Incident Postmortem: Malware Attack on Telstra’s NBN Network

## **Summary**

On March 20, 2022, at 03:16:34 UTC, our network experienced a confirmed malware attack that compromised Telstra's nbn services. The incident was detected through meticulous analysis of firewall logs, unveiling an exploitation of the Spring Framework utilizing the zero-day vulnerability known as Spring4Shell.

## **Impact**

The compromise of Telstra's nbn network posed a severe threat to data security and network integrity. The attacker gained unauthorized access, potentially compromising sensitive information and disrupting essential services.

## **Detection**

The detection of the NBN malware attack was a pivotal aspect of our incident response. The breach came to our attention through meticulous scrutiny of firewall logs, revealing abnormal patterns and suspicious activities within the network. Our enhanced monitoring systems, designed to detect anomalous behavior, played a crucial role in identifying the intrusion.

The specific indicators that triggered our investigation included unusual traffic patterns directed towards the Spring Framework, particularly requests targeting the "/tomcatwar.jsp" path. These requests were inconsistent with regular network traffic and raised immediate red flags during the log analysis.

Additionally, the detection mechanism focused on HTTP headers, specifically looking for patterns indicative of attempts to exploit the Spring4Shell vulnerability. The presence of certain headers, such as "suffix=%>//" and "c1=Runtime c2=", in incoming traffic triggered the alarm for a potential exploit.

The in-depth analysis allowed our security team to swiftly pinpoint the compromise, recognize the exploitation of the zero-day vulnerability.

## **Root Cause**

The root cause analysis reveals that the attacker successfully exploited a zero-day vulnerability, specifically a remote code execution (RCE) vulnerability known as Spring4Shell. This RCE vulnerability allowed the attacker to execute arbitrary code within the compromised Spring Framework supporting our nbn services. The compromise transpired as a result of the attacker's adept manipulation of the framework, providing them unauthorized access to the network.

This incident's severity was heightened due to the potential for malicious actions, data theft, and further network compromise associated with the RCE nature of the vulnerability. Firewall rule parameters were swiftly identified and implemented as part of the incident response to prevent future exploitation. These parameters included blocking incoming traffic on the client request path "/tomcatwar.jsp" and specific HTTP headers.

## **Resolution**

## In response to the incident, a dedicated Firewall server handler was promptly developed and deployed. This solution effectively blocked the malicious traffic associated with the RCE attack, restoring the integrity of the compromised Spring Framework and preventing further unauthorized access.

## **Action Items**

**Comprehensive Network Review**

Conduct a thorough assessment of the entire network infrastructure to identify and patch potential vulnerabilities similar to the exploited zero-day vulnerability, with a specific focus on RCE vectors.

**Enhanced Monitoring Systems**

Implement improvements to monitoring systems to enhance the early detection of suspicious activities, particularly those indicative of RCE attempts.

**Regular Security Audits and Penetration Testing**

Establish a proactive system of regular security audits and penetration testing with a targeted approach to identifying and mitigating RCE vulnerabilities.

**Collaboration with Security Experts**

Work closely with security experts and vendors to stay updated on emerging threats and vulnerabilities, with a particular emphasis on RCE-related advisories.

**Security Awareness Training**

Conduct security awareness training for all NBN team members, emphasizing the significance of RCE vulnerabilities and the associated security best practices.

Incident Response Procedures

Develop and document incident response procedures with specific protocols for addressing RCE incidents, ensuring a swift and coordinated response.