Author: Jack Fitzgerald

Official Incident Report

Date: Mar, 07, 2024, 11:44 AM

Event ID: 234

Rule Name: SOC176 - RDP Brute Force Detected

Table of Contents

Alert Details

Severity: Medium

Type: Brute Force

Source IP Address: 218.92.0.56

Destination IP Address: 172.16.17.148

Destination Hostname: Matthew

Protocol: RDP

Firewall Action: Allowed

Alert Trigger Reason: Login failure from a single source with different non existing accounts

Based on the information provided in the alert, it appears that brute force attempts have been identified on host **172.16.17.148** from a remote attacker on host **218.92.0.56**. The alert is triggered by rule SOC176 - RDP Brute Force Detected.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

The trigger indicates that the login attempt failed with different non-existent accounts. It is important to check Network traffic and System logs of the Host from Log Management.

Remote logons typically occur over protocol RDP (Remote Desktop Protocol).

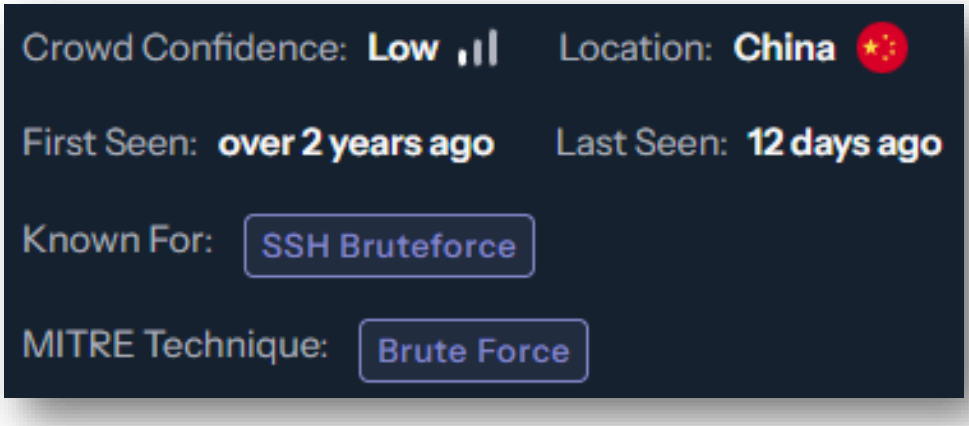
Analysis

We can begin the analysis by analyzing the attacker's IP address **218.92.0.56** using **VirusTotal**, **CrowdSec**, and **AbuseIPDB**.

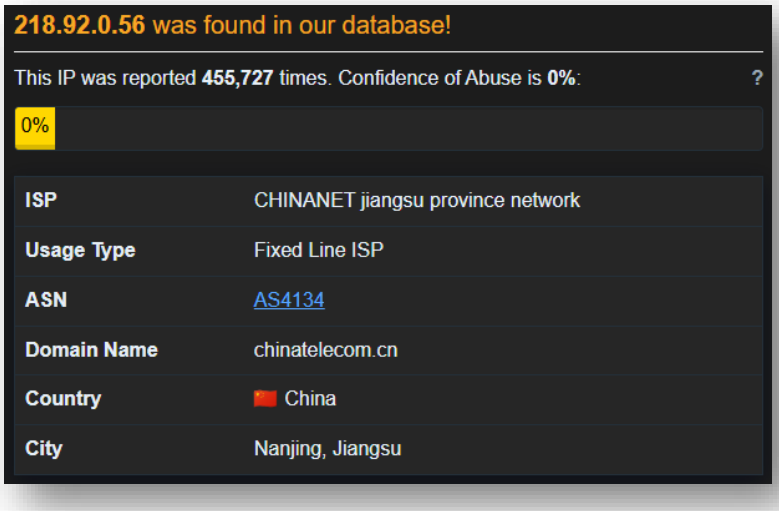
https://www.virustotal.com/gui/ip-address/218.92.0.56

