### **Firewall Rule Request Emails**

#### **1. Mobile Team – Mobile Tower Connection Firewall Rule Request**

**From:** Telstra Security Operations  
**To:** Mobile Team (mobileteam@email)  
**Subject:** Create Firewall Rule – Block Malicious Traffic Targeting Mobile Tower Connection

**Body:**  
Hello Mobile Team,

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

We have detected a **DDoS (Distributed Denial of Service) attack** targeting the **mobiletower.internal.network** infrastructure, flooding it with malicious requests and degrading service availability.

To mitigate this, we request that **incoming traffic from suspicious IP ranges and excessive requests per second exceeding threshold limits** be blocked. Additionally, traffic originating from **known botnets and untrusted geolocations** should be restricted.

Our security analysis indicates that the attack is leveraging **reflection amplification techniques**, and we recommend implementing **rate limiting and deep packet inspection** as additional safeguards.

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

**Kind regards,**  
Telstra Security Operations

#### **2. NBN Team – NBN Connection Firewall Rule Request**

**From:** Telstra Security Operations  
**To:** NBN Team (nbn@email)  
**Subject:** Create Firewall Rule – Block Unauthorized Access to NBN Connection

**Body:**  
Hello NBN Team,

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

A **credential stuffing attack** has been detected against the **nbn.external.network**, where attackers are using compromised credentials to gain unauthorized access.

To mitigate this risk, we request the **blocking of multiple failed login attempts from the same IP within a short timeframe** and the **blacklisting of IPs exhibiting brute-force login behaviors**. Additionally, implementing **geolocation-based access restrictions and multi-factor authentication (MFA) enforcement** would enhance security.

Research suggests that these attacks originate from **compromised cloud servers** using automation to bypass login protections. We recommend further investigation and logging enhancements to track anomalous behavior.

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

**Kind regards,**  
Telstra Security Operations

### **Incident Response Plan**

**Incident Name:** **Telstra Network Infrastructure Attack Response Plan**  
**Objective:** Mitigate and neutralize cybersecurity threats targeting Telstra's infrastructure networks.

#### **1. Detection & Identification**

* Utilize **SIEM tools and IDS/IPS** to detect abnormal traffic patterns.
* Analyze **log files, firewall events, and system alerts** for indications of compromise.
* Categorize incidents based on severity (P1 - Critical, P2 - High, etc.).

#### **2. Containment Strategy**

* Isolate compromised systems and redirect legitimate traffic.
* Deploy **firewall rule updates to block malicious IPs and traffic types**.
* Notify relevant infrastructure teams via **automated alerts and email communications**.

#### **3. Eradication & Recovery**

* Conduct **malware scans, vulnerability patches, and system integrity checks**.
* Restore affected systems from secure backups if required.
* Strengthen security policies (e.g., enforcing MFA, zero-trust access).

#### **4. Post-Incident Analysis & Prevention**

* Perform **root cause analysis (RCA)** to identify attack vectors.
* Implement **security updates and permanent firewall rule changes**.
* Conduct **training sessions for IT teams on recent attack methodologies**.
* Enhance **monitoring and logging** to detect early warning signs of similar attacks.