



## **Official incident report**

Event ID: 257

Rule Name: SOC282 – Phishing Alert (Deceptive Mail Detection)

# Table of contents

<b>Official incident report</b>	<b>1</b>
Event ID: 257	1
Rule Name: SOC282 –Phishing Alert (Deceptive Mail Detection)	1
<b>Table of contents</b>	<b>2</b>
<b>Event Details</b>	<b>3</b>
<b>Network Information Details</b>	<b>3</b>
<b>Detection</b>	<b>4</b>
Threat intelligence & Security Email	4
<b>Analysis</b>	<b>15</b>
Log management	15
End Point Security	17
<b>Conclusion</b>	<b>20</b>

# Event Details

**Event ID:**

257

**Event Date and Time:**

May, 13, 2024, 09:22 AM

**Rule:**

SOC251 – Phishing Alert (Deceptive Mail Detection)

**Level:**

Security Analyst

# Network Information Details

**Destination Address:**

172.16.20.151

**Source Address:**

103.80.134.63

**External / Internal Attack:**

External

# Detection:

## Threat Intelligence Results

Email Analysis: [free@coffeeshoop.com](mailto:free@coffeeshoop.com)

The screenshot shows the LetsDefend SIEM interface. On the left is a sidebar with navigation options: Monitoring (selected), Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main panel displays a table of alerts. The first alert is highlighted, showing details for a phishing attempt. An orange arrow points to the 'Source Address' field, which contains the email address free@coffeeshoop.com.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	May, 13, 2024, 09:22 AM	SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	>> ✓

**Alert Details:**

- This alert has been re-investigated
- ★ 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

We conducted a comprehensive threat intelligence search using four key websites. The results are as follows:

### 1. VirusTotal

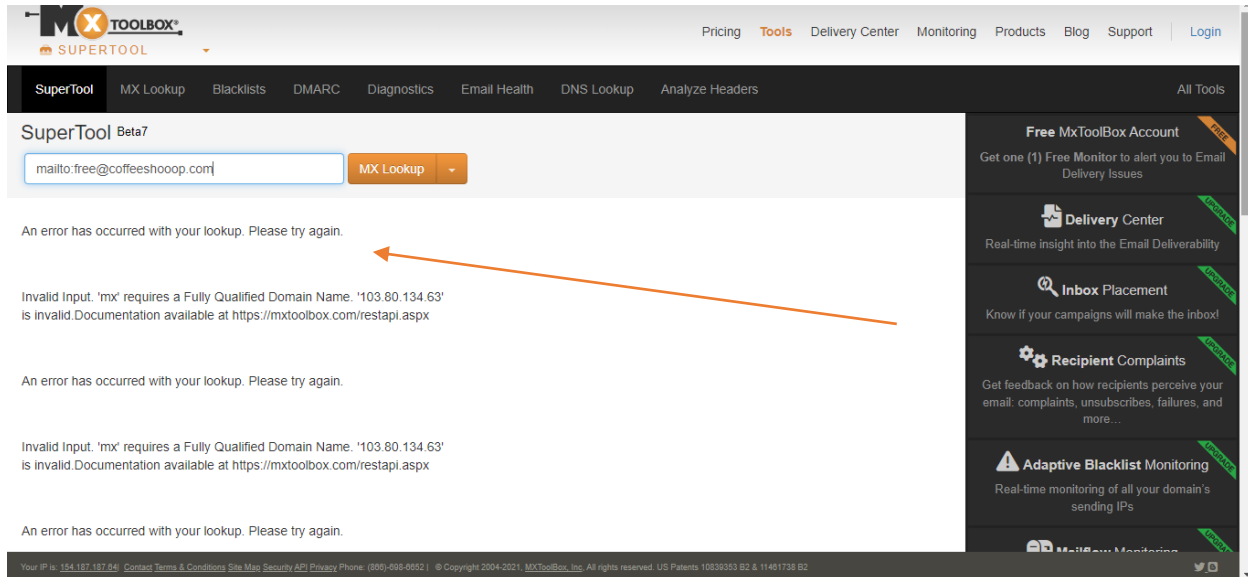
- **Result:** No findings (as shown in the attached photo)

The screenshot shows the VirusTotal search results page. The search bar at the top contains the email address mailto:free@coffeeshoop.com. Below the search bar is a large blue circle with a white question mark icon. Below this icon, the text 'No matches found' is displayed. At the bottom of the page, there are two buttons: 'Try out our offering' and 'Try a new search'. An orange arrow points from the search bar to the 'No matches found' text.

Alternatively, do you want to locate your threat based on static, dynamic, content, attribution or other advanced IoC context? Our platform allows you to search across our entire threat corpus using a myriad of modifiers, learn more.

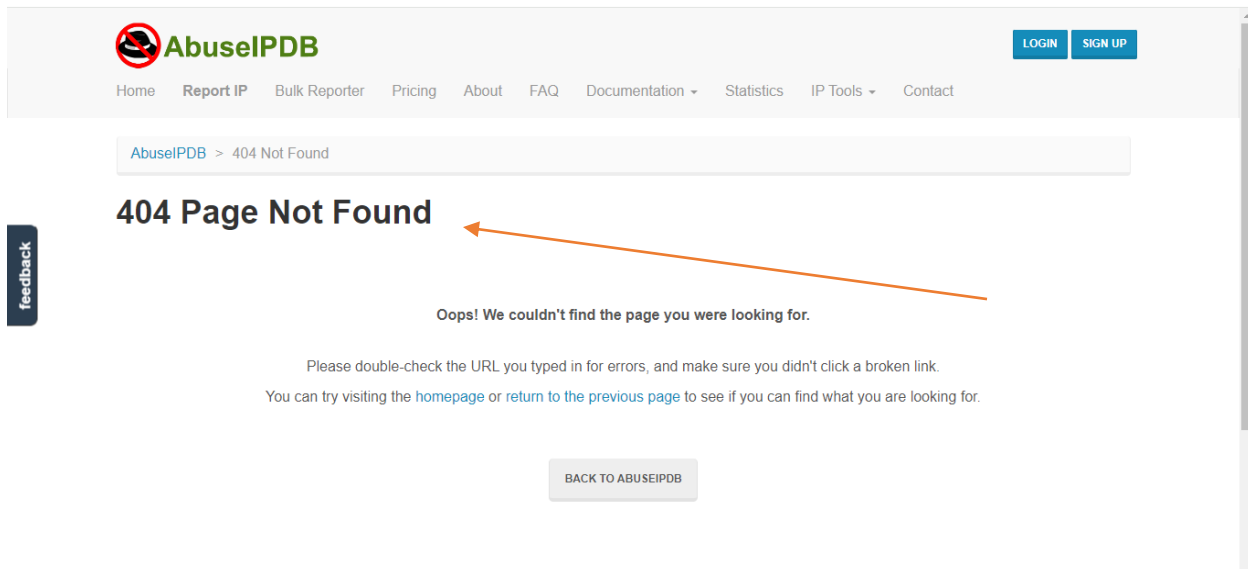
## 2. MXToolbox

- **Result:** No findings (as shown in the attached photo)



