JPAAWG JAPAN ANTI-ABUSE WORKING GROUP

DMARC Status and Related Activity

DMARC.org

Steven Jones

Topics

- IETF DMARC Working Group Status
- A New Email Authentication Initiative
- Some Statistics

IETF DMARC Working Group

DMARC Working Group Is Old

- Charter approved in 2014 8月
  - DKIM WG took 6 years, 2005 to 2011
- Main work items:
  1. Phase 1: Describe issues with indirect mail flows
  2. Phase 2
     - Improvements to support indirect mail flows
     - Draft Usage Guide for DMARC
  3. Phase 3
     - Refine DMARC specification
     - Complete DMARC Usage Guide
- New “DMARCbis” draft started in 2020 11月

DMARC WG Accomplishments

- Documents Published:
  - 2015 3月 – RFC 7489 DMARC
  - 2016 9月 – RFC 7960 Interoperability Issues (Phase 1)
  - 2019 5月 – RFC 8601 Authentication Results
  - 2019 6月 – RFC 8616 Authentication for i18n email
  - 2019 7月 – RFC 8617 ARC (Phase 2)
  - 2021 7月 – RFC 9091 Public Suffix Domains (Phase 3)

- Current draft documents:
  - `draft-ietf-dmarc-dmarcbis`
  - `draft-ietf-dmarc-aggregate-reporting`
  - `draft-ietf-dmarc-failure-reporting`

Status of DMARCbis Draft

- Document is in “Area Director Review”
- Area Director Kucherawy wrote a detailed review
- Still a few issues to address
- Target for DMARCbis is to be a *Standards Track* document
- Many IETF/IESG reviews before being accepted
- AD Kucherawy anticipates objections
  - Specifically, DMARCbis does not “fix” indirect mail flow issues

IETF Document Types

- Internet-Draft - No formal status
- Informational
  - “Specifications prepared outside may be published as Informational”
- Experimental
  - A specification that is part of a research or development effort
- Historical
- Standards Track
  - Proposed Standard – generally stable, but may be “immature”
  - Draft Standard – “quite stable,” multiple implementations
  - Internet Standard – very mature, “provides significant benefit”

Published Document Types

RFC 7489 DMARC	Informational
RFC 7960 Indirect Email Flows	Informational
RFC 8617 ARC	Experimental
RFC 9091 Public Suffix Domains	Experimental

- DMARCbis is intended for **Proposed Standard** status, to eventually become an Internet Standard
- A Proposed Standard cannot depend on an Experimental document

How the IETF Works

- The IETF uses mailing lists heavily
- In theory, all significant Working Group activity occurs on the mailing lists
- All IETF activity is coordinated via mailing lists
- Mailbox providers report less than 1% of all email they process is from mailing lists
- But to the IETF, mailing lists are critical channels
- This is why indirect mailflows cannot be ignored

There Is A Deadline

- Murray Kucherawy is Area Director (since 2020)
- Term was supposed to end in 2024
  - Extended to 2025 3月
- He will not allow the WG to continue past the end of his term
- Can the WG respond to feedback and objections to DMARCbis by then?
- What about the reporting documents?

Problems Moving Forward

- Too few people have been participating
  - This has been a problem for at least 5 years

- One person objecting can have outsized influence

- WG Chairs don’t always stop people from raising issues that were already resolved

Issue: Indirect Mail Flows

- Several mechanisms proposed and discussed
- Authenticated Received Chain (ARC) was published
- However, RFC 8617 is *Experimental*
- Nobody has published a report on the ARC experiment
- Without that, ARC cannot advance to Standards Track
- Without that, will DMARCbis have “addressed the issues with indirect mail flows” sufficiently?

Issues: Public Suffix Domains

- Bringing RFC 9091 and DNS Treewalk into DMARCbis
- PSD sending email wishes to receive aggregate reports
  - Wants to publish “np=“ and “rua=“ for non-existent child domains
  - Wants to get aggregate reports for PSD itself
- PSD is the child of another PSD that doesn’t publish DMARC
- Current language could have 2nd level PSD overriding child domains’ DMARC policy, or else unable to receive its own DMARC reports

DKIM2

A New Email Authentication Initiative

A New Email Authentication Protocol

- A small group is creating a new protocol
- Presented at IETF 121 in Dublin last week
- Participants include Google, Yahoo
- Draws heavily on DKIM Replay proposals from 2022
- Existing DKIM Working Group will be re-activated

https://datatracker.ietf.org/doc/draft-gondwana-dkim2-motivation/

Why Create DKIM2?

- DMARC has issues with forwarded and altered messages
- DKIM Replay Attacks have increased since 2021
- Not all receivers handle multiple DKIM signatures well
- No standard feedback loop for DKIM signers
- RSA is vulnerable, little DKIM using elliptical curve – and no support for Post-Quantum Cryptography (PQC)

Why Create DKIM2?

- ARC is not seen as a good solution
  - Depends on a reputation system
  - No reputation data available to small and medium organizations
- Bounces only go to one address
  - Original sender or intermediary, but not both
  - Backscatter, bounces being sent to forged addresses, is still a problem

Features of DKIM2

- Include “differences” to reverse any changes made by an intermediary
- Record the next “hop” in a signed field
- Change bounces, abuse reports, and feedback loops to allow for multiple recipients
- These will travel back along the same path that the original message took, hop by hop

How is DKIM2 Better?

- Every intermediary verifies all DKIM2 headers and records the result (like ARC)
- Bounces travel a reversed path, allows intermediaries to intercept bounces, avoid exposing addresses
  - Anonymizing forwarders, mailing list managers
- DKIM2 messages will not allow BCC addressing to verify
- DKIM2 signatures Includes timestamps, envelope To: and From: addresses, to combat DKIM Replay attacks
- Requires RSA, elliptic curve, and “post-quantum” capability

Challenges for DKIM2

- Technical specification hasn’t been written yet
- Draft “Motivation” states that the “change algebra” will be in a separate, perhaps later document
- Massive changes to how bounces are handled
- Assumption that all changes can occur in standard components/libraries already in use
- Mailing List Managers (MLMs) and other applications will need more updates for reversible changes

Challenges for DKIM2

- Might see DKIM2 signatures duplicated using RSA, elliptic curve, and “post-quantum” algorithms
- Unclear if BCC sending is still allowed under DKIM2
- DSN handling requires extensive changes to MTAs
    - Will the increased message volume cause problems for MLMs and forwarders?
- A message that traverses a non-DKIM2 hop can not be processed as a DKIM2 message

Challenges for DKIM2

- Intermediaries may make “complex” changes that are not reversible, breaking end-to-end verification
- These intermediaries must still be “trusted,” or the message should be rejected, but no trust model is specified
- Feedback features will still require registration with mailbox providers on a per-domain basis

