

SOC282 - Phishing Alert - Deceptive Mail Detected

Hey, Today I will write about investigation of “SOC282 - Phishing Alert - Deceptive Mail Detected”

Before we begin lets understand some keywords.

Phishing: It is a type of cyberattack where someone tricks you into giving away sensitive information like passwords, OTPs, bank details, or personal data by pretending to be a trusted person or organization.

Playbook: They are crucial for a Security Operations Center for several reasons. A couple of those reasons are Consistency and Standardization. Playbooks ensure that incident responses are handled consistently across the team. By standardizing procedures, SOC analysts can respond to threats in a uniform manner, reducing the chances of errors or missed steps.

VirusTotal: It is a free tool used by analyst for scanning URLs, IP addresses, and domains for malicious content

Now let's start investigating

This is the alert that appears in our investigation channel.

| MAIN CHANNEL | | INVESTIGATION CHANNEL | | CLOSED ALERTS | | |
|---|-------------------------|---|-------------------------|------------------|---|--------|
| SEVERITY | DATE | RULE NAME | | EVENTID | TYPE | ACTION |
| Medium | May, 13, 2024, 09:22 AM | ★ SOC282 - Phishing Alert - Deceptive Mail Detected | | 257 | Exchange | » ✓ |
| ★ This alert is prepared for the 'How to Investigate a SIEM Alert' course. If you haven't taken the course yet, please complete it first. | | | | | | |
| EventID : | 257 | Event Time : | May, 13, 2024, 09:22 AM | Rule : | SOC282 - Phishing Alert - Deceptive Mail Detected | |
| Level : | Security Analyst | SMTP Address : | 103.80.134.63 | Source Address : | free@coffeeshoop.com | |
| Destination Address : | Felix@letsdefend.io | E-mail Subject : | Free Coffee Voucher | Device Action : | Allowed | |
| Show Hint ⚡ | | | | | | |

Let's start with the playbook

Incident Details

| | |
|----------------|---|
| Incident Name: | EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected] |
| Description: | EventID: 257 |
| Incident Type: | Exchange |
| Created Date: | Nov, 24, 2025, 07:21 AM |

Start Playbook!

Click on >> Start Playbook button

The first step of the playbook is asking us to obtain the information about the alert

Parse Email

Before starting the analysis, information about the incoming email should be obtained.

- When was it sent?
- What is the email's SMTP address?
- What is the sender address?
- What is the recipient address?
- Is the mail content suspicious?
- Are there any attachment?

Next

- When was it sent?

May, 13, 2024, 09:22 AM

- What is the email's SMTP address?

103.80.134.63

- What is the sender address?

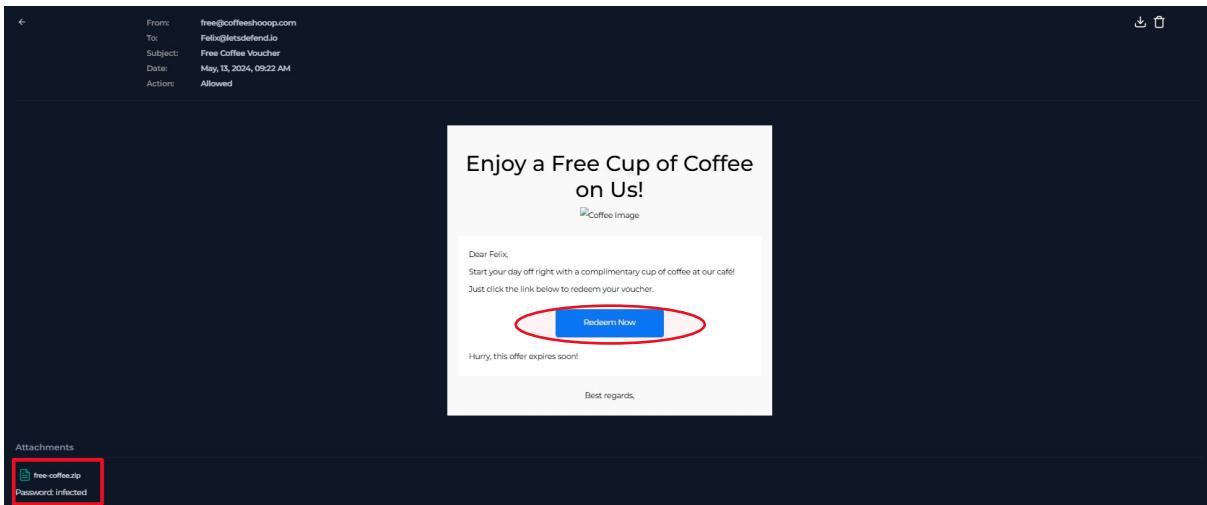
free@coffeeshoop.com

- What is the recipient address?

