Phishing E-mails
Topics

- Understand E-mail Security Incidents
- Explain different types of E-mail attacks and their impacts
- Discuss the preparation required to handle E-mail incidents
- Identify email attack indicator
- Detect phishing and spam mails
- Contain email attacks
- Device methods of eradicating email incidents
- Explain steps to follow to recover after email incidents
Overview of Email Security Incidents

- Introduction to Email Security Incidents
- Types of Email Incidents
Spamming

- Spam refers to undesired emails used to distribute malicious links and attachments, cause network congestion, perform phishing and financial frauds and so on.

- The spam may also consume bandwidth of the email servers causing DoS conditions.

- In the example the email address doesn't match the sender name or the content of message
Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

- The information is then used to access important accounts and can result in identity theft and financial loss.
Examples of phishing

- Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit cards) by masquerading as a trusted entity.
SPEAR-PHISHING

- Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons.

- This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online.
SPEAR-PHISHING VS. PHISHING

**PHISHING**
Is a broad, automated attack that is less sophisticated.

**SPEAR-PHISHING**
Is a customized attack on a specific employee & company.
Preparation for Handling Email Security Incidents
Preparation

- Email Filtering
- Email monitoring tools
- Communication
- Training and awareness to employees
- Acceptable usage policy
- Local archive or backups
- Email logs analysis tools
Detection and Containment of Email Security Incidents

- Indicators of Email attack
- Detecting Phishing/Spam emails
- Containing Email incidents
- Analyzing Email Headers
Indications of Email Attacks

- Unavailability of the email server.
- Inability to access the system or the email accounts after opening an email.
- System showing signs of malware attack after opening a link or attachment from an email such as finding suspicious process running on your system.
- Sudden increase of advertising and spam emails.
- Change to the theme or interface of the email web page.
Detecting Phishing/Spam Emails

- Unexpected attachment from user, client, vendor, or peers.
- Attachments with unusual or unrecognized formats.
- Difference in the email ID of the sender and display name.
- Email format IDs that don't have incomplete or incorrect organization name or use numbers in the place of letters in the name.
- Having generic greetings such as dear customers.
Detecting Phishing/Spam Emails

- Emails with links, which display a different website or URL when hovered on or have URL with incorrect name or domain.

- Emails presenting offers that are too attractive to believe, such as winning the lottery, a competition, a free subscription, vacation, and job offers.

- Emails that seem to be from user's bank, financial institution, organization, service provider, and other associate, which ask to reveal sensitive information or login to their accounts using provided links or install updates.
Tools for Detecting Phishing/Spam mails

- **PhishTank**
  - Phishtank is a collaborative clearing house for data and information about phishing on the internet.
  - It provides an open API for developers and researchers to integrate antiphishing data into their application.
  - It helps in detecting phishing and spam emails easier as API is available for all developers.
Containing Email Incidents

- Isolate the targeted system from the functional network immediately after receiving the incident report.

- Interview the users or compliment about the email incident to find details of the attack and user actions.

- Ask if the user had downloaded the attachment, clicked the link, provided the requested information, and so on.
Containing Email Incidents

- If the email consist of links, find further details of the link by opening it in a sandbox environment to perform behavior analysis.

- Report and block the malicious links in the server, network devices, and across all security solutions.

- In case of malicious attachment sent through email, incident responders must open the email account in sandbox environment, download the attachment and perform behavior analysis of the system and check if it has malicious code.
Containing Email Incidents

- Perform malware incident handling process if the email contain malicious programs.

- In case of spam or phishing emails, issue a notification to all the employees to find if others have been facing the same issue.

- Report the spam and phishing mail to service providers.
What is an Email Header

- The email header is a code snippet in an HTML email, that contains information about the sender, recipient, email’s route to get to the inbox and various authentication details.

- The email header always precedes the email body.
Email header Analysis Example
What purpose do email headers serve

- Providing information about the sender and recipient
- Preventing spam
- Identifying the email route
Example of Email Header

