



## **Official incident report**

Event ID: 234

Rule Name: SOC176- RDP Brute Force Detection

# Table of contents

<b>Official incident report</b>	<b>1</b>
Event ID: 234	1
Rule Name: SOC176- RDP Brute Force 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	4
<b>Analysis</b>	<b>7</b>
Log management	7
End Point Security	11
<b>Conclusion</b>	<b>12</b>

## Event Details

**Event ID:**

234

**Event Date and Time:**

Mar, 07, 2024, 11:44 AM

**Rule:**

SOC176 - RDP Brute Force Detected

**Level:**

Security Analyst

**Description:**

Login failure from a single source with different non existing accounts

## Network Information Details

**Destination Address:**

172.16.17.148

**Source Address:**

218.92.0.56

# Detection:

## Threat Intelligence Results

[www.virustotal.com](http://www.virustotal.com)

The screenshot shows the VirusTotal Threat Intelligence interface for the IP address 218.92.0.56. The interface is dark-themed. At the top, a circular gauge shows a score of 14/92. A prominent red banner states: "14/92 security vendors flagged this IP address as malicious". Below this, the IP address is listed as 218.92.0.56 (218.92.0.0/16) with AS 4134 (Chinanet). The last analysis date is 11 hours ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (13+). A green banner encourages joining the community. Below, a table titled "Security vendors' analysis" lists various vendors and their classifications. An orange arrow points from the red banner to the table. Another orange arrow points from the table to the "Do you want to automate checks?" link.

Vendor	Classification
alphaMountain.ai	Malicious
BitDefender	Phishing
Criminal IP	Malicious
EmergingThreats	Malicious
Antiy-AVL	Malicious
Certego	Malicious
CyRadar	Malicious
Fortinet	Malware

[www.letsdefend.io](http://www.letsdefend.io)

The screenshot shows the LetsDefend Threat Intelligence feed interface. The interface is dark-themed. At the top, the LetsDefend logo is visible, along with navigation links: Home, Learn, Practice, Challenge, Pricing. A sidebar on the left lists various security services: Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel (selected), and Sandbox. The main area has a search bar with the IP address 218.92.0.56 entered. Below the search bar, there are filters for Date range, Search by data type, and Search by data. A table at the bottom displays the search results. An orange arrow points from the search bar to the table.

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Mar, 08, 2024, 02:33 PM	IP	218.92.0.56	Malicious	Anonymous

www.letsdefend.io

AbuseIPDB » 218.92.0.56

Check an IP Address, Domain Name, or Subnet  
e.g. 156.197.32.19, microsoft.com, or 5.188.10.0/24

156.197.32.19 CHECK

**218.92.0.56** was found in our database!

This IP was reported **419,045** times. Confidence of Abuse is **100%** ?

100%

ISP	ChinaNet Jiangsu Province Network
Usage Type	Data Center/Web Hosting/Transit
Domain Name	chinatelecom.com.cn
Country	China

feedback

Type here to search

طقس حار 12:42 PM 7/24/2024

Based on the threat intelligence gathered from various reputable sources, the IP address 218.92.0.56 has been determined to be malicious. Below are the detailed findings:

VirusTotal:

14/92 security vendors flagged this IP address as malicious.

Notable detections include:

alphaMountain.ai: Malicious

Antiy-AVL: Malicious

BitDefender: Phishing

Certego: Malicious

Criminal IP: Malicious

CyRadar: Malicious

EmergingThreats: Malicious

Fortinet: Malware

G-Data: Phishing

GreenSnow: Malicious

Juniper Networks: Malicious

Lionic: Malicious

VIPRE: Phishing

Webroot: Malicious

Additional suspicious classifications by:

AlphaSOC: Suspicious

ArcSight Threat Intelligence: Suspicious

AbuseIPDB:

The IP address 218.92.0.56 was found in the AbuseIPDB database.

Reported 419,045 times with a 100% Confidence of Abuse.

Associated details:

ISP: ChinaNet Jiangsu Province Network

Usage Type: Data Center/Web Hosting/Transit

Domain Name: chinatelecom.com.cn

Country: China

City: Lianyungang, Jiangsu

LetsDefend:

The IP address 218.92.0.56 is flagged as malicious.

Conclusion:

The IP address 218.92.0.56 has been extensively reported and verified as malicious across multiple threat intelligence platforms. The significant number of reports and high confidence levels, coupled with its classification as a phishing and malware source, indicate that this IP poses a considerable threat. It is strongly recommended to block this IP address and monitor for any related activity within the network.

# Analysis:

## Log Management

\*I opened log management section then I filtered the results by choosing the source address and typing the attacker IP.

