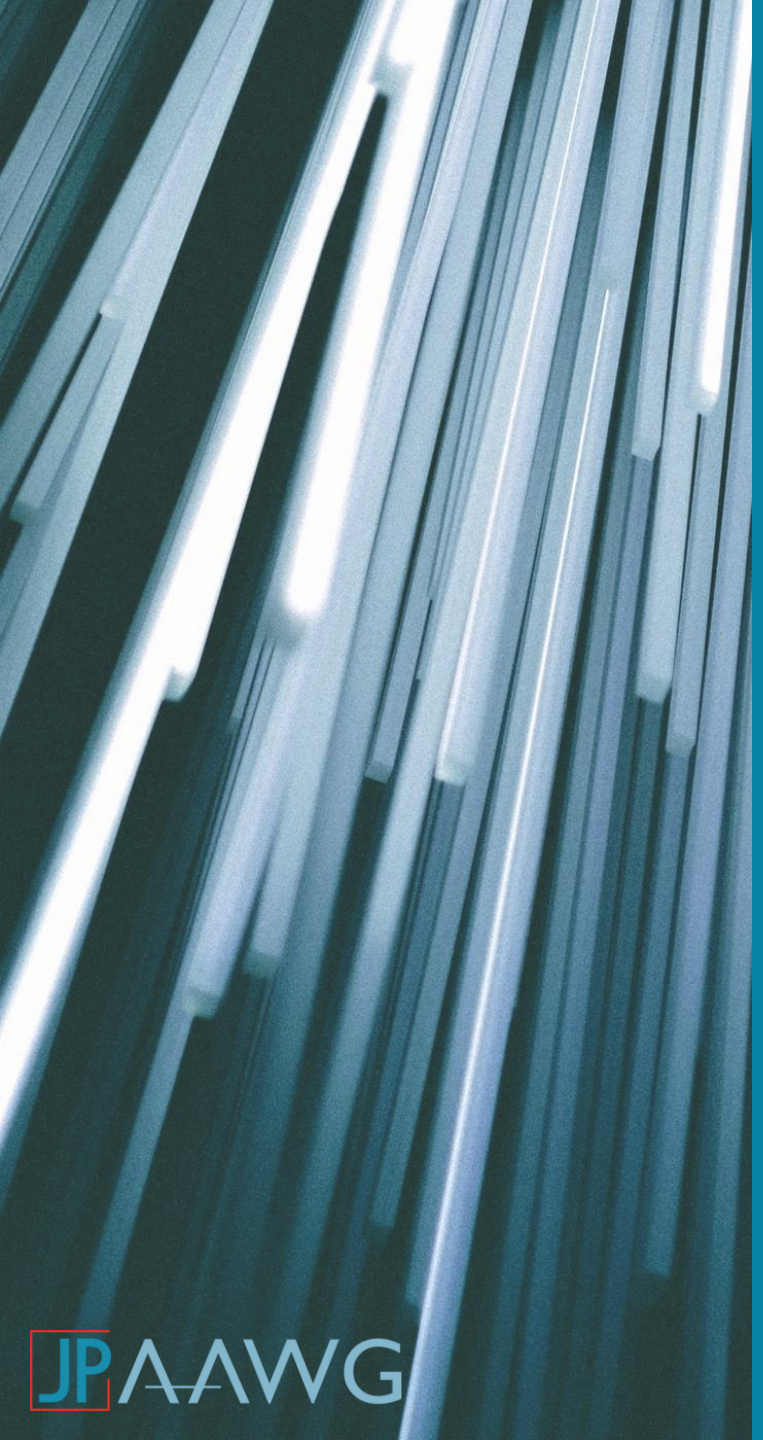
DMARC.org

Steven Jones

Topics

- IETF DMARC Working Group Activity
- IETF DKIM Working Group and DKIM Replay
- ARC Activity

