M3AAWG
MESSAGING MALWARE MOBILE

M3AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012

M3AAWG
MESSAGING MALWARE MOBILE

M3AAWG DMARC Training Videos

(2.5 hours of training)

This is Segment 4 of 6

The complete series of DMARC training videos is available at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **What is DMARC?** **(about 20 minutes)**	**Segment 2** **DMARC Identifier Alignment** **(about 20 minutes)**	**Segment 3** **DMARC Policy Records** **(about 30 minutes)**
Segment 4 **DMARC Reporting** **(about 15 minutes)**	**Segment 5** **DMARC Information for Mailbox Providers** **(about 20 minutes)**	**Segment 6** **DMARC Information for Domain Owners and 3rd Parties** **(about 40 minutes)**

M3AAWG
MESSAGING MALWARE MOBILE

DMARC Reporting

DMARC Segment 4 – about 15 minutes

Paul Midgen, DMARC.org

October 22, 2012

DMARC Spec – Reporting

M3AAWG
MESSAGING MALWARE MOBILE

Aggregate Reports

- Each report covers one RFC5322.From domain.
- You should get one from each supporting mailbox provider that sees email with your From domain.
- Daily by default, adjustable with ri= tag.

  Hourly : `ri=3600`

XML Format

- Organized by sending IP address
- Contains
  - Authentication Results (DKIM, SPF)
  - Alignment Results
  - Policy actions taken
  - Reasons for not taking policy actions

Just publish a record to see one

DMARC Spec – Reporting

XML Format

The policy they found.

```
<policy_published>
        <domain>facebookmail.com</domain>
        <adkim>r</adkim>
        <aspf>r</aspf>
        <p>reject</p>
        <sp>none</sp>
        <pct>100</pct>
</policy_published>
```

DMARC Spec – Reporting

M3AAWG
MESSAGING MALWARE MOBILE

XML Format

An example record.

```
<record>
  <row>
    <source_ip>106.10.148.108</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>facebookmail.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>facebookmail.com</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>NULL</domain>
      <result>none</result>
    </spf>
  </auth_results>
</record>
```

DMARC Spec – Reporting

M3AAWG
MESSAGING MALWARE MOBILE

Forensic Reports

- One per DMARC failure
- AFRF or IODEF formats
- Should include ‘call-to-action’ URIs
- Throttling
- Privacy issues
  - Might be redacted
  - Might not be supported

DMARC Spec – Reporting

DMARC URLs

Advertise the maximum report size a destination URI will accept

```
mailto:aggregate@example.com!25M
```

Works for both report types.

DMARC Spec – Reporting

M3AAWG
MESSAGING MALWARE MOBILE

Verifying 3rd party report destinations

If the record for example.com contains reporting URIs at other domains:

```
mailto:aggregate@foo.com
```

Report generators should verify that foo.com expects the reports by looking for:

```
example.com._report._dmarc.foo.com
```

The 3rd party can change the URI to a different address in their domain:

```
v=DMARC1; rua=mailto:reports@foo.com
```

This has been the fourth of six DMARC video segments

View the entire

M³AAWG DMARC Training Series

from the public training video pages on the M³AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org
for developing the material in this series
and allowing M³AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

For information about M3AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form