

# Phishing Analysis Tools

2026/01/12

## Phishing case 1

**Scenario:** You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

**Task:** Use the tools discussed throughout this room (or use your own resources) to help you analyze each email header and email body.

Step 1: What brand was this email tailored to impersonate?



After investigating the header, I was able to see the brand – **Netflix**.

Step 2: What is the From email address?



In the header again we can see that the ‘From’ email address is - **JGQ47wazXe1xYVBrkeDg-JOg7ODDQwWdR@JOg7ODDQwWdR-yVkCaBkTNp.gogolecloud.com**.

Name: Phish3Case1.eml  
Size: 58,107 bytes  
Type: message/rfc822  
Loaded: 100%

**Output** time: 40ms  
length: 58107  
lines: 1127

```
Received: from 10.197.37.234
by atlas105.free.mail.bf1.yahoo.com with HTTPS;
Wed, 7 Jul 2021 02:14:46 +0000
Return-Path: <postmaster@etekno.xyz>
X-Originating-IP: [209.85.167.226]
Received-SPF: none (domain of etekno.xyz does not
designate permitted sender hosts)
Authentication-Results:
atlas105.free.mail.bf1.yahoo.com:
```

STFP 

For this I opened up **Cyberchef** and opened up the 'Phish3Case1.eml' file in the input section and then was able to see the IP address - **209.85.167.226**.

Operations	Recipe	Input
defang	Defang IP Addresses	209.85.167.226
Defang URL		
Defang IP Addresses		
Favourites 		
Data format		
Encryption / Encoding		
Public Key		
Arithmetic / Logic		
...		

**Output** time: 1ms  
length: 20  
lines: 1

```
209[.]85[.]167[.]226
```

I then copied the IP address, cleared the input then entered the IP address only. I then went on the 'Operations' section on the far left and searched for the 'Defang IP Addresses' operation and dragged it to the **Recipe**. In the output I was able to get the defanged output – **209[.]85[.]167[.]226**

Step 3: From what you can gather, what do you think will be a domain of interest? Defang the domain.

**Input** length: 58,107 total: 2 loaded: 2 + ⌂ ⌄ ⌁ ⌃



Name: Phish3Case1.eml  
Size: 58,107 bytes  
Type: message/rfc822  
Loaded: 100%

**Output** start: 223 time: 55ms end: 233 length: 58151 length: 10 lines: 1127 ⌂ ⌄ ⌁ ⌃

```
Received: from 10[.]197[.]37[.]234
by atlas105.free.mail.bf1.yahoo.com with HTTPS;
Wed, 7 Jul 2021 02:14:46 +0000
Return-Path: <postmaster@etekno.xyz>
X-Originating-Ip: [209[.]85[.]167[.]226]
Received-SPF: none (domain of etekno.xyz does not
designate permitted sender hosts)
```

