The attack appears to be a phishing attack with elements of malware. The initial email campaign, which mimicked an HR communication, tricked employees into providing their credentials on a fake website, indicating a phishing attempt designed to steal login information. The malware component is suggested by the reports of file-share access issues and errors with Word documents, indicating that a malicious program was likely downloaded and executed after credentials were compromised.

The attack is a **phishing attack** combined with **malware**. The phishing aspect is evident from the email campaign that tricked employees into providing their credentials on a fake website.

Isolate Affected Systems: Immediately disconnect affected systems from the network to prevent the spread of malware and contain the attack.

Notify Key Stakeholders: Inform management, the incident response team, and relevant departments about the ongoing attack.

Identify the Scope: Determine how many systems and users are affected by the phishing email and potential ransomware infection.

Preserve Evidence: Ensure logs, emails, and other relevant data are preserved for further investigation and forensic analysis.

Reset Credentials: Promptly reset passwords for affected accounts and potentially all accounts in the organization if the breach is widespread.

Update Security Measures: Review and update firewall rules, intrusion detection systems (IDS), and email filters to block similar threats.

Engage External Experts: If necessary, bring in external cybersecurity experts or the organization's incident response partner to assist with containment and remediation.

Containment:

Quarantine Infected Machines: Disconnect compromised systems to prevent further spread of malware.

Disable Compromised Accounts: Temporarily disable accounts that were compromised to prevent unauthorized access.

Block Malicious IPs and URLs: Update firewalls and web filters to block known malicious IP addresses and the phishing website.

Resolution:

Remove Malware: Use anti-malware tools to scan and remove the ransomware or any other malware from infected systems.

Restore Systems: If ransomware is confirmed, restore affected systems from known clean backups. Ensure that backups are from a date prior to the infection.

Patch Vulnerabilities: Apply security patches and updates to all systems to close any vulnerabilities that may have been exploited.

Recovery:

Monitor Systems: Implement enhanced monitoring to detect any further suspicious activity or potential reinfection.

Reinstate Systems Gradually: Reconnect cleaned systems to the network one by one to ensure the infection is fully eradicated.

Test Restored Systems: Verify that restored systems and data are functioning correctly and that no remnants of the attack remain.

Conduct a Post-Incident Review: Analyze the incident to understand how the attack occurred, what was done well in the response, and where improvements can be made.

Update Incident Response Plan: Revise the incident response plan based on lessons learned to better prepare for future incidents.

Strengthen Employee Training: Reinforce phishing awareness and cybersecurity training for all employees to reduce the risk of future attacks.

Audit and Improve Security Measures: Perform a security audit to identify gaps and improve defenses, such as enhancing email security, implementing multi-factor authentication, and improving endpoint protection.

Report the Incident: If required, report the incident to relevant regulatory bodies or industry groups, following legal and compliance guidelines.

Communicate with Stakeholders: Provide a summary of the incident, response actions taken, and future preventive measures to stakeholders, including employees, customers, and partners.