

CYBLACK

EMAIL PHISHING INVESTIGATION & FORENSICS

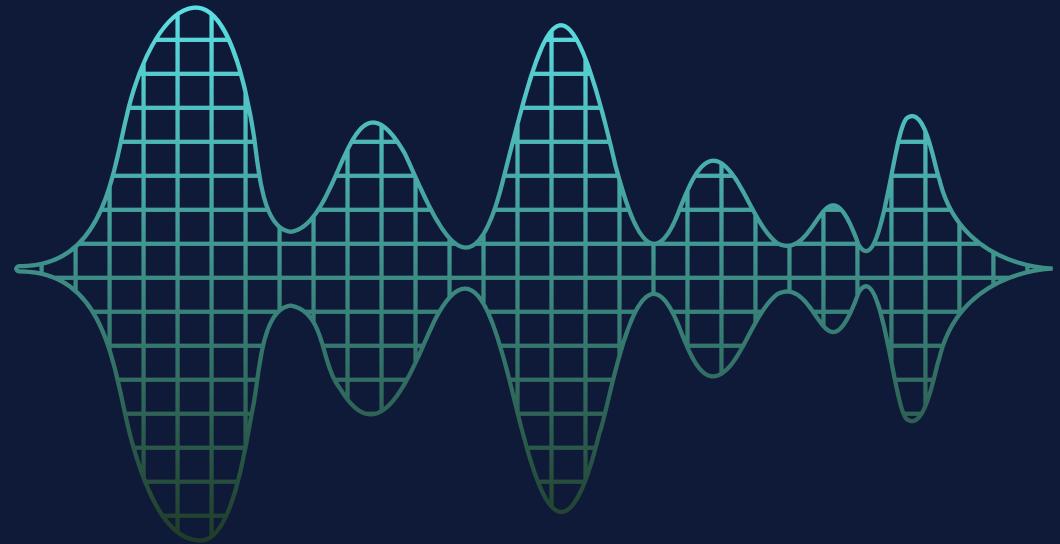
PRESENTATION

```
0.1]: "translation_enabled": false,
0.1]: "protected": false,
0.1]: "verified": false,
0.1]: "followers_count": 0,
0.1]: "friends_count": 0,
0.1]: "listed_count": 0,
0.1]: "favourites_count": 0,
0.1]: "statuses_count": 0,
0.1]: "created_at": "2010-10-04T13:45:37Z",
0.1]: "utc_offset": null,
0.1]: "time_zone": null,
0.1]: "geo_enabled": false,
0.1]: "lang": "en", "meta": {
```

Presented By: SOC TEAM 3
CYBLACK SOC ACADEMY

CONTENT OVERVIEW

- **EXECUTIVE SUMMARY**
- **ASSESSMENT SCOPE & METHODOLOGY**
- **ATTACK ANALYSIS**
- **TECHNICAL FINDINGS**
- **RISK ASSESSMENT**
- **RECOMMENDATIONS**





EXECUTIVE SUMMARY



At Cybertech Solutions, we the security team conducted a comprehensive forensic analysis of a suspicious email claiming to be from Microsoft's Account Team.

Through detailed header analysis and threat intelligence correlation, we identified a sophisticated phishing campaign employing domain spoofing, psychological manipulation, and credential harvesting techniques.



The investigation revealed complete authentication failures (SPF, DKIM, DMARC), blacklisted infrastructure, and multiple indicators of malicious intent, confirming this as a CRITICAL security threat requiring immediate containment and remediation.

OBJECTIVES



ANALYZE EMAIL HEADERS

Perform deep forensic analysis of suspicious email origin and routing path



VERIFY AUTHENTICATION

Validate SPF, DKIM, and DMARC protocols to detect spoofing



IDENTIFY THREATS

Detect phishing indicators and social engineering tactics



PROVIDE REMEDIATION

Deliver actionable security recommendations

KEY FINDINGS

Indicator	Observation	Interpretation
Originating IP	89.144.44.41 (GHOSTNET GmbH, Germany)	Not Microsoft-owned IP; Hosting provider used by attackers
Sender Domain	no-reply@access-accsecurity.com	Fake Microsoft-like domain
Reply-To Address	solutionteamrecognizd03@gmail.com	Suspicious attacker-controlled personal email
SPF/DKIM/DMARC	Failed or Missing	Domain not authorized; likely spoofed
Blacklist Check	IP & Server Blacklisted	Associated with malicious activity

ATTACK METHODOLOGY

5 Attack Techniques

1

DOMAIN SPOOFING

Used "access-accsecurity.com" to impersonate Microsoft

2

SOCIAL ENGINEERING

Created fear and urgency with "unusual sign-in activity" alert

3

HEADER MANIPULATION

Envelope sender mismatch and authentication bypasses

4

CREDENTIAL HARVESTING

Reply-To redirects to attacker-controlled Gmail account

5

TRACKING MECHANISMS

Hidden tracking links to monitor email opens and victim behavior

AUTHENTICATION FAILURES



SECURITY PROTOCOL VALIDATION

SPF (Sender Policy Framework)

- Status: FAILED ✗
- Result: None - Domain has no SPF record
- Impact: Sending IP not authorized

DKIM (DomainKeys Identified Mail)

- Status: FAILED ✗
- Result: No signature present
- Impact: Email cannot be cryptographically verified

DMARC (Domain-based Message Authentication)

- Status: FAILED ✗
- Result: Permerror - Permanent validation failure
- Impact: Domain authentication misconfigured

