Official incident report

Event ID:120

Rule Name: SOC170 - Passwd Found in Requested URL - Possible LFI Attack

Made By: Asmaa Abdelrahman

LinkedIn: https://www.linkedin.com/in/asmaa-abdelrahman-93ab46230/

Github link: https://github.com/Asma-Abdelrahman

Table of contents

By: Asmaa Abdelrahman

Event Details

Event ID: 120

Event Date and Time: Mar, 01, 2022, 10:10 AM

Rule: SOC170 - Passwd Found in Requested URL - Possible LFI Attack

Level: Security Analyst

Hostname: WebServer1006

HTTP Request Method: GET

Requested URL: https://172.16.17.13/?file=../../../../etc/passwd

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

Alert Trigger Reason: URL Contains passwd

Device Action: Allowed

Network Information Details

Destination Address:172.16.17.13 internal

Source Address:106.55.45.162 external

External / Internal Attack: Based on the event details, the attack appears to be **external**.

By: Asmaa Abdelrahman

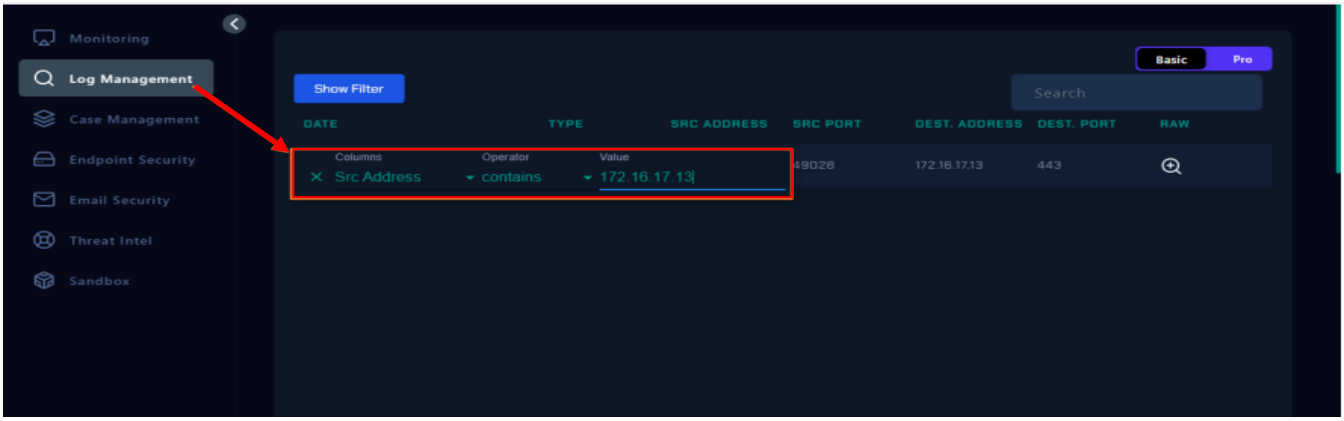
Analysis:

First, I started reading the information very carefully.

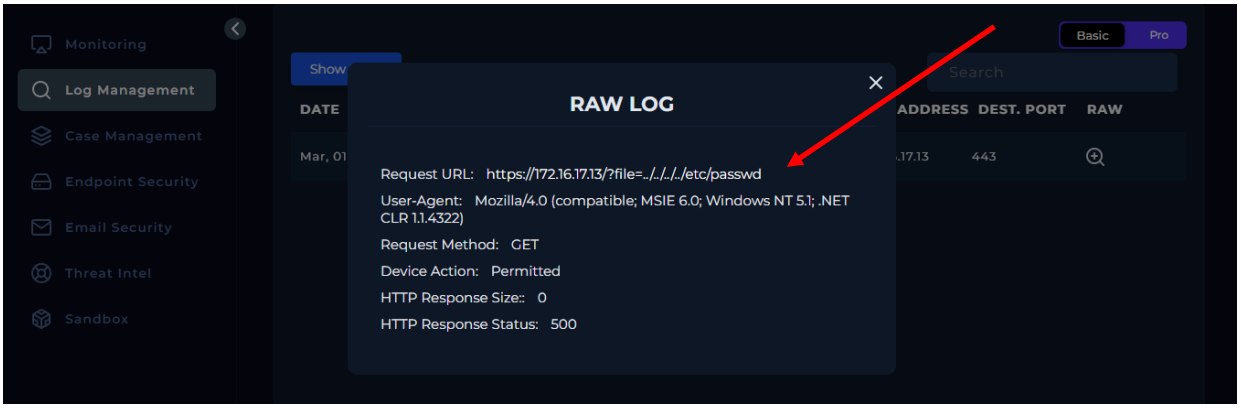
Log Management

We'll proceed by entering the source IP address and reviewing the results.

