Official incident report

Event ID:116

Rule Name: SOC166 - Javascript Code Detected in Requested URL

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:
116

Event Date and Time:
Feb, 26, 2022, 06:56 PM

Rule:
SOC166 - Javascript Code Detected in Requested URL

Level:
Security Analyst

Hostname:
WebServer1002

HTTP Request Method:
GET

Requested URL:
https://172.16.17.17/search/?q=<$script>javascript:$alert(1)<$/script>

User-Agent:
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1

Alert Trigger Reason:
Javascript code detected in URL

Device Action:
Allowed

Network Information Details

Destination Address:
172.16.17.17 internal

Source Address:
112.85.42.13 external

External / Internal Attack:

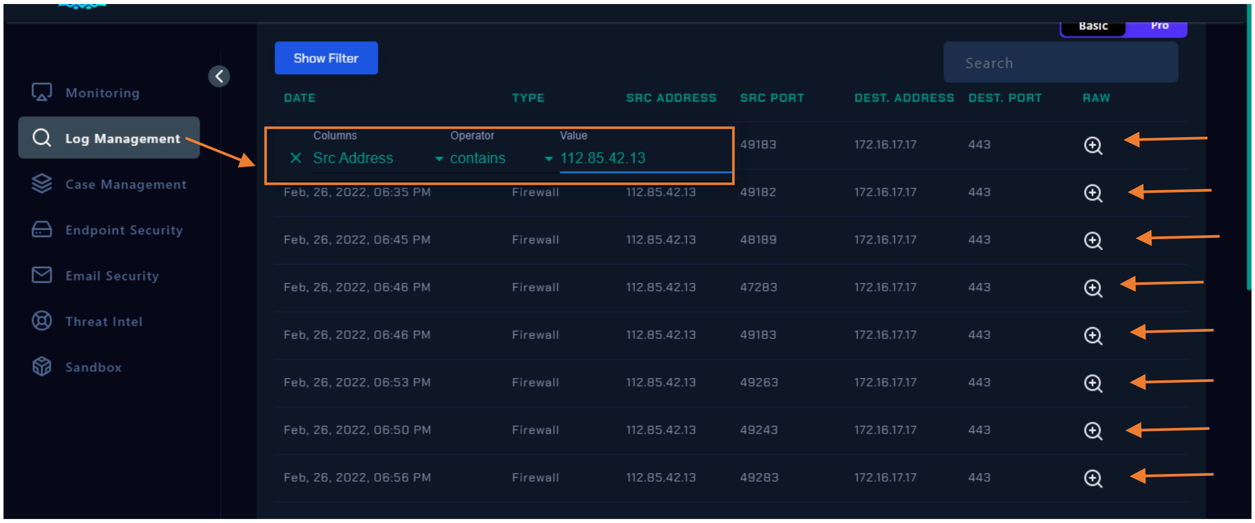
Based on the event details, the attack appears to be **external**.

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.



Columns: Src Address
Operator: contains
Value: 112.85.42.13

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			49183	172.16.17.17	443	⊕
Feb, 26, 2022, 06:35 PM	Firewall	112.85.42.13	49182	172.16.17.17	443	⊕
Feb, 26, 2022, 06:45 PM	Firewall	112.85.42.13	48189	172.16.17.17	443	⊕
Feb, 26, 2022, 06:46 PM	Firewall	112.85.42.13	47283	172.16.17.17	443	⊕
Feb, 26, 2022, 06:46 PM	Firewall	112.85.42.13	49183	172.16.17.17	443	⊕
Feb, 26, 2022, 06:53 PM	Firewall	112.85.42.13	49263	172.16.17.17	443	⊕
Feb, 26, 2022, 06:50 PM	Firewall	112.85.42.13	49243	172.16.17.17	443	⊕
Feb, 26, 2022, 06:56 PM	Firewall	112.85.42.13	49283	172.16.17.17	443	⊕

