CYBLACK

EMAIL PHISHING INVESTIGATION & FORENSICS

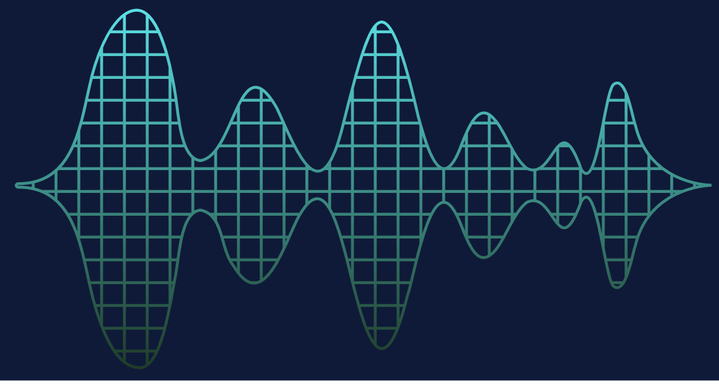
PRESENTATION

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

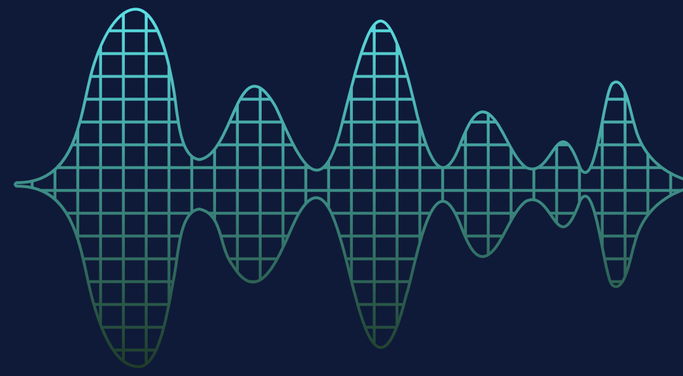
RISK ASSESSMENT

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)
- thebandalisty.com (tracking domain)

