Adversary Emulation & Detection Report

1. Executive Summary

On 26 December 2025, the SOC identified suspicious endpoint activity on a Windows workstation,identified by the hostname Windows (VBox) with IP address 10.0.2.30, following simulated spearphishing behavior. The activity involved execution of a masqueraded binary (splunkd.exe) from a user-writable directory (C:\Users\Public) and associated PowerShell activity consistent with post-phishing execution. The activity was detected by Wazuh through endpoint telemetry and behavioral analysis. The incident was contained by terminating the malicious process and removing the unauthorized executable. No lateral movement or data exfiltration was observed.

2. Incident Timeline

Timestamp	Event
2025-12-25 15:30:00	Endpoint establishes outbound HTTP connection
2025-12-25 15:30:00	PowerShell execution observed
2025-12-25 15:31:00	File created in C:\Users\Public
2025-12-25 15:31:00	splunkd.exe executed from non-standard path
2025-12-25 15:34:00	Wazuh raises behavioral alerts
2025-12-25 15:40:00	SOC triage initiated
2025-12-25 15:45:00	Malicious process terminated
2025-12-25 15:50:00	Host contained and cleaned

Table 1: Timeline

3. Threat Activity Analysis

3.1. Observed Behavior

The following behaviors were observed on the endpoint:

- Execution of PowerShell commands without user interaction prompts.
- Creation of an executable file in a publicly writable directory.
- Execution of splunkd.exe outside of the legitimate Splunk installation path.
- Masquerading of malicious payload as a trusted service binary.

- Silent execution without visible user interface.

This activity is consistent with post-delivery spearphishing execution, where a user opens a malicious attachment or payload delivered via phishing.

3.2. MITRE ATT&CK Mapping

Tactic	Technique
Initial Access	T1566 – Spearphishing
Execution	T1059 – PowerShell
Defense Evasion	T1036 – Masquerading

Table 2: MITRE

4. Detection

Wazuh detected the following indicators:

- Suspicious PowerShell execution.
- Executable creation in C:\Users\Public.
- Execution of a trusted-looking binary from an anomalous location.

During the incident window, Wazuh also reported multiple CVEs associated with installed software on the endpoint.

5. Impact Assessment

Area	Impact
Endpoint Integrity	Compromised
Data Exposure	None observed
Lateral Movement	None detected
Persistence	Not established
Business Impact	Low
Security Risk	Medium–High (contextual)

Table 3: Impact Assessment

6. Containment & Remediation

- Terminated unauthorized splunkd.exe process.
- Removed executable from C:\Users\Public.
- Verified no persistence mechanisms were created.
- Confirmed no lateral movement.
- Re-enabled endpoint protection.

7. Root Cause Analysis

User-executed content following spearphishing delivery led to execution of attacker-controlled code. Contributing Factors:

- Lack of pre-execution phishing prevention.
- User-writable directories not sufficiently monitored.
- Existing unpatched vulnerabilities increasing post-compromise risk.

8. Lessons Learned

- Endpoint detection successfully identified malicious execution.
- Masquerading remains an effective attacker technique.
- Vulnerability context is critical during incident triage.
- Detection occurred after execution, not before delivery.

9. Summary

This incident demonstrates a realistic spearphishing execution scenario and validates the SOC’s ability to detect and respond to endpoint-level threats. While containment was successful, the exercise highlighted gaps in pre-delivery phishing prevention and emphasized the importance of combining behavioral detection with vulnerability management.