Please refer to the attached image for further details regarding the attack.



Only 1 Log record for the source IP with the same date of the attack. Please refer to the attached image for further details regarding the attack.



By: Asmaa Abdelrahman

Log Breakdown

1. Request URL:

https://172.16.17.13/?file=../../../../etc/passwd

- **Description**: The attacker is attempting to perform a Local File Inclusion (LFI) attack by trying to access the file /etc/passwd on the web server. This file typically contains user account information on Unix/Linux systems.

2. User-Agent:

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)

- **Description:** This indicates the web client making the request. The User-Agent string is meant to mimic an older version of Internet Explorer on a Windows XP system, but this can be easily spoofed.

3. Request Method:

GET

- **Description:** This is a standard HTTP method used to request data from the server. In this case, the GET method is used to try to retrieve the contents of the file.

4. Device Action:

Permitted

- **Description:** The device (likely a web server or firewall) allowed the request to proceed. This suggests that there was no blocking rule or mechanism in place to prevent this specific request.

5. HTTP Response Size:

0

- **Description:** This indicates that the server did not return any content in the response. This could be due to an error or because the requested file does not exist or could not be read.

By: Asmaa Abdelrahman

6. HTTP Response Status:

500

- **Description:** This is an HTTP status code indicating a "500 Internal Server Error." This status code is returned when the server encounters an unexpected condition that prevents it from fulfilling the request. In this context, it means that the server encountered an error when trying to process the request.

Summary of the Incident

1. Attack Attempt:

- The attacker made a GET request to the web server at 172.16.17.13 trying to access the file /etc/passwd using a URL parameter. This suggests an attempt to exploit a Local File Inclusion (LFI) vulnerability in the web application.

2. Server Response:

- The server attempted to process the request but encountered an error, resulting in an HTTP 500 status code. This could mean that either the file /etc/passwd does not exist or the server's attempt to include or read the file resulted in a server-side error.

3. Security Implications:

- Although the request was permitted and processed (the device action was allowed), the actual result was an internal server error, which may indicate that the server has some form of protection or configuration issue that prevented the inclusion of the file.

4. Next Steps:

- Investigate the Error: Review server logs to understand why the 500 error occurred and if it's related to the LFI attempt.
- Check Security Configuration: Ensure that proper security measures are in place to prevent LFI attacks, such as input validation and restrictions on file paths.
- Monitor for Further Attempts: Keep an eye on similar requests to identify if this is part of a larger attack pattern.

In summary, while the request was allowed by the server, the attempt to exploit a vulnerability resulted in an error. It's crucial to investigate further to ensure that the server is protected against such attacks and to understand any potential security gaps.

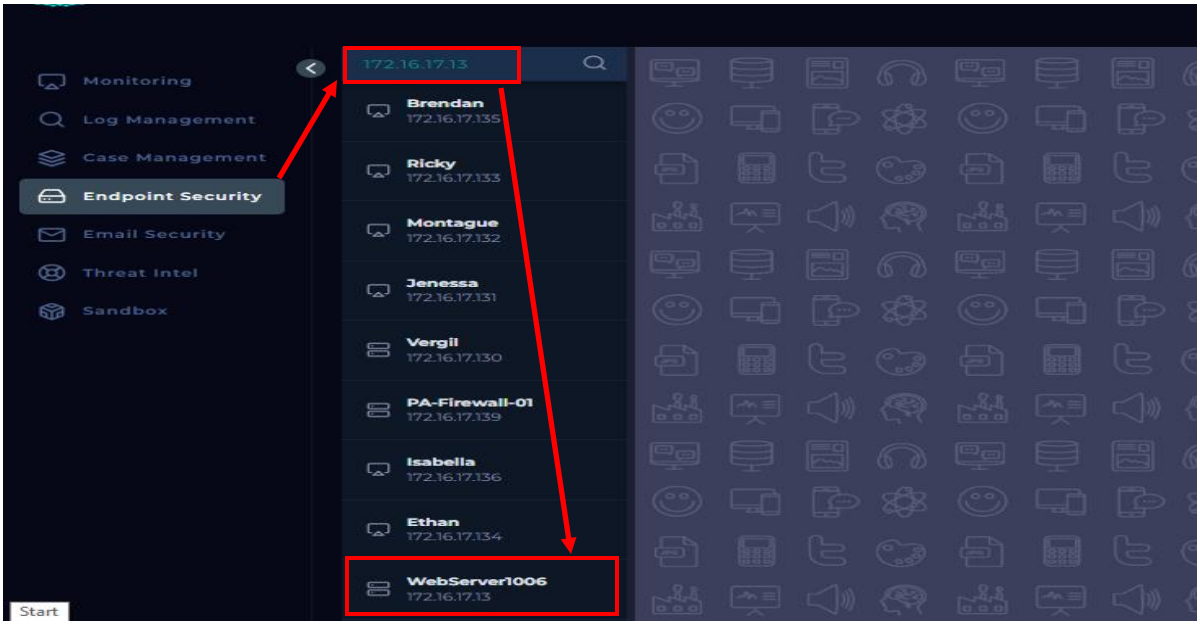
The attack was not successful in retrieving the /etc/passwd file or any other content.