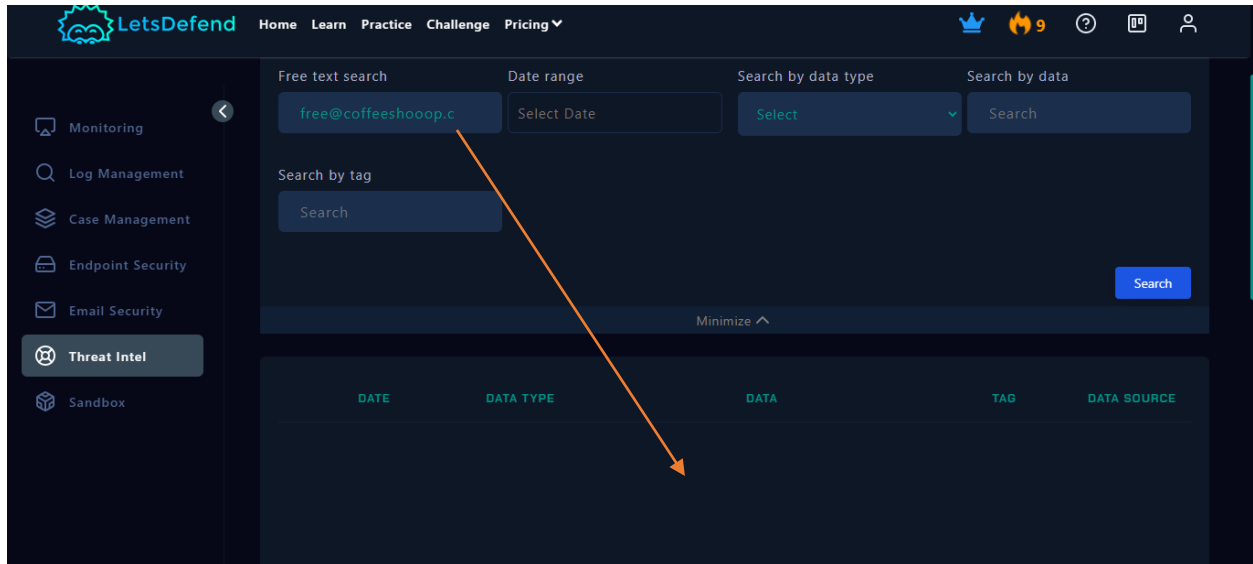
## 3. AbuseIPDB

- **Result:** No findings (as shown in the attached photo)



#### 4. LetsDefend

- **Result:** No findings (as shown in the attached photo)



## SMTP IP Address Analysis: 103.80.134.63

The IP address 103.80.134.63 was thoroughly investigated across multiple platforms. The detailed findings are as follows:

The screenshot displays the LetsDefend SIEM interface. The left sidebar contains navigation options: Monitoring (selected), Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main panel shows a table of alerts with columns: SEVERITY, DATE, RULE NAME, EVENTID, TYPE, and ACTION. A single alert is visible, dated May 13, 2024, 09:22 AM, with a severity of Medium. The rule name is 'SOC282 - Phishing Alert - Deceptive Mail Detected'. The event ID is 257, and the type is Exchange. The action column shows a checkmark and a double arrow. Below the table, a message states: 'This alert has been re-investigated. ★ 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.' A detailed view of the alert follows, listing fields: 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, highlighted with an orange arrow), Source Address (free@coffeeshoop.com), Destination Address (Felix@letsdefend.io), E-mail Subject (Free Coffee Voucher), Device Action (Allowed), and a Show Hint button.

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	May, 13, 2024, 09:22 AM	★ SOC282 - Phishing Alert - Deceptive Mail Detected	257	Exchange	>> ✓

This alert has been re-investigated  
★ 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

## 1. VirusTotal

- **Detection:** Please refer to the attached photo for specific details.

The screenshot shows the VirusTotal interface for the IP address 103.80.134.63. The top section displays a 'Community Score' of 13/93 and a warning that 13/93 security vendors flagged this IP address as malicious. Below this, the 'DETECTION' tab is active, showing a table of security vendors' analysis. Two orange arrows point to specific details: one points to the warning message at the top, and the other points to the 'Phishing' detection by BitDefender in the table.

Security vendors' analysis ⓘ			
alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Phishing
CyRadar	ⓘ Malicious	Emsisoft	ⓘ Phishing
Forcepoint ThreatSeeker	ⓘ Malicious	Fortinet	ⓘ Phishing
G-Dat	ⓘ Malware	Google Safebrowsing	ⓘ Phishing
Lionic	ⓘ Malicious	Netcraft	ⓘ Malicious
Seclookup	ⓘ Malicious	VIPRE	ⓘ Malware

- **Details:** Please refer to the attached photo for specific details.

The screenshot shows the 'DETAILS' tab for the IP address 103.80.134.63. It displays various properties including network information, JARM fingerprint, and the last HTTPS certificate. An orange arrow points to the 'Autonomous System Label' field, which identifies the organization as LG DACOM Corporation.

**Basic Properties ⓘ**

Network	103.80.134.0/24
Autonomous System Number	3786
Autonomous System Label	LG DACOM Corporation
Regional Internet Registry	APNIC
Country	KR
Continent	AS

**Last HTTPS Certificate ⓘ**

**JARM Fingerprint**

3fd3fd0003fd3fd21c42d42d000000307ee0eb468e9fdb5cfd698a80a67ef

**Last HTTPS Certificate**

Data:

- Version: V3
- Serial Number: 03e7c82907eff2868476646bc69e8650ab18
- Thumbprint: 67feddf6e7abd3c8d2f82db9d2120958b0253fff
- Signature Algorithm: sha256RSA
- Issuer: C=US , CN=R3 , O=Let's Encrypt
- Validity
  - Not Before: 2022-06-08 06:51:05
  - Not After: 2022-09-06 06:51:04



- **Relations:** Please refer to the attached photo for specific details.

The screenshot shows the VirusTotal interface for IP 103.80.134.63. The 'RELATIONS' tab is selected, displaying a table of Passive DNS Replication data. An orange arrow points to the 'Domain' column of this table.

Date resolved	Detections	Resolver	Domain
2024-06-03	5 / 93	VirusTotal	ltodcyvspg.duckdns.org
2024-06-03	0 / 93	VirusTotal	bzwvtpfczy.duckdns.org
2024-06-03	2 / 93	VirusTotal	eaxpmjhqk.duckdns.org
2024-06-03	2 / 93	VirusTotal	sfdccronqn.duckdns.org
2024-06-03	3 / 93	VirusTotal	yugdzvsqnf.duckdns.org
2024-06-03	3 / 93	VirusTotal	volwtpmjhe.duckdns.org
2024-06-03	4 / 93	VirusTotal	qmggesomkjj.duckdns.org
2024-05-20	8 / 93	VirusTotal	tjpatbcppj.duckdns.org
2024-05-20	12 / 93	VirusTotal	tivfbwtjkq.duckdns.org
2024-05-20	13 / 93	VirusTotal	tililsifou.duckdns.org

- **Community:** Please refer to the attached photo for specific details.

The screenshot shows the VirusTotal interface for IP 103.80.134.63. The 'COMMUNITY' tab is selected, displaying voting and comment details. An orange arrow points to the 'Voting details' section.