- Some BIMI Statistics

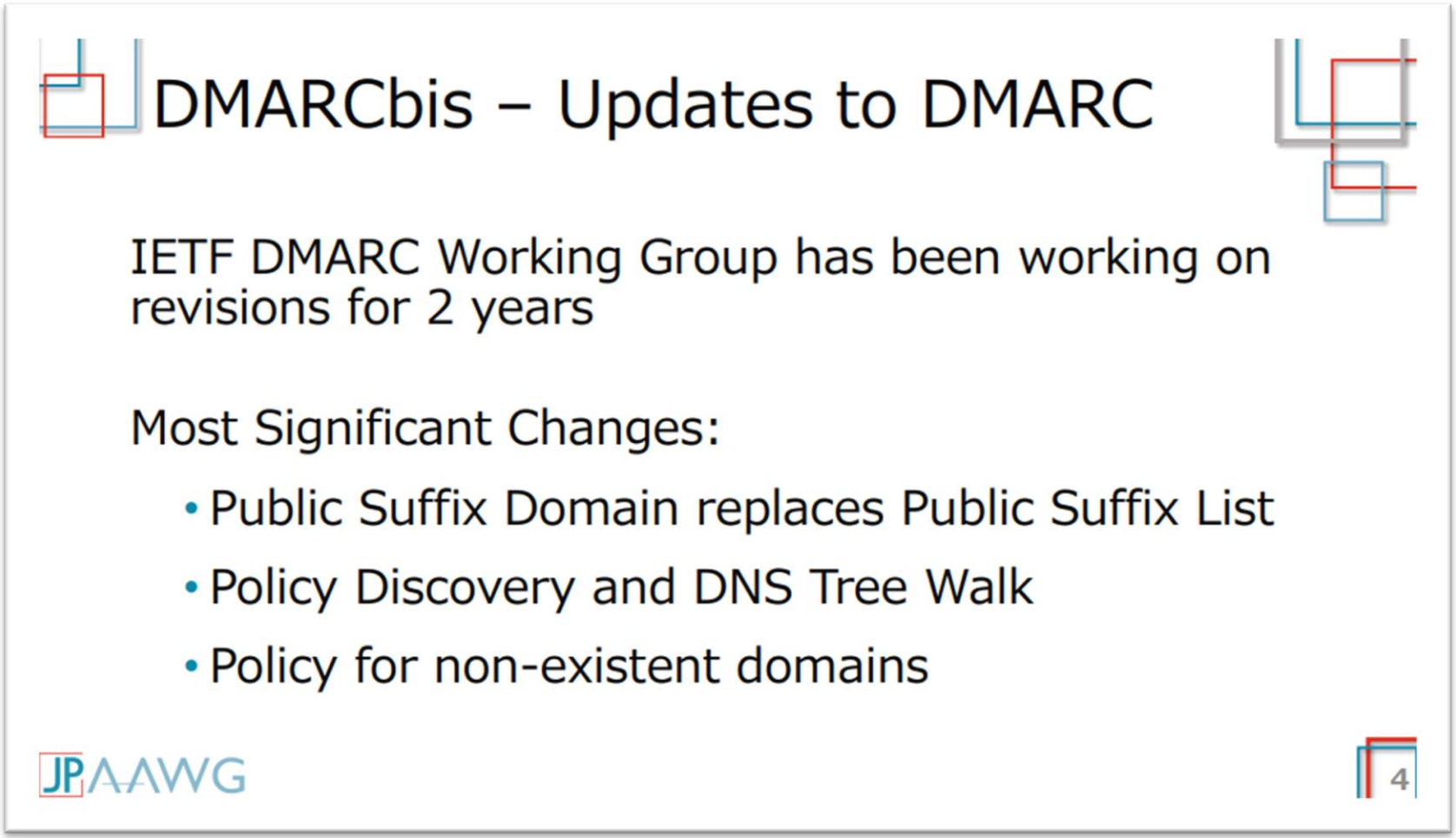


DMARC Working Group

JP AAWG

JPAAWG 5 and DMARCbis

JPAAWG 5 presentation: https://dmarc.org/presentations/JPAAWG-2022-Keynote-2.pdf



DMARC Working Group in 2023

- The DMARC Working Group was chartered in August 2014
- Documents produced:
  - 2015 3月 – RFC 7489 DMARC
  - ✓2016 9月 – RFC 7960 Interoperability Issues
  - 2019 5月 – RFC 8601 Authentication Results
  - 2019 6月 – RFC 8616 Authentication for i18n email
  - ✓2019 7月 – RFC 8617 ARC
  - 2021 7月 – RFC 9091 Public Suffix Domains
- Third goal was a revised DMARC protocol

