# Phishing Email Analysis

## Introduction

This report provides a forensic analysis of a suspected phishing email sample obtained from [Sample Phishing email]. The email appears to impersonate Banco do Bradesco, urging the recipient to take action regarding their loyalty points (Livelo). This analysis follows a structured methodology to determine whether the email is malicious and extract key Indicators of Compromise (IOCs).

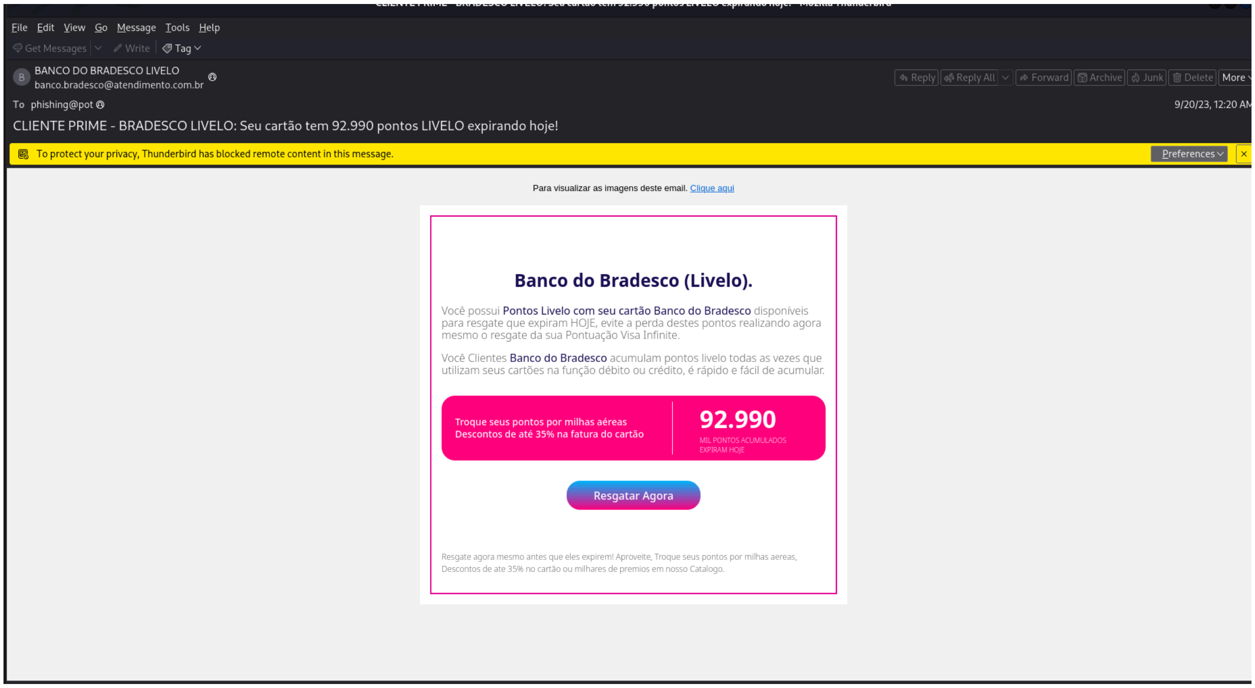
### The investigation includes:

- Email header analysis to verify sender authenticity.
- SPF, DKIM, and DMARC checks to validate email authentication mechanisms.
- Content and link analysis to detect phishing attempts.
- Attachment and URL scanning using Kali Linux tools and open-source intelligence (OSINT) platforms.

# Tools Used

## Kali Linux Tools:

- mutt / thunderbird (to read .eml files)



BANCO DO BRADESCO LIVELO
banco.bradesco@atendimento.com.br

To phishing@pot

9/20/23, 12:20 AM

CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

To protect your privacy, Thunderbird has blocked remote content in this message.

Para visualizar as imagens deste email. Clique aqui

Banco do Bradesco (Livelo).

Você possui Pontos Livelo com seu cartão Banco do Bradesco disponíveis para resgate que expiram HOJE, evite a perda destes pontos realizando agora mesmo o resgate da sua Pontuação Visa Infinite.

Você Clientes Banco do Bradesco acumulam pontos livelo todas as vezes que utilizam seus cartões na função débito ou crédito, é rápido e fácil de acumular.

Troque seus pontos por milhas aéreas
Descontos de até 35% na fatura do cartão

92.990
MIL PONTOS ACUMULADOS
EXPIRAM HOJE

Resgate agora mesmo antes que eles expirem! Aproveite, Troque seus pontos por milhas aereas, Descontos de ate 35% no cartão ou milhares de premios em nosso Catalogo.

- cat / less (to inspect raw email content)
- exiftool (to extract metadata from email headers)
- whois (to gather domain information)
- dig / nslookup (to analyze DNS records)
- curl / wget (to inspect URLs safely)
- strings (to extract hidden text in attachments)

1. **Email Source & Relays:**
    - Originated from `ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4)`
    - Passed through multiple Microsoft Exchange Online servers
    - Received from `BN8NAM11FT066.mail.protection.outlook.com`
2. **Authentication & Anti-Spam Results:**
    - **SPF:** `TempError` (DNS Timeout)
    - **DKIM:** `None` (Message not signed)
    - **DMARC:** `TempError`
    - **CompAuth:** `Fail` (Reason: 001)
    - **SCL (Spam Confidence Level):** `5`
    - **BCL (Bulk Complaint Level):** `9`
3. **Sender Information:**
    - **From:** `BANCO DO BRADESCO LIVELO <banco.bradesco@atendimento.com.br>`
    - **Return-Path:** `root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06`
    - **X-Sender-IP:** `137.184.34.4`
4. **Email Subject & Content Encoding:**
    - **Subject:** `CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!`
    - **Content-Type:** `text/html; charset=UTF-8`
    - **Content-Transfer-Encoding:** `base64`
5. **Miscellaneous Headers:**
    - **Message-ID:** `<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>`
    - **Received-SPF:** `TempError (DNS Timeout)`
    - **X-MS-Exchange-Organization-SCL:** `5` (Likely spam)
    - **X-MS-Exchange-Organization-AuthAs:** `Anonymous`

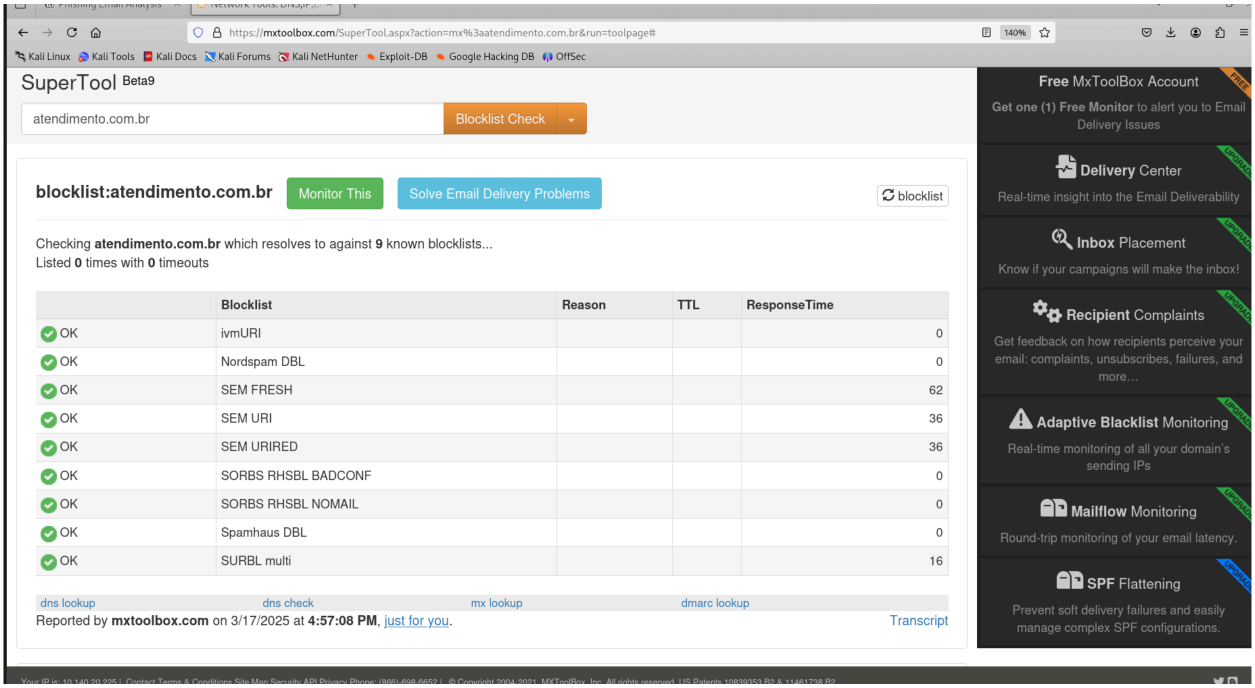
- **X-MS-Exchange-Organization-MessageDirectionality:** Incoming

