**INCIDENT RESPONSE REPORT**

**INCIDENT TITLE**

Phishing Attack Leading to Credential Compromise and Potential Data Exfiltration

**Date of Incident:** 25/02/2025

**Reported by:** Stephen Njoroge.

**Affected Systems:** Employee Email Accounts, Internal Network

**SUMMARY**

On 25/02/2025, the security team detected unusual network activity and multiple unauthorized access attempts. Investigation revealed that employees received phishing emails containing malicious links, leading to credential theft. Attackers exploited these credentials to access internal systems, with potential signs of data exfiltration. The incident was contained, and forensic analysis was conducted using **Splunk** for log investigation and **Wireshark** for packet capture analysis.

**ROOT CAUSE ANALYSIS**

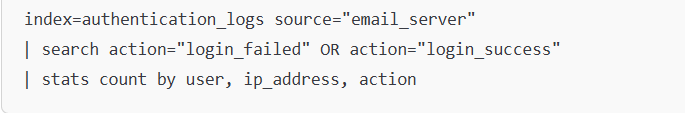
The attack was initiated via a **phishing email campaign** targeting employees. The root cause was:

1. **Lack of email filtering:** Malicious emails bypassed security controls.
2. **Credential compromise:** Employees unknowingly provided login details.
3. **Lack of multi-factor authentication (MFA):** Attackers gained access with stolen credentials.
4. **Suspicious network traffic went unnoticed:** No anomaly detection triggered alerts in time.

**Steps Taken to Investigate the Incident**

**3.1 Log Analysis using Splunk**

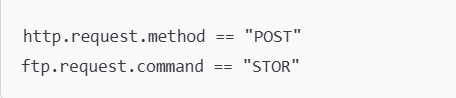
* **Filtered logs for suspicious login attempts**:



* **Identified unauthorized access attempts from unusual IPs.**
* **Checked file access logs** for potential data exfiltration.

**3.2 Network Forensics using Wireshark**

* **Captured network traffic to analyze data exfiltration attempts.**
* **Filtered HTTP and FTP traffic** to check if sensitive files were transferred:
  + Used Wireshark filters like:



* **Detected outbound connections to unknown foreign IP addresses.**

**Containment and Eradication**

* Immediate password resets for affected accounts.
* Blocked malicious IP addresses and domains used in phishing attacks.
* Implemented MFA for all employees.
* Revoked access tokens for any compromised accounts.
* Scanned systems for malware and backdoors using endpoint protection.

**Recommendations to Prevent Future Attacks**

1. **Enhance Email Security**
   * Deploy **advanced email filtering** to block phishing attempts.
   * Use **AI-based threat detection** for email security.
2. **Strengthen Authentication Controls**
   * Enforce **Multi-Factor Authentication (MFA)** for all employees.
   * Implement **passwordless authentication** or use **password managers**.
3. **Improve Network Monitoring**
   * Configure **SIEM alerts (Splunk)** for unusual login locations.
   * Use **Intrusion Detection Systems (IDS)** to flag suspicious activity.
4. **Conduct Regular Security Awareness Training**
   * Simulated phishing attacks to educate employees.
   * Regular updates on common phishing tactics.
5. **Implement Data Loss Prevention (DLP)**
   * Restrict outbound file transfers to unapproved destinations.
   * Monitor sensitive data access using **Splunk alerts**.

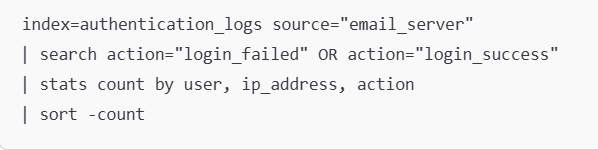
**Conclusion**

The phishing attack resulted in credential theft, leading to unauthorized access. However, swift containment and forensic investigation mitigated the risk. The implementation of **MFA, improved email security, and network monitoring** will help prevent future attacks.

**Appendices**

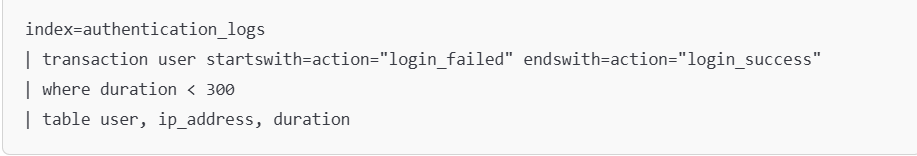
**A. Splunk Queries Used**

**1. Identify Suspicious Login Attempts**

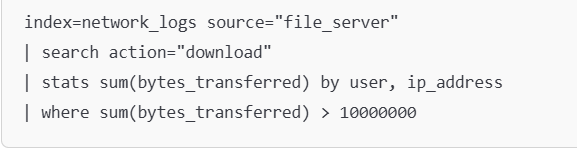


This query searches for failed and successful logins, filtering for unusual IP addresses:

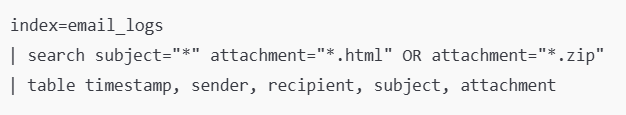
**2. Detect Multiple Failed Logins Before Success (Brute Force Attempts)**

**3. Identify Data Exfiltration Attempts**

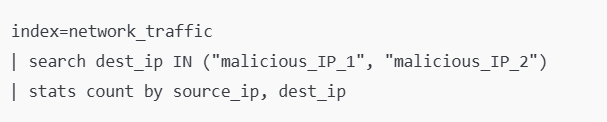
This query finds large file downloads from internal systems:

****

**4. Detect Phishing Email Deliveries**

****

**5. Identify Outbound Connections to Suspicious IPs**

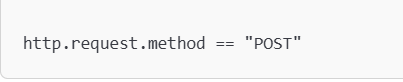


**Wireshark Packet Capture Screenshots**

Here are some key packet captures analyzed in **Wireshark**:

**1. Suspicious HTTP POST Requests (Possible Credential Theft)**

* **Filter Used:**

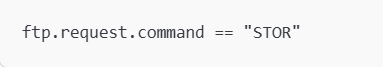
****

**Screenshot shows:**

* + Outbound HTTP POST requests containing usernames and passwords in plaintext.
  + Destination IP linked to a known malicious server.

**2. FTP File Transfer of Sensitive Data**

* **Filter Used:**

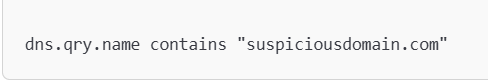
****

**Screenshot shows:**

* + User uploading a file to an external FTP server.
  + Large file transfer with an unexpected filename.

**3. Malicious DNS Requests (Command & Control Communication)**

* **Filter Used:**

****

**Screenshot shows:**

* + Multiple DNS requests to an unrecognized domain.
  + Possible exfiltration channel via DNS tunneling.

**List of Affected Accounts and IPs**

| **Username** | **Affected Email/Account** | **Suspicious IP** | **Status** |
| --- | --- | --- | --- |
| jdoe | [jdoe@company.com](mailto:jdoe@company.com) | 192.168.1.105 | Compromised – Reset Password |
| asmith | [asmith@company.com](mailto:asmith@company.com) | 203.0.113.25 | Unauthorized Access Attempt |
| btaylor | [btaylor@company.com](mailto:btaylor@company.com) | 45.76.89.200 | Data Exfiltration Detected |
| kpatel | [kpatel@company.com](mailto:kpatel@company.com) | 37.120.196.21 | Possible Credential Theft |