A Day in the Life of a SOC Analyst: IOC Triage

Executive Summary

Threat actors continue to exploit email, brute-force attempts, and phishing domains to infiltrate organizations. As a SOC Analyst, part of my role is to validate and triage **Indicators of Compromise (IOCs)** shared by colleagues. This ensures we distinguish **false positives** from **legitimate threats** and take swift action to safeguard business operations.

Recently, I received multiple suspicious files and logs from a coworker for triage. After analysis, several artifacts were confirmed as malicious—including phishing campaigns, brute-force IPs, and domains linked to fraudulent activity.

Possible IOC Samples. Please Review.

Inside the email, I find a list of suspicious artifacts gathered during system checks:

- Download_Updated_Project_Files.eml
- PrimeSoft_auth.log
- PrimeSoft_firewall.log
- PrimeSoft_phishing.eml
- Reported_phish_nike.png
- Suspicious_email_shina.png
- Team_Building_Activity.eml

My task: triage these Indicators of Compromise (IOCs) to determine if they're false positives or true threats**.**

Tech stark

Kali Linux – Investigation environment for log and IOC analysis

VirusTotal – Malware/file hash checks and URL/IP reputation

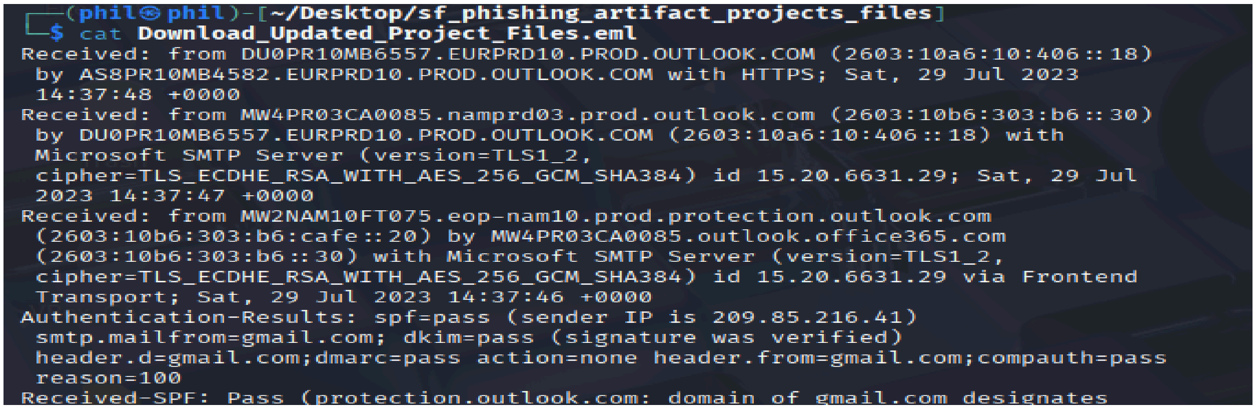
AbuseIPDB – IP enrichment, brute-force and abuse tracking

Hybrid Analysis – Sandbox testing for suspicious files

MXToolbox – Email header and DNS/SMTP verification

The Investigation Flow

Step 1: File Analysis [Download_Updated_Project_Files.em]



```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ cat Download_Updated_Project_Files.eml
Received: from DU0PR10MB6557.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:406::18)
 by AS8PR10MB4582.EURPRD10.PROD.OUTLOOK.COM with HTTPS; Sat, 29 Jul 2023
 14:37:48 +0000
Received: from MW4PR03CA0085.namprd03.prod.outlook.com (2603:10b6:303:b6::30)
 by DU0PR10MB6557.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:406::18) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29; Sat, 29 Jul
 2023 14:37:47 +0000
Received: from MW2NAM10FT075.eop-nam10.prod.protection.outlook.com
 (2603:10b6:303:b6:cafe::20) by MW4PR03CA0085.outlook.office365.com
 (2603:10b6:303:b6::30) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.29 via Frontend
 Transport; Sat, 29 Jul 2023 14:37:46 +0000
Authentication-Results: spf=pass (sender IP is 209.85.216.41)
 smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
 header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
```

On opening the file, it was found to be a suspicious phishing email with the following IOCs

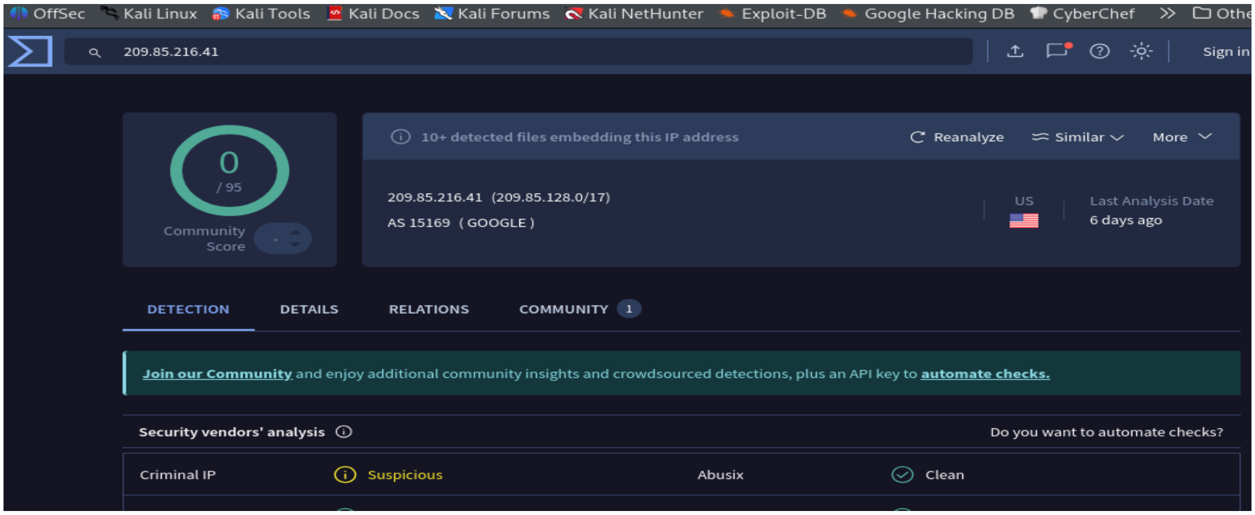
Ip	209.85.216.41 10.13.154.136

Url
htts://drive.google.com/uc?export=download&id=1bstuGMLer-fbJbcGG5JiqnlekTSKvq5y