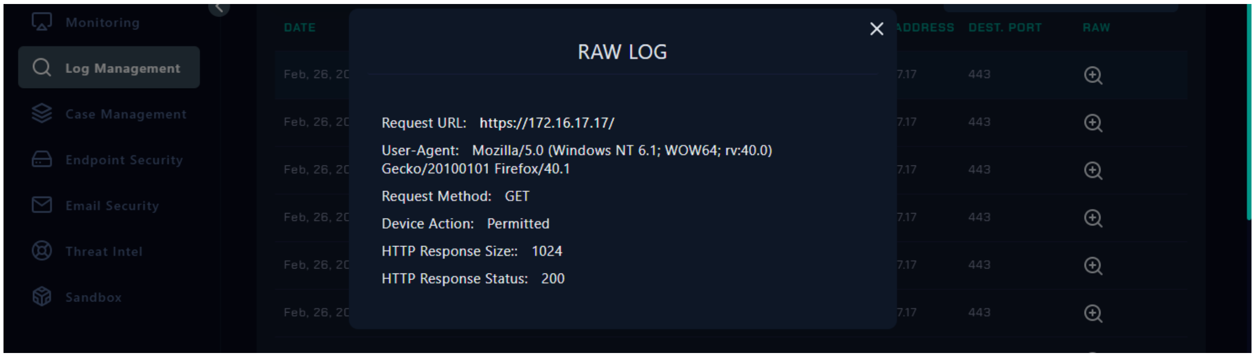
8 Logs records for the source IP.

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

We will explain all of them step by step

Log Analysis

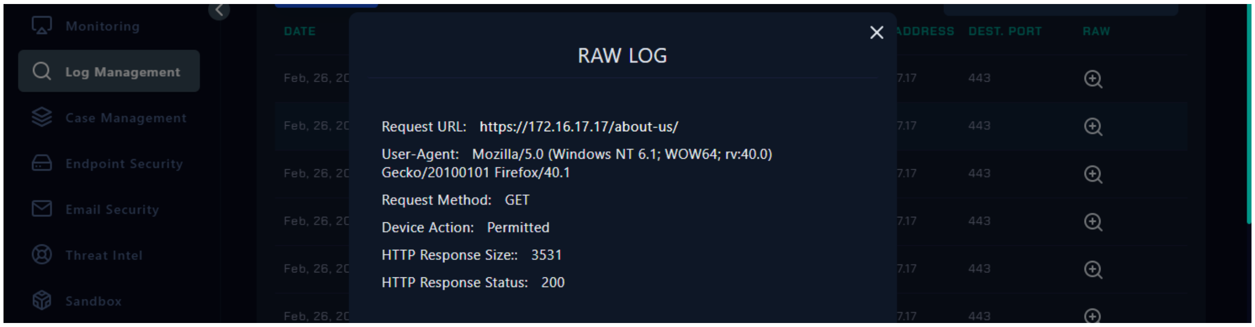
- **Log1:**



```
Request URL:   https://172.16.17.17/
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   1024
HTTP Response Status:   200
```

Explanation: This log indicates a standard GET request to the homepage. The server responded with a `200 OK` status and a response size of 1024 bytes. This is a normal request without any signs of malicious activity.

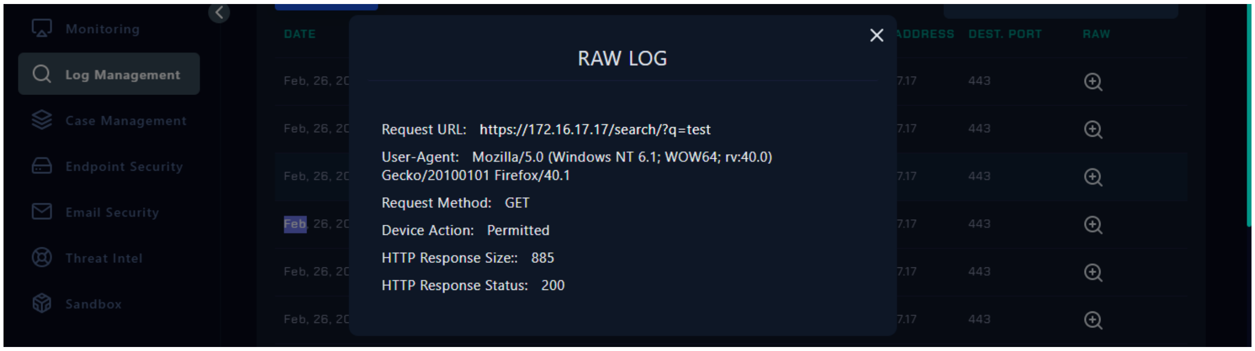
- **Log2:**



```
Request URL:   https://172.16.17.17/about-us/
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   3531
HTTP Response Status:   200
```