**Voting details (1)**

User	Score
publicarray 4 months ago	-1

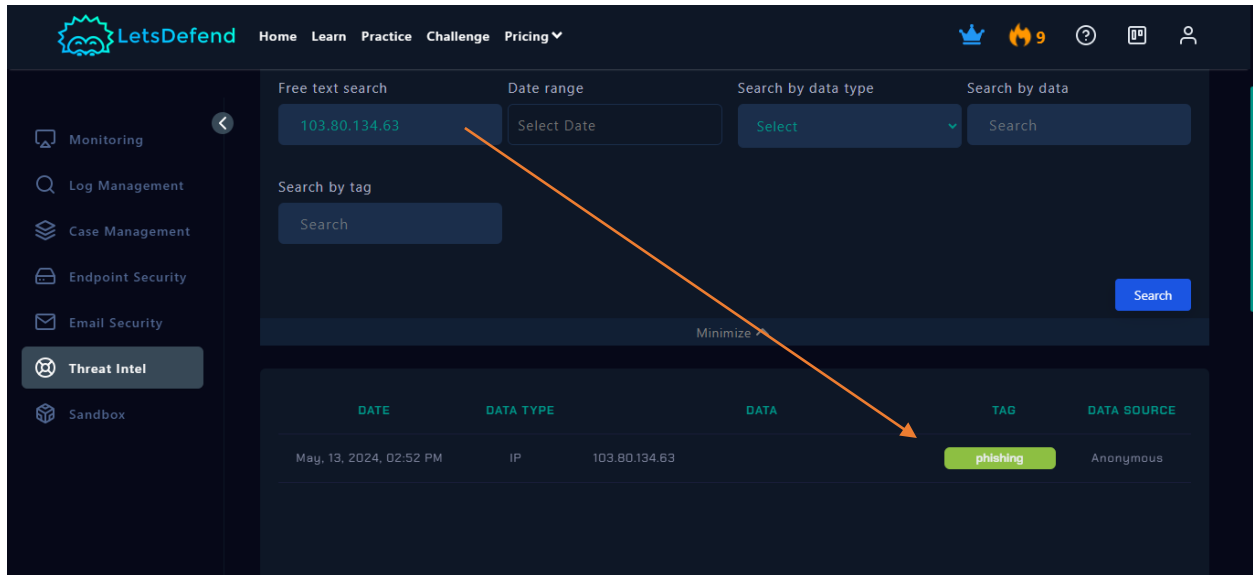
**Comments (1)**

publicarray  
4 months ago

Hosts Phishing pages targeting Apple <https://urlscan.io/search/#page.ip%3A%22103.80.134.63%22>

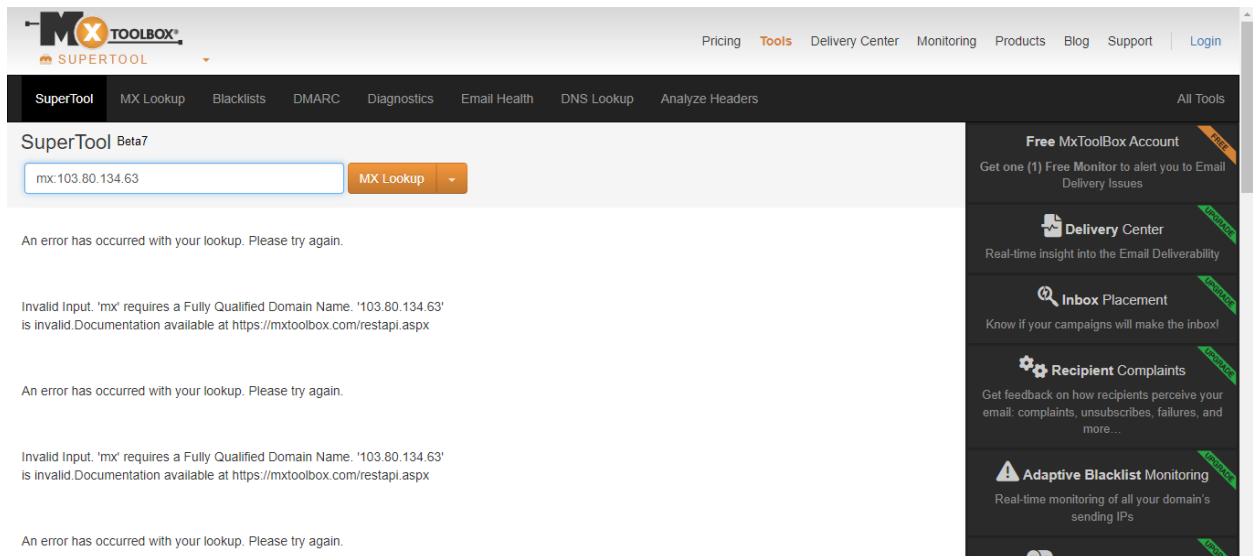
## 2. LetsDefend

- **Result:** Please refer to the attached photo for specific details.



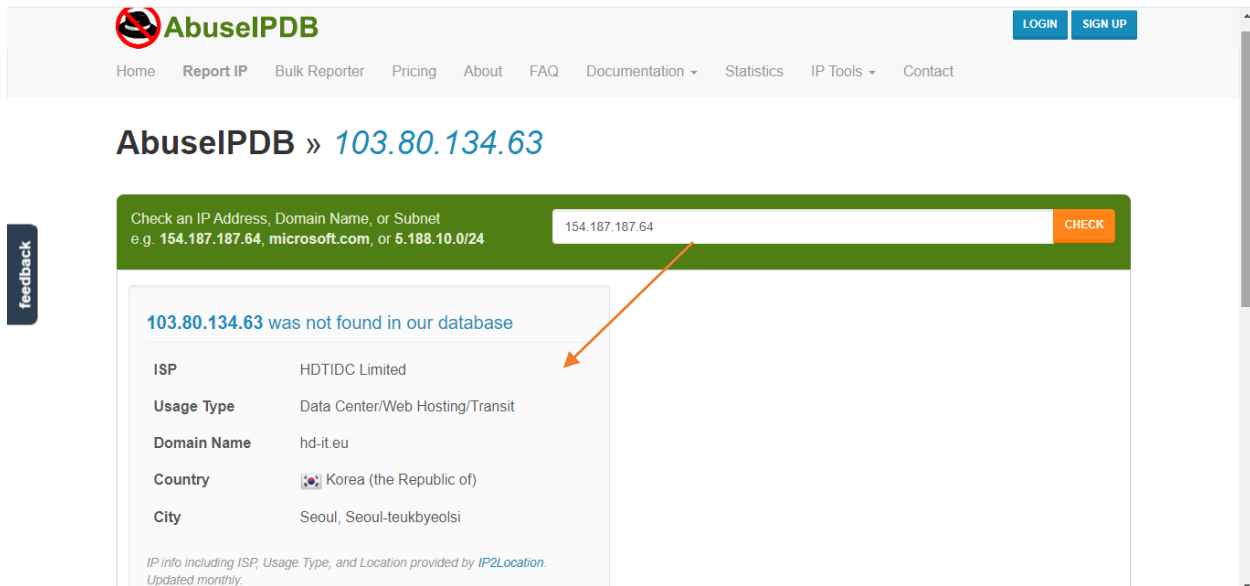
## 3. MXToolbox

- **Result:** No findings (as shown in the attached photo)




#### 4. AbuseIPDB

- **Result:** No findings (as shown in the attached photo)



The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with the AbuseIPDB logo and links for Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. A LOGIN and SIGN UP button is also present. Below the navigation bar, the main heading reads "AbuseIPDB » 103.80.134.63". A green search bar contains the text "Check an IP Address, Domain Name, or Subnet" and "e.g. 154.187.187.64, microsoft.com, or 5.188.10.0/24". The search bar also contains the IP address "154.187.187.64" and a "CHECK" button. Below the search bar, a message states "103.80.134.63 was not found in our database". An orange arrow points from the search bar to this message. Below the message, a table displays information about the IP address:

