***WARNING: STRESS INDUCING PRESENTATION***

# New Spam Filtering and Phishing Protection Approach called DMARC

**Ben Serebin**
***Ehlo & Cloud Consultant***
**REEF Solutions LLC (www.reefsolutions.com)**

Presented April 10, 2018 at NYExUG Meeting
Last Updated on April 10, 2018

# About Ben Serebin

- Working in the IT field since 1996 (over 20 years)

- Specialty is Exchange/Email Environments, Spam Filtering, DNS, & complex wireless deployments.

- Recent/Upcoming Fun Tech Projects: Upgrading Core Switching Infrastructure to L3 Stacked, In Private Cloud Datacenter upgraded to 220v power & forced to deploy step down transformer due to 256v, automatic transfer switches for 110v single PSU equipment.

- Current Environment: iPhone 7 Plus, Hyper-V 2012 R2/2016, Kemp Virtual LBs in HA, DAGed Exchange 2013. Clustered Barracuda Spam Filters and Mail Gateway (IceWarp). Lots of SSD DAS, RAID 5 (4-6 drive Samsung 840/850) based Dell R410/610, iSCSI Storage, and 10Gb SFP+.

# Planned Agenda – Will Go Off-Roading

1. DMARC via 30 Seconds Elevator Pitch
2. Example & D+M+A+R+C
3. Prerequisites Overall
4. Implementation Requirements
5. Office 365 Requirements
6. Example & Recommendations
7. DMARC DNS
8. Recommendations
9. Top 4 Challenges
10. Final Thoughts

# Elevator Pitch for DMARC

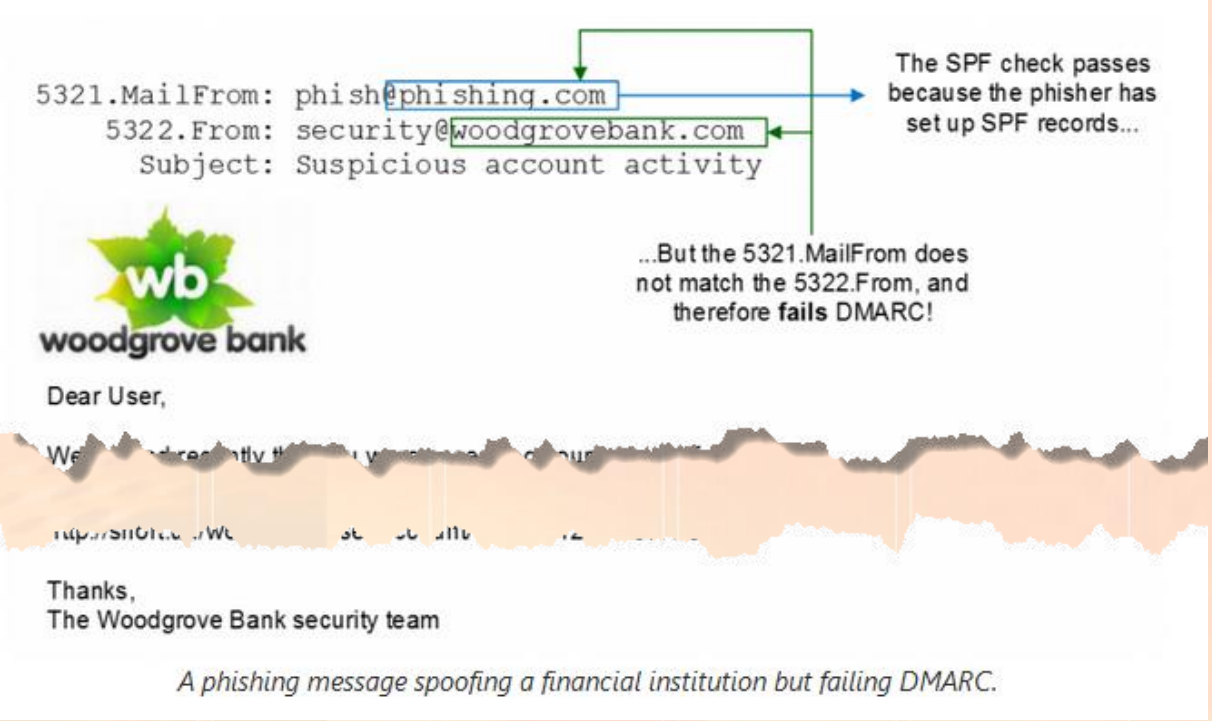
- **Does your organization (***especially hospitals, financial firms, regulatory agencies/organizations, etc).* **value your customers having trust that your emails are not fake?**
- **DMARC is a superhero for the job! It offers receiving servers a feedback loop for improving the awesome job they're doing!**
- **DMARC might be your favorite email validation mechanism built on top of 2 anti-spam approaches: SPF + DKIM.**

