DMARC Bootcamp

Shehzad Mirza
Director of Operations
smirza@globalcyberalliance.org
gca-dmarc@globalcyberalliance.org
Bootcamp Plan and upcoming Webinars
Weeks One-Two: Getting Started

• Sept 10th - Bootcamp introduction and DMARC: An Overview

• Sept 18th - What are SPF and DKIM
Weeks 3-4: Time to Implement!

- Participants should implement DMARC during these weeks

- Sept 24 or Sept 30 - DMARC Technical Details and Windows DNS
- Sept 25 or Oct 2 - DMARC Technical Details and BIND
- Sept 26 or Oct 3 - DMARC Technical Details and Cloud DNS
Weeks 5-6: On Going Management: Analyze, Review and Adjust

• Oct 8th - Matthew Vernhout (Director, Privacy & Industry Relations, 250ok)
• Oct 9th – John Wilson, Andrew Coyle (Agari) and John Aziz (Senior Security Engineer, InfoTrust)
• Oct 10th – Ash Morin (Deployment Manager – Americas, dmarcian)
• Oct 11th - Harry Frearson (Red Sift)
• Oct 14th - Sibrina Subedar (VP Product Marketing, Valimail)
• Oct 15th – Abdullah Mirza (Director, DMARC360) and Shahbaz Khan (DMARC360)
• Oct 16th - Ana-Maria Rosu, Rick Velthuijsen and Danny Hoogeveen, DMARC Analyzer

• On October 17th - DMARC Bootcamp wrap up session
PHISHING
PHISHING
PHISHING

- Could lead to
  - Ransomware or other malware
  - Fraud (false wire transfer requests)
  - Theft of PII

- Why is it successful?
  - Difficulty in determining if message came from legitimate source
  - From\$Sender address is spoofed
### PHISHING STATISTICS

#### Global Phishing Statistics
- **76% of businesses** reported being victim of a phishing attack in 20171.
- **90% of all breaches** involve phishing attacks*.
- **Nearly 1.5 million** new phishing sites were created monthly in 20172.
- **76,328 phishing sites** were detected by APWG for 2018 Q4 report*.
- **180,768 phishing sites** were detected 1st quarter 2019 3.
- **3.4 billion fake emails** are sent daily worldwide2.
- **138,328 phishing sites** were detected by APWG for 2018 Q4 report.
- **180,768 phishing sites** were detected 1st quarter 2019.
- **3.4 billion fake emails** are sent daily worldwide.
- **80% of mailboxes** worldwide are doing DMARC checks on inbound mail4.
- **Only 1 out of 5 DMARC records** is actually protecting its domain from fake email4.

#### Europe Phishing Statistics
- **74% of cyber-attacks** entered a system as an email attachment or link in 20177.
- **15,549,633 suspicious emails** came from Europe in 2018, and 23.4% were actually suspicious*.
- **10,856,172 suspicious emails** came from the United Kingdom in 2016, and 66.6% were actually suspicious*.
- **5,607,213 suspicious emails** came from France in 2018, and 54.0% were actually suspicious*.
- **5,207,620 suspicious emails** came from the Netherlands in 2018, and 66.6% were actually suspicious*.
- **9% increase** in phishing volume for Great Britain in 20189.
- **9% increase** in phishing volume for Great Britain in 2018.

#### USA Phishing Statistics
- **38 million** fake messages in 1st quarter 2019 sample emanate from US-based sources7.
- **16,956,172 suspicious emails** came from the United States in 2018, and 66.6% were actually suspicious*.
- **5,207,620 suspicious emails** came from France in 2018, and 54.0% were actually suspicious*.
- **84% of total phishing volume target organizations in the United States8**.
- **84% of total phishing volume target organizations in the United States**.

#### New Zealand Phishing Statistics
- **1,131 incidents** were reported in 2017 with over a $5.3 million total financial loss11.
- **1,131 incidents** were reported in 2017 with over a $5.3 million total financial loss.
- **New Zealand saw a 93% increase in phishing volume in 2019**.
- **New Zealand saw a 93% increase in phishing volume in 2019**.
- **42% of phishing attacks** still get through to employees even though 50% of small businesses provide cyber security training13.

#### Canada Phishing Statistics
- **1,550 incidents** were related to phishing and credential harvesting in 201812.
- **1,550 incidents** were related to phishing and credential harvesting in 2018.
- **84% of total phishing volume target organizations in the United States**.
- **84% of total phishing volume target organizations in the United States**.

---

7. https://valimail.docsend.com/view/7w8ggxf
Business Email Compromise (BEC) in $$$

City - $1.04 million
City - $1.73 million
City - $800K
Religious Institution - $1.75 million

(source: bleepingcomputer.com)
Types of Spoofing

• Display NameSpoofing - “Company <person@yahoo.com>”

• Domain Spoofing - “Company <person@company.com>”

• Lookalike Domain Spoofing - “Company <person@c0rnpany.com>”
SOLUTION: DMARC

A PROVEN WAY TO MITIGATE RISK

Domain-based Message Authentication, Reporting and Conformance (DMARC)

It’s like an identity check for your organization’s domain name.
What is DMARC?

A DMARC policy allows a sender to indicate that their messages are protected, and tells a receiver what to do if one of the authentication methods passes or fails – such as send the message or junk/reject the message.
**DMARC** prevents spammers or **phishers** from using valid organization names for email fraud.