X-MS-Exchange Authentication

- Status: ANONYMOUS !
- Result: Sender not authenticated to Microsoft services

RISK ASSESSMENT



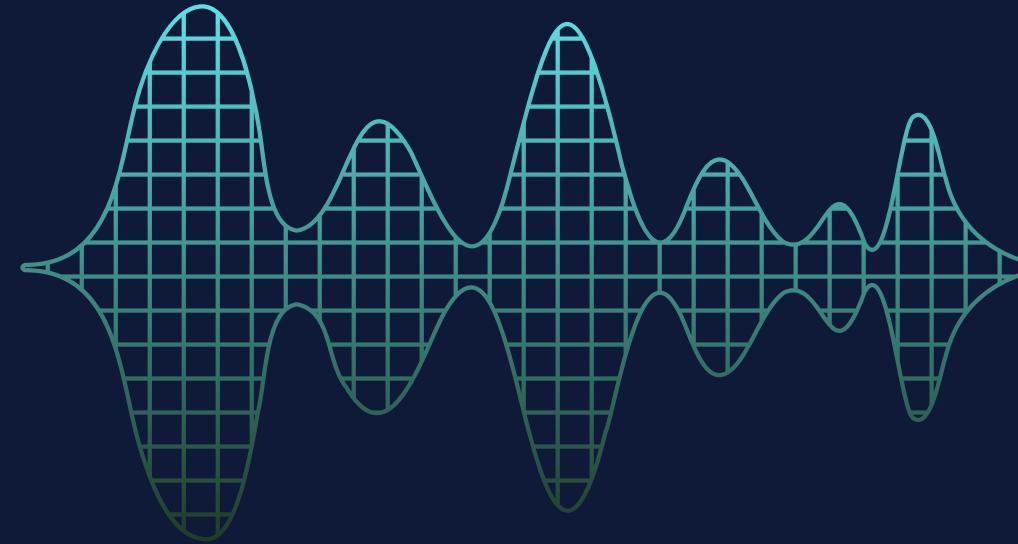
Risk Scoring Table

Risk Category	Max Score	Actual Score	Rating
Originating IP	75	75	CRITICAL
Sender Domain	40	40	CRITICAL
Reply-To Address	20	20	HIGH
SPF/DKIM/DMARC	135	135	CRITICAL

CONFIDENCE LEVEL: HIGH (95%+)

ASSESSMENT METHOD: Manual Forensic Analysis

INDICATORS OF COMPROMISE (IOCS)



MALICIOUS DOMAINS

- **access-accsecurity.com** (spoofed sender)
- **atujpdfghher.co.uk** (envelope sender)
- **thebandalisy.com** (tracking domain)



IP ADDRESSES

- **89.144.44.41** (originating IP - GHOSTNET GmbH)
- **103.225.77.255** (false IP claimed in email body)



EMAIL ADDRESSES

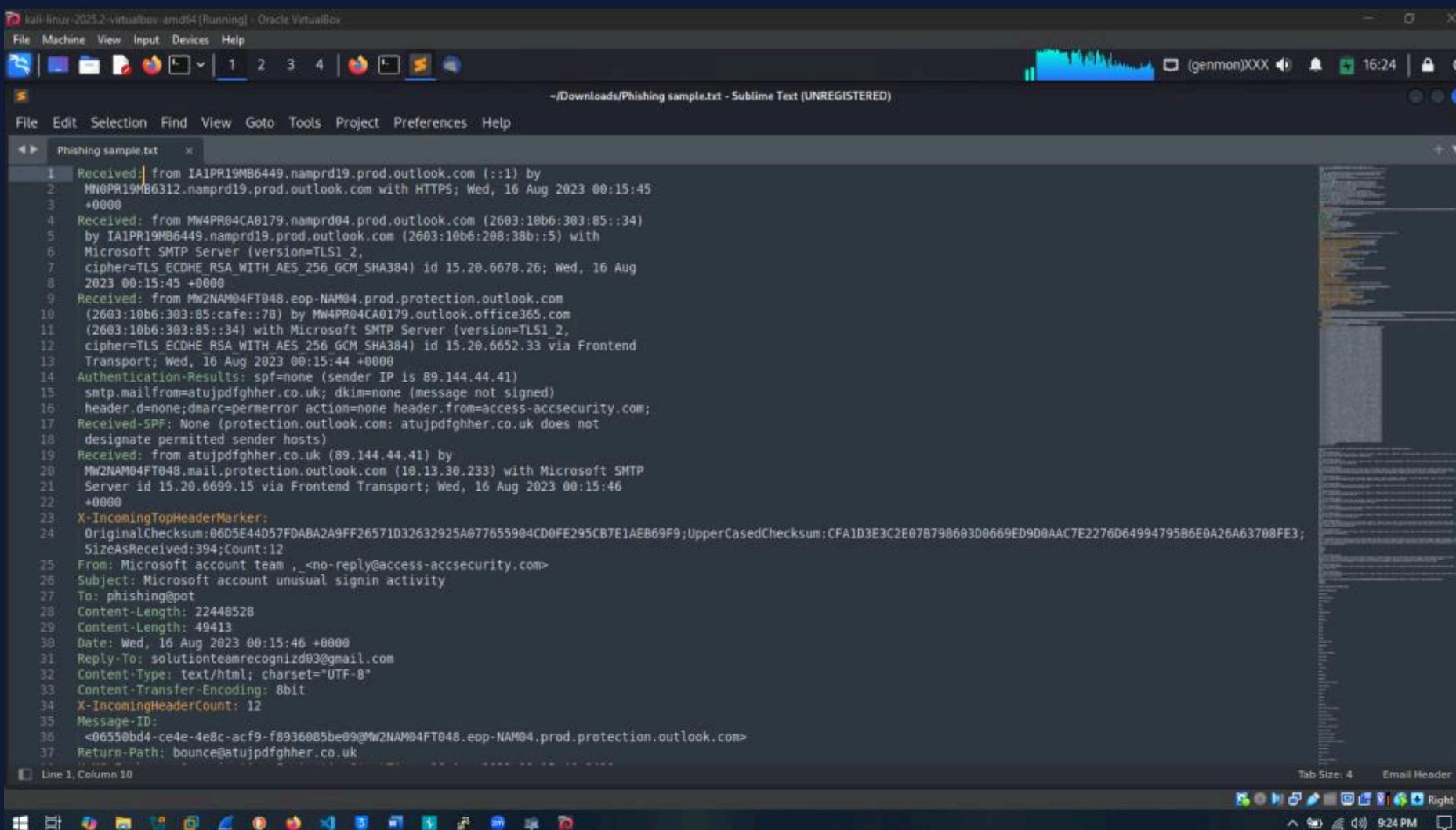
- **no-reply@access-accsecurity.com** (display sender)
- **bounce@atujpdfghher.co.uk** (return path)
- **solutionteamrecognizd03@gmail.com** (Reply-To)



