RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-F01

It's Not Dead Yet – *Email Security Matters*

J. Trent Adams

Director, Ecosystem Security

PayPal

@jtrentadams

DISCLAIMER: *The views expressed in this presentation are my own, and not necessarily those of PayPal Holdings, Inc. or any of its affiliates.*

#RSAC

It's Not Dead Yet – *Email Security Matters*

Topics Covered

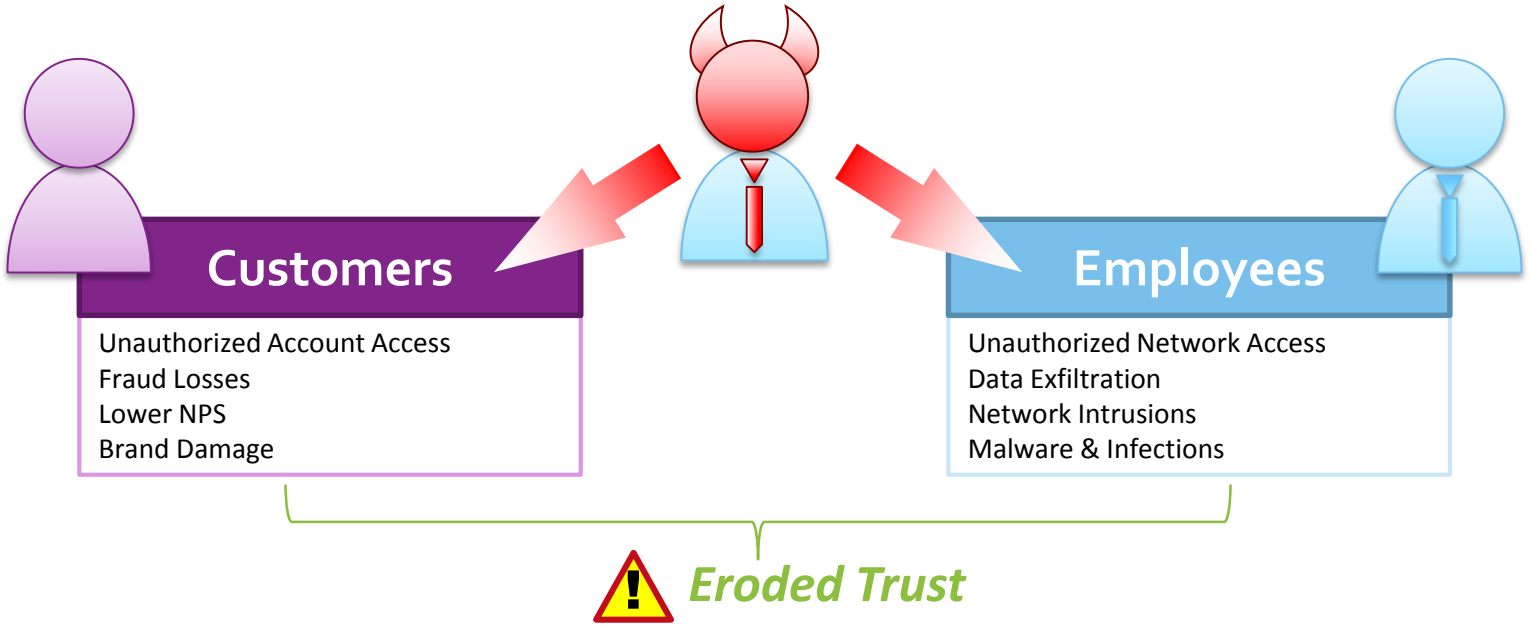
- **Overview**
  - Trust Matters
  - Attack Types
  - Table Stakes Checklist
- **Securing Your Own Email Flow**
  - Policies & Guidelines
  - Outbound Authentication
  - Inbound Verification & Defenses
- **Securing Email Flows of Your Vendors**
  - Sending On Your Behalf
  - Sending To Your Employees

Case Studies

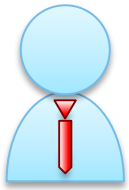
- **Operation PEST Control**
- **It's All About the Data**
- **3rd Parties Part 1:** *The Clueful*
- **3rd Parties Part 2:** *The Clueless*

Email Security – *Trust Matters*

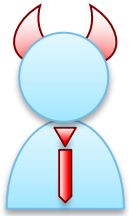
We rely on email being a ***trusted*** **channel of communication,**
and **malicious email** attacking **customers** & **employees** erodes trust.



