



ELECTIVE-III

DIGITAL FORENSICS AND INCIDENT

RESPONSES

MINI-PROJECT REPORT

Project Title: Email Analysis

By

Navya Peram	PES1UG21CS924
Namita Patil	PES1UG21CS357
Navaneetha N	PES1UG21CS365

Contents

Abstract	-----3
Problem Description	-----3
Implementation	-----3
Results	-----4
Conclusion	-----8
Appendix	-----

○ Abstract:

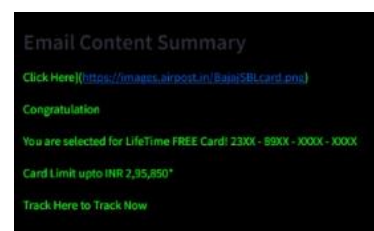
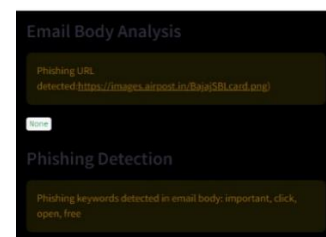
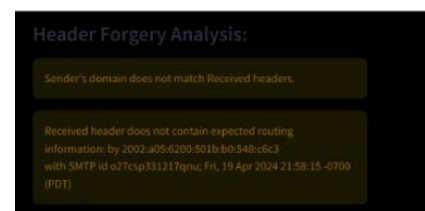
Our project focuses on developing an advanced email analysis tool to enhance email security. The tool offers features such as header analysis for detecting phishing attempts, content analysis for identifying suspicious content, and attachment analysis for detecting potentially malicious files. It also integrates sender reputation analysis and threat intelligence feeds to provide real-time updates on emerging threats. With a user-friendly interface, our tool aims to empower users to make informed decisions and mitigate the risks associated with email-based threats.

○ Problem Description:

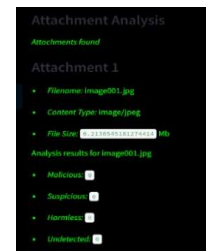
Email communication is a cornerstone of modern communication, yet it is increasingly targeted by malicious actors through techniques like phishing and malware distribution. Existing email security measures often fall short in detecting sophisticated threats, leaving users vulnerable to data breaches and financial losses. Moreover, users may lack the tools and knowledge to assess the legitimacy of incoming emails effectively. Thus, there is a pressing need for an advanced email analysis tool that can comprehensively evaluate email headers, content, and attachments to identify potential threats and provide users with real-time updates on emerging cybersecurity risks. By empowering users to make informed decisions and mitigate email-based threats, such a tool can significantly enhance overall email security posture and protect against cyber-attacks.

○ Implementation:

1. Header Analysis: Extraction and analysis of email headers to identify suspicious patterns, inconsistencies, and potential indicators of phishing or spoofing attempts.
2. Content Analysis: Examination of the email body for phishing keywords, suspicious URLs, and other indicators of malicious intent. Utilization of machine learning-based summarization techniques to provide users with concise summaries of email content.



3. Attachment Analysis: Detection and analysis of email attachments to identify potentially malicious files using advanced threat intelligence feeds.



4. Sender Reputation Analysis: Evaluation of sender reputation by querying external threat intelligence sources and analyzing sender IP addresses extracted from email headers.



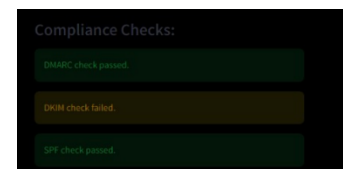
5. Threat Intelligence Integration: Integration with external threat intelligence feeds to provide users with real-time updates on emerging threats and trends in the cybersecurity landscape.



6. User-Friendly Interface: Implementation of an intuitive and user-friendly interface for seamless navigation and interaction with the email analysis tool.



7. Compliance Checks: Implement checks for compliance with email security standards such as DMARC, DKIM, and SPF to verify email authenticity and reduce the likelihood of spoofed emails.