Sender	projectdpt@kanzalshamsprojectmgt.com
Receiver	nikefury@company.com

Enrichment of IOCs

Ip 209.85.216.41 Suspicious {Virustotal , Abuseipdb}



209.85.216.41

0 / 95 Community Score

10+ detected files embedding this IP address

209.85.216.41 (209.85.128.0/17)
AS 15169 (GOOGLE)

US

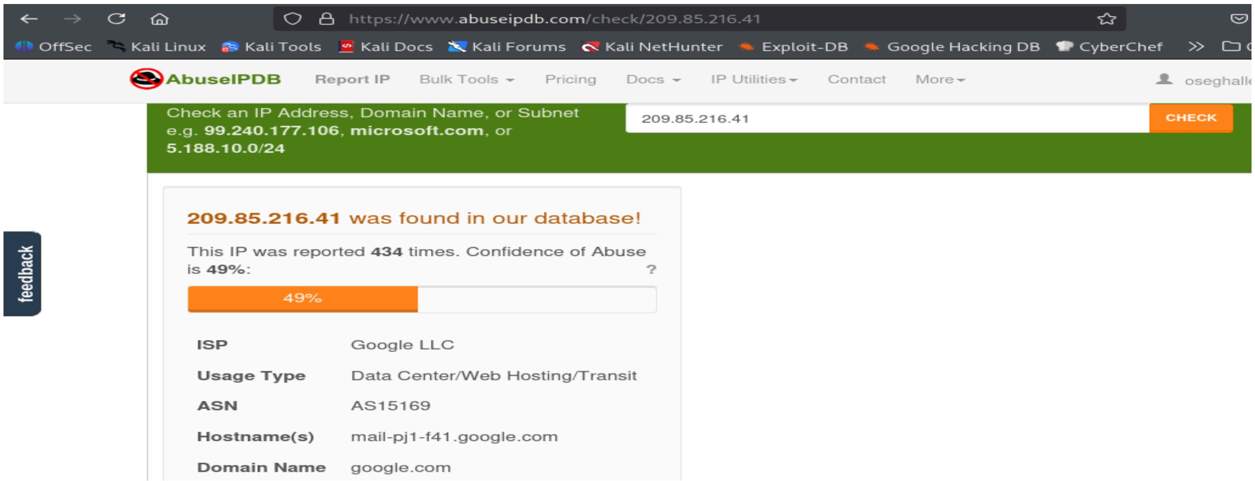
Last Analysis Date
6 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Criminal IP	Suspicious	Abusix	Clean



Check an IP Address, Domain Name, or Subnet
e.g. **99.240.177.106**, **microsoft.com**, or **5.188.10.0/24**

209.85.216.41

209.85.216.41 was found in our database!

This IP was reported **434** times. Confidence of Abuse is **49%**: ?

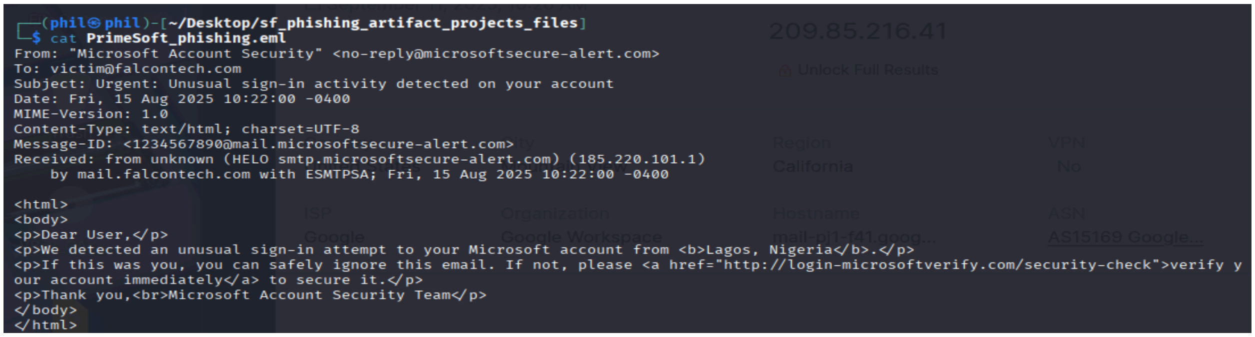
49%

ISP	Google LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	AS15169
Hostname(s)	mail-pj1-f41.google.com
Domain Name	google.com

Sender projectdpt@kanzalshamsprojectmgt.com This domain is different from the receiver domain; if coming from the same organization, it has to be the same

Receiver nikefury@company.com
Email address: Malicious (phishing campaign).

Step 2: File Analysis [PrimeSoft_phishing.eml]



```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ cat PrimeSoft_phishing.eml
From: "Microsoft Account Security" <no-reply@microsoftsecure-alert.com>
To: victim@falcontech.com
Subject: Urgent: Unusual sign-in activity detected on your account
Date: Fri, 15 Aug 2025 10:22:00 -0400
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Message-ID: <1234567890@mail.microsoftsecure-alert.com>
Received: from unknown (HELO smtp.microsoftsecure-alert.com) (185.220.101.1)
    by mail.falcontech.com with ESMTPSA; Fri, 15 Aug 2025 10:22:00 -0400

<html>
<body>
<p>Dear User,</p>
<p>We detected an unusual sign-in attempt to your Microsoft account from <b>Lagos, Nigeria</b>.</p>
<p>If this was you, you can safely ignore this email. If not, please <a href="http://login-microsoftverify.com/security-check">verify y
our account immediately</a> to secure it.</p>
<p>Thank you,<br>Microsoft Account Security Team</p>
</body>
</html>
```