By: Asmaa Abdelrahman

Endpoint Security

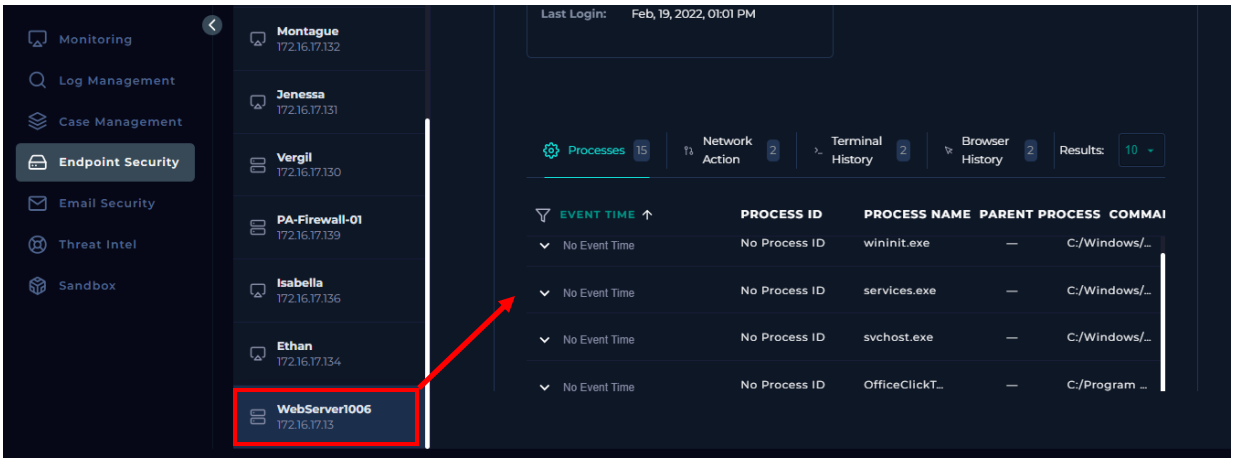
We will enter either the source IP to check the activity that happened on the server.

Refer to the attached image for further details.



Incident Overview: During our routine endpoint security checks, no significant issues were found on the alert date. However, network activity logs revealed connections between our server and two potentially