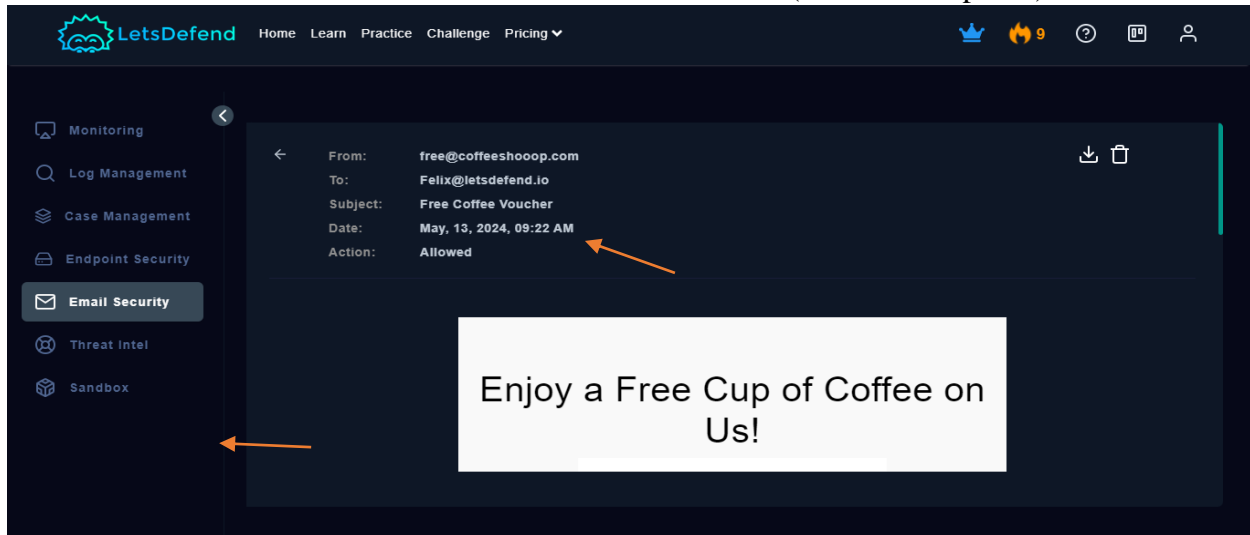
ISP	HDTIDC Limited
Usage Type	Data Center/Web Hosting/Transit
Domain Name	hd-it.eu
Country	 Korea (the Republic of)
City	Seoul, Seoul-teukbyeolsi

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).  
Updated monthly.

As part of our threat analysis, we conducted a thorough investigation of a flagged email. The steps and findings are detailed below:

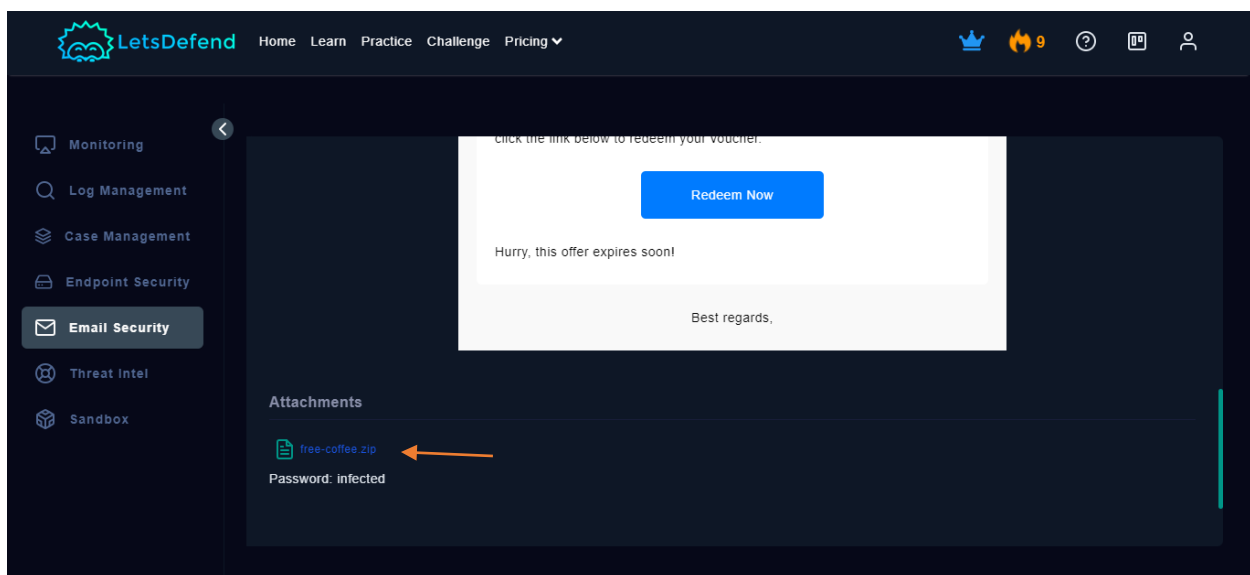
### 1. Email Review

- The email was accessed through the Email Security section, and the sender's email address was identified and documented (see attached photo).



### 2. Attachment Analysis

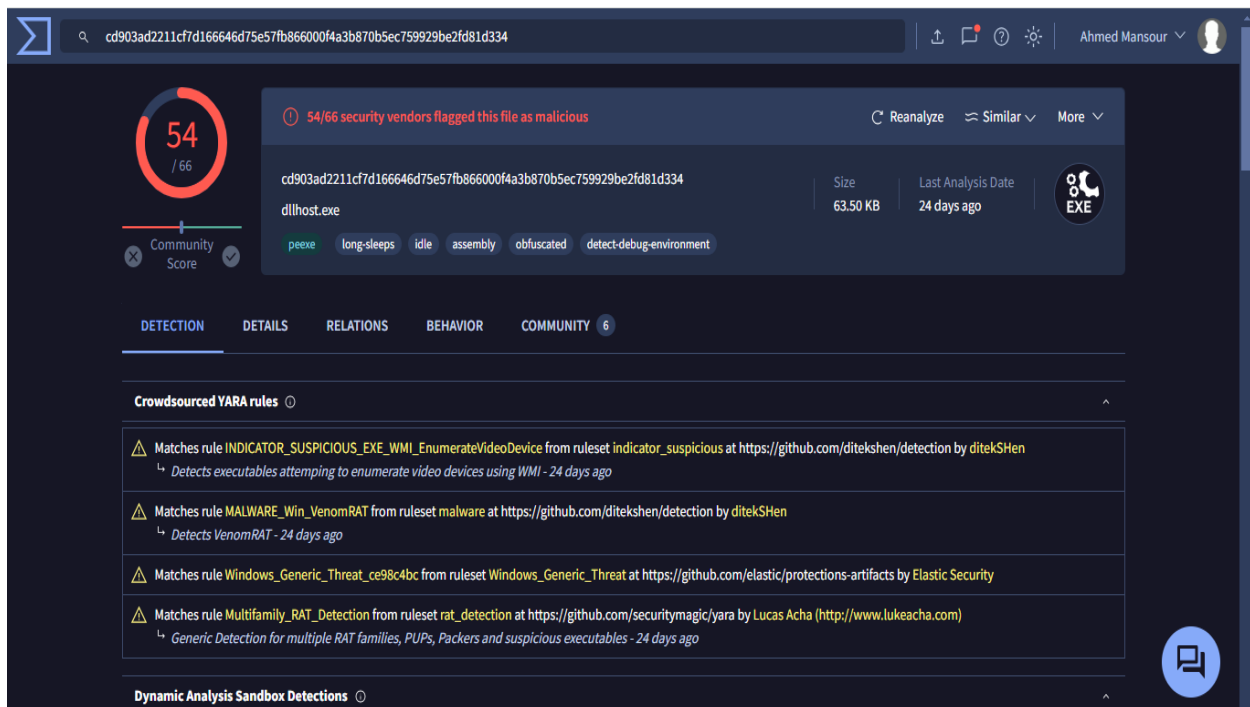
- The email contained an attachment named `free-coffee.zip` (see attached photo).