***[Note to Self: we're on the honeymoon phase of the presentation]***

***[no comment]***

# Example & DMARC Acronym

Outlook vs Gateway Filtering
5321.MailFrom = SMTP
5322.From = Outlook Display




above image from https://blogs.office.com/en-us/2015/01/20/enhanced-email-protection-dkim-dmarc-office-365/

**DMARC**

**D**omain = email sender's

**M**essage = relates to

**A**uthentication = headers modified

**R**eporting = DNS based reporting addresses

**C**onformance = how in compliance are you

# Prerequisites

**1) Working Email Sending Server (e.g. Exchange, Office 365)**

**2) SPF (Sender Policy Framework) Setup**

- **Uses DNS records to validate the authenticity of email messages.**
- **No 3rd party software is required.**

**3) DKIM (DomainKeys Identified Mail) Setup**

- **Signing software is required on all sending mail servers.**
- **Signing is based on public (in DNS) and private (on sending server) keys**

# Implementation Requirements (Private Cloud)

DKIM Signer from Stefan Profanter & Alexandre Laroche (open-source $0) – OUTBOUND ONLY

- .NET 3.5 (Exchange 2007 & 2010). 2007 SP3+, 2010 RTM+, SP1+, SP2+, SP3+,
- .NET 4.0 (Exchange 2013 & 2016) 2013 CU1-CU19 (not CU20), 2016 RTM-CU8 (not CU9)
- Latest March 2018 CU's for 2013 & 2016 are not officially supported yet as of 4/8/18. Last 48 hrs, developer commits are in place for release for 2013 CU20 and 2016 CU9.

DKIM for Exchange from Email Architect (commercial $300/$800) – INBOUND & OUTBOUND

- Edge or Hub Transport for Exchange 2007, 2010, 2013, 2016 (2000 and later)
- Enabled Default is OUTBOUND
- INBOUND filtering is Disabled. Config file for enabling.
- INBOUND quarantine filtering leverages Transport Rules

**Recommended Solutions**

DKIM Signer - https://github.com/Pro/dkim-exchange/blob/master/README.md

Email Architect - https://www.emailarchitect.net/domainkeys/kb/dkim_exchange_2007_2010_2013.aspx

# How To Implement in Office 365

**Congrats, it's easy! No Action Required** - Office 365 enables DKIM Signing by default.

- Verify by going to Office 365 – Exchange admin center – dashboard – dkim (under protection section) – confirm it's enabled for your domains.
- Outbound requires DNS record like Private Cloud

**IMPORTANT POINTS**

Office 365 is currently ignore "reject" settings. It will only quarantine.

Primary MX must be Exchange Online Protection, otherwise DMARC will not work.

Excellent Resources

https://blogs.msdn.microsoft.com/tzink/2014/12/03/using-dmarc-in-office-365/

https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx

# Example & Recommendations for DMARC Record

Email Sender -> ben@to-dmarc-or-not.com

v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarc@to-dmarc-or-not.com,fo=1

**Tags [recommendation]**

v = version [DMARC1]
p = policy for org domain (none, quarantine or reject) [quarantine]
sp = policy for subdomains of org domain (none, quarantine or reject) [quarantine]
pct = % of messages that are filtered [100]
rua = reporting URI or address for aggregate reports XML (can be 3rd party)
ruf = reporting URI or address for forensic reports (can be 3rd party) [dedicated email account]
fo= reporting for pass failures, 1 = any fails to pass, 0 = everything fails to pass [1]
adkim = alignment mode for DKIM (relaxed or strict, “s” or “r” which is default) [r]
aspf = alignment mode for SPF (relaxed or strict, “s” or “r” which is default) [r]

Show & Tell: Hotmail.com Example
https://dmarcian-eu.com/dmarc-inspector/hotmail.com

# Creating the DMARC DNS Record

1) Determine your DMARC configuration
2) Create a DNS TXT Record in your email domain using "_dmarc".
3) TXT value per previous example "v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarc@to-dmarc-or-not.com,fo=1"
4) TXT value minimum requirements:"v=DMARC1;p=quarantine"

# Recommendations

**If you manage large environments – 3rd Party Reporting Solutions**

Agari http://agari.com – Microsoft, AOL, etc use for aggregated reporting

DMARCIAN, https://dmarcian.com – Google, Linkedin, Yahoo, etc use for aggregated reporting

ReturnPath, http://www.returnpath.com – aggregated DMARC reporting tools for senders and receivers