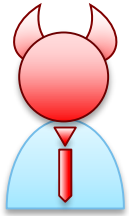
Email Security – *Attack Types*



Spoofed Domain Attacks – These are the most convincing to a recipient as the entire message is designed to mimic the legitimate sender. These messages purport to be from one of our domains, and are nearly indistinguishable to the victim from a legitimate message. The only differences are the IP address of the sending server and the existence of a malicious link, attachment, or illegitimate content. All other aspects of the email appear legitimate.



Cousin Domain Attacks – These attacks differ slightly in that they mimic everything of a legitimate message other than the sending domain. Rather than spoofing a legitimate domain, the malicious email is sent from a domain that either looks convincingly like a legitimate one (e.g. “pavpal.com”) or is otherwise obfuscated, often by confusing subdomains (e.g. “paypal.customer.service.com”).



Display Name Abuse – These attacks may come from any domain (whether a “cousin domain” or something different entirely), but the “display name” portion of the “From” field is modified to look as if it came from one of our brands or products. This may take the form of a legitimate email address (e.g. “service@paypal.com”) or a functional role (e.g. “PayPal Customer Service”).

Email Security – *Table Stakes*

- **Table Stakes Checklist**
  - ✓ Simplify & Standardize Mail Flows *(don't forget to monitor them)*
  - ✓ Throttling & Blackholing *(immediately drop what you can on the floor)*
  - ✓ Employ StartTLS *(with modern cypher suites)*
  - ✓ Authorize Sending Servers with SPF *(be careful with includes)*
  - ✓ Sign & Verify Email Using DKIM *(2048-bit keys; rotate frequently)*
  - ✓ Publish and Obey DMARC Policies *(be a "reject")*
  - ✓ Scan and Quarantine / Reject *(with extreme prejudice)*
  - ✓ Demand the Same from Vendors *(write security policies into contracts)*

It's Not Dead Yet—*Email Security Matters*

Case Studies

- **Operation PEST Control**
- It's All About the Data
- 3rd Parties Part 1: *The Clueful*
- 3rd Parties Part 2: *The Clueless*

Case Study 1: *Operation PEST Control*

- **Problem Statement:**
  - How to strategically address email security and what organizational structure would be the most effective?
- **Solution:**
  - ✓ Create a loosely coordinated operational task force made up of collaborators across the company focused on securing email.

Email Security – *Organizational Approach*

Email Security - *Coordination*

Principles, Standards, & Guidelines

Ensures coordination, consistency, future-proofing.

Tool Deployment, Operations, & Monitoring

Enables oversight & drives compliance with policies.

Data Aggregation, Analysis, & Alerting

Collecting & analyzing data to improve defenses & alert on threats.

Education, Training, & Communications

Phishing awareness & training is key to closing the loop.

External Standards Development & Evangelism

Ensures scalable interoperability & prevents vendor lock-in.

Incident Analysis & Response

Actual & suspected attacks must be investigated and handled.

Email Security – *Operation PEST Control*

Intelligence

Visibility into the problem & measuring the effectiveness of solutions.

Prevention

Minimizing the virulence of known attacks as early as possible.

Reaction

Quick and effective action when an attack is detected.

Innovation

Addressing emerging attacks and future-proofing defenses.

Case Study 1: *Operation PEST Control*

- **Results:**
  - ✓ An incredibly talented and effective cross-functional team.
  - ✓ Visibility across the company (by and of the team).
  - ✓ Dynamic, agile-type development / deployment / reactions.
- **Challenges:**
  - ✧ Maintaining continuity through organizational changes.
  - ✧ Budget questions when solutions cross departments.

It's Not Dead Yet – *Email Security Matters*

Case Studies

- Operation PEST Control
- **It's All About the Data**
- 3rd Parties Part 1: *The Clueful*
- 3rd Parties Part 2: *The Clueless*