TRACKING URL

- **<http://thebandalisy.com/track/o41799GCMXp22448528...>**

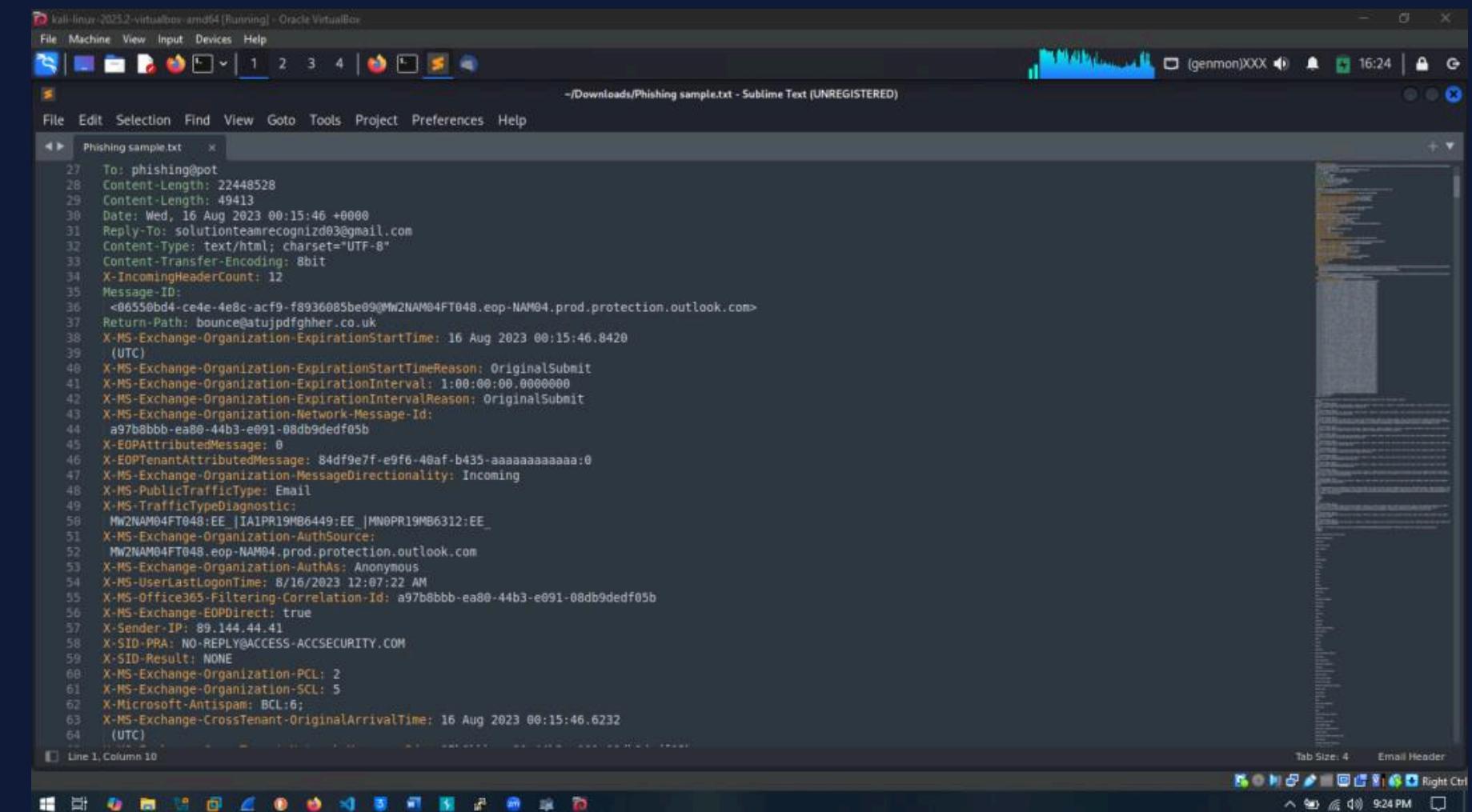
FORENSIC EVIDENCE



```
Received: from IA1PR19MB6449.namprd19.prod.outlook.com (::1) by MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Wed, 16 Aug 2023 00:15:45 +0000
Received: from Mw4PR04CA0179.namprd04.prod.outlook.com (2603:10b6:303:85::34) by IA1PR19MB6449.namprd19.prod.outlook.com (2603:10b6:208:38b::5) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6678.26; Wed, 16 Aug 2023 00:15:45 +0000
Received: from Mw2NAM04FT048.eop-NAM04.prod.protection.outlook.com (2603:10b6:303:85::cafe::78) by Mw4PR04CA0179.outlook.office365.com (2603:10b6:303:85::34) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6652.33 via Frontend Transport; Wed, 16 Aug 2023 00:15:44 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.41)
smtp.mailfrom=atujpdfghher.co.uk; dkim=none (message not signed)
.header.d=none; dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF: None (protection.outlook.com: atujpdfghher.co.uk does not designate permitted sender hosts)
Received: from atujpdfghher.co.uk (89.144.44.41) by Mw2NAM04FT048.mail.protection.outlook.com (10.13.30.233) with Microsoft SMTP Server id 15.20.6699.15 via Frontend Transport; Wed, 16 Aug 2023 00:15:46 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:0605E44D57FDABA2A9FF26571D32632925A077655904CD0FE295CB7E1AEB69F9;UpperCasedChecksum:CFA1D3E3C2E07B790603D0669ED9D0AAC7E2276D6499479586E0A26A63708FE3;
SizeAsReceived:394;Count:12
From: Microsoft account team , <no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Wed, 16 Aug 2023 00:15:46 +0000
Reply-To: solutionteamrecognizd03@gmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID: <06550bd4-ce4e-4e8c-acf9-f8936085be09@Mw2NAM04FT048.eop-NAM04.prod.protection.outlook.com>
Return-Path: bounce@atujpdfghher.co.uk
Line 1, Column 10
```

