

LetsDefend Sample

On **June 21, 2023, at 01:51 PM**, the Security Operations Center (SOC) detected a suspicious activity on the organization's **VPN server (vpn-letsdefend.io)**. Event ID **162** was triggered under the rule **SOC210 – Possible Brute Force Detected on VPN**.

The source IP address **37.19.221.229** initiated multiple failed login attempts targeting several usernames, including invalid accounts (sane@letsdefend.io, fane@letsdefend.io, zane@letsdefend.io, tane@letsdefend.io) and the valid account mane@letsdefend.io. Shortly after repeated failures, a **successful login** occurred for this account, indicating a **possible successful brute force attack**

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Jun, 21, 2023, 01:51 PM	SOC210 - Possible Brute Force Detected on VPN	162	Brute Force	>> ✓
<div><div>EventID :</div><div>Event Time :</div><div>Rule :</div><div>Level :</div><div>Source Address :</div><div>Destination Address :</div><div>Destination Hostname :</div><div>Username :</div><div>Alert Trigger Reason :</div><div>L1 Note :</div><div>Show Hint ⚙</div></div> <div><div>162</div><div>Jun, 21, 2023, 01:51 PM</div><div>SOC210 - Possible Brute Force Detected on VPN</div><div>Security Analyst</div><div>37.19.221.229</div><div>33.33.33.33</div><div>Mane</div><div>mane@letsdefend.io</div><div>A successful VPN login was detected shortly after failed login attempts from the same source IP address</div><div>I checked the authentication logs and saw many login failures from the same IP address. It was also detected that the same IP address was attempting to login for different users. Successful login looks suspicious after these failed login attempts.</div></div>					

Log Analysis

To verify the activity and assess the impact, the authentication and firewall logs were reviewed in **Log Management**. The analysis focused on identifying:

1. **Source IP activity** – checking all login attempts originating from **37.19.221.229**.
2. **Target system** – identifying which servers or services were accessed (VPN, SSH, RDP).
3. **Brute force indications** – repeated failed login attempts followed by a successful login.

Log Findings

Upon reviewing the authentication logs for the VPN server (vpn-letsdefend.io), multiple login attempts were observed from the attacker IP **37.19.221.229**:

1. Several attempts used **non-existent usernames** (sane@letsdefend.io, fane@letsdefend.io, zane@letsdefend.io, tane@letsdefend.io) – all of these attempts **failed**.
2. The attacker then focused on the **valid account** mane@letsdefend.io, generating multiple **failed login attempts** with incorrect passwords.
3. After repeated failures, the attacker successfully logged in as mane@letsdefend.io at **01:51 PM on June 21, 2023**.

And we can say that :

- *The attack clearly demonstrates a **brute force attempt**: trying multiple usernames, failing, then eventually successfully authenticating into a valid account.*
- *Targeted only the VPN service (port 443); no SSH (22) or RDP (3389) activity was observed.*

Destination Address contains "33.33.33.33"		All Time ↓	Q
✓ 39 events (before Feb, 13, 2024, 02:03 AM UTC)		< 1 2 3 4 >	
< Hide Fields	📄 Event		
INTERESTING FIELDS	▼ [Jun, 21, 2023, 01:45 PM] source_address=37.19.221.229 source_port=4508 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
α type	▼ [Jun, 21, 2023, 01:47 PM] source_address=37.19.221.229 source_port=3548 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
α source_address	▼ [Jun, 21, 2023, 01:48 PM] source_address=37.19.221.229 source_port=37004 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
# source_port	▼ [Jun, 21, 2023, 01:49 PM] source_address=37.19.221.229 source_port=46087 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
α destination_address	▼ [Jun, 21, 2023, 01:49 PM] source_address=37.19.221.229 source_port=4713 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
# destination_port	▼ [Jun, 21, 2023, 01:50 PM] source_address=37.19.221.229 source_port=44023 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
α raw_log	▼ [Jun, 21, 2023, 01:51 PM] source_address=37.19.221.229 source_port=45045 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
	▼ [Jun, 21, 2023, 01:44 PM] source_address=37.19.221.229 source_port=12435 destination_address=33.33.33.33 destination_port=443 raw_log: {D...		
1 row selected			

