



Official Incident Report

Event ID: 162

Rule Name: SOC210 - Possible Brute Force Detected on VPN

Table of contents

Official Incident Report	1
Event ID: 162	1
Rule Name: SOC210 - Possible Brute Force Detected on VPN	1
Table of Contents	2
Alert	3
Detection	4
Verify	4
IP Reputation	6
Initial Access	7
Containment	11
Lesson Learned	11
Appendix	12
MITRE	12
Artifacts	12

Alert

The alert was triggered due to a successful login from the same source IP address in a short period of time after failed login activities. When the L1 Analyst's note was analyzed, it was determined that there were attempts with different usernames from the same Source IP (37[.]19.221.229) and that it was successful with the user named Mane.

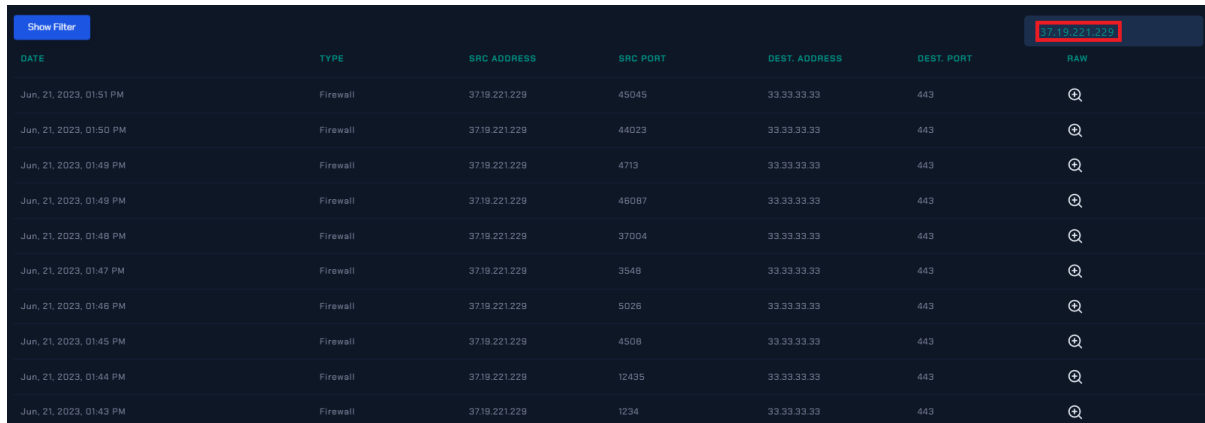
SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Jun, 21, 2023, 01:51 PM	SOC210 - Possible Brute Force Detected on VPN	162	Brute Force	
EventID : 162					
Event Time : Jun, 21, 2023, 01:51 PM					
Rule : SOC210 - Possible Brute Force Detected on VPN					
Level : Security Analyst					
Source Address : 37.19.221.229					
Destination Address : 33.33.33.33					
Destination Hostname : Mane					
Username : mane@letsdefend.io					
Alert Trigger Reason : A successful VPN login was detected shortly after failed login attempts from the same source IP address					
L1 Note : 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.					

First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

Verify

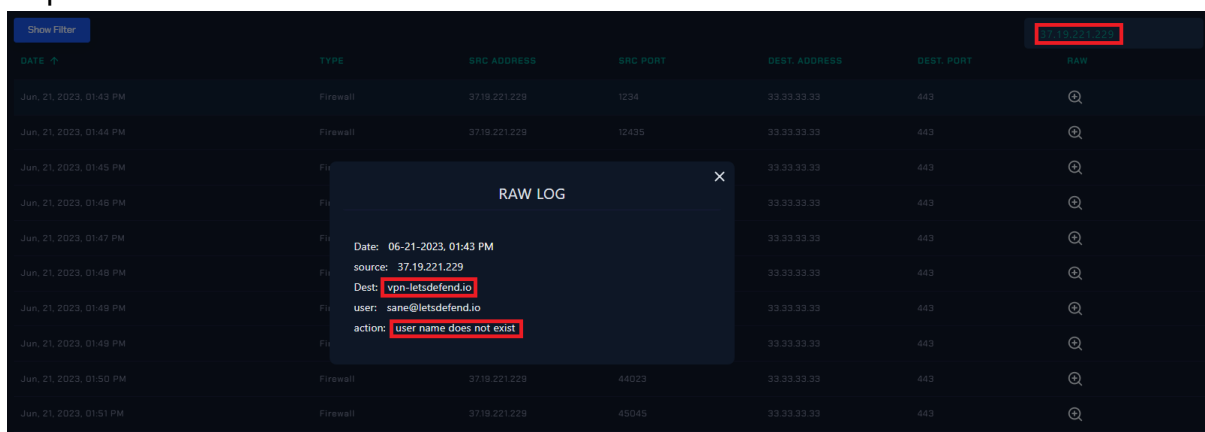
In Log Management, search for the source IP address (37.[.]19.221.229) in the alert and examine the logs among the results. This way, all logs belonging to the attacker IP are seen. As a result, Firewall logs were seen.