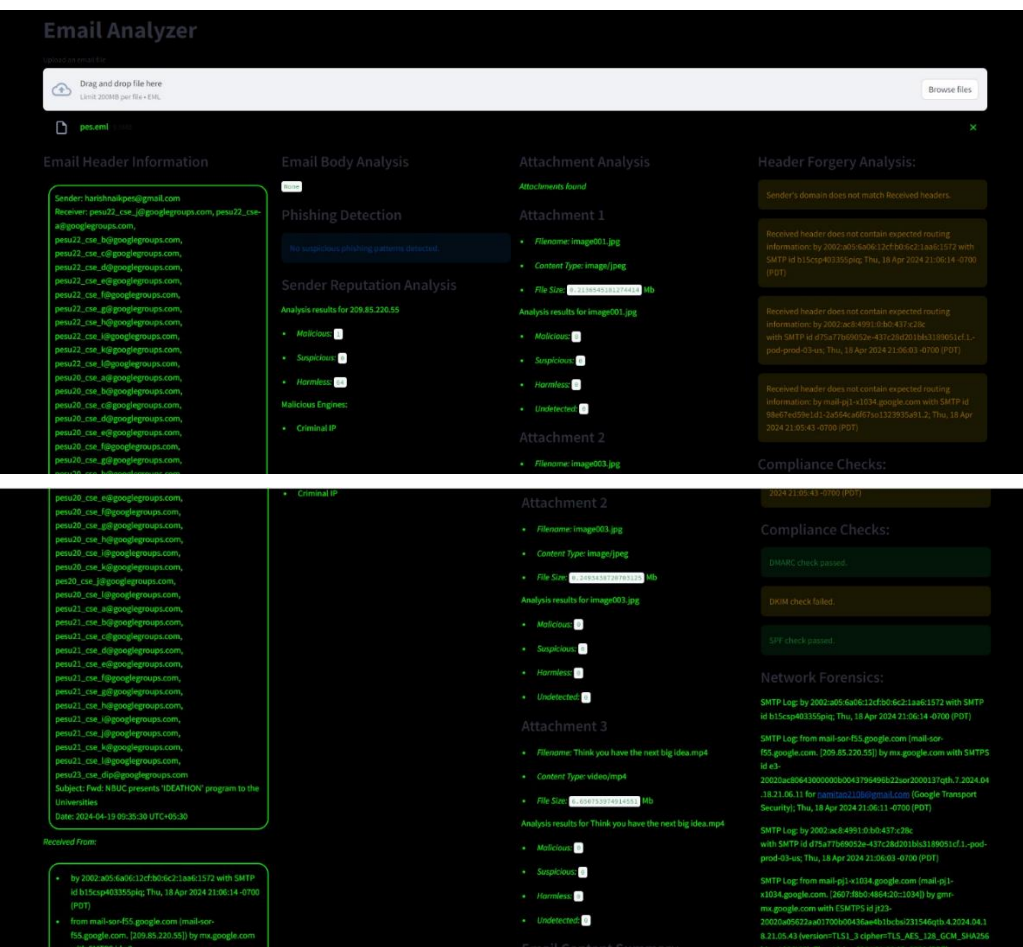


8. Network Forensics:
 - Analyze network traffic associated with the email transmission, including SMTP (Simple Mail Transfer Protocol) logs, email server logs, and firewall logs.
 - Look for suspicious patterns or anomalies in the network traffic that may indicate malicious activities, such as unusual email attachment sizes, multiple failed delivery attempts, or connections to known command-and-control servers.