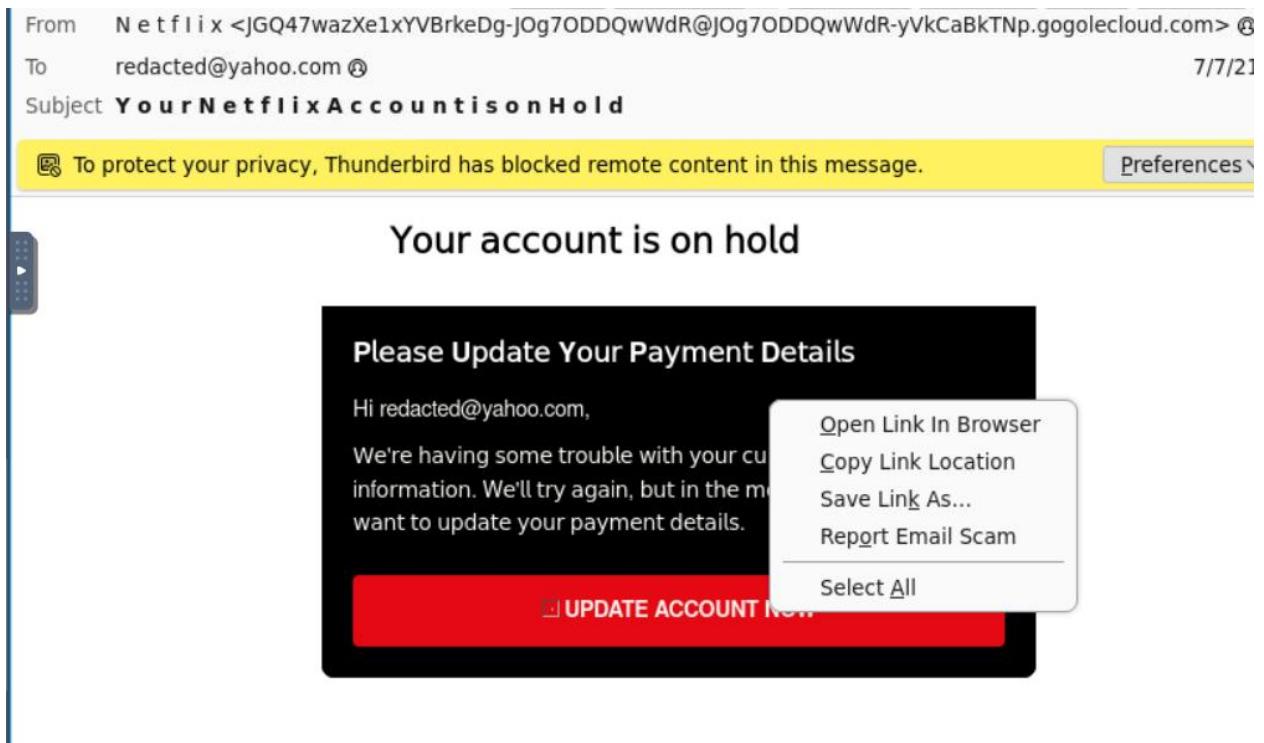
For the following task, I was able to open up the ‘Phish3Case1.eml’ file again and found the domain in the output – **etekno.xyz**.

The screenshot shows the CyberChef interface with a pipeline for processing an EML file. The left sidebar lists various operations under the 'Operations' category, with 'Defang URL' selected. The main area shows a 'Recipe' step with three checked options: 'Escape dots', 'Escape http', and 'Escape ::/'. Below this is a 'Process' step with the placeholder 'Valid do...'. The 'Input' section shows a file named 'Phish3Case1.eml' with the following details: Name: Phish3Case1.eml, Size: 58,107 bytes, Type: message/rfc822, Loaded: 100%. The 'Output' section displays the raw header information of the file:

```
Received: from 10[.]197[.]37[.]234  
by atlas105[.]free[.]mail[.]bf1[.]yahoo[.]com with  
HTTPS; Wed, 7 Jul 2021 02:14:46 +0000  
Return-Path: <postmaster@etekno[.]xyz>  
X-Originating-Ip: [209[.]85[.]167[.]226]  
Received-SPF: none (domain of etekno[.]xyz does not  
designate permitted sender hosts)  
Authentication-Results:
```

At this point I was surprised at the fact that the previous IP address we were working with had been defanged. The operations seem to work with the contents from outside the file. I added the 'Defang URL' operation and was able to defang the domain - **etekno[.]xyz**.

Step 4: What is the shortened URL? Defang the URL.



For this I opened up the email on outlook, right clicked on the update... button and clicked 'Copy link location'.

The screenshot shows the Defang tool interface. On the left is a sidebar with categories: Operations, defang, Defang URL (which is selected), Defang IP Addresses, Favourites (with a star icon), Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, and Networking. The main area has tabs for Recipe, Input, and Output. Under Recipe, there is a "Defang URL" section with checkboxes for "Escape dots", "Escape http", and "Escape ://". Under Input, the URL "https://t.co/yuxfZm8KPg?amp=1" is shown. Under Output, the transformed URL "hxps[://]t[.]co/yuxfZm8KPg?amp=1" is displayed. The status bar at the bottom indicates "time: 2ms", "length: 33", and "lines: 1".

I opened up **Cyberchef** once again and pasted the link in the input section. I looked on the left side again and searched for the ‘Defang URL’ operation and dragged it to the **Recipe** section and only then I was able to get the defanged output - **hxxps[://]t[.]co/yuxfZm8KPg?amp==1**.