The screenshot shows a log management interface with a table of firewall logs. The table has columns for DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. The SRC ADDRESS column is filtered to show only logs from 37.19.221.229. The logs show various firewall events, including connections and disconnections, with timestamps ranging from 01:43 PM to 01:51 PM on June 21, 2023.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 21, 2023, 01:51 PM	Firewall	37.19.221.229	45045	33.33.33.33	443	🔍
Jun, 21, 2023, 01:50 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	4713	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	48087	33.33.33.33	443	🔍
Jun, 21, 2023, 01:48 PM	Firewall	37.19.221.229	37004	33.33.33.33	443	🔍
Jun, 21, 2023, 01:47 PM	Firewall	37.19.221.229	3548	33.33.33.33	443	🔍
Jun, 21, 2023, 01:46 PM	Firewall	37.19.221.229	5028	33.33.33.33	443	🔍
Jun, 21, 2023, 01:45 PM	Firewall	37.19.221.229	4508	33.33.33.33	443	🔍
Jun, 21, 2023, 01:44 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun, 21, 2023, 01:43 PM	Firewall	37.19.221.229	1234	33.33.33.33	443	🔍

When the traffic from 37.[.]19.221.229 IP located in the USA was examined in detail, it was seen that "sane@letsdefend.io", "zane@letsdefend.io", "fane@letsdefend.io" and "tane@letsdefend.io" were used in incoming requests. It was seen that FW "user name does not exist" response was returned in these requests.



The screenshot shows a log management interface with a table of firewall logs. The table has columns for DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. The SRC ADDRESS column is filtered to show only logs from 37.19.221.229. A 'RAW LOG' modal is open, displaying details for a specific log entry. The modal shows the date, source IP, destination IP, user, and action. The action is 'user name does not exist'.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 21, 2023, 01:43 PM	Firewall	37.19.221.229	1234	33.33.33.33	443	🔍
Jun, 21, 2023, 01:44 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun, 21, 2023, 01:45 PM	Firewall	37.19.221.229	4508	33.33.33.33	443	🔍
Jun, 21, 2023, 01:46 PM	Firewall	37.19.221.229	5028	33.33.33.33	443	🔍
Jun, 21, 2023, 01:47 PM	Firewall	37.19.221.229	3548	33.33.33.33	443	🔍
Jun, 21, 2023, 01:48 PM	Firewall	37.19.221.229	48087	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	4713	33.33.33.33	443	🔍
Jun, 21, 2023, 01:50 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:51 PM	Firewall	37.19.221.229	45045	33.33.33.33	443	🔍

RAW LOG

Date: 06-21-2023, 01:43 PM

source: 37.19.221.229

Dest: vpn-letsdefend.io

user: sane@letsdefend.io

action: user name does not exist

The request from the same IP at 01:47 PM returned the response "user name is correct but the password is wrong". With this information, the attacker has obtained that there is a user named "mane[.]@letsdefend.[.]io" in the "vpn-letsdefend.io" structure. Therefore, they will continue with different passwords over the username "mane[.]@letsdefend.[.]io" in their next requests.

