[SOC-AI-AGENT]

Automated Investigation Report

Alert ID: 25439c6e-424c-4657-bbbd-d3c83b52af3f | Generated: 2026-02-13 04:28:23 UTC

Executive Summary

Verdict: FALSE_POSITIVE (82.596% confidence) — benign activity (false positive). Key factors: IOC 91.195.240.12 flagged by 2 source(s) (risk score: 46.6). IOCs appeared in 2 false positive(s). May reduce malicious confidence.

Verdict

Confidence: 82.6%

Alert Details

Field	Value
Alert Type	firewall
Timestamp	2026-02-13T04:27:50.189558
Classification	c2_communication
Initial Severity	LOW

Investigation Timeline

Triage — Complete

Classified as c2_communication. Severity: LOW.

Ioc Extraction — Complete

Extracted 19 IOCs: {'md5': 1, 'url': 4, 'email': 4, 'ipv4': 2, 'domain': 8}

Enrichment — Complete

Enriched 19 IOCs across threat intel sources.

Correlation — Complete

Found 2 related investigation(s). Shared IOCs: 185.234.72.19 (seen 2x). 2 related investigation(s) were previously classified as false positives.

Att&ck Mapping — Complete

Matched 1 techniques across 1 tactics.

Verdict — Complete

FALSE_POSITIVE (confidence: 82.6%)

IOC Enrichment Results

IOC	Type	Risk Score	Sources Flagged	Summary
5f4d3c2b1a0e9f8d7c6b[redacted]938271605		0.0	0 / 3	OTX: 0 pulses reference this IOC. Tags: none
https://company-port[redacted].com/verify		0.0	0 / 3	
http://evil-phish.ru[redacted]steal?id=3D12345&amp		0.0	0 / 3	
https://company-port[redacted].com/verif=		0.0	0 / 3	
http://evil-phish.ru[redacted]rack?id=3D12345&amp		0.0	0 / 3	
it-security-noreply@[redacted]-corp.com		0.0	0 / 0	
mthompson@acme-corp.[redacted]		0.0	0 / 0	
5f4d3c2b1a0e9f8d7c6b[redacted]38271605@acm3-corp.com		0.0	0 / 0	
it-helpdesk-verify@p[redacted]n-secure-mail.ru		0.0	0 / 0	

91.195.240.12	🟩	46.6	2 / 5	VT: 7/93 engines flagged as malicious. AS: SEDO GmbH, Country: DE AbuseIPDB: Abuse confidence 13%, 21 reports. ISP: Sedo Domain Parking, Usage: Data Center/Web Hosting/Transit, Country: DE Shodan: 2 open ports, 0 vulns. Org: Sedo Domain Parking, OS: None, Country: DE OTX: 50 pulses reference this IOC. Tags: threat roundup, cndigicert sha2, checks, media center, alerts GreyNoise: IP not observed scanning the internet

185.234.72.19	🟩	0.0	0 / 5	VT: 0/93 engines flagged as malicious. AS: ITP-Solutions GmbH & Co. KG, Country: DE AbuseIPDB: Abuse confidence 0%, 0 reports. ISP: DeinServerHost, Usage: Data Center/Web Hosting/Transit, Country: DE OTX: 0 pulses reference this IOC. Tags: none GreyNoise: IP not observed scanning the internet
acm3-corp.com	🟩	0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

`acme-corp.com`	🟩	0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: GANDI SAS OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=GANDI SAS, Created=2002-09-25 22:07:45, Expires=2027-09-25 22:07:50, Country=N/A
`mx01.acme-corp.com`	🟩	0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: GANDI SAS OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=GANDI SAS, Created=2002-09-25 22:07:45, Expires=2027-09-25 22:07:50, Country=N/A

mail.acme-corp.com [redacted]		0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: GANDI SAS OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=GANDI SAS, Created=2002-09-25 22:07:45, Expires=2027-09-25 22:07:50, Country=N/A
mail-out.suspicious-[redacted].net		0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A
proton-secure-mail.r[redacted]		0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

company-portal.com	🟩	0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=Netowl, Inc., Created=2024-08-28 14:08:35, Expires=2026-08-28 14:08:35, Country=N/A
evil-phish.ru	🟩	0.0	0 / 4	VT: 0/93 engines flagged as malicious. Registrar: N/A OTX: 0 pulses reference this IOC. Tags: none WHOIS: Registrar=N/A, Created=N/A, Expires=N/A, Country=N/A