DMARC Working Group in 2023

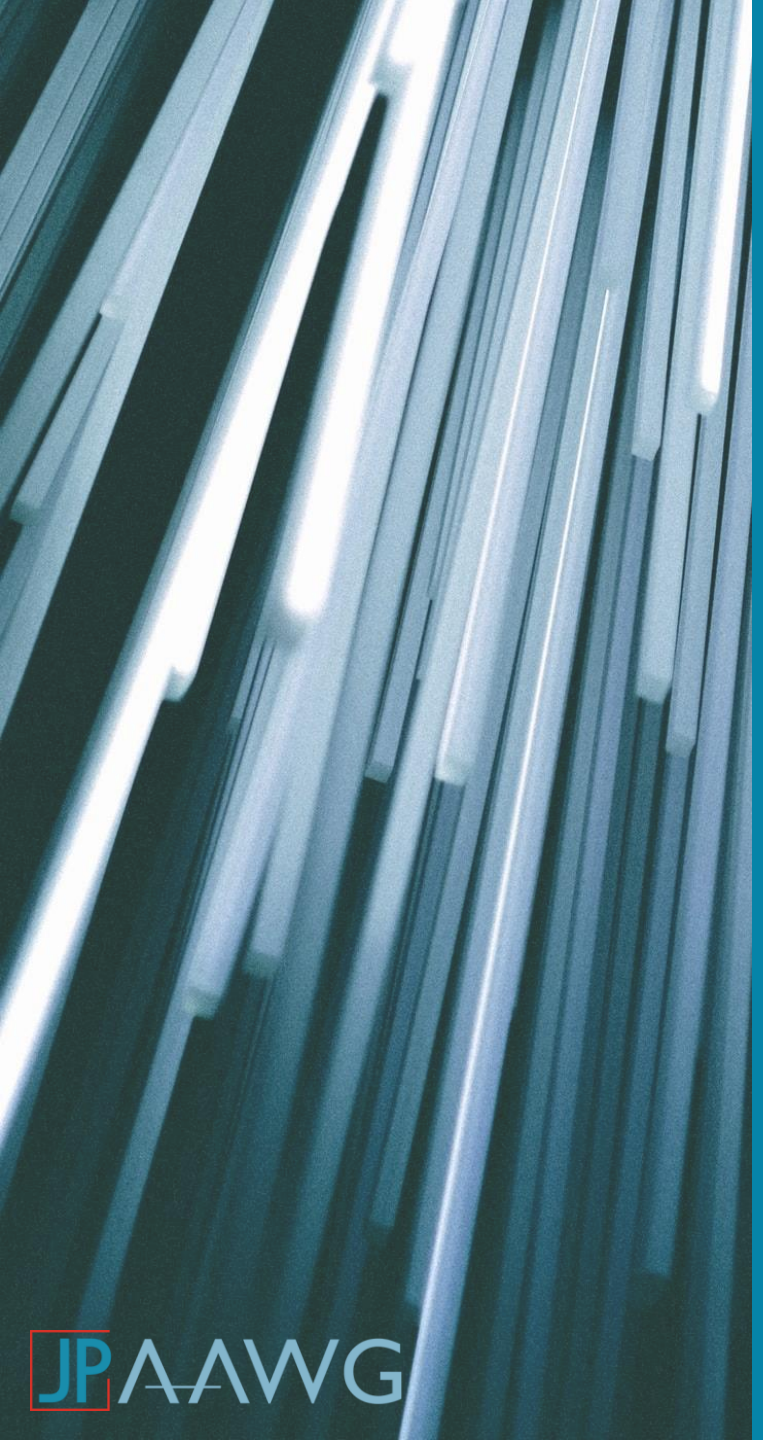
- “Most IETF WG do not take 9 years to deliver their primary document”
- Criticisms include “lookalike” domains, display name attacks, etc - which DMARC cannot fix
- Regressions and distractions have been frequent
  - With low participation, individuals can halt the group by revisiting old issues
- Current Area Director would like to see a finished document by 2024 3月

Does “Standards Track” Matter?