This email is likely **phishing** based on:

- SPF/DMARC failures
- Use of a generic Ubuntu-based mail server
- High SCL/BCL values
- Misleading sender address (Bradesco would use their own domain)

## Open-Source Online Tools

- MXToolBox (https://mxtoolbox.com) – Email header analysis and SPF/DKIM/DMARC lookup



https://mxtoolbox.com/SuperTool.aspx?action=mx%3aatendimento.com.br&run=toolpage#
140%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
SuperTool Beta9
Blocklist Check
Monitor This
Solve Email Delivery Problems
blocklist
Free MxToolBox Account
Get one (1) Free Monitor to alert you to Email Delivery Issues
Delivery Center
Real-time insight into the Email Deliverability
Inbox Placement
Know if your campaigns will make the inbox!
Recipient Complaints
Get feedback on how recipients perceive your email: complaints, unsubscribes, failures, and more...
Adaptive Blacklist Monitoring
Real-time monitoring of all your domain's sending IPs
Mailflow Monitoring
Round-trip monitoring of your email latency.
SPF Flattening
Prevent soft delivery failures and easily manage complex SPF configurations.
dns lookup
dns check
mx lookup
dmarc lookup
Transcript

atendimento.com.br

**blocklist:atendimento.com.br**

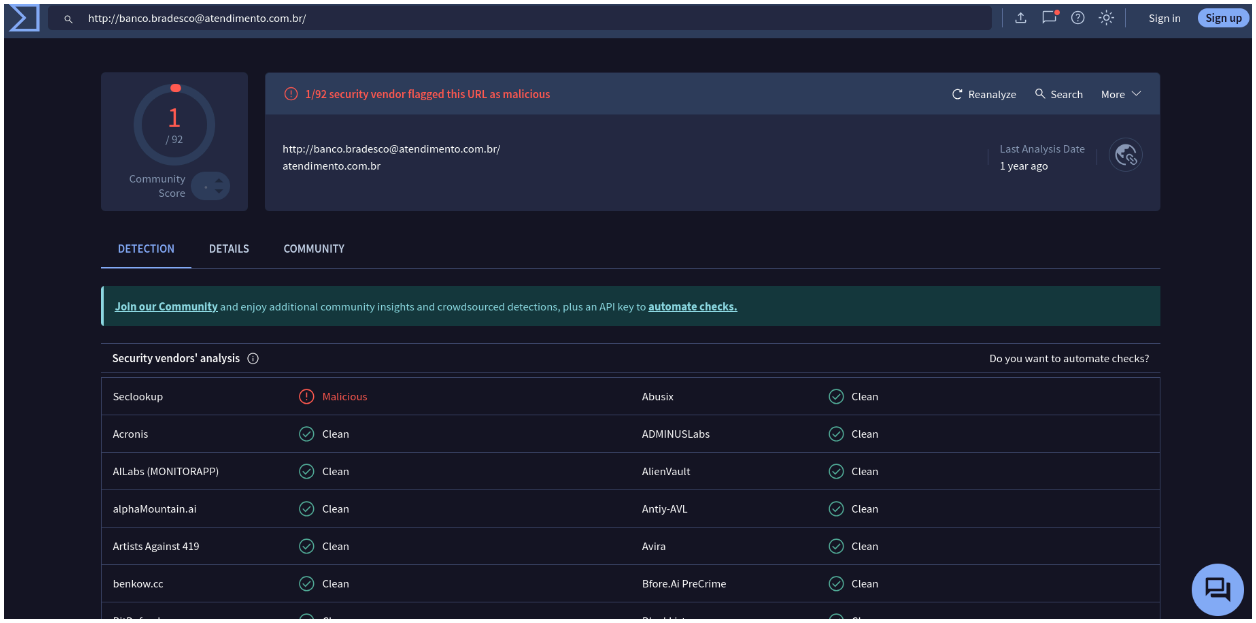
Checking **atendimento.com.br** which resolves to against **9** known blocklists...
Listed **0** times with **0** timeouts

| | Blocklist | Reason | TTL | ResponseTime |
|---|---|---|---|---|
| ✓ OK | ivmURI | | | 0 |
| ✓ OK | Nordspam DBL | | | 0 |
| ✓ OK | SEM FRESH | | | 62 |
| ✓ OK | SEM URI | | | 36 |
| ✓ OK | SEM URIRED | | | 36 |
| ✓ OK | SORBS RHSBL BADCONF | | | 0 |
| ✓ OK | SORBS RHSBL NOMAIL | | | 0 |
| ✓ OK | Spamhaus DBL | | | 0 |
| ✓ OK | SURBL multi | | | 16 |

Reported by **mxtoolbox.com** on 3/17/2025 at **4:57:08 PM**, just for you.

Your IP is: 10.140.20.225 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc, All rights reserved. US Patents 10839353 B2 & 11461738 B2

- VirusTotal (https://www.virustotal.com) – URL, domain, and attachment scanning



1/92 security vendor flagged this URL as malicious

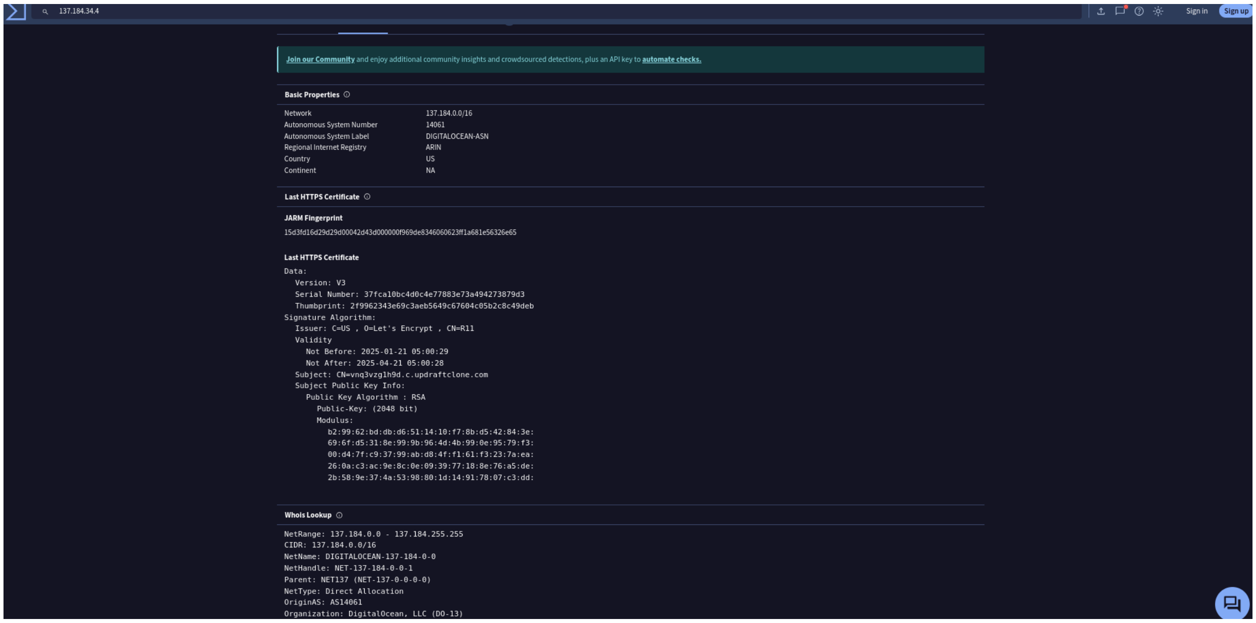
http://banco.bradesco@atendimento.com.br/
atendimento.com.br