The screenshot shows the LetsDefend web application interface. The left sidebar contains navigation options: Monitoring, Log Management (selected), Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main content area displays a log table with columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. A filter is applied to the SRC ADDRESS column, showing 'contains 218.92.0.56'. The table lists several log entries, all with the same source address (218.92.0.56) and destination address (172.16.17.148). The log entries are dated Mar, 07, 2024, 11:44 AM. The log types are OS, Firewall, Firewall, Firewall, Firewall, and Firewall. The source ports are 18845, 51707, 50807, 24319, 10098, 41175, and 61506. The destination ports are all 3389. The RAW column contains magnifying glass icons. A 'Show Filter' button is visible above the table. A search bar is also present.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Mar, 07, 2024, 11:44 AM	OS	218.92.0.56	18845	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	51707	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	50807	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	24319	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	10098	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	41175	172.16.17.148	3389	
Mar, 07, 2024, 11:44 AM	Firewall	218.92.0.56	61506	172.16.17.148	3389	

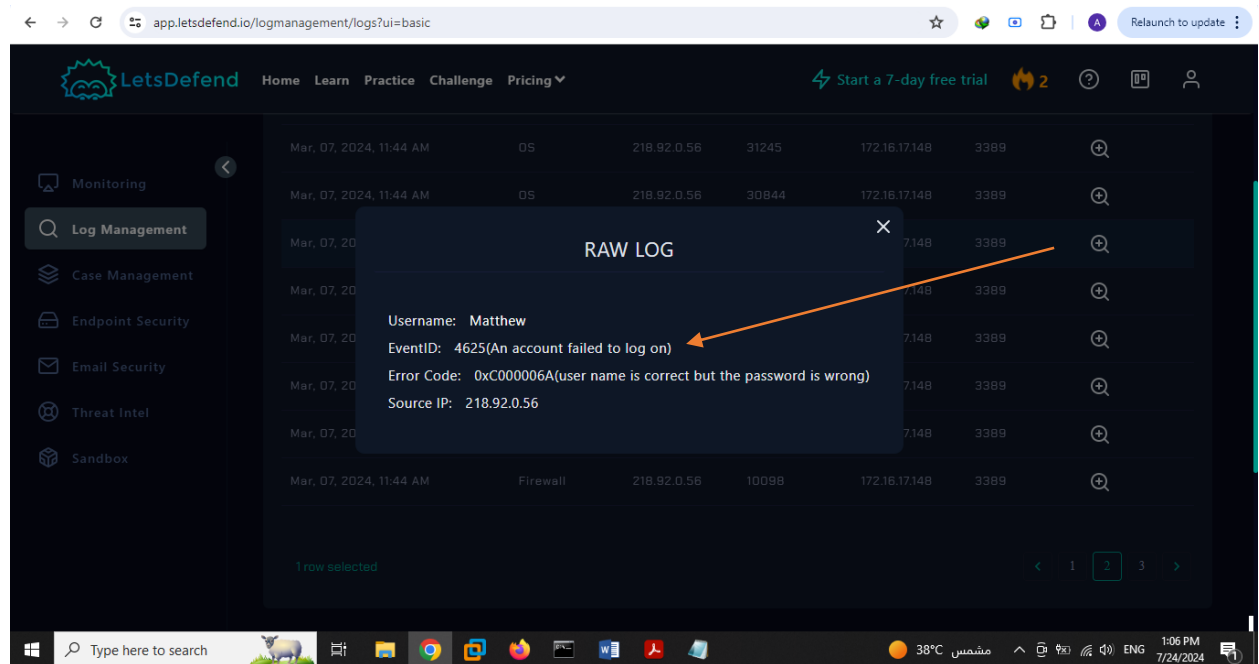
\*I Checked all the Firewall results and its all the same

The screenshot shows the same LetsDefend web application interface. A modal window titled 'RAW LOG' is open, displaying the raw log data for the selected entry. The modal window has a close button (X) in the top right corner. The log data is displayed in a table with columns: DATE, ADDRESS, DEST. PORT, and RAW. The log entry is dated Mar, 07, 2024, 11:44 AM. The address is 218.92.0.56. The destination port is 3389. The RAW column contains a magnifying glass icon. An arrow points from the 'RAW LOG' modal window to the log entry in the table.

