### **Post-Mortem Report: Malware Attack on Spring Framework Infrastructure**

**Date of Incident:** March 20, 2022  
**Report Date:** September 05, 2024  
**Incident Lead:** Junaid Arshad Malik

#### **1. Summary of Incident**

On March 20, 2022, a malware attack targeted multiple critical services running the Spring Framework within the organization’s infrastructure. The attack was identified as an exploitation of the **Spring4Shell (CVE-2022-22965)** vulnerability, which allowed the attackers to attempt remote code execution on vulnerable systems.

The attack impacted critical services such as NBN Connection, Mobile Tower Connection, and Home & Business Lines, posing a significant risk to business continuity.

#### **2. Impact Analysis**

The following critical infrastructure was affected:

* **NBN Connection (P1 - Critical):** The malware targeted the high-speed NBN service, which is vital for customer connectivity.
* **Mobile Tower Connection (P2 - High):** The service that provides cellular connectivity between towers was affected.
* **Home & Business Lines (P2 - High):** VoIP products and business lines were at risk of compromise.

Despite the attempts, no sensitive data was confirmed to be compromised, and services were restored after remediation.

#### **3. Timeline of Events**

* **03:21 UTC, March 20, 2022:** Attack detected by firewall logs on nbn.external.network.
* **03:25 UTC:** SOC initiated incident response and began analysis of attack vectors.
* **03:40 UTC:** Identified malicious requests targeting Spring Framework vulnerabilities.
* **03:55 UTC:** Blocked suspicious traffic by creating firewall rules.
* **04:15 UTC:** Relevant teams were notified and remediation actions began.
* **05:00 UTC:** Mitigation completed and normal service restored.

#### **4. Root Cause Analysis**

The root cause of the incident was the exploitation of the **Spring4Shell (CVE-2022-22965)** vulnerability in services running outdated versions of the Spring Framework. Attackers leveraged vulnerabilities in request headers and POST data to attempt command execution via malicious payloads.

#### **5. Resolution and Remediation Steps**

* **Firewall Rule Implementation:** Immediate blocking of malicious requests with patterns matching the attack:
  + Headers: suffix, c1, c2, Content-Type: application/x-www-form-urlencoded
  + POST data containing class.module.classLoader.resources.context.parent.pipeline.first.pattern
* **Patch Deployment:** Upgraded affected services to patched versions of the Spring Framework.
* **Service Monitoring:** Enhanced monitoring for any suspicious traffic or new exploits.
* **Team Collaboration:** Engaged with the NBN, Mobile, and Networks teams to ensure proper incident response and future prevention strategies.

#### **6. Lessons Learned**

* **Regular Patching:** Critical services must be patched promptly when vulnerabilities such as Spring4Shell are disclosed.
* **Proactive Monitoring:** Early detection through firewall logs helped contain the attack before damage could occur.
* **Clear Communication Channels:** Timely notification and collaboration between SOC and service teams enabled quick mitigation.

#### **7. Recommendations**

* **Regular Security Audits:** Perform regular vulnerability assessments and patch management for all critical infrastructure.
* **Enhanced Firewall Rules:** Implement advanced firewall rules to monitor for emerging threats related to new vulnerabilities.
* **Employee Awareness:** Conduct training and simulations to ensure readiness for similar incidents in the future.

**Prepared By:**  
Junaid Arshad Malik  
Information Security Analyst, Telstra Security Operations