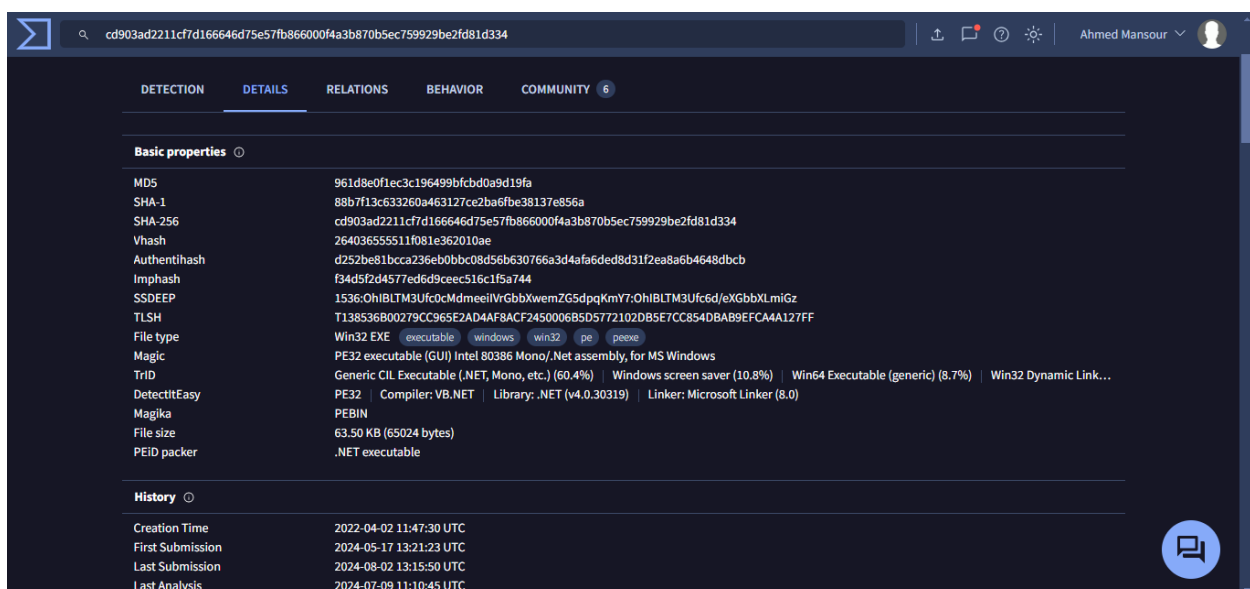
- We proceeded to download the attachment and performed a scan using VirusTotal.com.

### 3. VirusTotal Analysis Results

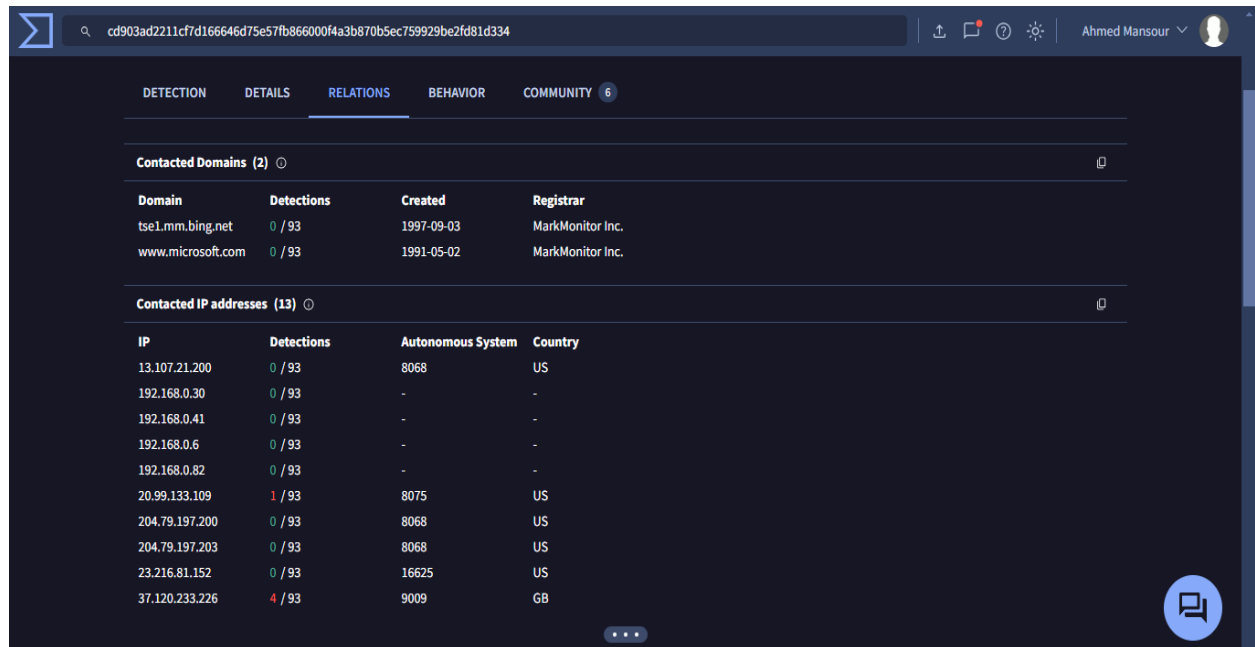
- The scan results indicated that the file was flagged as malicious by several security vendors. The findings from VirusTotal are categorized and summarized as follows:
  - **Detection:** Summary of the threats detected by various security vendors (see attached photo).



- **Details:** Comprehensive metadata and additional file information (see attached photo).



- **Relations:** Connections to other known malicious entities or files (see attached photo).



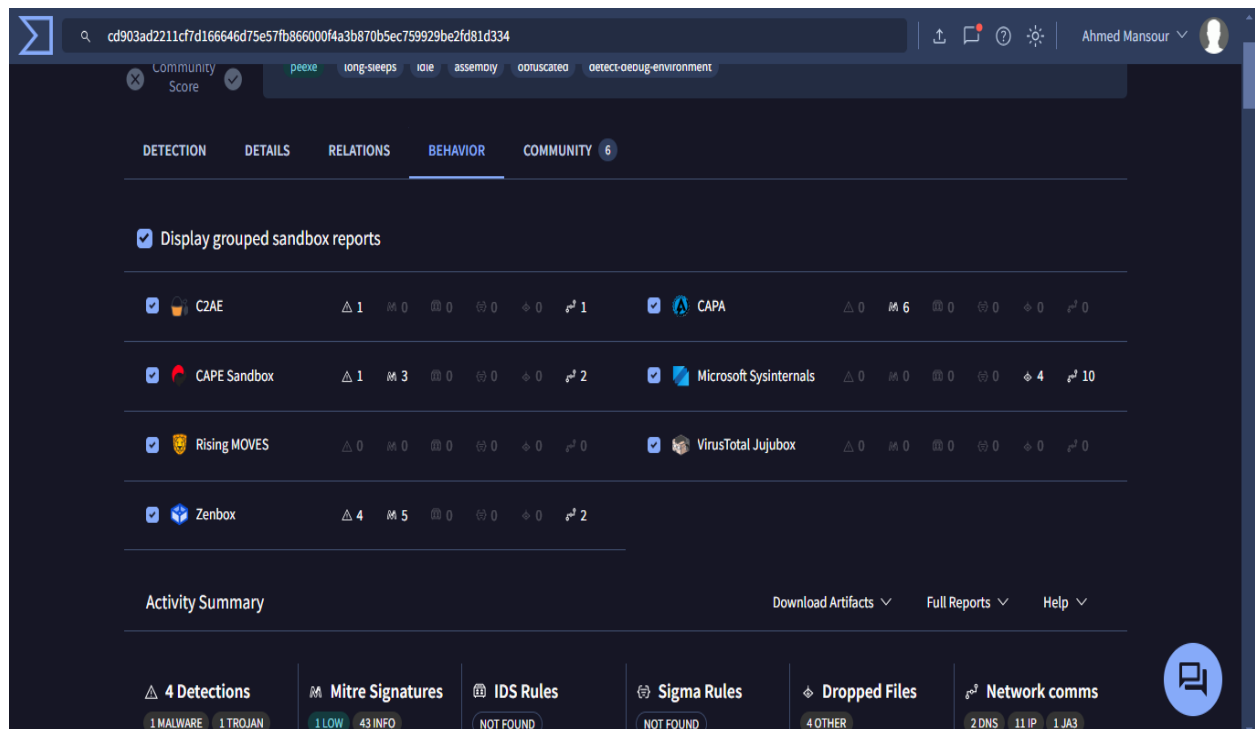
The screenshot shows the VirusTotal interface for a specific file hash. The 'RELATIONS' tab is selected, displaying two sections: 'Contacted Domains (2)' and 'Contacted IP addresses (13)'.

