DMARC

Continuing to enable trust between brand owners and receivers

February 2014

DMARC Defined

DMARC stands for:

Domain-based Message Authentication, Reporting & Conformance

(pronounced “dee-mark”)

DMARC.org

DMARC.org is a loose collaboration between organizations working together to combat spoofed domain mail by developing a standardized solution across the Internet.

Agari AMERICAN GREETINGS Aol.

Bank of America CLOUDMARK

comcast facebook Fidelity INVESTMENTS

Google LinkedIn Microsoft

PayPal Return Path TDP Trusted Domain Project

YAHOO! JPMORGAN CHASE & CO. 163 网易免费邮 mail.163.com

For Context: *Phishing continues to be a major pain point across Internet*

The worldwide impact of phishing could be as high as **$2.4 billion.**[1]

The cost per individual to recover from a phishing attack is estimated to be $158.[1]

Email attacks on vendors can mean disastrous results for major brands.[2]

Significant brand damage can occur due to phishing of social media credentials.[3]

Phishing attacks effectively circumvent multi-million dollar security initiatives.[4]

1. 2013 Microsoft Computing Safety Index
2. “Email Attack on Vendor Set Up Breach at Target”, Krebs on Security, February 12, 2014
3. “Phishing Attacks Enabled SEA To Crack CNN's Social Media”. Dark Reading, January 27, 2014
5. “Bad behavior, not malware, puts more of your corporate data at risk”, ZD Net, February 11, 2014

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 simply protected.

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.*

Proof – *Mailbox Adoption*

- **> 60%** of the world's email boxes are protected by DMARC, representing ~ **2 billion** accounts.

- Major Mailboxes Providers Deploying DMARC:
  - GMail, Yahoo, AOL, Comcast, Outlook.com
  - Mail.ru *(largest mailbox provider in Russia)*
  - NetEase *(largest mailbox provider in China)*
  - XS4All *(largest mailbox provider in Netherlands)*

- **> 80%** of typical US users are protected by DMARC.

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

Proof – *Sender Adoption*

- **76.9%** of email received by Gmail is signed using **DKIM**
- Over **500,000 active domains** send email signed using DKIM.
- **89.1%** of email received by Gmail comes from SMTP servers that are authenticated using the **SPF**.
- Over **3.5 million active domains** publish SPF records.
- **74.7%** of email Gmail receives is protected by both **DKIM** & **SPF**.
- Over **80,000 active domains** have already deployed **DMARC**.
- Gmail is able to reject **hundreds of millions** of unauthenticated emails every week using DMARC.

Source: *GMail data released on December 6, 2013*

Proof – *Real Value Proposition*

- **Return Path** reports a **130% increase** in clients and domains publishing DMARC.
- **PayPal** reports a **70% drop** in reported phishing in 2013, and that DMARC stopped ~**25 million** spoofed email messages from reaching their customers during the 2013 holiday buying season.
- **Twitter** reports nearly **110 million** messages per day were spoofing its domains prior to deploying DMARC, reduced to only **1,000** per day after publishing a "reject" policy.
- **Outlook.com** reports a **50% drop** in reported phishing in 2013, in part due to enforcing DMARC.
- **Gmail** reports that a major company benefited from their DMARC policy by a **5000%** decline in spoofed domain attacks during their peak season in 2013.
- **Agari** reports that one of their financial services clients saw a **67% drop** in spoofing levels since deploying DMARC.
- **Publishers Clearing House** reports they used DMARC to block over **100,000** unauthenticated messages in a single 90 day period during 2013.