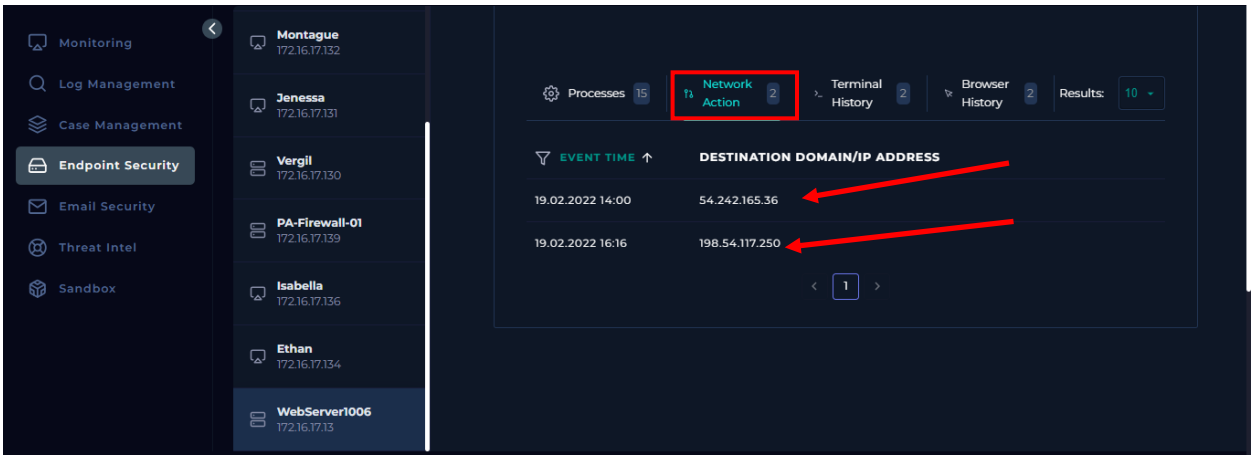
malicious IP addresses. Our firewall successfully detected and addressed these connections.



By: Asmaa Abdelrahman

Detailed Analysis of Network Actions section:

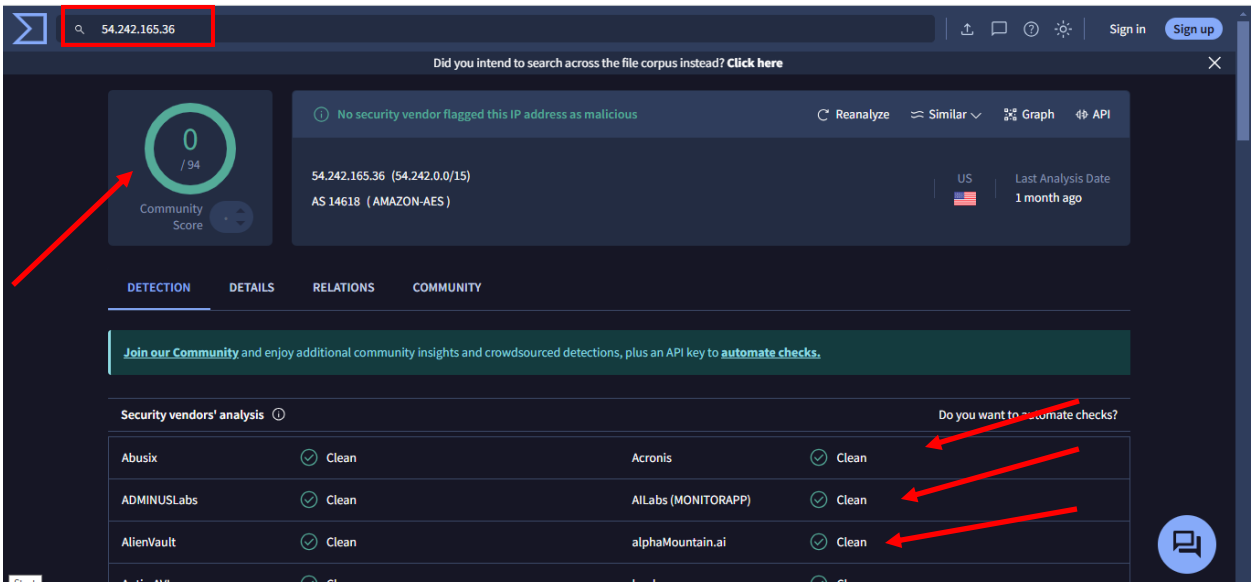
1. Record 1:



1-Date and Time: February 19,02. 2022, 14:00

- IP Address: 54.242.165.36
- Initial Assessment: No issues detected
- Additional Checks: Refer to the attached photo for details and analysis

I will check if this is malicious or not.



