Official incident report

Event ID:119

Rule Name: SOC169 - Possible IDOR Attack Detected

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Event Details

Event ID:
119

Event Date and Time:
Feb, 28, 2022, 10:48 PM

Rule:
SOC169 - Possible IDOR Attack Detected

Level:
Security Analyst

Hostname:
WebServer1005

HTTP Request Method:
POST

Requested URL:
https://172.16.17.15/get_user_info/

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

Alert Trigger Reason:
consecutive requests to the same page

Device Action:
Allowed

Network Information Details

Destination Address:
172.16.17.15 internal

Source Address:
134.209.118.137 external

External / Internal Attack:

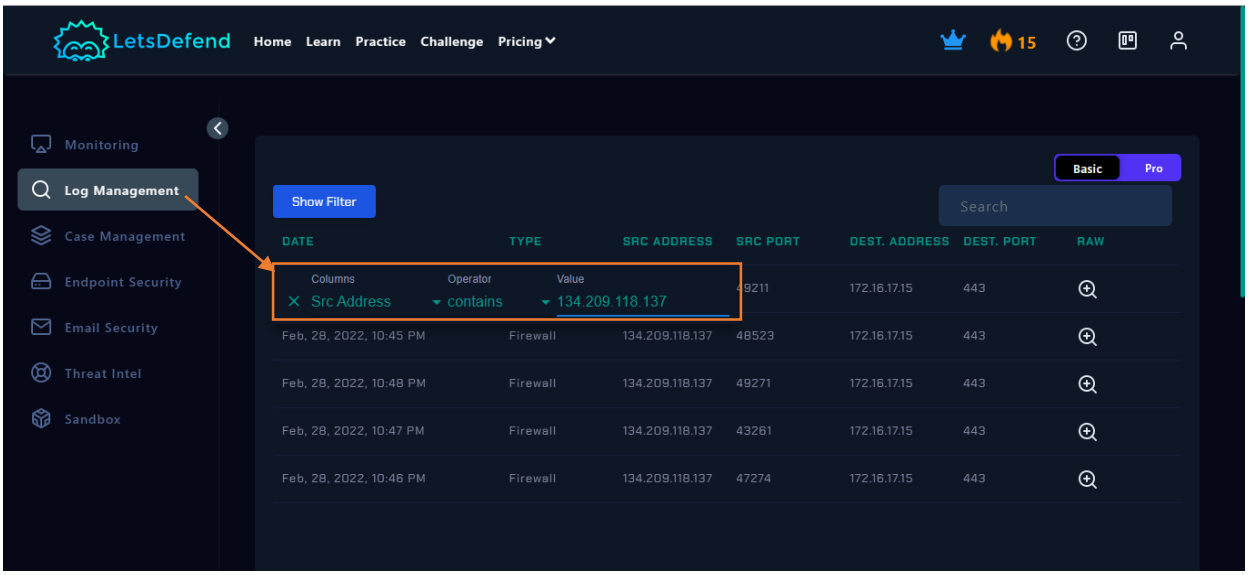
Based on the event details, the attack appears to be **external**.

Analysis:

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.