Statistics

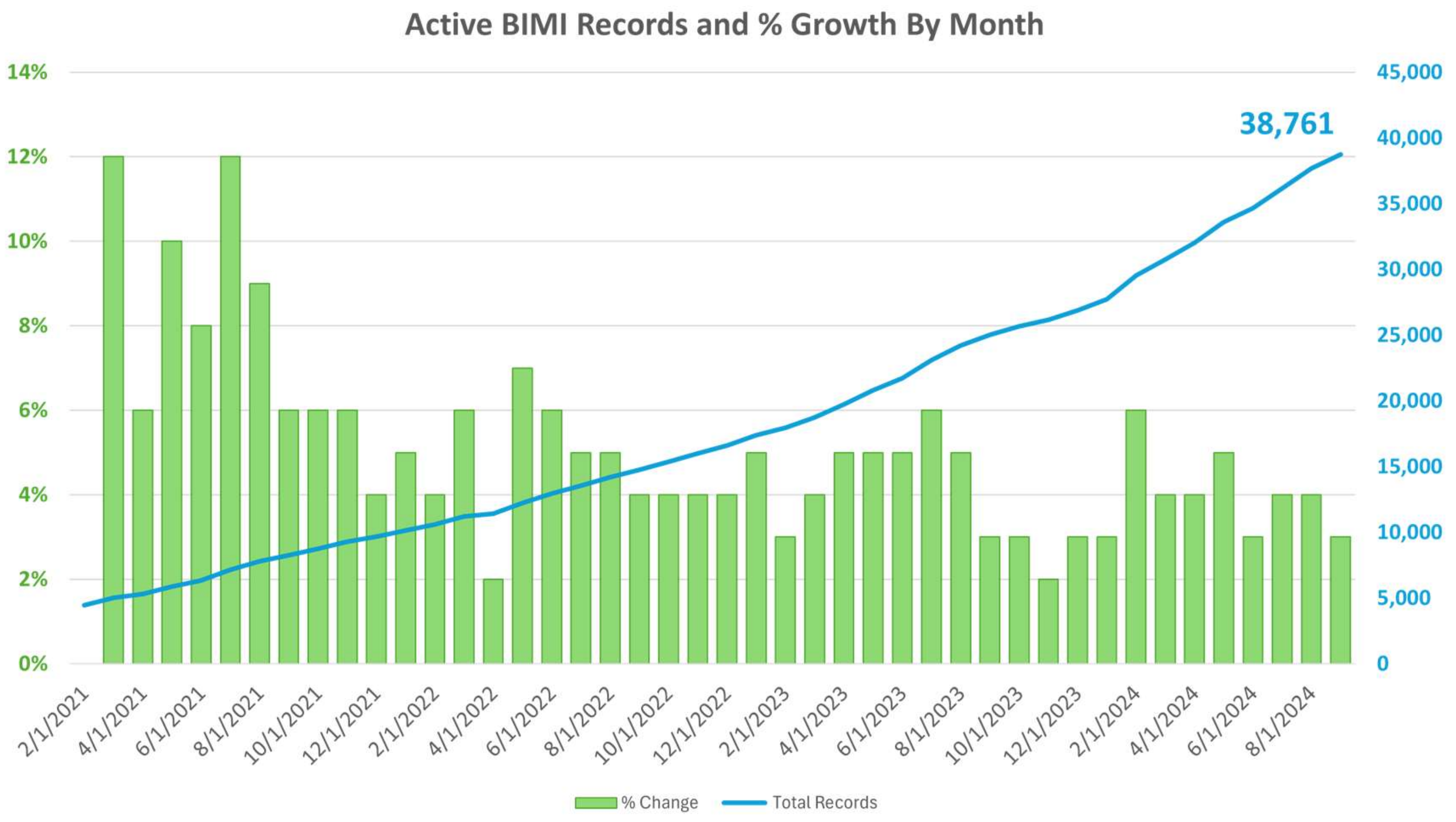
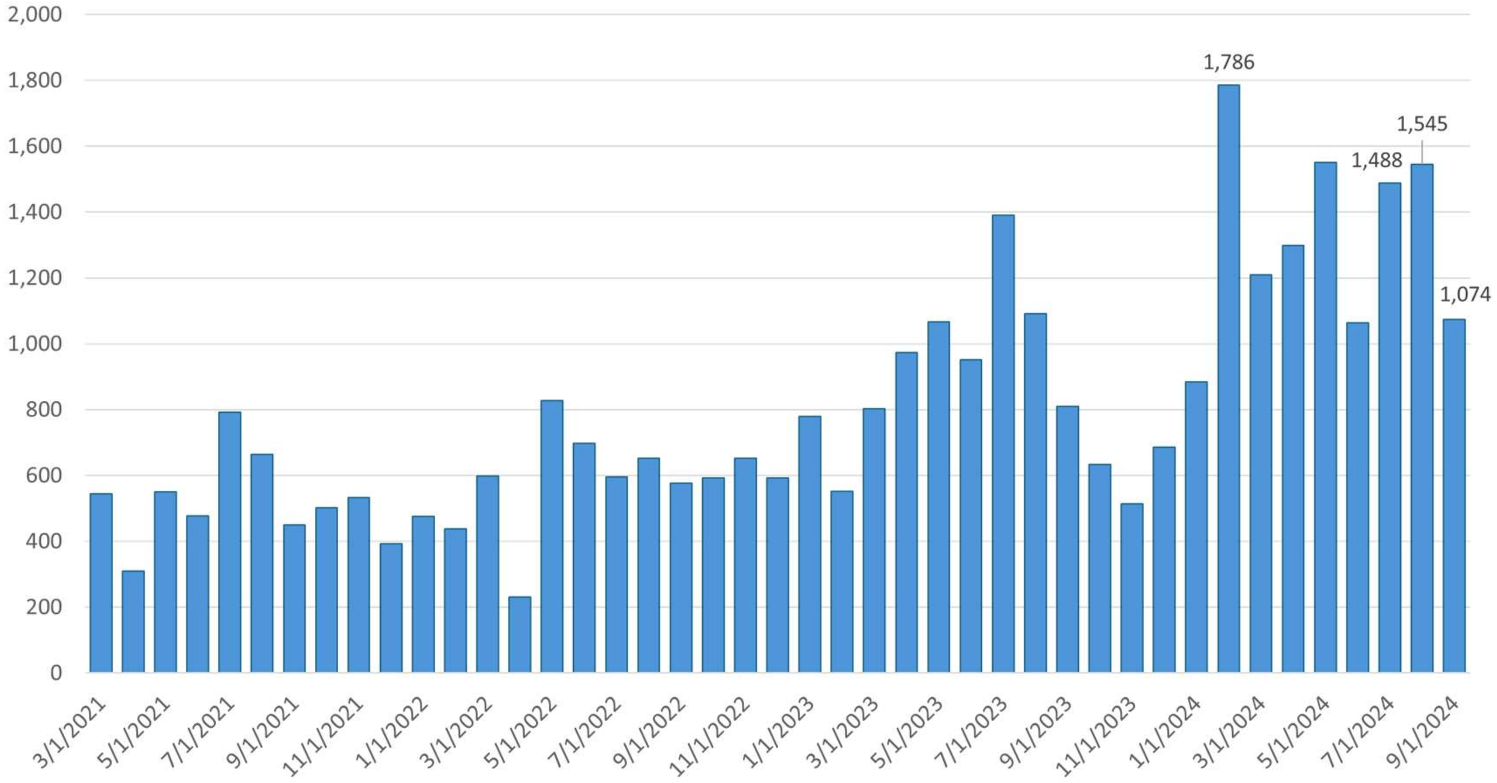
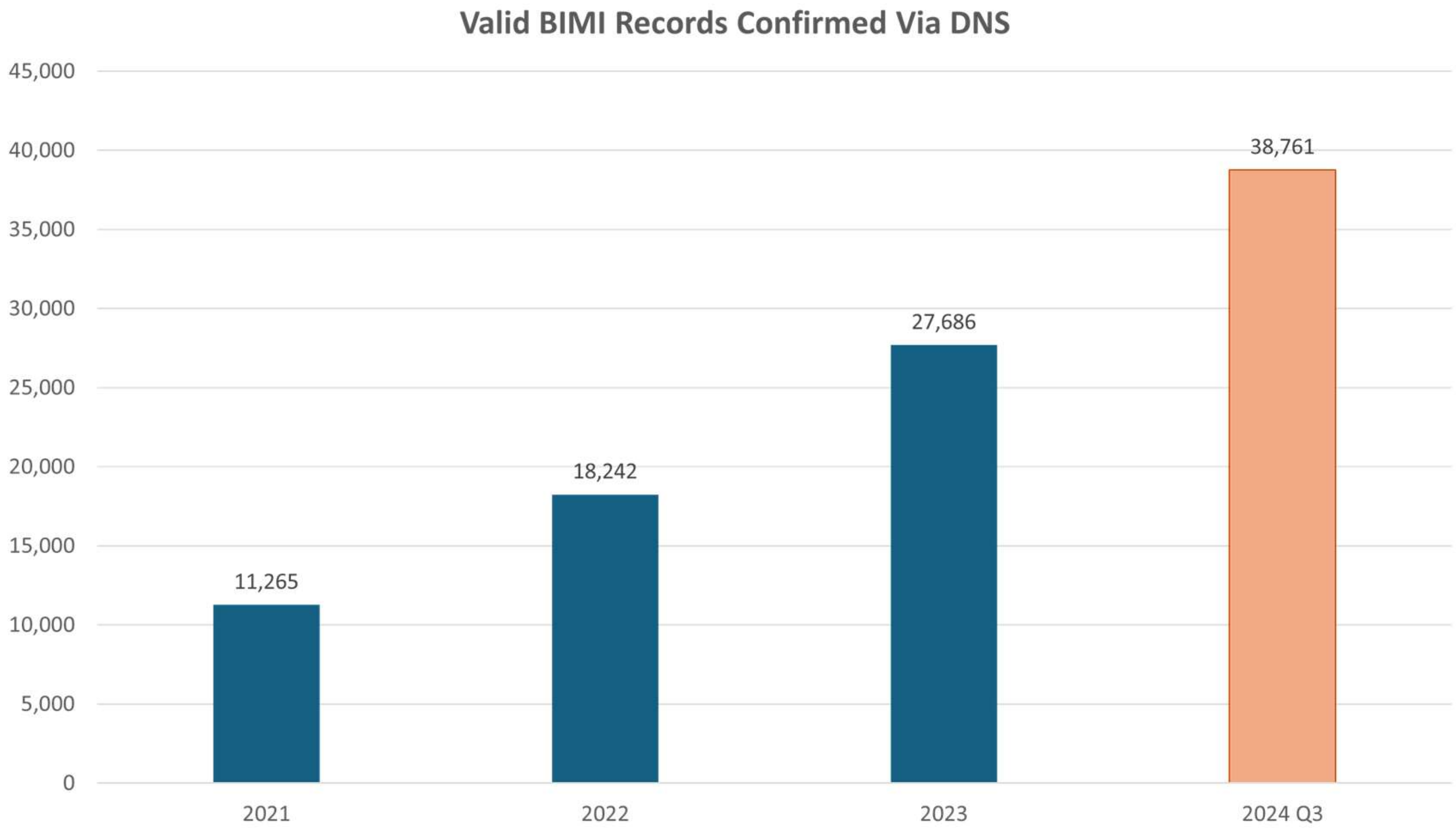