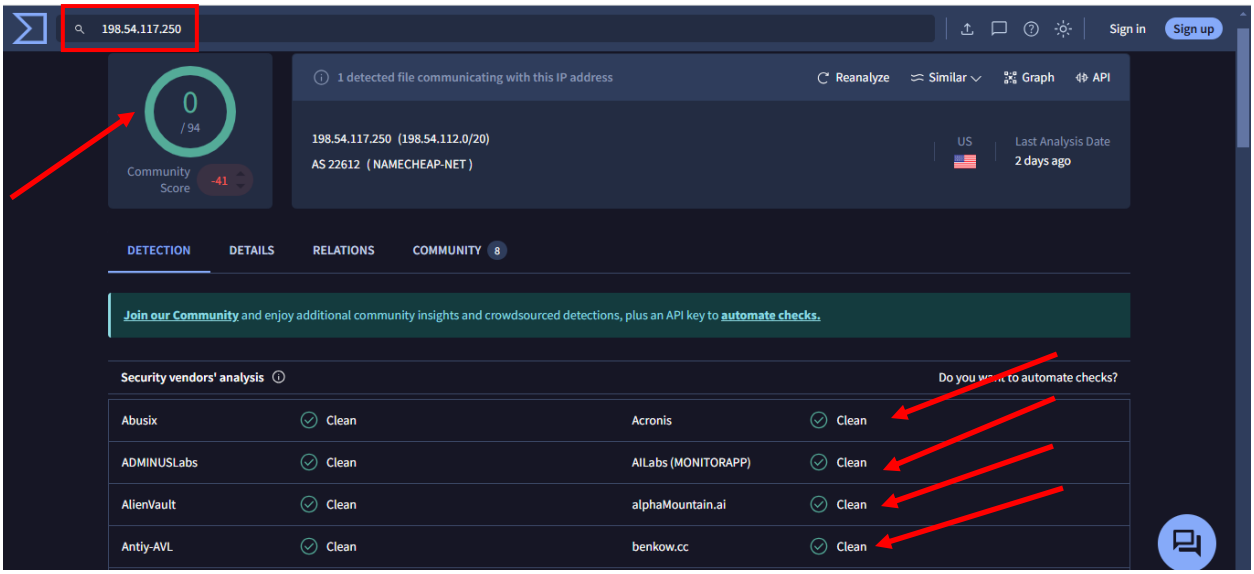
VirusTotal Analysis:

The results from VirusTotal for this IP address indicated no significant threats. For more details, please refer to the provided link.

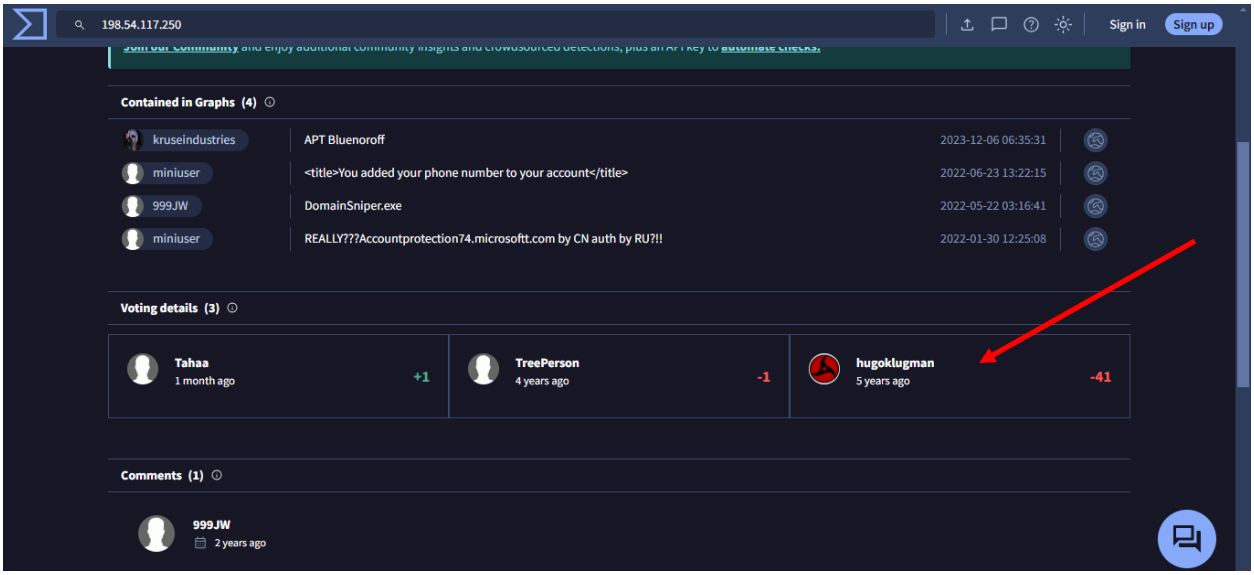
By: Asmaa Abdelrahman

2. Record 2:

- Date and Time: February 19, 2022, 16:16
- IP Address: 198.54.117.250
- Initial Assessment: Analysis appears clear in the detection section.