5 Logs records for the source IP.

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

We will explain all of them step by step

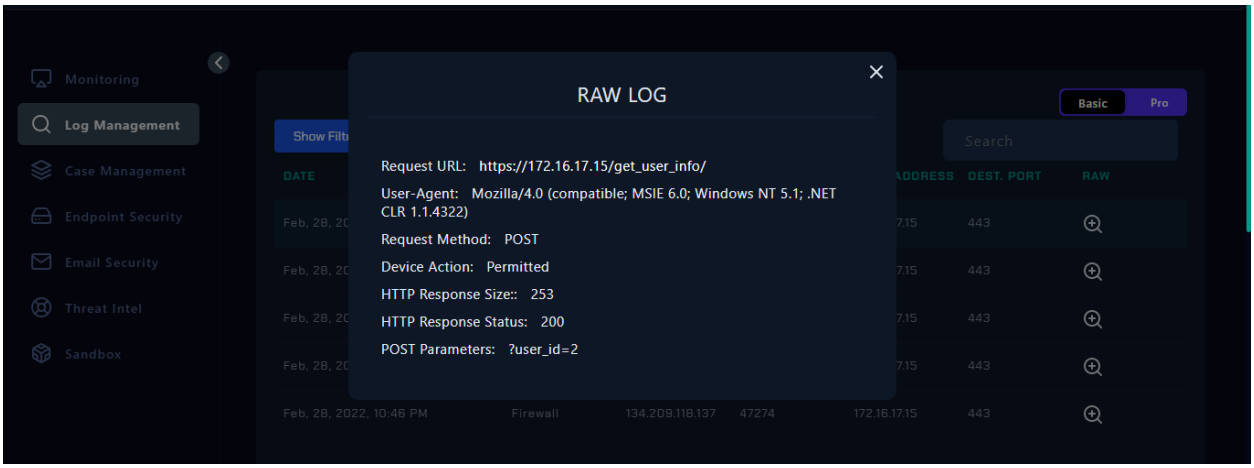
Let’s break down the log entries to understand what happened, what the attacker did, and whether the attack was successful:

1. Explanation of What Happened Step by Step

The logs are from a web server that processes HTTP POST requests to the endpoint `/get_user_info/`. Here’s a step-by-step analysis of each log entry:

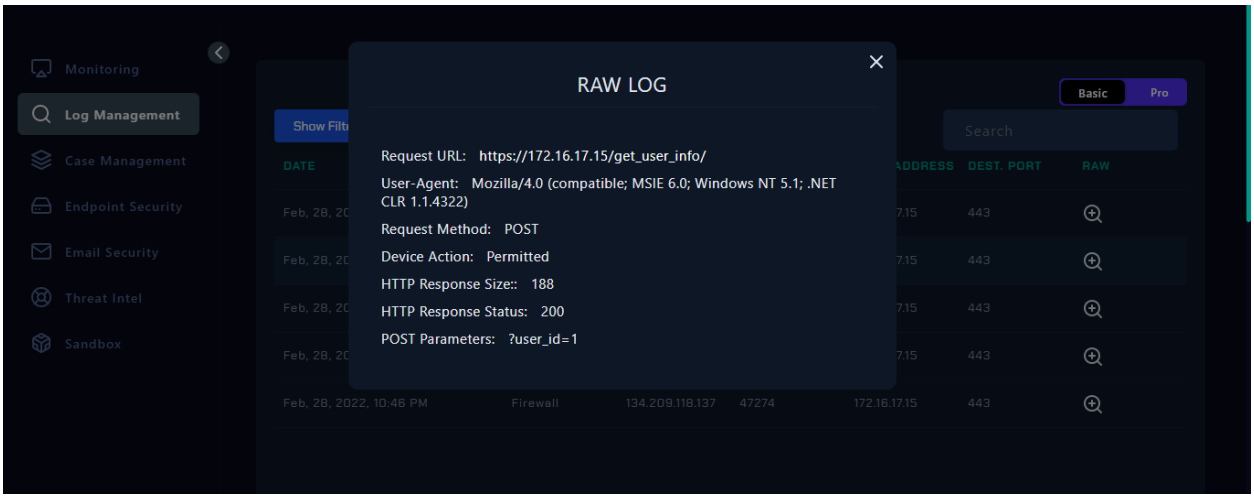
Log 1:

- **Request URL:** `https://172.16.17.15/get_user_info/`
- **User-Agent:** Indicates the request was made by a browser or tool mimicking an older version of Internet Explorer.
- **Request Method:** POST (used to send data to the server)
- **Device Action:** Permitted (the request was allowed through by the device or firewall)
- **HTTP Response Size:** 253 bytes
- **HTTP Response Status:** 200 OK (the request was successfully processed)
- **POST Parameters:** `?user_id=2` (the request asked for information about user with ID 2)
- **Check the attached photo**