Case Study 2: *Data, Data Everywhere*

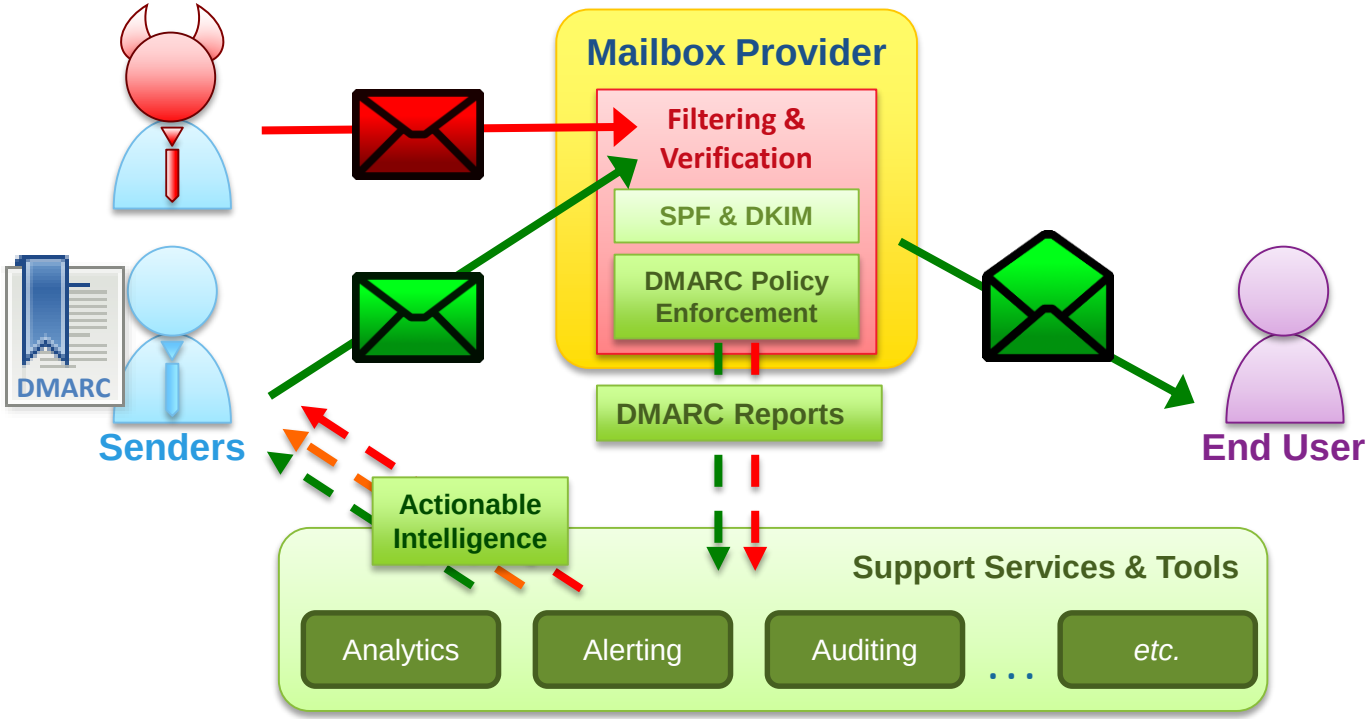
- **Problem Statement:**
  - To secure our email, we need to define “malicious email” and then quantify, measure, analyze, and report on the volume, virulence, and risk posed by various types. How can we do this in a holistic manner?
- **Solution:**
  - ✓ Tap into all available touch points and data flows. Analyze the data for useful information and build dashboards, alerts, and automated responses.

Email Security – *Define "Malicious Email"*

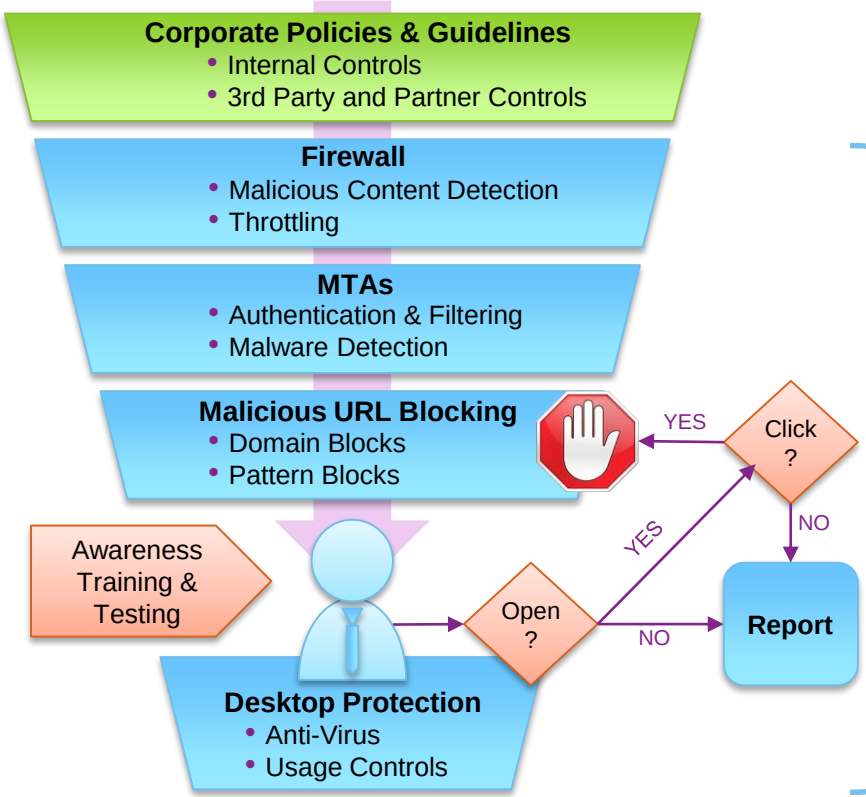
- **Malicious Email Includes:**
  - **Phishing** – Tricking receivers into revealing sensitive information.
  - **Malware Delivery** – Installing malware on the receiver's computer.
  - **False Pretenses** – Tricking receivers into taking unauthorized actions.