Additional Comments: Notably, there are over 40 comments in the VirusTotal community section regarding this IP address. Please refer to the attached photo for detailed analysis and the provided link for community feedback.



By: Asmaa Abdelrahman

Detection:

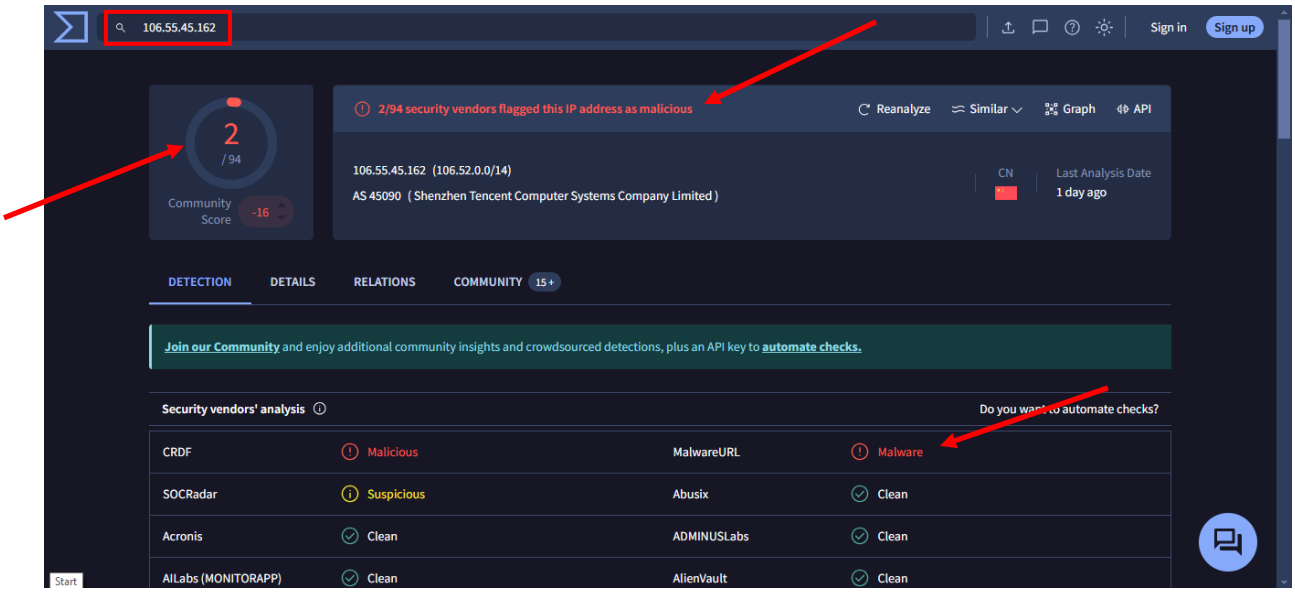
Threat Intelligence Results

Analysis of the source IP address on VirusTotal

Objective: Evaluate the source IP address using VirusTotal and review the results in different sections.

1. Detection Section

- Status: The Detection section shows detections. This indicates that no security vendor has flagged the IP address as malicious at this time.