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Evidence
Command and Control	T1090	Proxy	`Enrichment tag: generator`

Attack chain analysis:
1. **Command and Control**: Proxy (T1090)

Historical Correlation

Found 2 related investigation(s). Shared IOCs: 185.234.72.19 (seen 2x). 2 related investigation(s) were previously classified as false positives.

Alert ID	Type	Verdict	Matching IOC	Date
c84ae2e5...	firewall	FALSE_POSITIVE	185.234.72.19	2026-02-13T03:56:27.3924
85818467...	firewall	FALSE_POSITIVE	185.234.72.19	2026-02-13T04:14:02.6716

Reasoning Chain

IOC 91.195.240.12 flagged by 2 source(s) (risk score: 46.6).

No significant behavioral indicators detected.

IOCs found in 2 previous investigation(s).

IOCs appeared in 2 false positive(s). May reduce malicious confidence.

Matched 1 MITRE ATT&CK technique(s) across 1 tactic(s).

Alert occurred during off-hours (04:00). Slightly elevated risk.

Score Breakdown

Component	Score	Weight	Weighted Score
Enrichment	46.6	35.0%	16.3
Behavioral	0.0	25.0%	0.0
Correlation	0	20.0%	0.0
Mitre	8	15.0%	1.2
Temporal	20.0	5.0%	1.0