Source: *DMARC.org press release published on February 18, 2014*

DMARC Case Studies

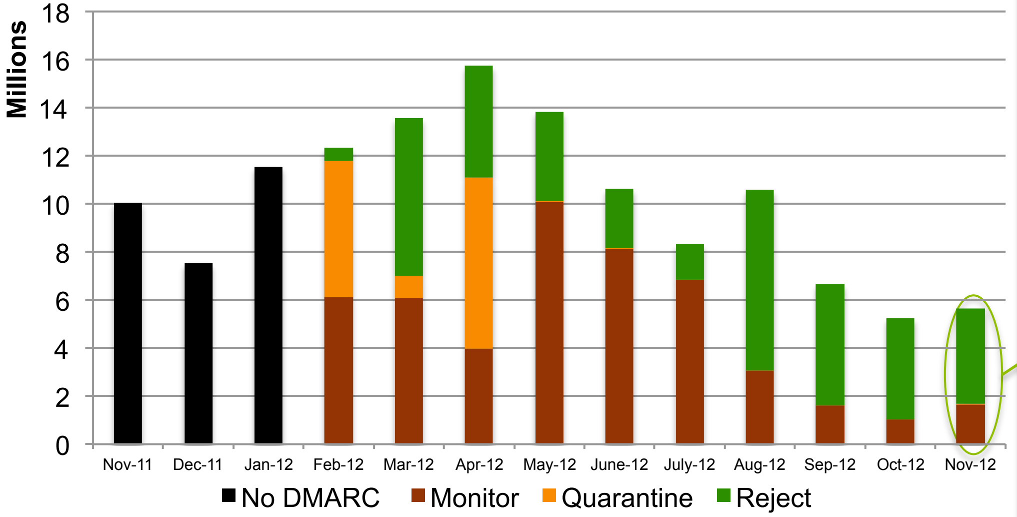
- Adoption & Utility Trends in a Large Bank
  - *Provided by Agari*
- Business Intelligence Enabled by DMARC
  - *Provided by Message Bus*
- Reducing Potential Account Compromises
  - *Provided by Return Path*

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.*

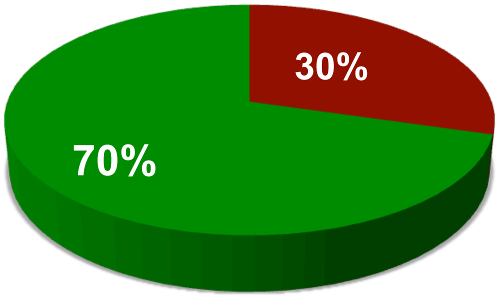
Case Study: *DMARC & a Large Bank*

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)*

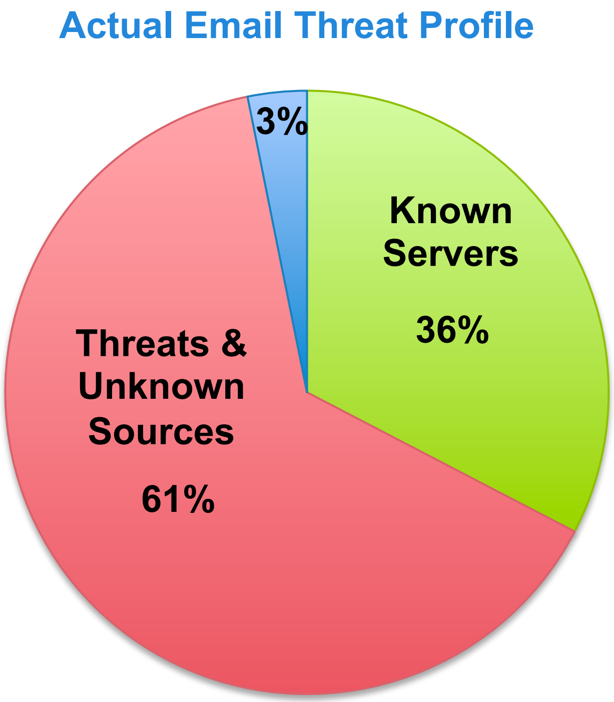


Policies Applied to Malicious Messages



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.



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*

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

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**.

DMARC

Domain-based Message Authentication, Reporting & Conformance

Join the discussion at **dmarc.org**