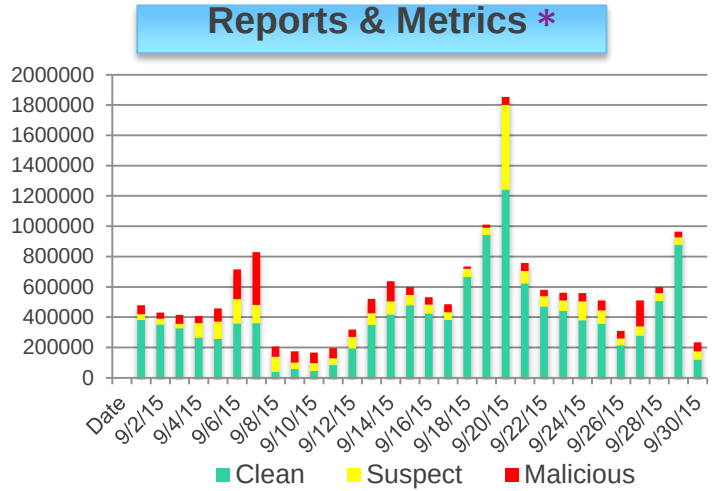
- **Malicious Email Abuses all Email Flows:**
  - **Transactional** (e.g. system-generated receipts, password reset confirmations, etc.)
  - **Communication** (e.g. account notices, product updates, etc.)
  - **Marketing** (e.g. new product offerings, promotions, etc.)
  - **Conversational** (i.e. person-to-person messages sent to/from people internally and externally)
  - **3rd Parties** (i.e. email sent by a 3rd party, including email sent to customers or employees)

Email Security – *Authentication is Key*



Email Security – *Data, Data, Everywhere*





**Simulated Data & Chart*

Case Study 2: *Data, Data Everywhere*

- **Results:**
  - ✓ Analyzed existing logs and data sources.
  - ✓ Added and refined logging to fill gaps and improve utility.
  - ✓ Gained visibility into hitherto unknown problems.
  - ✓ Significantly improved dashboards and metrics for tracking effectiveness.
- **Challenges:**
  - ✧ Normalizing data from various sources into meaningful information requires careful consideration.
  - ✧ Operationalizing research analytics processes can be difficult.

It's Not Dead Yet – *Email Security Matters*

Case Studies

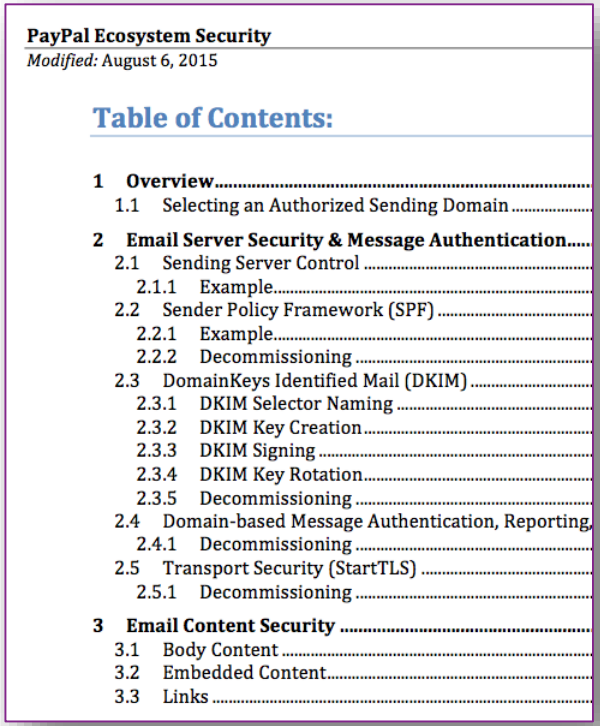
- Operation PEST Control
- It's All About the Data
- **3rd Parties Part 1: *The Clueful***
- 3rd Parties Part 2: *The Clueless*

Case Study 3: *Clueful 3rd Parties*

- **Problem Statement:**
  - Given that email must be sent by 3rd parties, both on behalf of the company and to employees, how can we ensure their email flows are secure?
- **Solution:**
  - ✓ Develop a comprehensive "3rd Party Email Security Guidelines" that act as a cookbook for implementing email security according to our requirements.