- Goal has been to make DMARC “Standards Track”
  - There is still push-back re: list/forwarding problems
- DMARC has been a de facto standard for 10 years because of global mailbox providers
  - Gmail, Hotmail (Microsoft), Yahoo (US) at launch
  - AOL and Yahoo (US) publishing “p=reject” in 2014
- GMail and Yahoo announced stricter email authentication requirements for 2024

SPF Will Continue in DMARC

- There was a request to remove SPF as a mechanism used in DMARC evaluations
- Argument: Too many bad and overly-broad SPF records requested by mailbox providers, ESPs, etc
  - Plus “SPF Upgrade” attacks via forwarding
- This request has been rejected
- Guidance will be included on ways to use SPF modifiers for vendors with shared IP addresses
  - `v=spf1 ?include:vendor-with-sharedIPs.com -all`
  - SPF gives a “neutral” result, DMARC ignores as a not-pass



DKIM Working Group

JP AAWG

DKIM Working Group & DKIM Replay

- Working Group has not agreed on a problem statement
- Work happening on technical proposals like DARA, Mailpath
- Report of DKIM Replay + SPF Upgrade observed – `ups.com`

DKIM Working Group & DKIM Replay

- Why isn't there a problem statement?
  - Replay activity shifts over time, not always happening at Internet scale for every receiver
  - Parties targeted for unique weaknesses
  - Individual senders/receivers implement counter measures, and their problem decreases
  - Some feeling that operational guidance ("best common practices" document) is enough

DKIM Replay - Countermeasures

- Limit the time each DKIM key and/or signature is valid
  - More frequent DKIM key rotation
  - Use the `x=` tag (expiration time) in DKIM signatures
- Always sign `From:`, `To:` and `Cc:` headers even if empty
  - Sign as many headers as you reasonably can
  - Review all header signing – `Date:`, `Reply-To:`, `Subject:`, etc
- Content scan messages sent from new/trial accounts
- Disallow pre-shortened links in messages
- Limit `To:` addresses for trial accounts