Last Analysis Date
1 year 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?

| | | | |
|---|---|---|---|
| Seclookup | ⓘ Malicious | Abusix | ✓ Clean |
| Acronis | ✓ Clean | ADMINUSLabs | ✓ Clean |
| AILabs (MONITORAPP) | ✓ Clean | AlienVault | ✓ Clean |
| alphaMountain.ai | ✓ Clean | Antiy-AVL | ✓ Clean |
| Artists Against 419 | ✓ Clean | Avira | ✓ Clean |
| benkow.cc | ✓ Clean | Bfore.Ai PreCrime | ✓ Clean |



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

**Basic Properties** ⓘ

| | |
|---|---|
| Network | 137.184.0.0/16 |
| Autonomous System Number | 14061 |
| Autonomous System Label | DIGITALOCEAN-ASN |
| Regional Internet Registry | ARIN |
| Country | US |
| Continent | NA |

**Last HTTPS Certificate** ⓘ

**JARM Fingerprint**

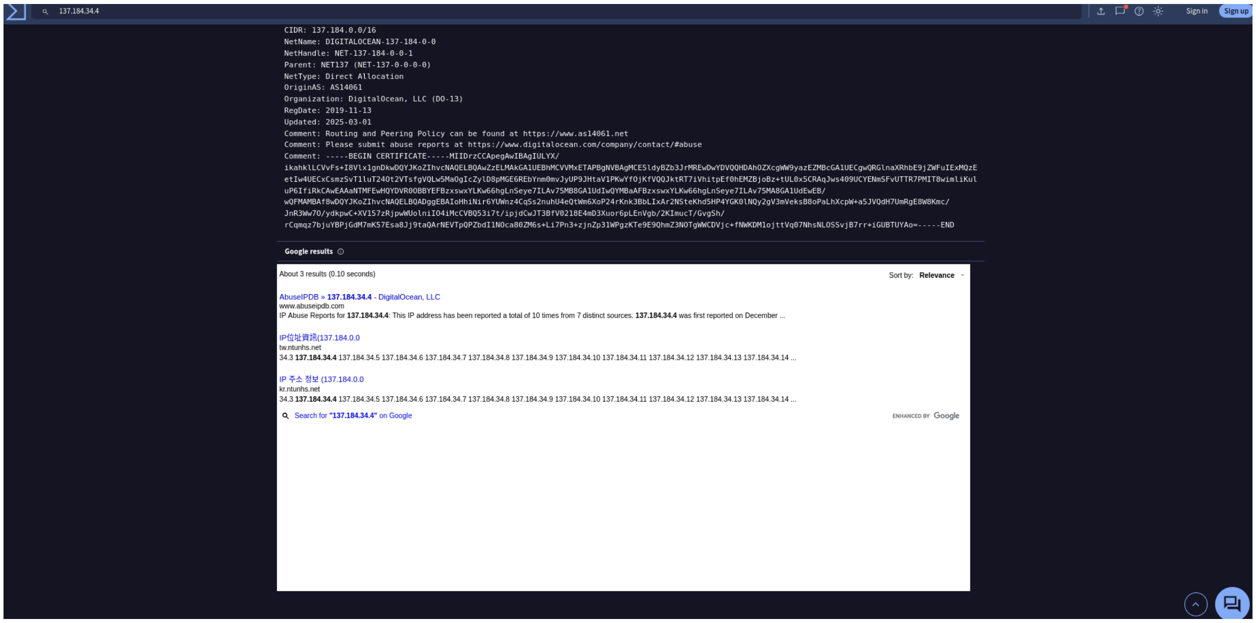
15d3fd16d29d29d00042d43d000000f969de8346060623ff1a681e56326e65

**Last HTTPS Certificate**

```
Data:
  Version: V3
  Serial Number: 37fca10bc4d0c4e77883e73a494273879d3
  Thumbprint: 2f9962343e69c3aeb5649c67604c05b2c8c49deb
Signature Algorithm:
  Issuer: C=US , O=Let's Encrypt , CN=R11
  Validity
    Not Before: 2025-01-21 05:00:29
    Not After: 2025-04-21 05:00:28
  Subject: CN=vnq3vzg1h9d.c.updraftclone.com
  Subject Public Key Info:
    Public Key Algorithm : RSA
      Public-Key: (2048 bit)
      Modulus:
        b2:99:62:bd:db:d6:51:14:10:f7:8b:d5:42:84:3e:
        69:6f:d5:31:8e:99:9b:96:4d:4b:99:0e:95:79:f3:
        00:d4:7f:c9:37:99:ab:d8:4f:f1:61:f3:23:7a:ea:
        26:0a:c3:ac:9e:8c:0e:09:39:77:18:8e:76:a5:de:
        2b:58:9e:37:4a:53:98:80:1d:14:91:78:07:c3:dd:
```

**Whois Lookup** ⓘ

```
NetRange: 137.184.0.0 - 137.184.255.255
CIDR: 137.184.0.0/16
NetName: DIGITALOCEAN-137-184-0-0
NetHandle: NET-137-184-0-0-1
Parent: NET137 (NET-137-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS14061
Organization: DigitalOcean, LLC (DO-13)
```



```
CIDR: 137.184.0.0/16
NetName: DIGITALOCEAN-137-184-0-0
NetHandle: NET-137-184-0-0-1
Parent: NET137 (NET-137-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS14061
Organization: DigitalOcean, LLC (DO-13)
RegDate: 2019-11-13
Updated: 2025-03-01
Comment: Routing and Peering Policy can be found at https://www.as14061.net
Comment: Please submit abuse reports at https://www.digitalocean.com/company/contact/#abuse
Comment: -----BEGIN CERTIFICATE-----MIIDrzCCApegAwIBAgIULYX/
ikahklLCVvFs+I8Vlx1gnDkwDQYJKoZIhvcNAQELBQAwZzELMAkGA1UEBhMCVVMxETAPBgNVBAgMCE5ldyBZb3JrMREwDwYDVQQHDAhOZXcgWW9yazEZMBcGA1UECgwQRGlnaXRhbE9jZWFuIExMQzE
etIw4UECxCsmzSvT1luT24Ot2VTsfgVQLw5MaOgIcZylD8pMGE6REbYnm0mvJyUP9JHtaV1PKwYfOjKfVQQJktRT7iVhitpEf0hEMZBjoBz+tUL0x5CRAqJws409UCYENmSFvUTTR7PMIT8wimliKul
uP6IfiRkCAwEAAaNTMFEwHQYDVR0OBBYEFBzxswxYLKw66hgLnSeye7ILAv75MB8GA1UdIwQYMBaAFBzxswxYLKw66hgLnSeye7ILAv75MA8GA1UdEwEB/
wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAIoHhiNir6YUWnz4CqSs2nuhU4eQtWm6XoP24rKnk3BbLIxAr2NSteKhd5HP4YGK0lNQy2gV3mVeksB8oPaLhXcpW+a5JVQdH7UmRgE8W8Kmc/
JnR3Ww7O/ydkpwC+XV157zRjpwWUolniIO4iMcCVBQ53i7t/ipjdCwJT3BfV0218E4mD3Xuor6pLEnVgb/2KImucT/GvgSh/
rCqmqz7bjuYBPjGdM7mK57Esa8Jj9taQArNEVTpQPZbdI1NOca80ZM6s+Li7Pn3+zjnZp31WPgzKTe9E9QhmZ3NOTgWWCDVjc+fNWKDM1ojttVq07NhsNLOSSvjB7rr+iGUBTUYAo=-----END
```