IP ADDRESSES

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

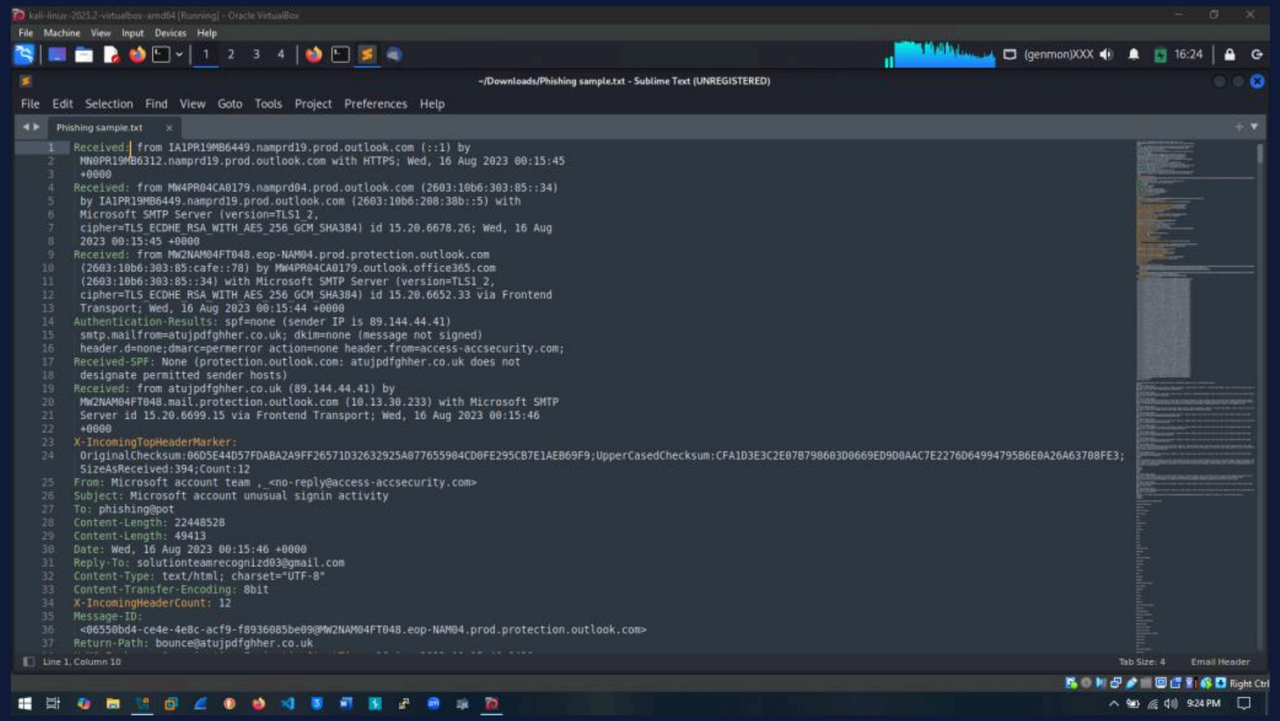
EMAIL ADDRESSES

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

TRACKING URL

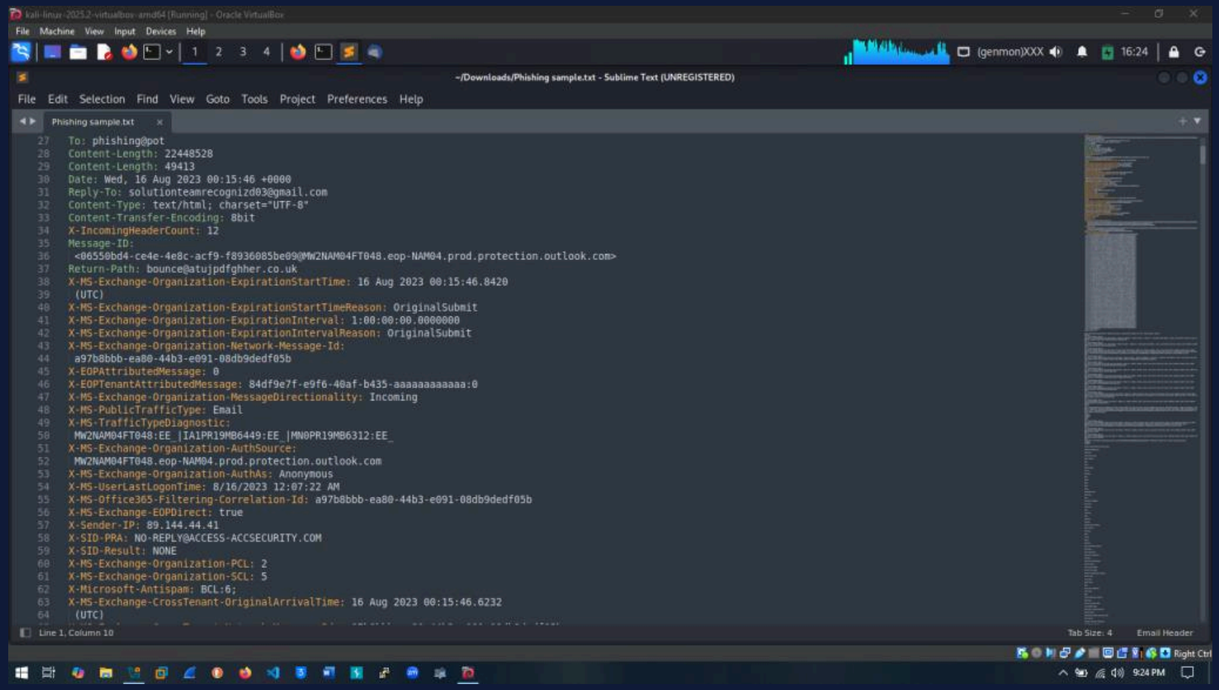
- http://thebandalisty.com/track/o41799GCMXp22448528...