Felix@letsdefend.io

- Is the mail content suspicious?

Yes, the mail contains suspicious content. The attacker is trying to trick the user by sending free vouchers!



- Are there any attachment?

Yes, there is an attachment with file name **free-coffee.zip**

The playbook's next phase is to look for attachments

Monitoring Log Management Case Management Endpoint Security Email Security Threat Intel Sandbox

Incident Details

Are there attachments or URLs in the email?

Please click "Yes" if there are an attachments or URLs in the email, if there are no attachments or URLs in the email please click "No".

Contains Attachment or Url?

No Yes

Click on >> Yes, because we found both attachment and URL in the email

Monitoring Log Management Case Management Endpoint Security Email Security Threat Intel Sandbox

Analyze Url/Attachment

Analyze Url/Attachment in 3rd party sandboxes. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

You can use the free products/services below.

- AnyRun
- VirusTotal
- URLHouse
- URLScan
- HybridAnalysis

Malicious Non-malicious

Let us analyze the attached URL on VirusTotal

The screenshot shows the VirusTotal analysis interface. At the top, a summary card displays a 'Community Score' of 9 / 98, with 9/98 security vendors flagged as malicious. Below this, the main analysis card shows the URL <https://download.cyberlearn.academy/download/download?url=https://files-1d.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip>. The status is 200, content type is text/html; charset=utf-8, and it was last analyzed 1 day ago. The detection tab is selected, showing a table of vendor detections:

| Security vendor | Detection | Do you want to automate checks? |
|------------------|-----------|---------------------------------|
| alphaMountain.ai | Malicious | BitDefender |
| CyRadar | Malicious | Forcepoint ThreatSeeker |
| Fortinet | Malicious | G-Data |
| Lionic | Malicious | Sophos |

The URL is flagged as malicious!

The screenshot shows the Hybrid Analysis report for the file. The analysis overview section includes details like submission name (59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip), size (30KB), type (data compressed zip), mime (application/zip), and SHA256 (6f33ae4bf134c49faa14517a275c039ca1818b24fc2304649869e399ab2fb389). It also shows the threat score (100/100), AV detection (8%), and labels (Trojan.Generic #uricario). The anti-virus results section shows a single scan from MetaDefender with a result of 'Malicious' (2/23).

Click on >> Malicious

The screenshot shows the LetsDefend platform's incident details page. The sidebar includes links for Monitoring, Log Management, Case Management (selected), Endpoint Security, Email Security, Threat Intel, and Sandbox. The main content area is titled 'Incident Details' and contains a modal window asking 'Check If Mail Delivered to User?'. The modal provides instructions to determine if an e-mail is delivered by looking at the 'device action' part of the alert details. Two buttons are available: 'Delivered' and 'Not Delivered'. The footer of the page includes links for Resources, Community, Roles, Support, and a 'Download Mobile App' button.

Let us go to Email Security page and find this out

| Date | Sender | Recipients | Subject | Final Action |
|------------------------|----------------------|---------------------|---------------------|--------------|
| May 13, 2024, 09:22 AM | free@coffeeshoop.com | Felix@letsdefend.io | Free Coffee Voucher | Allowed |

As we can see the final action is displayed as **Allowed** that means the message was delivered to the user.

Click on >> Delivered

Incident Details

EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]

Delete Email From Recipient!

You should delete the malicious email from user's mailbox.
Please click "DELETE" button to delete malicious email.

Delete

For this go to Email Security Page and delete the mail

From: free@coffeeshoop.com
To: Felix@letsdefend.io
Subject: Free Coffee Voucher
Date: May, 13, 2024, 09:22 AM
Action: Allowed

Enjoy a Free Cup of Coffee on Us!

