DMARC and Security

An overview of how DMARC works and what security-related data it can provide

Introduction to DMARC.org

The mission of DMARC.org is to promote the use of DMARC and related email authentication technologies to reduce fraudulent email, in a way that can be sustained at Internet scale. This overall goal is met by educating individuals and organizations through a combination of articles, tutorials, and presentations.

For more information, please visit https://dmarc.org

DMARC.org is an initiative of the non-profit Trusted Domain Project (TDP). For more about TDP, please visit http://trusteddomain.org

Introduction to DMARC.org

The work of DMARC.org is made possible through the generous support of these companies:

Sponsors

Supporters

Have You Got A Phishing Problem?

- How would you know if/when bad actors are impersonating you today?
- Do you know who legitimately sends as you?
- Are you paying third parties to send email using your domain(s) to your employees?
- Would you know if somebody signed a contract to do that tomorrow?
  - It only takes one marketing person with a corporate card…

What Does DMARC Do About That?

- DMARC reports show exactly where messages using your domain come from
- See where all the spammers and phishers send those messages from
- Identify all legitimate senders and verify they implement authentication methods correctly
- DMARC policies can request that all messages failing authentication be blocked
- Protect your customers, partners, and employees

Before There Was DMARC…

- Early 2000's – spam is a nuisance, not a threat

- **Sender Policy Framework** (SPF) emerges in 2003
- One hop - checks the RFC5321.MailFrom ("envelope From")
- Inspired originally by spammers who impersonate random addresses to avoid receiving bounces

- DomainKeys (DK) released in 2004 – later developed into **DomainKeys Identified Message** (DKIM), IETF published 2007
- Cryptographic signature of the message, checked via key in DNS
- Applies even when message is forwarded, *so long as the message is not altered* in any significant way

DKIM and SPF Don't End Spam

- SPF was easy for senders to adopt, no software required
  - Even easier to deploy incorrectly or unwisely!
  - Unclear what action to take when messages don't pass
- DomainKeys known to be temporary, pending release of DKIM
- DKIM work in IETF proceeded very slow (2004-2007)
  - When finally ready, required new/updated software
  - Commercial products delayed until years† after IETF finished
  - Initially imposed a measurable (~10%) overhead on messaging infrastructure

† FOSS code was available quickly, but some vendors still hadn't finished 4 years after

Changes Over The Decade

By 2008:

- Fraudulent (spam and phish) messages deliberately impersonating domains are the norm
- Spam volumes have skyrocketed
- Phishing of customers is a major problem
- Phishing of employees is becoming a problem
- **Mailbox providers still couldn't or wouldn't rely on SPF/DKIM failure alone to automatically block a message**

Promising Signs

- 2007 – eBay/PayPal and Yahoo make a bi-lateral agreement to use DomainKeys to block fraudulent messages

REUTERS EDITION: UK Oct 4, 2007 SIGN IN

Technology | Thu Oct 4, 2007 3:06pm BST

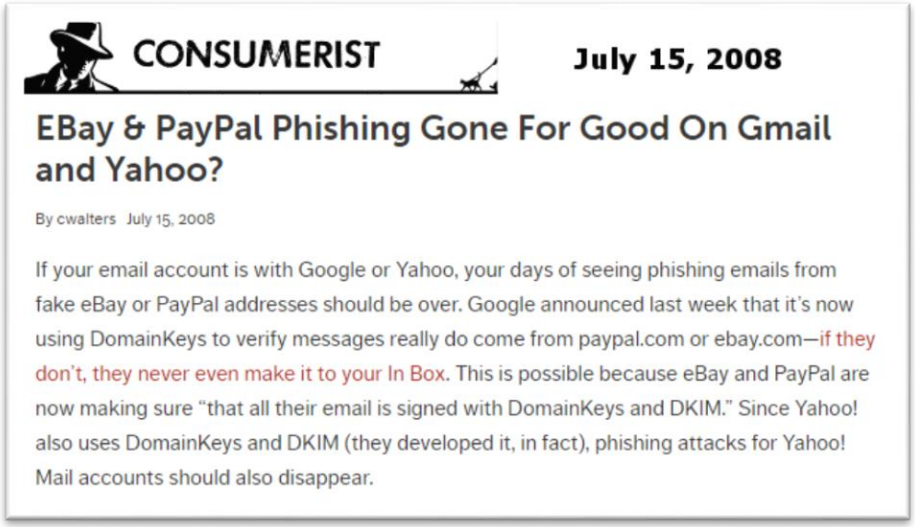
Yahoo, eBay work to block phishing

Yahoo Inc (YHOO.O), is working with auction leader eBay Inc (EBAY.O) and its PayPal payments unit to block fake e-mails to users purporting to be from eBay and PayPal, hoping to spur on an industry that has been slow to fight the scourge of so-called phishing attacks.