Show Filter						
DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun. 21, 2023, 01:43 PM	Firewall	37.19.221.229	1234	33.33.33.33	443	🔍
Jun. 21, 2023, 01:44 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:45 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:46 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:47 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:48 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:49 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun. 21, 2023, 01:50 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun. 21, 2023, 01:51 PM	Firewall	37.19.221.229	45045	33.33.33.33	443	🔍

RAW LOG

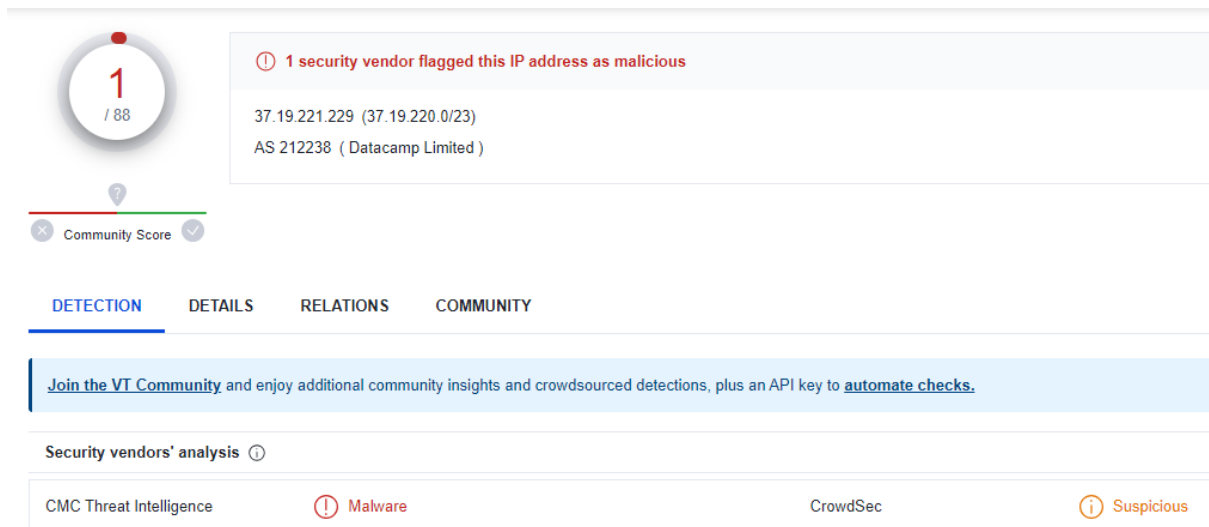
Date: 06-21-2023, 01:47 PM
source: 37.19.221.229
Dest: vpn-letsdefend.io
user: mane@letsdefend.io
action: user name is correct but the password is wrong

The requests received with the username "mane[@]letsdefend[.]io" show that at 01:51 PM, the attacker received "Login Successful" action in FW. Thus, the alert can be called True Positive.

Analysis

IP Reputation

The attacker IP address is an external IP address. Therefore, the validity of the analysis can be strengthened by performing a reputation check.



The image shows the VirusTotal IP reputation interface. On the left, there is a circular gauge with a red needle pointing to '1' out of 88, labeled 'Community Score'. To the right, a warning message states: '1 security vendor flagged this IP address as malicious'. Below this, the IP address '37.19.221.229 (37.19.220.0/23)' and its AS 'AS 212238 (Datacamp Limited)' are listed. A navigation bar includes 'DETECTION', 'DETAILS', 'RELATIONS', and 'COMMUNITY'. A blue banner encourages joining the VT Community. Under 'Security vendors' analysis', a table shows results from CMC Threat Intelligence (Malware), CrowdSec, and Suspicious.

Security vendors' analysis
CMC Threat Intelligence
Malware
CrowdSec
Suspicious

<https://www.virustotal.com/gui/ip-address/37.19.221.229>



The image shows the AbuseIPDB IP reputation interface. At the top, it states '37.19.221.229 was found in our database!'. Below, it says 'This IP was reported 14 times. Confidence of Abuse is 20%'. A progress bar shows 20% confidence. A table lists details: ISP (DataCamp Limited), Usage Type (Data Center/Web Hosting/Transit), Hostname(s) (unn-37-19-221-229.datapacket.com), Domain Name (datacamp.co.uk), Country (United States of America), and City (Houston, Texas).