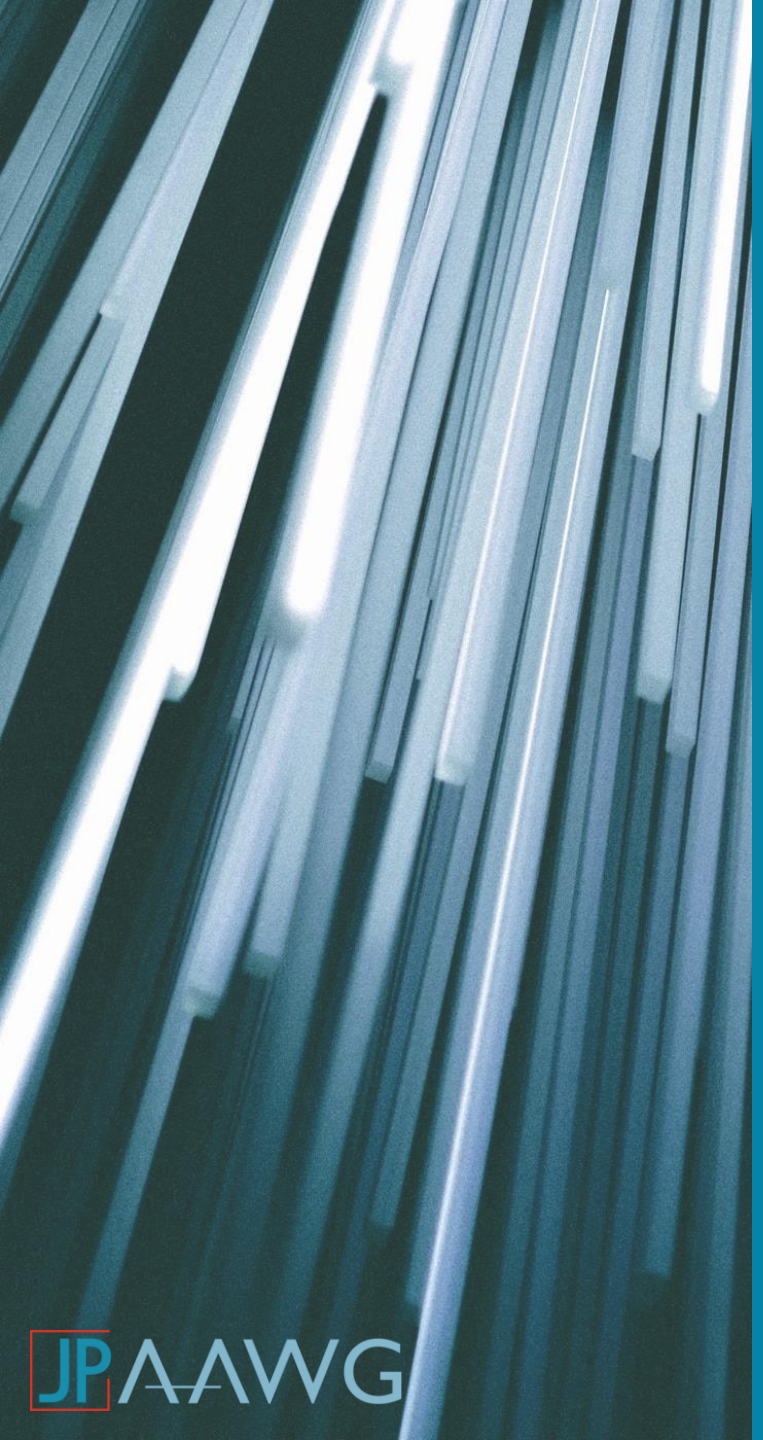
➢ Receivers: record hashes of DKIM signatures, possibly limit # of messages accepted using same signature

DKIM Replay Technical Proposals

- Kucherawy: Include Envelope in DKIM Signature
  - https://datatracker.ietf.org/doc/draft-kucherawy-dkim-anti-replay/
- Chuang: Replay Resistant ARC
  - https://datatracker.ietf.org/doc/draft-chuang-replay-resistant-arc/
- Bradshaw: DKIM Envelope Validation Extension
  - https://www.ietf.org/id/draft-bradshaw-envelope-validation-extension-dkim-00.html
- Gondwana: Mailpath, an Email Chain of Custody
  - https://datatracker.ietf.org/doc/draft-gondwana-email-mailpath

DKIM WG Next Steps

- Concern about level of participation in WG
  - M3AAWG Brooklyn, 10 volunteers to participate
- Complete the Problem Statement
  - Define impact of Replay attacks
  - Document mitigations for senders, receivers
- Decide if protocol/standards work is needed, or operational guidance is sufficient (BCP)



