

Post-Incident Analysis Report

Prepared by: Mr. Chandan Prasad

Position: SOC Analyst Intern

Company: CYART Tech

Incident Type: Phishing Attack

Executive Summary

A phishing email was sent to multiple employees. One user opened the email and clicked a malicious link. The attack was detected after 2 hours and contained within 4 hours. This report documents what happened, why it happened, and what we can do to prevent it in the future.

Incident Timeline

14:00 - Phishing email sent to company

14:30 - User receives email in inbox

14:45 - User opens email and clicks link

16:00 - Security alert triggered (MTTD: 2 hours)

16:15 - SOC team begins investigation

16:45 - Email marked as phishing and blocked

18:00 - Incident contained (MTTR: 4 hours from detection)

Root Cause Summary

The primary cause is insufficient security awareness training. Users don't know how to identify phishing emails, so they click malicious links. Secondary causes include weak email filtering and lack of immediate onboarding training for new employees.

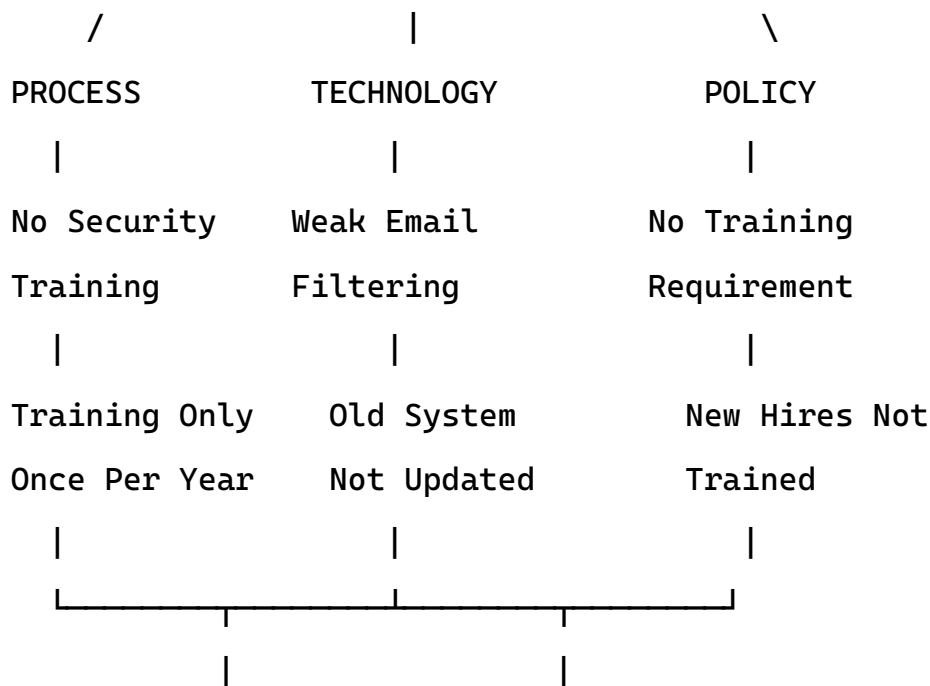
What Went Wrong – Fishbone Diagram

PEOPLE

1

Lack of Training

1



ROOT CAUSE IDENTIFIED

- User clicked phishing link
- No training provided
- Email filtering failed

Contributing Factors

- People: Users not trained on phishing indicators
- Process: No immediate security training for new hires. Annual training is insufficient.
- Technology: Email filtering system doesn't catch sophisticated phishing. No multi-factor authentication for email access.
- Policy: No requirement for security training. No policy on email authentication (SPF, DKIM, DMARC).

Metrics Calculation

Detection Time (MTTD): 2 hours

- Email sent: 14:00
- Alert triggered: 16:00
- Time to detect: 2 hours

Response Time (MTTR): 4 hours

- Detection: 16:00
- Containment: 20:00

- Time to respond: 4 hours

Dwell Time: 4 hours 15 minutes

- User clicked link: 14:45
- Incident fully contained: 19:00
- Total time attacker could have accessed: 4 hours 15 minutes

False Positive Rate: 0%

- This alert was genuine phishing
- No false positives in this incident

Lessons Learned

What worked well:

- Alert system detected the phishing email within 2 hours
- SOC team responded quickly once alert was triggered
- Incident was contained before major damage

What didn't work well:

- User didn't recognize phishing email
- Email filtering didn't block it automatically
- Detection took too long (2 hours is slow for phishing)
- No immediate response when user clicked link

What we need to improve:

- Better email security training for all employees
- Improve email filtering rules
- Implement multi-factor authentication
- Create quick phishing reporting button
- Monthly security awareness training instead of annual

Recommendations

Immediate (This week):

- Reset password for affected user
- Check what the malicious link accessed
- Remove any malware if installed
- Block the malicious email sender

Short-term (Next 2 weeks):

- Add email authentication (SPF, DKIM, DMARC)
- Implement multi-factor authentication for all users
- Create phishing reporting system
- Start monthly security training

Long-term (Next month):

- Deploy advanced email filtering with AI
- Create security awareness program with monthly updates
- Conduct phishing simulations quarterly
- Track and measure phishing click rates
- Update security policies

Metrics Summary

Detection Time (MTTD): 2 hours – acceptable but can be better

Response Time (MTTR): 4 hours – good response time

Total Dwell Time: 4 hours 15 minutes – should be under 1 hour

User Impact: 1 user compromised – limited impact

Incident Severity: Medium – email phishing, not critical system

Overall Effectiveness: 60% – detected and contained but slower than desired

Action Items

Action	Owner	Due Date	Priority
Reset user password	IT Team	Today	High
Review email logs	SOC Analyst	Tomorrow	High
Implement MFA	IT Security	Next week	High
Start monthly training	HR/Security	Next week	Medium
Deploy email filters	IT	Next 2 weeks	Medium
Quarterly phishing sim	SOC	Next month	Medium

Conclusion

This phishing incident revealed gaps in our security awareness and email filtering. The good news is the SOC team detected and contained it within 4 hours. The key to preventing future incidents is employee training and better email security. With the recommended improvements, we can reduce detection time from 2 hours to 30 minutes and response time from 4 hours to 1 hour.

Incident Closed

Status: Contained and analyzed

Recommendation: Approved for implementation of all short-term recommendations

Follow-up: Review effectiveness in 30 days

Report prepared by: Mr. Chandan Prasad, SOC Analyst Intern, CYART Tech