Malware Analysis Episode 3: Demo of Email Analysis [PART 2]



**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, [Network Tools](https://www.broadbandsearch.net/network-tools)

**Resources:**

[Email analysis | Infosec Resources (infosecinstitute.com)](https://resources.infosecinstitute.com/topic/email-analysis/)

[What is Email Analytics: 15 Metrics & KPIs to Track Performance (mailmodo.com)](https://www.mailmodo.com/guides/email-analytics/)

[Email Header Analysis. Best Email Forensics Software (stellarinfo.com)](https://www.stellarinfo.com/article/email-header-structure-forensic-analysis.php)

[5 Simple Tips for Phishing Email Analysis | Fortinet](https://www.fortinet.com/resources/cyberglossary/phishing-email-analysis)

**PHISHING ANALYSIS: Demo of Email Analysis [Sample 1 – Gmail sample]**

**STEP 1:** Go through how the email body looks, if there are URLs and Attachments you will need to test them in sandbox environment [Virtual Machine]

Graphical user interface

Description automatically generated with medium confidence

**Sandbox Environment – (static & dynamic analysis)**

To test the links/attachments in sandbox environment make use of Virus Total for URL reputation check/ file hash check, Urlscan.io, palo alto url filtering, whois domaintools, haveibeenpwned, Inspect element of webpage -> check network activity, google dorks, Browserling, can run E-discovery check for user click actions on the links/attachments. You can also use other OSINT tools for analysing the links/attachments within sandbox environment.

**STEP 2:** To analyse the email header and email body begin with downloading the email in .eml format.

Graphical user interface, application

Description automatically generated

**STEP 3:** You will be greeted with Original Message page. If you select “Download Original” you will be able to download email in .eml format for header analysis or if you prefer using “Copy to Clipboard” to directly copy the header and paste in any email header analyzer tool for header analysis.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**STEP 4:** Email Header Analysis: SPF, DKIM, DMARC, SCL & BCL score

Header analysis is done on [MxtoolBox](https://mxtoolbox.com/EmailHeaders.aspx) for sample 1

A picture containing graphical user interface

Description automatically generated

We see that SPF Alignment, SPF Authenticated, DKIM Alignment, and DKIM Authenticated all are PASS. (Please refer the notes below)

**Important Note: (Informative on Email 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.

**What is SPF, DKIM, DMARC?**

Sender Policy Framework (SPF) is a way for a domain to list all the servers they send emails from. Think of it like a publicly available employee directory that helps someone to confirm if an employee works for an organization.

SPF record typically looks like v=spf1 ip4:123.123.123.123 ~all

SPF distinguishes between **“soft” and “hard” fails**. Writing ~all in your header indicates a soft fail when an unauthorized sender is encountered; -all instructs the receiving server to use a hard fail.

The email will be discarded entirely in a hard fail scenario. Soft fails may permit the email to be delivered to the recipient’s junk folder. Now DMARC is widely available, which we’ll see below, it’s generally recommended to use ~all (soft fail). This avoids false positives with legitimate emails, hands more control to DMARC, and can aid debugging in later verification stages.

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses cryptography to mathematically verify that the email came from the domain.

Domain-based Message Authentication Reporting and Conformance (DMARC) tells a receiving email server what to do given the results after checking SPF and DKIM. A domain's DMARC policy can be set in a variety of ways — it can instruct mail servers to quarantine emails that fail SPF or DKIM (or both), to reject such emails, or to deliver them.

DMARC DNS Record v=DMARC1; p=none; rua=mailto:user@example.com

**Reference:** [What are DMARC, DKIM, and SPF? | Cloudflare](https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/)

[DKIM, DMARC, and SPF: Setting Up Email Security (howtogeek.com)](https://www.howtogeek.com/devops/dkim-dmarc-and-spf-setting-up-email-security/)

[What are DMARC, SPF and DKIM? How to master email security with these protocols | CSO Online](https://www.csoonline.com/article/3254234/mastering-email-security-with-dmarc-spf-and-dkim.html)

Unlike SPF and DKIM, DMARC gives domain owners a way to specify what happens when an email server receives a message without proper authentication. There are three supported actions:

* none – The server can continue to deliver the message.
* quarantine – Deliver the message to junk or spam.
* reject – Reject and bounce the message.

