**Incident Postmortem Report**

**Incident Title:** Malware Attack Mitigation

**Incident Date:** [Start Date and Time] - [End Date and Time]

**Incident Summary:** On [Start Date], our systems were targeted by a distributed malware attack exploiting the Spring4Shell vulnerability. The attack was detected and mitigated through the implementation of a firewall rule. The incident lasted approximately 2 hours before full mitigation was achieved.

**Timeline of Events:**

1. **[Start Date and Time]:** Initial detection of unusual network activity and malware attack. Firewall logs indicated a potential breach.
2. **[Date and Time]:** Notification sent to the relevant infrastructure team regarding the attack.
3. **[Date and Time]:** Analysis of firewall logs and identification of the Spring4Shell vulnerability exploitation.
4. **[Date and Time]:** Implementation of a custom firewall rule to block malicious requests.
5. **[Date and Time]:** Verification of the firewall rule effectiveness using test\_requests.py.
6. **[Date and Time]:** Confirmation that the firewall rule successfully mitigated the attack.

**Incident Details:**

* **Affected Infrastructure:** [Specify affected systems or components]
* **Vulnerability Exploited:** Spring4Shell
* **Pattern Used by Attackers:** [Describe specific characteristics of the malicious requests, e.g., specific headers, payloads]
* **Firewall Rule Implemented:** [Summarize the rule added to the firewall]

**Root Cause Analysis:** The malware attack exploited the Spring4Shell vulnerability. The attackers utilized specific patterns in their requests to bypass standard security measures. The vulnerability allowed unauthorized access and execution of malicious payloads.

**Actions Taken:**

1. **Immediate Response:**
   * Alerted the infrastructure team of the attack.
   * Analyzed firewall logs to identify the malicious patterns.
   * Implemented a custom firewall rule to block malicious traffic.
2. **Post-Incident Actions:**
   * Tested the firewall rule to ensure it effectively blocked malicious requests.
   * Monitored the system to ensure no further malicious activity was detected.

**Lessons Learned:**

* **Detection Improvement:** Enhance monitoring to quickly identify and respond to similar attacks in the future.
* **Pattern Identification:** Regularly update firewall rules to recognize and block new attack patterns.
* **Communication Protocol:** Ensure timely and clear communication among teams during an incident to facilitate a swift response.

**Recommendations:**

1. **Review and Update Security Measures:** Regularly review and update security measures to address emerging threats.
2. **Training and Awareness:** Conduct training sessions to familiarize the team with incident response procedures and common attack patterns.
3. **Documentation:** Maintain detailed documentation of incidents and responses to improve future incident handling and compliance audits.

**Involved Teams:**

* **Infrastructure Team:** Notified and assisted in identifying affected systems.
* **Networks Team:** Developed and implemented the firewall rule.

**Attachments:**

* Proof of Concept Payload
* Firewall Server Code
* Firewall Logs Analysis

**Prepared by:** Yengkong Sayaovong

**Position:** Information Security Analyst

**Date:** 08.15.2024