Return-Path: <BraylonHuff@metrowg.pronaceouses.com>
Received: from metrowg.pronaceouses.com (metrowg.pronaceouses.com [138.128.6.57])
by mail.identityvector.com (8.13.8/8.13.8) with ESMTP id sA4GciOh009308
for <recip@identityvector.com>; Tue, 4 Nov 2014 11:38:45 -0500
Message-ID: <92861425.aLg7bOBpFjmWCE2014110408308444444@mx1.metrowg.pronaceouses.com>
Date: Tue, 04 Nov 2014 08:38:44 -0800
From: Lazy Weight Loss <Braylon@pronaceouses.com>
To: <recip@identityvector.com>
Subject: Too Self-Conscious about your body?
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
MIME-Version: 1.0
X-Spam-Checker-Version: SpamAssassin 3.3.1 (2010-03-16) on quaaff.identityvector.com
X-Spam-Level: :
X-Spam-Status: No, score=1.8 required=5.0 tests=BAYES_00,HTML_MESSAGE,
MIME_HTML_ONLY,RP_MATCHES_RCVD,SPF_HELO_PASS,SPF_PASS autolearn=no
version=3.3.1
X-Virus-Scanned: clamav-milter 0.98.4 at mail.identityvector.com
X-Virus-Status: Clean
X-Greylist: Sender passed SPF test, not delayed by milter-greylist-4.4.3
(mail.identityvector.com [205.186.148.46]);
Tue, 04 Nov 2014 11:38:46 -0500 (EST)

This is some content that is supposed to look legit...
Completely Legit.
Click the link, because you do what you're supposed to do.
Just like a good little human does.
Obey your email master.
http://hfdklashgfjkdlishgfdlsjhgklksd.cz.cc/pwnme/please

Header/body separator
The appearance of the email header differs between ESPs. To analyze it, you need to find the email header and examine the lines of interest to you. All the code from the beginning, until the `<body>` tag, represents the header.

**Analyzing an Email Header**
Analyzing an Email Header

- return path
- Recipient's email address
- Name of the email server
- Type of email sending server
- IP address of sending server
- Unique message number
- Date and time of email was sent
- Attachment file information
- Sender Policy Framework (SPF)
- Domain Key Identified Mail (DKIM)
Example of Email Header Analysis

Consider an example: Rudy sends an Email to Timmy

From: rudy@bieberdorf.edu (Rudy)
To: timmy@immense-isp.com
Date: Tue, Dec 11 2018 14:36:14 PST
X-Mailer: Loris v2.32
Subject: Lunch today?

Received: from mail.bieberdorf.edu (mail.bieberdorf.edu [124.211.3.78]) by mailhost.immense-isp.com (8.8.5/8.7.2) with ESMTP id LAAs8699; Tue, Dec 11 2018 14:39:24 -0800 (PST)

Received: from alpha.bieberdorf.edu (alpha.bieberdorf.edu [124.211.3.11]) by mail.bieberdorf.edu (8.8.5) id 004A21; Tue, Dec 11 2018 14:36:17 -0800 (PST)
From: rudy@bieberdorf.edu (R.T. Hood)
To: timmy@immense-isp.com
Date: Tue, Dec 11 2018 14:36:14 PST
Message-Id: <rth031897143614-000000298@mail.bieberdorf.edu>
X-Mailer: Loris v2.32
Subject: Lunch today?
Sender Policy Framework (SPF)

- SPF is an email validation protocol used to by domain owners for preventing spoofing of email.
- Incident responders can analyze the authenticity of the sender using the SPF results.
- The SPF will display results mentioned in the following:
  1. **None**: no SPF records are found for this domain
  2. **Pass**: SPF records exist and IP address is authorized it include plus (+) sign in front of the IP
  3. **Fail**: IP address is not authorized to send email for this domain. This shown by a –all command in the record
Steps to Analyze Email in Gmail

- Open an email you want to analyze.
- Click "more" option (three vertical dots) from the top right of the message.
- From the drop down menu click "show original" option.
- The mail will open a new tab display the original message.
Steps to Analyze Email in Yahoo Mail

- Open the mail you want to analyze.
- Click the "more" option (three horizontal dots) from the top of the message.
- From the drop-down menu, click "view raw message" option to see the complete message source.
Tools to Analyze Email headers

- MxToolbox

This tool will make email headers human readable.
Email Header Analysis using mxtoolbox
Email Header Analysis using mxtoolbox
Exercising The originating IP Address

- Open the email to trace and find its header.
- Collect IP Address of the sender from the header of the received mail.
- Search for IP in the WHOIS database.
- Look for the geographic address of the sender in the WHOIS database.
Example using WHOIS database
Eradication of Email Security Incidents

- Eradicating Email attacks
- Report Phishing and Spam Emails to Email Service Provider
- Guidelines Against Spam
- Guidelines Against Phishing
Eradicating Email Attacks

- Collect details of an email security incident such as URL, subject, links, sender, and IP address, from email header analysis and block them across servers, security tools, and network devices. We can seek help from ISPs to help us performing these actions.

- Immediately alert employees about the incident and train them to diagnose it, inform Network administrators to guide employees who to deal with the current situation.

- Update antiphishing and antispam tools with the newly found signature and details of the attack to prevent similar attacks in the future.