Active BIMI Records and % Growth By Month
14%
12%
10%
8%
6%
4%
2%
0%
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
38,761
2/1/2021
4/1/2021
6/1/2021
8/1/2021
10/1/2021
12/1/2021
2/1/2022
4/1/2022
6/1/2022
8/1/2022
10/1/2022
12/1/2022
2/1/2023
4/1/2023
6/1/2023
8/1/2023
10/1/2023
12/1/2023
2/1/2024
4/1/2024
6/1/2024
8/1/2024
🟩 % Change
Total Records

Chart New BIMI Records By Month



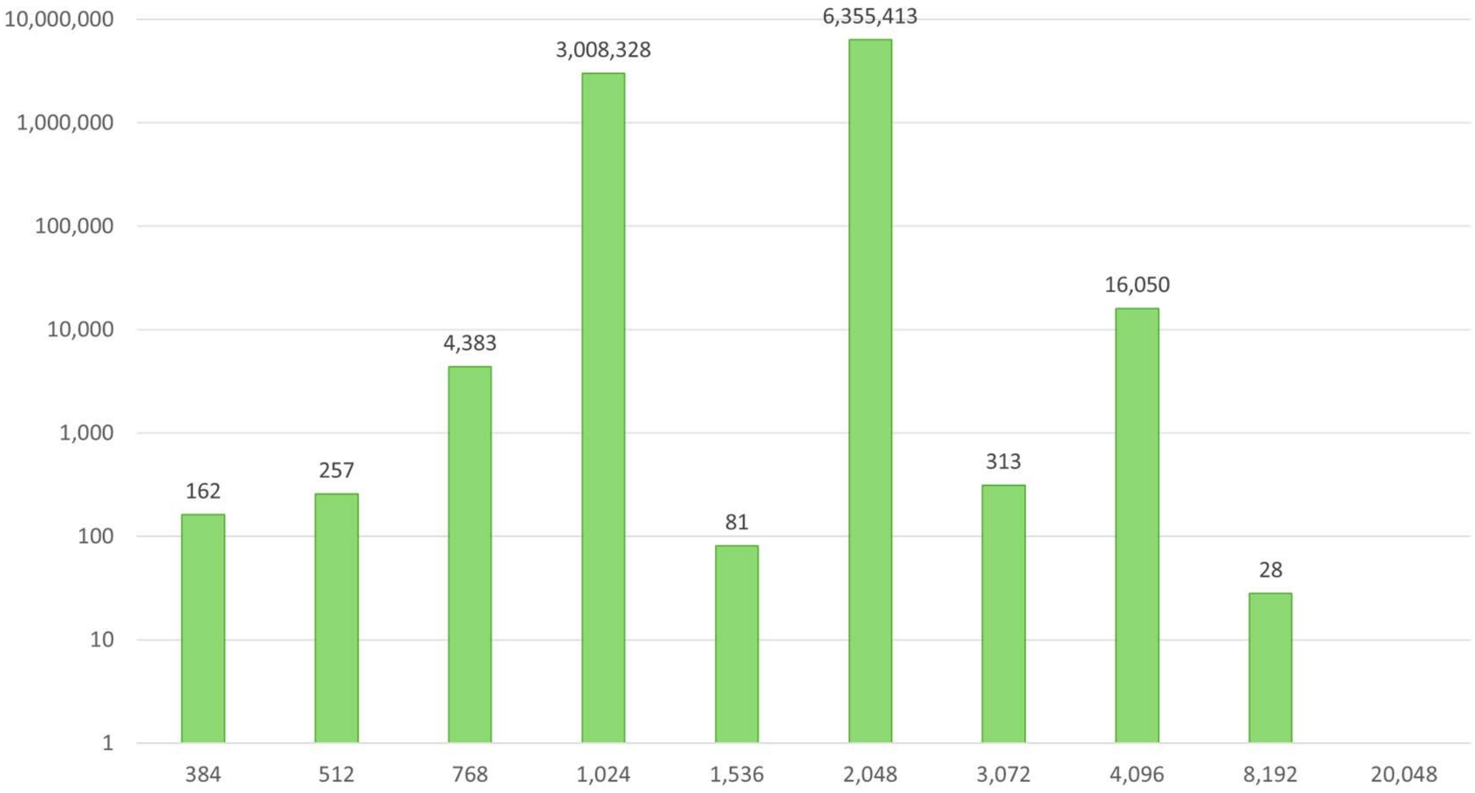

Valid BIMI Records Confirmed Via DNS
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
11,265
18,242
27,686
38,761
2021
2022
2023
2024 Q3