## Phishing case 2

**Scenario:** You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to AnyRun for analysis.

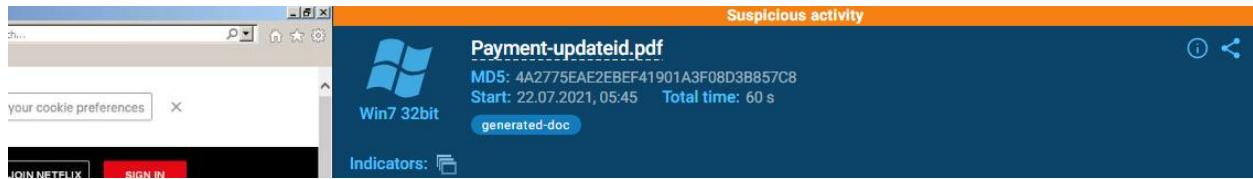
**Task:** Investigate the analysis and answer the questions below.

Step 1: What does AnyRun classify this email as?

The screenshot shows the AnyRun analysis interface. On the left, there's a small window showing a browser tab with a 'your cookie preferences' button and a 'JOIN NETFLIX' button. The main interface is titled 'Suspicious activity' and shows a file named 'Payment-updateid.pdf'. It provides basic metadata: MD5: 4A2775EAE2EBEF41901A3F08D3B857C8, Start: 22.07.2021, 05:45, Total time: 60 s, and a status 'generated-doc'. Below this, there's a toolbar with 'Get sample', 'IOC', 'MalConf', 'Restart', 'Text report', 'Graph', 'ATT&CK', 'Tools', 'Export', and a dropdown for 'Only important'. A chart at the bottom shows CPU usage across 17 processes, with one process highlighted: AcroRd32.exe (PID 2088) running 'C:\Users\admin\AppData\Local\Temp\Payment-updateid.pdf'. The interface has a dark theme with blue and orange highlights.

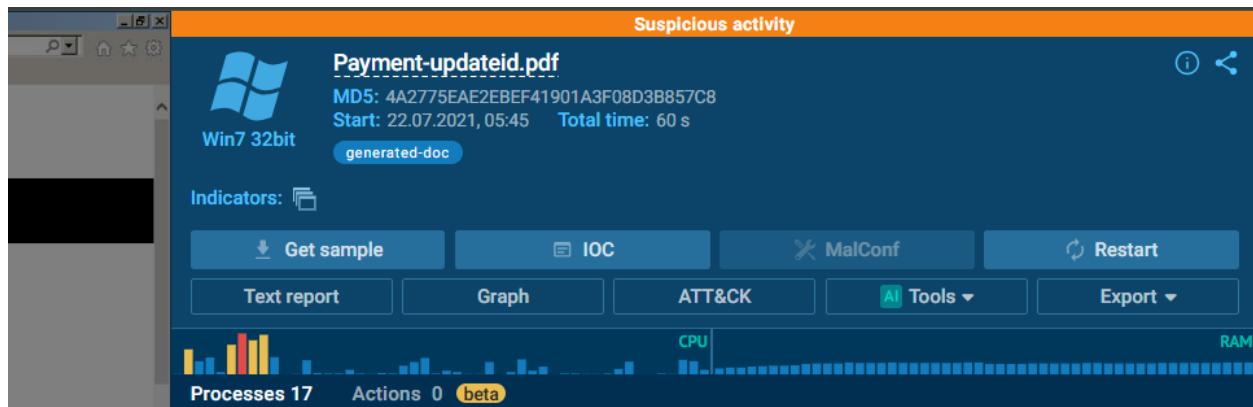
I opened up AnyRun and at the top right I was able to find that it's classified as – **Suspicious activity**.

Step 2: What is the name of the PDF file?



Right under the classification of the email, I found the name of the PDF file – **Payment-updateid.pdf**.

Step 3: What is the SHA 256 hash for the PDF file?



For this I clicked on 'Text report'.

