DMARC

A first year enabling trust between brand owners and receivers

February 2013

Data Source Statement

DMARC.org members provided the data in this presentation under conditions the data would be released in aggregate. Accuracy of the reported data has been verified and otherwise validated by the members, and should be sourced as coming from DMARC.org.

© 2013 DMARC.org

DMARC Defined

DMARC stands for:

Domain-based Message Authentication, Reporting & Conformance

(pronounced “dee-mark”)

© 2013 DMARC.org

DMARC.org

Loose collaboration, based on common goals to combat spoofed mail, standardizing an effective solution for the overall Internet ecosystem.

© 2013 DMARC.org

Phishing continues to be a major pain point for the consumer Internet

90% peak spoof rates[1]

100k's account hijackings daily [2]

10% average spoof rate of the Internet Retail 500[1]

30% average spoof rate for top federal government sites[1]

Incidence and costs related to spear phishing rising quickly [2]

91% of targeted attacks involve spear-phishing emails.[3]

Loss of trust in online resources
Decrease in future online activity

[1] Courtesy, Online Trust Alliance

[2] Courtesy, DMARC.org Members

[3] Trend Micro Report: "Spear-Phishing Email: Most Favored APT Attack Bait", 2012

© 2013 DMARC.org

DMARC – *What does it do?*

- **Senders**
  - authenticate their mail, and
  - publish a policy for how to handle unauthenticated mail.
- **Receivers**
  - retrieve the sender policy,
  - take action on unauthenticated mail, and
  - report on the outcome to the sender.
- **Consumers**
  - … are protected.

© 2013 DMARC.org

DMARC – *Why is it important?*

- It is an **ecosystem** story.
  - Protects **brands** by defending against their email being spoofed.
    - Shuts down an avenue leading to orchestrated, large-scale fraud, as well as more targeted spear phishing.
  - Protects **consumers** by ensuring the email they believe to be from the brand is authentic.
    - Helps prevent account hijacking and identity theft.
  - Empowers **mailbox providers** to take definitive action on fraudulent mail.
    - Feedback reporting supports enforcement activities to further increase protection by the entire ecosystem.

© 2013 DMARC.org

60%

global protection in just 1 year

Proof – *Mailbox Adoption in 1 Year*

- **60%** of the world's email boxes are protected by DMARC, representing **1.976 billion** accounts.

- Mailboxes deploying DMARC in 2012:
  - Google (at launch), Yahoo, AOL, & Microsoft
  - Mail.ru (largest mailbox provider in Russia)
  - NetEase (largest mailbox provider in China)

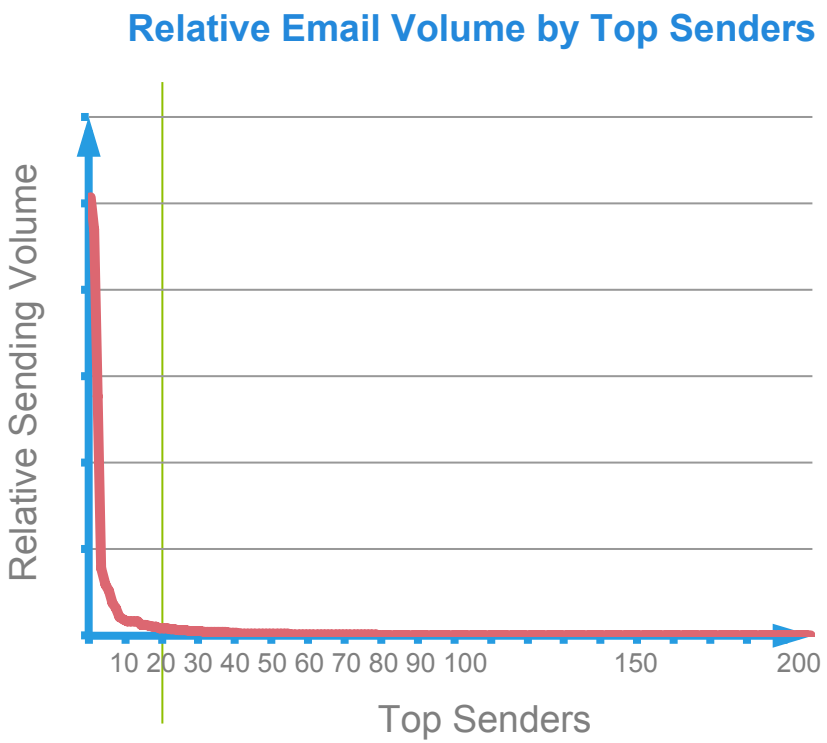
- **80%** of typical US customers are now protected by DMARC.