Explanation: This GET request was made to the `/about-us/` page and resulted in a `200 OK` response. The response size was 3531 bytes. This indicates a standard request without malicious intent.

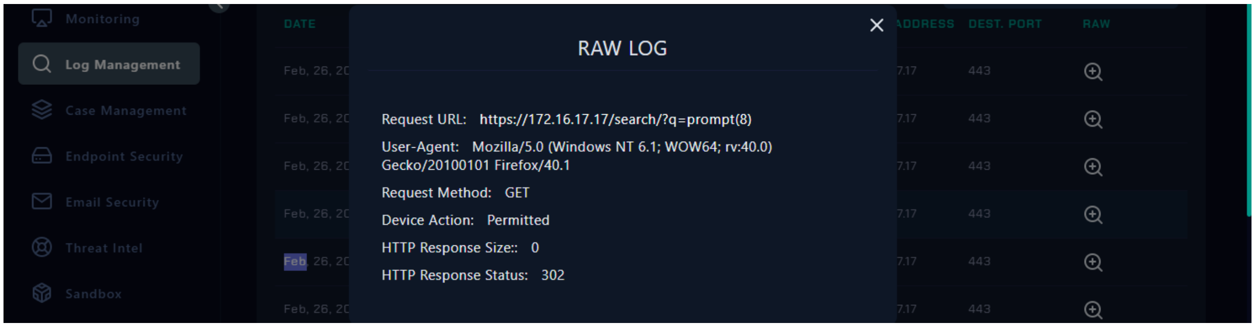
- **Log3:**



Request URL: https://172.16.17.17/search/?q=test
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method: GET
Device Action: Permitted
HTTP Response Size:: 885
HTTP Response Status: 200

Explanation: This request was for the search endpoint with a benign query parameter `q=test`. The server returned a `200 OK` status, indicating normal functionality.

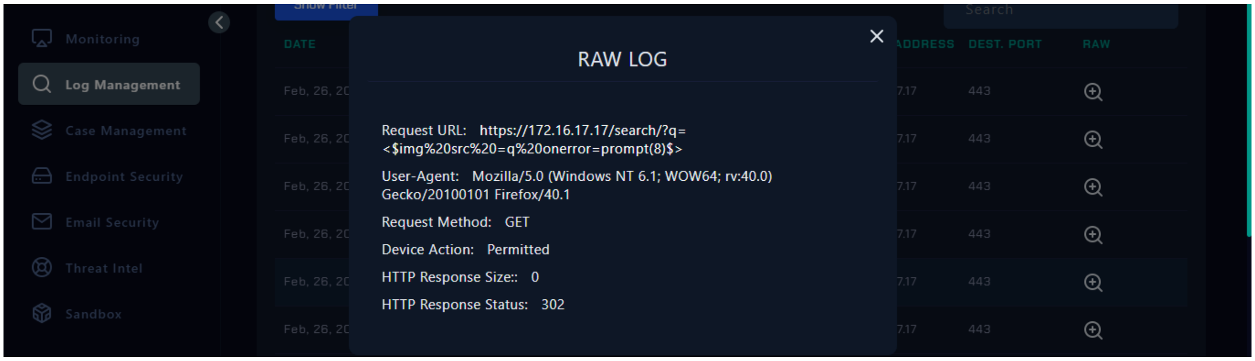
- **Log4:**



Request URL: https://172.16.17.17/search/?q=prompt(8)
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
Request Method: GET
Device Action: Permitted
HTTP Response Size:: 0
HTTP Response Status: 302

Explanation: This log shows an attempt to execute a JavaScript `prompt` function via a search query. The server responded with a `302 Found` status and no content, suggesting a possible mitigation mechanism in place.