**Tools for Checking DMARC**

DMARCIAN, https://dmarcian.com

# Top 4 Challenges of DMARC

1. **DMARC only is for FROM address. Ignores the MESSAGE BODY and ATTACHMENTS**. Example: Fails to detect URLs in body not matching MailFrom / From.
2. **Ridiculously Complicated to Implement**. Take the 3 hardest approaches for spam filtering and then there's no guarantee you'll see any reduction in spam.
3. **Camouflaging domain names.** Worse when you have o/0 or L/i/1 in your domain name.

accounting@woodgrovebank.COM

ACC0UNTING@W00DGR0VEBANK.COM

ACCOUNTING@WOODGR0VEBANK.COM

accounting@ClTI.COM

accounting@lDBNY.COM

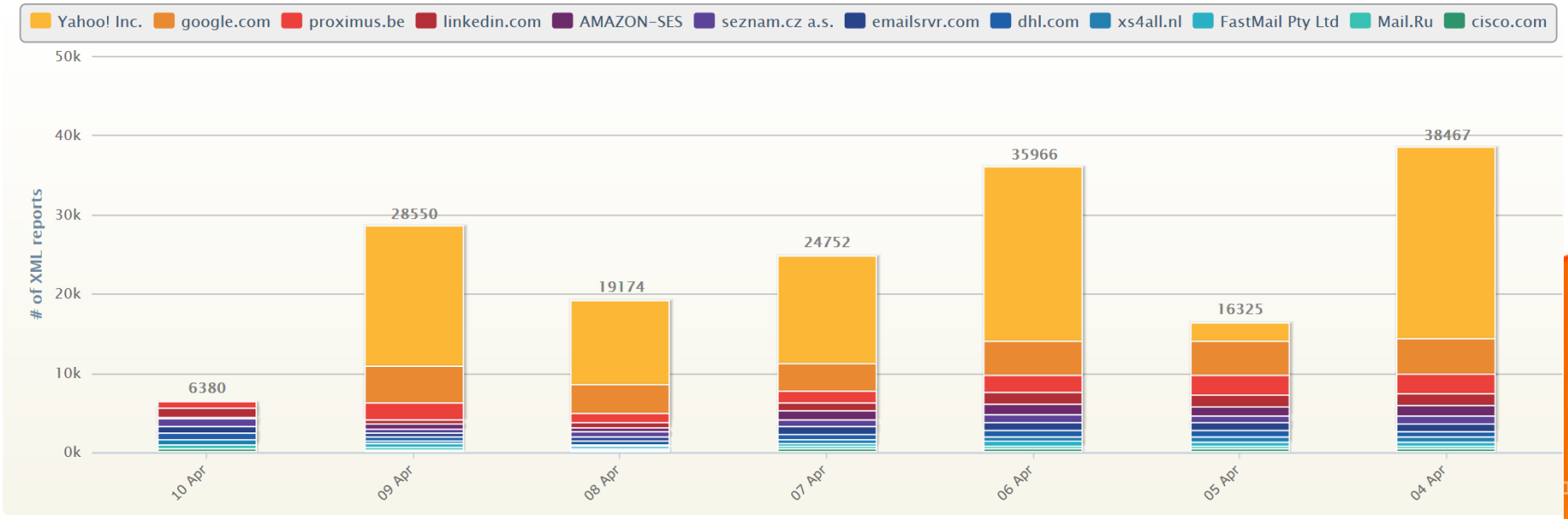
4**. Failure of Adoption: Sender ID, DomainKeys (DK), etc.**

Examples of Compliance

https://www.phishingscorecard.com/ScoreCard/International/Internet/Mailproviders/MTAtOS0zNw%3d%3d

# Final Thoughts in DMARC
# WHERE, WHEN, WHY
# Or a Better Solution in 5 Letters (S/MIME)?

This graph shows dmarcian-eu's top 12 DMARC XML data providers for the past week (dates in UTC):




The following is an exhaustive list of all providers that have sent us data over the past week (UTC). Counts indicate the number of XML reports received.

Search:

| Provider | Total | 2018/04/10 | 2018/04/09 | 2018/04/08 | 2018/04/07 | 2018/04/06 | 2018/04/05 | 2018/04/04 |
|---|---|---|---|---|---|---|---|---|
| Yahoo! Inc. | 90263 | 0 | 17705 | 10612 | 13585 | 21979 | 2280 | 24102 |
| google.com | 25018 | 0 | 4577 | 3703 | 3428 | 4267 | 4442 | 4601 |
| proximus.be | 12572 | 792 | 2238 | 1129 | 1501 | 2211 | 2342 | 2359 |