Cybersecurity Incident Report

Incident ID: CYB-2025-03-SYNFLOOD

Date of Report: March 28, 2025

Reported by: Charles J. Wasson

Role: Security Analyst

Company: Cortex Systems Inc.

Incident Severity: Moderate

Classification: Network-Level Denial of Service (DoS)

1. Executive Summary

At approximately 2:14 PM EST on March 28, 2025, automated monitoring systems at Cortex Systems Inc. detected unusual traffic targeting the company's public web server. This anomaly triggered alerts regarding connection timeouts and unresponsive service. Manual verification confirmed that employees and external users could not access the site.

Packet analysis via Wireshark indicated a high volume of TCP SYN packets sent to the server's HTTPS port (443), consistent with a SYN flood attack. The excessive number of half-open TCP connections resulted in degraded server performance and denial of service for legitimate users.

2. Incident Timeline

Time (EST)	Event
2:14 PM	Automated monitoring triggered alert for web server unresponsiveness
2:15 PM	Security analyst attempted access – connection timeout confirmed
2:20 PM	Packet capture initiated; abnormal volume of SYN packets identified
2:25 PM	Traffic isolated and IP 203.0.113.0 blocked via perimeter firewall
2:30 PM	Server taken offline to clear connection queue
2:55 PM	Server returned to service and resumed normal operation
3:30 PM	Log data reviewed and retained for investigation

3. Technical Analysis

Attack Type: SYN Flood Denial-of-Service Attack
Protocol Affected: TCP
Target System: Public Web Server (192.0.2.1)
Target Port: 443 (HTTPS)

Indicators:
- Abnormal spike in SYN requests without corresponding ACKs
- Traffic source: 203.0.113.0
- Frequent resets (RST, ACK) and HTTP 504 Gateway Timeout errors
- No payload in SYN packets, indicating malicious intent

Impact:
- Service disruption for internal and external users
- Inability to complete TCP three-way handshakes
- Overloaded connection queue causing timeout errors

4. Containment and Mitigation

Immediate containment involved blocking the source IP address at the firewall. The server was reset to clear lingering half-open sessions. Monitoring rules were updated to flag high SYN rates in real-time. Rate limiting was considered for future prevention.

5. Root Cause

The incident was caused by an external actor intentionally sending a high volume of TCP SYN packets to the company's web server. These packets initiated the TCP handshake but did not complete it, creating a backlog of half-open connections and preventing new connections from being established.

6. Recommendations

Recommendation	Action Status
Implement SYN cookies to prevent backlog exhaustion	Pending
Enforce rate limiting for new inbound TCP connections	In Progress
Configure intrusion detection/prevention to flag SYN anomalies	In Progress
Evaluate external DDoS mitigation (e.g., Cloudflare, AWS Shield)	Under Review
Conduct tabletop response exercise based on this scenario	Scheduled

7. Post-Incident Review

A full after-action review (AAR) is scheduled with the IT, Security, and Infrastructure teams. Logs have been archived and tagged for potential use in future forensic analysis or legal response.

8. Status

Current Status: Resolved
Date Closed: March 28, 2025
Ongoing Monitoring: Enabled