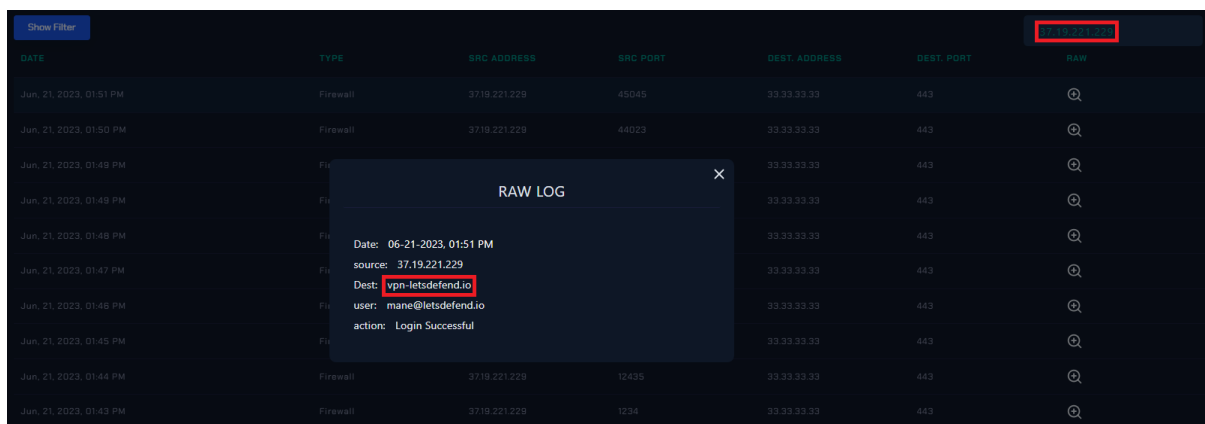
ISP	DataCamp Limited
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	unn-37-19-221-229.datapacket.com
Domain Name	datacamp.co.uk
Country	United States of America
City	Houston, Texas

<https://www.abuseipdb.com/check/37.19.221.229>

The query on Virus Total showed that the IP has been reported as both Suspicious and Malware by two different sources in the past. According to AbusIPDB, it has a 20% risk record. It was reported by different sources in categories such as E-mail spam, phishing, and Brute Force.

Initial Access

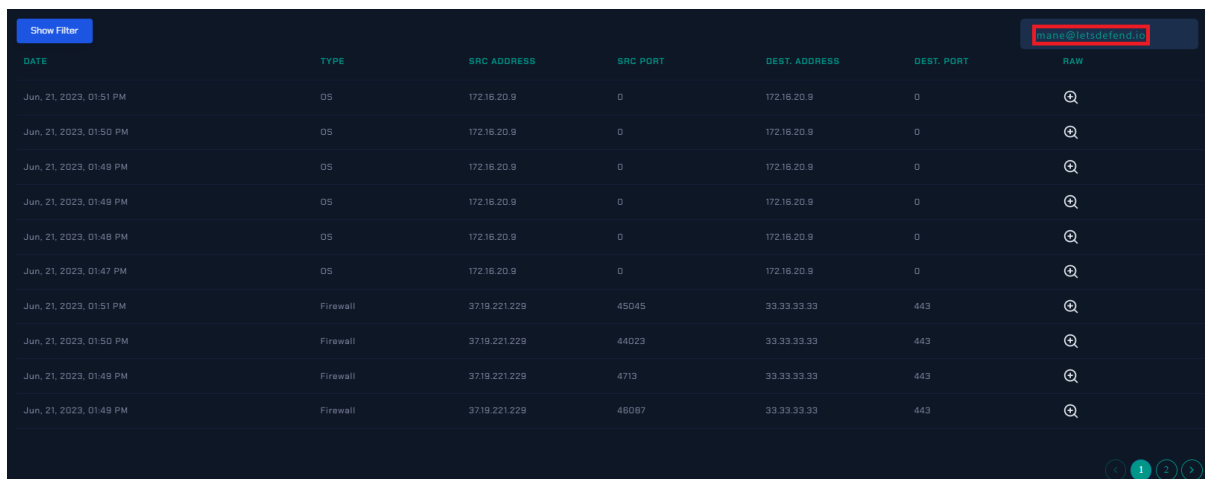
When the logs of the attacker IP 37[.]19.221.229 were analyzed in Log Management, requests to the address "vpn-letsdefend.io" were seen. The system was logged in to the relevant address with Brute Force with multiple users. Thus, it can be said that "External Remote Services(T1133)" technique was used for initial access.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 21, 2023, 01:51 PM	Firewall	37.19.221.229	45045	33.33.33.33	443	🔍
Jun, 21, 2023, 01:50 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:48 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:47 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:46 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:45 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:44 PM	Firewall	37.19.221.229	12435	33.33.33.33	443	🔍
Jun, 21, 2023, 01:43 PM	Firewall	37.19.221.229	1234	33.33.33.33	443	🔍