Source: *Aggregate data provided by DMARC.org Members*

© 2013 DMARC.org

Proof – *Sender Adoption in 1 Year*

- **50%** of the top **20** sending domains publish a DMARC policy
- **60%** of these domains publishing policy belong to companies not directly affiliated with DMARC.org
- **70%** of those domains contain a policy directing receivers take action against unauthenticated messages.



Source: *Aggregate data provided by DMARC.org Members*

© 2013 DMARC.org

Proof – *Effective Protection*

- **118 billion** DMARC messages with a “reject” policy were sent to DMARC compliant receivers in November and December of 2012.
- Mailbox providers blocked more than **325 million** messages because of a DMARC “reject” policy in November and December of 2012
- Of those, **49 million** were from “highly phished” domains – *defined as domains with a DMARC reject policy and more than 10 percent of all messages purporting to be from that domain failing authentication checks.*

Source: *Aggregate data provided by DMARC.org Members*

© 2013 DMARC.org

DMARC Case Studies

- Adoption & Utility Trends in a Large Bank
  - *Provided by Agari*
- Business Intelligence Enabled by DMARC
  - *Provided by Message Bus*
- Reducing Potential Account Compromises
  - *Provided by Return Path*

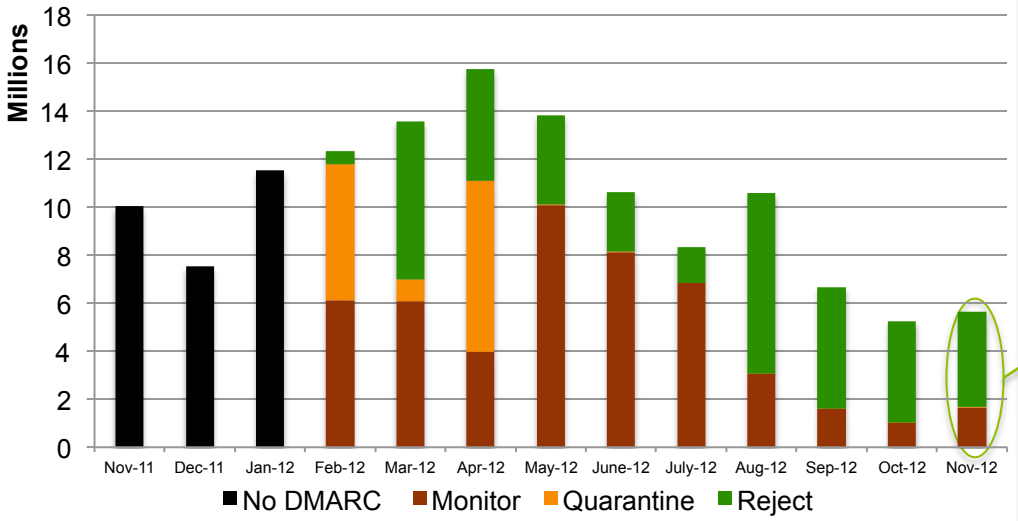
NOTE: *The case studies are provided by permission for use within this presentation. The claims, representations, and data presented are their own and not that of DMARC.org.*