On opening the file, it was found to be a suspicious phishing email with the following IOCs

Ip 185.220.101.1

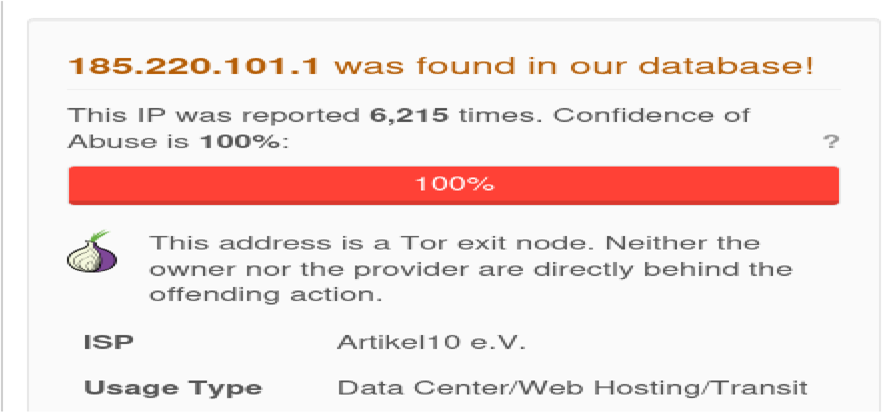
Url http://login-microsoftverify.com/security-check microsoftsecure-alert.com

Sender Microsoft Account Security <no-reply@microsoftsecure-alert.com>

Receiver Victim@falcontech.com

Enrichment

Ip 185.220.101.1 {Abuseipdb & Virustotal}
Country Germany

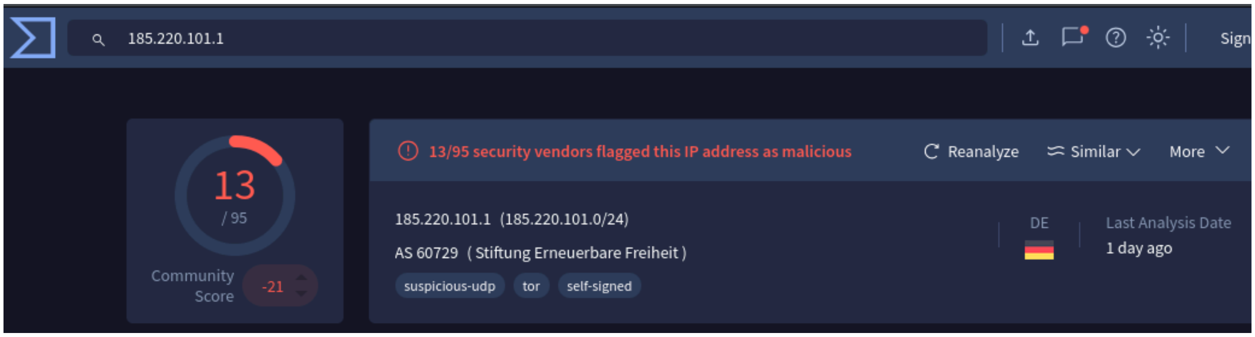


185.220.101.1 was found in our database!

This IP was reported **6,215** times. Confidence of Abuse is **100%**:

This address is a Tor exit node. Neither the owner nor the provider are directly behind the offending action.

ISP	Artikel10 e.V.
Usage Type	Data Center/Web Hosting/Transit



13/95 security vendors flagged this IP address as malicious

185.220.101.1 (185.220.101.0/24)
AS 60729 (Stiftung Erneuerbare Freiheit)

Last Analysis Date
1 day ago

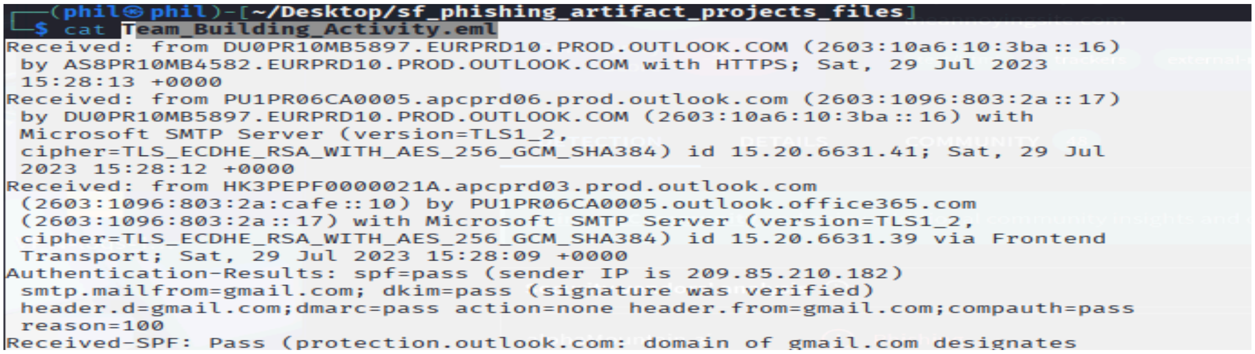
microsoftsecure-alert.com This domain is linked to this ip 185.220.101.1
Email address: Malicious (phishing campaign)

Step3: File Analysis[Team_Building_Activity.eml]

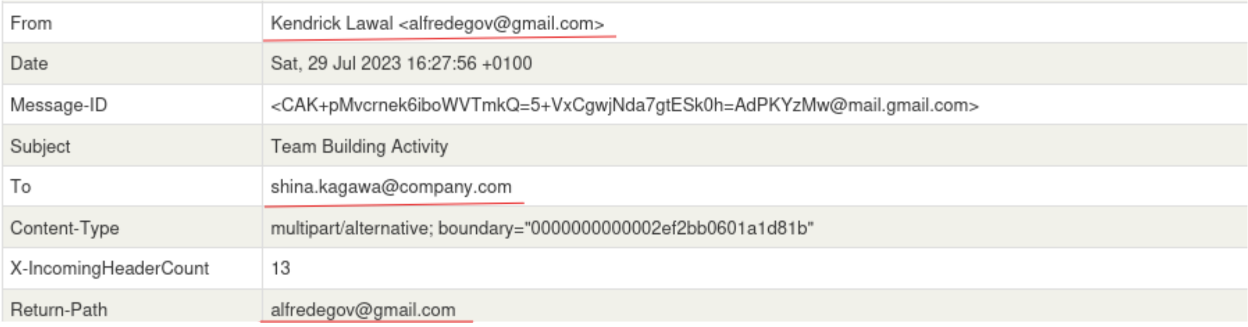
On opening the file, it was found to be a suspicious phishing email with the following IOCs