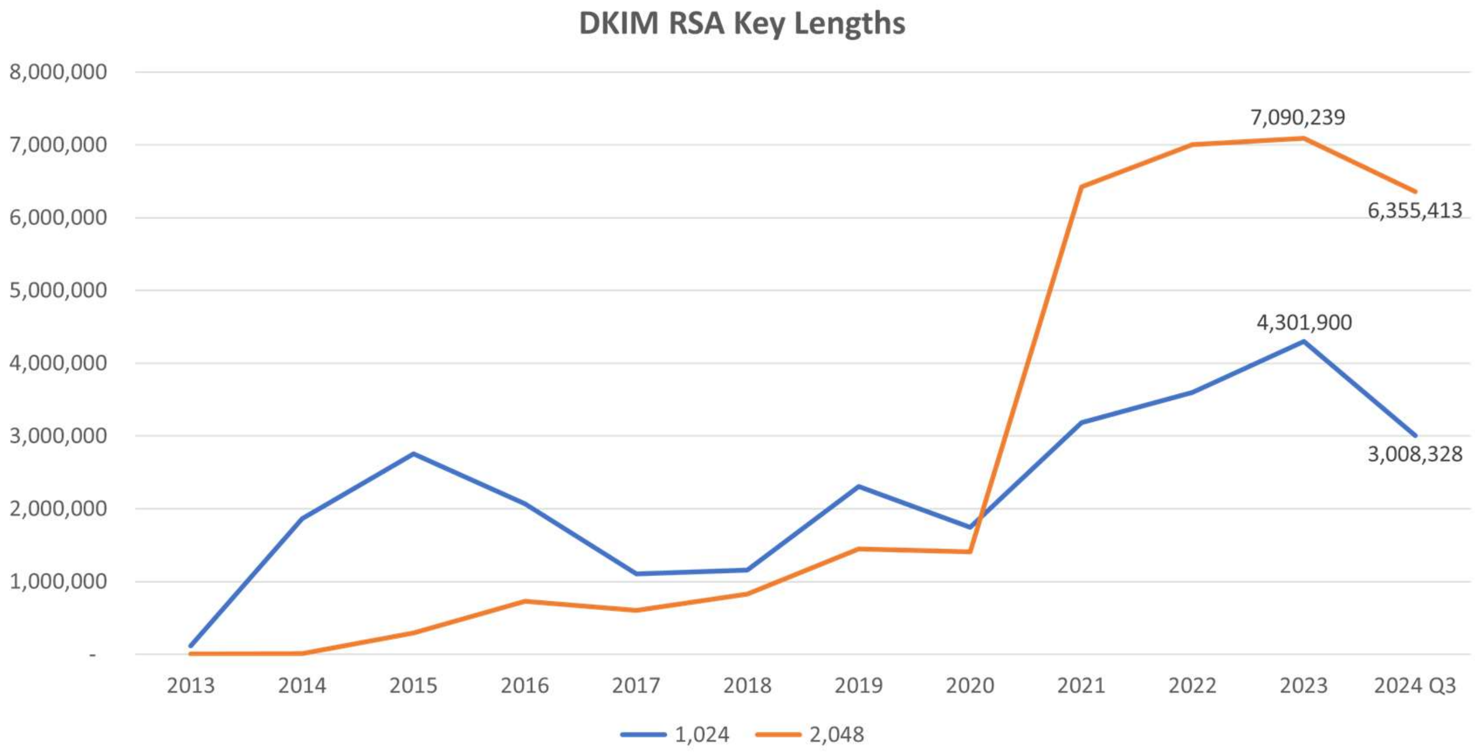
DKIM

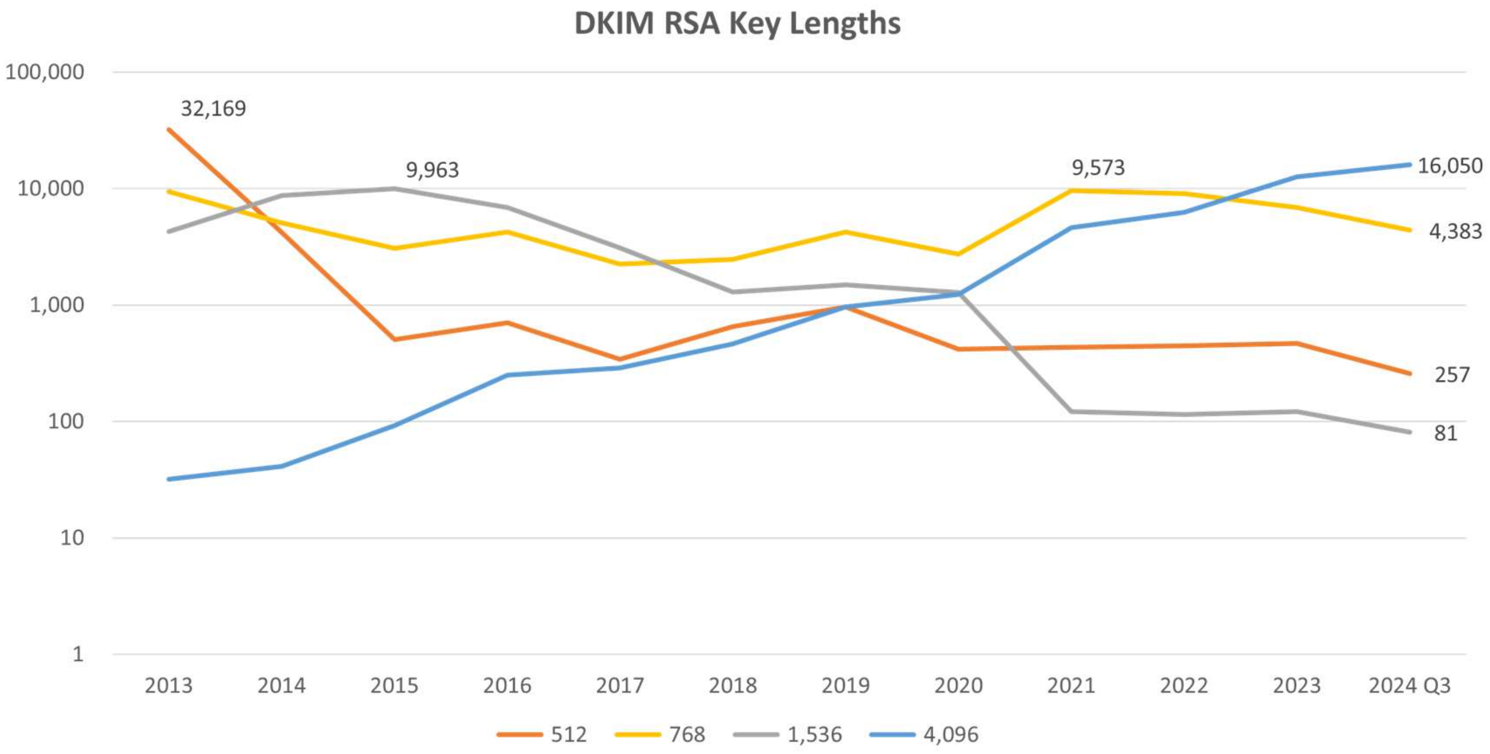
- Are senders moving from RSA to elliptical curve (EC) algorithm for DKIM signing?

Year	EC Keys	RSA Keys
2021	2,108	9,752,141
2022	2,454	10,817,441
2023	126,735	12,001,226
2024 Q3	132,369	9,590,100
2011 – 2024 Q3	200,080	52,821,176

