Designing an open source DMARC aggregation tool.

Yadvir Singh

University of Amsterdam

June 30, 2016

Supervised by Michiel Leenaars

Yadvir Singh (University of Amsterdam) Designing an open source DMARC aggregation

June 30, 2016 1 / 17

Introduction

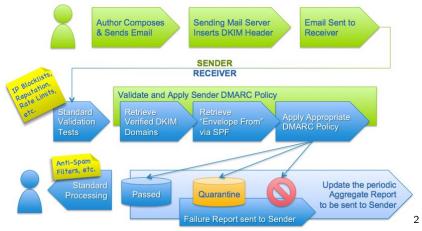
- Domain owner receives daily DMARC reports
- Difficult to process by hand
- Organize reports into a clear overview

DMARC

Research question

How can aggregated DMARC reports provide domain administrators insight into their email domain?

DMARC



DMARC record

v=DMARC1 p=none sp=none rua=mailto:rua@dmarc-research.nl ruf=mailto:ruf@dmarc-research.nl rf=afrf pct=100 ri=86400

▶ ◀ Ē ▶ Ē ∽ � < ⊂ June 30, 2016 3 / 17

イロト イポト イヨト イヨト

DMARC Report

<report_metadata> <org_name>acme.com</org_name> <email>noreply-dmarc-support@acme.com</email> <extra_contact_info>http://acme.com/dmarc/support</ extra_contact_info> <report_id>9391651994964116463</report_id> <date_range> <begin>1335571200</begin> <end>1335657599</end> </date_range>

DMARC Report

<row>

```
<source_ip>192.0.0.1</source_ip>
<count>2</count>
<policy_evaluated>
    <disposition>none</disposition>
     <dkim>fail</dkim>
     <spf>pass</spf>
</policy_evaluated>
</row>
```

<u>Tools</u> Commercial parties

- Several commercial parties
 - Dmarcian
 - Dmarcanalyzer
 - Agari
 - ▶ ...
- Security concerns
- No Open source alternative



- Back end: 100 % Python
- Front end: Bootstrap + Javascript
- MySQL database

- Test domain: dmarc-research.nl
- SMTP server: Postfix
- OpenDMARC, OpenDKIM, pypolicyd-spf



DMARC deployer

Phase 1



Domain	Email Volume	DMARC record
msn.com	3	"v=DMARC1; p=none; pct=100; rua=mailto:d@rua.agari.com; fo=1"
google.com	1	"v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
microsoft.com	1	"v=DMARC1; p=quarantine; pct=1; rua=mailto:d@rua.agari.com,mailto:dmarc_agg@auth.returnpath.net; ruf=mailto:d@ruf.agari.com; fo=1"
gmail.com	3	"v=DMARC1; p=none; rua=mailto:mailauth-reports@google.com"
os3.nl	7	None
posteo.net	1	None

イロト イポト イヨト イヨト



< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

<u>Tools</u> Implementation 2

Status

DMARC status

Policy configured

Sub-policy configured

RUA configured

RUF configured

PCT configured

DMARC record

v=DMARC1; p=none; sp=none; rua=mailto:r

DMARC test

Result

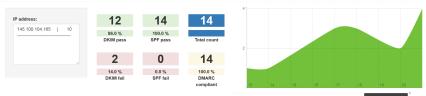
Subject: The contents of

DKIM check passed

SPF check passed sender SPF authorized

DMARC check passed

June 30, 2016 10 / 17



Trusted hosts

Dmarc Compliant

3

<ロト < 回ト < 回ト < 回ト



Foreign hosts

Yadvir Singh (University of Amsterdam) Designing an open source DMARC aggregation

June 30, 2016 12 / 17

Ξ

ヘロト ヘロト ヘヨト ヘヨト

Visualization

- Visualize incoming & outgoing DMARC reports
- Insight into domain abuse
 - by Domain
 - ▶ by IP adress



Visualization Heatmap

Besgygwa.com Tear Bes DMARC 7 TES DMARC 7 GB	kttrevdy.com	jzcaalxc.com traites cenerc.e 201 cenerc.e 50	jmjfkymu.com 1844-337 084462-9-338 084462-9-33	fqxqgxst.com Text 835 CMARC # 833 CMARC # 23	Socipbnx.com Bair 713 CRANC.P 608 DRMAC # 13	etizgmvn.com Bor 203 DHUAC/2 233 DHUAC/2 2	doqkzydn.com Bai 171 CHARC # 170 CHARC # 1
						kjyhalay.com Inter113 Inter210 Inter210	yszxqeoc.com biacarr biaccare citikacare
qumtkqjj.com Tear 951 DMAC # 365 DMAC # 365							mnuviycq.com bid 418 croute # 256 biolog # 117
The Transmost of the Transmost of Transmost	LDCXODZDI.COM Tead ARL DMARC # 201 DMARC # 200	friulhun.com	gvjjtfqp.com Beal BB1 CBMAC # 405 CBMAC # 408	ombbomrc.com Intel 113 DIMAC P 61 DIMAC P 52	xsctvgvo.com 344 343 CRANC # 248 CRANC # 248	gkipmret.com Institut DRAG-9 381 DRAG-7 256	emxkrvnc.com Bisl 302 DMAC-F 305 DMAC-F 187
				X7Wretyy.com Brai 092 CRANC P 338 CRANC P 338	pzdpmjra.com Trai 371 CRANC # 172 CRANC # 159	SSwewbdn.com Brai 426 DRMAC # 189 DRMAC # 227	ansdgoui.com Trai 728 BMARC# 352 BMARC# 376
							wgyfyoqt.com Bouilis chunciens chunciens
Vnpddzmi.com Baar 383 EMMC + 20 EMMC + 283	Caulurqi.com Barezz DRANC P ID DRANC P 127	cdvxprfr.com Brai 231 DRMCCP 39 DRMCCP 292	jzzzgeen.com Bai (9) DRAC 9 13 DRAC 9 13	ywxolbvc.com Bra 778 CRAVE P 329 CRAVE P 328		hwqkzvkd.com	gbduzuby.com brailee cease = 10 beac = 10
akwucon.com	zbrsejnh.com	mfrxqggy.com teat iss onwice 22 convect #23	rvunvggp.com	obyzgtvj.com text 803 Ometice 34 Devec + res	dykvkzcv.com text too 044462943 049462943	lebthssw.com	mfwnpzmk.com

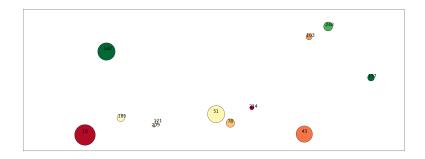


イロト イポト イヨト イヨト

June 30, 2016 14 / 17

Э

Visualization Bubblechart



June 30, 2016 15 / 17

프 > 프

Image: A math a math

Conclusion

- DMARC reports can give domain owners insight into their security configuration
- Can provide insights into domain abusage
- Track domain health over longer timespans.

Questions



²https://dmarc.org/overview/

Yadvir Singh (University of Amsterdam) Designing an open source DMARC aggregati

June 30, 2016 17 / 17

H 1

¹ https://dmarc.org/