EBay and PayPal have upgraded their computer systems to support an emerging technology standard known as DomainKeys invented by Yahoo that authenticates e-mail senders are who they say they are, allowing Yahoo to block fake e-mails.

The technology upgrade will be made available to Yahoo Mail users worldwide over the

- 2008 – GMail joins the program, which includes DKIM
- Demonstrates effectiveness, but not a scalable solution



CONSUMERIST July 15, 2008

EBay & PayPal Phishing Gone For Good On Gmail and Yahoo?

By cwalters July 15, 2008

If your email account is with Google or Yahoo, your days of seeing phishing emails from fake eBay or PayPal addresses should be over. Google announced last week that it's now using DomainKeys to verify messages really do come from paypal.com or ebay.com—if they don't, they never even make it to your In Box. This is possible because eBay and PayPal are now making sure "that all their email is signed with DomainKeys and DKIM." Since Yahoo! also uses DomainKeys and DKIM (they developed it, in fact), phishing attacks for Yahoo! Mail accounts should also disappear.

Now How To Do This At Scale?

- **Open**: A standard freely available to even the smallest sender
- **Simplicity**: Minimize configuration errors
- **Opt-In**: Domain owners will advertise that they're participating
- **Visibility**: Receivers will share statistics with the domain owner
- **Incremental**: Provide features for senders to ramp-up slowly
- **Automatic**: Receivers will honor policies that block messages
  - Good faith, best effort - subject to "local policy overrides"

All these ideas went into the design of DMARC, plus…

What Else Went Into DMARC?

- Nothing wrong with DKIM and SPF as protocols
  - Needed to tie what they authenticate to what the end user / recipient sees
- DMARC relies on DKIM and SPF, but adds **alignment**
  - Alignment requires that the domains DKIM and SPF authenticate must match the domain in the email address in the RFC5322.From header
  - RFC5322.From header is what Outlook, Mail.app, etc show the end user

The details of all three protocols are described in this slide deck:
https://dmarc.org/presentations/Email-Authentication-Basics-2015Q2.pdf

Publishing the DMARC Protocol

- By December 2011 the protocol passed preliminary testing
- The Plan:
  - Publish now (early 2012)
  - Collect real world feedback at Internet-wide scale for a year
  - Then submit to IETF
- Announced and published on January 30, 2012
- 60% of mailboxes worldwide protected by DMARC in six months
- Revised/published as IETF Internet Draft on March 31, 2013
- Published as RFC7489 on March 18th, 2015
- RFC7489 is classed as *Informational* – it is not currently mandatory, or *Standards Track*, like RFC7230/7231

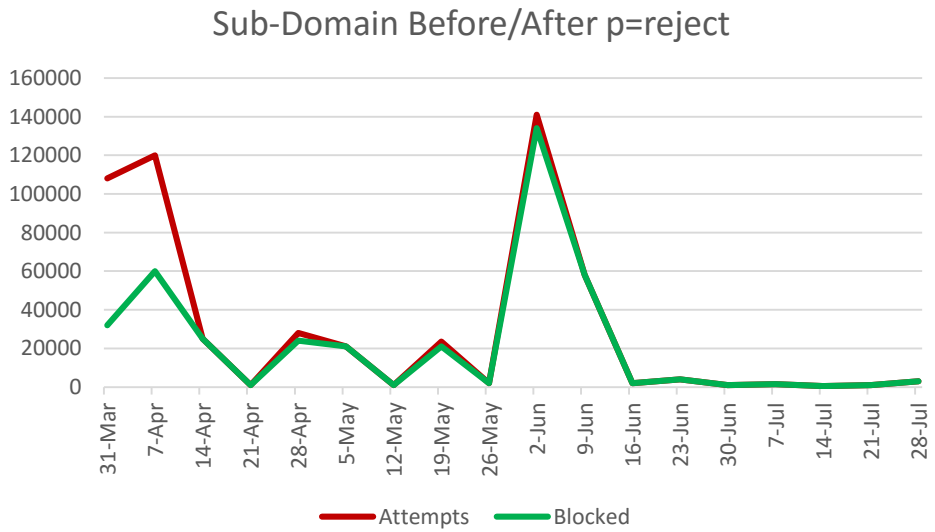
Is DMARC Effective?