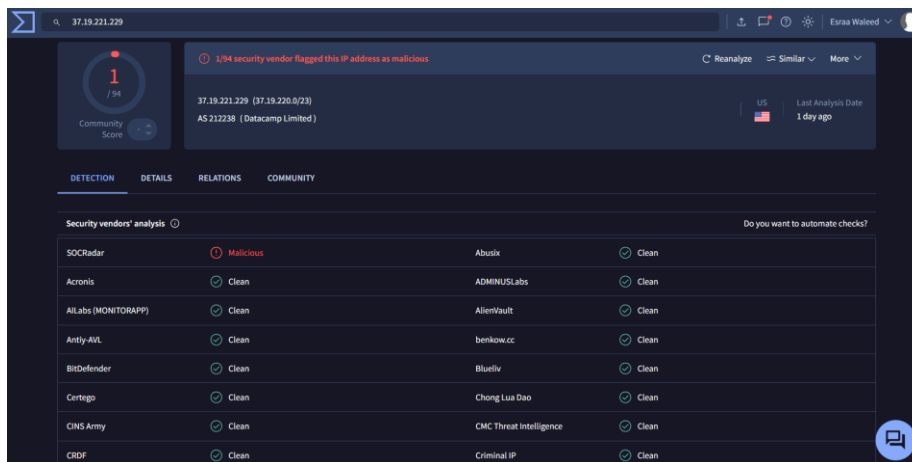
IP Enrichment – Combined Analysis

The attacker IP **37.19.221.229** was analyzed across multiple sources to assess its risk and context.

- **VirusTotal Analysis:**
 - **Community Score:** 1/94 security vendors flagged as malicious
 - **Detection Overview:** Only **SOCRadar** reported as malicious; all major security vendors (Abusix, Acronis, BitDefender, Fortinet, Google Safebrowsing, Sophos, etc.) reported the IP as clean.

- **Interpretation:** While only 1 vendor flagged it, the IP is considered **suspicious** due to the brute force activity observed on the VPN server.
- **AbuseIPDB Analysis:**
- **Reported Incidents:** 61 reports
 - **Confidence of Abuse:** 14%
 - **Interpretation:** Community reports confirm potential malicious activity such as brute force attacks and scanning.
 - **Additional Context / IP Information:**
 - **ISP / Organization:** Datacamp Limited
 - **Usage Type:** Data Center / Web Hosting / Transit
 - **ASN:** AS212238
 - **Hostname:** unn-37-19-221-229.datapacket.com
 - **Domain:** datacamp.co.uk
 - **Location:** Houston, Texas, United States

And this means: *The combined enrichment confirms that **37.19.221.229** is an **external and potentially malicious IP**, associated with data center hosting, and aligns with the observed **successful brute force attack**. Immediate actions such as **blocking the IP, monitoring network activity, and reviewing similar external connections** are recommended.*



Security vendors' analysis			
SOCRadar	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
All.labs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CNS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean

37.19.221.229 was found in our database!

This IP was reported **61** times. Confidence of Abuse is **14%**: [?](#)

14%

ISP	Datacamp Limited
Usage Type	Data Center/Web Hosting/Transit
ASN	AS212238
Hostname(s)	unn-37-19-221-229.datapacket.com
Domain Name	datacamp.co.uk
Country	us United States of America
City	Houston, Texas

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

REPORT 37.19.221.229

WHOIS 37.19.221.229

Enrichment & Context

The source IP address **37.19.221.229** is **external** to the organization's network.

Supporting Details:

- **ISP / Organization:** Datacamp Limited
- **Usage Type:** Data Center / Web Hosting / Transit
- **ASN:** AS212238
- **Hostname:** unn-37-19-221-229.datapacket.com
- **Domain Name:** datacamp.co.uk
- **Location:** Houston, Texas, United States
- **Threat Intelligence:**
 - **VirusTotal:** 1/94 vendors flagged as malicious (SOCRadar)
 - **AbuseIPDB:** Reported 61 times with 14% confidence of abuse

The attacker IP is confirmed to be **external** and associated with hosting infrastructure, which aligns with observed malicious activity (brute force attack on VPN). This confirms the need for immediate containment actions, including **IP blocking and monitoring**.

Containment & Mitigation Actions

Following the detection of a **successful brute force attack** from attacker IP **37.19.221.229**, the following containment actions were implemented to reduce impact and prevent further compromise:

1. Account Lock & Password Reset

- The targeted VPN account mane@letsdefend.io was **disabled/locked** immediately after detecting suspicious login activity.
- The account password was **reset** to prevent unauthorized access.