Recommended Response Actions

1. No immediate action required.

2. Consider adding to allowlist/exception list if recurring.

3. Document the false positive for tuning detection rules.

Raw Evidence

```
Return-Path: <it-security-noreply@acm3-corp.com> Delivered-To: mthompson@acme-corp.com
Received: from mx01.acme-corp.com (mx01.acme-corp.com [10.0.0.25]) by mail.acme-corp.com
(Postfix) with ESMTPS id 4T2BxR6QKMz9vGH for <mthompson@acme-corp.com>; Mon, 15 Jan 2024
08:45:12 -0500 (EST) Received: from mail-out.suspicious-relay.net
(mail-out.suspicious-relay.net [91.195.240.12]) by mx01.acme-corp.com (Postfix) with ESMTP id
4T2BxQ3FfKz3kLN for <mthompson@acme-corp.com>; Mon, 15 Jan 2024 08:45:11 -0500 (EST) Received:
from localhost (unknown [185.234.72.19]) by mail-out.suspicious-relay.net (Postfix) with ESMTPA
id 8B34A2E019F for <mthompson@acme-corp.com>; Mon, 15 Jan 2024 13:45:09 +0000 (UTC)
Authentication-Results: mx01.acme-corp.com; spf=fail (sender IP is 91.195.240.12)
smtp.mailfrom=acm3-corp.com smtp.helo=mail-out.suspicious-relay.net; dkim=none; dmarc=fail
(p=none dis=none) header.from=acm3-corp.com X-Spam-Status: Yes, score=8.7 required=5.0
tests=BAYES_99,DKIM_NONE, SPF_FAIL,SUSPICIOUS_LINK,FROM_DISPLAY_SPOOF,PHISH_AZUREBLOBSTORAGE
autolearn=spam autolearn_force=no version=3.4.6 X-Spam-Score: 8.7 Message-ID:
<5f4d3c2b1a0e9f8d7c6b5a4938271605@acm3-corp.com> Date: Mon, 15 Jan 2024 13:45:08 +0000 From:
"ACME Corp IT Security Team" <it-security-noreply@acm3-corp.com> Reply-To:
it-helpdesk-verify@proton-secure-mail.ru To: mthompson@acme-corp.com Subject: [URGENT]
Mandatory Password Reset Required - Account Compromise Detected X-Mailer: Microsoft Outlook
16.0 X-Priority: 1 (Highest) MIME-Version: 1.0 Content-Type: multipart/alternative;
boundary="----=_Part_8847_1052394812.1705322708" ------=_Part_8847_1052394812.1705322708
Content-Type: text/plain; charset="UTF-8" Content-Transfer-Encoding: 7bit ACME Corp IT Security
Alert Dear Employee, Our security monitoring systems have detected suspicious activity on your
corporate account. As a precautionary measure, you are required to verify your identity and
reset your password within the next 24 hours. Failure to complete this verification will result
in your account being temporarily suspended per our IT Security Policy (Section 4.2.1). Please
verify your account immediately: https://company-portal.com/verify This is an automated message
from the ACME Corp IT Security Team. Do not reply to this email. Regards, IT Security
Operations Center ACME Corporation Phone: +1 (555) 012-3456
------=_Part_8847_1052394812.1705322708 Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable <!DOCTYPE html> <html> <head> <meta
http-equiv=3D"Content-Type" content=3D"text/html; charset=3DUTF-8"> </head> <body
style=3D"font-family: Calibri, Arial, sans-serif; color: #333333; ba= ckground-color: #f5f5f5;
margin: 0; padding: 0;"> <table width=3D"100%" cellpadding=3D"0" cellspacing=3D"0"
style=3D"max-wid= th: 600px; margin: 20px auto; background-color: #ffffff; border: 1px solid=
#dddddd;"> <tr> <td style=3D"background-color: #003366; padding: 20px; text-align: center;= ">
<img src=3D"cid:logo_placeholder" alt=3D"ACME Corp" style=3D"height: 40px;= "
onerror=3D"this.style.display=3D'none'"> <h2 style=3D"color: #ffffff; margin: 10px 0 0 0;">IT
Security Alert</h2> </td> </tr> <tr> <td style=3D"padding: 30px;"> <p style=3D"font-size:
14px;">Dear Employee,</p> <p style=3D"font-size: 14px;">Our security monitoring systems have
detected= <strong style=3D"color: #cc0000;">suspicious activity</strong> on your cor= porate
account. As a precautionary measure, you are required to verify your= identity and reset your
password within the next <strong>24 hours</strong>= .</p> <p style=3D"font-size: 14px;
background-color: #fff3cd; border: 1px solid = #ffc107; padding: 10px; border-radius:
```

```
4px;"><strong>=E2=9A=A0 Warning:</s= trong> Failure to complete this verification will result
in your account be= ing temporarily suspended per our IT Security Policy (Section 4.2.1).</p>
<table cellpadding=3D"0" cellspacing=3D"0" style=3D"margin: 25px auto;"> <tr> <td
style=3D"background-color: #003366; border-radius: 4px; padding: 12px = 30px; text-align:
center;"> <a href=3D"http://evil-phish.ru/steal?id=3D12345&amp;user=3Dmthompson&amp;=
ts=3D1705322708" style=3D"color: #ffffff; text-decoration: none; font-size:= 16px; font-weight:
bold; display: block;">https://company-portal.com/verif= y</a> </td> </tr> </table> <p
style=3D"font-size: 12px; color: #666666;">This is an automated message= from the ACME Corp IT
Security Team.<br>Do not reply to this email. If you= believe this is an error, contact the
helpdesk at ext. 4357.</p> <hr style=3D"border: none; border-top: 1px solid #dddddd; margin:
20px 0;"= > <p style=3D"font-size: 11px; color: #999999;"> ACME Corporation | 1234 Corporate
Blvd, Suite 500 | New York, NY 10001<br> This email and any attachments are confidential. If
you are not the intende= d recipient, please notify the sender and delete this message. </p>
</td> </tr> </table> <!-- Tracking pixel --> <img src=3D"http://evil-phish.ru/track?id
```

Generated by SOC-AI-Agent | Automated Security Investigation Platform
Report generated at 2026-02-13 04:28:23 UTC