In the role for which it was designed, DMARC is very effective:

- Retired domain, not being used by the business
- Several weeks of monitoring showed no activity
- DMARC `p=reject` policy published
- A month later it was used in spam campaign over a major US holiday weekend
- Blocked 99.6% of the 1.8MM message campaign before anybody returned to the office & saw reports

Is DMARC Effective?

- Lookalike sub-domain being used by phishers
- 1/3 or less detected and blocked by content filters
- After `p=reject` policy 97-99% were blocked
- Since messages were blocked, phishers moved on



Does DMARC Provide Useful Data?

Yes! Two kinds of reporting built into DMARC:

- **Aggregate reports** – all email traffic observed using a given domain during the reporting period, typically 8-24 hours
- **Failure reports** – details for specific messages that failed to authenticate

DMARC Aggregate Reports

- Aggregate Reports
  - Report from a Mail Receiver of all email traffic using a given domain in the RFC5322.From
    - Doesn't matter what source it came from, you'll see it
  - Message counts broken out by
    - Sending IP address
    - Authentication results
    - Disposition (delivered, quarantined, rejected, etc)
  - Generally sent daily, or up to several times a day, depending on the Mail Receiver
  - XML format text file, sent via email to an address the domain owner specifies in the DMARC record in DNS

DMARC Aggregate Reports – XML

```
1. <?xml version="1.0" encoding="UTF-8" ?>
2. <feedback>
3.   <report_metadata>
4.     <org_name>google.com</org_name>
5.     <email>noreply-dmarc-support@google.com</email>
6.     <extra_contact_info>http://support.google.com/a/bin/a
7.     <report_id>14093921091532388656</report_id>
8.     <date_range>
9.       <begin>1432598400</begin>
10.      <end>1432684799</end>
11.    </date_range>
12.  </report_metadata>
13.  <policy_published>
14.    <domain>dmarctest.org</domain>
15.    <adkim>r</adkim>
16.    <aspf>r</aspf>
17.    <p>none</p>
18.    <sp>none</sp>
19.    <pct>100</pct>
20.  </policy_published>
```

ct_info>

Who sent the report, what period does it cover, etc.

