Incident Postmortem

Malware Attack on NBN Network

Summary:

- **Incident Start Time:** March 20, 2022, 2:16:34 PM AEDT
- **Incident End Time:** March 20, 2022, 4:31 PM AEDT
- **Participants:** Telstra Security Operations, NBN Team, Networks Team
- **Status:** Resolved
- **Impact Level:** Critical
- **Detection Time:** Immediate (via firewall alerts and customer complaints)
- **Root Cause Fixed Time:** Approximately 2 hours and 15 minutes after detection

Impact:

The malware attack led to impaired functionality and downtime of critical NBN services. The exploitation of a remote code execution (RCE) vulnerability resulted in service disruptions across the "nbn.external.network." Affected systems experienced degraded performance, leading to an increase in customer complaints.

Detection:

- Firewall logs detected suspicious HTTP POST requests with malicious query data targeting the **/tomcatwar.jsp** path.
- Service degradation and outages were reported by customers, further confirming the impact of the attack.

Root Cause:

The attack exploited a recently disclosed zero-day vulnerability, **Spring4Shell** (**CVE-2022-22965**), which targeted the widely used Spring Framework. The NBN Team hosted this framework, making it an attractive target.

At **2:16:34 PM AEDT on March 20, 2022**, an attacker began sending specially crafted HTTP POST requests to the Telstra NBN network's public-facing address (**nbn.external.network**). The payload leveraged **Spring4Shell** to achieve remote code execution (RCE) on vulnerable servers.

Firewall alerts were triggered due to abnormal request patterns, and customer complaints about degraded performance further confirmed the attack's impact. Forensic analysis later confirmed that the attacker had successfully executed remote code on the affected systems.

Resolution:

- **Within 30 minutes of detection**, Telstra Security Operations identified the attack and alerted the NBN Team.
- **Over the next 45 minutes**, security analysts conducted forensic analysis of firewall logs and identified the attack pattern. The findings were shared with the Networks Team for mitigation.
- **In the following 60 minutes**, the Networks Team developed a **Python-based firewall rule** to block any requests containing the malicious **Spring4Shell payload**, following the proof-of-concept (**PoC**) attack patterns.
- Once the firewall rule was deployed, the attack was effectively mitigated, and NBN service functionality was restored.
- A full forensic investigation was launched post-mitigation to assess potential lingering threats and reinforce security measures.

Action Items:

1. **Deploy and maintain firewall rules** to block future attacks leveraging the Spring4Shell exploit or similar techniques.
2. **Enhance threat intelligence monitoring** to proactively detect and analyze similar attack patterns for improved firewall detection.
3. **Conduct security awareness training** for development and operations teams to ensure timely patching of critical vulnerabilities.
4. **Update the incident response playbook** to include specific mitigation steps for Spring4Shell and other emerging zero-day threats.

Conclusion:

This incident highlights the importance of proactive security monitoring and rapid response in mitigating zero-day exploits. Strengthening firewall rules, enhancing threat intelligence, and ensuring timely patch management are crucial steps in preventing similar attacks in the future. Continuous learning and improvement in incident response processes will further reinforce the security posture of NBN services.