DATE	ADDRESS	DEST. PORT	RAW
Mar, 07, 2024, 11:44 AM	218.92.0.56	3389	

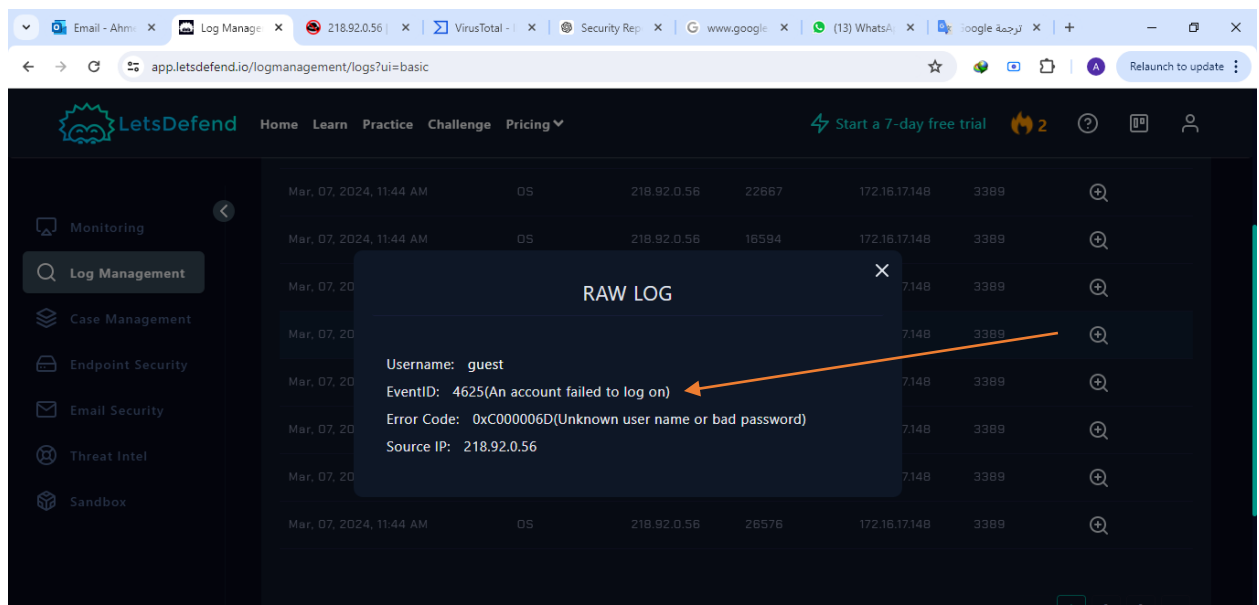
1. Attacker tried to login by correct user name: Matthew, but failed to login because he doesn't know the password and he is trying to make brute force attack to login.

Event ID 4625, Error Code: 0xC000006A (user name is correct but the password is wrong) , Target service ( Destination port ): RDP 3389.



2. Attacker tried to login by wrong user name: guest, but failed to login because he doesn't know the username and password and he is trying to make brute force attack to login.

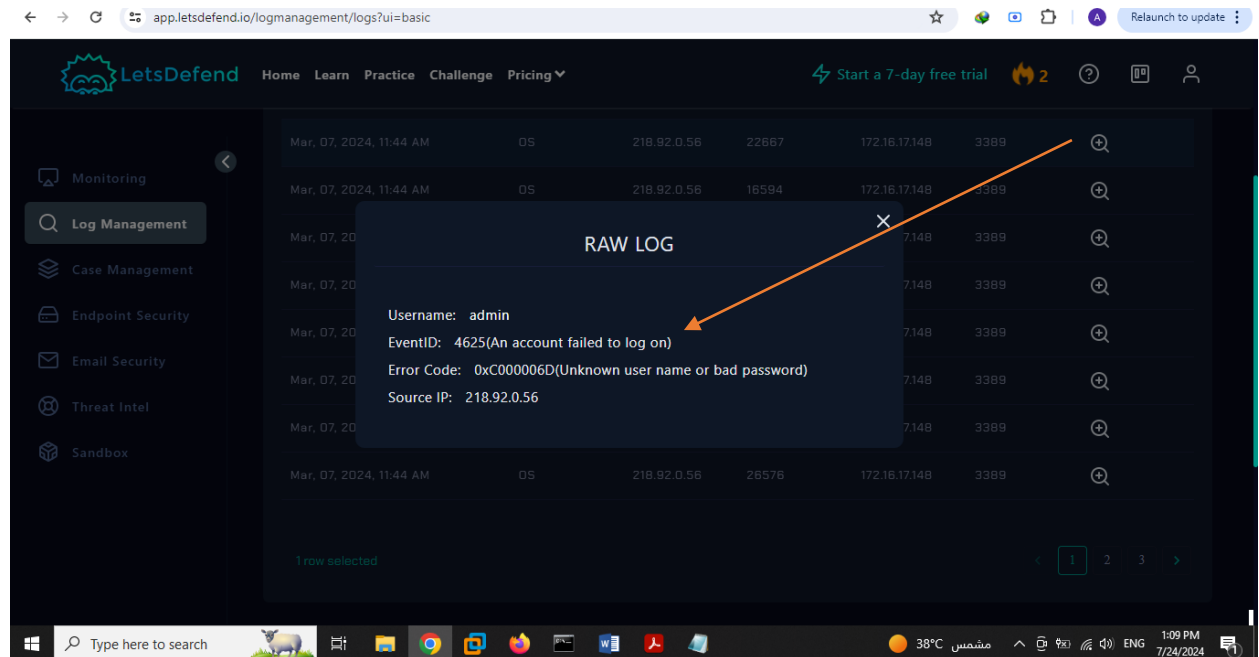
Event ID 4625, Error Code: 0xC000006D (Unknown user name or bad password), Target service (Destination port): RDP 3389.