Domain	Detections	Created	Registrar
tse1.mm.bing.net	0 / 93	1997-09-03	MarkMonitor Inc.
www.microsoft.com	0 / 93	1991-05-02	MarkMonitor Inc.

IP	Detections	Autonomous System	Country
13.107.21.200	0 / 93	8068	US
192.168.0.30	0 / 93	-	-
192.168.0.41	0 / 93	-	-
192.168.0.6	0 / 93	-	-
192.168.0.82	0 / 93	-	-
20.99.133.109	1 / 93	8075	US
204.79.197.200	0 / 93	8068	US
204.79.197.203	0 / 93	8068	US
23.216.81.152	0 / 93	16625	US
37.120.233.226	4 / 93	9009	GB

- **Behavior:** Analysis of the file's potential actions and behaviors (see attached photo).



The screenshot shows the VirusTotal interface for the same file hash, with the 'BEHAVIOR' tab selected. It displays a list of sandbox reports and an activity summary.

☒ Display grouped sandbox reports

Sandbox	Delta	Malware	Info	Network	Files	Commands	Process	Clipboard	Mouse	Keyboard	Other
C2AE	1	0	0	0	0	1	0	0	0	0	0
CAPE Sandbox	1	3	0	0	0	2	0	0	0	0	0
Rising MOVES	0	0	0	0	0	0	0	0	0	0	0
Zenbox	4	5	0	0	0	2	0	0	0	0	0
CAPA	0	6	0	0	0	0	0	0	0	0	0
Microsoft Sysinternals	0	0	0	0	0	4	0	0	0	10	0
VirusTotal Jujubox	0	0	0	0	0	0	0	0	0	0	0

**Activity Summary**

Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
4 Detections 1 MALWARE 1 TROJAN	1 LOW 43 INFO	NOT FOUND	NOT FOUND	4 OTHER	2 DNS 11 IP 1 JA3

- **Community:** Insights and feedback from the cybersecurity community (see attached photo).

The screenshot displays the ANY.RUN web interface for file analysis. At the top, a search bar contains the SHA256 hash: `cd903ad2211cf7d166646d75e57fb866000f4a3b870b5ec759929be2fd81d334`. The user profile 'Ahmed Mansour' is visible in the top right corner.

The main analysis section shows a file named `dllhost.exe` with a size of 63.50 KB and a last analysis date of 24 days ago. A circular progress indicator shows a community score of 54/66. A warning message states: '54/66 security vendors flagged this file as malicious'. Below this, a list of tags includes: `peexe`, `long-sleeps`, `idle`, `assembly`, `obfuscated`, and `detect-debug-environment`.

The interface has tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (6). The COMMUNITY tab is active, showing a section for 'Comments (6)'. A comment from 'ANY\_RUN' (posted 24 days ago) is visible, containing the following text:

ANY.RUN Sandbox Analysis:

Verdict: Malicious activity

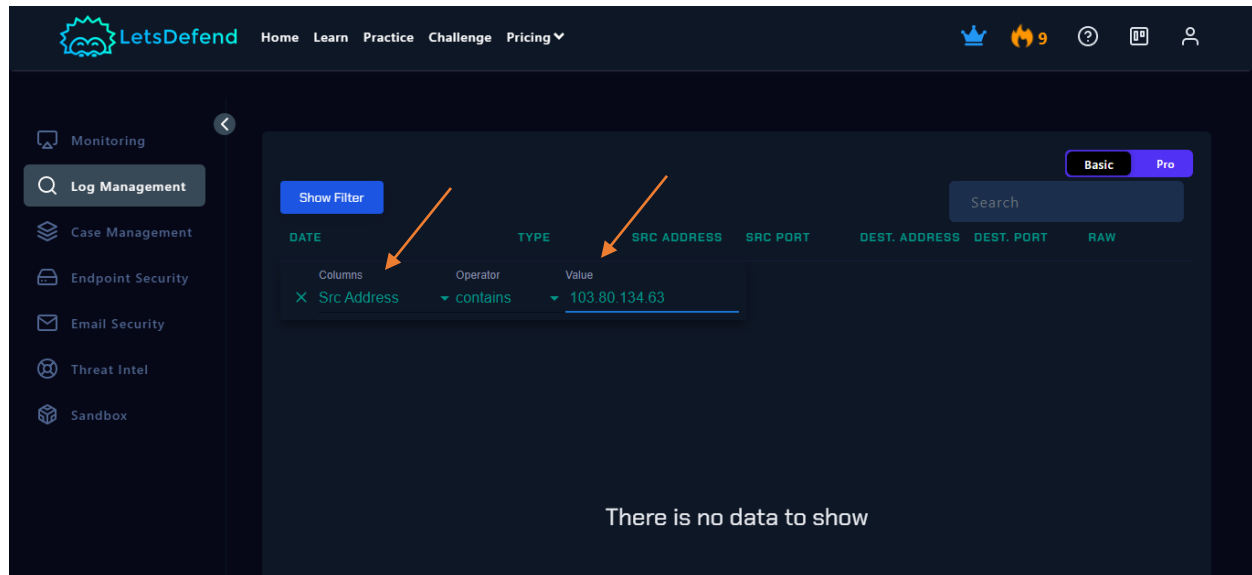
Tags: asynrat

C2: 127.0.0.1, 37.120.233.226

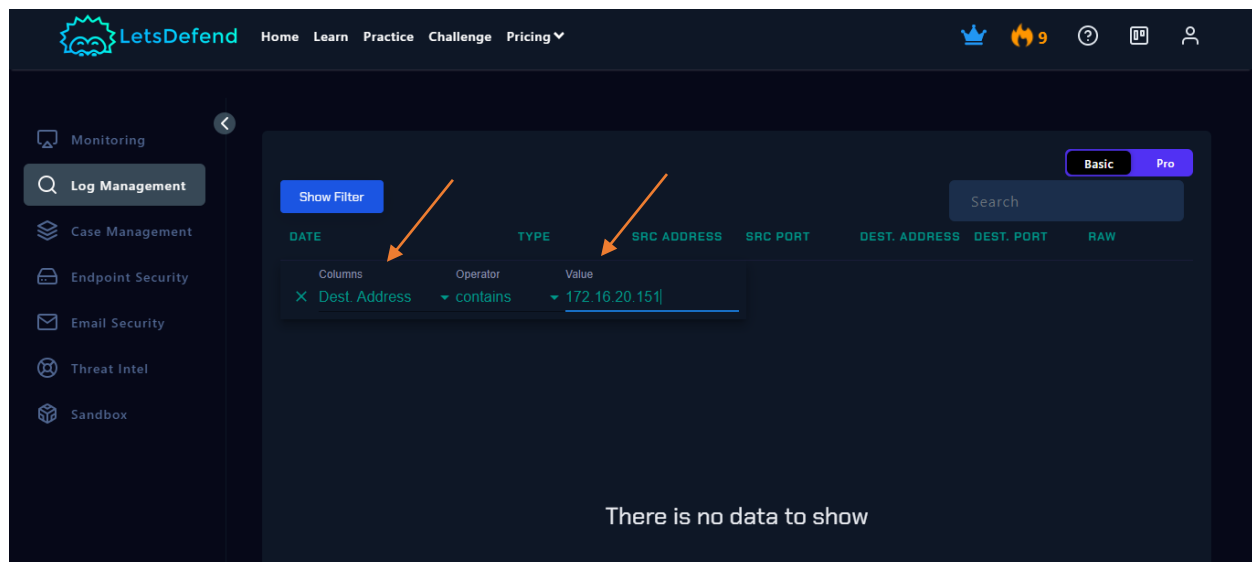
HTML Report: <https://any.run/report/cd903ad2211cf7d166646d75e57fb866000f4a3b870b5ec759929be2fd81d334/f28dd36f-63d4-4eae-ae70-d27b7f7fb6ba>