FORENSIC EVIDENCE

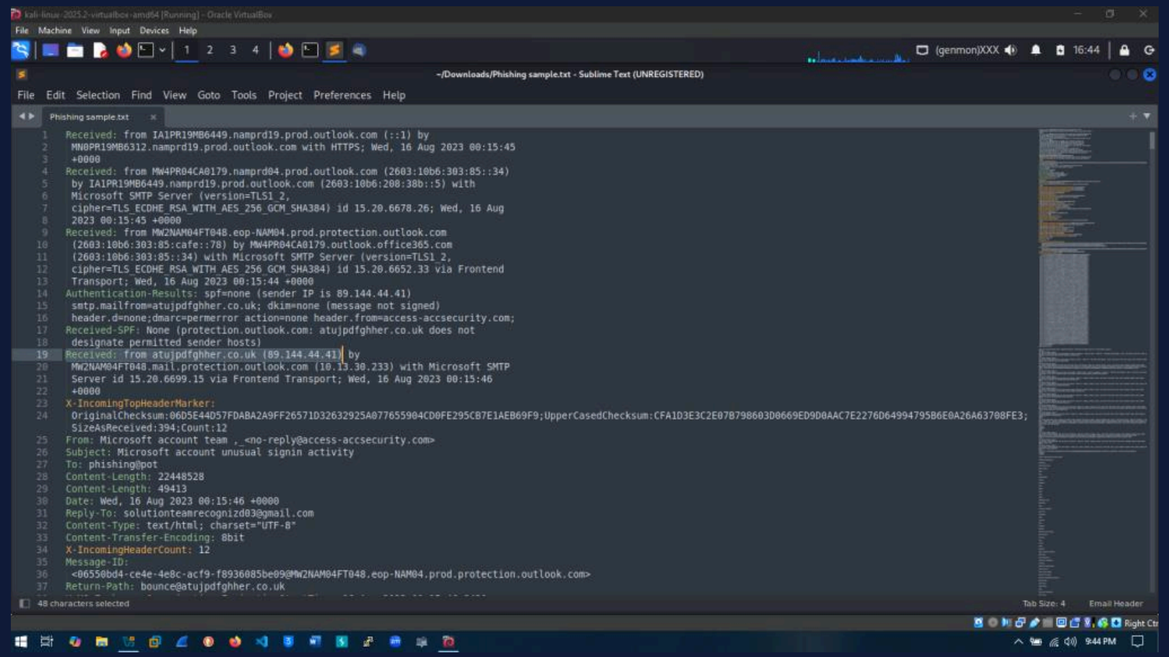


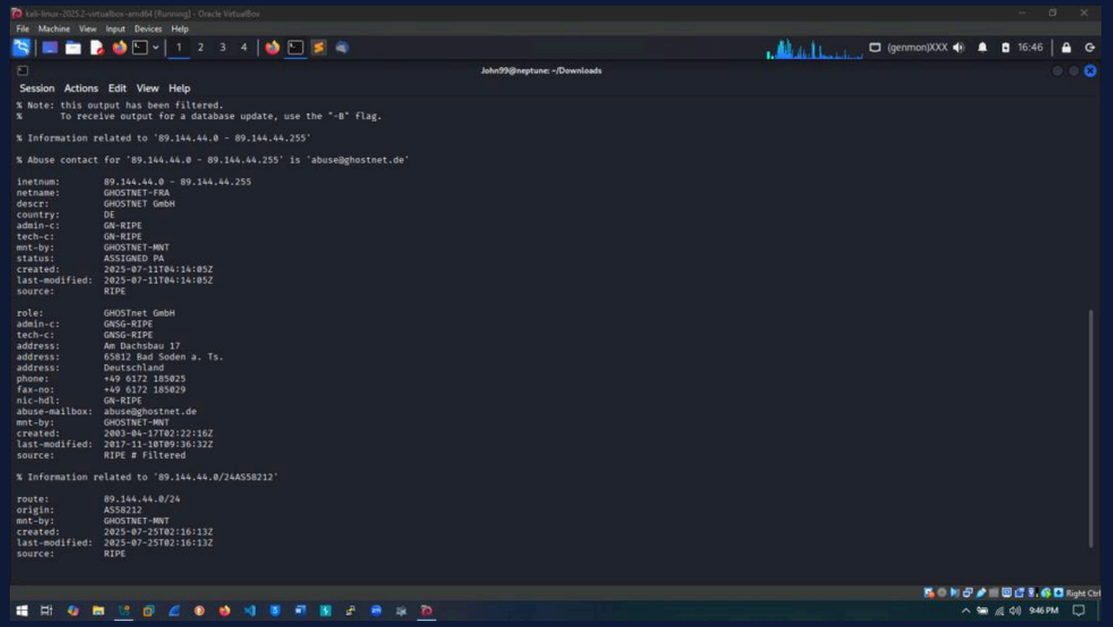
Email Header Analysis

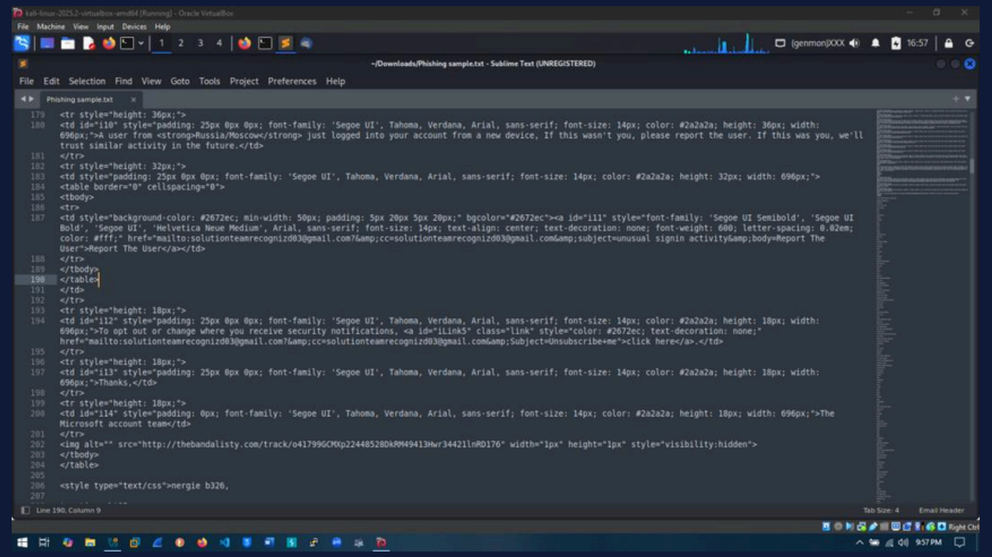
SPF/DKIM/DMARC Results



FORENSIC EVIDENCE (CONTD)







IP Geolocation Data & Tracking Pixel Detection

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