Author: Jack Fitzgerald

Official Incident Report

Date: Feb, 13, 2024, 02:04 AM

Event ID: 225

Rule Name: SOC257 - VPN Connection Detected from Unauthorized Country

Table of Contents

Alert Details

Severity: Low

Source Address: 113.161.158.12

Destination Address: 33.33.33.33

Destination Hostname: Monica

Username: monica@letsdefend.io

Alert Trigger Reason: Vpn Connection Detected from Unauthorized Country

URL: https://vpn-letsdefend.io

Based on the information provided in the alert, it appears that a VPN connection was detected from an unauthorised country. The alert is triggered by rule SOC257 - VPN Connection Detected from Unauthorized Country.

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.

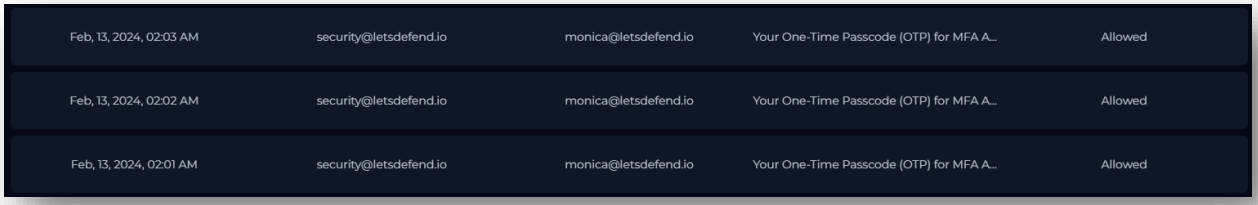
Detection

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 investigate the VPN connection.

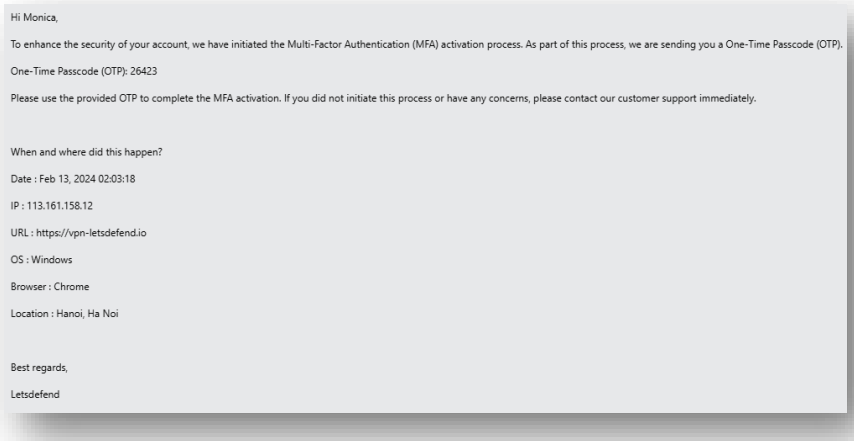
A VPN, which stands for virtual private network, establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet.

Our first step is to identify any emails that were sent to **monica@letsdefend.io**.



Feb, 13, 2024, 02:03 AM	security@letsdefend.io	monica@letsdefend.io	Your One-Time Passcode (OTP) for MFA A...	Allowed
Feb, 13, 2024, 02:02 AM	security@letsdefend.io	monica@letsdefend.io	Your One-Time Passcode (OTP) for MFA A...	Allowed
Feb, 13, 2024, 02:01 AM	security@letsdefend.io	monica@letsdefend.io	Your One-Time Passcode (OTP) for MFA A...	Allowed

There were 3 identified emails sent to this inbox from **security@letsdefend.io**, from 02:01 – 02:03 AM, providing OTP for MFA. The email notifies an MFA request from IP **113.161.158.12** coming from URL **https://vpn-letsdefend.io** from **Hanoi**, Ha Noi.



Hi Monica,

To enhance the security of your account, we have initiated the Multi-Factor Authentication (MFA) activation process. As part of this process, we are sending you a One-Time Passcode (OTP).

One-Time Passcode (OTP): 26423

Please use the provided OTP to complete the MFA activation. If you did not initiate this process or have any concerns, please contact our customer support immediately.

When and where did this happen?