ARC Activity

ARC Activity

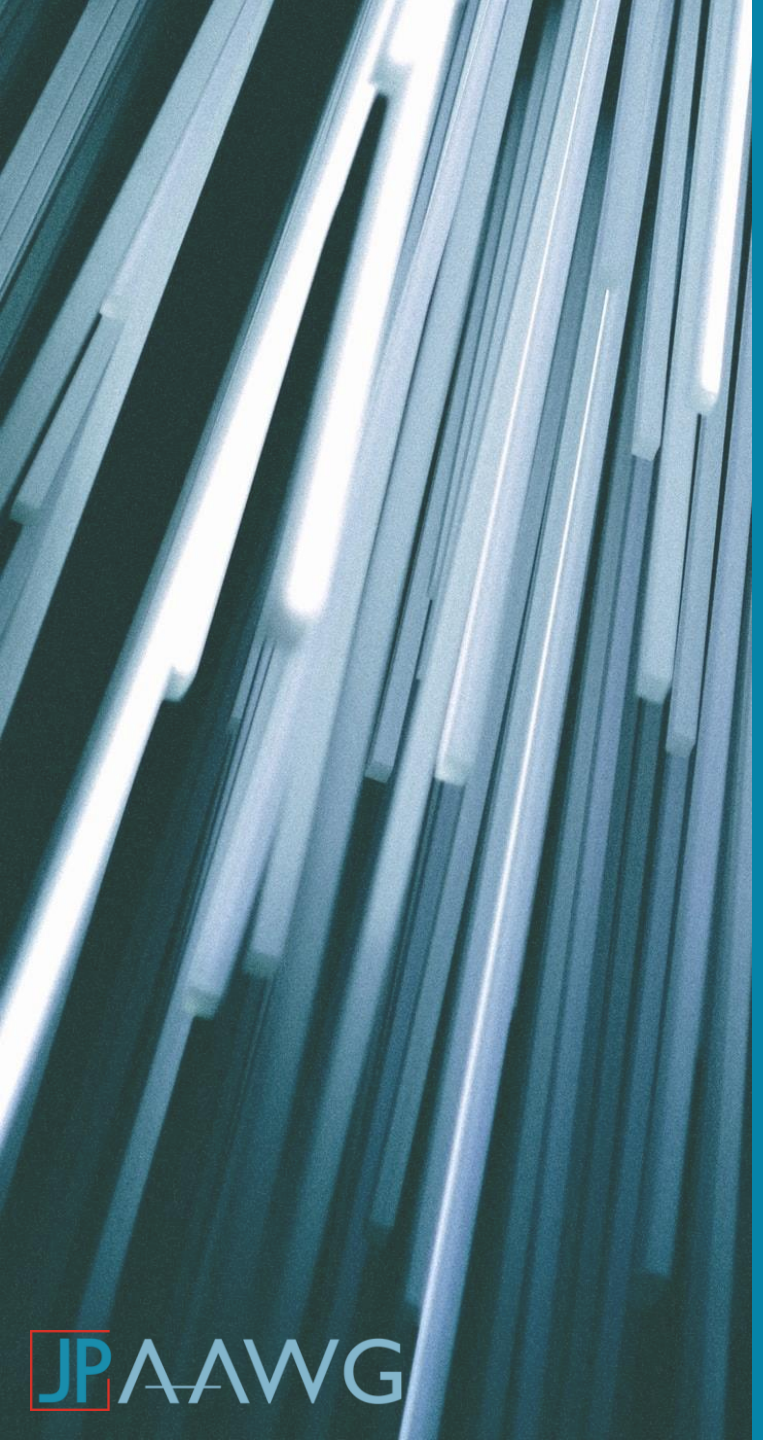
- Not a lot of discussion or data around adoption
- M3AAWG ARC group
  - Promoting the use of ARC
  - Once again, group needs more participants
  - Brooklyn meeting in October, 10-12 volunteers

ARC Activity

- Most visible users of ARC are Microsoft and Google
- Some receivers overwhelmed by Microsoft volume
- Main benefit seems to be for internal purposes

ARC Activity

- Last year Microsoft allowed Office 365 tenants to create *Trusted ARC Sender* lists
- Many use cases like spam filtering services, compliance/regulatory services
- Have not seen data about adoption or effectiveness