2. IP Blocking

- The malicious IP **37.19.221.229** was **blocked** on the firewall and VPN.
- This prevents any further login attempts or lateral movement from this external source.

3. Session Termination

- All active sessions associated with the compromised account were **terminated** to ensure the attacker could not maintain access.

4. Device Isolation Assessment

- The VPN server was **assessed** for compromise.
- Since no evidence of lateral movement, malware deployment, or additional service compromise was found, **full isolation of the device was not required**.
- The system continues to be **monitored** closely for any suspicious activity.

5. Monitoring & Review

- Continuous monitoring of authentication and network logs is in place to detect any further suspicious attempts.
- Any similar external IPs attempting multiple login attempts will be **reviewed and blocked** as necessary.

Lessons Learned

1. How did the cyber attack happen?

- The attack was a **brute force attempt** targeting the organization's VPN server (vpn-letsdefend.io) on port 443.
- The attacker IP **37.19.221.229** tried multiple usernames, including invalid accounts, before successfully compromising the valid account mane@letsdefend.io.
- The attack leveraged **credential guessing** rather than exploiting system vulnerabilities.

2. How well did staff and management perform in dealing with the incident?

- The Security Operations team **quickly identified** the suspicious activity using log monitoring and alerting (SOC210 rule).
- Immediate containment actions were taken: account lock, password reset, IP blocking, and session termination.

- The team **effectively minimized the impact**, preventing further compromise.

3. What would the staff and management do differently the next time a similar incident occurs?

- **Implement stricter password policies** and enforce multi-factor authentication (MFA) for VPN accounts to reduce the risk of brute force success.
- **Increase alert sensitivity** for repeated failed logins from external IPs, even if only a single account is targeted.
- **Automate immediate blocking** of suspicious IPs to shorten response time.

4. What corrective actions can prevent similar incidents in the future?

- Enforce **MFA** for all remote access accounts.
- Apply **rate limiting or lockout policies** for repeated failed login attempts.
- Maintain an updated **threat intelligence database** to preemptively block known malicious IPs.
- Conduct **regular staff training** on security awareness and incident reporting.

5. What precursors or indicators should be watched for in the future to detect similar incidents?

- Multiple failed login attempts from **external IP addresses** targeting multiple accounts.
- Successful login immediately following repeated failures from the same IP.
- Unusual login times or locations for VPN accounts.
- Alerts from threat intelligence sources (VirusTotal, AbuseIPDB) about suspicious IPs attempting access.

After thorough investigation of the VPN brute force incident involving the external IP 37.19.221.229, the following observations and actions were recorded:

- Multiple login attempts targeting different usernames were detected, with a **successful login on mane@letsdefend.io** after repeated failures.
- The source IP is **external**, associated with **Datacamp Limited**, located in Houston, Texas, USA, and has been reported for malicious activity in threat intelligence databases (VirusTotal & AbuseIPDB).
- Immediate containment actions were implemented:
 - Compromised account **locked and password reset**
 - **IP blocked** on firewall/VPN
 - **Active sessions terminated**
- No evidence of lateral movement or compromise of other servers/services was found.
- Continuous monitoring remains in place to detect any further suspicious activity.

Conclusion / Analyst Recommendation:

- The incident was **successfully contained** with minimal impact.
- Implement **MFA for all VPN accounts** and enforce strong password policies.
- Monitor for repeated failed login attempts and any new suspicious IPs.
- Maintain updated threat intelligence and integrate automated alerts for faster response.

Overall Assessment:

The Security Operations team performed effectively, responding promptly and taking all necessary containment measures. Future incidents can be mitigated further with stronger authentication controls and proactive monitoring

×

Add Artifacts

+

Value	Comment	Type	Remove
37.19.221.229	Attacker IP used in b	IP Address	
mane@letsdefend.i	Compromised VPN a	E-mail Senc	
letsdefend.io	Domain of comprom	E-mail Dom	
https://www.abusei	61 reports, 14% confid	URL Addres	
https://www.virustot	1/94 vendors flagged	URL Addres	
Firewall /VPN block	IP blocked to prevent	MD5 Hash	
<u>session termination</u>	All active sessions of	MD5 Hash	

Next