A screenshot of the 'Text report' section under 'General Info'. It lists various file details:

- File name: Payment-updateid.pdf
- Full analysis: <https://app.any.run/tasks/8bf4c58-ec0d-4371-bfeb-52a334b69f59>
- Verdict: **Suspicious activity**
- Analysis date: July 22, 2021 at 05:45:38
- OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
- Tags: **generated-doc**
- Indicators:
- MIME: application/pdf
- File info: PDF document, version 1.7
- MD5: 4A2775EAE2EBEF41901A3F08D3B857C8
- SHA1: 8B3439F5EA2F20C6BE329C4C6B8EAA9CC439233B
- SHA256: CC6F1A04B10BCB168AEEC8D870B97BD7C20FC161E8310B5BCE1AF8ED420E2C24
- SSDEEP: 3072:eiII[NpcqF7c/DTmHbARHwHfScBb/]KPNsxcQ0XLN40/yU:pTpocqF7IPmHbGHwHfSEg2xcVXLNP/h

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

After opening up the document I skimmed through each line looking for the SHA256 and I found it - **CC6F1A04B10BCB168AEEC8D870B97BD7C20FC161E8310B5BCE1AF8ED420E2C24**.

Step 4: What two IP addresses are classified as malicious? Defang the IP addresses.  
(answer: IP\_ADDR,IP\_ADDR)

#### Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2088	AcroRd32.exe	2.16.107.24:443	acroipm2.adobe.com	Akamai International B.V.	-	malicious
1776	svchost.exe	2.16.107.83:443	ardownload3.adobe.com	Akamai International B.V.	-	malicious
3812	AdobeARM.exe	2.16.107.83:443	ardownload3.adobe.com	Akamai International B.V.	-	malicious

I scrolled down the page to connections and I found the IP addresses – ‘2.16.107.24’ and ‘2.16.107.83’.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations: 'Operations' (selected), 'defang', 'Defang URL', 'Defang IP Addresses' (which is highlighted in green), 'Favourites' (with a star icon), 'Data format', 'Encryption / Encoding', 'Public Key', and 'Arithmetic / Logic'. The main area is divided into 'Recipe' and 'Input' sections. In the 'Recipe' section, the 'Defang IP Addresses' operation is selected. In the 'Input' section, the IP addresses '2.16.107.24' and '2.16.107.83' are listed. Below this, the 'Output' section shows the defanged versions: '2[.]16[.]107[.]24' and '2[.]16[.]107[.]83'. The interface includes various icons for file operations like copy, paste, and save.

I opened up **Cyberchef**. I copied and pasted both IP addresses in the input section on the right, went to the left side and looked for the ‘Defang IP Addresses’ operation. I dragged it to the **Recipe** section and clicked ‘Bake!’. The two defanged IP addresses were -  
2[.]16[.]107[.]24,2[.]16[.]107[.]83.

Step 5: What Windows process was flagged as **Potentially Bad Traffic**?

#### Threats

PID	Process	Class	Message
1776	svchost.exe	Potentially Bad Traffic	ET INFO TLS Handshake Failure

I scrolled further down to 'Threats' and the Process flagged as **Potentially Bad Traffic** - **svchost.exe**.

### Phishing case 3

**Scenario:** You are a Level 1 SOC Analyst. Several suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email for your team to implement the appropriate rules to prevent colleagues from receiving additional spam/phishing emails.

A malicious attachment from a phishing email inspected in the previous Phishing Room was uploaded to Any Run for analysis.

**Task:** Investigate the analysis and answer the questions below.

Step 1: What is this analysis classified as?

The screenshot shows the AnyRun analysis interface. At the top, there's a red bar with the text "Malicious activity" next to a biohazard icon. Below this, the file name "CBJ200620039539.xlsx" is displayed, along with its MD5 hash ("F7F4EC2A0ADC9CC33CDBC7D548A6BEF9") and the analysis start time ("22.07.2021, 07:05"). The total analysis time is listed as "60 s". At the bottom of the interface, there are three tags: "trojan", "exploit", and "cve-2017-11882". On the far right of the interface, there are icons for information and sharing.

I opened up AnyRun. Looking at the top right, I identified the analysis classified – **Malicious activity**.