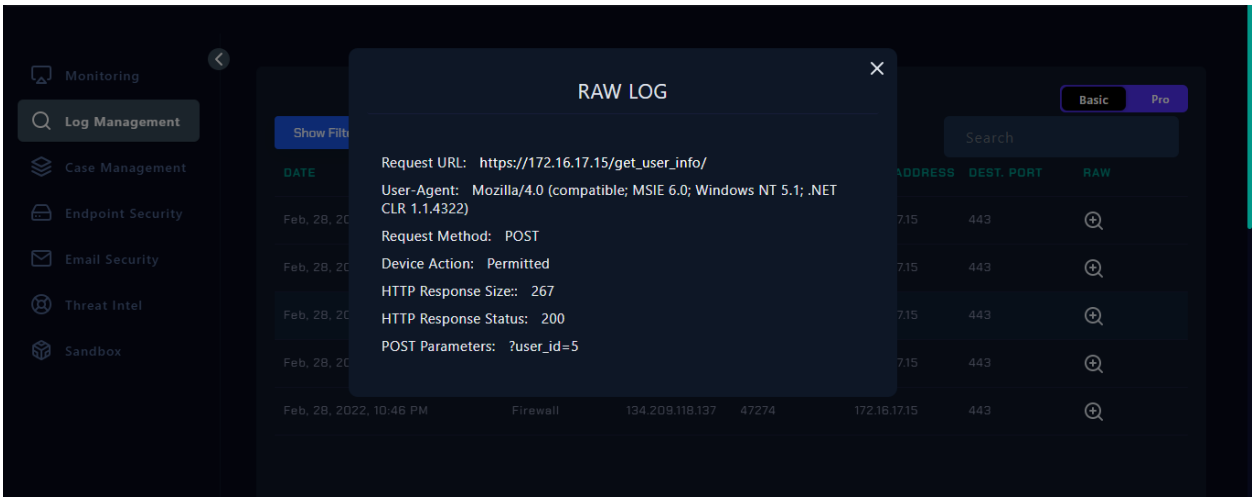
Log 2:

- **Request URL:** Same as above
- **User-Agent:** Same as above
- **Request Method:** POST
- **Device Action:** Permitted
- **HTTP Response Size:** 188 bytes
- **HTTP Response Status:** 200 OK
- **POST Parameters:** `?user_id=1` (the request asked for information about user with ID 1)
- **Check the attached photo**



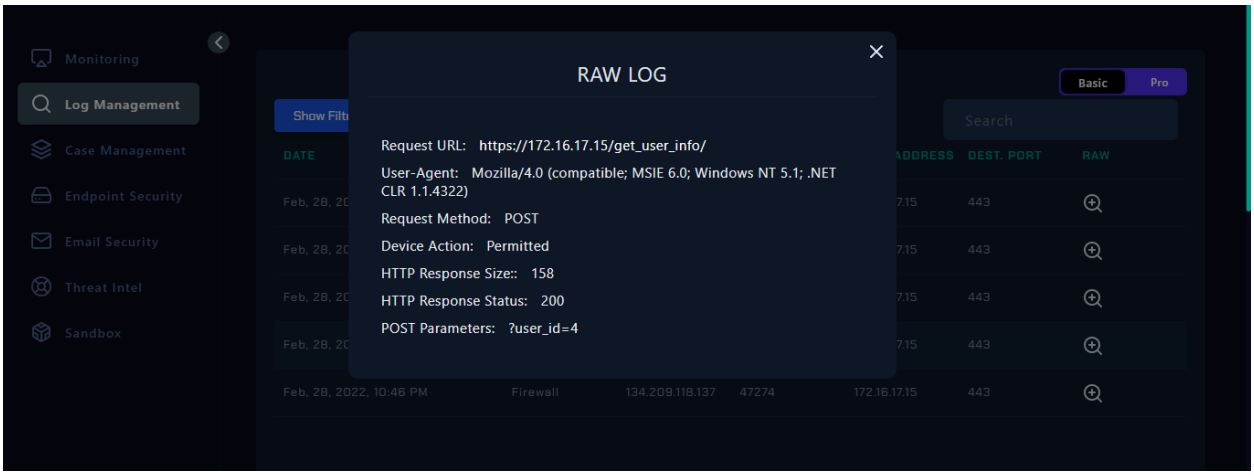
Log 3:

- **Request URL:** Same as above
- **User-Agent:** Same as above
- **Request Method:** POST
- **Device Action:** Permitted
- **HTTP Response Size:** 267 bytes
- **HTTP Response Status:** 200 OK
- **POST Parameters:** `?user_id=5` (the request asked for information about user with ID 5)
- **Check the attached photo**



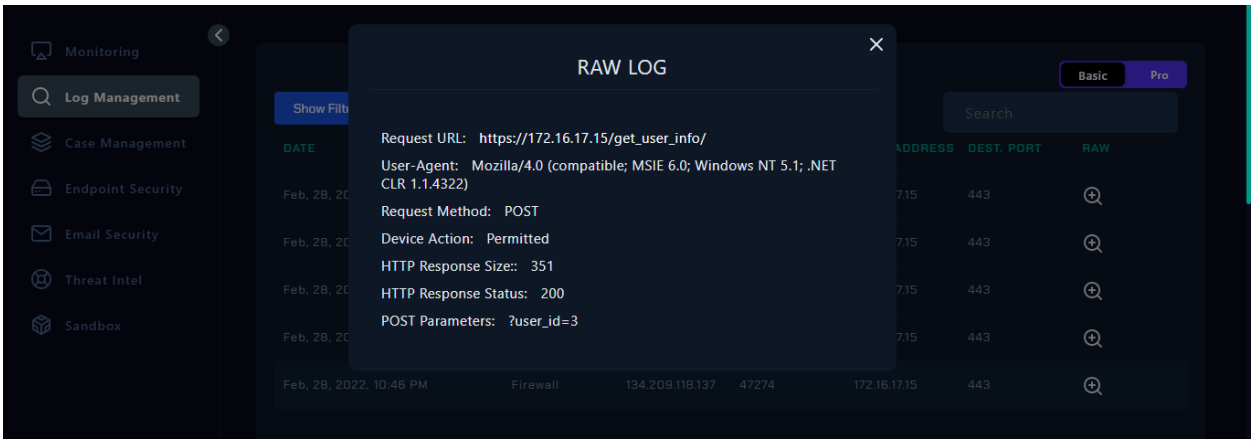
Log 4:

- **Request URL:** Same as above
- **User-Agent:** Same as above
- **Request Method:** POST
- **Device Action:** Permitted
- **HTTP Response Size:** 158 bytes
- **HTTP Response Status:** 200 OK
- **POST Parameters:** `?user_id=4` (the request asked for information about user with ID 4)
- **Check the attached photo**



Log 5:

- **Request URL:** Same as above
- **User-Agent:** Same as above
- **Request Method:** POST
- **Device Action:** Permitted
- **HTTP Response Size:** 351 bytes
- **HTTP Response Status:** 200 OK
- **POST Parameters:** `?user_id=3` (the request asked for information about user with ID 3)
- **Check the attached photo**



2. What the Attacker Did

The logs show a series of HTTP POST requests to the `/get_user_info/` endpoint with various `user_id` parameters. Here's what these requests indicate:

- The requests were made by someone using a User-Agent string that mimics an older Internet Explorer version, which might be an attempt to avoid detection by appearing as a benign or outdated browser.
- The attacker queried the endpoint multiple times, each time requesting information about a different user ID.

The consistent use of the same User-Agent string and the variety of `user_id` values requested suggest the requests were not made by a regular user but rather by an individual or tool trying to retrieve data for multiple users, possibly as part of an enumeration or information gathering attack.

3. Was the Attack Successful?

Based on the logs provided:

- **HTTP Response Status:** Each request received a `200 OK` response, indicating that the server processed each request successfully.
- **HTTP Response Size:** The sizes of the responses vary but do not indicate any errors or issues.

