Author: Jack Fitzgerald

Official Incident Report

Date: Jan, 01, 2024, 12:37 PM

Event ID: 214

Rule Name: SOC251 - Quishing Detected (QR Code Phishing)

Table of Contents

Alert Details

Severity: Medium

Type: Exchange

SMTP Address: 158.69.201.47

Source Address: security@microsecmfa.com

Destination Address: Claire@letsdefend.io

E-mail Subject: New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious **QR code phishing email** sent to **Claire@letsdefend.io** has been detected. The alert is triggered by rule SOC251 - Quishing Detected (QR Code Phishing).

Upon reviewing the alert, it is observed that an email with the subject **New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)** was sent from **security@microsecmfa.com** with an SMTP of **158.69.201.47**.

The device action is marked **allowed**, indicating that the email was delivered to the **Claire@letsdefend.io** inbox.

Overall, it appears that the email 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

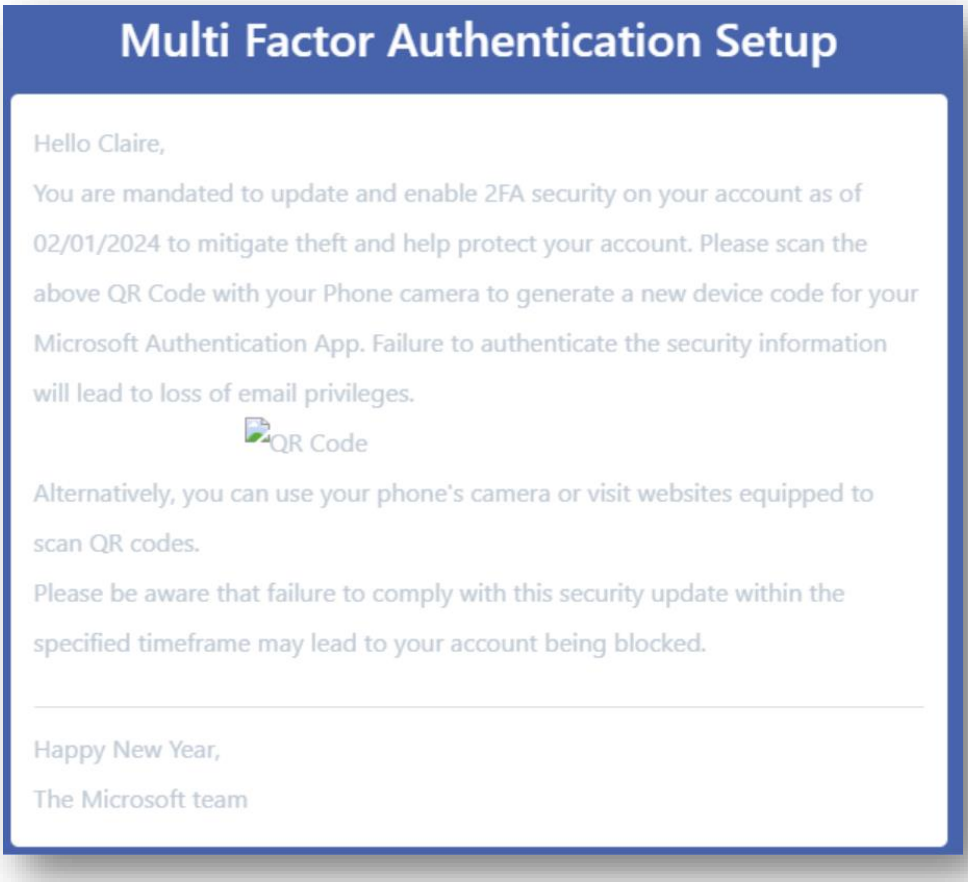
As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

It is important to check the Email Security product and analyze QR code to reveal evil. QR codes can be scanned by users' personal devices, like phones. So, there might not be logs every time about the related host.

Alarms escalated from Tier1 to Tier2 should be caused by a truly harmful event, but escalated alarms by Tier1 analysts are not always True Positive due to technical inadequacy, faulty/incomplete analysis, and authorization problems. Before initiating Incident Response processes, please verify that the alarm from the Tier1 analyst was caused by malicious activity.

Reconnaissance is an important phase of an attack where the attacker gathers information about the target system and network. This playbook aims to identify potential reconnaissance activity.

By searching for the email sender of **security@microsecmfa.com** in Email Security, we can find the email and some further details.