7/95 security vendors flagged this IP address as malicious

https://app.crowdsec.net/cti/218.92.0.56

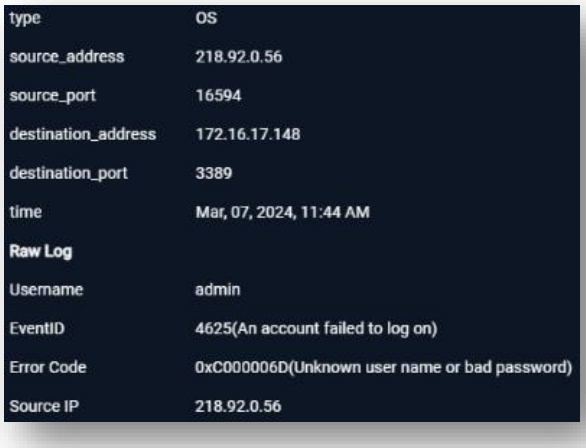


https://www.abuseipdb.com/check/218.92.0.56

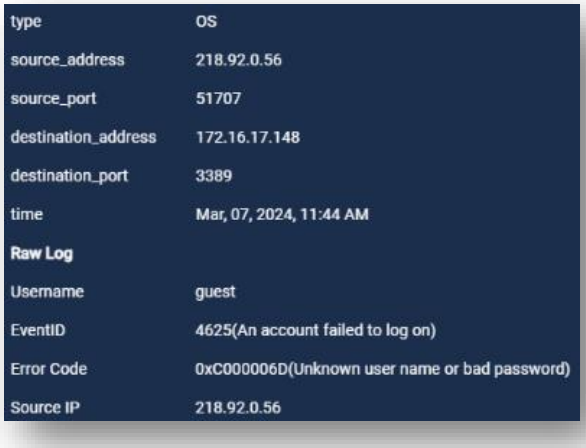


Next, we can analyse the logs found for this incident, where we discovered 30 events related to the attacker's IP address.

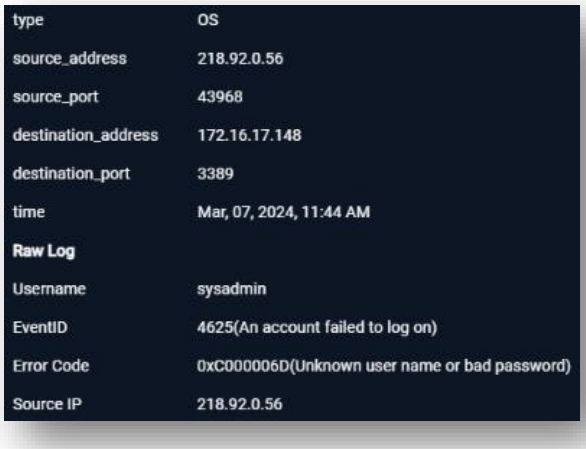
We found 3 **failed** brute force attempts on the target machine for username **admin**, using 3 different source ports 18845, 22667, 16594. The reason for the account log on failure is due to an **unknown username** or **bad password**.



We found 3 **failed** brute force attempts on the target machine for username **guest**, using 3 different source ports in use 51707, 35346, 47409. The reason for the account log on failure is due to an **unknown username** or **bad password**.

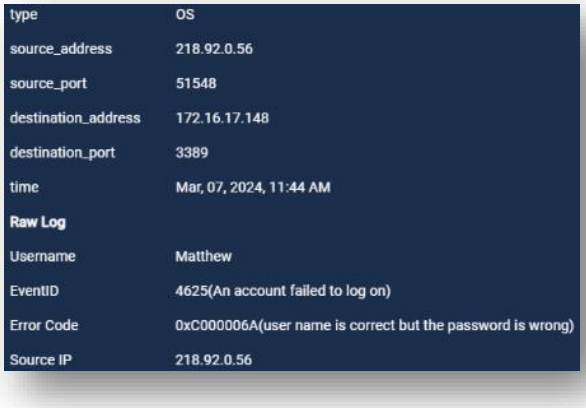


We found 6 **failed** brute force attempts on the target machine for username **sysadmin**, using 6 different source ports 42044, 43968, 31696, 26576, 37633, 22383. The reason for the account log on failure is due to an **unknown username** or **bad password**.



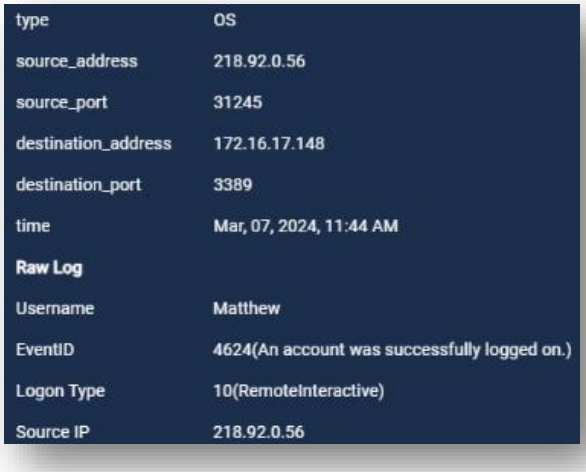
type	OS
source_address	218.92.0.56
source_port	43968
destination_address	172.16.17.148
destination_port	3389
time	Mar, 07, 2024, 11:44 AM
Raw Log	
Username	sysadmin
EventID	4625(An account failed to log on)
Error Code	0xC000006D(Unknown user name or bad password)
Source IP	218.92.0.56