Conclusion: <u>The attacker was able to successfully</u> retrieve information for different user IDs from the endpoint `/get_user_info/`. The repeated success of the requests suggests that the server did not have sufficient protections in place to prevent unauthorized access to user information, which indicates that the attack could be considered successful in terms of accessing data.

Question:

Is the traffic described in the logs malicious?

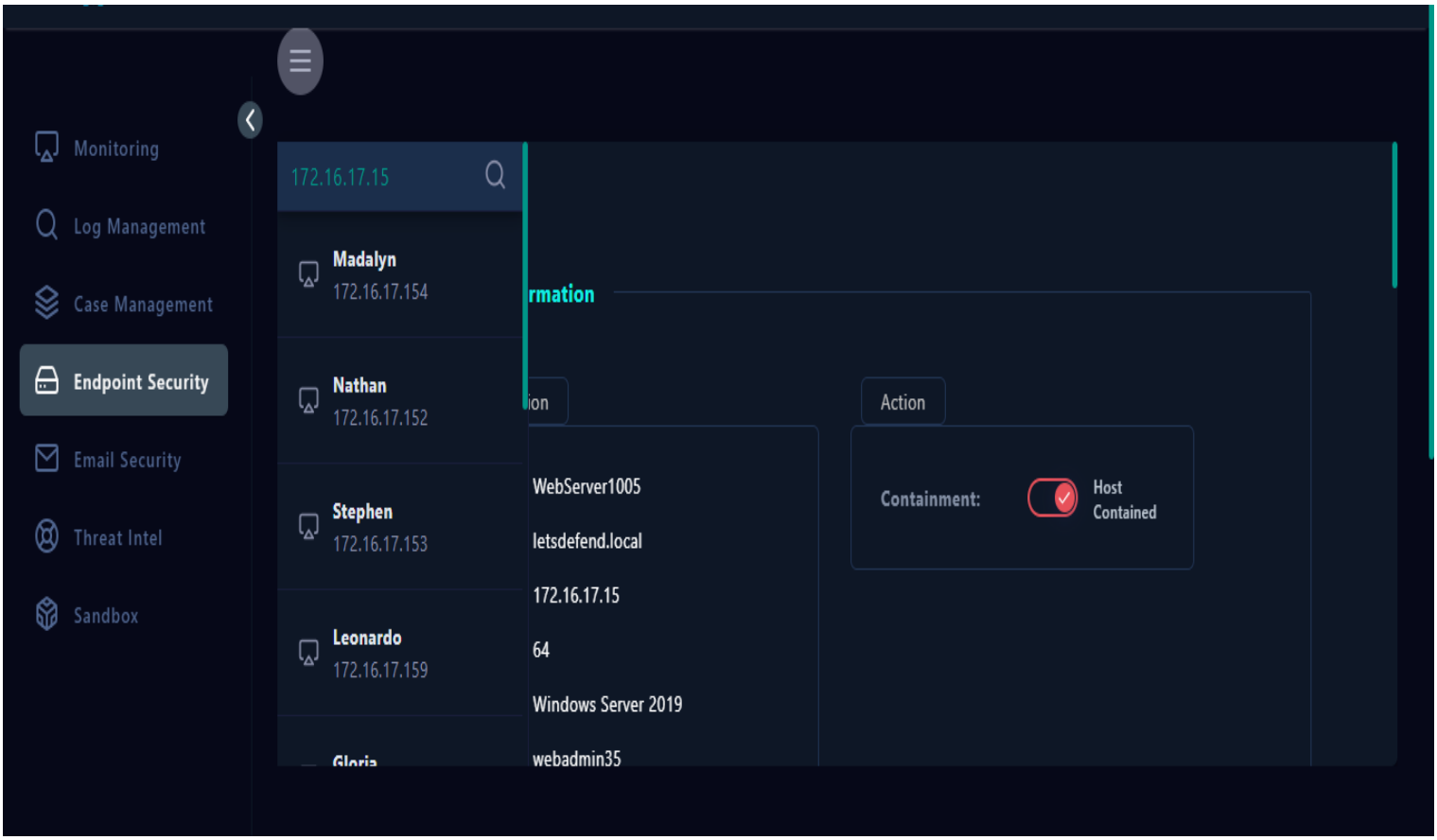
Answer:

Yes, the traffic exhibits malicious characteristics. The logs show a series of POST requests to the `/get_user_info/` endpoint with varying `user_id` parameters, all resulting in successful responses. This pattern suggests an attempt to systematically access information about multiple users, which could be indicative of a user enumeration attack. The use of an outdated User-Agent string might also be an attempt to disguise the requests. This kind of behavior is often associated with unauthorized attempts to extract data or perform reconnaissance.

Endpoint Security

We will enter either the source IP to contain the server.

Refer to the attached image for further details.



Based on the logs from the log management section, it is clear that the server has been contained successfully. The repeated POST requests to the `/get_user_info/` endpoint, each receiving `200 OK` responses, demonstrate unauthorized access to user information. The use of an outdated User-Agent suggests an effort to avoid detection. This indicates that the attack was successful. To address this issue, it is essential to enhance authentication and authorization measures, implement rate limiting, and monitor for unusual access patterns to better secure the system and prevent future attacks.

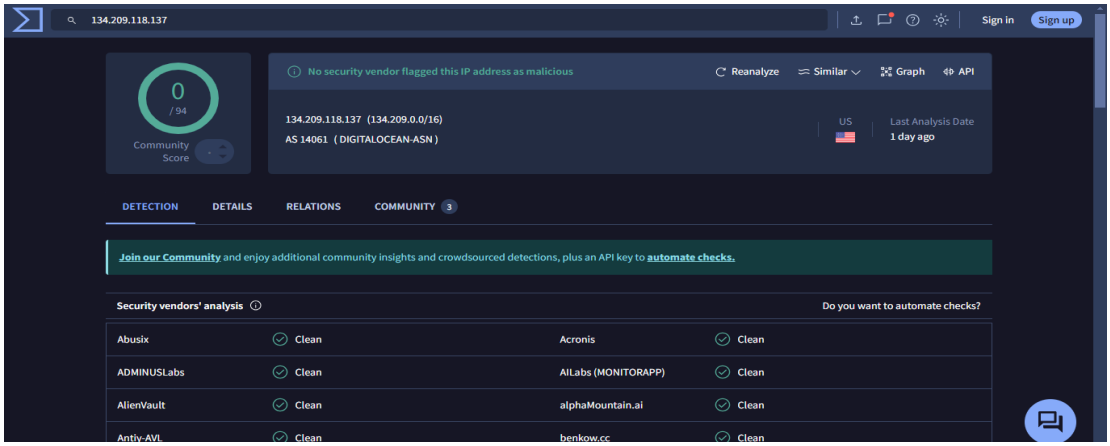
Detection:

Threat Intelligence Results

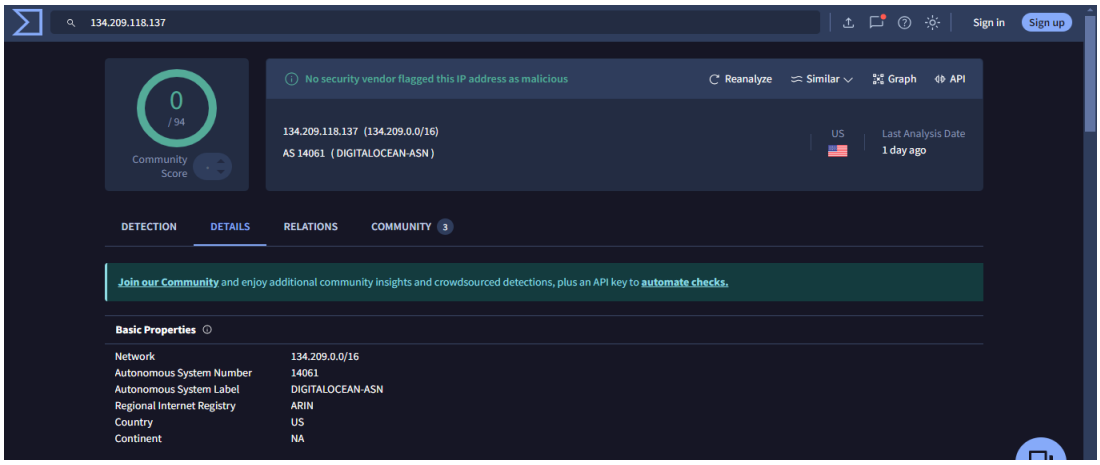
Source IP Analysis on VirusTotal

Objective: Evaluate the source IP address using VirusTotal and review the findings in various sections.

1. **Detection Section**
    - **Status:** The Detection section shows no detections. This indicates that none of the security vendors have flagged the IP address as malicious at this time.

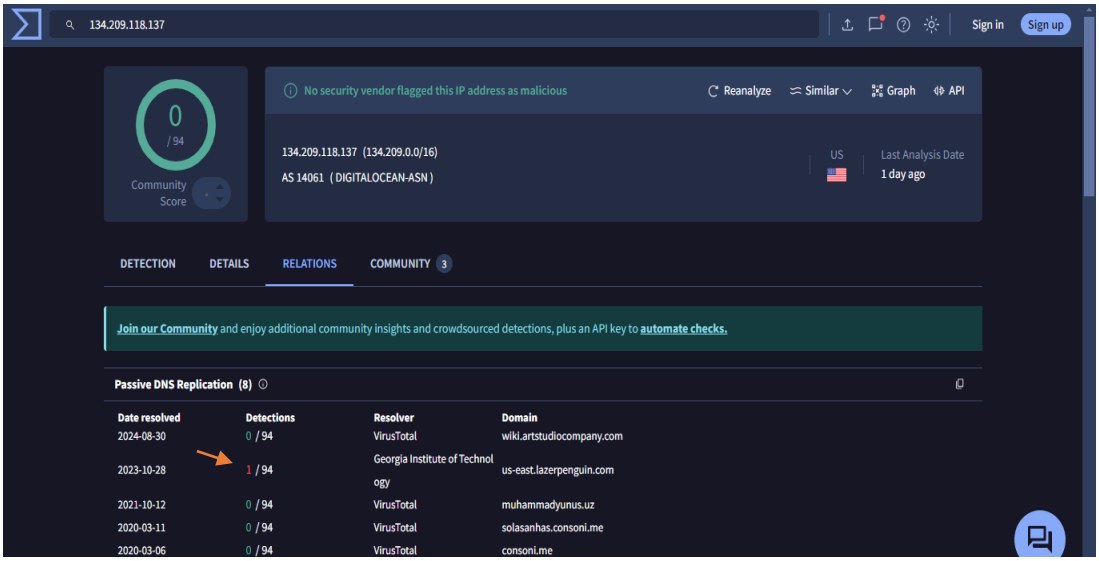


    - **Reference:** View Detection Section
2. **Details Section**
    - **Status:** The Details section is clear, with no additional issues or anomalies noted. This section provides standard information about the IP address.