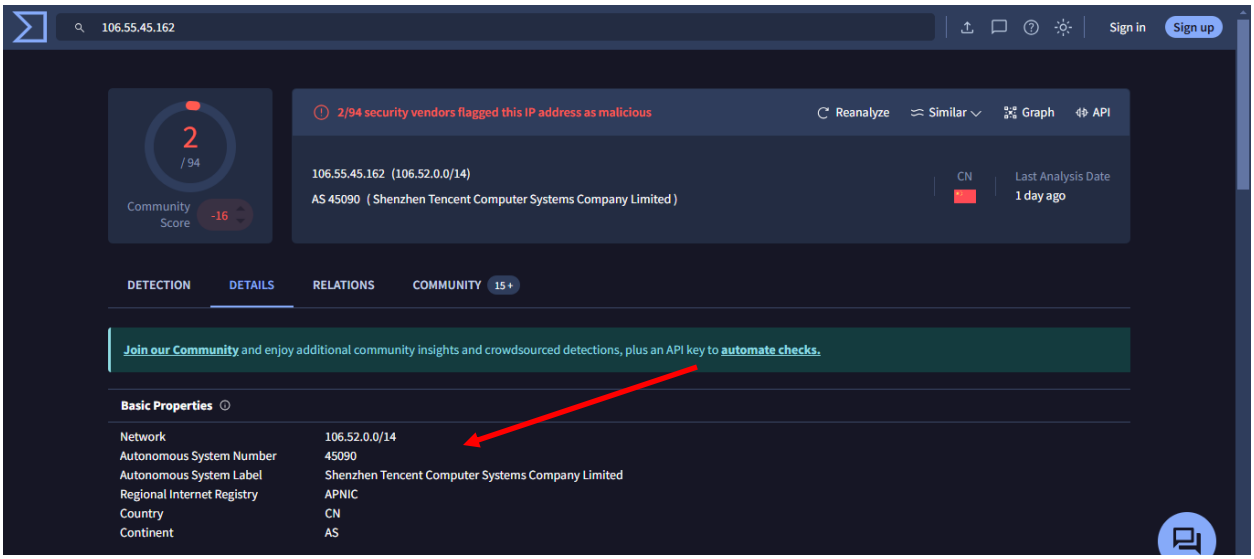


- Reference: View Detection Section

2. Details Section

- Status: There is a slight possibility that it is malicious.
  provides standard information about the IP address.

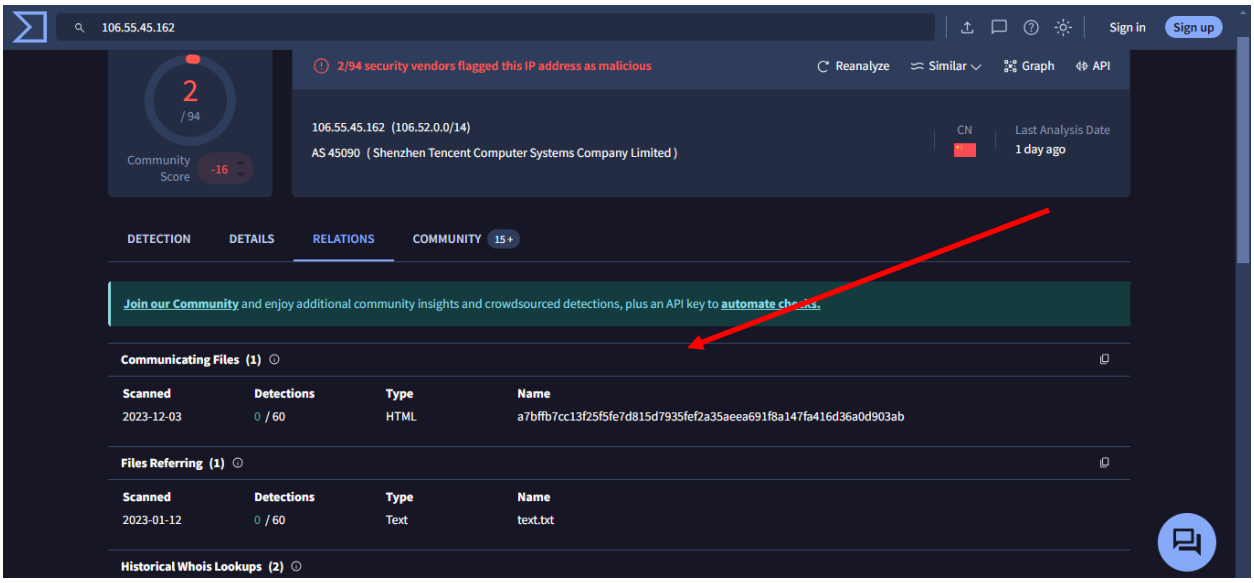
By: Asmaa Abdelrahman



Reference: View Details Section

3. Relationship Section

Status: The relationship section indicates the presence of harm and connections with other known malicious entities or infrastructure.