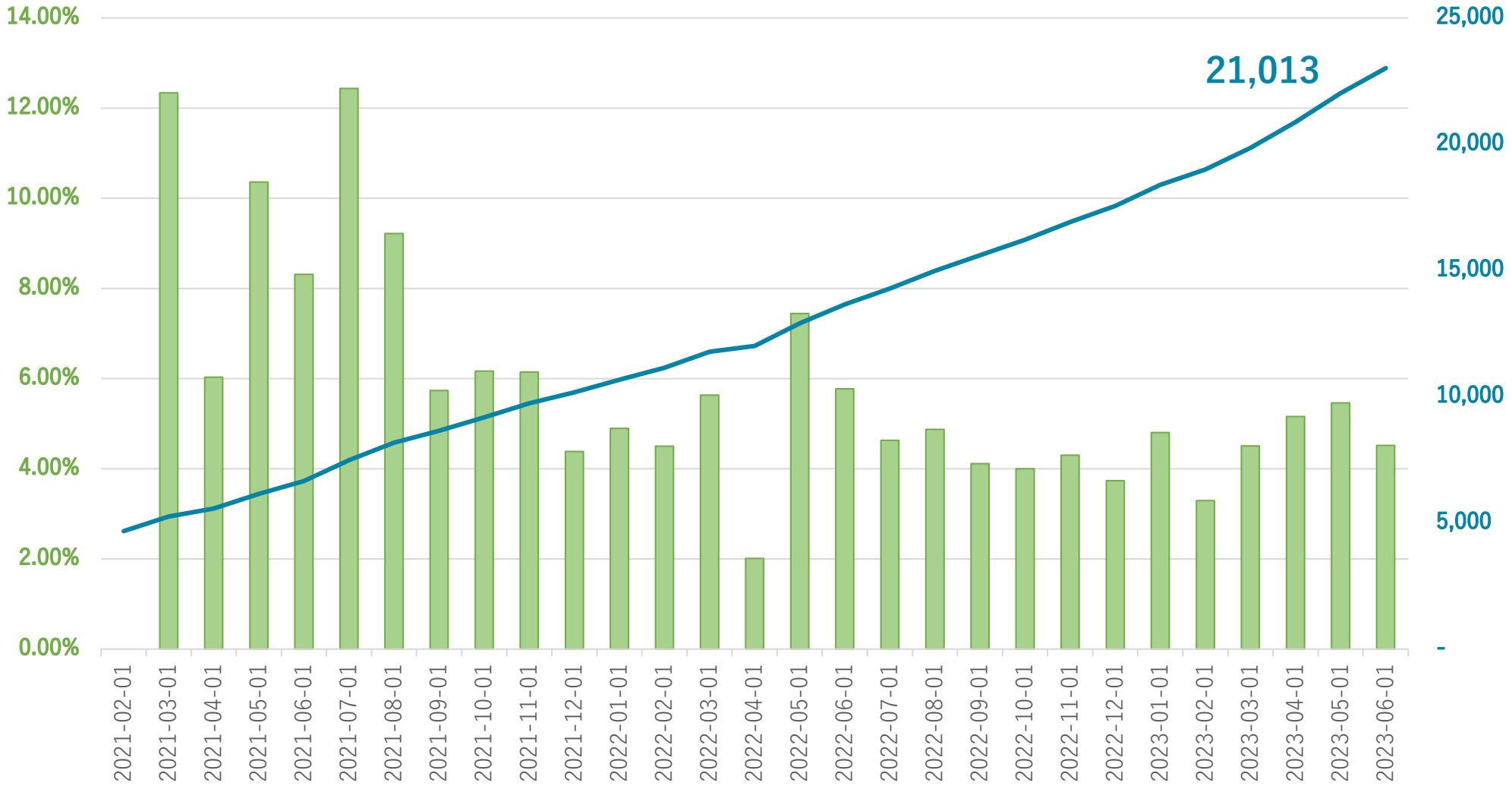


Some BIMI Statistics

About This Data

- Raw data supplied by DomainTools
- DNS request/response data captured from sensors widely deployed across the Internet
- Not 100% coverage of Internet, but a stable sensor network useful for comparisons over time
- DMARC.org thanks DomainTools for their continuing support