Ip 209.85.210.182

Url http://theannoyingsite.com



```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ cat Team_Building_Activity.eml
Received: from DU0PR10MB5897.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:3ba::16)
 by AS8PR10MB4582.EURPRD10.PROD.OUTLOOK.COM with HTTPS; Sat, 29 Jul 2023
 15:28:13 +0000
Received: from PU1PR06CA0005.apcprd06.prod.outlook.com (2603:1096:803:2a::17)
 by DU0PR10MB5897.EURPRD10.PROD.OUTLOOK.COM (2603:10a6:10:3ba::16) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.41; Sat, 29 Jul
 2023 15:28:12 +0000
Received: from HK3PEPF0000021A.apcprd03.prod.outlook.com
 (2603:1096:803:2a:cafe::10) by PU1PR06CA0005.outlook.office365.com
 (2603:1096:803:2a::17) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6631.39 via Frontend
 Transport; Sat, 29 Jul 2023 15:28:09 +0000
Authentication-Results: spf=pass (sender IP is 209.85.210.182)
 smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
 header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
```

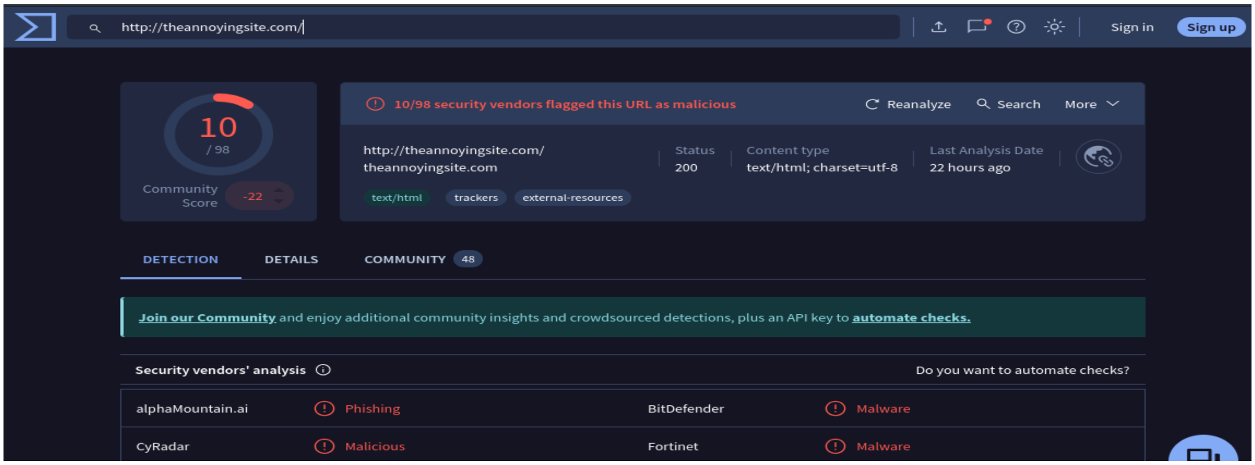


From	Kendrick Lawal <alfredegov@gmail.com>
Date	Sat, 29 Jul 2023 16:27:56 +0100
Message-ID	<CAK+pMvcrnek6iboWVTmkQ=5+VxCgwjNda7gtESk0h=AdPKYzMw@mail.gmail.com>
Subject	Team Building Activity
To	shina.kagawa@company.com
Content-Type	multipart/alternative; boundary="0000000000002ef2bb0601a1d81b"
X-IncomingHeaderCount	13
Return-Path	alfredegov@gmail.com

Sender and Receiver

Enrichment of IOCs

Url   http://theannoyingsite.com phishing malicious



10 / 98

Community Score -22

10/98 security vendors flagged this URL as malicious

http://theannoyingsite.com/
theannoyingsite.com

Status 200

Content type text/html; charset=utf-8

Last Analysis Date 22 hours ago

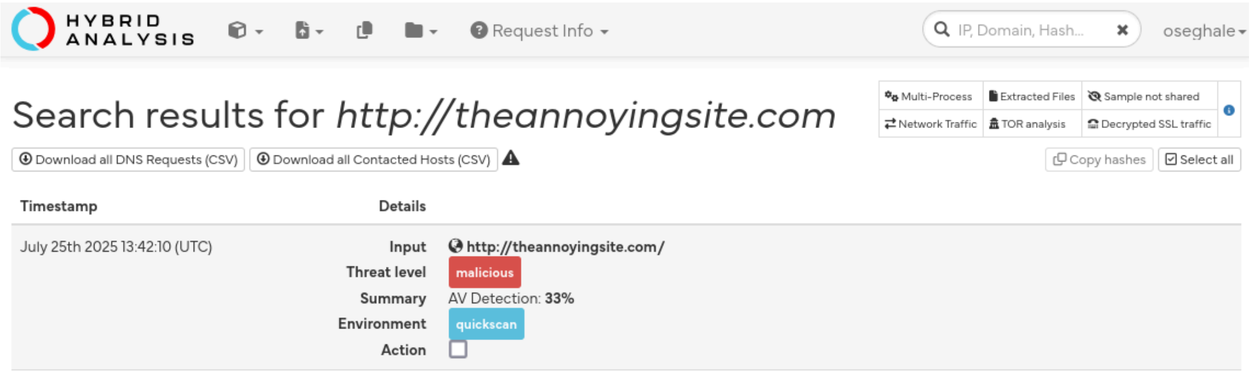
text/html · trackers · external-resources

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

alphaMountain.ai	Phishing	BitDefender	Malware
CyRadar	Malicious	Fortinet	Malware

Url   http://theannoyingsite.com malicious



Search results for *http://theannoyingsite.com*

Timestamp	Details	
July 25th 2025 13:42:10 (UTC)	Input	http://theannoyingsite.com/
	Threat level	malicious
	Summary	AV Detection: **33%**
	Environment	quickscan
	Action	□

theannoyingsite.com

Creation Date 7 years ago

10/94 security vendors flagged this domain as malicious

MITRE ATT&CK™ Techniques Detection

This report has 44 indicators that were mapped to 24 attack techniques and 8 tactics.