- **Results:**

1. No suspicious content



Received From:

- by 2002a056a06130f3b06c21aw61572 with SMTP id b15csp493895ng; Thu, 18 Apr 2024 21:06:14 -0700 (PDT)
- from mail-ser-fkx.google.com [mail-ser-fkx.google.com, [209.85.220.105]] by mx.google.com with SMTPS id c8-20020ac806430000000043796496b22car2000137qph.1.2024.04.18.21.06.11 for <medhini4202@gmail.com> (Google Transport Security); Thu, 18 Apr 2024 21:06:11 -0700 (PDT)
- by 2002a056a06130f3b06c21aw61572 with SMTP id d75a77069052a-437c3b4201b3a1189651c11-pod-prod-43-us; Thu, 18 Apr 2024 21:06:08 -0700 (PDT)
- from mail-gj1-x1034.google.com [mail-gj1-x1034.google.com, [2007.880.4864.20:1034]] by gmv-mx.google.com with SMTPS id j03-20020ac806430000000043796496b22car2000137qph.1.2024.04.18.21.06.08 for <medhini4202@gmail.com> (version=TLS1_3, cipher=TLS_AES_128_GCM_SHA256, bits=128/128); Thu, 18 Apr 2024 21:06:02 -0700 (PDT)
- by mail-gj1-x1034.google.com with SMTP id 986e7ed5b1d1-2a564ca0f7a132935a91.2; Thu, 18 Apr 2024 21:05:43 -0700 (PDT)

Multiple "Received" headers detected, potential email forwarding.

• Malicious
• Suspicious
• Harmless
• Undetected

Email Content Summary

- Nokia is organizing an Ideathon (online only) in the domain of 5G/4G use cases. To view this discussion on the web visit <https://groups.google.com/it/mgpd-5g-wireless-ecocsa-ideathon>
- SMTP Log: from mail-gj1-x1034.google.com [mail-gj1-x1034.google.com, [2007.880.4864.20:1034]] by gmv-mx.google.com with SMTPS id j03-20020ac806430000000043796496b22car2000137qph.1.2024.04.18.21.05.43 (version=TLS1_3, cipher=TLS_AES_128_GCM_SHA256, bits=128/128); Thu, 18 Apr 2024 21:05:02 -0700 (PDT)
- SMTP Log: by mail-gj1-x1034.google.com with SMTP id d75a77069052a-437c3b4201b3a1189651c11-pod-prod-43-us; Thu, 18 Apr 2024 21:06:08 -0700 (PDT)

Threatpost Articles

Watering Hole Attacks Push Scanbox Developer

Ransomware Attacks are on the Rise

Being Prepared for Adversarial Attacks - Podcast

Protecting Phones From Pegasus-Like Spyware Attacks

Breaking Down Joe Roberts' 5108 Cybersecurity "Down Payment"

Cyber-Spies: Ops Suffer 305 Attacks per Week, an All-Time High

Being Prepared for Adversarial Attacks - Podcast

How Email Attacks are Evolving in 2023

Patrick Wardle on Hackers Leveraging "Powerful" iOS Bugs in High-Level Attacks

2. Detected phishing content


4/26/24, 8:53 PM Gmail - Your SBI_Credit_Card application has been approved | medhini4202@gmail.com

Medhini P <medhini4202@gmail.com>

🌟 Your SBI_Credit_Card application has been approved || (medhini4202@gmail.com).

Ready to Dispatch <notifications@tripshrip.com> 20 April 2024 at 10:28
Reply-To: notifications@tripshrip.com
To: medhini4202@gmail.com

Having trouble viewing this image? [Please Click Here](#)



Congratulation

You are selected for LifeTime FREE Card!

Card No.: 23XX - 89XX - XXXX - XXXX

Card Limit upto INR 2,95,850*

<https://mail.google.com/mail/u/0/?ui=2&ik=cf&ik=pf&ik=ecocsa-ideathon&ik=mg-17566203688650322&ik=mg-17566203688650322> 1/2

4/26/24, 8:53 PM Gmail - Your SBI_Credit_Card application has been approved | medhini4202@gmail.com

Track Here to Track Now

If you wish to opt out of all type of emails, click [Unsubscribe](#).

You can update your preferences on the type of emails you want to receive from us [Making Preferences](#).