- **Log5:**

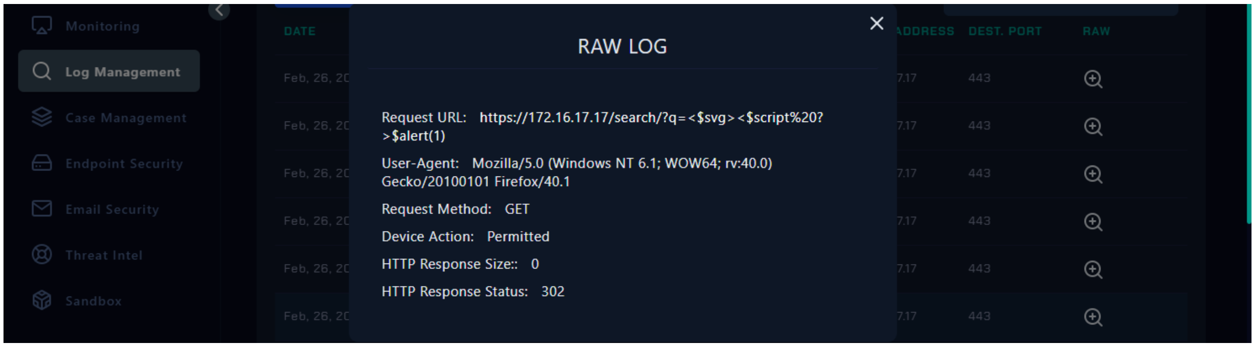


RAW LOG

```
Request URL:   https://172.16.17.17/search/?q=
<$img%20src%20=q%20onerror=prompt(8)$>
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   0
HTTP Response Status:   302
```

Explanation: **This request includes an XSS payload using an image tag with an `onerror` attribute. The server's `302 Found` response and zero response size suggest that the payload was blocked or sanitized.**

- **Log6:**

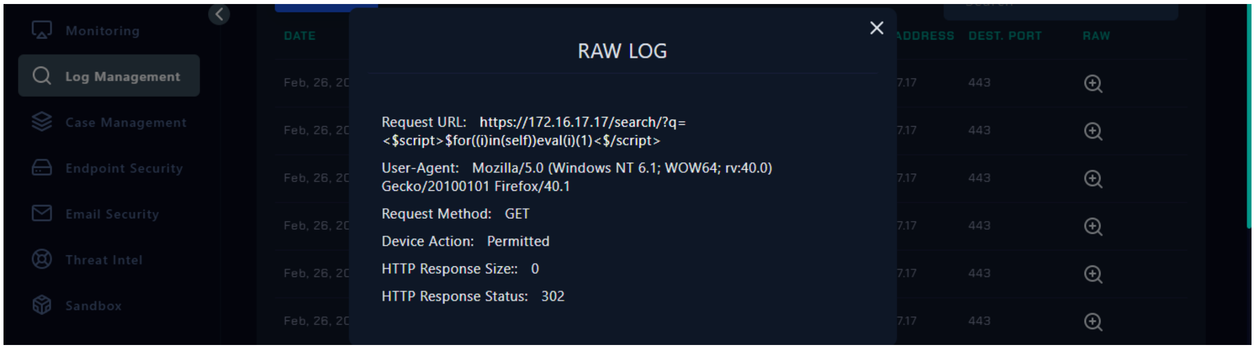


RAW LOG

```
Request URL:   https://172.16.17.17/search/?q=<$svg><$script%20?
>$alert(1)
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   0
HTTP Response Status:   302
```

Explanation: This log shows an attempt to inject SVG and script payloads. The `302 Found` response with no content indicates that the server may be redirecting or blocking such attempts.