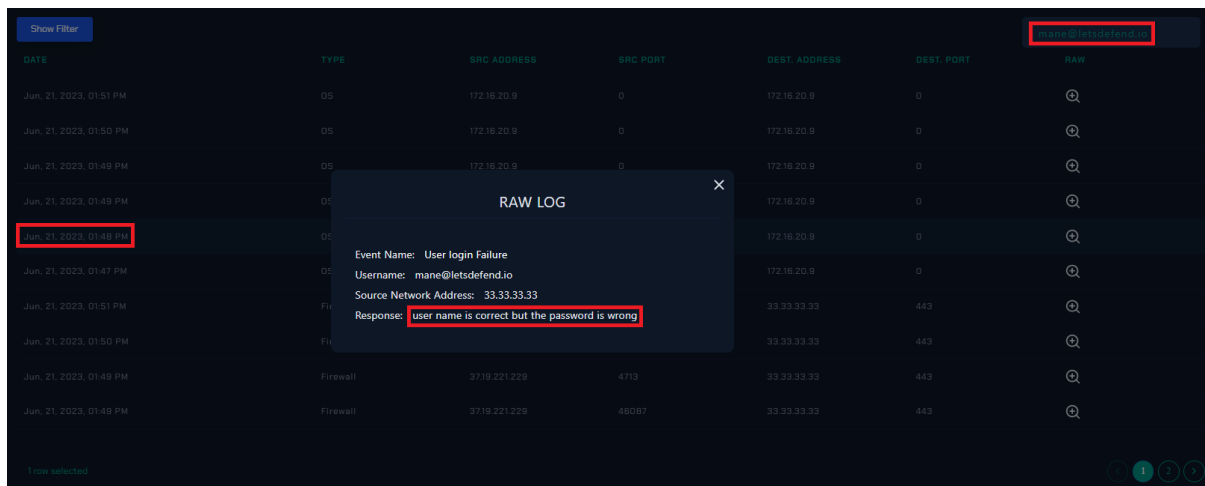
RAW LOG
Date: 06-21-2023, 01:51 PM
source: 37.19.221.229
Dest: vpn-letsdefend.io
user: mane@letsdefend.io
action: Login Successful

The analysis so far has been made on the IP belonging to the attacker. If you search victim(mane[@]letsdefend[.]io) on Log Management, you can see OS logs as well as FW logs.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 21, 2023, 01:51 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:50 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:49 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:49 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:48 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:47 PM	OS	172.16.20.9	0	172.16.20.9	0	🔍
Jun, 21, 2023, 01:51 PM	Firewall	37.19.221.229	45045	33.33.33.33	443	🔍
Jun, 21, 2023, 01:50 PM	Firewall	37.19.221.229	44023	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	4713	33.33.33.33	443	🔍
Jun, 21, 2023, 01:49 PM	Firewall	37.19.221.229	48087	33.33.33.33	443	🔍

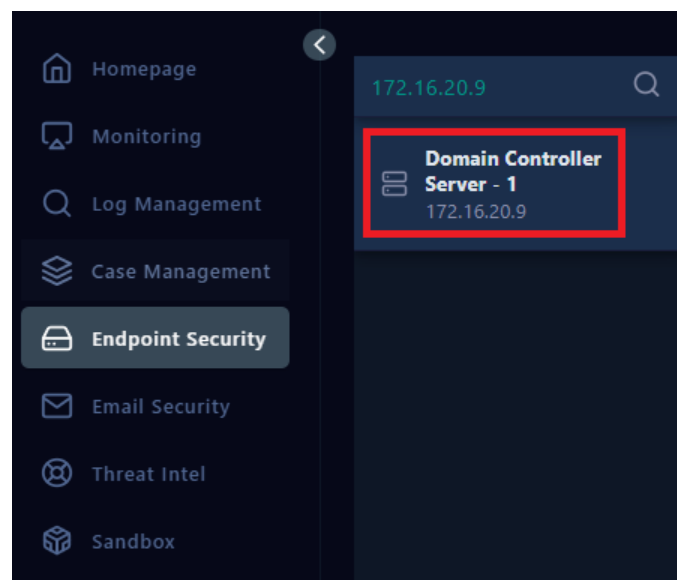
You should examine the OS logs in detail to deepen the analysis. The source IP appears as 172[.]16.20.9 in OS logs. You can search on Endpoint Security to get information about the related IP.