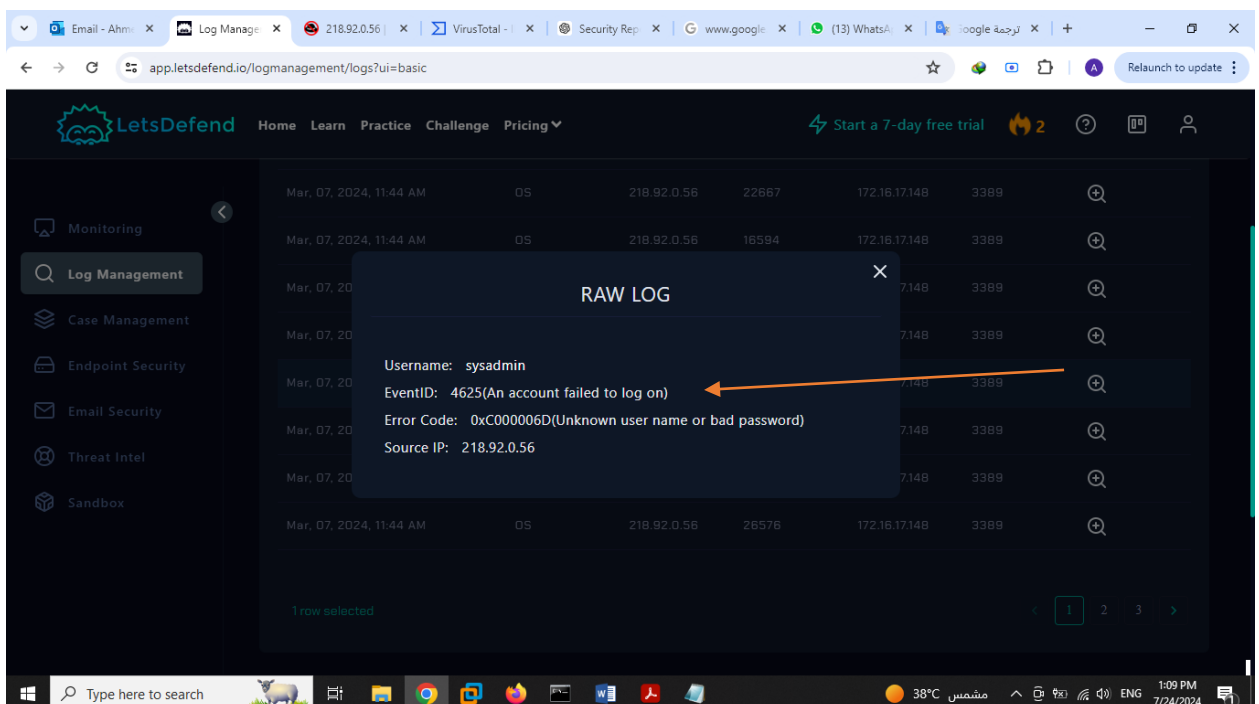


- Attacker tried to login by wrong user name: admin, but failed to login because he doesn't know the username and password and he is trying to make brute force attack to login.

Event ID 4625, Error Code: 0xC000006D (Unknown user name or bad password) , Target service ( Destination port ): RDP 3389.