Google results

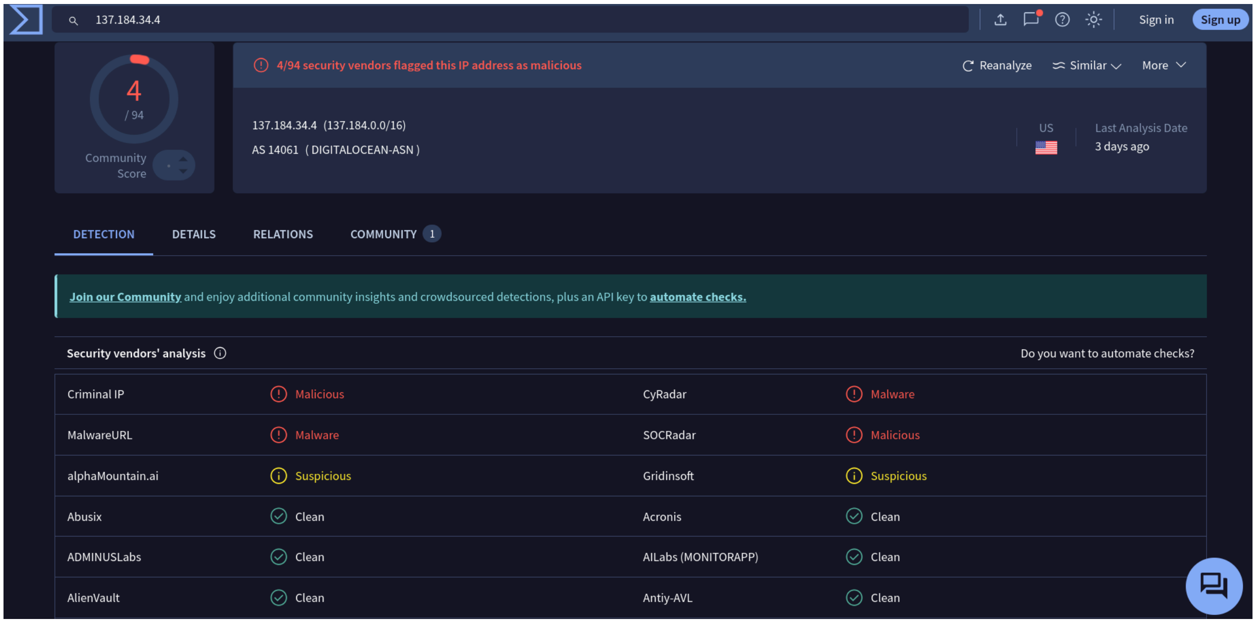
About 3 results (0.10 seconds) Sort by: Relevance

AbuseIPDB » **137.184.34.4** - DigitalOcean, LLC
www.abuseipdb.com
IP Abuse Reports for **137.184.34.4**: This IP address has been reported a total of 10 times from 7 distinct sources. **137.184.34.4** was first reported on December ...

IP位址資訊(137.184.0.0
tw.ntunhs.net
34.3 **137.184.34.4** 137.184.34.5 137.184.34.6 137.184.34.7 137.184.34.8 137.184.34.9 137.184.34.10 137.184.34.11 137.184.34.12 137.184.34.13 137.184.34.14 ...

IP 주소 정보 (137.184.0.0
kr.ntunhs.net
34.3 **137.184.34.4** 137.184.34.5 137.184.34.6 137.184.34.7 137.184.34.8 137.184.34.9 137.184.34.10 137.184.34.11 137.184.34.12 137.184.34.13 137.184.34.14 ...

Search for "**137.184.34.4**" on Google



4/94 security vendors flagged this IP address as malicious

137.184.34.4 (137.184.0.0/16)
AS 14061 ( DIGITALOCEAN-ASN )

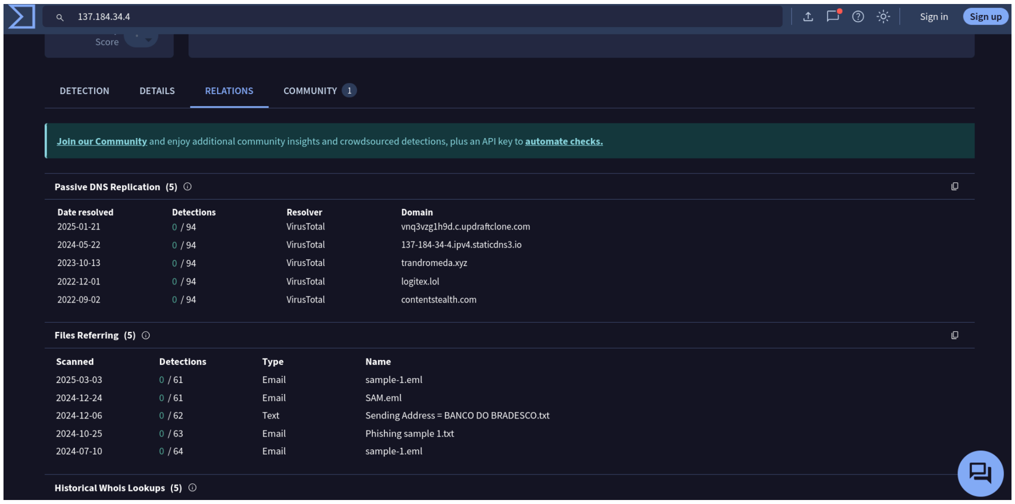
US

Last Analysis Date
3 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 | ⓘ Malicious | CyRadar | ⓘ Malware |
| MalwareURL | ⓘ Malware | SOCRadar | ⓘ Malicious |
| alphaMountain.ai | ⓘ Suspicious | Gridinsoft | ⓘ Suspicious |
| Abusix | ✓ Clean | Acronis | ✓ Clean |
| ADMINUSLabs | ✓ Clean | AILabs (MONITORAPP) | ✓ Clean |
| AlienVault | ✓ Clean | Antiy-AVL | ✓ Clean |