We found 2 **failed** brute force attempts on the target machine for username **Matthew**, using 2 different source ports 30844, 51548. The reason for the account log on failure is due to a **correct username but wrong password**.



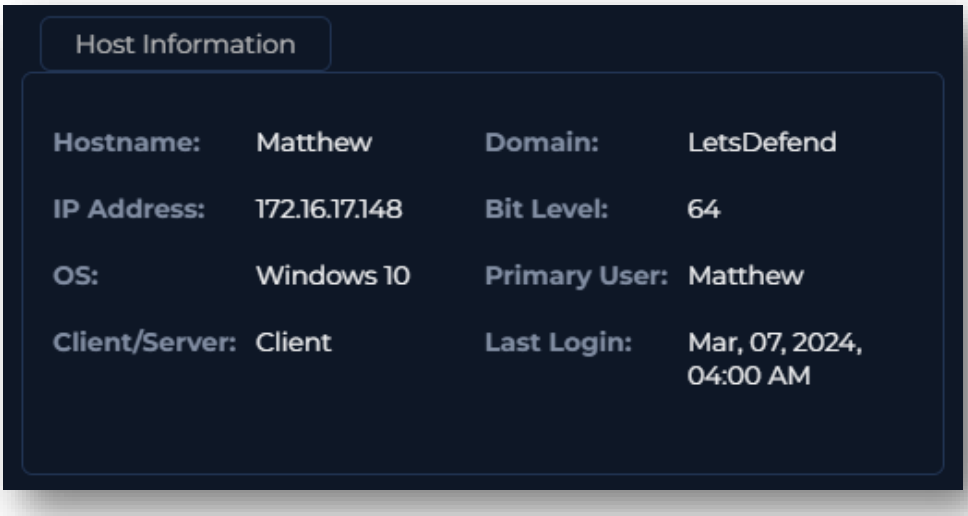
type	OS
source_address	218.92.0.56
source_port	51548
destination_address	172.16.17.148
destination_port	3389
time	Mar, 07, 2024, 11:44 AM
Raw Log	
Username	Matthew
EventID	4625(An account failed to log on)
Error Code	0xC000006A(user name is correct but the password is wrong)
Source IP	218.92.0.56

We found 1 **successful** brute force attempt on the target machine for username **Matthew**, using 1 source port 31245. This time, the remote log on was a success, indicating a **breach in the system**.