Email Indicators:

- Identifiable as a phishing email, more specifically a quishing email (QR code phishing)
- Asks the user to generate a new device code for an authentication app using a QR code
- Threatens loss of email privileges, if actions are not performed
- Directs the user to use a different device, to obfuscate activity (no log data about the related host)
- The “t” in “The Microsoft team” is not even capitalized, need to educate users on identifying email phishing attacks
- This should never happen, and is not standard Microsoft procedure

The first step we take when investigating a potential phishing email is to parse the email information.

When was it sent?

Jan, 01, 2024, 12:00 PM

What is the email's SMTP address?

158.69.201.47

What is the sender's address?

security@microsecmfa.com

What is the recipient's address?

Claire@letsdefend.io

After analyzing the QR with **CyberChef**, we attain the URL that the QR code sends you to **https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#**.

https://www.virustotal.com/gui/url/65b3237d11b6668f5b2278f0d3bd44c9831941f99e08ffda297cc27c6a9fafd1

8/98 security vendors flagged this URL as malicious

The URL serves **209.94.90.1** IP address.

Analysis

Identify the relevant log sources to be analyzed for the discovery activity (e.g. firewall, proxy, event, Sysmon, etc.). Checks can be provided on the Log Management page for related searches.

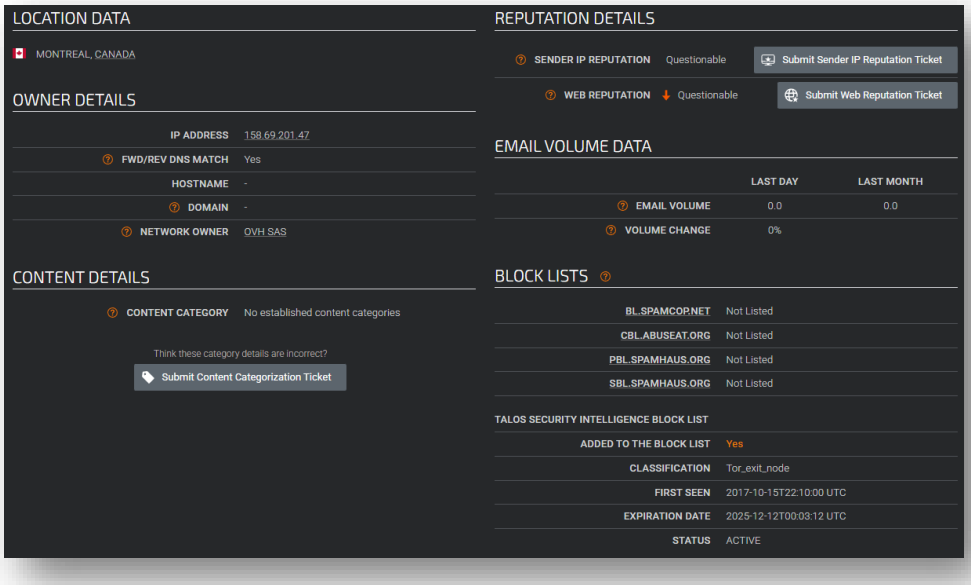
Look for any unusual or suspicious domain name requests. Check for any unusual or suspicious HTTP requests. Look for any unusual or suspicious DNS requests. Against phishing for information, check email security. You can check Endpoint Security and Email Security for related searches.

The first step is to analyse the SMTP address **158.69.201.47** provided. We upload this to online analysis tools such as **VirusTotal** and **Talos Intelligence** to determine its behaviour and whether this address is malicious.