## Step 2: What is the name of the Excel file?

The screenshot shows a Microsoft Excel window titled "CBJ200620039539.xlsx - Microsoft Excel". The "Developer" tab is selected. In cell B56, there is a warning message in Chinese:

免责声明：  
此电子邮件及随之传送的任何文件均为  
机密信息，仅供其所针对的个人或实体  
使用。  
本电子邮件的内容（包括附件或附件的  
内容，如果有的话）是Menon and  
Menon  
有限公司的特权和机密材料，不得以任何方式  
披露、使用或复制除了预定的收件人  
之外的任何人。  
如果收到此电子邮件（包括机密或附件  
）（如果有），请立即通知发件人并从  
系统中删除。

To the right of the Excel window, there is a vertical sidebar titled "Indicators" and "Processes".

I identified the name of the file after navigating to the screenshots on AnyRun - CBJ200620039539.xlsx.

## Step 3: What is the SHA 256 hash for the file?

The screenshot shows the AnyRun analysis interface for the file "CBJ200620039539.xlsx". The file is identified as a "Trojan" and has a MD5 hash of "F7F4EC2A0ADC9CC33CDBC7D548A6BEF9". The analysis started at "22.07.2021, 07:05" and took "60 s".

Indicators: 🛡️ 🚧 🗃️ \*

Tracker: Trojan

Buttons: Get sample, IOC, MalConf, Restart, Text report, Graph, ATT&CK, Tools, Export.

I opened up Text report.

## General Info

Add for printing ▾

File name:	CBJ200620039539.xlsx
Full analysis:	<a href="https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83">https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83</a>
Verdict:	<span style="background-color: red; color: white; padding: 2px 5px;">Malicious activity</span>
Threats:	<span style="background-color: red; color: white; padding: 2px 5px;">Trojan</span>
Trojans are a group of malicious programs distinguished by their ability to masquerade as benign software. Depending on their type, trojans possess a variety of capabilities, ranging from maintaining full remote control over the victim's machine to stealing data and files, as well as dropping other malware. At the same time, the main functionality of each trojan family can differ significantly depending on its type. The most common trojan infection chain starts with a phishing email.	

Malware Trends Tracker >>

Analysis date:	July 22, 2021 at 07:05:05
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	<span style="border: 1px solid black; border-radius: 15px; padding: 2px 5px;">trojan</span> <span style="border: 1px solid black; border-radius: 15px; padding: 2px 5px;">exploit</span> <span style="border: 1px solid black; border-radius: 15px; padding: 2px 5px;">cve-2017-11882</span>
Indicators:	<span style="color: #ccc; font-size: small;">* ☰ 📈 📈</span>
MIME:	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
File info:	Microsoft Excel 2007+
MD5:	F7F4EC2A0ADC9CC33CDCB7D548A6BEF9
SHA1:	D460315F92AA3DCA63617431883834ED94C09F45
SHA256:	5F94A66E0CE78D17AFC2D27FC17B44B3FFC13AC5F42D3AD6A5DCF836715F3E9
SSDeep:	384:jhzRPm16A+FEAgjnjp505ykBmx4ml/NhQqhKZLOU2puVnF5:NzsAMpE5TsWGHhKZ+

In the document, I swiftly skimmed through to find the SHA256 - **5f94a66e0ce78d17afc2dd27fc17b44b3ffc13ac5f42d3ad6a5dcfb36715f3eb**.

Step 4: What domains are listed as malicious? Defang the URLs & submit answers in alphabetical order. (answer: **URL1,URL2,URL3**)

### Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1068	EQNEDT32.EXE	204.11.56.48:80	biz9holdings.com	Confluence Networks Inc	VG	<span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>
1068	EQNEDT32.EXE	103.224.182.251:80	findresults.site	Trellian Pty. Limited	AU	<span style="background-color: orange; color: black; padding: 2px 5px;">suspicious</span>
1068	EQNEDT32.EXE	75.2.11.242:80	ww38.findresults.site	AT&T Services, Inc.	US	<span style="background-color: red; color: white; padding: 2px 5px;">malicious</span>

I scrolled down to connections and Identified 3 malicious domains namely - **biz9holdings.com**, **findresults.site**, **ww38.findresults.site**.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like 'defang', 'Defang URL', 'Defang IP Addresses', etc. The main area has a 'Recipe' section where 'Defang URL' is selected. Under 'Defang URL', three checkboxes are checked: 'Escape dots', 'Escape http', and 'Esc ://'. Below this is a 'Process' button and a placeholder 'Valid do...'. To the right, there are 'Input' and 'Output' sections. The 'Input' section contains three lines of text: 'biz9holdings.com', 'findresults.site', and 'ww38.findresults.site'. The 'Output' section shows the results after processing: 'biz9holdings[.]com', 'findresults[.]site', and 'ww38[.]findresults[.]site'.