Policy this domain published during this reporting period

DMARC Aggregate Reports – XML

```
<record>
  <row>
    <source_ip>2607:f8b0:400e:c03::232</source_ip>
    <count>21</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>dmarctest.org</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>dmarctest.org</domain>
      <result>softfail</result>
    </spf>
  </auth_results>
</record>
```

```
<record>
  <row>
    <source_ip>72.52.75.16</source_ip>
    <count>42</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>dmarctest.org</header_from>
  </identifiers>
  <auth_results>
    <spf>
      <domain>dmarctest.org</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

DMARC Aggregate Reports – XML

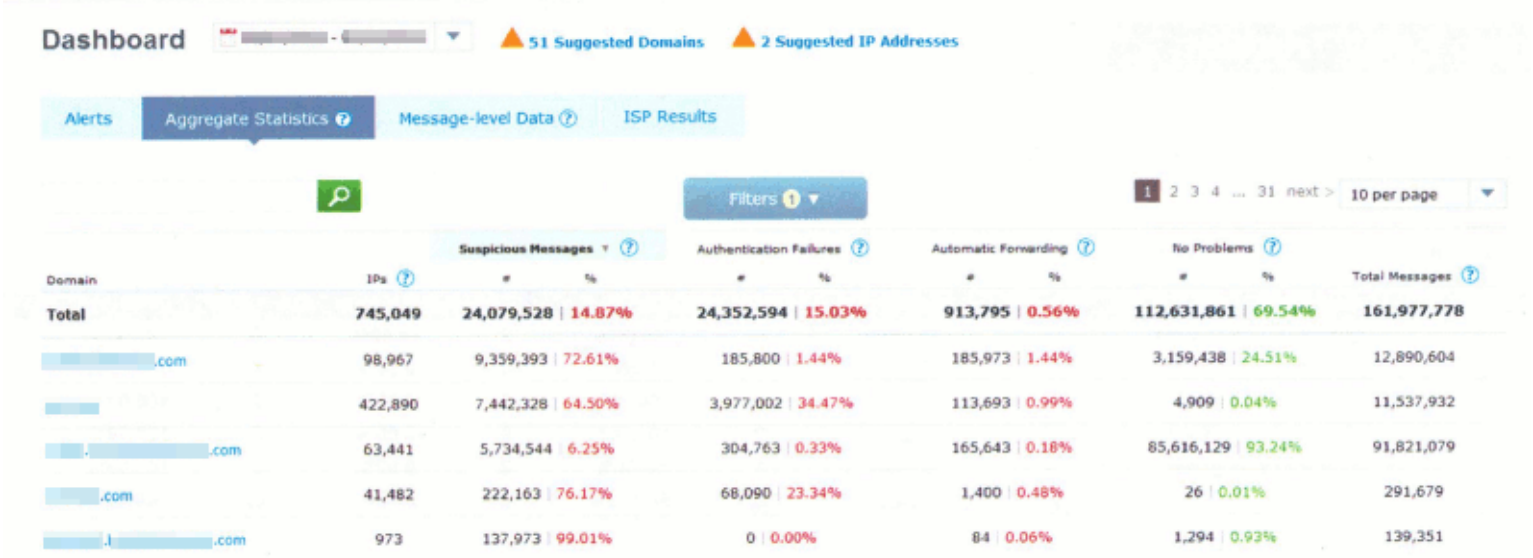
The bulk of the aggregate report consists of records:

- Sending IP address
- Number of messages
- Authentication results
- Disposition (delivered, rejected, etc)

Each IP address usually has several records, reflecting different dispositions, different authentication results, etc.

- Corporate email gateways not signing all messages would surface
- Zombie PCs impersonating different sub-domains would be shown