Malicious Indicators

The site has a relationship with this IP address: 50.116.11.184

Further inquiry into this IP address, 50.116.11.184 revealed that

High Risk - It is likely this IP address will be used for fraudulent

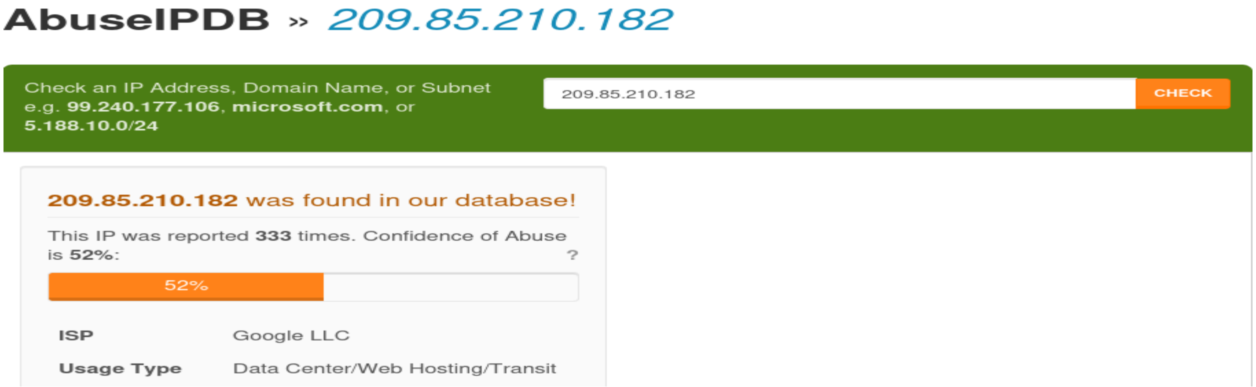
behaviour and malicious activity based on recent actions by this IP address.

IPQS has recently detected abusive behaviour from this connection.

It's a virus, don't even try to open the site.

Sender and receiver domains are not the same, but the email is meant to be from a teammate.

Ip 209.85.210.182 malicious



AbuseIPDB » 209.85.210.182

Check an IP Address, Domain Name, or Subnet
e.g. **99.240.177.106**, **microsoft.com**, or
5.188.10.0/24

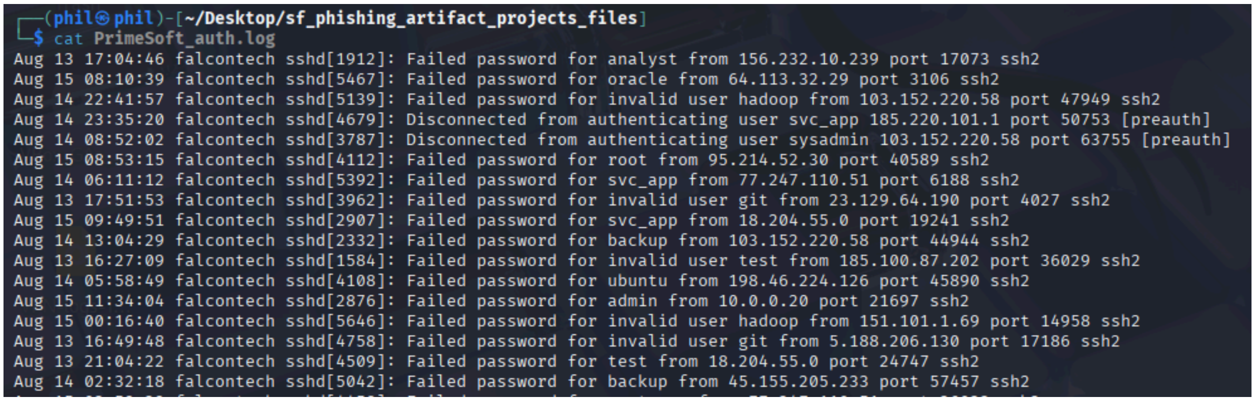
209.85.210.182 was found in our database!

This IP was reported **333** times. Confidence of Abuse is **52%**: ?

ISP	Google LLC
Usage Type	Data Center/Web Hosting/Transit

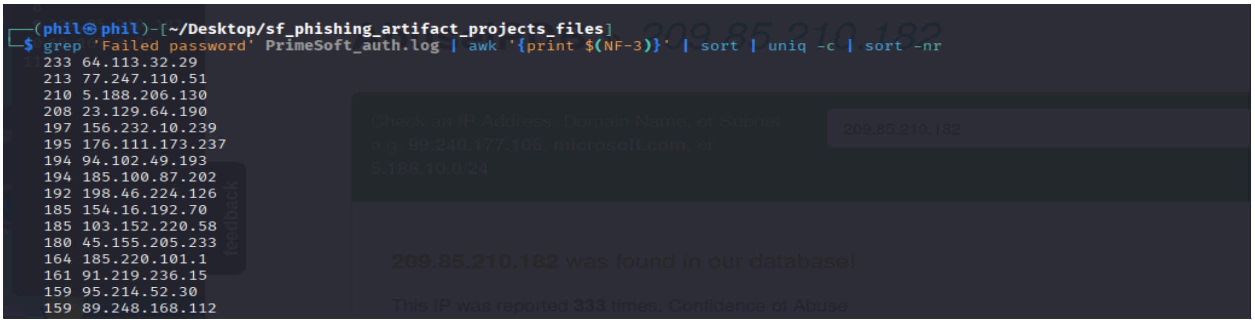
Email: Malicious (phishing campaign)