[Report Abuse](#)

<https://mail.google.com/mail/u/0/?ui=2&ik=cf&ik=pf&ik=ecocsa-ideathon&ik=mg-17566203688650322&ik=mg-17566203688650322> 2/2

Drag and drop file here
Limit 20MB per file • PNG

🌟 Your SBI_Credit_Card application has been approved | medhini4202@gmail.com

Email Header Information

Sender: notifications@tripshrip.com
Receiver: medhini4202@gmail.com
Subject: 🌟 Your SBI_Credit_Card application has been approved | (medhini4202@gmail.com).
Date: 2024-04-20 04:58:14 UTC

Email Body Analysis

Phishing URL detected: <https://images.airmobi.in/StaticSBIcard.png>

Phishing Detection

Phishing keywords detected in email body: important, click, open, free

Sender Reputation Analysis

Analysis results for 103.197.36.240

• Malicious
• Suspicious
• Harmless

Attachment Analysis

No attachments found.

Email Content Summary

Click Here(<https://images.airmobi.in/StaticSBIcard.png>)

Congratulation

You are selected for LifeTime FREE Card! 23XX - 89XX - XXXX - XXXX

Card Limit upto INR 2,95,850*

Track Here to Track Now

Header Forgery Analysis:

Sender's domain does not match Received headers.

Received header does not contain expected routing information: by 2002a056a06130f3b06c21aw61572 with SMTP id c27csp31217qnu; Fri, 19 Apr 2024 21:58:15 -0700 (PDT)

Compliance Checks:

DMARC check passed.

DKIM check failed.

SPF check passed.

Network Forensics:

SMTP Log: by 2002a056a06130f3b06c21aw61572 with SMTP id c27csp31217qnu; Fri, 19 Apr 2024 21:58:15 -0700 (PDT)

SMTP Log: from mail1.tripshrip.com [mail1.tripshrip.com, [103.197.36.240]] by mx.google.com with SMTPS id c8-20020ac806430000000043796496b22car2000137qph.1.2024.04.19.21.58.15 for medhini4202@gmail.com (version=TLS1_3, cipher=ECDSA-CHACHA20-POLY1305, bits=256/256); Fri, 19 Apr 2024 21:58:15 -0700 (PDT)

Threatpost Articles

Watering Hole Attacks Push Scanbox Developer

Ransomware Attacks are on the Rise

Being Prepared for Adversarial Attacks - Podcast

Protecting Phones From Pegasus-Like Spyware Attacks

Breaking Down Joe Roberts' 5108 Cybersecurity "Down Payment"

Cyber-Spies: Ops Suffer 305 Attacks per Week, an All-Time High

Being Prepared for Adversarial Attacks - Podcast

How Email Attacks are Evolving in 2023

Patrick Wardle on Hackers Leveraging "Powerful" iOS Bugs in High-Level Attacks

2020 Cybersecurity Trends to Watch



Email Analyzer

Upload an email file

Drag and drop file here
Limit: 20MB per file - EML

Browse files

[URGENT] Registrations for UNSAT close today .eml

Email Header Information

Sender: blprtya29@gmail.com
Receiver: purplekysnp16@gmail.com
Subject: Fwd: [URGENT] Registrations for UNSAT close today
Date: 2024-04-26 19:36:45 UTC+05:30

Received From:

- by 2002:a02:cb55:0:b0:484:587c:fb5 with SMTP id v5csp378585app; Fri, 26 Apr 2024 07:07:03 -0700 (PDT)
- from mail-sor-f41.google.com [mail-sor-f41.google.com, 209.85.220.41] by mx.google.com with SMTPS id c14-20020a170906694e00b0a587f4ed092sor2642437eqs.2.20240426.07.07.02 for <purplekysnp16@gmail.com> [Google Transport Security]; Fri, 26 Apr 2024 07:07:02 -0700 (PDT)

Subject line contains the word 'urgent'. Potential spam.

Email Body Analysis

Phishing URL detected: <http://delivery.unacademy.com/02MJC0UN7...>

Attachment Analysis

No attachments found.