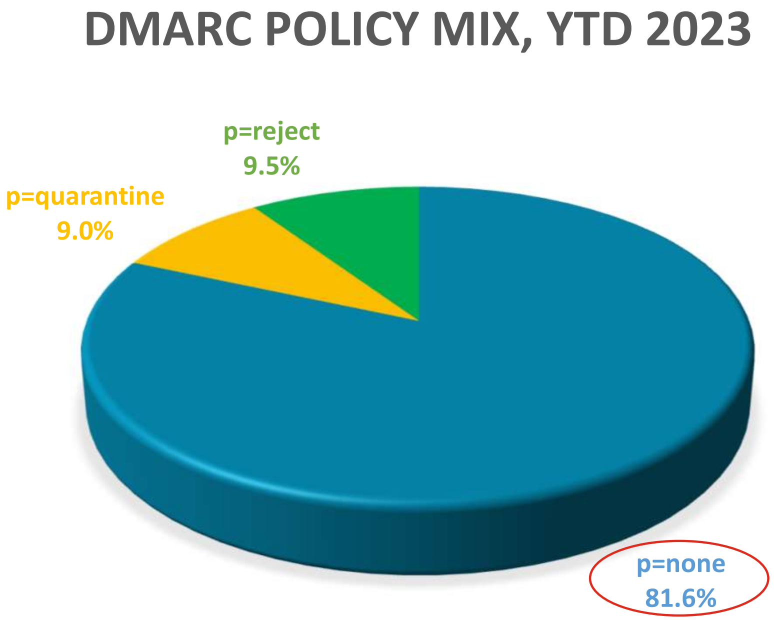
DKIM RSA Key Lengths Year-To-Date 2024

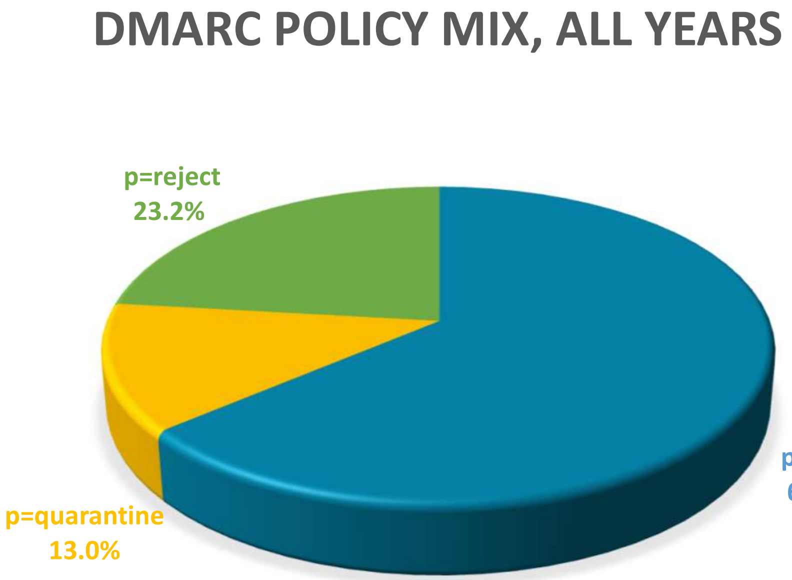


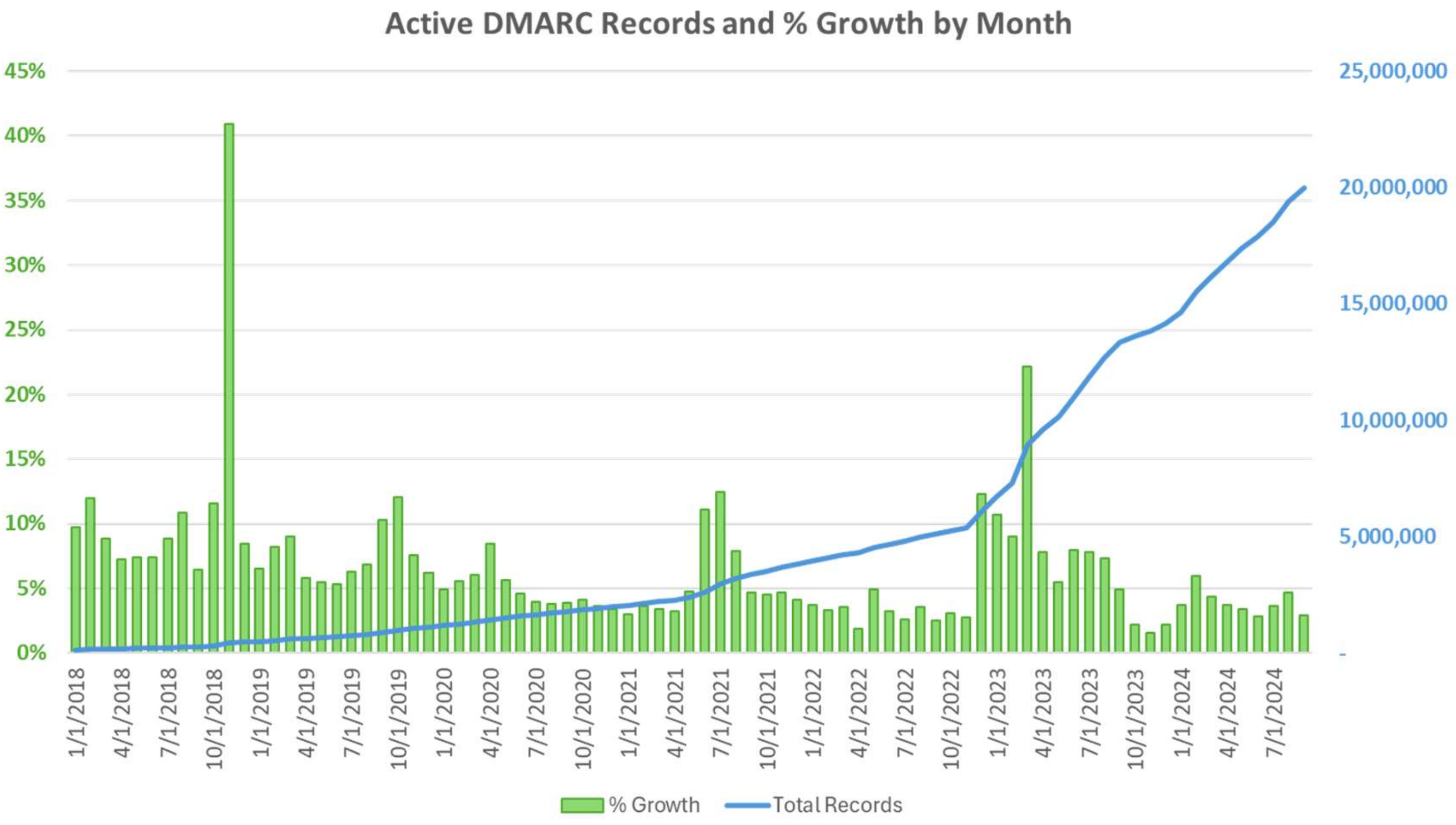

DKIM RSA Key Lengths
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
-
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024 Q3
7,090,239
6,355,413
4,301,900
3,008,328
1,024
2,048


DKIM RSA Key Lengths
100,000
10,000
1,000
100
10
1
32,169
9,963
9,573
16,050
4,383
257
81
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024 Q3
512
768
1,536
4,096

