Incident Postmortem: Malware Attack leading to nbn outtage

Summary

Incident Start Time: 2022-03-20T03:16:34Z
Incident End Time: 2022-03-20T05:16:34Z
Participants: Telstra Security Operations, nbn team, Networks team
Status: Resolved
Impact: Severity 1 - Critical
Detection Time: 2022-03-20T03:16:34Z
Root Cause Fixed Time: 2022-03-20T02:16:34Z

Impact

Impaired functionality and downtime on nbn services. Critical service impact. Remote code execution on nbn service infrastructure.

Detection

Firewall logs notified abnormal activity. Impaired functionality and downtime on nbn services through customer complaints.

Root Cause

An attacker exploited the recently released zero-day vulnerability, Spring4Shell, attacking the externally exposed Spring Framework hosted by the nbn services team.

At 2022-03-20T03:16:34Z, an attacker began using a Spring4Shell payload to perform remote code execution on the Telstra nbn network address "nbn.external.network" using HTTP POST requests with malicious query data on the path "/tomcatwar.jsp".

Firewall alerts triggered on this event, as well as an increase in customer complaints about degraded performance. Forensics revealed that remote code execution was successfully performed by the attacker.

Resolution

In the 30 minutes following 2022-03-20T03:16:34Z, Telstra Security Operations triaged the alert and notified the nbn team about the incident.

After, in the following 30 minutes, Telstra Security Operations performed data analysis on the firewall events and identified a pattern in the malicious requests, forwarding this information to the Networks team to create a firewall rule.

In the following 60 minutes, Telstra Networks team created the firewall rule in Python to mitigate malicious requests by blocking out any request which used the malicious Spring4Shell payload, as listed in this PoC:
https://github.com/craig/SpringCore0day/blob/main/exp.py

After the firewall rule was deployed, the malware attack was mitigated and service functionality was restored. Forensic process was then initiated.

Action Items

- Deploy firewall rule to ensure future attacks from this tool are mitigated
- Notify threat intelligence to find similar malicious payloads to improve firewall detection of future attacks