Email Content Summary

Forwarded message — From: Unacademy
to: purplekysnp16@gmail.com Date: Thu, 2 Jun 2022, 8:16 pm Subject: [URGENT] Registrations for UNSAT close today To: blprtya29@gmail.com

[Image: Unacademy National Scholarship Admission Test. If you haven't enrolled yet, today's your last chance to do so!]

Threatpost Articles

- Warning: Hike Attacks Push ScanBox Keylogger
- Ransomware Attacks are on the Rise
- Being Prepared for Adversarial Attacks - Podcast
- Protecting Phones from Pegasus Like Spyware Attacks
- Breaking Down Joe Biden's 510B Cybersecurity 'Down Payment'
- Cyber Spies: Ops Suffer 925 Attacks per Week - an All-Time High

Header Forgery Analysis:

Sender's domain does not match Received headers.

Received header does not contain expected routing information by 2002:a02:cb55:0:b0:484:587c:fb5 with SMTP id v5csp378585app; Fri, 26 Apr 2024 07:07:03 -0700 (PDT)

Compliance Checks:

- DMARC: check passed.
- DKIM: check failed.
- SPF: check passed.

Network Forensics:

SMTP Log by 2002:a02:cb55:0:b0:484:587c with SMTP id v5csp378585app; Fri, 26 Apr 2024 07:07:03 -0700 (PDT)

Phishing Detection

Phishing keywords detected in email body: urgent, important, download, win

Sender Reputation Analysis

Analysis results for 209.85.220.41

- Malicious: 0
- Suspicious: 0
- Harmless: 0

Suspicious Engines:

- Criminal IP
- URL Query

○ Conclusion:

The experiment conducted with our email analysis tool yielded promising results, showcasing its efficacy in enhancing email security and mitigating the risks associated with email-based threats. By analyzing email headers, content, and attachments, the tool successfully identified phishing attempts, malicious content, and suspicious sender behavior. Additionally, integration with real-time threat intelligence feeds provided users with timely updates on emerging cybersecurity risks, enabling proactive defense against potential threats. Overall, the experiment underscores the value of our email analysis tool in empowering users to make informed decisions and bolstering email security posture.

Recommendations for Future Use/Development/Behavior:

Looking ahead, it is imperative to continue refining and advancing the capabilities of the email analysis tool to address evolving email security challenges effectively. This entails further optimization of threat detection algorithms, expansion of threat intelligence integration, and enhancement of user interface and usability aspects. We can enable continuous monitoring and analysis of email traffic for detecting and responding to security threats or anomalies in real-time. To achieve this, enhancing authentication mechanisms such as IMAP (Internet Message Access Protocol) or OAuth (Open Authorization) authentication could be crucial. IMAP authentication could be improved to provide better integration with real-time monitoring systems, allowing for seamless access to email data streams for analysis purposes. Similarly, leveraging OAuth authentication, which provides secure, token-based access to email accounts, could enhance the security and reliability of real-time monitoring systems by ensuring proper authorization and access control.

Moreover, ongoing user education and training initiatives are essential to ensure widespread adoption and effective utilization of the tool across various user demographics. By prioritizing continuous improvement and user engagement, our email analysis tool can serve as a crucial asset in safeguarding against email-based threats and promoting a secure email communication environment.

○ Appendix:

Sample Email Files: Gmail

External Libraries and APIs: VirusTotal, Streamlit, BeautifulSoup, Bert, Email, Summarizer, Requests, Html

Contribution:

1. Namita Patil – Email header information, Attachment analysis, Sender reputation analysis
2. Navya Peram – Email body analysis, Phishing detection, Email content summary, Threatpost articles
3. Navaneetha N- Header forgery analysis, Compliance checks, Network forensics

References: <https://docs.streamlit.io/>, <https://docs.python.org/3/library/email.html>, <https://www.crummy.com/software/BeautifulSoup/bs4/doc/>, <https://docs.python-requests.org/en/latest/>, <https://docs.python.org/3/library/html.html>, <https://developers.virustotal.com/v3.0/reference>.