- **Log7:**

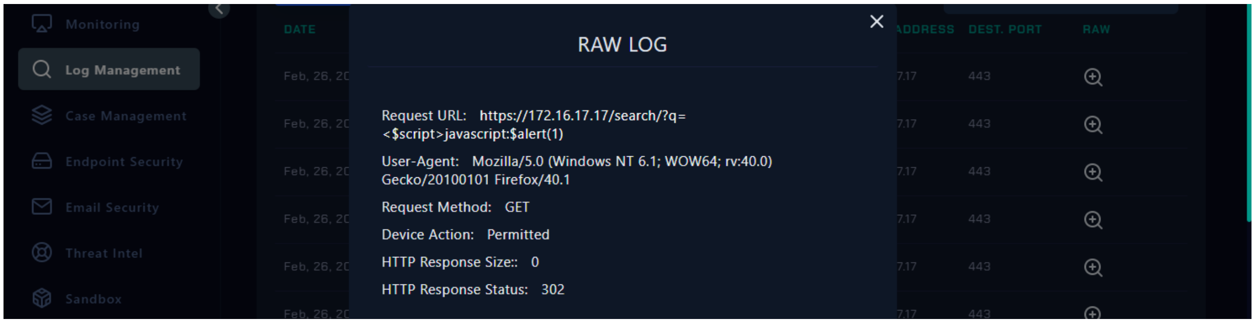


RAW LOG

```
Request URL:   https://172.16.17.17/search/?q=
<$script>$for((i)in(self))eval(i)(1)<$/script>
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   0
HTTP Response Status:   302
```

Explanation: This log indicates an attempt to execute a script with `eval` functionality. The server responded with a `302 Found` status and zero bytes of content, suggesting that such requests are being redirected or blocked.

- **Log8:**



RAW LOG

```
Request URL:   https://172.16.17.17/search/?q=
<$script>javascript:$alert(1)
User-Agent:   Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0)
Gecko/20100101 Firefox/40.1
Request Method:   GET
Device Action:   Permitted
HTTP Response Size::   0
HTTP Response Status:   302
```

Explanation: **This log shows another attempt to execute a script with JavaScript alerts. The response was `302 Found` with no content, indicating that the request was blocked or redirected.**

Summary of Logs

The provided logs capture various HTTP requests made to a web server, with several entries indicating attempts to perform potentially malicious activities. Here’s a concise summary:

1. **Normal Requests:**
   - **Logs 1, 2, and 3** show standard GET requests to various pages (`/`, `/about-us/`, and `/search/?q=test`). These requests were processed normally, receiving `200 OK` responses with content delivered as expected.
2. **Malicious Requests:**
   - **Logs 4 to 8** document multiple attempts to exploit Cross-Site Scripting (XSS) vulnerabilities. Each of these logs contains a query parameter designed to inject and execute scripts:
     - **Log 4**: Contains `prompt(8)` intended to trigger a JavaScript prompt.
     - **Log 5**: Uses an image tag with `onerror=prompt(8)` to test for XSS.
     - **Log 6**: Contains SVG and script elements designed to execute an alert box.
     - **Log 7**: Attempts to execute a script with `eval` functionality.
     - **Log 8**: Tests with a script to execute a JavaScript alert.

   Each malicious request resulted in a `302 Found` status with no content returned, suggesting that the server's security measures effectively redirected or blocked the attempts.

The logs reveal that while there were multiple attempts to exploit XSS vulnerabilities, these attacks were unsuccessful due to the server’s protective responses.

1. **Is Traffic Malicious?**

   Based on our analysis, the traffic appears to be malicious. The requests contained various XSS payloads designed to execute scripts, which are characteristic of attempted cross-site scripting (XSS) attacks.

2. **What Is The Attack Type?**

   The attack type identified is a Cross-Site Scripting (XSS) attack. The logs show attempts to inject and execute malicious scripts via search queries, which is indicative of XSS exploitation techniques.