- Vendors contracted to send 1MM messages a week and only sending 750k would be evident
- All stats can be compared across all major mailbox providers

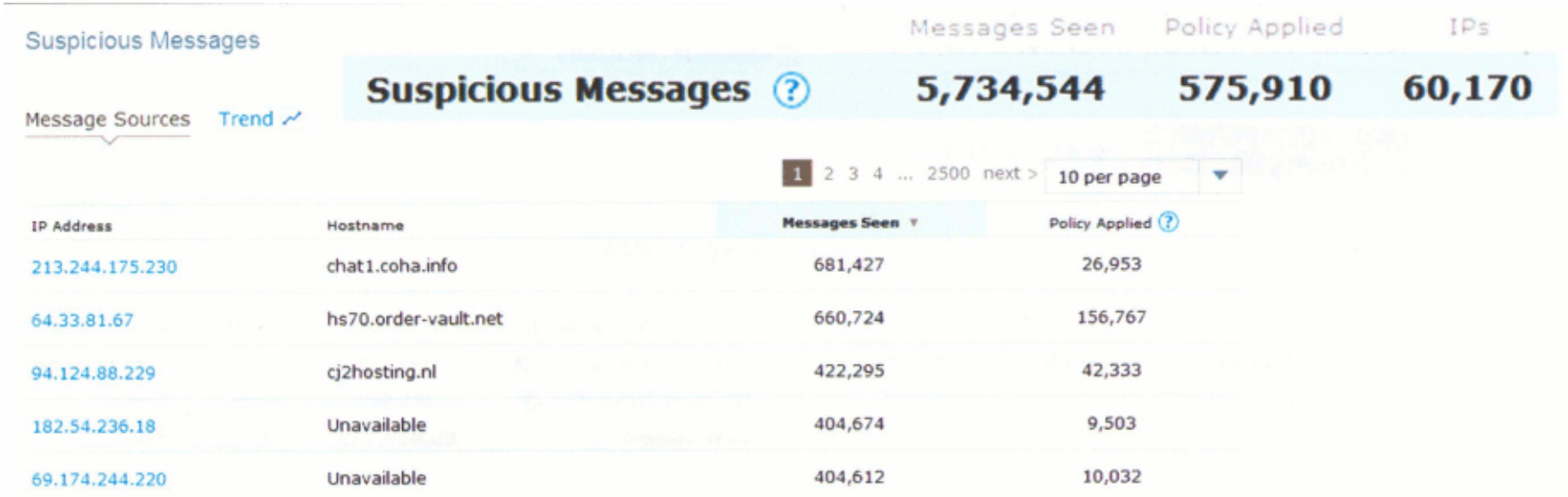
Processed Aggregate Reports



Example of what you might see from processed aggregate reports, showing:

- All messages observed and reported
- How many of those passed authentication checks
- How many of those failed to pass authentication but are probably legit
- How many failed to pass authentication checks but were forwarded (e.g. mailing lists, alumni accounts, etc)
- How many failed to pass authentication and are from unknown sources

Which IPs/Hosts Are Impersonating Us?



Suspicious Messages

Message Sources Trend

	Messages Seen	Policy Applied	IPs
Suspicious Messages	5,734,544	575,910	60,170

1 2 3 4 ... 2500 next > 10 per page

IP Address	Hostname	Messages Seen	Policy Applied
213.244.175.230	chat1.coha.info	681,427	26,953
64.33.81.67	hs70.order-vault.net	660,724	156,767
94.124.88.229	cj2hosting.nl	422,295	42,333
182.54.236.18	Unavailable	404,674	9,503
69.174.244.220	Unavailable	404,612	10,032