Date : Feb 13, 2024 02:03:18

IP : 113.161.158.12

URL : https://vpn-letsdefend.io

OS : Windows

Browser : Chrome

Location : Hanoi, Ha Noi

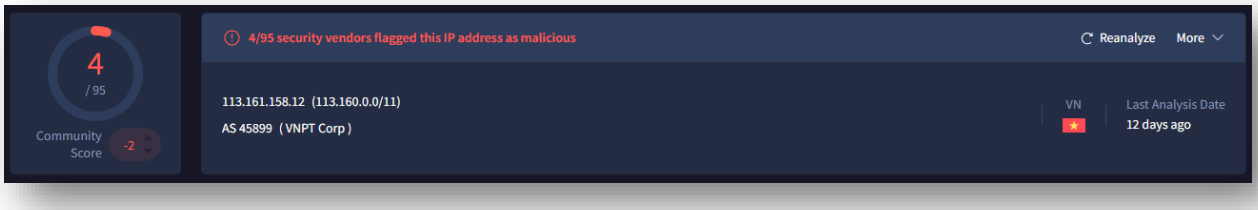
Best regards,

Letsdefend

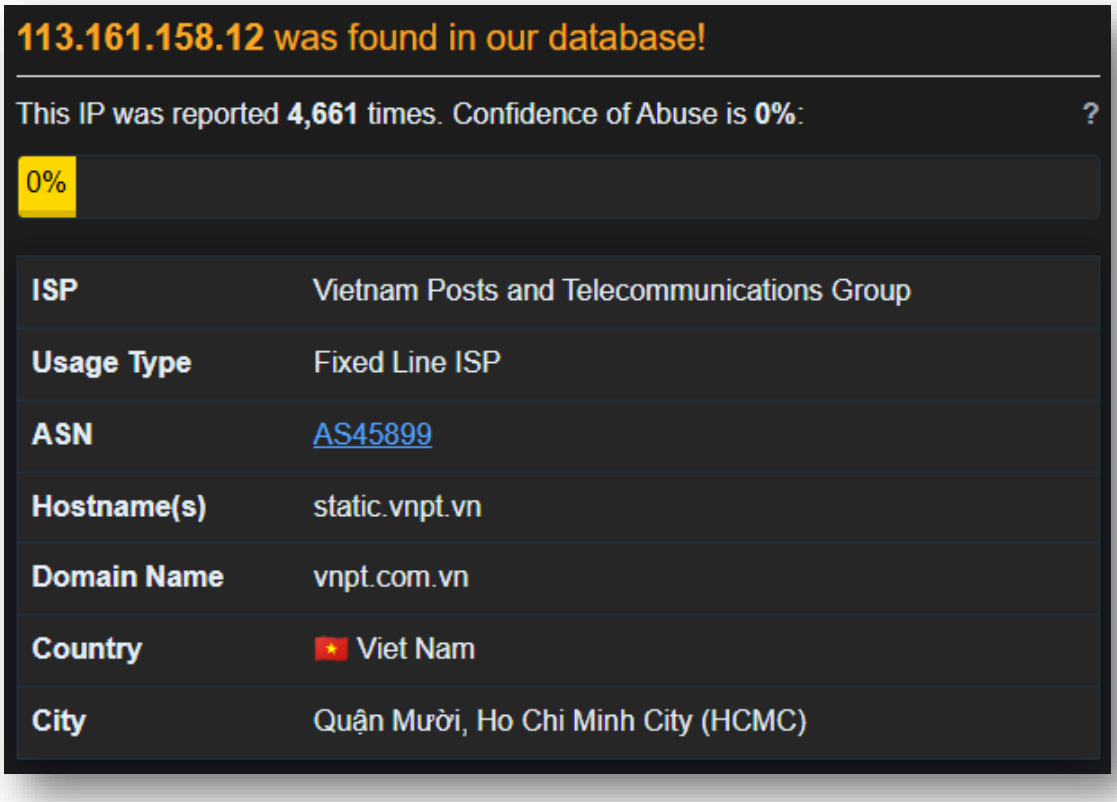
Analysis

Now that we have detected the alert and its details, we can start by analyzing the IP found in the email.