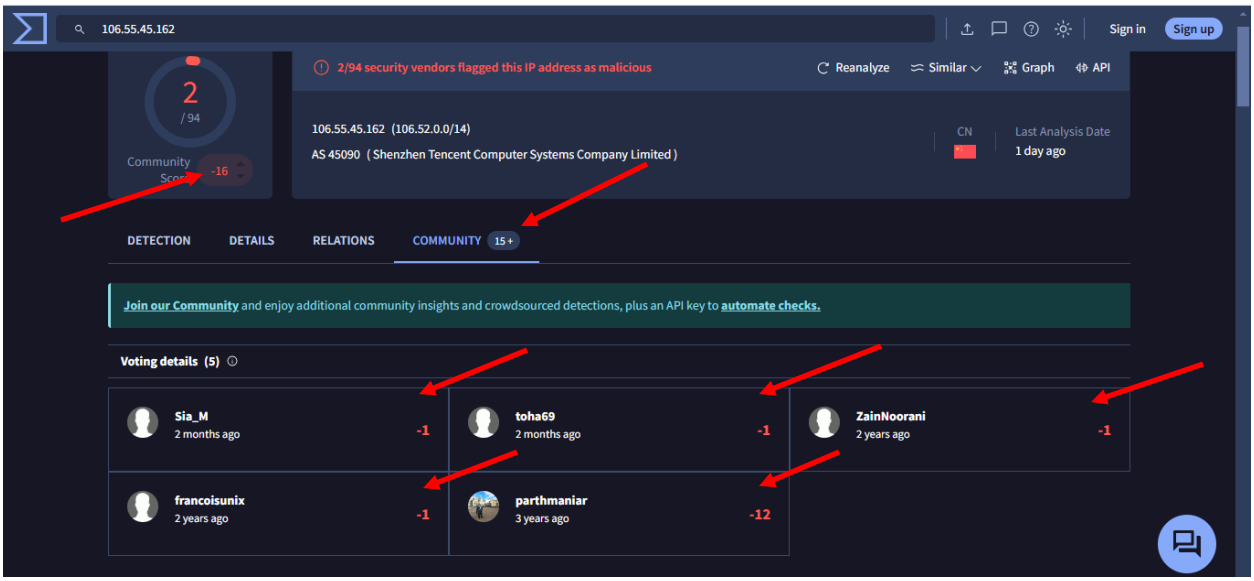


Reference: View Relations Section

By: Asmaa Abdelrahman

4. Community Section

- **Status:** The Community section shows substantial activity, with over 15 comments concerning this IP address. This indicates a significant level of interest or concern from the security community.



- Reference: View Community Section

By: Asmaa Abdelrahman

Conclusion

In conclusion, our investigation into the incident has revealed several critical insights that provide a comprehensive understanding of the attack and its context.

Incident Summary: On March 1, 2022, at 10:10 AM, an attempt was made to launch a Local File Inclusion (LFI) attack against the WebServer1006 web server with the URL https://172.16.17.13/?file=../../../etc/passwd. The HTTP request was intended to access the /etc/passwd file, a critical system file that could potentially reveal sensitive user information. Despite the attempt, the server responded with a 500 Internal Server Error, indicating that the file was inaccessible or an error occurred during processing.

Key Findings:

1. Security Analysis: The server's permission of the request indicates a potential gap in security configurations that may have facilitated this attack attempt. However, the failure to retrieve the file successfully and the server error provide some level of protection against outright exploitation.

2. Network Activity: Log records and endpoint security scans did not show any significant issues or successful threats from the external IP addresses involved. VirusTotal analysis of these IP addresses returned minor concerns, which could be attributed to minor damage.

3. Infrastructure and Commands: Docker command analysis revealed routine maintenance activities, which appear to be unrelated to the incident. The commands executed were standard for building and deploying Docker containers, indicating a direct link to the attack.

Action Items:

1. Investigate Server Configuration: It is imperative to conduct additional review of the server configuration and logs to understand the cause of the internal server error and ensure that appropriate defenses against LFI attacks are in place.

2. Strengthen Security Measures: Implement strong input validation, enforce strict file path restrictions, and review existing security policies to mitigate future vulnerabilities.

3. Monitor Network Traffic: Continue to monitor network traffic and logs for any signs of recurring or related malicious activity. Engage with the security community to stay abreast of potential threats and gather additional context from community feedback on VirusTotal.

Final assessment: While the zero-day attack attempt did not compromise sensitive data, the incident highlights the need for continued vigilance and improvement of our security posture. By addressing identified vulnerabilities and strengthening our preventative measures, we can strengthen our defenses against future threats and more effectively protect our critical assets.

By: Asmaa Abdelrahman