You can see which messages failed to authenticate, and don't come from sources you know are permitted to send on your behalf

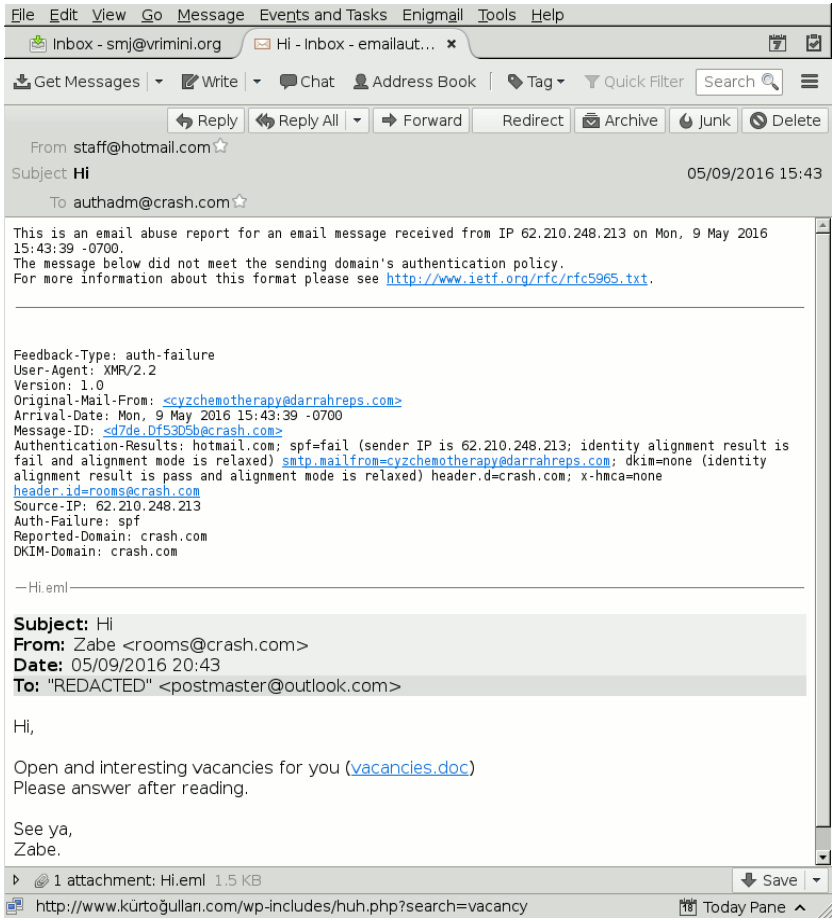
- Includes each IP address sending to each reporting Mail Receiver
- Includes counts of how many of those messages were allowed through, quarantined, or rejected

Who Processes Aggregate Reports?

- There are some scripts/libraries, but not a comprehensive open source package
- You can roll your own – it's just XML…
- Be advised that report volumes can be high for active domains

- Or, over a half dozen commercial firms will do it
- For more information on either option, visit https://dmarc.org/resources/products-and-services

DMARC Failure Reports



- Standard AFRF or IODEF format
- Not batched overnight – generally sent when detected
- May be redacted
- Some just include RFC5822 headers
- Might include URLs from the body
- Others, as here, include the whole email message
- That means you get to see the call-to-action payload…

DMARC Failure Reports

File Edit View Help

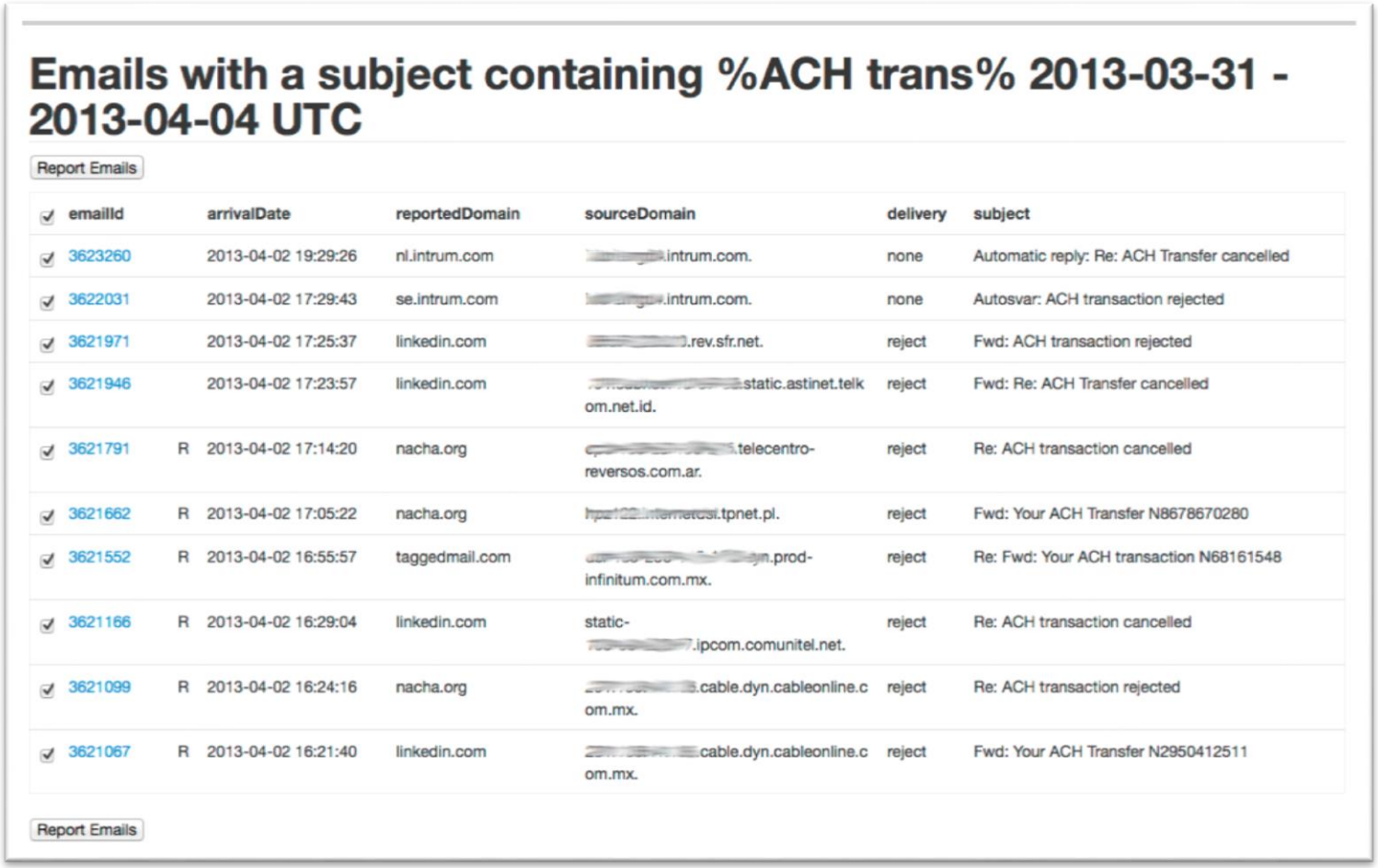
```