3. **Is the Malicious Traffic Caused by a Planned Test?**

   After reviewing the email security section, it has been confirmed that this traffic **was not part of a planned test**. There is no indication that these requests were authorized or scheduled.

4. **Was the Attack Successful?**

   No, the attack was not successful. The server responded to all malicious attempts with a `302 Found` status and zero content. This suggests that the payloads were either redirected or blocked by security mechanisms in place.

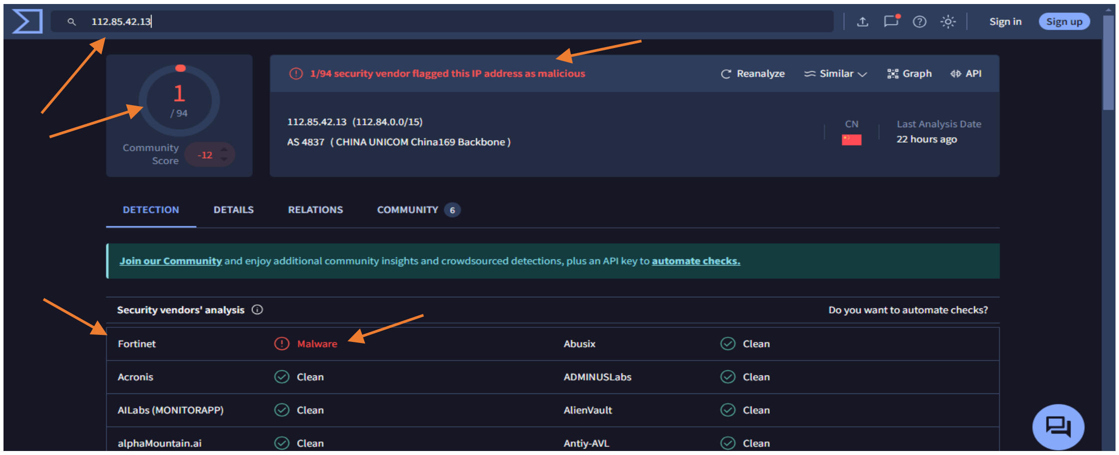
Detection:

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 us its **malicious IP.**



1/94 security vendor flagged this IP address as malicious

112.85.42.13 (112.84.0.0/15)
AS 4837 (CHINA UNICOM China169 Backbone)

Last Analysis Date
22 hours ago

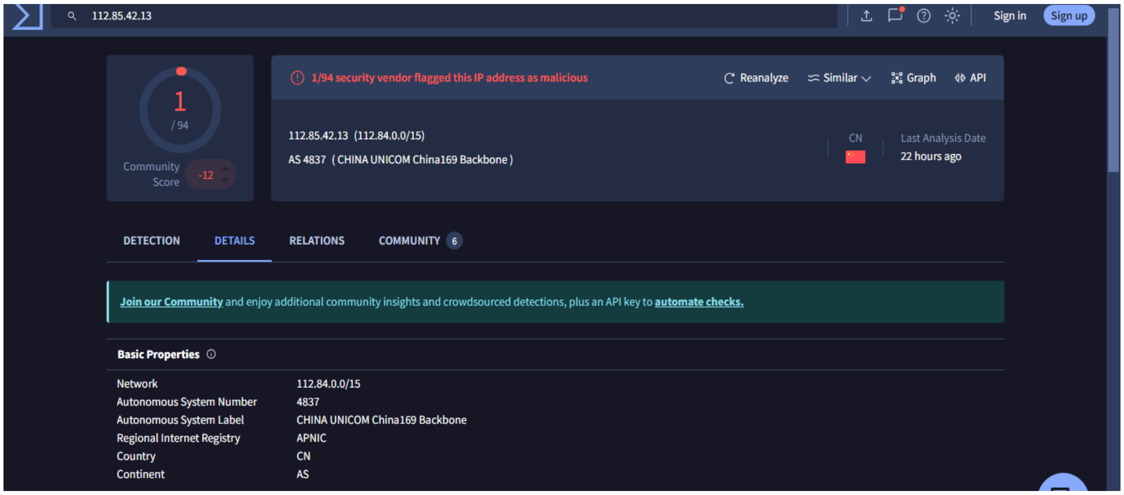
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Fortinet	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean

   - **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.