DMARC Policies

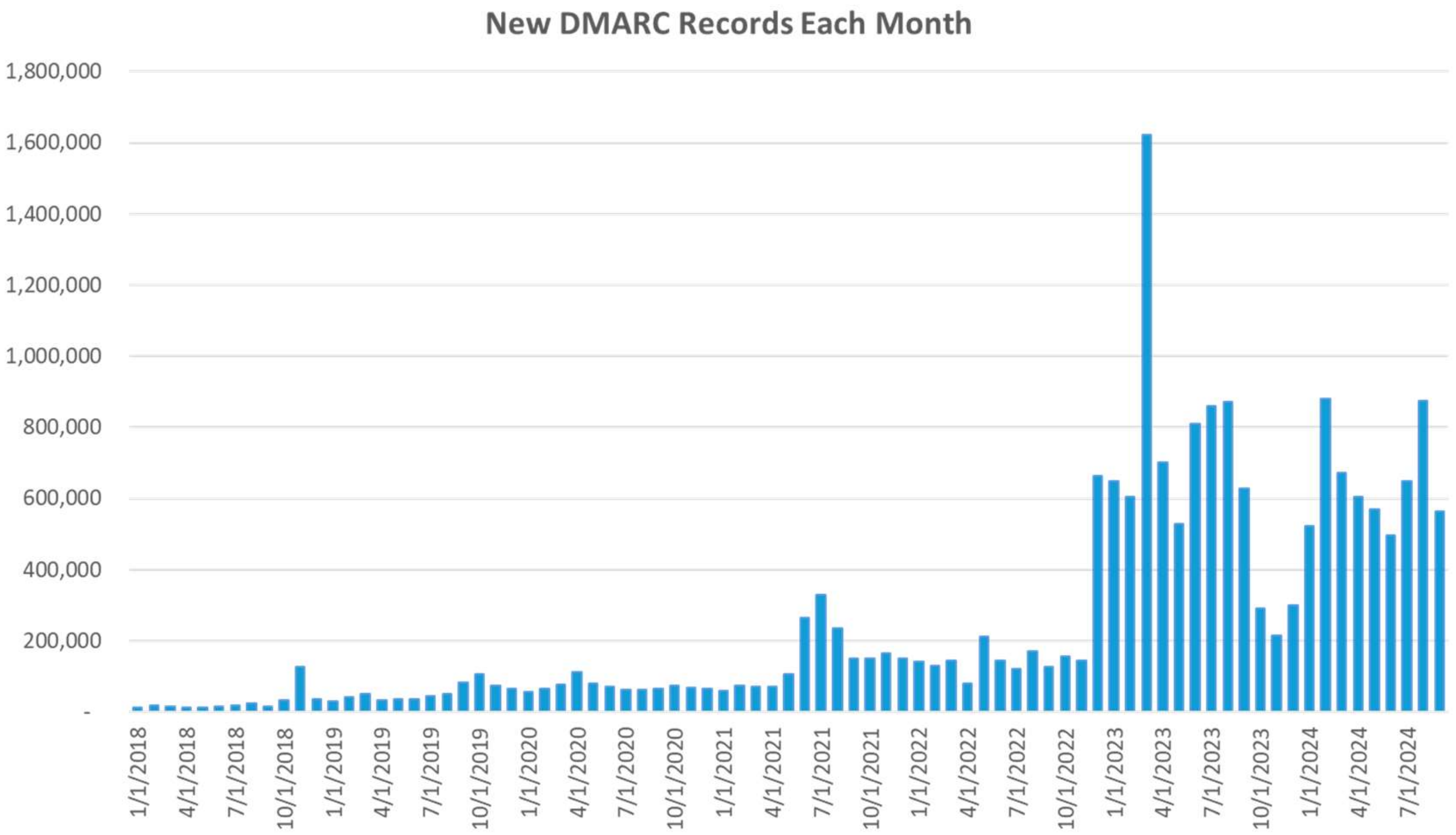




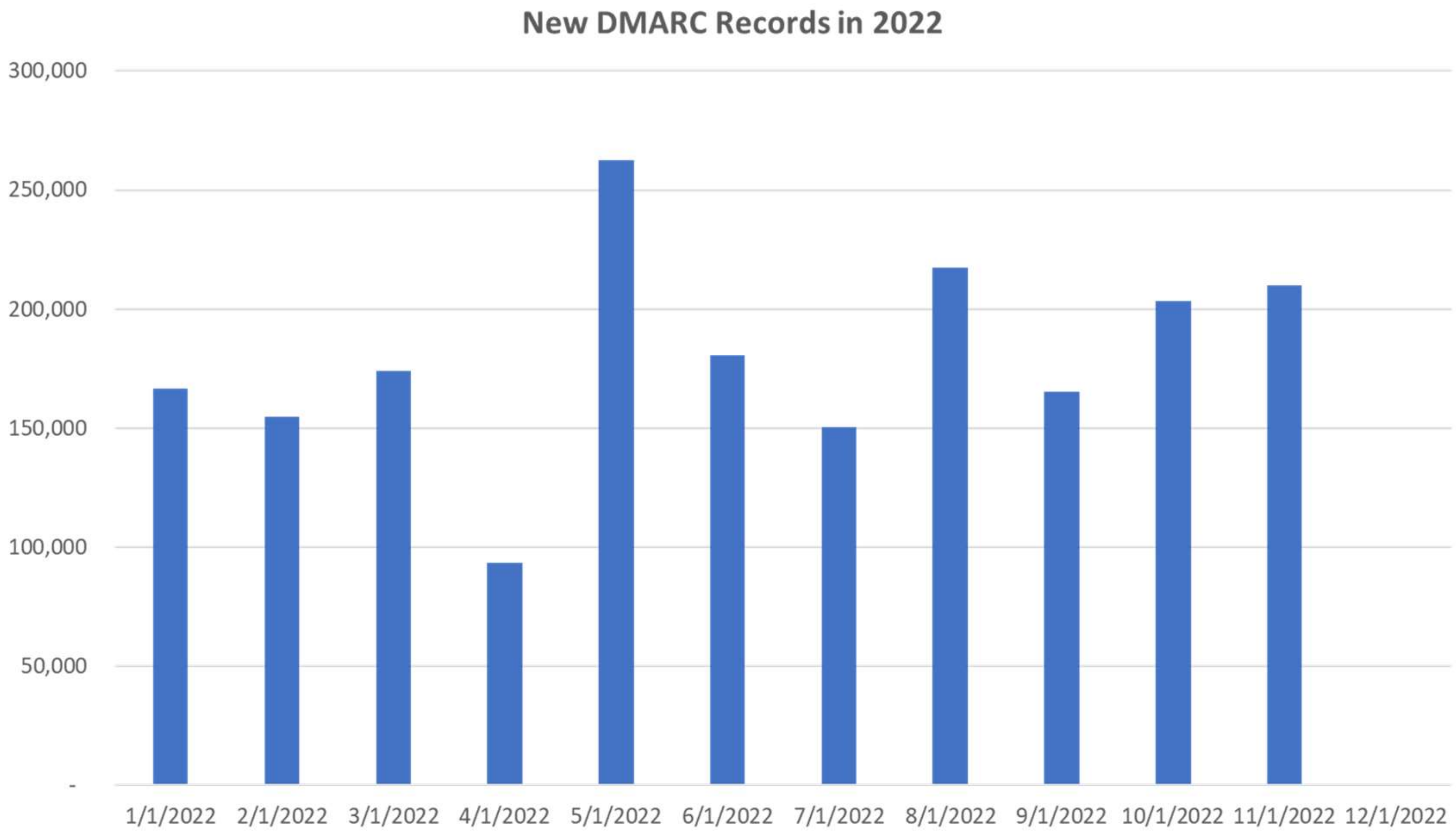


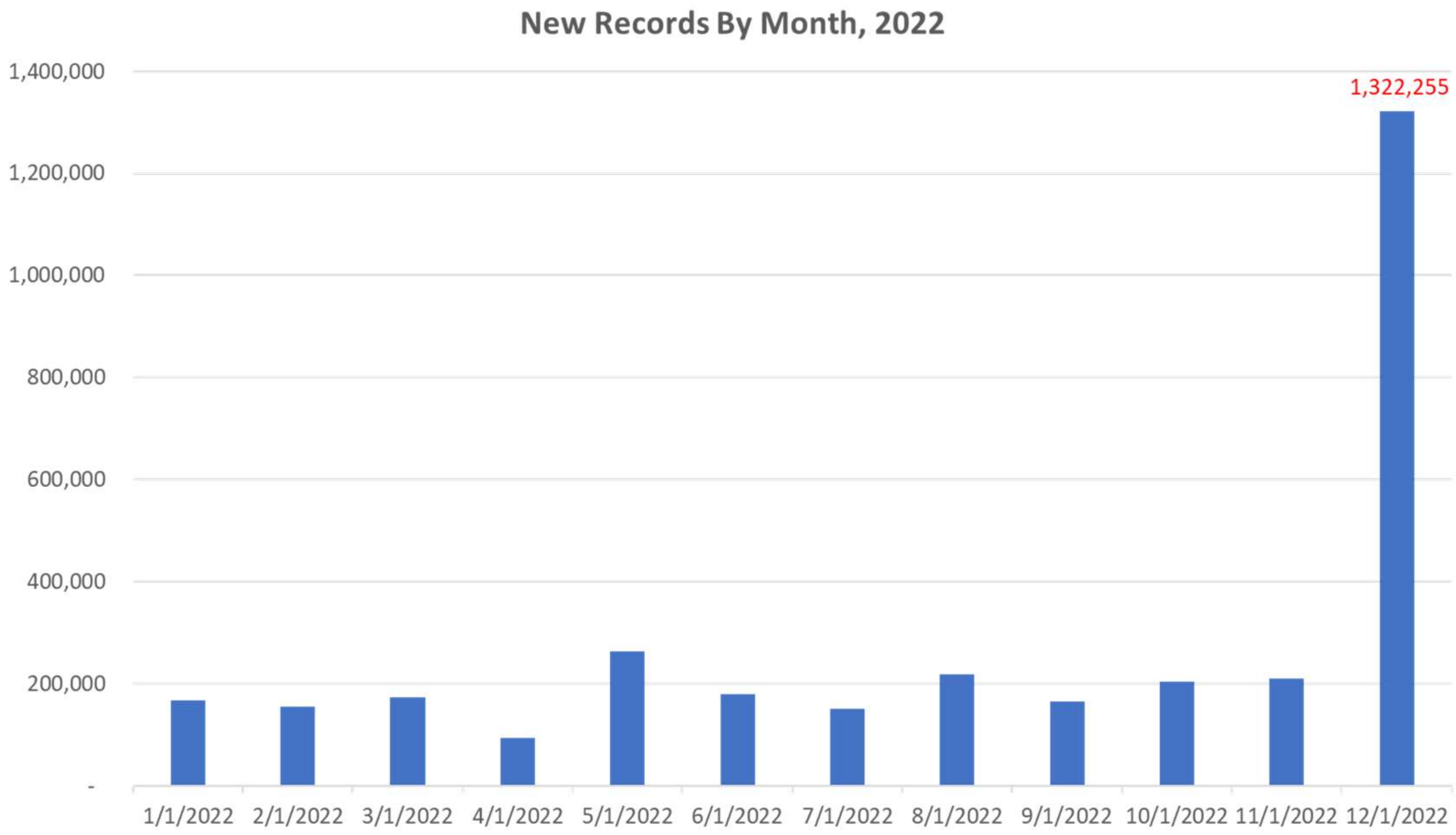
Active DMARC Records and % Growth by Month
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
-
1/1/2018
4/1/2018
7/1/2018
10/1/2018
1/1/2019
4/1/2019
7/1/2019
10/1/2019
1/1/2020
4/1/2020
7/1/2020
10/1/2020
1/1/2021
4/1/2021
7/1/2021
10/1/2021
1/1/2022
4/1/2022
7/1/2022
10/1/2022
1/1/2023
4/1/2023
7/1/2023
10/1/2023
1/1/2024
4/1/2024
7/1/2024
% Growth
Total Records