**DMARC** increases customer confidence and trust.

It protects the integrity of your brand.
Additional Benefits of DMARC

• Inbox Protection on the Consumer side:
  • DMARC Verification, not policy
  • 80 percent of the current total number of worldwide email accounts (source: Valimail).

• Deliverability

• Visibility: Provides insight into attempts to spam, phish, or even spear-phish using your organization’s brand/name
What is DMARC? (con’t)

**Domain-based Message Authentication, Reporting & Conformance**

Policy Is FREE To Use
Uses Domain Name Server to define the policy

Verification portion will have cost**
What does DMARC apply to?

• ANY PUBLIC DOMAIN
  • whether used for email or not
Items Needed for Implementation

- IP addresses of Mail system(s)/server(s) used for org
- Admin level access to DNS for organization
Items to Plan for

• Understanding SPF, DKIM and DMARC
• Understand the three policy levels of DMARC
• Does email server support DKIM?
• List of public domains used by organization

• Potential Unknowns:
  • Is your organization using 3rd party vendors?
    • Do they support SPF and/or DKIM?
    • Mail systems that IT staff is unaware of

• If you have subdomains - Consider creating a DMARC policy for subdomains.

• DMARC report analysis
  • email address to send reports
Proper Implementation

DMARC implementation requires Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) in order to work

• SPF is used to define which mail servers are authorized to send mail
• DKIM is used to add a digital signature for an additional layer to authenticate the sender
DMARC

What happens to the messages?

• Depends on the policy setting:
  • **None** - reports possible suspicious mail messages, but all mail is sent to Inbox
  • **Quarantine** - fail SPF/DKIM and alignment, message is sent to spam/junk folder
  • **Reject** - fail SPF/DKIM and alignment, message is dropped and not delivered at all

• Best practice is to start at None and gradually move to Reject
Overview

1. DMARC
   - Published DMARC Record

2. Sender's Inbox
   - Sends Email

3. Sending Org's Email Server
   - Sends Email

4. Recipient's Email Server
   - Sends Email

5. DMARC
   - Check sending org's DMARC record upon receipt

6. Recipient's Inbox
   - Pass on Valid Email
     - Reject Policy
     - Quarantine Policy

7. Send Reports Back
   - Quarantine - failed DMARC policy, message is sent to Recipient's SPAM/Junk folder.
   - Rejected - failed DMARC policy, message is dropped and not delivered at all.
DMARC DNS TXT Record

- Basic:
  Host: _dmarc. <domainname>
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
ruf=mailto:<email address>;

- Complex:
  Host: _dmarc. <domainname>
  Value: v=DMARC1; p=none; rua=mailto:<email address>;
ruf=mailto:<email address>; fo=1; adkim=r; aspf=r; pct=100; rf=afrf;
ri=86400; sp=reject;
DMARC Reports

• DMARC generates two types of reports:
  • Aggregate
  • Forensic (or Failure)

• Reports sent in XML format to email of choice (can be sent to multiple addresses)
• Number and length of reports is dependent on amount of email sent
• Reports will provide insight as to which messages were marked as suspicious
• Allows for IT staff to correct any issues with valid messages being dropped by the policy
Sample Aggregate Report

<?xml version="1.0" encoding="UTF-8"?>
<feedback>
<report_metadata>
<org_name>google.com</org_name>
<email>noreply-dmarc-support@google.com</email>
<extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
<report_id>6156901232184779430</report_id>
<date_range>
<begin>1466121600</begin>
<end>1466207999</end>
</date_range>
<policy_published>
<domain>globalcyberalliance.org</domain>
adkim<r>aspf<r>p<quarantine>sp<quarantine>pct100</pct>
<policy_published>
<record>
<source_ip>2607:f8b0:4001:c0b::22f</source_ip>
<count>2</count>
policy_evaluated
disposition<dkim>spf<result>pass<result>
dkim<spf<result>pass<result>
<identifiers>
<header_from>globalcyberalliance.org</header_from>
<auth_results>
dkim<domain>globalcyberalliance.org</domain><result>pass</result>
<spf<domain>globalcyberalliance.org</domain><result>pass</result>
<auth_results>
Concerns with Implementation

• Not a silver bullet
  • Only protects domain policy is applied to
  • Does not protect against variations of organization’s domain name
  • Limitations of SPF
  • Protects against one type of email spoofing

• Email could break
  • Consider implementing DMARC at level ‘none’ to start

• Not enough resources
  • Implementation can be time consuming, especially if there are multiple sub-domains
  • Resources needed more for analysis of reports than implementation

• Mailing list and Mail forwarders
  • Breaks DMARC (as well as SPF and DKIM)
  • Solution – Authenticated Received Chain (ARC) – arc-spec.org
The ROI of DMARC

- **326%** Return on investment
- **$19M - $66M** (USD) annual savings
- **4m** Increase return on customer engagement
- **1.1m** Reduced need for customer support
- **718k** Reduced cost of cybersecurity insurance
- **10%** Rise in response rate to email campaigns

Report released on BEC:
- **1,046** domains that have deployed DMARC at a policy level of “reject” or “quarantine,” after using GCA’s Setup Guide
- Full report at [www.globalcyberalliance.org](http://www.globalcyberalliance.org)

Read the full report at agari.com/roi
Next Webinar:
Overview of SPF and DKIM
Sept 18, 2019
Thank You!

Shehzad Mirza
gca-dmarc@globalcyberalliance.org
smirza@globalcyberalliance.org