I copied them and pasted them into **Cyberchef** where I navigated to the left side of the page to discover the ‘Defang URL’ operation and dragged and dropped in the **Recipe** section. I was then able to get the defanged Output - **biz9holdings[.]com, findresults[.]site, ww38[.]findresults[.]site**.

Step 5: What IP addresses are listed as malicious? Defang the IP addresses & submit answers from lowest to highest. (answer: **IP1,IP2,IP3**)

#### Connections

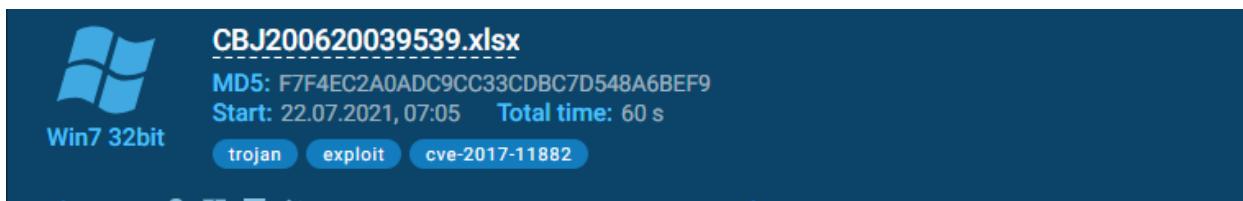
PID	Process	IP	Domain	ASN	CN	Reputation
1068	EQNEDT32.EXE	204.11.56.48:80	biz9holdings.com	Confluence Networks Inc	VG	malicious
1068	EQNEDT32.EXE	103.224.182.251:80	findresults.site	Trellian Pty. Limited	AU	suspicious
1068	EQNEDT32.EXE	75.2.11.242:80	ww38.findresults.site	AT&T Services, Inc.	US	malicious

I copied all the IP Addresses - **75.2.11.242, 103.224.182.251, 204.11.56.48**.

The screenshot shows the CyberChef interface with the 'Defang IP Addresses' recipe selected. The input section contains three IP addresses: 75.2.11.242, 103.224.182.251, and 204.11.56.48. The output section shows the defanged versions: 75[.]2[.]11[.]242, 103[.]224[.]182[.]251, and 204[.]11[.]56[.]48.

I opened up **Cyberchef** once again and changed the recipe to the ‘Defang IP Addresses’ operation and Baked it. I was then able to get the defanged IP addresses –  
**75[.]2[.]11[.]242,103[.]224[.]182[.]251,204[.]11[.]56[.]48.**

Step 6: What vulnerability does this malicious attachment attempt to exploit?



It attempts to exploit the – **cve-2017-11882** vulnerability.

## Summary Conclusion

This exercise provided comprehensive, hands-on experience with phishing analysis tools and workflows commonly used by Level 1 SOC Analysts. Across all three phishing cases, I applied systematic email analysis techniques to extract actionable indicators of compromise (IOCs), including spoofed sender details, malicious domains, shortened URLs, IP addresses, file hashes, and associated processes.

In Phishing Case 1, I analyzed email headers and body content to identify brand impersonation, suspicious sender infrastructure, and malicious links. By using CyberChef to safely defang domains, URLs, and IP addresses, I demonstrated secure handling of phishing artifacts and produced indicators suitable for detection and blocking rules.

Phishing Cases 2 and 3 focused on attachment-based threats analyzed through AnyRun. I interpreted sandbox classifications, extracted file metadata and SHA-256 hashes, identified malicious network connections, and observed flagged system processes and exploit behavior. These cases highlighted the importance of correlating dynamic analysis results with static indicators to fully understand attacker intent and impact.

Overall, this activity strengthened my ability to use industry-standard tools such as CyberChef and AnyRun to investigate phishing threats, document findings clearly, and support SOC teams with reliable, defanged indicators for prevention and response.