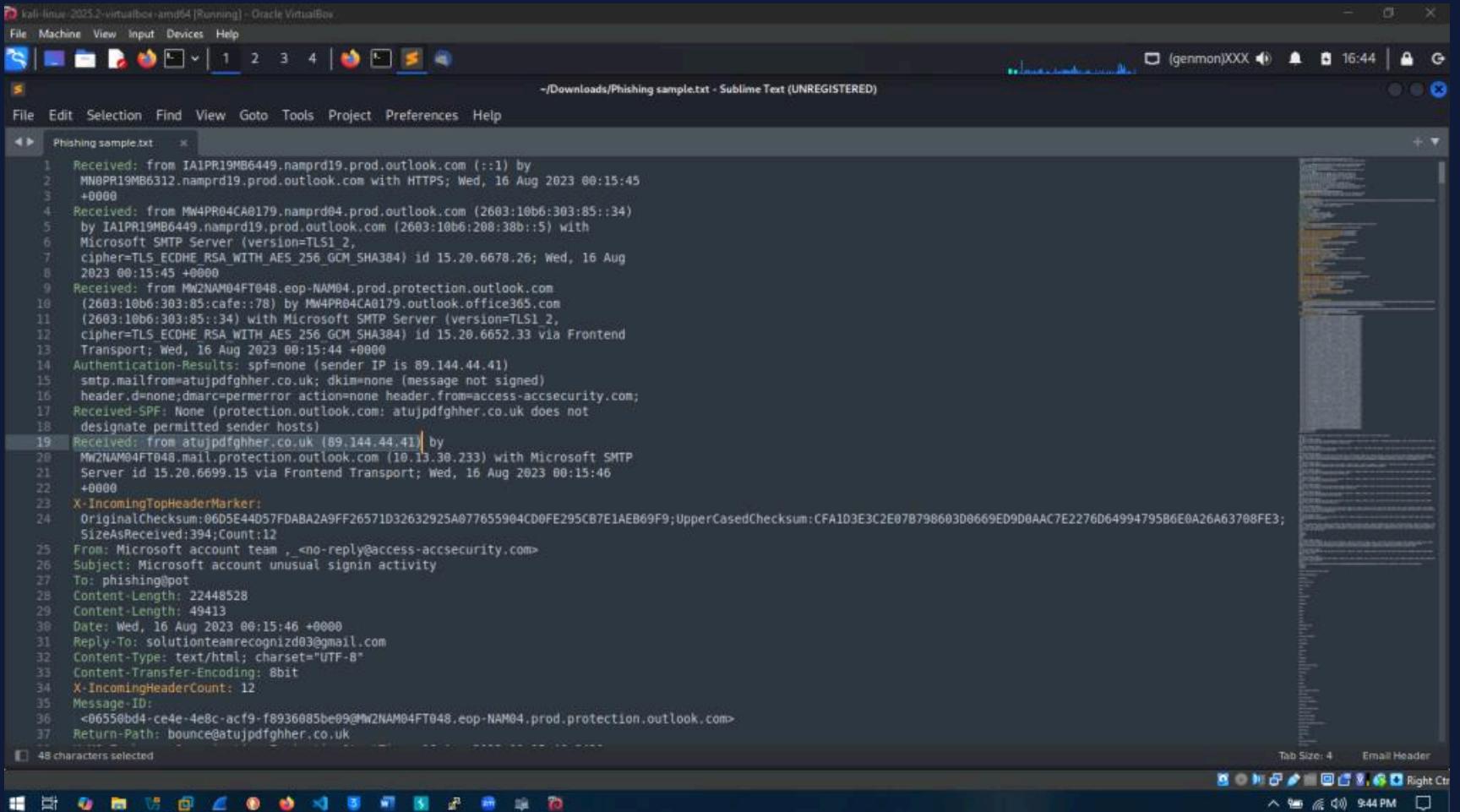
Email Header Analysis

SPF/DKIM/DMARC Results



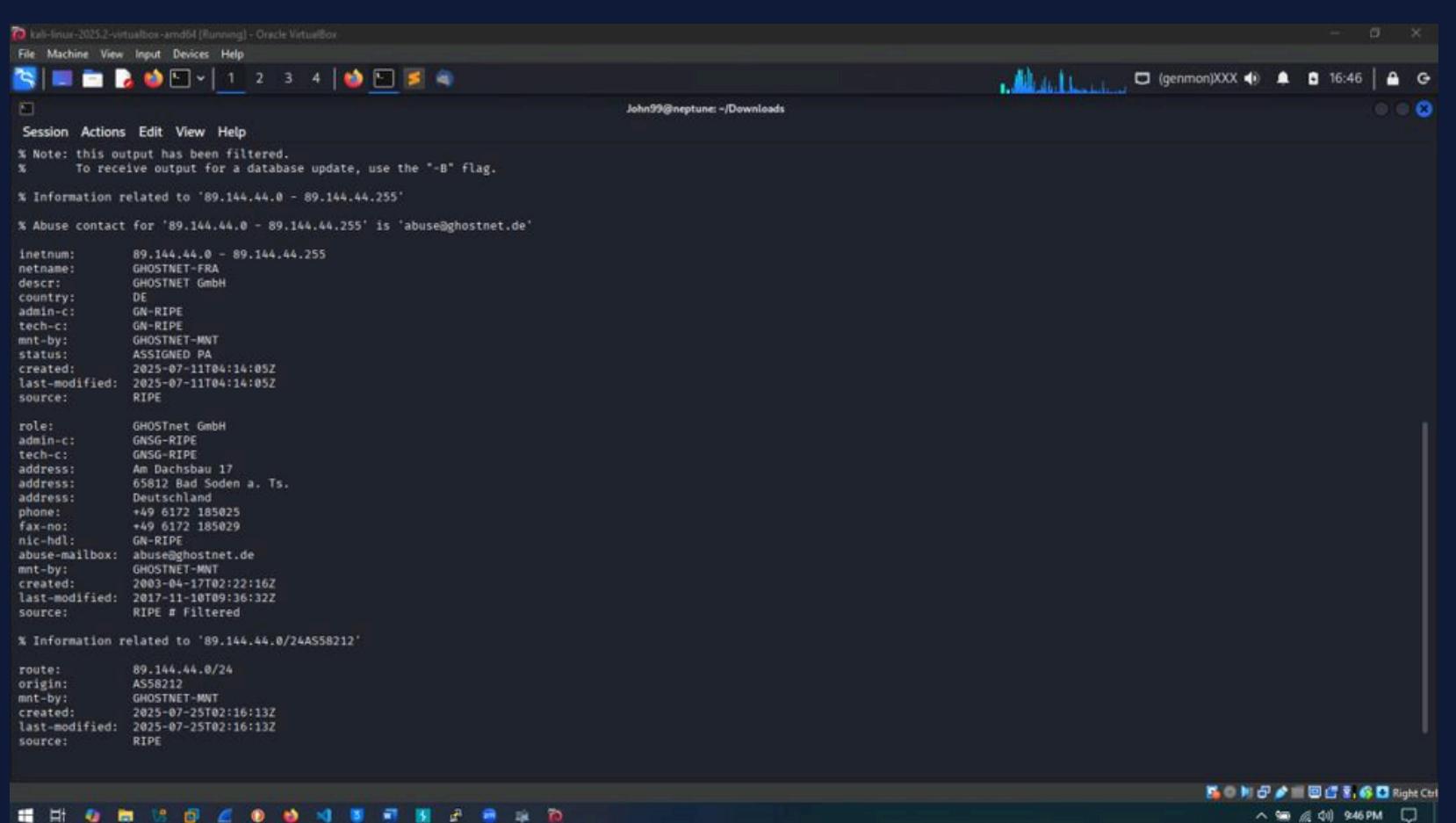
```
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Wed, 16 Aug 2023 00:15:46 +0000
Reply-To: solutionteamrecognizd03@gmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID: <06550bd4-ce4e-4e8c-acf9-f8936085be09@Mw2NAM04FT048.eop-NAM04.prod.protection.outlook.com>
Return-Path: bounce@atujpdfghher.co.uk
X-MS-Exchange-Organization-ExpirationStartTime: 16 Aug 2023 00:15:46.8420 (UTC)
X-MS-Exchange-Organization-ExpirationTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00.00.000000
X-MS-Exchange-Organization-Network-Message-Id: a97b0bbb-ea0-44b3-e091-08db9dedf05b
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435aaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-MS-PublicTrafficType: Email
X-MS-TrafficTypeDiagnostic:
Mw2NAM04FT048.IEE_|A1PR19MB6449.IEE_|MN0PR19MB6312.IEE_
X-MS-Exchange-Organization-AuthSource: Mw2NAM04FT048.eop-NAM04.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-UserLastLogonTime: 8/16/2023 12:07:22 AM
X-MS-Office365-Filtering-Relation-Id: a97b0bbb-ea0-44b3-e091-08db9dedf05b
X-MS-Exchange-EDirect: true
X-Sender-IP: 89.144.44.41
X-SID-PRA: NO-REPLY@ACCESS-ACCSECURITY.COM
X-SID-Result: NONE
X-MS-Exchange-Organization-PCL: 2
X-MS-Exchange-Organization-SCL: 5
X-Microsoft-Antispam: BCL:6
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 16 Aug 2023 00:15:46.6232 (UTC)
Line 1, Column 10
```