Authentication-Results: hotmail.com; spf=fail (sender IP is 62.210.248.213; identity alignment
result is fail and alignment mode is relaxed) smtp.mailfrom=cyzchemotherapy@darrahreps.com;
dkim=none (identity alignment result is pass and alignment mode is relaxed) header.d=crash.com;
x-hmca=none header.id=rooms@crash.com
X-Envelope-Sender: cyzchemotherapy@darrahreps.com
X-SID-PRA: rooms@crash.com
X-AUTH-Result: NONE
X-SID-Result: NONE
Received: from 62-210-248-213.rev.poneytelecom.eu ([62.210.248.213]) by COL004-MC5F31.hotmail.com
with Microsoft SMTPSVC(7.5.7601.23143);
     Mon, 9 May 2016 15:43:39 -0700
Feverish-Equipped-Grassed: 33625
To: "REDACTED" <postmaster@outlook.com>
Content-Type: text/html; charset=iso-8859-1
Thoughtlessness-Sequentialized: b25ba2cac
From: Zabe <rooms@crash.com>
Terrors-Bestow: buggies
Subject: Hi
Message-ID: <d7de.Df53D5b@crash.com>
MIME-Version: 1.0
Fighting-Worriers: 5998326ad13c22cd
Date: Tue, 10 May 2016 00:43:39 -0300
X-Mailer: Testicles 7[string].25[string] (usable)
Content-Transfer-Encoding: 7bit
Return-Path: cyzchemotherapy@darrahreps.com
X-OriginalArrivalTime: 09 May 2016 22:43:39.0939 (UTC) FILETIME=[3B45E730:01D1AA44]