Coffee Image

Dear Felix,
Start your day off right with a complimentary cup of coffee at our café!

Click on >> Delete

The screenshot shows the LetsDefend dashboard with a sidebar containing links like Monitoring, Log Management, Case Management (highlighted), Endpoint Security, Email Security, Threat Intel, and Sandbox. A central modal window is open with the title "Check If Someone Opened the Malicious File/URL?". The modal text says: "Please go to the \"Log Management\" page and check if the c2 address accessed. You can check if the malicious file is run by searching the c2 addresses of the malicious file." Below this, it says: "Please click \"Opened\" if someone access the malicious address. Otherwise please click \"Not Opened\" button." At the bottom are two buttons: "Not Opened" and "Opened".

To find this we need to go to Endpoint Security Page, as we know the users email address we can find out his name

Destination Address :

Felix@letsdefend.io

So the name of the user is **Felix**.

Search the same of the EDR page

The screenshot shows the LetsDefend Endpoint Security page. The left sidebar has a link to "Endpoint Security" (highlighted). The main area has a search bar with "Felix" typed in. Below the search bar is a list item "Felix 172.16.20.151". To the right is a large grid of icons representing different endpoint activities like file operations, network connections, and system monitoring. A callout box at the bottom right of the grid says "Select an endpoint from the list."

Click on >> Felix

The screenshot shows the LetsDefend Endpoint Security page for user "Felix". The search bar shows "felix". The main pane displays detailed host information for "Felix" (IP 172.16.20.151) including Hostname, Domain, IP Address, Bit Level, OS, Client/Server, and Last Login. Below this is a timeline of events. One event is highlighted with a red box: "2024-05-13 12:59 files-id.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip". Other event details include "Event Time" (2024-05-13 12:57) and "Domain Name/URL" (login.live.com/).

As we can see that the user has opened the malicious URL

Click on >> Opened

The screenshot shows the LetsDefend platform's interface. On the left, there's a sidebar with various navigation options like Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The 'Case Management' option is currently selected. The main area displays 'Incident Details' for an incident named 'EventID: 257 - [SOC282 - Phishing Alert - Deceptive Mail Detected]'. A central modal window is open, titled 'Containment', with the instruction: 'Please go to the "EDR" page and contain the user machine! After containment please click "Next" button to finish playbook.' A blue 'Next' button is visible at the bottom of the modal. At the bottom of the page, there's a footer with links to Resources (Blog, MITRE ATT&CK Map, Dictionary, Use Cases), Community (Discord, Contribute, Forum), Roles (SOC Analyst, Incident Responder, Detection Engineer, DFIR), Support (Contact us, Help Center, Forum, Walkthroughs), and a 'Download Mobile App' section with QR codes for App Store and Google Play.

We need to make sure that this infected machine does not infect other systems connected to the same network. So, Isolate the infected machine

This screenshot shows the LetsDefend platform's host information for a machine named 'Felix'. The host information panel shows details like Hostname: Felix, Domain: LetsDefend, IP Address: 172.16.20.151, Bit Level: 64, OS: Windows 10, Primary User: Felix, Client/Server: Client, and Last Login: May 13, 2024, 12:04 PM. To the right, there's an 'Action' section with a 'Containment' toggle switch that is currently off. A modal window is overlaid, asking 'Do you want to change the containment situation?' with 'Close' and 'Change' buttons. The 'Change' button is highlighted with a red box. Below the host information, there are tabs for Processes (86), Network Action (23), Terminal History (8), and Browser History (12). The results section shows 10 items. The browser history tab is active, displaying two entries: '2024-05-13 12:57 login.live.com/' and '2024-05-13 12:59 files-id.s3.us-east-2.amazonaws.com/59cbd215-76ea-434d-93ca-4d6aec3bac98-free-coffee.zip'. The page number is set to 2.

Click on >> Change

This screenshot shows the same host information for 'Felix' as the previous one, but the 'Containment' toggle switch is now turned on, and the status is 'Host Contained'. The rest of the interface is identical to the previous screenshot, including the tabs for Processes, Network Action, Terminal History, and Browser History, and the results section showing 10 items.