DMARC also provides a reporting mechanism. You can specify a server endpoint that receiving mail servers will call when they get an email purporting to be from your domain. This gives you a cross-internet view of the servers that are sending as your domain.

**Another important part to know about SCL and BCL score?**

 Use mail flow rules to set the spam confidence level (SCL) in messages. Similar to the SCL, the**bulk complaint level** (BCL) identifies bad bulk email (also known as Gray mail). A higher BCL indicates a bulk mail message is more likely to generate complaints (and is therefore more likely to be spam).

Graphical user interface, text, application, email

Description automatically generated

**Reference:**

[Spam confidence level - Office 365 | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-spam-confidence-level-scl-about?view=o365-worldwide)

[Email Protection Basics in Microsoft 365: Bulk Email - Microsoft Community Hub](https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/email-protection-basics-in-microsoft-365-bulk-email/ba-p/3445337)

[Bulk Complaint Level (BCL) & Spam Confidence Level (SCL) overview. - Microsoft Q&A](https://learn.microsoft.com/en-us/answers/questions/443679/bulk-complaint-level-(bcl)-spam-confidence-level-(?orderBy=Helpful)

[What is SCL and BCL? – Blackestfest.com](https://blackestfest.com/what-is-scl-and-bcl/)

[BCL Score reputation - Microsoft Community Hub](https://techcommunity.microsoft.com/t5/microsoft-365/bcl-score-reputation/m-p/86721)

Graphical user interface, text, application

Description automatically generated

Application

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

**Breaking Down an Email-**

Let us first go through some of the important headers to understand what they represent. It is ideal to read message headers from bottom to top to be able to properly understand where the email is originated from.

* **X-priority:**X-priority is an optional parameter in the email spec used to specify the priority of the email. Values can be 1 (Highest), 2 (High), 3 (Normal), 4 (Low) or 5 (Lowest). Three is default if the field is omitted. Most email programs don’t fill it in unless it is set low or high. Client side programs will highlight the inbound message (!) if it is 1 or 2.
* **Content-Type:** This header specifies the type of content in the email. The preceding email is of plain text.
* **Reply-To:** This header specifies whom to send the reply when the receiver replies to the email received.
* **Message-Id:** Message Id is a unique identifier that can be used to identify the message.
* **From:**This header is used to display the username or email from which email is sent. Note that spoofed emails typically modify this header to appear to have come from a known source.
* **Received:**This header represents the recipient details. There can be multiple entries of this header as the email traverses through multiple servers.
* **Received-SPF:** This header represents the Sender Policy Framework (SPF) results, which tells whether the sender is a permitted sender or not.
* **Delivered-To:**This header represents the destination email id that the email is delivered to.

In addition to the headers discussed so far, we can see three additional headers as shown below.

* ARC-Seal
* ARC-Message-Signature
* ARC-Authentication-Results

ARC-XXXX headers help preserve email authentication results and verify the identity of email intermediaries that forward a message on to its final destination.

* **ARC Authentication Results**: This header contains email authentication results like SPF, DKIM, and DMARC
* **ARC-Message-Signature:** This is a DKIM-like signature and takes a snapshot of the message header information. This includes to, from, subject and body
* **ARC-Seal**: This header contains a signature which includes the ARC-Message-Signature and the ARC Authentication Results header information.

**STEP 5:** Email Body Analysis: sender, subject, email body, embedded URL/Attachments

Check the subject of the email to understand what it is about. Check the sender domain in Virus Total, Whois DomainTools, Urlscan.io, Browserling, and Palo Alto Url Filtering. You can test your personal email ID in Have I been Pwned to check if your id is breached or safe. Don’t enter professional/ Corporate email ID here - Have I been Pwned (as it is a public repo). Use of Inspect element -> Network is also important to check the redirected URL activity and real intent of the Base/original URL.

Fields to check are Subject, Sender, Sender Domain, Recipient, Recipient Domain, Network Message ID, Latest email delivery, Original email delivery.