<html>

<body logs="77"> Hi,<br/><br/>  Open and interesting vacancies for you (<a href="http://www.xn--
krtoullar-q9a20blh.com/wp-includes/huh.php?search=vacancy">vacancies.doc</a>)<br/> Please answer
after reading.<br/><br/>
```

Line 23, Col 1

Who Processes Failure Reports?

- You can roll your own – there's at least one complete FOSS package (Lafayette, on Source Forge)
- Same commercial firms that process aggregate reports will generally process failure reports
- For more information on either option, visit https://dmarc.org/resources/products-and-services

Collect and Search Failure Reports



Emails with a subject containing %ACH trans% 2013-03-31 - 2013-04-04 UTC

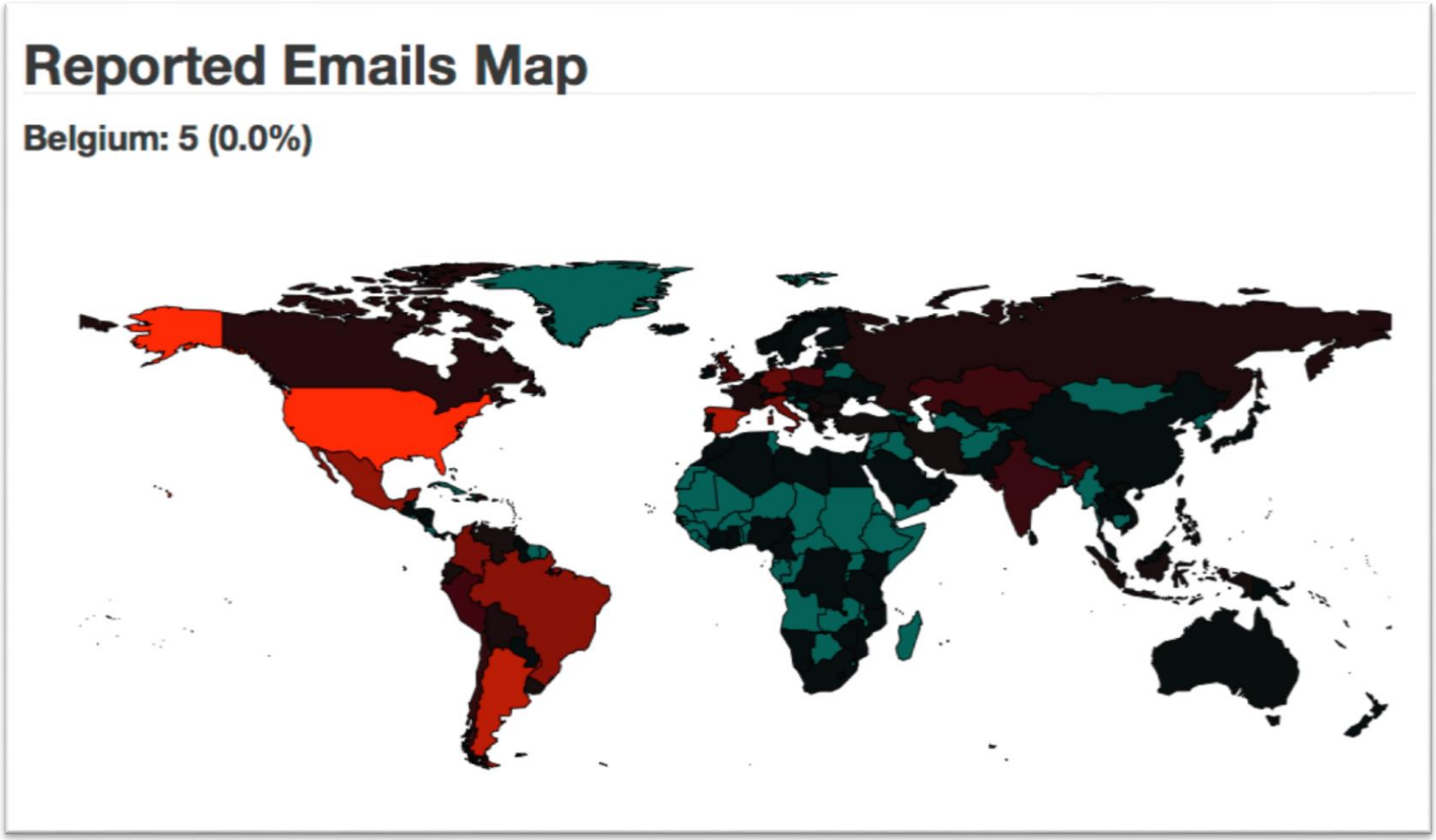
Report Emails

emailId		arrivalDate	reportedDomain	sourceDomain	delivery	subject
3623260		2013-04-02 19:29:26	nl.intrum.com	[redacted].intrum.com.	none	Automatic reply: Re: ACH Transfer cancelled
3622031		2013-04-02 17:29:43	se.intrum.com	[redacted].intrum.com.	none	Autosvar: ACH transaction rejected
3621971		2013-04-02 17:25:37	linkedin.com	[redacted].rev.sfr.net.	reject	Fwd: ACH transaction rejected
3621946		2013-04-02 17:23:57	linkedin.com	[redacted].static.astinet.telkom.net.id.	reject	Fwd: Re: ACH Transfer cancelled
3621791	R	2013-04-02 17:14:20	nacha.org	[redacted].telecentro-reversos.com.ar.	reject	Re: ACH transaction cancelled
3621662	R	2013-04-02 17:05:22	nacha.org	[redacted].tpnet.pl.	reject	Fwd: Your ACH Transfer N8678670280
3621552	R	2013-04-02 16:55:57	taggedmail.com	[redacted].prod-infinitum.com.mx.	reject	Re: Fwd: Your ACH transaction N68161548
3621166	R	2013-04-02 16:29:04	linkedin.com	static-[redacted].ipcom.comunitel.net.	reject	Re: ACH transaction cancelled
3621099	R	2013-04-02 16:24:16	nacha.org	[redacted].cable.dyn.cableonline.com.mx.	reject	Re: ACH transaction rejected
3621067	R	2013-04-02 16:21:40	linkedin.com	[redacted].cable.dyn.cableonline.com.mx.	reject	Fwd: Your ACH Transfer N2950412511

Report Emails

Lafayette, FOSS by LinkedIn

Mapping Reported Messages



Lafayette, FOSS by LinkedIn

Reporting Summary

DMARC reporting can provide a lot of interesting data:

- IP addresses of all hosts – or bots – using your domain
  - Can be geo-located and mapped
  - Identify and compare footprints of different botnets
  - Compare those to botnets used to attack websites
- Which mailbox providers (Gmail, Yahoo, etc) are being targeted
- How many of those messages are being blocked before/after I deploy a DMARC policy
- Headers, URLs, and other details from spoofed messages
- Are any messages from my authorized senders being blocked?
- Are my vendors and ESPs sending authenticated messages?

Presentation Summary

- DMARC will let you see who sends email using your domain, and block unauthorized senders
- Identify vendors, partners and ensure they authenticate correctly
- Map and track all hosts spoofing your domain
- See what payloads, URLs, or other call-to-action they are sending
- Block all unauthorized messages from reaching your customers, partners, and employees

More Information

For more information, including other presentations on DMARC and related email authentication protocols, articles, tutorials, and videos, please visit DMARC.org:

https://dmarc.org