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

**Passive DNS Replication (5)**

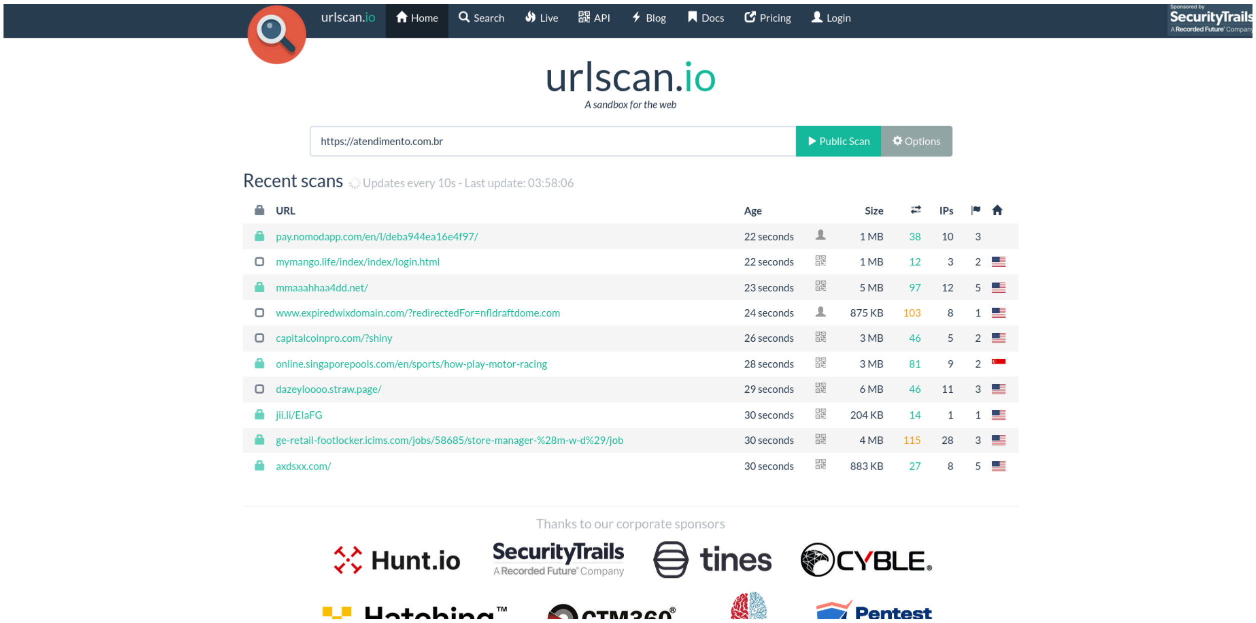
| Date resolved | Detections | Resolver | Domain |
|---|---|---|---|
| 2025-01-21 | 0 / 94 | VirusTotal | vnq3vzg1h9d.c.updraftclone.com |
| 2024-05-22 | 0 / 94 | VirusTotal | 137-184-34-4.ipv4.staticdns3.io |
| 2023-10-13 | 0 / 94 | VirusTotal | trandromeda.xyz |
| 2022-12-01 | 0 / 94 | VirusTotal | logitex.lol |
| 2022-09-02 | 0 / 94 | VirusTotal | contentstealth.com |

**Files Referring (5)**

| Scanned | Detections | Type | Name |
|---|---|---|---|
| 2025-03-03 | 0 / 61 | Email | sample-1.eml |
| 2024-12-24 | 0 / 61 | Email | SAM.eml |
| 2024-12-06 | 0 / 62 | Text | Sending Address = BANCO DO BRADESCO.txt |
| 2024-10-25 | 0 / 63 | Email | Phishing sample 1.txt |
| 2024-07-10 | 0 / 64 | Email | sample-1.eml |

**Historical Whois Lookups (5)**

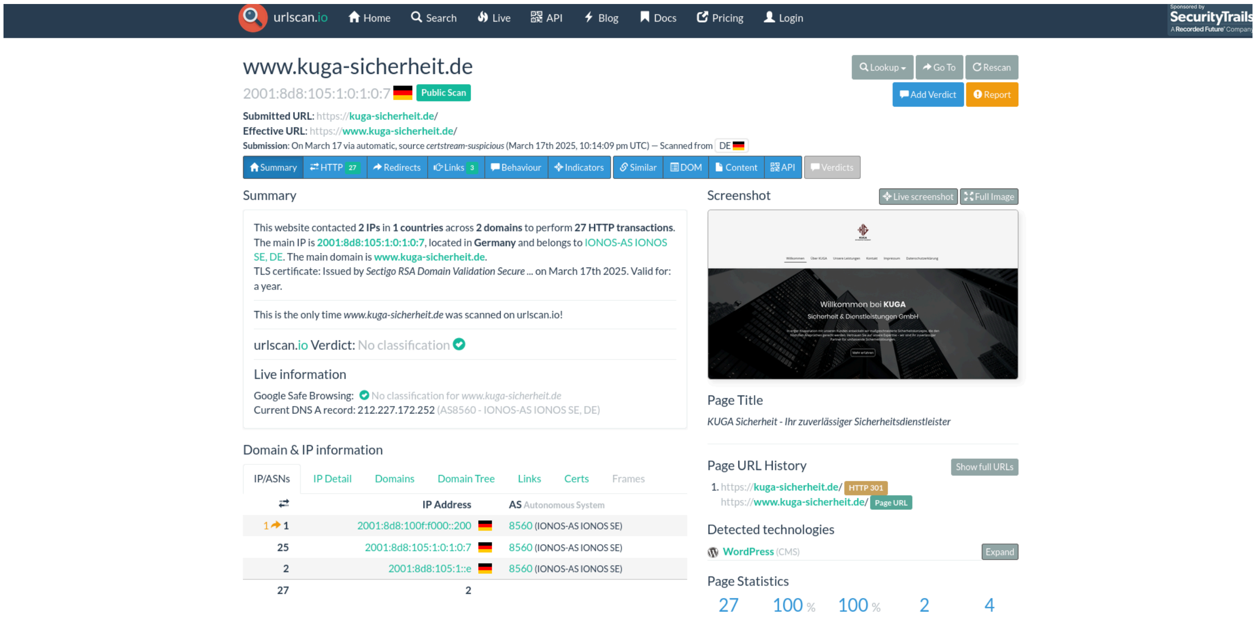
- URLScan.io (https://urlscan.io) – URL behavior analysis



Recent scans Updates every 10s - Last update: 03:58:06

| 🔒 | URL | Age | | Size | ⇄ | IPs | ⚑ | ⌂ |
|---|---|---|---|---|---|---|---|---|
| 🔒 | pay.nomodapp.com/en/l/deba944ea16e4f97/ | 22 seconds | 👤 | 1 MB | 38 | 10 | 3 | |
| □ | mymango.life/index/index/login.html | 22 seconds | ▦ | 1 MB | 12 | 3 | 2 | 🇺🇸 |
| 🔒 | mmaaahhaa4dd.net/ | 23 seconds | ▦ | 5 MB | 97 | 12 | 5 | 🇺🇸 |
| □ | www.expiredwixdomain.com/?redirectedFor=nfldraftdome.com | 24 seconds | 👤 | 875 KB | 103 | 8 | 1 | 🇺🇸 |
| □ | capitalcoinpro.com/?shiny | 26 seconds | ▦ | 3 MB | 46 | 5 | 2 | 🇺🇸 |
| 🔒 | online.singaporepools.com/en/sports/how-play-motor-racing | 28 seconds | ▦ | 3 MB | 81 | 9 | 2 | 🇸🇬 |
| □ | dazeyloooo.straw.page/ | 29 seconds | ▦ | 6 MB | 46 | 11 | 3 | 🇺🇸 |
| 🔒 | jii.li/ElaFG | 30 seconds | ▦ | 204 KB | 14 | 1 | 1 | 🇺🇸 |
| 🔒 | ge-retail-footlocker.icims.com/jobs/58685/store-manager-%28m-w-d%29/job | 30 seconds | ▦ | 4 MB | 115 | 28 | 3 | 🇺🇸 |
| 🔒 | axdsxx.com/ | 30 seconds | ▦ | 883 KB | 27 | 8 | 5 | 🇺🇸 |

Thanks to our corporate sponsors
Hunt.io
SecurityTrails A Recorded Future Company
tines
CYBLE
Hatching
CTM360
Pentest



www.kuga-sicherheit.de

2001:8d8:105:1:0:1:0:7 Public Scan

**Submitted URL:** https://kuga-sicherheit.de/
**Effective URL:** https://www.kuga-sicherheit.de/
**Submission:** On March 17 via automatic, source *certstream-suspicious* (March 17th 2025, 10:14:09 pm UTC) — Scanned from DE

Summary

This website contacted **2 IPs** in **1 countries** across **2 domains** to perform **27 HTTP transactions.** The main IP is **2001:8d8:105:1:0:1:0:7**, located in **Germany** and belongs to IONOS-AS IONOS SE, DE. The main domain is **www.kuga-sicherheit.de**.
TLS certificate: Issued by *Sectigo RSA Domain Validation Secure ...* on March 17th 2025. Valid for: a year.