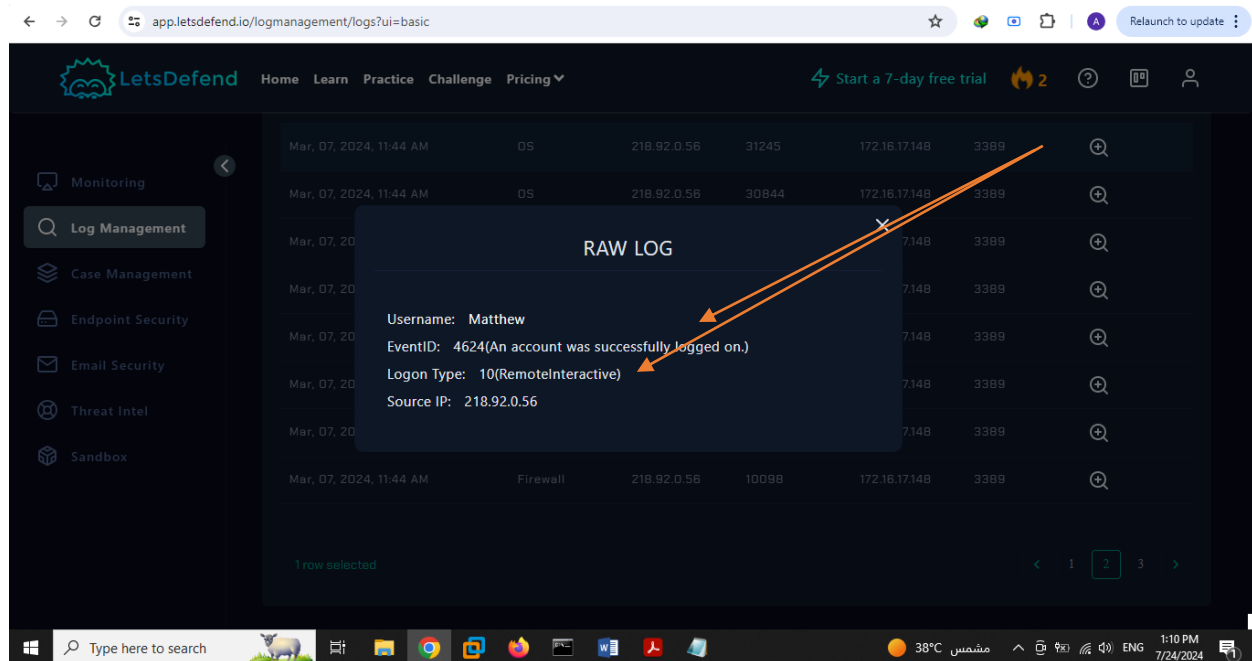
- Attacker tried to login by wrong user name: sysadmin, but failed to login because he doesn't know the username and password and he is trying to make brute force attack to login.



5. Attacker logged in by correct username: Matthew, and correct password.

Event ID: 4624(An account was successfully logged on.)

Logon Type: 10(Remote Interactive)



The attacker initiated a brute force attack on the system's RDP service (port 3389), attempting multiple logins with both correct and incorrect usernames. Initial attempts with the username "Matthew" failed due to incorrect passwords (Event ID 4625, Error Code: 0xC000006A). Subsequent attempts using "guest," "admin," and "sysadmin" also failed due to incorrect usernames and passwords (Event ID 4625, Error Code: 0xC000006D). Eventually, the attacker succeeded in logging in with the correct credentials for the username "Matthew" (Event ID 4624, Logon Type: 10). This indicates a successful brute force attack, necessitating immediate security measures to prevent further unauthorized access.

# Endpoint Security

**Based on our detection and analysis we contained the device**

## Conclusion

On March 07, 2024, at 11:44 AM, a security event (Event ID: 234) was detected under SOC Rule SOC176, indicating a brute force attack on the RDP service (port 3389) targeting our system. The attacker, originating from the malicious IP address 218.92.0.56, attempted multiple login attempts using both correct and incorrect usernames.

The attack sequence included:

1. Multiple failed login attempts with the username "Matthew" due to incorrect passwords (Event ID 4625, Error Code: 0xC000006A).
2. Failed login attempts using non-existing usernames "guest," "admin," and "sysadmin" (Event ID 4625, Error Code: 0xC000006D).
3. A successful login using the correct username "Matthew" and password (Event ID 4624, Logon Type: 10).

Threat intelligence from VirusTotal, AbuseIPDB, and LetsDefend consistently flagged the source IP as malicious, with significant evidence of phishing, malware, and other malicious activities. Given the high confidence levels and extensive reports, it is evident that this IP poses a significant threat.

Our analysis confirmed repeated brute force attempts, ultimately leading to unauthorized access. Immediate actions have been taken to contain the compromised endpoint and prevent further breaches. It is strongly recommended to block the IP address 218.92.0.56 and monitor for any related suspicious activity within the network.