FORENSIC EVIDENCE (CONTD)



The screenshot shows a Kali Linux desktop environment with a Sublime Text window open. The window title is 'Phishing sample.txt'. The content of the file is a long string of text representing a phishing email message. The text includes various headers such as 'Received', 'From', 'To', 'Subject', and 'Content-Type', along with body content and footer information. The file is identified as being UNREGISTERED.

```
Received: from IAIPR19MB6449.namprd19.prod.outlook.com (:) by MNOPR19MB6312.namprd19.prod.outlook.com with HTTPS; Wed, 16 Aug 2023 00:15:45 +0000
Received: from MW4PR04CA0179.namprd04.prod.outlook.com (2603:10b6:303:85::34) by IAIPR19MB6449.namprd19.prod.outlook.com (2603:10b6:200:30b::5) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6678.26; Wed, 16 Aug 2023 00:15:45 +0000
Received: from MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com (2603:10b6:303:85::cafe::78) by MW4PR04CA0179.outlook.office365.com (2603:10b6:303:85::34) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6652.33 via Frontend Transport; Wed, 16 Aug 2023 00:15:45 +0000
Authentication-Results: spf=none (sender IP is 89.144.44.41)
smtp.mailfrom=atujpdfghher.co.uk; dkim=none (message not signed)
header.d=none;dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF: None (protection.outlook.com: atujpdfghher.co.uk does not designate permitted sender hosts)
Received: from atujpdfghher.co.uk [89.144.44.41] by MW2NAM04FT048.mail.protection.outlook.com (10.13.38.233) with Microsoft SMTP Server
Server id 15.20.6699.15 via Frontend Transport; Wed, 16 Aug 2023 00:15:46 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:06D5E44D57FDABA2A9FF26571D32632925A077655904C0FE295CB7E1AEB69F9;UpperCasedChecksum:CFA1D3E3C2E078798603D0669ED9D0AAC7E2276D64994795B6E0A26A63708FE3;
SizeAsReceived:394;Count:12
From: Microsoft account team ,<no-reply@access-accsecurity.com>
Subject: Microsoft account unusual signin activity
To: phishing@pot
Content-Length: 22448528
Content-Length: 49413
Date: Wed, 16 Aug 2023 00:15:46 +0000
Reply-To: solutionteamrecogniz0@gmail.com
Content-type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
X-IncomingHeaderCount: 12
Message-ID: <06550d4-d4e4-4e8c-acf9-f8936085be09@MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com>
Return-Path: bounce@atujpdfghher.co.uk
48 characters selected
```



