Identifying the Attack

The incident described and the error page provided suggest a **phishing attack** combined with a **malware infection**. Here's why:

1. **Phishing Emails**: Employees received emails prompting them to click on a link and enter their credentials on a fake website, indicating a phishing attempt to steal login information.
2. **Fake Website**: The fake website likely captured user credentials and could have initiated a download of malicious software.
3. **Malware Symptoms**: Reports of inaccessible file-shares and Word documents suggest that the malware may have encrypted files or corrupted them, indicating a potential ransomware attack.

Next Steps for a Cyber Security Analyst

Immediate Actions

1. **Isolate Affected Systems**
   - Disconnect infected systems from the network to prevent the spread of malware.
   - Advise employees not to use their computers until further notice.
2. **Identify and Contain the Phishing Attack**
   - Block the phishing email at the email gateway to prevent further delivery.
   - Identify the fake website and work with the hosting provider to take it down.
   - Notify all employees about the phishing email and instruct them not to click on any links.
3. **Investigate and Analyze Malware**
   - Retrieve samples of the malware from infected systems.
   - Use sandboxing and other analysis tools to understand the malware's behavior and payload.
   - Update antivirus and anti-malware definitions to detect and remove the specific malware.

Containment, Resolution, and Recovery

1. **Reset Compromised Credentials**
   - Force a password reset for all employees who clicked on the phishing link.
   - Enable multi-factor authentication (MFA) for additional security.
2. **Remove Malware**
   - Run full antivirus and anti-malware scans on all systems to identify and remove infections.
   - Use specialized tools to decrypt files if ransomware is involved, or restore from backups.
3. **Restore Data and Services**
   - Restore file-shares and documents from clean backups.
   - Ensure that all systems are fully cleaned before reconnecting to the network.
4. **Strengthen Security Measures**
   - Implement stricter email filtering and spam detection.
   - Enhance network segmentation to limit the spread of malware in the future.

- Deploy intrusion detection and prevention systems (IDPS) to monitor and block suspicious activity.

Post-Incident Activities

1. **Post-Mortem Analysis**
   - Conduct a thorough review of the incident to understand how the attack occurred and what could have been done to prevent it.
   - Document the timeline of events, actions taken, and lessons learned.
2. **Update Incident Response Plan**
   - Revise the incident response plan based on insights gained from the incident.
   - Ensure the plan includes clear procedures for phishing and malware attacks.
3. **Employee Training and Awareness**
   - Conduct regular security awareness training sessions for employees.
   - Provide guidance on recognizing phishing emails and reporting suspicious activities.
4. **Security Enhancements**
   - Regularly update and patch all systems and software to protect against vulnerabilities.
   - Perform routine security assessments and penetration testing to identify and mitigate potential weaknesses.
   - Implement advanced threat detection solutions and continuously monitor the network for signs of compromise.

By following these steps, you can effectively contain, resolve, and recover from the phishing and malware incident, as well as strengthen the organization's security posture to prevent future attacks.