Malware Analysis Episode 2: Phishing Email Analysis [PART 1]

Whiteboard

Description automatically generated with medium confidence

**Disclaimer: Please use the below information only for learning, if the below information is used for any unethical activity, I am not accountable for that.**

**Reference:** [Email Header Analysis Tutorial](https://www.youtube.com/watch?v=3wwaYc_Yuhc), [Incident Response Training-Phishing Incident](https://www.youtube.com/watch?v=DGwUGqnEbag), [SOC-Detect Phishing Emails](https://www.youtube.com/watch?v=Xrzsu-FFvu8), [Detect Phishing Emails Playlist](https://www.youtube.com/playlist?list=PLGEXXg4RVghB2EkpjG4EtmsjrTyrqtHJU),

**Tools to analyse email**: [Whois](https://whois.domaintools.com/), [SPF record Check](https://www.spf-record.com/spf-lookup), [mxtoolbox](https://mxtoolbox.com/EmailHeaders.aspx), [Message Header Analyzer](https://mha.azurewebsites.net/), [dnschecker](https://dnschecker.org/email-header-analyzer.php), [OutlookAttackView](http://www.nirsoft.net/utils/outlook_attachment.html), [Msg-extractor,](https://github.com/TeamMsgExtractor/msg-extractor) [Eml-extractor](https://github.com/diogo-alves/eml-extractor), [UUDWIN](https://www.marks-lab.com/), [Intezer Analyze](https://analyze.intezer.com/) - Scan and analyze URLs automatically with Intezer

**Resources:**

<https://www.intezer.com/blog/incident-response/automate-analysis-phishing-email-files/>

<https://www.intezer.com/blog/malware-analysis/url-analysis-phishing-part-1/>

<https://www.intezer.com/blog/research/elephant-malware-targeting-ukrainian-orgs/>

<https://www.intezer.com/blog/product-updates/automatically-scan-urls-and-analyze-malware/>

**PHISHING ANALYSIS**

**Starting** with example – How exactly Spam emails look like-

Graphical user interface, text

Description automatically generated Graphical user interface, application

Description automatically generated

**Email:** sending and receiving of information through internet is known as an E-mail. Sharing an email is done using email address.

**Basic Flow of an Email:** (image attached below)

Diagram

Description automatically generated with low confidence

**Parts of an Email:**

* Email address is a unique address for the delivery of messages.
* Email Body contains the actual content of the message.
* Email Header Analysis:

1. **Basic parts of email header**

* The “From:” section displays the sender’s name and email address.
* The “Created at:” provides with Date-Time of delivery.
* The “To:” represent the receiver’s email details, containing CC and BCC.
* The “Subject:” gives the topic of the mail’s content.

Graphical user interface, text, application, email

Description automatically generated

1. **Return-Path:** display the email address of return-path, which display the return address. This field indicates if the email is bounced how it will be taken care of , this address is different from sender’s address and is specifically for collecting and processing bounced emails.
2. **DKIM Signatures:** This filed shows what different kinds of authentication is required to identify an email whether the email sent is the authenticated version or it has been tempered/ modified.
3. **Message ID:** a unique combination of numbers and letters, used to identify each mail, no emails have the same Message ID. It is generated by first MTA, also referred to as MSA (Mail Submission Agent).
4. **MIME-Version:** This internet standard changes non-text content such as images, videos attachment into text, so they can be sent through mail. Provides conversion for media into text format to be attached in an email as email can consist of only text format.
5. **Received**: Lists the servers that an email traverses through before arriving at the receiver. The top is the last server that goes through, and the bottom is originating email.
6. **X-Spam Status:** this informs about the SPAM SCORE. If the score crosses a certain point the mail is termed as “Spam”.

**Risk of an Email Attack:**

* Spam is nothing but unwanted mail or junk mail.
* User of email spam is done mostly for scamming purposes through marketing mails.
* To obtain target information or send virus programs are also done through email spam.

**How to Analyse Emails:** (Gmail Emails)

* STEP 1: Access any email, to see header.
* STEP 2: Click on “More” 
* STEP 3: Select “Show Original” option to open header details.

Graphical user interface, application, Word

Description automatically generated

* STEP 4: Email header details are now open in a new window.

Graphical user interface, text, application, email

Description automatically generated

**Importance of Email Header Analysis:**

* **Protection against Spam** and **phishing** attacks due to several fields that help identify the legitimacy of the email.
* Identification of sender and receiver information, using **From** and **To** fields along with **Subject** field and date.
* Helps in **tracking the email’s route** from the sender to receiver.

Graphical user interface

Description automatically generated

**Phishing Attack Flow:**

Diagram, schematic

Description automatically generated

**How Email files are used by Threat Actors:** The goal is to make the email look legitimate to increase the chances of the victim to-

* Open link provided in the email: Enter credentials or sensitive information.
* Open malicious attached files

**How to inspect Email files:** Email Structure

Diagram

Description automatically generated

Email file header: To, From, Received, DKIM Signature, SPF

Email Spoofing Methods:

* Spam Folder:

1. Content-flag words, large image with short texts
2. Sender IP and domain reputation

* Suspicious sender:

1. Email received from outside the org.
2. Suspicious sender- The @<something> part and public domain, Domain name is misspelt, you did not expect to receive the emails.

* Spoofed address: email spoofed address = forged sender (example attached below)

Graphical user interface

Description automatically generated with medium confidence Graphical user interface, website

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

* Remember to inspect embedded Links, URLS, files or any attachments.
* Extract and Inspect attachments: common attachments are -Microsoft Office Files, PDFs, ZIP and Archive, ISO and IMG disk image.

**Important Note: (Informative for upcoming Demo Episode on Phishing Analysis)**

* To check Spoof -> click on -> original message -> check Message ID [If there is difference between Message ID value and “From” Field value, then indication is of spoofing]
* SPF Alignment – The SPF Alignment is PASS only when “Return-Path” And “From” domain is same. Different between which helps us understand email could be spoofed.
* SPF Authentication – If SPF authentication is FAIL, it means the sender IP address is not authorized to send email on behalf of the legit domain.
* DKIM Alignment- compare the DKIM Signature field [d=domain.com] with “From” , if it does not match then the result marks DKIM Alignment as FAIL.
* DKIM Authentication- If DKIM Signature field [b=……..] is not verified so we can say that the email has been modified or tempered.

Please let me know if this has helped you in any way. You can also add your views on lab safety through comments. I will be back next time with demo on phishing email analysis in Malware Analysis Episodes.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>

<https://www.instagram.com/cybersecurity.cyber_seek/>

<https://twitter.com/Shefali37920461>

**About SCL and BCL score. Soft faild , hard fail,**

**Demo of Email Analysis**

paste the email header in three tools to check headers

copy header from clipboard and paste in mx tool for header analyssi.

Graphical user interface, text, application, email

Description automatically generated

**Email Header Analysis: SPF, DKIM, DMARC**

**Email Body Analysis: sender, subject, email body, embedded URL/Attachments**

**Remediation/Mitigation:**

**Awareness:**

Please let me know if this has helped you in any way. You can also add your views on lab safety through comments. I will be back next time with some more sharp insights on Malware Analysis Episodes.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>

<https://www.instagram.com/cybersecurity.cyber_seek/>

<https://twitter.com/Shefali37920461>