https://www.virustotal.com/gui/ip-address/158.69.201.47

6/95 security vendors flagged this IP address as malicious

https://talosintelligence.com/reputation_center/lookup?search=158.69.201.47

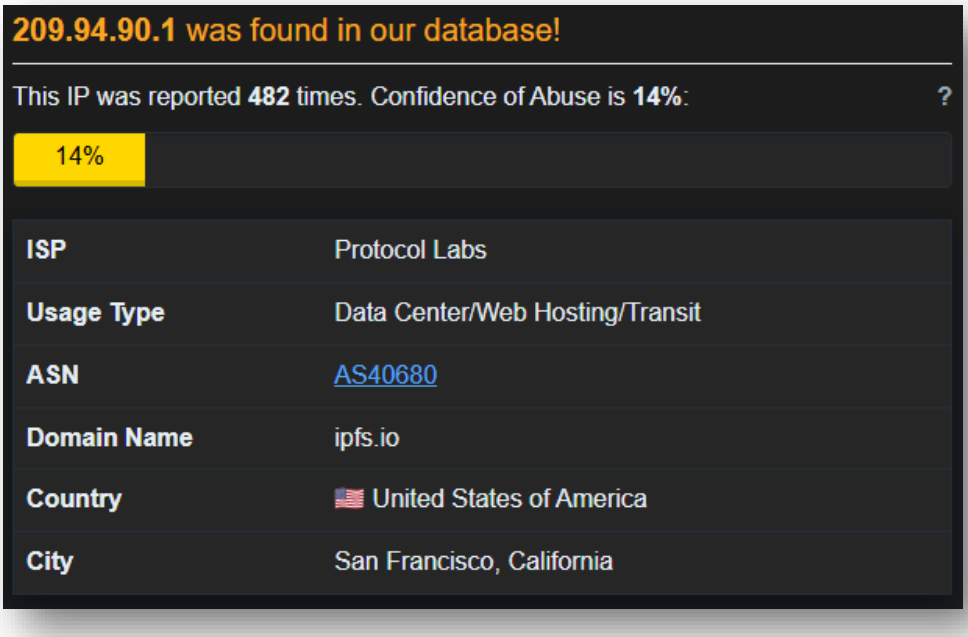


The next step is to analyse the QR code URL IP address.

https://www.virustotal.com/gui/ip-address/209.94.90.1

7/95 security vendors flagged this IP address as malicious

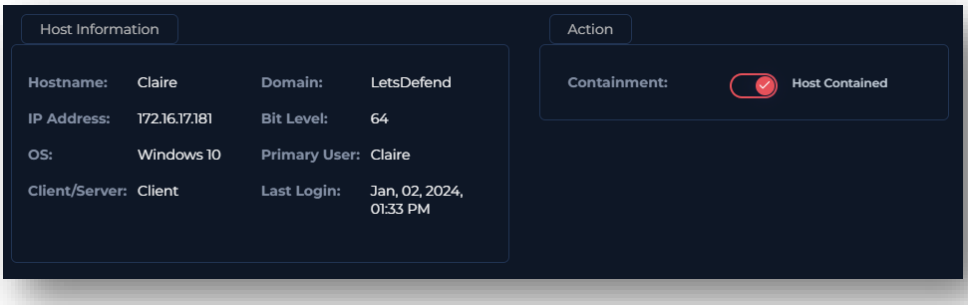
https://www.abuseipdb.com/check/209.94.90.1



Reports indicate that this IP is hosting a fake (phishing) login page – presumably imitating a Microsoft login page.

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 to prevent further spread of malicious content.



Summary

The incident involves a compromised system called **Claire**. The alert was triggered by the detection of a suspicious **QR code phishing email**, sent to **Claire@letsdefend.io**, based on the rule SOC251 - Quishing Detected (QR Code Phishing).

Claire@letsdefend.io received a malicious phishing email containing a QR code from IP address **158.69.201.47**. The email was not quarantined and allowed to be served to the user's inbox. The email impersonates **Microsoft**, requesting the user to visit the link from the QR code to generate a new device code for the Microsoft Authentication App. The SMTP address was confirmed as suspicious by various security vendors and online analysis tools.

In future, please block incoming emails containing QR codes, and require manual inspection from a security officer before forwarding to the end user. Please educate users on identifying and reporting suspicious emails.

Lessons Learned

- Suspicious sender addresses should be watched for
- QR code phishing is a new attack vector that users are not familiar with

Remediation Actions

- Delete the identified email from the user's inbox and maintain a block to the email sender and associated IPs
- Conduct targeted security awareness training, focusing on social engineering recognition and reporting suspicious emails promptly
- Run simulated phishing campaigns to test and improve readiness
- Implement an auto-block rule on all emails containing QR codes, requiring manual inspection from a security officer before it can be forwarded through to the end user

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1598.003 - Spearfishing Link
Execution	T1204.001 - User Execution: Malicious Link
Credential Access	T1056.003 - Input Capture: Web Portal Capture

Artifacts

Value	Comment	Type
https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#	QR Code URL to a fake login page	URL Address
security@microsecmfa.com	Malicious email sender from Montreal, Canada	E-mail Sender
microsecmfa.com	Malicious email domain, NOT from Microsoft	E-mail Domain
158.69.201.47	Attacker's IP address, from Montreal, Canada	IP Address

209.94.90.1	Fake login page's serving IP address	IP Address

LetsDefend Playbook

LetsDefend Event ID: 214