Step4: File Analysis[PrimeSoft_auth.log]



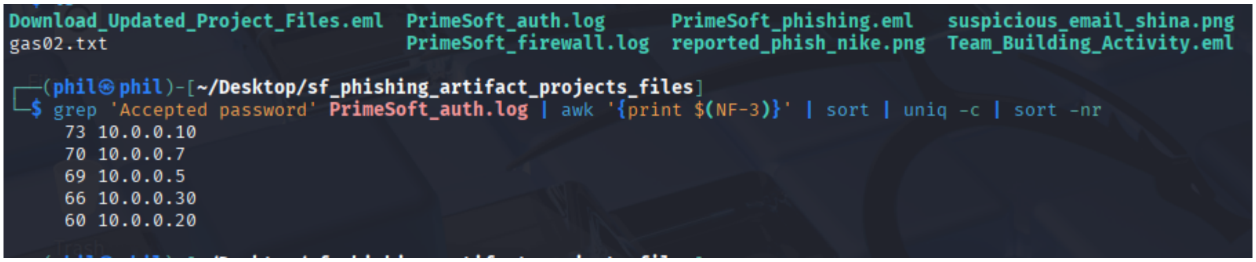
```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ cat PrimeSoft_auth.log
Aug 13 17:04:46 falcontech sshd[1912]: Failed password for analyst from 156.232.10.239 port 17073 ssh2
Aug 15 08:10:39 falcontech sshd[5467]: Failed password for oracle from 64.113.32.29 port 3106 ssh2
Aug 14 22:41:57 falcontech sshd[5139]: Failed password for invalid user hadoop from 103.152.220.58 port 47949 ssh2
Aug 14 23:35:20 falcontech sshd[4679]: Disconnected from authenticating user svc_app 185.220.101.1 port 50753 [preauth]
Aug 14 08:52:02 falcontech sshd[3787]: Disconnected from authenticating user sysadmin 103.152.220.58 port 63755 [preauth]
Aug 15 08:53:15 falcontech sshd[4112]: Failed password for root from 95.214.52.30 port 40589 ssh2
Aug 14 06:11:12 falcontech sshd[5392]: Failed password for svc_app from 77.247.110.51 port 6188 ssh2
Aug 13 17:51:53 falcontech sshd[3962]: Failed password for invalid user git from 23.129.64.190 port 4027 ssh2
Aug 15 09:49:51 falcontech sshd[2907]: Failed password for svc_app from 18.204.55.0 port 19241 ssh2
Aug 14 13:04:29 falcontech sshd[2332]: Failed password for backup from 103.152.220.58 port 44944 ssh2
Aug 13 16:27:09 falcontech sshd[1584]: Failed password for invalid user test from 185.100.87.202 port 36029 ssh2
Aug 14 05:58:49 falcontech sshd[4108]: Failed password for ubuntu from 198.46.224.126 port 45890 ssh2
Aug 15 11:34:04 falcontech sshd[2876]: Failed password for admin from 10.0.0.20 port 21697 ssh2
Aug 15 00:16:40 falcontech sshd[5646]: Failed password for invalid user hadoop from 151.101.1.69 port 14958 ssh2
Aug 13 16:49:48 falcontech sshd[4758]: Failed password for invalid user git from 5.188.206.130 port 17186 ssh2
Aug 13 21:04:22 falcontech sshd[4509]: Failed password for test from 18.204.55.0 port 24747 ssh2
Aug 14 02:32:18 falcontech sshd[5042]: Failed password for backup from 45.155.205.233 port 57457 ssh2
```

A long list of IPs was seen trying to intrude on the system with **Failed password** within the 48 hours.



```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ grep 'Failed password' PrimeSoft_auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
    233 64.113.32.29
    213 77.247.110.51
    210 5.188.206.130
    208 23.129.64.190
    197 156.232.10.239
    195 176.111.173.237
    194 94.102.49.193
    194 185.100.87.202
    192 198.46.224.126
    185 154.16.192.70
    185 103.152.220.58
    180 45.155.205.233
    164 185.220.101.1
    161 91.219.236.15
    159 95.214.52.30
    159 89.248.168.112
```

However 5 set of unique Ip were authenticated “**Accepted password “** 338 time within the 48 hours period which are shown in the screenshot below

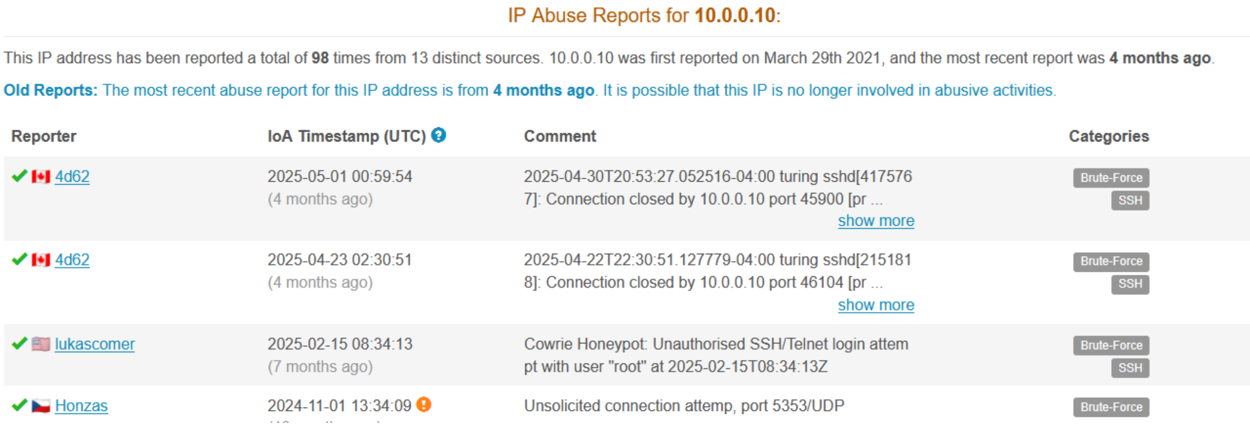


```
Download_Updated_Project_Files.eml  PrimeSoft_auth.log      PrimeSoft_phishing.eml   suspicious_email_shina.png
gas02.txt                           PrimeSoft_firewall.log  reported_phish_nike.png  Team_Building_Activity.eml

┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ grep 'Accepted password' PrimeSoft_auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr
     73 10.0.0.10
     70 10.0.0.7
     69 10.0.0.5
     66 10.0.0.30
     60 10.0.0.20
```