1/94 security vendor flagged this IP address as malicious

112.85.42.13 (112.84.0.0/15)
AS 4837 (CHINA UNICOM China169 Backbone)

Last Analysis Date
22 hours ago

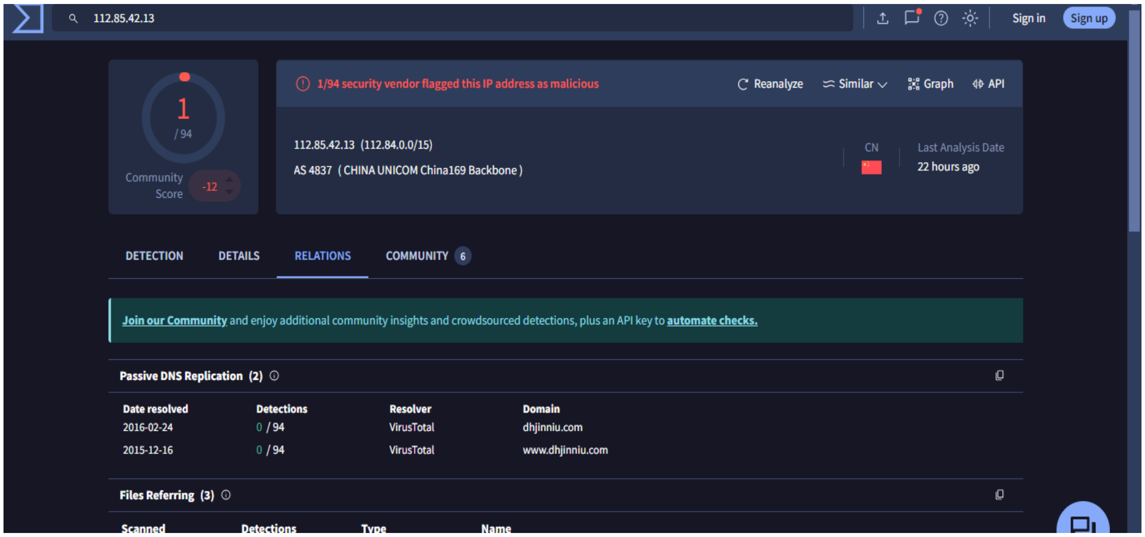
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic Properties

Network	112.84.0.0/15
Autonomous System Number	4837
Autonomous System Label	CHINA UNICOM China169 Backbone
Regional Internet Registry	APNIC
Country	CN
Continent	AS

   - **Reference:** View Details Section

3. **Relation Section**
   - **Status:** The Relation section is clear.



112.85.42.13

1 / 94

Community Score -12

1/94 security vendor flagged this IP address as malicious

112.85.42.13 (112.84.0.0/15)

AS 4837 (CHINA UNICOM China169 Backbone)

CN

Last Analysis Date 22 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (2)

