Shehzad Mirza
Director of Operations
smirza@globalcyberalliance.org
gca-dmarc@globalcyberalliance.org
Bootcamp Plan and Upcoming Webinars
Bootcamp Overview

Must attend live sessions for certificate (1 per week)

• **Week One: Getting Started**
  • *May 5th*: Webinar - BEC and DMARC in a Nutshell

• **Weeks Two and Three: Time to Implement!!**
  • *May 12*: What are SPF and DKIM?
  • DMARC in Detail and Online Technical Demos (*only need to attend one of the three*).
    • *Tuesday, May 18th*: demo of Window DNS
    • *Wednesday, May 19th*: demo Linux DNS
    • *Thursday, May 20th*: demo of Cloud DNS

• **Week Four: Ongoing Management**
  • *May 26th*: DMARC Reporting & Analysis: What Happens Next

• **Week Five: Wrap-up Session**
  • *June 2nd*: Bootcamp Review and Additional Protocols
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
### Business Email Compromise (BEC) in $$$

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

(source: bleepingcomputer.com)

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Loss</th>
<th>Crime Type</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEC/EAC</td>
<td>$1,866,642,107</td>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>241,342</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>$600,249,821</td>
<td>Non-Payment/Non-Delivery</td>
<td>108,869</td>
</tr>
<tr>
<td>Investment</td>
<td>$336,469,000</td>
<td>Extortion</td>
<td>76,741</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>$265,011,249</td>
<td>Personal Data Breach</td>
<td>45,330</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>$219,484,699</td>
<td>Identity Theft</td>
<td>43,330</td>
</tr>
<tr>
<td>Spoofing</td>
<td>$216,513,728</td>
<td>Spoofing</td>
<td>28,218</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>$213,196,082</td>
<td>Misrepresentation</td>
<td>24,276</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>$194,473,055</td>
<td>Confidence Fraud/Romance</td>
<td>23,751</td>
</tr>
<tr>
<td>Tech Support</td>
<td>$146,477,709</td>
<td>Harassment/Threats of Violence</td>
<td>20,604</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>$129,820,792</td>
<td>BEC/EAC</td>
<td>19,369</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>$128,916,648</td>
<td>Credit Card Fraud</td>
<td>17,614</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>$109,938,030</td>
<td>Employment</td>
<td>16,879</td>
</tr>
<tr>
<td>Other</td>
<td>$101,523,082</td>
<td>Tech Support</td>
<td>15,421</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>$83,215,405</td>
<td>Real Estate/Rental</td>
<td>13,638</td>
</tr>
<tr>
<td>Extortion</td>
<td>$70,935,939</td>
<td>Advanced Fee</td>
<td>13,020</td>
</tr>
<tr>
<td>Employment</td>
<td>$62,314,015</td>
<td>Government Impersonation</td>
<td>12,827</td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>$61,111,319</td>
<td>Overpayment</td>
<td>10,988</td>
</tr>
</tbody>
</table>

FBI 2020 Internet Crime Report
Agari Cyber Intelligence Division (ACID) – Threat Intel Brief: The Geography of BEC

Types of Spoofing

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

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

• Domain Spoofing - “Company <person@company.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
Two Parts to DMARC

• DMARC Policy
  • sending organization
  • use existing DNS infrastructure

• DMARC Verification
  • receiving organization
  • enable on email security system
  • checks all incoming messages for DMARC policy
DMARC Myth ONE

It's used on email domain only

ANY domain can be impersonated and used in phishing attacks, so we need to do more than just securing only the domains used to send mail. Every domain owned by your organization should be secured with its own DMARC policy.

#GOTheDMARCWay
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 Policy

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
   - Sends Email

2. **Sender’s Inbox**
   - Sends Email

3. **Sending Organization’s DNS Server**
   - Sends Email

4. **DMARC**
   - Check sending org’s DMARC record upon receipt

5. **DMARC**
   - Rejected – failed DMARC policy, message is dropped and not delivered at all.

6. **Recipient’s Inbox**
   - Pass on Valid Email
   - Quarantine Policy

7. **Recipient’s Email Server**
   - Quarantine – failed DMARC policy, message is sent to Recipient’s SPAM/Junk folder.

8. **Send Reports Back**
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 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
Sample Forensic/Failure Report
Concerns with Implementation
DMARC Myth TWO

“It’s a Silver Bullet
DMARC is not the cure for every cyber risk. It protects only one type of spoofing and should never be used alone. You need a layered defense with securing email, and DMARC is an important layer. I recommend integrating it with DANE.”

DMARC Myth THREE

“It’s not good for privacy
With DMARC, you can view who is sending emails on your domain’s behalf, thus protecting privacy by preventing hackers from using your domain to send suspicious messages within your organization and to your customers. DMARC reporting sets it above other secure email practices.”
DMARC Myth

It’s easy
Starting the implementation of DMARC may be relatively simple, but the real work – and the most important part – comes with analyzing reports and adjusting your policy level for future.

DMARC Myth

It’s going to negatively impact my email
DMARC actually improves the delivery rate of the email you send to customers and others.
DMARC Myth

It’s only for large entities
Every organization with a public-facing domain

DMARC Myth

Antispam filters are enough
While antispam software and email security gateways can protect against inbound phishing attempts, DMARC protects emails originating from your domain from being spoofed and used for phishing attacks.

#GOTheDMARCWay
Concerns with Implementation

• 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
Items to Plan for

• Understanding SPF, DKIM, and DMARC
• Access to DNS
• Understand the three policy levels of DMARC
• Does email server support DKIM?
• List of public domains used by organization
  • If you have subdomains - Consider creating a DMARC policy for sub-domains
• Potential Unknowns:
  • Is your organization using 3rd party vendors?
    • Do they support SPF and/or DKIM?
  • Mail systems that IT staff is unaware of
• DMARC report analysis
  • email address to send reports
Additional Resources

• DMARC.org (http://www.dmarc.org) - Great source for DMARC information
• GCA DMARC - https://dmarc.globalcyberalliance.org
• Community Forum – https://community.globalcyberalliance.org
• GCA YouTube Channel
  • Webinars
  • Videos for GCA DMARC Setup Guide
  • DMARC Bootcamp
Q&A
Thank You!

Next Session:
May 12th – What are SPF and DKIM?

Shehzad Mirza
(gca-dmarc@globalcyberalliance.org)

Copyright @ 2020 Global Cyber Alliance