Enrichment of IOCs

These ips with accepted assword are all internal ips and were all involved in brute force ad port scanning activities



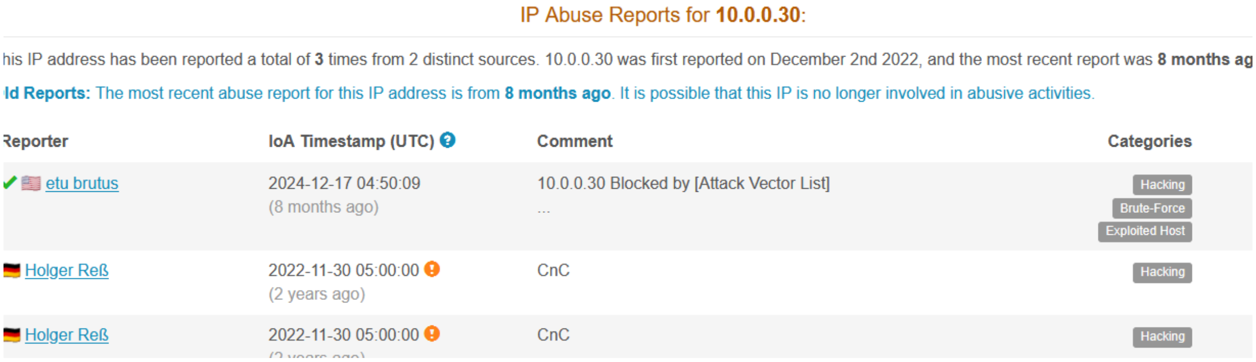
IP Abuse Reports for **10.0.0.10**:

This IP address has been reported a total of **98** times from 13 distinct sources. 10.0.0.10 was first reported on March 29th 2021, and the most recent report was **4 months ago**.

Old Reports: The most recent abuse report for this IP address is from **4 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ 4d62	2025-05-01 00:59:54 (4 months ago)	2025-04-30T20:53:27.052516-04:00 turing sshd[417576 7]: Connection closed by 10.0.0.10 port 45900 [pr ... show more	Brute-Force SSH
✓ 4d62	2025-04-23 02:30:51 (4 months ago)	2025-04-22T22:30:51.127779-04:00 turing sshd[215181 8]: Connection closed by 10.0.0.10 port 46104 [pr ... show more	Brute-Force SSH
✓ lukascomer	2025-02-15 08:34:13 (7 months ago)	Cowrie Honeypot: Unauthorised SSH/Telnet login attem pt with user "root" at 2025-02-15T08:34:13Z	Brute-Force SSH
✓ Honzas	2024-11-01 13:34:09	Unsolicited connection attemp, port 5353/UDP	Brute-Force

IP 10.0.0.10
IP 10.0.0.7
IP 10.0.0.5



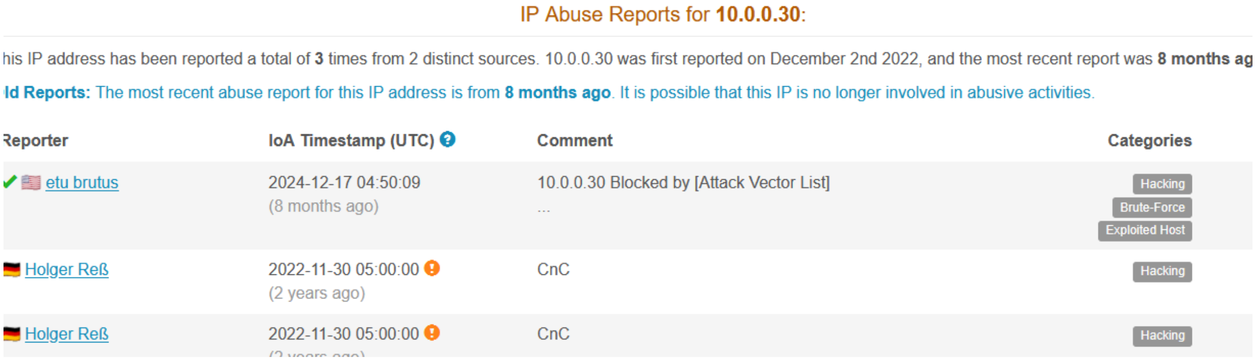
IP Abuse Reports for **10.0.0.30**:

his IP address has been reported a total of **3** times from 2 distinct sources. 10.0.0.30 was first reported on December 2nd 2022, and the most recent report was **8 months ag**

ld Reports: The most recent abuse report for this IP address is from **8 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ etu brutus	2024-12-17 04:50:09 (8 months ago)	10.0.0.30 Blocked by [Attack Vector List] ...	Hacking Brute-Force Exploited Host
Holger Reß	2022-11-30 05:00:00 (2 years ago)	CnC	Hacking
Holger Reß	2022-11-30 05:00:00	CnC	Hacking

IP 10.0.0.30



IP Abuse Reports for **10.0.0.30**:

his IP address has been reported a total of **3** times from 2 distinct sources. 10.0.0.30 was first reported on December 2nd 2022, and the most recent report was **8 months ag**

ld Reports: The most recent abuse report for this IP address is from **8 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ etu brutus	2024-12-17 04:50:09 (8 months ago)	10.0.0.30 Blocked by [Attack Vector List] ...	Hacking Brute-Force Exploited Host
Holger Reß	2022-11-30 05:00:00 (2 years ago)	CnC	Hacking
Holger Reß	2022-11-30 05:00:00 (2 years ago)	CnC	Hacking