This is the only time *www.kuga-sicherheit.de* was scanned on urlscan.io!

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *www.kuga-sicherheit.de*
Current DNS A record: 212.227.172.252 (AS8560 - IONOS-AS IONOS SE, DE)

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

| ⇄ | IP Address | | AS Autonomous System |
|---|---|---|---|
| 1 ➔ 1 | 2001:8d8:100f:f000::200 | DE | 8560 (IONOS-AS IONOS SE) |
| 25 | 2001:8d8:105:1:0:1:0:7 | DE | 8560 (IONOS-AS IONOS SE) |
| 2 | 2001:8d8:105:1::e | DE | 8560 (IONOS-AS IONOS SE) |
| 27 | 2 | | |

Screenshot

Page Title

*KUGA Sicherheit - Ihr zuverlässiger Sicherheitsdienstleister*

Page URL History

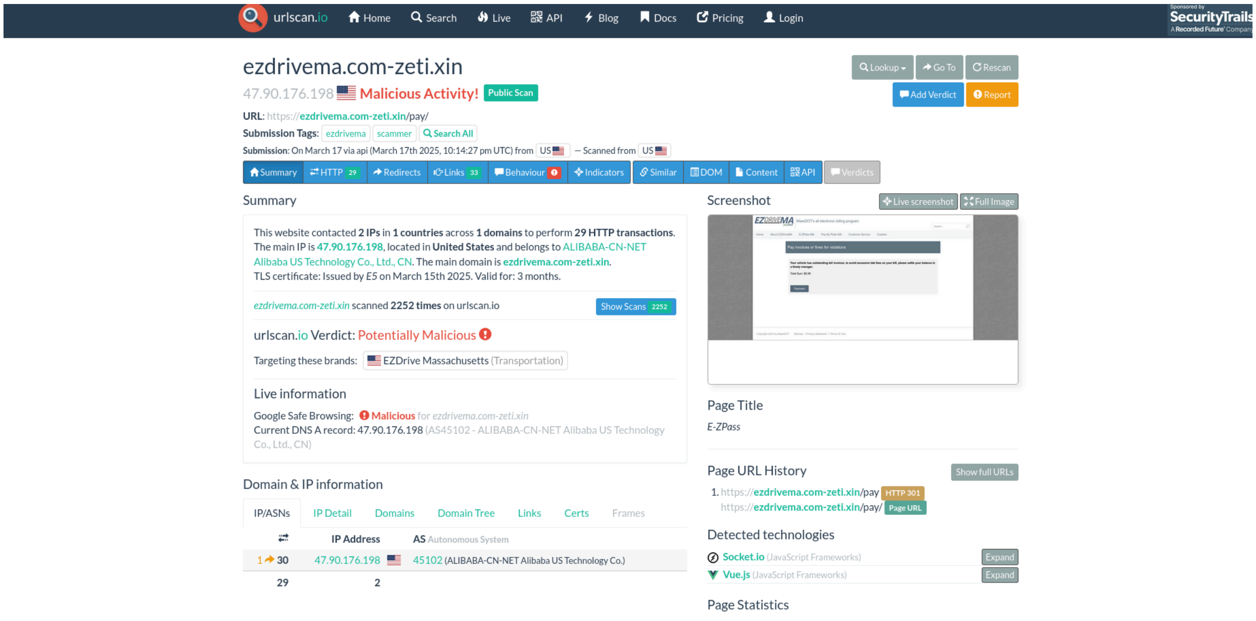
1. https://kuga-sicherheit.de/ HTTP 301
   https://www.kuga-sicherheit.de/ Page URL

Detected technologies

WordPress (CMS)

Page Statistics

27 100 % 100 % 2 4



ezdrivema.com-zeti.xin

47.90.176.198 Malicious Activity! Public Scan

**URL:** https://ezdrivema.com-zeti.xin/pay/
**Submission Tags:** ezdrivema scammer Search All
**Submission:** On March 17 via api (March 17th 2025, 10:14:27 pm UTC) from US — Scanned from US

Summary

This website contacted **2 IPs** in **1 countries** across **1 domains** to perform **29 HTTP transactions.** The main IP is **47.90.176.198**, located in **United States** and belongs to ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN. The main domain is **ezdrivema.com-zeti.xin**.
TLS certificate: Issued by *E5* on March 15th 2025. Valid for: 3 months.

*ezdrivema.com-zeti.xin* scanned **2252 times** on urlscan.io Show Scans 2252

urlscan.io Verdict: Potentially Malicious ❗

Targeting these brands: EZDrive Massachusetts (Transportation)

Live information

Google Safe Browsing: ❗ Malicious for *ezdrivema.com-zeti.xin*
Current DNS A record: 47.90.176.198 (AS45102 - ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

Domain & IP information

IP/ASNs IP Detail Domains Domain Tree Links Certs Frames

| ⇄ | IP Address | | AS Autonomous System |
|---|---|---|---|
| 1 ➔ 30 | 47.90.176.198 | US | 45102 (ALIBABA-CN-NET Alibaba US Technology Co.) |
| 29 | 2 | | |

Screenshot

Page Title

*E-ZPass*

Page URL History

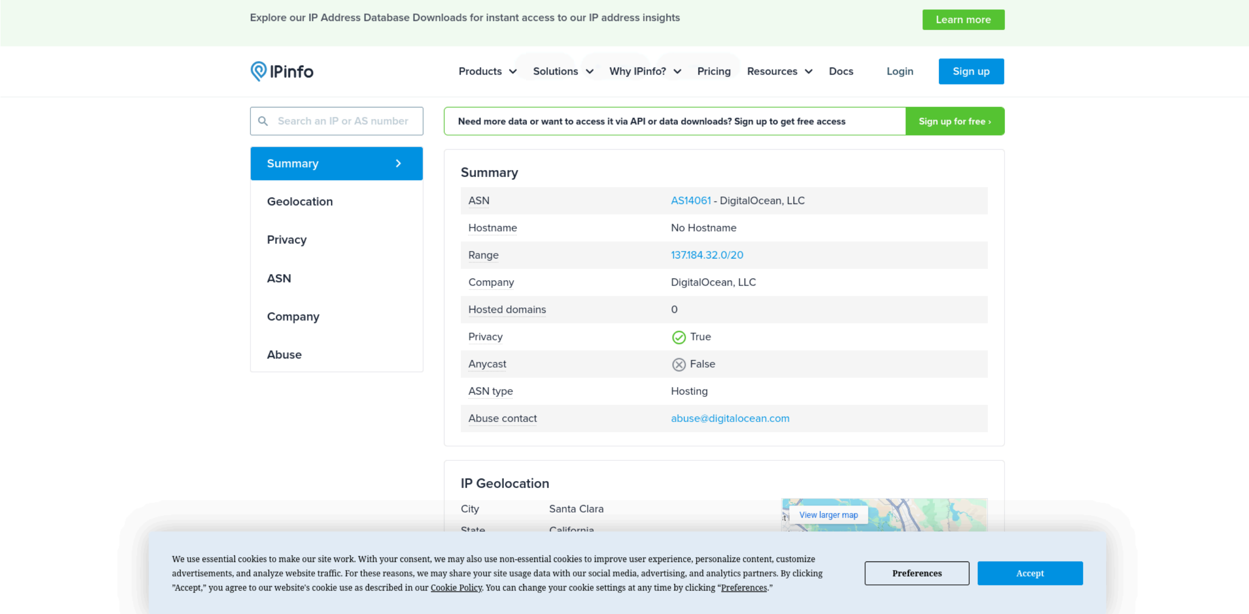
1. https://ezdrivema.com-zeti.xin/pay HTTP 301
   https://ezdrivema.com-zeti.xin/pay/ Page URL