BIMI Records as of 2023 6月



BIMI Records

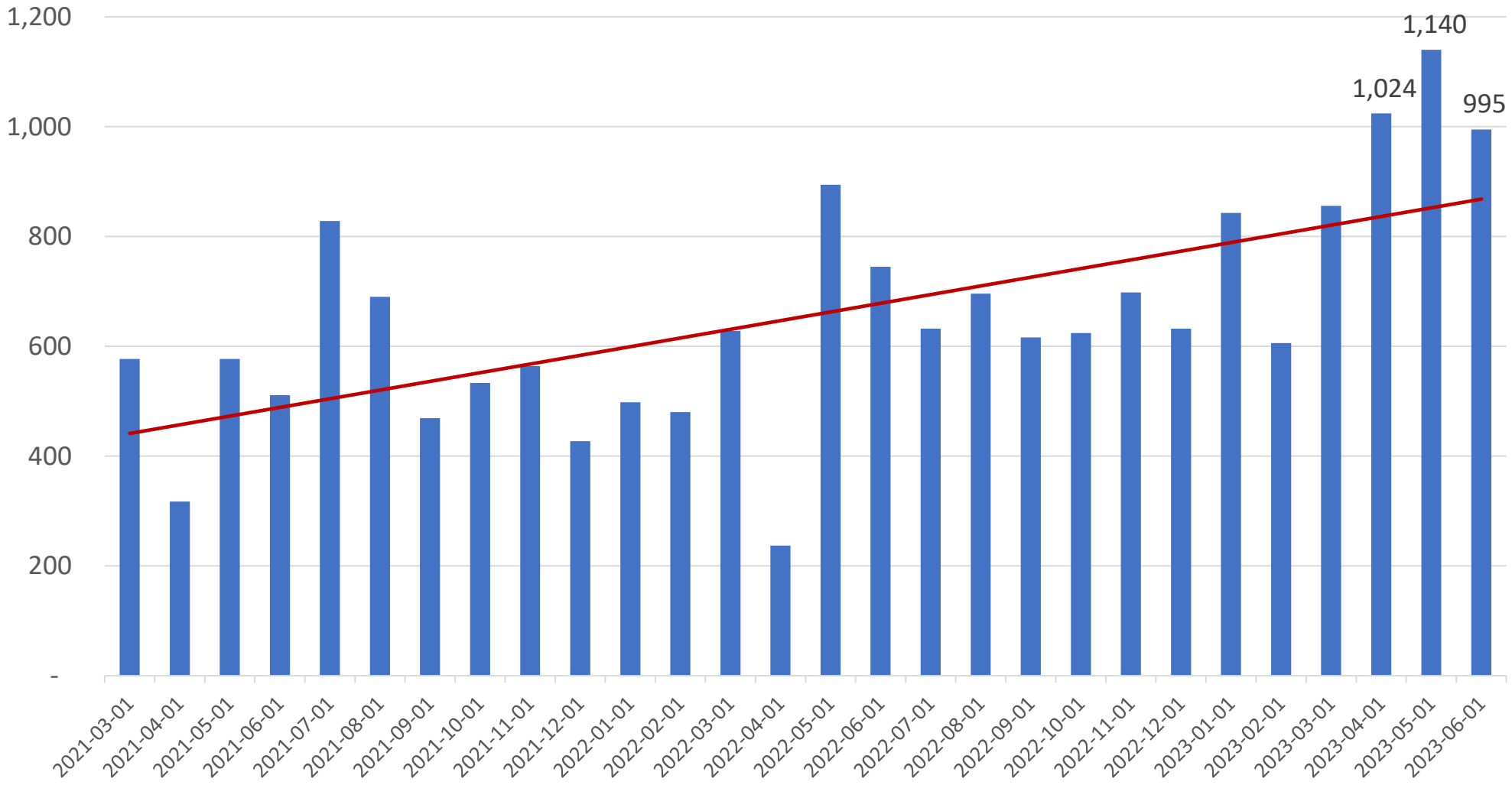
2022 Q2

- Total BIMI records observed: **15,004**
- Including link to VMC: **930**

2023 Q2

- Total BIMI records observed: **21,013**
- Including link to a VMC: **1,691**

New BIMI Records by Month



Thank you