Incident Postmortem: Malware Attack on the NBN Connection Infrastructure

Summary

On 2022-03-20 at 03:16:34 UTC, Telestra Security Operations has detected a malware attack on the NBN Connection infrastructure using a zero-day vulnerability affecting the Spring Framework. Users across the NBN network are experiencing downtime and impaired service functionality. The severity of this breach is high considering it allowed threat actors to utilize remote code execution (RCE).

Impact

Users across the NBN network are experiencing downtime and impaired service functionality.

Detection

The incident was discovered by routine firewall alerts showing there were over 1.5k connection request attempts which bypasses current firewall filters.

Root Cause

Threat actors caused the incident by utilizing a zero-day vulnerability affecting the Spring Framework via data binding on JDK 9+. The exploit requires the application to run on Tomcat as a WAR deployment, which was this case in this incident.

Resolution

A new firewall rule to block all incoming traffic that uses /tomcatwar.jsp as a clientRequestPath was implemented.

Action Items

A firewall rule to block all incoming traffic that uses /tomcatwar.jsp as a clientRequestPath was implemented via python onto the firewall server. The new rule was tested before being deployed onto the server to ensure it would operate correctly. Remediation efforts include upgrading the Spring Framework to a specific version to prevent this vulnerability from affecting systems further.