https://www.virustotal.com/gui/ip-address/113.161.158.12



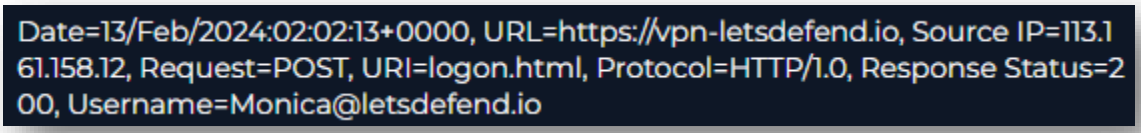
https://www.abuseipdb.com/check/113.161.158.12



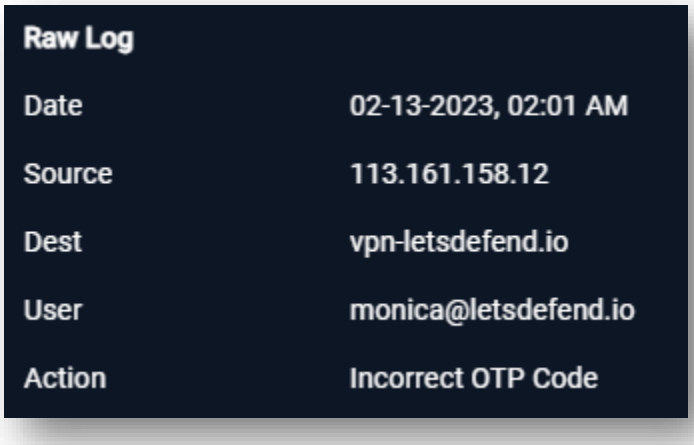
These analyses show indicators of **brute force attacks through SSH**, which match the MFA OTP requests through Monica's inbox.

Next, we will investigate Log Management to find any further details of the alert. There were 21 events (before Feb, 13, 2024, 02:03 AM UTC).

The logs show user Monica was logged in with status 200 from the malicious IP **113.161.158.12**.



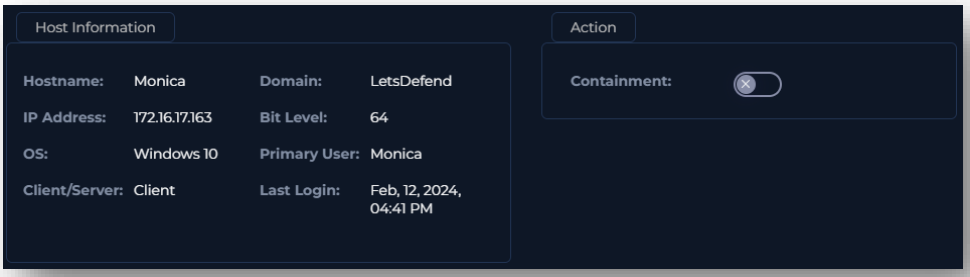
The logs show incorrect OTP codes were used.



These logs show that no password was used in the initial login attempt; however, **OTP MFA prevented the attacker from gaining unauthorised access** into the Monica account.

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 an attempt to compromise a system named **Monica** with an IP address of **172.16.17.163**. The alert was triggered by the detection of an unauthorised VPN connection from Vietnam, based on the rule SOC257 - VPN Connection Detected from Unauthorized Country.

The identified email contained OTP for MFA from the security team at letsdefend, due to the multiple connection attempts from IP **113.161.158.12**. This IP has been reported for brute force attacks via SSH.

Investigating the logs showed that the attacker successfully used the username for Monica@letsdefend.io, however, was prevented from gaining access to the account due to the MFA setup by the letsdefend security team.

Based on the findings of the incident, no immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Proactively block connection attempts from countries that are on a ‘no-access’ list

- Treat all VPN traffic as untrusted and potentially malicious, terminate VPN connections within a DMZ (Demilitarized Zone) to allow for proper inspection and auditing of unencrypted traffic before it can access the internal network

Remediation Actions

- Force a password reset for the account

- Add the unauthorized VPN's IP range to the network's block list or firewall rules to prevent future access attempts

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1133 - External Remote Services
Initial Access	T1078 - Valid Accounts

Artifacts

Value	Comment	Type
113.161.158.12	Unauthorised VPN connection from Vietnam	IP Address

LetsDefend Playbook

LetsDefend Event ID: 225