# Analysis:

## Log Management



No data at all for attacker or victim

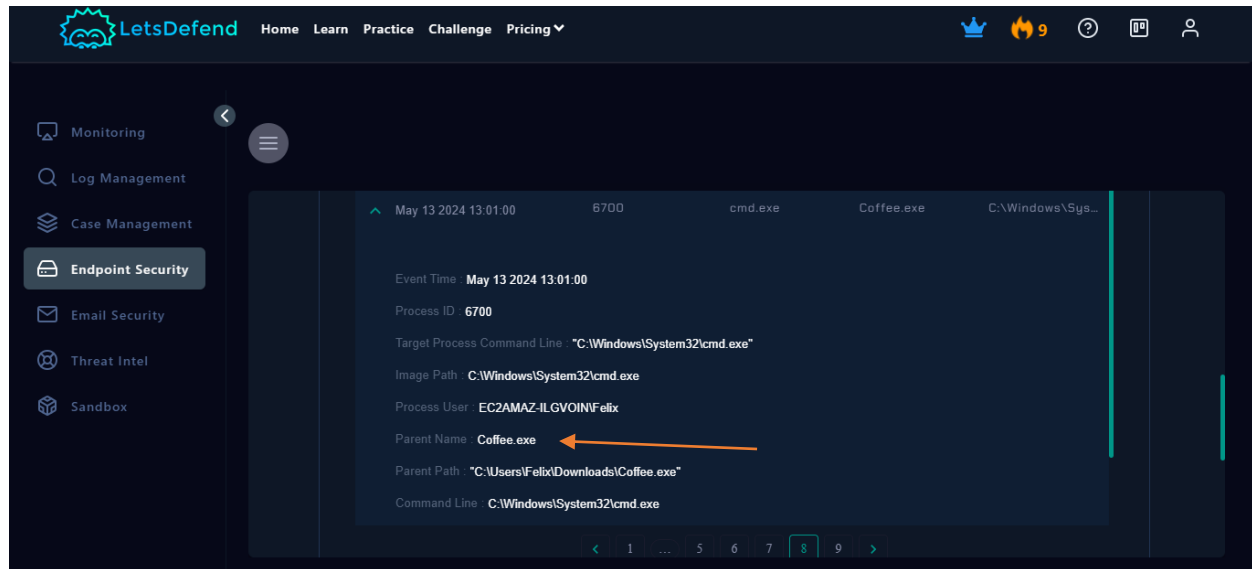




# Endpoint Security

## 1. Process Monitoring

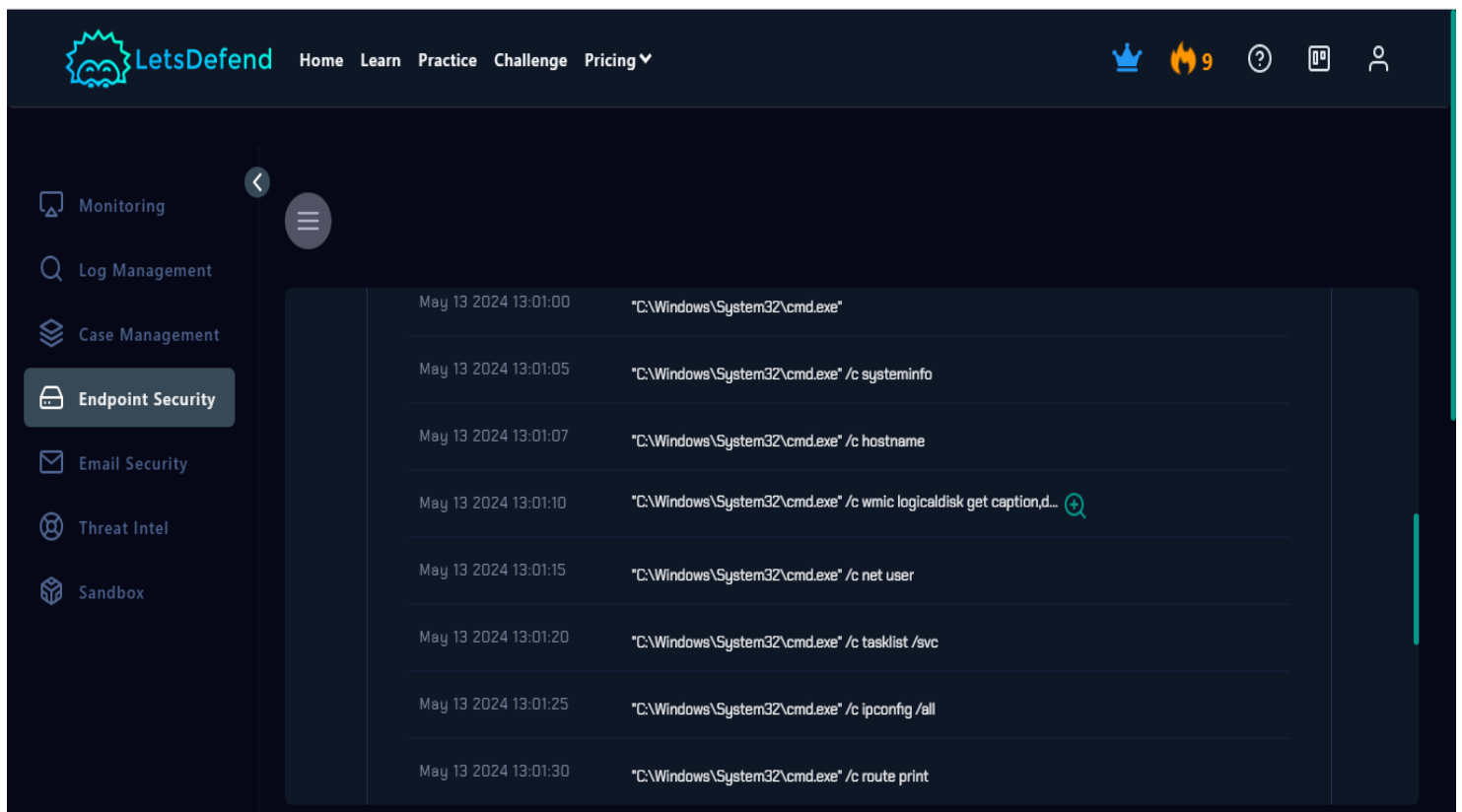
- It was detected that the process `coffee.exe` was executed (see attached photo).