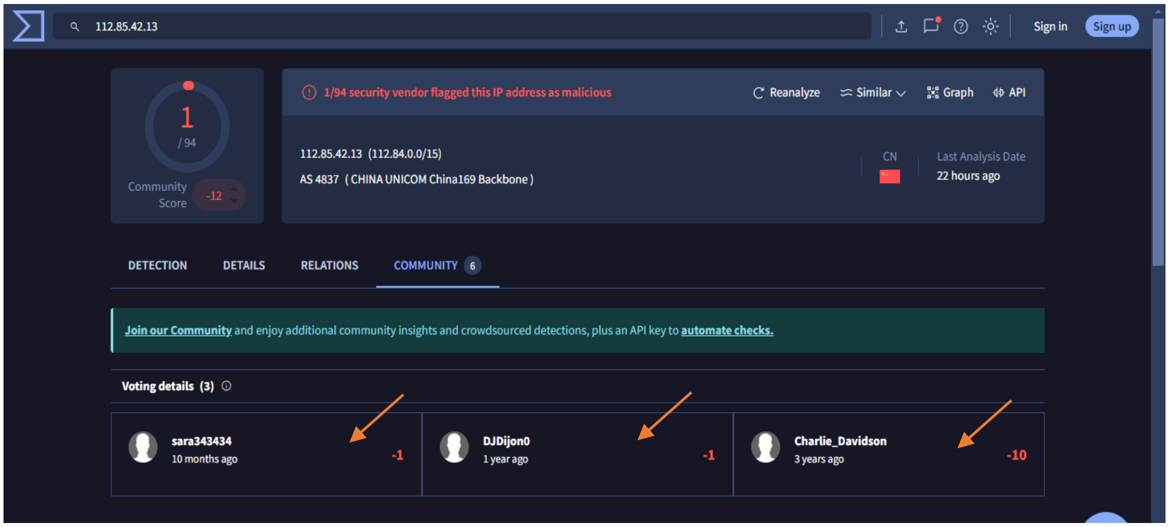
Date resolved	Detections	Resolver	Domain
2016-02-24	0 / 94	VirusTotal	dhjinniu.com
2015-12-16	0 / 94	VirusTotal	www.dhjinniu.com

Files Referring (3)

Scanned	Detections	Type	Name

   - **Reference:** View Relations Section

4. **Community Section**
   - **Status:** The Community section is not clear, there is more than 10 comments.



112.85.42.13

1 / 94

Community Score -12

1/94 security vendor flagged this IP address as malicious

112.85.42.13 (112.84.0.0/15)

AS 4837 (CHINA UNICOM China169 Backbone)

CN

Last Analysis Date 22 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Voting details (3)

sara343434 10 months ago -1	DJDijon0 1 year ago -1	Charlie_Davidson 3 years ago -10

   - **Reference:** View Community Section

5. **Do You Need Tier 2 Escalation?**

There is no need for Tier 2 escalation at this time. Based on our analysis, the attacks were unsuccessful, and the security measures effectively mitigated the potential threats.

Conclusion

Event Overview: On February 26, 2022, at 06:56 PM, an alert was triggered on WebServer1002 under Event ID 116, due to the detection of JavaScript code in the URL. The request, made from an external IP (112.85.42.13) to an internal server (172.16.17.17), contained XSS payloads aimed at exploiting Cross-Site Scripting (XSS) vulnerabilities.

Log Analysis Summary: The logs show a mix of standard and malicious requests. Logs 1 through 3 recorded typical GET requests to the homepage, `/about-us/`, and a search query with no signs of malicious intent. Logs 4 through 8, however, captured attempts to inject and execute JavaScript through various payloads, including `<script>` tags, `eval` functions, and SVG elements. Despite these attempts, each malicious request received a `302 Found` status and zero content, indicating that the server's security mechanisms successfully blocked or redirected the malicious traffic.

Conclusion: The analysis confirms that the traffic was indeed malicious, characterized by attempts to exploit XSS vulnerabilities. However, the attack was thwarted effectively by the server's security measures. The successful application of these defenses ensured that no harmful scripts were executed, and no content was delivered in response to the malicious requests.

Additional Findings: The source IP address was checked on VirusTotal, revealing a history of malicious activity. Despite this, the analysis showed no additional issues or anomalies related to the IP address in the Detection, Details, and Relation sections. The Community section indicated some concerns, but these did not impact the immediate threat assessment.

Recommendation: Given that the attack was unsuccessful and effectively mitigated, there is no need for Tier 2 escalation at this time. The security measures in place have demonstrated their capability to handle such threats, and the incident should be considered contained.

This analysis underscores the robustness of our defensive measures and highlights the importance of continuous monitoring and evaluation to maintain security efficacy.