The screenshot shows a Kali Linux desktop environment with a terminal window open. The window title is 'John99@neptune: ~/Downloads'. The terminal output displays a WHOIS record for the IP address 89.144.44.255. The record includes information such as the network name (GHOSTNET-FRA), description (GHOSTNET GmbH), country (DE), administrative contact (GN-RIPE), technical contact (GN-RIPE), and management contact (GHOSTNET-MNT). It also shows the status (ASSIGNED PA), creation date (2025-07-11T04:14:05Z), last modification date (2025-07-11T04:14:05Z), and source (RIPE). The output is preceded by a note stating 'Session Actions Edit View Help % Note: this output has been filtered.' and '% To receive output for a database update, use the "-B" flag.'

```
Session Actions Edit View Help
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '89.144.44.0 - 89.144.44.255'

% Abuse contact for '89.144.44.0 - 89.144.44.255' is 'abuse@ghostnet.de'

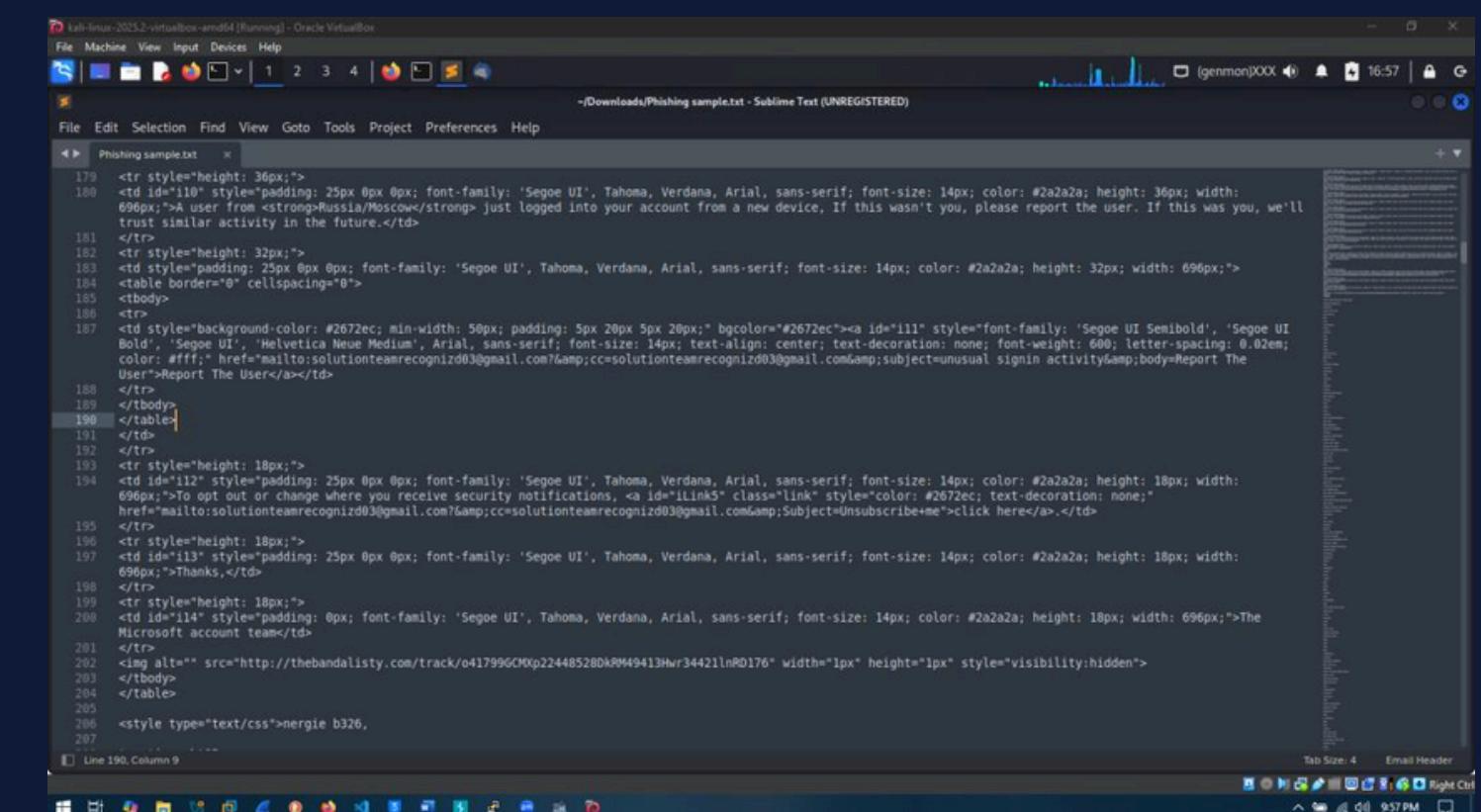
inetnum: 89.144.44.0 - 89.144.44.255
netname: GHOSTNET-FRA
descr: GHOSTNET GmbH
country: DE
admin-c: GN-RIPE
tech-c: GN-RIPE
mnt-by: GHOSTNET-MNT
status: ASSIGNED PA
created: 2025-07-11T04:14:05Z
last-modified: 2025-07-11T04:14:05Z
source: RIPE

role: GHOSTNet GmbH
admin-c: GNSG-RIPE
tech-c: GNSG-RIPE
address: Am Dachsbau 17
address: 65812 Bad Soden a. Ts.
address: Deutschland
phone: +49 6172 185025
fax-no: +49 6172 185029
nic-hdl: GNS-RIPE
abuse-mailbox: abuse@ghostnet.de
mnt-by: GHOSTNET-MNT
created: 2003-04-17T02:22:16Z
last-modified: 2017-11-10T09:36:32Z
source: RIPE # Filtered

% Information related to '89.144.44.0/24AS58212'

route: 89.144.44.0/24
origin: AS58212
mnt-by: GHOSTNET-MNT
created: 2025-07-25T02:16:13Z
last-modified: 2025-07-25T02:16:13Z
source: RIPE
```

IP Geolocation Data & Tracking Pixel Detection



The screenshot shows a Kali Linux desktop environment with a Sublime Text window open. The window title is 'Phishing sample.txt'. The content of the file is a long string of HTML code representing a phishing email message. The code includes several tracking pixels, which are represented by small images with specific URLs. These URLs often contain parameters like 'cc', 'subject', and 'body' to track user interactions. The file is identified as being UNREGISTERED.

```
179 <tr style="height: 36px;">
180 <td id="i10" style="padding: 25px 0px 0px; font-family: 'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size: 14px; color: #2a2a2a; height: 36px; width: 696px;">A user from <strong>Russia/Moscow</strong> just logged into your account from a new device. If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.</td>
181 </tr>
182 <tr style="height: 32px;">
183 <td style="padding: 25px 0px 0px; font-family: 'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size: 14px; color: #2a2a2a; height: 32px; width: 696px;">
184 <table border="0" cellspacing="0">
185 <tbody>
186 <tr>
187 <td style="background-color: #2672ec; min-width: 50px; padding: 5px 20px 5px 20px;"><a href="#" id="i11" style="font-family: 'Segoe UI Semibold', 'Segoe UI Bold', 'Segoe UI', 'Helvetica Neue Medium', Arial, sans-serif; font-size: 14px; text-align: center; text-decoration: none; font-weight: 600; letter-spacing: 0.02em; color: #fff;">Report The User</a></td>
188 </tr>
189 </tbody>
190 </table>
191 </td>
192 </tr>
193 <tr style="height: 18px;">
194 <td id="i12" style="padding: 25px 0px 0px; font-family: 'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size: 14px; color: #2a2a2a; height: 18px; width: 696px;">To opt out or change where you receive security notifications, go to <a href="mailto:solutionteamrecogniz0@gmail.com?amp;cc=solutionteamrecogniz0@gmail.com&subject=unusual signin activity&body=Report The User">Report The User</a>.
195 </tr>
196 <tr style="height: 18px;">
197 <td id="i13" style="padding: 25px 0px 0px; font-family: 'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size: 14px; color: #2a2a2a; height: 18px; width: 696px;">Thanks,</td>
198 </tr>
199 <tr style="height: 18px;">
200 <td id="i14" style="padding: 0px; font-family: 'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size: 14px; color: #2a2a2a; height: 18px; width: 696px;">The Microsoft account team/>
201 </tr>
202 
203 </tbody>
204 </table>
205 <style type="text/css">nergie b326,
206 ...
```