IP 10.0.0.50

Ip 64.113.32.26   Malware, Malicious {Virustotal Abuseipdb Hybrid analysis}

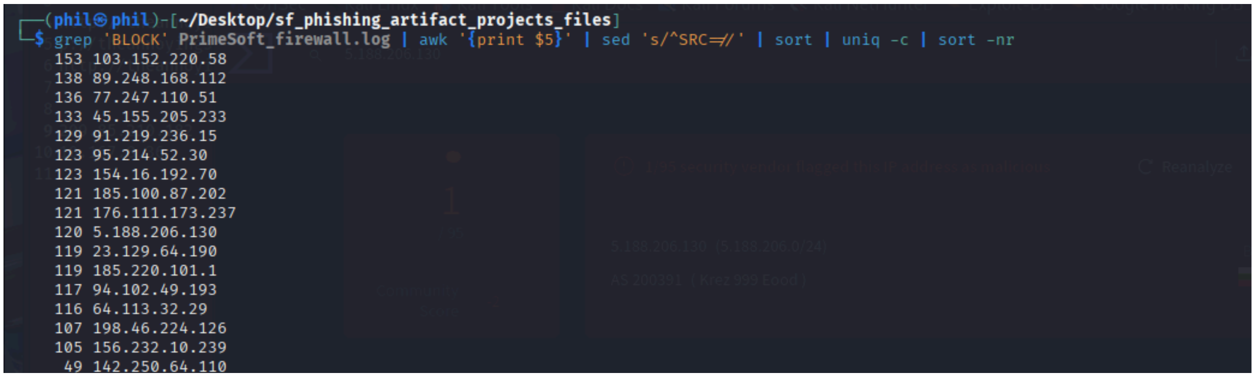
Ip   77.247.110.51   Netherlands   Malicious {Virustotal Abuseipdb}

Ip   5.188.206.130,   Bulgaria   Malicious {Virustotal Abuseipdb} Brute force attacks

These IPs are malicious and are used for brute-force attacks.

Step5: File Analysis[PrimeSoft_firewall.log]

A long list of IPs were blocked by the firewall, most of them were blocked multiple times within the 48-hour period



```
┌──(phil㉿phil)-[~/Desktop/sf_phishing_artifact_projects_files]
└─$ grep 'BLOCK' PrimeSoft_firewall.log | awk '{print $5}' | sed 's/^SRC=//' | sort | uniq -c | sort -nr
    153 103.152.220.58
    138 89.248.168.112
    136 77.247.110.51
    133 45.155.205.233
    129 91.219.236.15
    123 95.214.52.30
    123 154.16.192.70
    121 185.100.87.202
    121 176.111.173.237
    120 5.188.206.130
    119 23.129.64.190
    119 185.220.101.1
    117 94.102.49.193
    116 64.113.32.29
    107 198.46.224.126
    105 156.232.10.239
     49 142.250.64.110
```

Enrichment of IOCs

IP 103.152.220.58   country Hong Kong, Domain Name is interstellarbd.net, suspicious

IP 89.248.168.122   1/94 security vendor flagged this IP address as malicious(Virus Total)

Country Netherlands

IP 77.247.110.51   1/94 security vendor flagged this IP address as malicious(Virus Total)

It was first reported on June 17th, 2021, and the most recent report was 3 years ago

IP 77.247.110.51 was found in our database. This IP was reported 199 times (AbuseIPDB)

Ip 45.155.205.233

IP 45.155.205.233 was found in our database and has been reported 1612 times (AbuseIPDB) Country Russian Federation, 19/94 security vendors flagged this IP address as malicious(Virus Total)

Ip 91.219.236.15 Country Hungary/ was not found in most databases but is still suspicious, as one vendor has flagged it as such (ArcSight threat intel.)

These IPs are malicious and are used for brute-force attacks

Final Triage Report

- Download_Updated_Project_Files.eml **Email** Malicious (phishing campaign).
- PrimeSoft_auth.log **IPs** are malicious and are used for brute-force attacks.
- PrimeSoft_firewall.log **IPs** are malicious and are used for brute-force attacks
- PrimeSoft_phishing.eml **Email** Malicious (phishing campaign)
- Team_Building_Activity.eml **Email:** Malicious (phishing campaign)

Key Takeaway

Effective IOC triage isn't just about spotting bad actors—it's about validating evidence, enriching with intelligence, and making fast, informed decisions.

As cyber threats evolve, SOC analysts stand as the frontline, ensuring that noise is filtered out and real threats are acted upon swiftly.

Recommendations

- **Strengthen Email Security**
    - Enforce SPF, DKIM, and DMARC policies.
    - Run phishing simulations and awareness training.
- **Harden Authentication Systems**
    - Require FA for critical accounts.
    - Monitor and block repeated failed logins at the firewall/IDS.
- **Threat Intelligence Integration**
    - Automate IOC enrichment with VirusTotal, AbuseIPDB, Hybrid Analysis, and MXToolbox.
    - Continuously update SIEM correlation rules.
- **Network Defense**
    - Block malicious IPs/domains identified in triage.
    - Apply geo-blocking for high-risk regions when business context allows.
- **Incident Response Playbook**
    - Document and rehearse playbooks for phishing, brute force, and impersonation attempts.
    - Define clear escalation paths for true positives.

Conclusion

In conclusion, this IOC triage demonstrated how systematic analysis, enrichment, and correlation transform raw artifacts into actionable intelligence. Multiple phishing emails, malicious domains, and numerous IP addresses tied to brute-force and suspicious activity were confirmed as true threats rather than false positives. By validating evidence with tools like VirusTotal, AbuseIPDB, and by reviewing authentication and firewall logs, we identified immediate risks and prioritized mitigations. Moving forward, implementing the recommended controls stronger email authentication (SPF/DKIM/DMARC), MFA, automated threat-intelligence integration, targeted blocking, and rehearsed incident playbooks will reduce risk exposure and shorten detection-to-remediation time. Ultimately, continuous triage and collaboration across SOC, IT, and users will keep the organization resilient against evolving phishing and intrusion attempts.