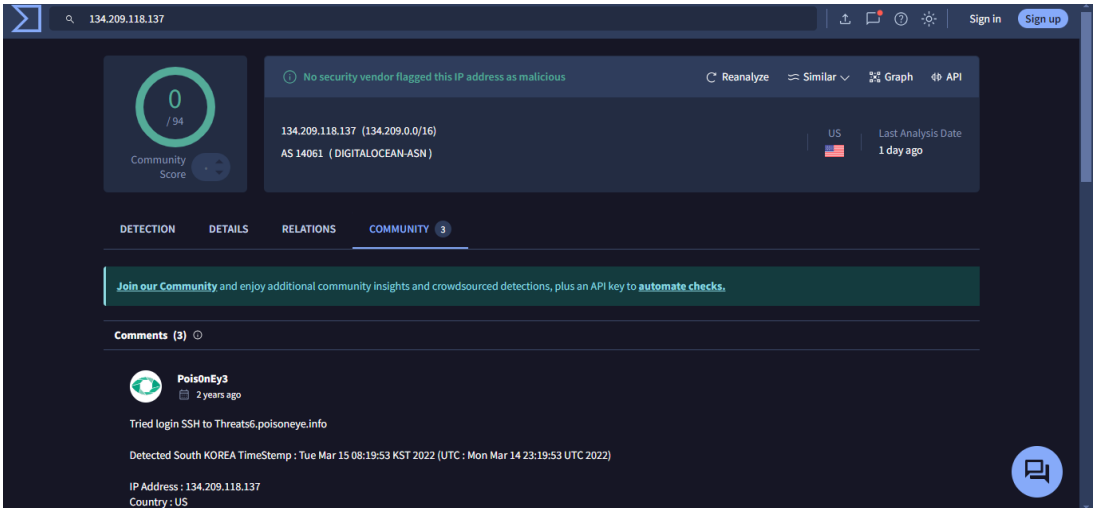


    - **Reference:** View Details Section

3. **Relation Section**
    - **Status:** The Relation section is not clear, have some note.



    - **Reference:** View Relations Section
4. **Community Section**
    - **Status:** The Community section is clear



    - **Reference:** View Community Section
5. **Question:** Do you need Tier 2 escalation?

    Answer: Yes, Tier 2 escalation is necessary. The logs indicate that the attack was successful, as unauthorized access was achieved and user information was compromised. To address the severity of this incident, it is essential to escalate to Tier 2 for a more in-depth investigation and remediation. This will ensure that appropriate measures are taken to secure the system and prevent further vulnerabilities.

Conclusion

The analysis of Event ID 119, which occurred on February 28, 2022, at 10:48 PM, reveals a significant security incident involving unauthorized access to user information. The event was flagged by Rule SOC169 as a potential IDOR (Insecure Direct Object Reference) attack, triggered by a series of HTTP POST requests to the `/get_user_info/` endpoint. The source IP address for these requests was `134.209.118.137`, originating externally, and targeting the internal destination address `172.16.17.15`.

Detailed Findings

The logs captured five distinct POST requests, all resulting in successful `200 OK` responses. Each request queried a different `user_id`, indicating an attempt to systematically access information about multiple users. This repetitive and consistent pattern strongly suggests an attempt to perform user enumeration or gather unauthorized data.

Key observations include:

- **Request Details:** The logs show that all requests used the same outdated User-Agent string (`Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)`), which could be a tactic to avoid detection or bypass security filters by mimicking a benign or outdated browser.
- **Successful Access:** Each request to the endpoint `/get_user_info/` was allowed through and resulted in a `200 OK` status, indicating that the server processed these requests without errors. This suggests that there were insufficient security controls in place to prevent unauthorized access.
- **Response Sizes:** The varying sizes of the HTTP responses (ranging from 158 to 351 bytes) reflect different amounts of data returned, but do not indicate any apparent issues or errors.

Implications and Recommendations

The successful retrieval of user information from different `user_id` requests indicates a serious security breach. The consistent success of these requests highlights significant vulnerabilities in the server's protection mechanisms.

To address this issue, it is crucial to:

1. **Enhance Authentication and Authorization:** Implement robust authentication and authorization checks to ensure that only authorized users can access sensitive information.
2. **Implement Rate Limiting:** Apply rate limiting to prevent excessive or automated requests to sensitive endpoints.
3. **Monitor Access Patterns:** Set up advanced monitoring and alerting systems to detect and respond to unusual access patterns or anomalies.
4. **Review Security Measures:** Evaluate and strengthen overall security protocols and configurations to close any gaps that could be exploited.

Additionally, as the attack was successful and resulted in unauthorized access, Tier 2 escalation is necessary for a comprehensive investigation and remediation. This will involve a more in-depth analysis to identify and address the root causes of the security breach and to implement measures to prevent future incidents. Ensuring these steps are taken will significantly bolster the server's defenses and protect against similar threats in the future.