From: Telstra Security Operations
To: Networks Team (networks@email)
Subject: [URGENT] Create Firewall Rule - Mitigate Malware Attack
—
Body:
Hello Networks Team,

We would like to request the creation of a firewall rule and provide you more information about the ongoing malware attack.

Attack Type Information:
An attacker compromised the Spring Framework on our nbn services using zero-day vulnerability (Spring4Shell).

Firewall Rule Parameters:

- Block incoming traffic on client request path “/tomcatwar.jsp”
- Block incoming traffic with HTTP headers:

```
suffix =%>//
c1=Runtime
c2=<%
DNT=1
Content-Type=application/x-www-form-urlencoded
```

Additional information:

- The attacker appears to have targeted our externally facing infrastructure using Spring Framework 5.3.0 - monitor for future requests to this path.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,
Telstra Security Operations