Detected technologies

Socket.io (JavaScript Frameworks)
Vue.js (JavaScript Frameworks)

Page Statistics

- IPinfo.io (https://ipinfo.io) – IP address lookup



Explore our IP Address Database Downloads for instant access to our IP address insights

Need more data or want to access it via API or data downloads? Sign up to get free access

Summary

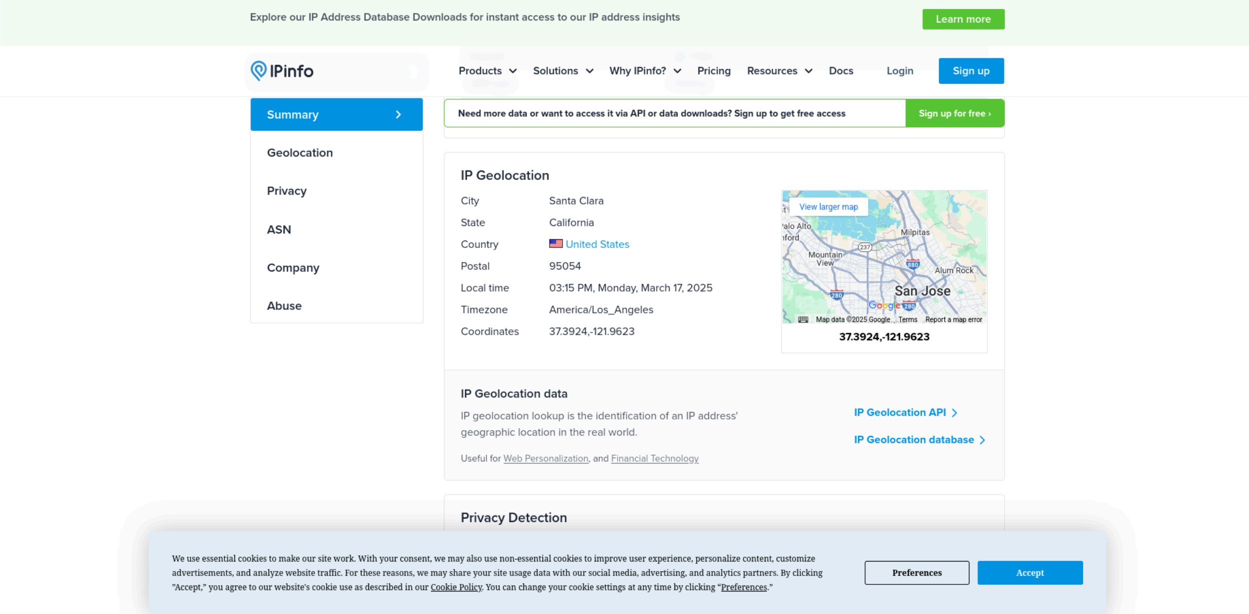
| | |
|---|---|
| ASN | AS14061 - DigitalOcean, LLC |
| Hostname | No Hostname |
| Range | 137.184.32.0/20 |
| Company | DigitalOcean, LLC |
| Hosted domains | 0 |
| Privacy | ✓ True |
| Anycast | ☒ False |
| ASN type | Hosting |
| Abuse contact | abuse@digitalocean.com |

IP Geolocation

City Santa Clara

State California

We use essential cookies to make our site work. With your consent, we may also use non-essential cookies to improve user experience, personalize content, customize advertisements, and analyze website traffic. For these reasons, we may share your site usage data with our social media, advertising, and analytics partners. By clicking "Accept," you agree to our website's cookie use as described in our Cookie Policy. You can change your cookie settings at any time by clicking "Preferences."



Explore our IP Address Database Downloads for instant access to our IP address insights

Need more data or want to access it via API or data downloads? Sign up to get free access

IP Geolocation

| | |
|---|---|
| City | Santa Clara |
| State | California |
| Country | United States |
| Postal | 95054 |
| Local time | 03:15 PM, Monday, March 17, 2025 |
| Timezone | America/Los_Angeles |
| Coordinates | 37.3924,-121.9623 |

37.3924,-121.9623

IP Geolocation data

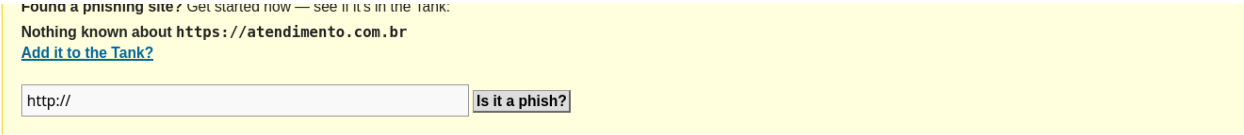
IP geolocation lookup is the identification of an IP address' geographic location in the real world.

Useful for Web Personalization, and Financial Technology

Privacy Detection

We use essential cookies to make our site work. With your consent, we may also use non-essential cookies to improve user experience, personalize content, customize advertisements, and analyze website traffic. For these reasons, we may share your site usage data with our social media, advertising, and analytics partners. By clicking "Accept," you agree to our website's cookie use as described in our Cookie Policy. You can change your cookie settings at any time by clicking "Preferences."

- PhishTank (https://www.phishtank.com) – Phishing link verification



**Found a phishing site?** Get started now — see if it's in the Tank:

Nothing known about `https://atendimento.com.br`
Add it to the Tank?

# Email Header Analysis

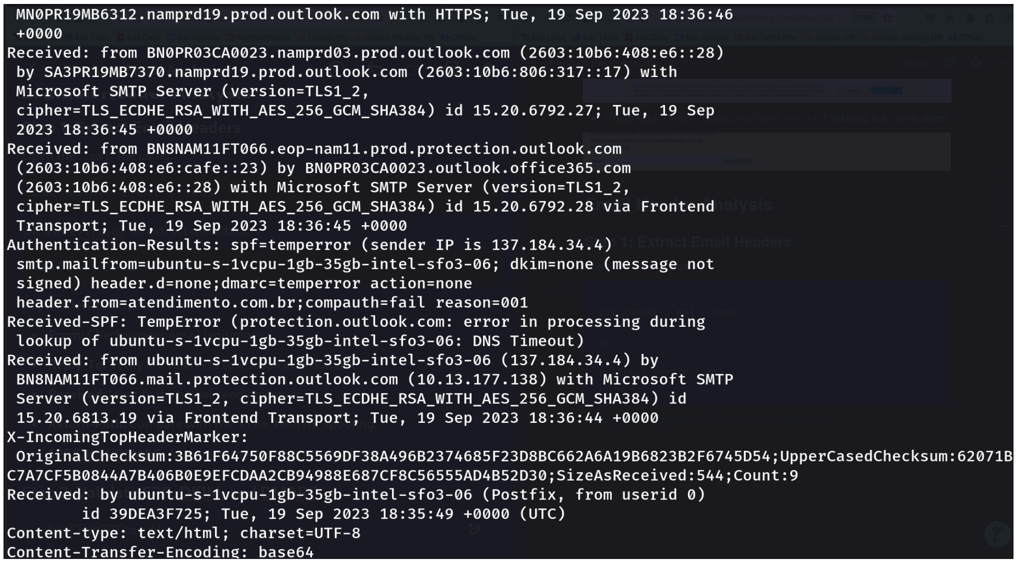
## Step 1: Extract Email Headers

open the .eml file using:

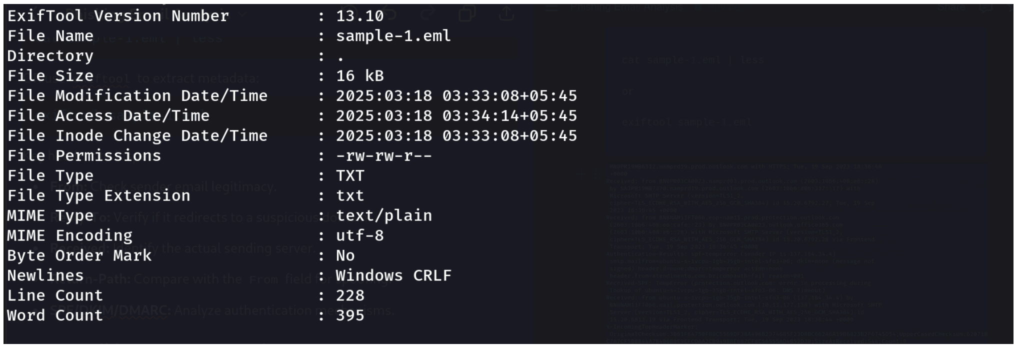
```
cat sample-1.eml | less

or

exiftool sample-1.eml
```



```
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46
 +0000
Received: from BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28)
 by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.27; Tue, 19 Sep
 2023 18:36:45 +0000
Received: from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com
 (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com
 (2603:10b6:408:e6::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend
 Transport; Tue, 19 Sep 2023 18:36:45 +0000
Authentication-Results: spf=temperror (sender IP is 137.184.34.4)
 smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not
 signed) header.d=none;dmarc=temperror action=none
 header.from=atendimento.com.br;compauth=fail reason=001
Received-SPF: TempError (protection.outlook.com: error in processing during
 lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)
Received: from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4) by
 BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6813.19 via Frontend Transport; Tue, 19 Sep 2023 18:36:44 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071B
C7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Count:9
Received: by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)
        id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
Content-type: text/html; charset=UTF-8
Content-Transfer-Encoding: base64
```



```
ExifTool Version Number         : 13.10
File Name                       : sample-1.eml
Directory                       : .
File Size                       : 16 kB
File Modification Date/Time     : 2025:03:18 03:33:08+05:45
File Access Date/Time           : 2025:03:18 03:34:14+05:45
File Inode Change Date/Time     : 2025:03:18 03:33:08+05:45
File Permissions                : -rw-rw-r--
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : utf-8
Byte Order Mark                 : No
Newlines                        : Windows CRLF
Line Count                      : 228
Word Count                      : 395
```

## Key headers to inspect:

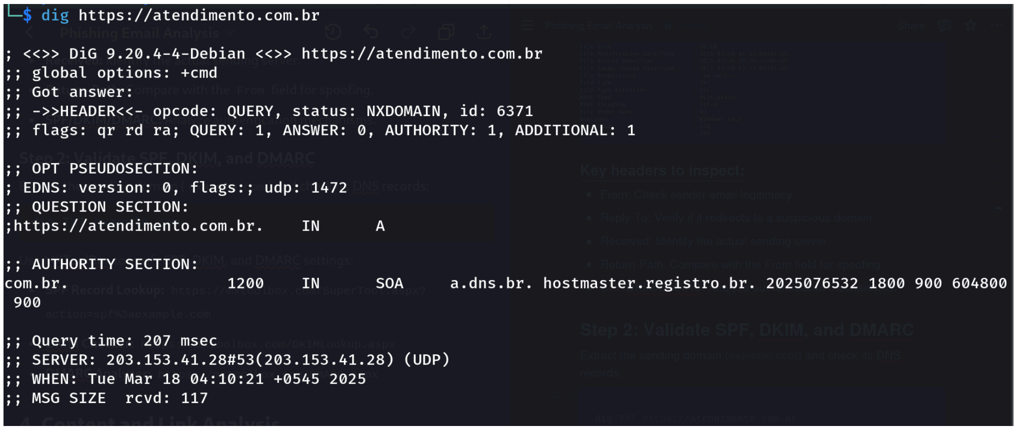
- From: Check sender email legitimacy.
- Reply-To: Verify if it redirects to a suspicious domain.
- Received: Identify the actual sending server.

- Return-Path: Compare with the From field for spoofing.
- SPF/DKIM/DMARC: Analyze authentication mechanisms.

## Step 2: Validate SPF, DKIM, and DMARC

Extract the sending domain (example.com) and check its DNS records:

```
dig TXT https://atendimento.com.br
```



```
└─$ dig https://atendimento.com.br

; <<>> DiG 9.20.4-4-Debian <<>> https://atendimento.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6371
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;https://atendimento.com.br.    IN      A

;; AUTHORITY SECTION:
com.br.                 1200    IN      SOA     a.dns.br. hostmaster.registro.br. 2025076532 1800 900 604800
 900

;; Query time: 207 msec
;; SERVER: 203.153.41.28#53(203.153.41.28) (UDP)
;; WHEN: Tue Mar 18 04:10:21 +0545 2025
;; MSG SIZE  rcvd: 117
```

### Use MXToolBox to verify SPF, DKIM, and DMARC settings:

- SPF Record Lookup: https://mxtoolbox.com/SuperTool.aspx?action=spf%3Aexample.com
- DKIM Checker: https://mxtoolbox.com/DKIMLookup.aspx
- DMARC Analyzer: https://mxtoolbox.com/DMARC.aspx

# Content and Link Analysis

## Step 1: Extract Links from the email

```
grep -oP '(http|https)://[^"\s]+' sample-1.eml
```

### Analyze extracted URLs:

- Check with VirusTotal: https://www.virustotal.com/gui/home/url

- Scan with URLScan.io: https://urlscan.io/
- Verify with PhishTank: https://www.phishtank.com/

### Step 2: Fetch URL Headers (Without Clicking)

```
curl -I https://atendimento.com.br
```

Look for redirects, suspicious headers, or anomalies.

## Attachment Analysis (If applicable)

### Step 1: Extract and Identify File Type

```
file attachment.pdf
```

### Step 2: Analyze for malicious content

```
strings attachment.pdf | less

clamscan --infected --recursive attachment.pdf
```

## Conclusion

### Based on the findings:

- If the email contains spoofed headers, fails SPF/DKIM/DMARC checks, and includes phishing links, it is likely a phishing attack.
- If the domain is newly registered and flagged by OSINT tools, it is highly suspicious.
- If attachments contain malware, they pose a serious threat.

## Recommendations

- Never click on links or download attachments from suspicious emails.

- Verify sender authenticity before taking action.
- Use email filtering solutions to block phishing attempts.
- Educate users on phishing awareness and detection techniques.
- Report phishing emails to security teams or anti-phishing organizations.

> This report provides a structured approach for investigating phishing emails using Kali Linux tools and open-source platforms. By following this methodology, analysts can effectively detect, analyze, and mitigate phishing threats.