REMEDIATION ACTIONS

Three Timeframes



IMMEDIATE (0-30 Days)

- Block malicious IPs and domains
- Quarantine similar emails
- Notify users of phishing campaign
- Enable MFA across all accounts



SHORT-TERM (1-3 Months)

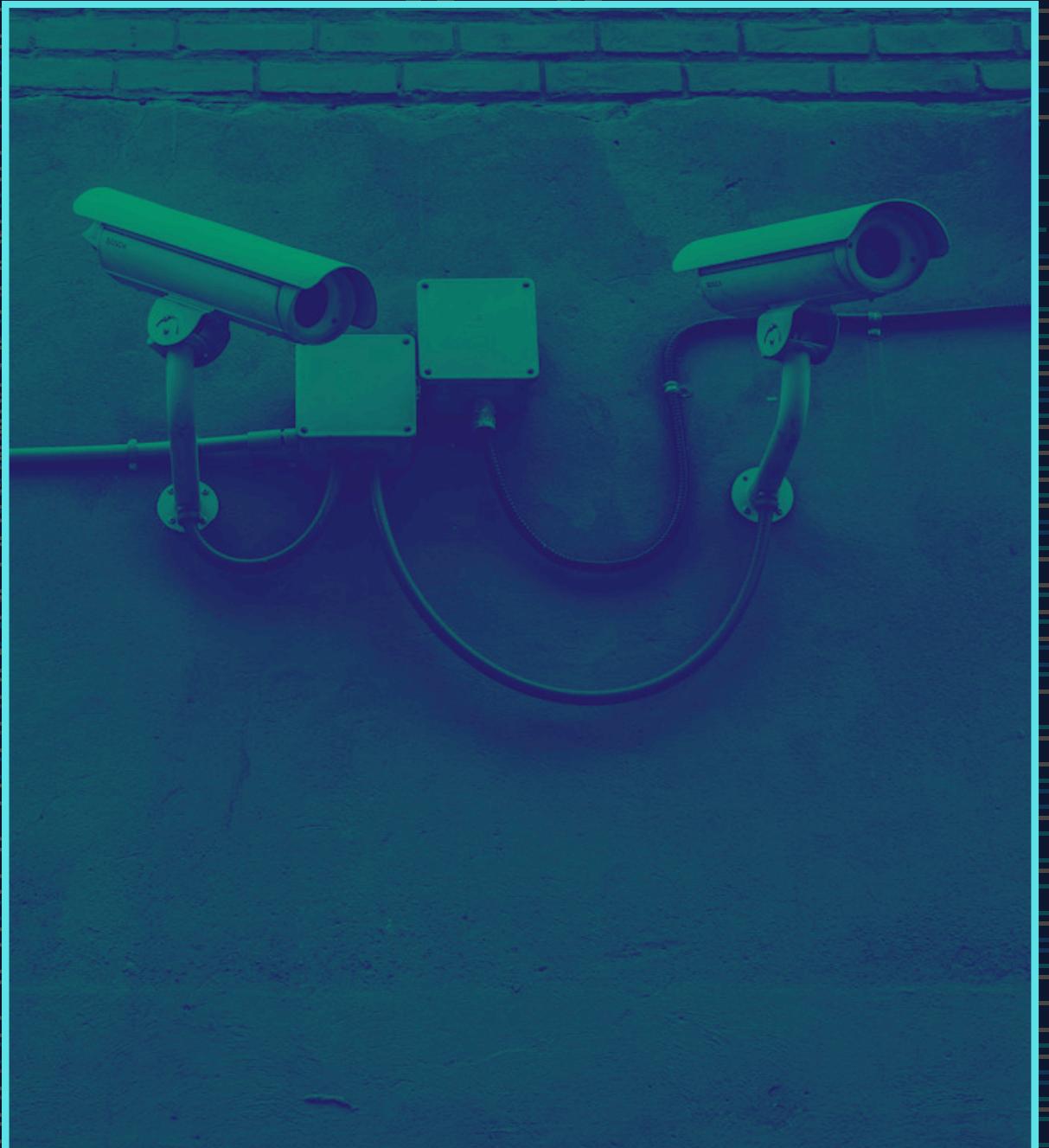
- Implement SPF, DKIM, DMARC enforcement
- Integrate threat intelligence feeds
- Refine email filtering rules



LONG-TERM (3-12 Months)

- Adopt Zero-Trust email model
- Quarterly phishing simulations
- SOAR automation for faster response
- Establish CERT collaboration

CONCLUSION



The forensic investigation successfully identified and analyzed a sophisticated Microsoft impersonation phishing campaign with CRITICAL risk severity.

Through comprehensive header analysis, authentication validation, and threat intelligence correlation, the team confirmed multiple definitive indicators of malicious intent including complete SPF/DKIM/DMARC failures, blacklisted infrastructure, and advanced social engineering tactics.

Immediate containment measures have been recommended, and all IOCs have been documented for threat intelligence sharing and enhanced organizational email security posture.



THANK YOU

Presented By: SOC TEAM 3
CYBLACK SOC ACADEMY