Email Security – *3rd Party Guidelines*

- **Example DKIM Guidance:**
  1. DKIM keys must be 2048-bit
  2. Signing canonicalization must be set to "relaxed/relaxed"
  3. The "d=" domain set to the domain in the Addr-Spec portion of the RFC5322.From field.
  4. The "s=" selector set to the selector name we provide.
  5. The following headers must be signed:
     - From
     - Subject
     - Date
     - To
     - MIME-Version
     - Content-Type



PayPal Ecosystem Security

Modified: August 6, 2015

Table of Contents:

Case Study 3: *Clueful 3rd Parties*

- **Results:**
  - ✓ Vastly improved our process of on-boarding new vendors.
  - ✓ Simplified and standardized vendor deployments.
  - ✓ Clarified the security expectations for project management staff.
- **Challenges:**
  - ✧ There are always challenges in deployment; the requirements can be met in various ways and creative, unique solutions are often required.
  - ✧ Some (often the large, well-known) vendors have hard-coded products that take months (and in some cases years) to become compliant.

It's Not Dead Yet – *Email Security Matters*

Case Studies

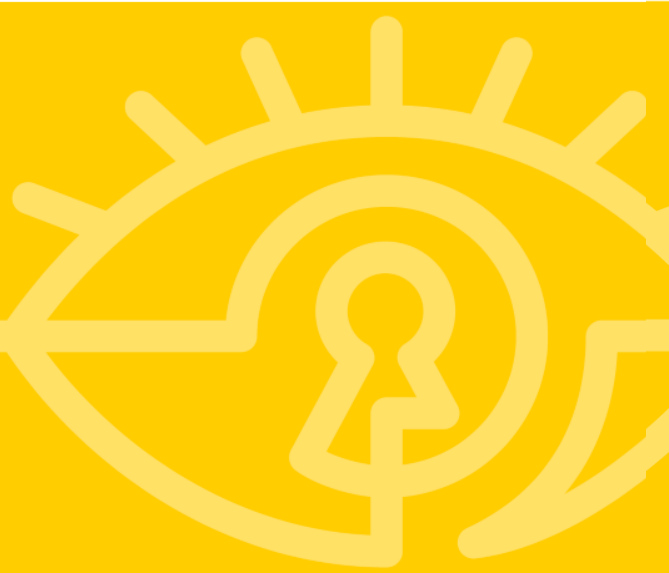
- Operation PEST Control
- It's All About the Data
- 3rd Parties Part 1: *The Clueful*
- **3rd Parties Part 2: *The Clueless***

Case Study 3: *Clueless 3rd Parties*

- **Problem Statement:**
  - Given that email must be sent by 3rd parties, both on behalf of the company and to employees, how can we ensure their email flows are secure*… when the vendor has no idea how to secure their email flow?*
- **Solution:**
  - ✓ Send them a copy of the "3rd Party Email Security Guidelines".
  - ✓ Provide a subject matter expert to educate and guide them.
  - ✓ Replace the vendor if they cannot comply.

Case Study 3: *Clueless 3rd Parties*

- **Results:**
  - ✓ Clarified the process of a vendor becoming compliant.
  - ✓ Helped vendors modernize and improve their email security for all customers.
  - ✓ Ensured that we only use compliant vendors.
- **Challenges:**
  - ✧ Vendors with non-compliant solutions prior to the guidelines being enforced had to be retroactively brought into compliance.
  - ✧ Projects started without fully understanding the ramifications of non-compliance were stalled (or canceled).
  - ✧ Requires executive leadership willing to support drawing a hard line (which, fortunately, we have).



Email Security – *Takeaways*

Email Security – *Takeaways*

1. If you haven't already done so, immediately deploy DMARC to begin receiving reports.
2. Catalog all email flows (think hard about this, as some may not be obvious) and log meaningful data from them.
3. Document policies, standards, and guidelines covering internal and 3rd party email.
4. Create a tiger team representing all stakeholders identified by the catalog, and empower them to improve your email security posture.
5. Unleash the tiger team to "move the needle" of the metrics indicated by the data that has been gathered.
6. Ensure that vendors are held accountable to being compliant with your requirements.

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: TECH-F01

Thanks!

(Questions?)

PS: *Yes, I was in **Star Wars: The Force Awakens**. If you have no questions about this presentation, I'll happily talk your ear off about that experience.*

J. Trent Adams

Director, Ecosystem Security
PayPal
@jtrentadams

#RSAC