JPAAWG


New DMARC Records Each Month
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
-
1/1/2018
4/1/2018
7/1/2018
10/1/2018
1/1/2019
4/1/2019
7/1/2019
10/1/2019
1/1/2020
4/1/2020
7/1/2020
10/1/2020
1/1/2021
4/1/2021
7/1/2021
10/1/2021
1/1/2022
4/1/2022
7/1/2022
10/1/2022
1/1/2023
4/1/2023
7/1/2023
10/1/2023
1/1/2024
4/1/2024
7/1/2024

JPAAWG


New DMARC Records in 2022
300,000
250,000
200,000
150,000
100,000
50,000
-
1/1/2022
2/1/2022
3/1/2022
4/1/2022
5/1/2022
6/1/2022
7/1/2022
8/1/2022
9/1/2022
10/1/2022
11/1/2022
12/1/2022


New Records By Month, 2022
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
-
1,322,255
1/1/2022
2/1/2022
3/1/2022
4/1/2022
5/1/2022
6/1/2022
7/1/2022
8/1/2022
9/1/2022
10/1/2022
11/1/2022
12/1/2022

New Records Under One TLD?

.com	517,266
.net	116,955
.nl	100,545
.pl	40,999
.de	37,418
.in	34,288
.br	31,633
.uk	24,417
.fr	23,869
.org	21,410

New Records Under One Domain?

.net.easyblock	81,943
.br.com	28,797
.uk.co	20,567
.com.4008114112	16,856
.com.cntoaster	16,405
.com.51379285	15,395
.tv.arias	15,339
.in.net	14,675
.com.bjdhbl	12,942
.mx.com	9,647

Match Records By DMARC Policy?

```
Counts of lines with the same indexed element:

  354301: v=DMARC1; p=reject; rua=mailto:dmarc_report@mail.liamfactory.com;
ruf=mailto:dmarc_report@mail.liamfactory.com; fo=1; pct=100
  229482: v=DMARC1; p=none
  112622: v=DMARC1; p=none;
   41254: v=DMARC1; p=reject
   33774: v=DMARC1;p=none;sp=none;adkim=r;aspf=r;pct=100
   28632: v=DMARC1; p=none; sp=none;
   18226: v=DMARC1; p=none; sp=none
   16344: v=DMARC1; p=quarantine;
   11944: v=DMARC1;p=none;sp=none;adkim=r;aspf=r;pct=100;fo=0;rf=afrf;ri=86400
   11191: v=DMARC1; p=none; sp=none; rf=afrf; pct=100; ri=86400
```

Hmm… Let’s look at all the domains with that first DMARC policy…

Match Records By DMARC Policy?

```
Counts of lines with the same indexed element:

   14284: in.net.static-vsnl
    9225: com.cntoaster.2013
    8038: mx.com.clientesbestel
    7231: com.51379285.2013
    6985: in.co.27-tataidc
    4990: com.4006138024.2013
    3868: com.4008114112.2013
    3548: in.182-airtelbroadband.65
    2221: com.51zgszw.2013
    1778: ua.net.home-net
```

The new records were not just under a few domains. What do the domains look like?

Match Records By DMARC Policy?

```
grep 4006138024 labels | head -10
_dmarc.10033.4006138024.com.
_dmarc.10133.4006138024.com.
_dmarc.10181.4006138024.com.
_dmarc.10259.4006138024.com.
_dmarc.102a4.4006138024.com.
_dmarc.102fc.4006138024.com.
_dmarc.1031e.4006138024.com.
_dmarc.10531.4006138024.com.
_dmarc.10540.4006138024.com.
_dmarc.106cd.4006138024.com.
$
$ grep 4006138024 labels | wc -l
    8105
$
```

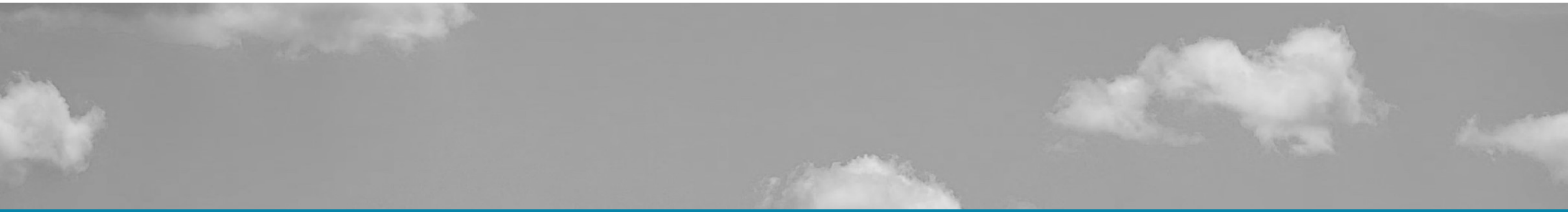
Match Records By DMARC Policy?

```
_dmarc.070liftservice.nl.
_dmarc.avplumber.co.il.
_dmarc.cockleshellholidays.co.uk.
_dmarc.elks1805.org.
_dmarc.gulf-hiring.com.
_dmarc.jyotienterprise.in.
_dmarc.mattheeusen.be.
_dmarc.nextconcept.ro.
_dmarc.parkinnsarvar.hu.
_dmarc.sakanatsuri.jp.
_dmarc.tapico.eu.
_dmarc.twizi.it.
_dmarc.yogomusic.club.
```

Sometimes They Go Away

- In February 2023, 1.32 million of the new records from December 2023 were still active in DNS

- In October 2024, only 662,421 of those records were still active in DNS



ありがとうございました

Thank you