Malicious Logon Activity Report

linux-target-1

# 📌 Executive Summary

This report documents a brute-force attack targeting the cloud-hosted Linux device 'linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net'. Over a 30-day window, the host received 714 failed logon attempts from IP address '218.92.0.187', targeting the 'root' account. The pattern of activity is consistent with automated SSH brute-force attempts commonly performed by low-sophistication threat actors or botnets. No successful logons were detected.

# 🕵️ The 5 Ws of the Incident

## 1. Who

- Target System: linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net  
- Target Account: root  
- Source IP Address: 218.92.0.187 (CHINANET Jiangsu Province Network, China)  
- Account Domain: linux-target-1

## 2. What

- Event Type: LogonFailed  
- Attack Technique: SSH brute-force password guessing  
- Attack Tool: Likely automated botnet agent or SSH scanner  
- Detection Method: Microsoft Defender for Endpoint (DeviceLogonEvents)

## 3. When

- Log Observation Period: Last 30 days  
- Peak Activity: Detected within the window using Defender telemetry  
- Log Source Table: DeviceLogonEvents

## 4. Where

- Host Environment: Azure-hosted Linux virtual machine  
- Hostname: linux-target-1  
- DNS Context: Internal Azure DNS naming indicates cloud deployment

## 5. Why

- Motivation: Gain unauthorized access to the root account using default or weak SSH credentials  
- Intentions May Include:  
 - Deploying malware or crypto miners  
 - Establishing persistent access  
 - Using host as a pivot for lateral movement  
 - Exfiltrating sensitive data or credentials

# 🔍 Key Findings

Device Name: linux-target-1.p2zfvso05mlezjev3ck4vqd3kd.cx.internal.cloudapp.net  
Remote IP: 218.92.0.187  
Targeted Account: root  
Logon Result: LogonFailed  
Total Attempts: 714

# 🧠 MITRE ATT&CK Mapping

This activity maps to the following MITRE ATT&CK tactics and techniques:

## Tactic: Initial Access

[T1110.001] Brute Force: Password Guessing  
- 714 failed SSH logon attempts were recorded from IP 218.92.0.187, directly targeting the root account.

## Tactic: Credential Access

[T1110] Brute Force  
- Although no credentials were successfully stolen, the pattern clearly matches brute-force behavior.

## Tactic: Discovery (Expected if Access Gained)

[T1082] System Information Discovery  
- If login were successful, attacker would likely enumerate the host environment and connected network.

## Tactic: Persistence (Expected if Access Gained)

[T1053.003] Scheduled Task/Job: Cron  
- Common persistence mechanism used in Linux compromises, especially via shell scripts or crypto miners.

# 🛠️ Recommended Remediation

## SSH and Credential Hardening

- Disable password-based SSH logins in /etc/ssh/sshd\_config:  
 PermitRootLogin no  
 PasswordAuthentication no  
- Enforce SSH key-based authentication  
- Implement two-factor authentication (2FA) where feasible

## Network-Level Protections

- Block inbound SSH traffic from 218.92.0.0/16  
- Deploy fail2ban or sshd\_config rate limiting  
- Apply geo-blocking for inbound SSH access where appropriate

## Monitoring & Detection Improvements

- Enable SIEM alerts for:  
 - Multiple failed logins from a single external IP  
 - Repeated logon attempts to high-privilege accounts  
- Monitor DeviceNetworkEvents for C2 traffic if access is later gained  
- Enable file integrity monitoring on /etc/passwd, /etc/ssh/, and crontab directories

# 📊 Severity Assessment

Likelihood of Compromise: Medium  
Threat Actor Sophistication: Low (automated botnet)  
Recommended Response Time: High  
Follow-up Investigation Needed? Yes

# 🔚 Conclusion

The volume and pattern of failed root login attempts from 218.92.0.187 clearly demonstrate an automated brute-force attack against the host linux-target-1. While the attempts were unsuccessful, they reflect persistent and targeted adversarial behavior. Immediate SSH hardening, network-level protections, and system monitoring are recommended to prevent future compromise.