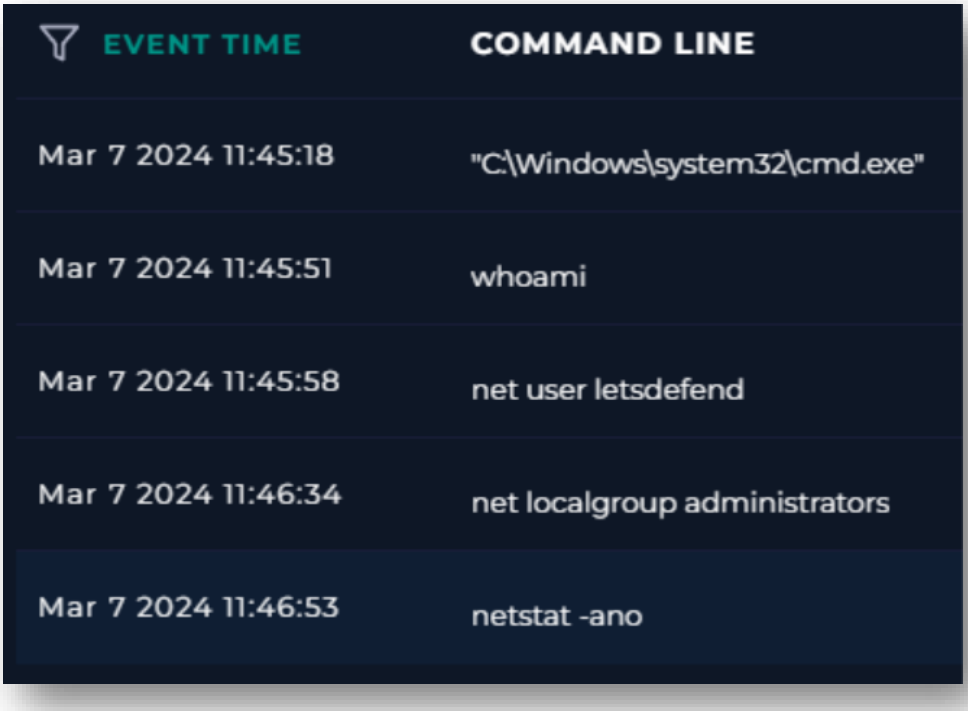


type	OS
source_address	218.92.0.56
source_port	31245
destination_address	172.16.17.148
destination_port	3389
time	Mar, 07, 2024, 11:44 AM
Raw Log	
Username	Matthew
EventID	4624(An account was successfully logged on.)
Logon Type	10(RemoteInteractive)
Source IP	218.92.0.56

We can further investigate this incident by reviewing Endpoint Security for **Matthew**.



We can review the Terminal History of the machine after the successful brute force login is performed.

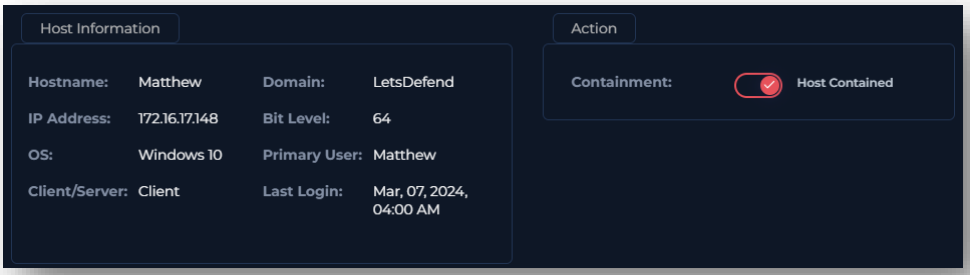


EVENT TIME	COMMAND LINE
Mar 7 2024 11:45:18	"C:\Windows\system32\cmd.exe"
Mar 7 2024 11:45:51	whoami
Mar 7 2024 11:45:58	net user letsdefend
Mar 7 2024 11:46:34	net localgroup administrators
Mar 7 2024 11:46:53	netstat -ano

The attacker runs **cmd.exe**, followed by **whoami** to gain an understanding of the user they logged in as **Matthew**. The attacker then views the letsdefend **user details** and the **administrators local group details** using **net user** and **net localgroup**. The attacker then uses **netstat -ano** to **display all active network connections and listening ports**, along with the **associated process IDs PIDs**.

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **Matthew** with an IP address of **172.16.17.148**. The alert was triggered by multiple remote logon attempts from non-existing accounts on the host, based on the rule SOC176 - RDP Brute Force Detected.

Upon further analysis, it was discovered that host machine **Matthew 172.16.17.148** fell victim to an **RDP Brute Force** attack from **218.92.0.56**. The attacker initially tried to brute force into **admin**, **guest**, and **sysadmin** accounts.

After attempting to brute force into **Matthew**, the attacker was notified that the username was correct, but the password was wrong. Once **successfully logging** on to **Matthew**, the user performed some terminal commands to gain information on **users**, **groups**, and **active network connections** and **open ports**. The **172.16.17.148** device has been contained.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Brute force attacks are highly successful against short, simple, or reused passwords
- Attackers use automated tools to make high volumes of guesses quickly
- Many organizations fail to notice ongoing brute force attacks because they do not have comprehensive logging or fail to review their security logs consistently
- Many devices and services still use default passwords, which are easy targets for automated attacks

Remediation Actions

- Lock out accounts after a defined number of incorrect password attempts
- Use cookies to differentiate known and unknown browsers/devices to implement separate lock out mechanisms
- Implement random pauses when checking passwords, adding delay to slow brute force attacks
- Lock out an IP address with multiple failed logins
- Implement secret questions after multiple failed logins
- Use CAPTCHAs to prevent automated attacks

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Credential Access	T1110.003 - Brute Force: Password Spraying
Command and Control	T1041 - Exfiltration Over C2 Channel

Artifacts

Value	Comment	Type
218.92.0.56	Performs SSH Brute Force attacks	IP Address

LetsDefend Playbook

LetsDefend Event ID: 234