- Find common pattern and signatures from the email to block them on the SMTP server.
Eradicating Email Attacks

- Check the SMTP logs to find if the same email is sent to other employees and remove them from the inboxes.

- Check if other users have been impacted with the attack and perform incident handling process on their system as well.

- Use DNS blocking to block IP addresses used to send the malicious emails.

- Harden the security of the email server and clients.
Train the employees to check email headers from the email asking for immediate action such as financial transactions.

Blacklist the malicious websites and disable automatic download across all the systems and devices.

Ensure removal of malware related data from affected systems such as text files, process executed by the malware.

Block and remove the impacted accounts and re-issue new accounts to the employees.
Eradicating Email Attacks

- Request all employees to change password, ensure it's complicated password and implement multiple authentication for their accounts.

- Install browser extensions and tools that help in detecting and preventing phishing and spam emails.

- Blacklist the email using signature, sender's address, or other details of malicious email.

- Inform the organizations, bank, or entities whose email being spoofed by the attackers.
Reporting Phishing and Spam Emails to Email Service Providers

Gmail
- Report spam
- Report phishing

Outlook.com
- Junk
- Phishing scam

Yahoo Mail
- Report Spam
- Report a Hacked Account
- Report a Phishing Scam
- Not My Mail
Guidelines Against Spam

- Avoid giving email ID to unnecessary or unsecured websites.

- Before giving email ID to a website check its privacy policy and website certificate.

- Block spamming email IDs and regularly update recipient's address book.
Guidelines Against Spam

- Block potential offensive images in email to prevent attack using luring technique.

- Never give your email ID in clickable form on the web to prevent spam bots from stealing your email ID.

- Maintain a personal email ID which is shared only with friends and family members and never use that email ID for any other purpose.

- Use long email ID with numbers and underscore to prevent spammers.
Guidelines Against Spam

- Never use unsubscribe links in email messages.
- Do not use or subscribe to sites that access email contact list.
- Do not choose numbers that reflect personal identification information such as social security number, street address, and telephone number.
- Avoid buying products from web links in email to discourage them as well as to avoid bogus and fraud related issues.
Guidelines Against Phishing

- Do not transfer sensitive data such as credentials, personal and financial information through emails.

- Do not enter personal details in suspicious links sent in email form and pop-up screen.

- Protect the computer with a security software such as antivirus, antisyware, antimalware, firewalls etc.

- Beware of the too good to be true or over attractive schemes and offers.
Guidelines Against Phishing

- Never open the email marked as spam even if the subject line seems to be interesting, and delete such email immediately.

- Avoid accessing the links from the instant messengers.

- Maintain different passwords for different accounts and change them frequently.

- Check the domain name/URL and security indicators before logging in to bank accounts.
Recovery After Email Security Incidents

- Recovery Steps to Follow after Email Incidents
- Recover of Deleted Emails
- Email Security Checklist
Recovery Steps to Follow After Email Incidents

- Change password of the email accounts related to it.
- Inform banks and financial institutions about the attack and block the compromised accounts.
- Restore the compromised systems using backups.
- Contact law enforcements.
- Claim insurance if there huge financial loss
Recovery of Deleted Emails

- Gmail:

1. Log in to Gmail

1. In the left pan, scroll down and find the trash folder

2. Click the trash folder and you can view the list of all deleted emails in the right pane of the window
Recovery of Deleted Emails

- **Outlook**:

1. Login to MS outlook
2. The folder will contain recently deleted items
3. In the home tab click recover deleted items from server
4. Click on the email you want recover and select restore selected items button
5. Then click OK button
6. Now, navigate back to the deleted item folder; you can find the recovered emails
Email Security Checklists

- Enable HTTPS for secure connection/transactions.
- Be delightful while opening email attachments.
- Do not click the links provided in the email message.
- Follow email etiquette while forwarding messages.
- Do not forward or replay to spam and suspicious emails; delete them.
Email Security Checklists

- Avoid accessing emails via unsecured public wireless.
- Avoid accessing email accounts on shared computers and sending large attachments in emails.
- Never save your password on web browser.
- Sort message by priority, subject date, sender, and other options.
Email Security Checklists

- Avoid sending confidential, sensitive, personal, and classified information in emails.
- Clean your inbox regularly.
- Create folders and move emails accordingly.
- Digital sign your outgoing emails.
- Send attachment in PDF format rather than word or excel.
Email Security Checklists

- Scan email attachments for malware.
- Use security certified email service provider.
- Maintain separate email for personal and public communications.
- Disable keep me signed in/stay signed in functions.
- Turn off the preview feature.
Thank You