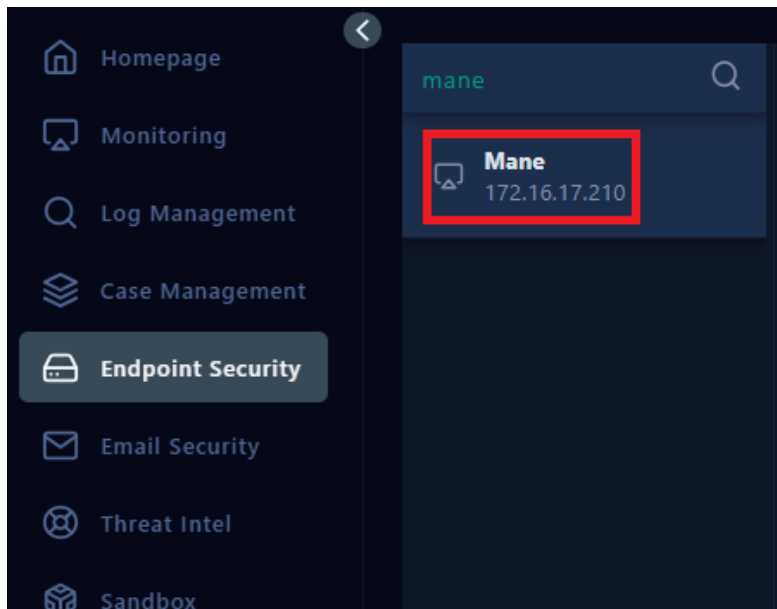


The screenshot shows a log management interface with a table of logs. A 'RAW LOG' popup is displayed over one of the log entries. The table has columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST ADDRESS, DEST PORT, and RAW. The log entry selected in the popup is dated Jun. 21, 2023, 01:46 PM, with TYPE OS, SRC ADDRESS 172.16.20.9, SRC PORT 0, DEST ADDRESS 172.16.20.9, and DEST PORT 0. The popup shows the following details:

- Event Name: User login Failure
- Username: mane@letsdefend.io
- Source Network Address: 33.33.33.33
- Response: User name is correct but the password is wrong

As a result of the search, it was seen that the relevant IP belongs to the Domain Controller. So what is the IP information of the user named "mane[@]letsdefend[.]io"? For this, you can make a search on Endpoint Security. As a result of the search, it was seen that the IP information of the relevant User was 172[.]16.17.210.





Upon further examination on Log Management, it was seen that the OS logs belong to the Domain Controller. As seen in the screenshot below, the Source Network Address information can be used to determine from which address this request was made to the Domain Controller. Previously, it was observed in the firewall logs that the IP address 33[.]33.33.33 belonged to vpn.letsdefend.io.

The screenshot shows a log management interface with a table of logs. A 'RAW LOG' popup window is open, displaying details for a specific event. The table has columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST ADDRESS, DEST PORT, and RAW. The popup window shows the following details:

- Event Name: Authentication success
- Username: mane@letsdefend.io
- Source Network Address: 33.33.33.33
- Response: Login Successful

The table below shows several log entries, with the last two rows highlighted in red in the original image:

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST ADDRESS	DEST PORT	RAW
Jun. 21, 2023, 01:51 PM	OS	172.16.20.9	0	172.16.20.9	0	[icon]
Jun. 21, 2023, 01:50 PM	OS	172.16.20.9	0	172.16.20.9	0	[icon]
Jun. 21, 2023, 01:49 PM	OS	172.16.20.9	0	172.16.20.9	0	[icon]
Jun. 21, 2023, 01:48 PM	OS	172.16.20.9	0	172.16.20.9	0	[icon]
Jun. 21, 2023, 01:47 PM	OS	172.16.20.9	0	172.16.20.9	0	[icon]
Jun. 21, 2023, 01:51 PM	FW	33.33.33.33	443	33.33.33.33	443	[icon]
Jun. 21, 2023, 01:50 PM	FW	33.33.33.33	443	33.33.33.33	443	[icon]
Jun. 21, 2023, 01:49 PM	Firewall	3719.221.229	4713	33.33.33.33	443	[icon]
Jun. 21, 2023, 01:48 PM	Firewall	3719.221.229	48087	33.33.33.33	443	[icon]

The above log shows that the Domain Controller received a successful response for the login request for mane[.]letsdefend[.]io via VPN. This proved that the attacker successfully VPN logged into the system via mane[.]letsdefend[.]io. So why was a second check done here? The reason for this is to check whether there is MFA (Multi-factor authentication) in the structure.

#Multi-factor authentication (MFA), also known as two-factor authentication (2FA) or strong authentication, is a security mechanism that requires users to provide multiple forms of identification or credentials to verify their identity when

accessing a system, service, or application. It adds an extra layer of protection beyond just using a username and password combination.

If there was MFA in the structure, even if the attacker managed to pass the password of mane[[@](mailto:mane@letsdefend.io)]letsdefend[.]io with a brute force attack, they would not be able to access the system because there would need to be a second authentication. Since the second authentication here would be transmitted to the user by OTP (one-time passwords) via message/email, the attacker would not be able to access the system because they would not be able to enter this password. Of course, this applies to the case where the information of the structure in the second verification method does not fall into the hands of the attacker.

It was observed that the attacker received a "user name does not exist" response for users with which they tried to log in before the mane[[@](mailto:mane@letsdefend.io)]letsdefend[.]io user. Can this be confirmed from the platform? You can make a search on Endpoint Security for this. As a result of the search, it was seen that there were no results for all four users.

sane@letsdefend.io

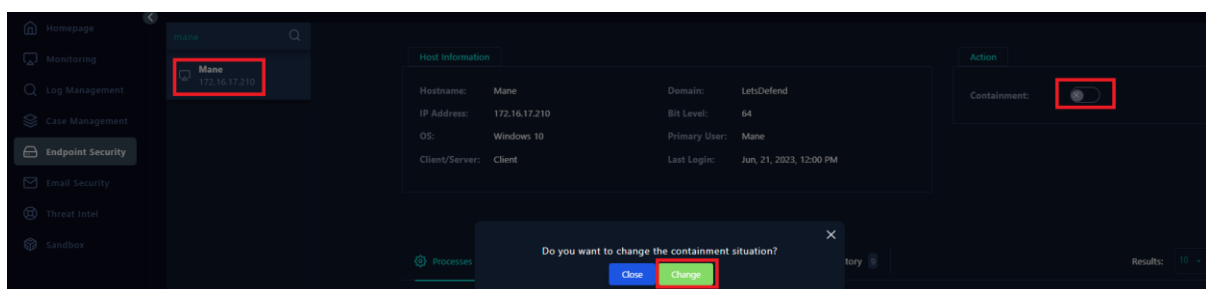
zane@letsdefend.io

fane@letsdefend.io

tane@letsdefend.io

Containment

The relevant host should be isolated from the network since it is certain that the attacker successfully logged into the system. To do this, go to the host named Mane via Endpoint Security and click on "containment". An example is shared below.



Lesson Learned

- Especially in structures open to the outside world, MFA (Multi-Factor Authentication) must be active.
- It is recommended to set a strong password policy on clients and servers.
- End users should be trained periodically to raise awareness on information security.

Appendix

MITRE

Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/1)
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access
Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)
Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)
Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/6)
Valid Accounts (0/4)	Serverless Execution	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception
	Shared Modules	External Remote Services		Execution Guardrails (0/1)	
				Exploitation for Defense Evasion	

MITRE Tactics	MITRE Techniques
Initial Access	Valid Accounts(T1078)
Credential Access	Brute Force(T1110)

Artifacts

Field	Value
Attacker IP Address	37[.]19.221.229
User	mane[@]letsdefend[.]io