Incident Report: Phishing Email Indicators

Incident ID: INC-PHISH-001
Date / Time: 2025-10-05 (UTC)
Prepared by: Hardeep Singh — SOC Lab Project
Contact: hardeep.paul16@gmail.com

Executive Summary

On the lab environment, multiple mock phishing email indicators were detected and indexed into the local SIEM (Elasticsearch index mac-security-events). The events were flagged for header anomalies such as lookalike sender domains, sender/reply-to mismatch, and received hops from unknown hosts. No credential compromise was observed (controlled lab simulation).

Incident Details

- **Type:** Phishing (email header anomalies)
- **Date/Time Detected:** See timestamps in attached logs and screenshots
- **Index:** mac-security-events
- **Notable source domains observed:** micr0s0ft-secure.com, amaz0n-payments.top, yourbank.cn
- **Indicators observed:** lookalike domains, sender/reply-to mismatch, received from unknown hosts

Evidence & Indicators

- email.from: IT Support <it-support@micr0s0ft-secure.com> → flagged as lookalike domain
- email.from: Billing <billing@amaz0n-payments.top> → flagged for suspicious TLD (.top) and suspicious domain
- email.from: Support <support@yourbank.cn> → flagged for unknown received hop and suspicious TLD (.cn)
- threat.indicators: from_reply_mismatch, lookalike_domain_or_suspicious_tld, received_unknown_hosts

Timeline (simplified)

1. Phishing events indexed into mac-security-events via simulated injector script (phishing_parser.py).
2. Events observed in Kibana Discover and added to the SOC dashboard under **Phishing Indicators Table**.
3. Analyst reviewed headers and flagged lookalike domains and unknown hops. No follow-up lateral movement observed (lab environment).

Actions Taken

- Indexed mock phishing events into Elasticsearch for analysis and evidence capture.
- Built a Kibana table visualization showing email.from, email.subject, source.domain, threat.indicators, and message.
- Saved the visualization to the SOC dashboard for monitoring and reporting.

Impact & Assessment

Assessment: Low impact — controlled lab simulation. No user credentials were captured and no production systems were affected. The indicators mirror real-world phishing techniques and demonstrate detection capability.

Recommendations

1. Implement email gateway filtering and sender verification (SPF / DKIM / DMARC).
2. Create an alert rule in Kibana to trigger when threat.indicators contains phishing flags.
3. Enforce MFA for privileged accounts and conduct phishing awareness training.
4. Keep attack/simulation scripts separated from the deployment and run only in isolated test environments.

Attachments / Evidence References

- Kibana screenshots: docs/screenshots/bar_chart.png, docs/screenshots/table_feed.png (phishing events visible in the table)
- Raw event log (spreadsheet): docs/Authentication Event Log - Recent.xlsx
- Exported dashboard: kibana_exports/dashboard-mac-security-events.ndjson