Later check the tone of the email body/email content. If any link (URL) or Attachment is embedded in the email, extract the URL/Attachment not by clicking it (don’t interact with it) Instead by coping it [Right click -> Copy Hyperlink / Copy] and paste to test the URL/File in Windows sandbox / Sandbox Environment or test the Attachment within the sandbox environment (example – windows sandbox)

**PHISHING ANALYSIS: Demo of Email Analysis [Sample 2 – Email sample]**

**STEP 1:** Go through how the email body looks, if there are URLs and Attachments you will need to test them in sandbox environment [Virtual Machine]

Graphical user interface, text, application, Teams

Description automatically generated

Graphical user interface, application

Description automatically generated

**Sandbox Environment – (static & dynamic analysis)**

To test the links/attachments in sandbox environment make use of Virus Total for URL reputation check/ file hash check, Urlscan.io, palo alto url filtering, whois domaintools, haveibeenpwned, Inspect element of webpage -> check network activity, google dorks, Browserling, can run E-discovery check for user click actions on the links/attachments. You can also use other OSINT tools for analysing the links/attachments within sandbox environment.

**STEP 2:** To analyse the email header and email body begin with downloading the email in .eml format

Graphical user interface, application

Description automatically generated

**STEP 3:** You will be greeted with Original Message page. If you select “Download Original” you will be able to download email in .eml format for header analysis or if you prefer using “Copy to Clipboard” to directly copy the header and paste in any email header analyzer tool for header analysis.

Graphical user interface, text, application, email

Description automatically generated

**STEP 4:** Email Header Analysis: SPF, DKIM, DMARC, SCL & BCL score

Header analysis is done on [Message Header Analyzer](https://mha.azurewebsites.net/pages/mha.html) for sample 2

**Reference:** [Email Header Analysis. Best Email Forensics Software (stellarinfo.com)](https://www.stellarinfo.com/article/email-header-structure-forensic-analysis.php)

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Application, Word

Description automatically generated

Graphical user interface, application, Word

Description automatically generated

**STEP 5:** Email Body Analysis: sender, subject, email body, embedded URL/Attachments

Check the subject of the email to understand what it is about. Check the sender domain in Virus Total, Whois DomainTools, Urlscan.io , and Palo Alto Url Filtering. You can test your personal email ID in Have I been Pwned to check if your id is breached or safe. Don’t enter professional/ Corporate email ID here. Use of Inspect element -> Network is also important to check the redirected URLs.

Fields to check are Subject, Sender, Sender Domain, Recipient, Recipient Domain, Network Message ID.

Later check the tone of the email body/email content. If any link (URL) or Attachment is embedded in the email, extract the URL/Attachment not by clicking it (interacting with it) Instead by coping it [Right click -> Copy Hyperlink] and paste the URL in sandbox browser or test the Attachment within the sandbox environment (example – windows sandbox)

**REMEDIATION/MITIGATION- (Personal / Corporate)**

**STEP 6:** Remediation/Mitigation – If the users have either received phishing or spam email

* Enable [multi-factor authentication (MFA)](https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication) systems in place for accounts that can contain personal (PII)/ confidential/ Highly-Confidential/ Sensitive information.
* Perform email purge (email deletion) from the mailbox.
* Report the email as abuse of Phishing/Spam to your email service provider.
* Educate the mail service provider (eg- gmail) or tool used within corporate environment by reporting it as either phishing or spam based on your findings.
* If needed, you can also perform URL block for Malicious/suspicious URL/Domain.
* Or Submit Request to decommission of base URL/ Redirected URL to your mail service provider.
* Now look for number of users who might have clicked on the URL/attachment of the email, if identified any reset credential for that/those user(s)
* You can also perform actions from the below image.

Graphical user interface, text, application

Description automatically generated

**USER AWARENESS**

**STEP 7:** USER Awareness / Phishing Simulation emails

Create awareness banners, brochures for the users to keep them educated on How to spot Phishing email & protect themselves.

For Corporate environment, Scheduled events on Phishing Simulation Activity within the environment helps the organization evaluate employees’ understanding about Phishing attacks.

Please let me know if this has helped you in any way. You can also add your views about the episode 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/>