## 2. Terminal Command History

- The following commands were executed in the Command Prompt on May 13, 2024, starting at 13:01:00:
  - **13:01:00:** `cmd.exe` was launched.
  - **13:01:05:** `cmd.exe /c systeminfo` - This command collected comprehensive system information.
  - **13:01:07:** `cmd.exe /c hostname` - Retrieved the hostname of the machine.
  - **13:01:10:** `cmd.exe /c wmic logicaldisk get caption,description,drivetype` - Obtained details about the system's logical drives.
  - **13:01:15:** `cmd.exe /c net user` - Listed all user accounts present on the system.
  - **13:01:20:** `cmd.exe /c tasklist /svc` - Displayed a list of running tasks and their associated services.
  - **13:01:25:** `cmd.exe /c ipconfig /all` - Provided a detailed network configuration report, including IP address information.
  - **13:01:30:** `cmd.exe /c route print` - Displayed the system's routing table.

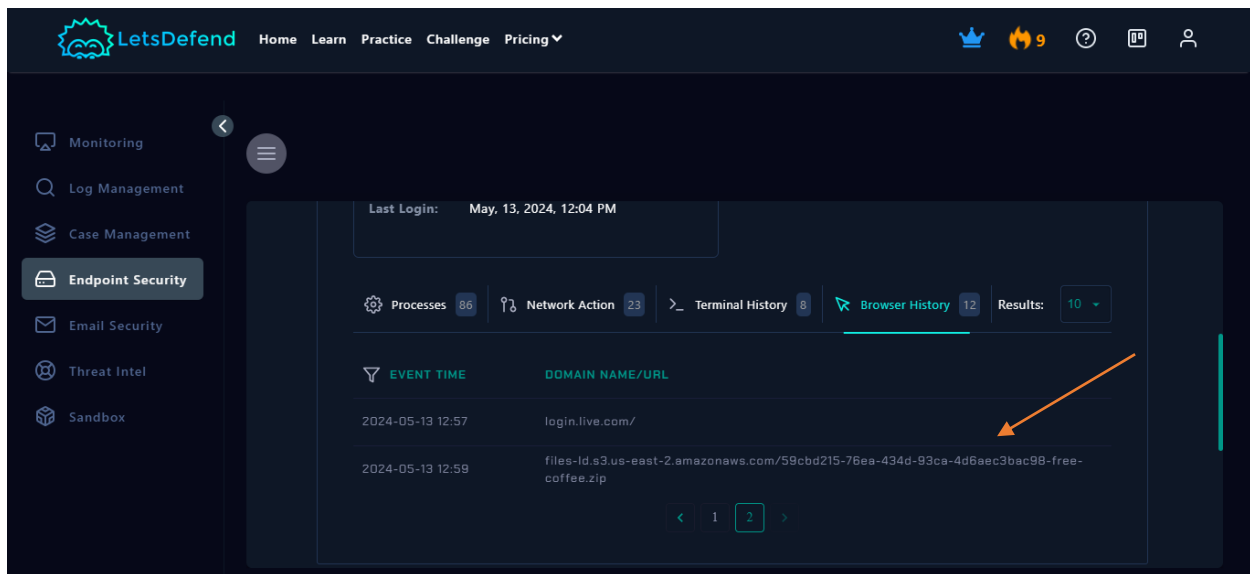
These commands are commonly used for system diagnostics, information gathering, and troubleshooting. They offer valuable insights into system configuration, network settings, user accounts, and running processes (see attached photo).



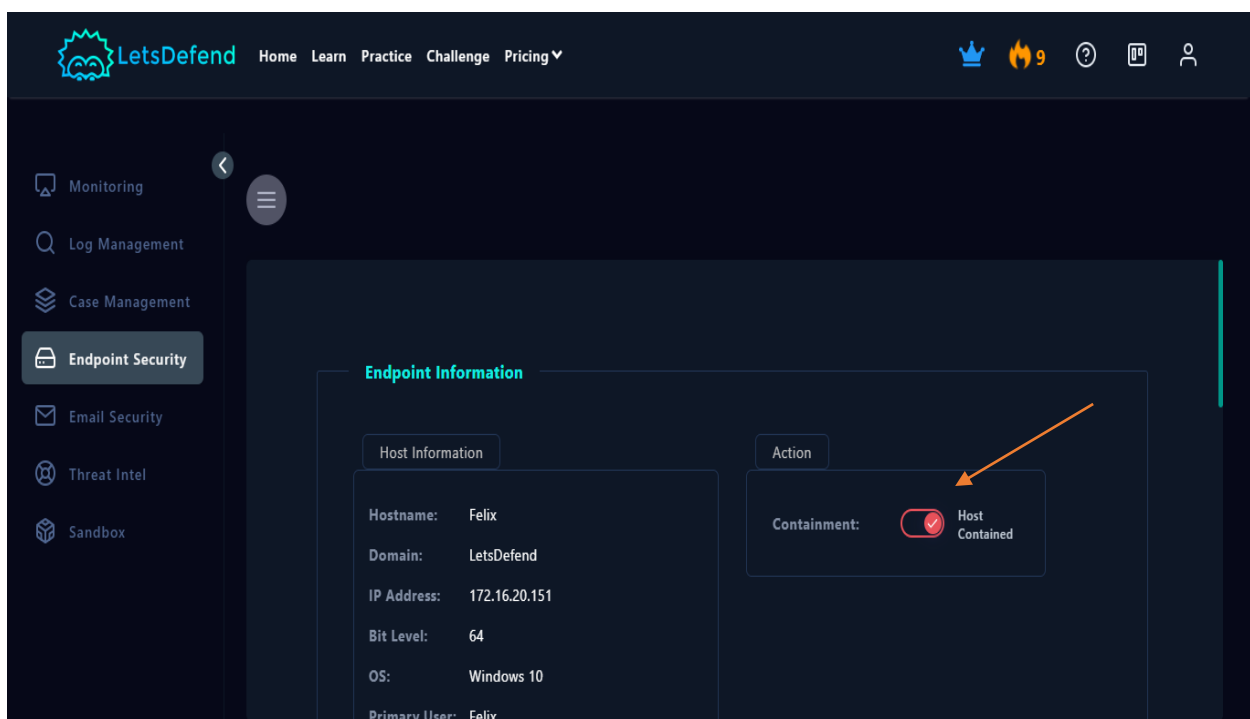
### 3. Browser History Analysis

- The browser history indicates that the user Felix downloaded a file at 12:59 on May 13, 2024 (see attached photo).

This sequence of actions—downloading a file, executing diagnostic commands, and running `coffee.exe`—suggests a deliberate exploration of the system's state, potentially for unauthorized purposes. The combination of these actions warrants a closer examination to assess any security risks and ensure the integrity of our systems.



SO, we must contain the device



## Conclusion

On May 13, 2024, at 09:22 AM, a security event (Event ID: 257) was triggered by SOC251, indicating a Phishing Alert (Deceptive Mail Detection). The incident involved an external attack from source IP address 103.80.134.63 targeting the internal network at IP address 172.16.20.151.

In response, a comprehensive threat intelligence search was conducted using VirusTotal, MXToolbox, AbuseIPDB, and LetsDefend. These searches yielded no findings, suggesting that the IPs and associated entities did not have prior malicious indicators in the public threat databases consulted.

Further analysis involved an email review from the Email Security section, identifying a suspicious attachment named `free-coffee.zip`. Upon scanning the file with VirusTotal, several security vendors flagged it as malicious. The analysis revealed connections to known malicious entities and potentially harmful behaviors.

Additionally, Endpoint Security monitoring detected the execution of a process named `coffee.exe`. The terminal command history showed a series of commands executed in the Command Prompt shortly after the file download, indicating potential system reconnaissance and information gathering activities. The commands collected system information, network configurations, and user account details.

The investigation revealed that these actions, particularly the sequence of downloading a file, executing diagnostic commands, and running `coffee.exe`, likely constitute a deliberate attempt to explore the system's state, possibly for unauthorized purposes.