The Host is now contained

Click on >> Next

The screenshot shows the LetsDefend interface. On the left, there's a sidebar with various navigation options: Monitoring, Log Management, Case Management (which is selected), Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area is titled 'Incident Details' and contains fields for 'Incident Name', 'Description', 'Incident Type', and 'Created Date'. A modal window titled 'Add Artifacts' is open, listing two artifacts: 'free@coffeeshoop.com' (Comment: Phising mail, Type: E-mail Sent) and 'files-ld.s3.us-east-2' (Comment: This is a Malicious UF, Type: URL Address). A 'Next' button is at the bottom of the modal.

Add Artifacts

Click on >> Next

The screenshot shows the LetsDefend interface. The sidebar and incident details fields are the same as the previous step. A modal window titled 'Analyst Note' is open, with the instruction 'Please enter your analysis comments.' Below it is a text area containing the note: 'This is a Phishing email. The attacker with email address "free@coffeeshoop.com" tried to sent malicious content to the victim and was successful. The email is deleted from the Host machine and the machine is contained'. A progress bar indicates 219 / 3000 characters used. A 'Next' button is at the bottom of the modal.

Click On >> Next

The screenshot shows the LetsDefend interface. The sidebar and incident details fields are the same. A modal window titled 'Finish Playbook!' is open, with the instruction 'Please click confirm button to finish playbook. Your answers will be saved and case will be closed. Your artifacts should list in case after clicking finish button.' A 'Confirm' button is at the bottom of the modal.

Click on >> Confirm

The screenshot shows a table titled "CLOSED ALERTS" with columns: SEVERITY, DATE, RULE NAME, EVENTID, TYPE, and ACTION. The first row, highlighted with a red border, corresponds to the alert described in the text. The "ACTION" column for this row contains a button labeled "Close Alert" with a red box drawn around it.

| SEVERITY | DATE | RULE NAME | EVENTID | TYPE | ACTION |
|----------|-------------------------|--|---------|------------|--|
| Medium | May, 13, 2024, 09:22 AM | SOC224 - Phishing Alert - Deceptive Mail Detected | 257 | Exchange | >> <input checked="" type="checkbox"/> |
| Medium | Mar, 13, 2021, 08:20 PM | SOC13B - Detected Suspicious Xls File | 77 | Malware | >> <input type="checkbox"/> |
| Medium | Mar, 14, 2021, 07:15 PM | SOC137 - Malicious File/Script Download Attempt | 76 | Malware | >> <input checked="" type="checkbox"/> |
| Critical | Oct, 06, 2023, 08:05 PM | SOC227 - Microsoft SharePoint Server Elevation of Privilege - Possible CVE-2023-29357 Exploitation | 189 | Web Attack | >> <input checked="" type="checkbox"/> |
| Critical | Apr, 18, 2024, 03:09 AM | SOC274 - Palo Alto Networks PAN-OS Command Injection Vulnerability Exploitation (CVE-2024-3400) | 249 | Web Attack | >> <input checked="" type="checkbox"/> |

Click on >> Close Alert

The screenshot shows a modal dialog box titled "Close Alert". It contains fields for "Event ID" (set to 257), "True Positive" (radio button selected), and "False Positive" (radio button). A note section contains the text: "to sent malicious content to the victim and was successful. The email is deleted from the Host machine and the machine is contained". At the bottom is a blue "Close Alert" button.

Click on >> Closed Alert

Lessons Learned

- Email security filters aren't foolproof: This email bypassed initial security measures, highlighting the need for multiple layers of defense.
- User awareness is critical: Even with technical controls, users remain the last line of defense. Security awareness training could have prevented Felix from opening the malicious URL.
- Quick response matters: Rapid identification and containment prevented the potential compromise from spreading across the network.
- Documentation is essential: Proper artifact collection enables future analysis and helps identify patterns in attacker behavior.

Conclusion

This investigation demonstrates a typical phishing attack lifecycle: from initial delivery to user interaction and finally containment. The quick response prevented a potentially serious security incident from escalating. As SOC analysts, our role is not just to respond to threats but to continuously learn from each incident to strengthen our organization's security posture.