© 2013 DMARC.org

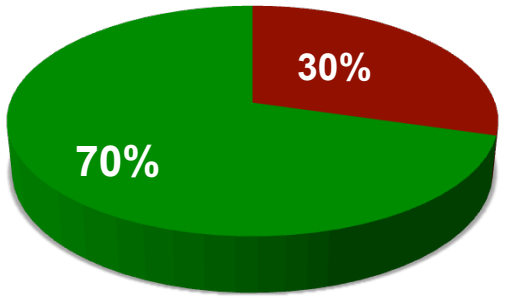
Case Study: *DMARC & a Large Bank*

November 2011 – November 2012	Legitimate Messages	Malicious Attempted	Malicious URLS Submitted for Takedown
Messages Purporting to be from a Large Bank's 200+ domains @ DMARC compliant receivers	1.37 Billion	132 Million	1.4 Million

Policies Applied to Malicious Attempted *(Nov 2011 – Nov 2012)*



Policies Applied to Malicious Messages

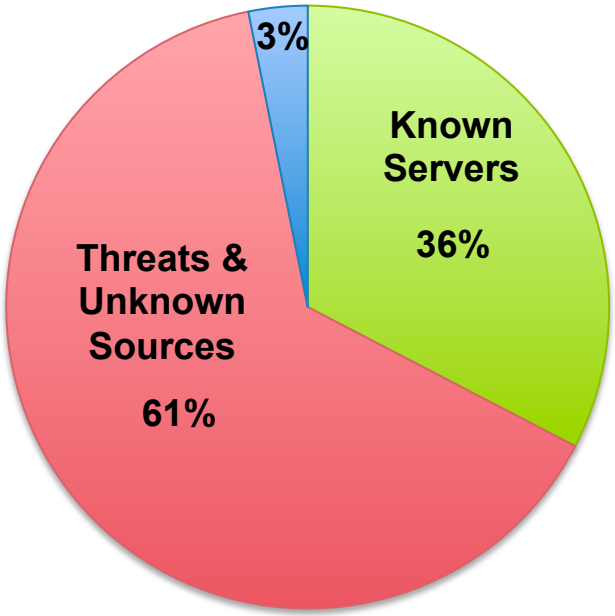


© Copyright 2013, Agari Data, Inc., used with permission in this presentation.

Case Study: *Business Intelligence*

- A large international conglomerate didn't know if they had a spoofing problem or not.
- They published a DMARC "monitor" record (ie. "p=none") to receive RUF & RUA reports.
- They quickly determined they had a problem, and now knew how bad it was.

Actual Email Threat Profile



36% - Known Servers:
Messages sent from servers that were identified as belonging to the organization

3% - Forwarders:
Messages determined to be forwarded by third parties (eg. discussion lists)

61% - Threats & Unknown Sources:
Messages sent by unknown and/or potentially malicious senders

Source: *Case study provided by Message Bus*

© 2013 DMARC.org

Case Study: *Reducing Account Compromises*

Challenge

- Large auction website that sends more than 3 million emails a day

Solution

- DMARC enables security and fraud teams to proactively block customer targeted phishing attacks
- Team uses DMARC to audit mail sending domains to ensure they are properly authenticated and categorizes all mail streams, making it easy to identify suspicious email traffic

Results

- **31% decrease in phishing attempts**
- **62% reduction in incidents of unauthorized account access**
- Safeguarding of brand reputation providing a better user experience for the site's members

Challenge

- The highly recognizable web properties of a global online gaming company were repeatedly getting phished

Solution

- Using DMARC with a rejection policy to block the fraudulent email (phish) being sent purporting to come from these spoofed domains

Results

- Proactive blocking of 100% of all fraudulent mail received at ISP's from highly recognizable, and commonly phished domains

© Copyright 2013, Return Path, Inc., used with permission in this presentation.

DMARC Take-Away

- **DMARC works today**, and continues to improve in effectiveness with each adopter.
- **DMARC adoption** by receivers continues to **accelerate** worldwide.
- **DMARC adoption** by senders is spreading -- we need more to join. All senders should publish a DMARC "**monitor**" record to gain insight.
- Brands in danger of being spoofed should gauge their needs and publish an appropriate "**quarantine**" or "**reject**" record.
- DMARC reporting provides real, meaningful, and actionable **business intelligence**.

© 2013 DMARC.org

DMARC

Domain-based Message Authentication, Reporting & Conformance

Join the discussion at **dmarc.org**