Cybersecurity Incident Analysis Report

Date: February 20, 2025
Classification: CRITICAL
Incident Type: SYN Flood DDoS Attack
Status: Resolved

Executive Summary

A critical security incident was detected affecting the company's travel website, resulting in complete service disruption. Analysis confirmed a SYN Flood DDoS attack originating from IP address 203.0.113.0, preventing employees from accessing critical sales resources.

Key Impact Metrics

- **Attack Duration:** 47.8 seconds
- **Malicious Packets:** 100+ SYN requests
- **Service Impact:** Complete outage
- **Affected Systems:** Web server, sales portal
- **Business Impact:** Employee productivity loss, potential revenue impact

---

Technical Analysis

Attack Pattern Identification

Network analysis through Wireshark packet capture revealed the following attack signatures:

```
Source IP: 203.0.113.0
Target: Port 443 (HTTPS)
Attack Vector: TCP SYN Flood
Pattern: Repeated SYN packets without completion of TCP handshake
```

Attack Characteristics

1. **TCP Handshake Manipulation**
   - Attacker sent continuous stream of TCP SYN packets
   - Server resources exhausted from half-open connections
   - Legitimate connection attempts resulted in timeouts
2. **Server Impact**

- TCP connection queue saturation
- Resource exhaustion
- Connection timeout errors for legitimate users
- Multiple RST packets indicating connection failures

Timeline of Events

Time (s)	Event Description
3.144	Initial legitimate connections observed
3.298	Normal HTTP GET requests processing
3.390	Start of SYN flood from 203.0.113.0
7.330	First connection timeouts observed
51.823	Attack continuing with sustained SYN packets

Attack Mechanics

The SYN Flood attack exploited the TCP three-way handshake process:

1. **Normal TCP Handshake Process:**
   - Client sends SYN
   - Server responds with SYN-ACK
   - Client completes with ACK
2. **Attack Method:**
   - Attacker floods server with SYN packets
   - Server allocates resources for each connection
   - Attacker never completes handshake
   - Server resources become exhausted
3. **Impact:**
   - Server TCP backlog queue saturated
   - Legitimate connections blocked
   - System resources depleted
   - Service effectively denied to valid users

Immediate Actions Taken

1. **Containment**
   - Server temporarily taken offline
   - Recovery of normal operation status initiated
   - Firewall rules updated to block attacking IP
2. **Investigation**
   - Packet capture analysis performed
   - Attack pattern identified
   - System logs reviewed
   - Impact assessment completed

Recommendations

Immediate Technical Controls

1. **SYN Flood Prevention:**
   - Implement SYN cookies
   - Configure rate limiting for incoming SYN packets
   - Increase TCP backlog queue size
   - Adjust connection timeout settings
2. **Network Security Enhancement:**
   - Deploy dedicated DDoS mitigation solution
   - Implement network behavior analysis
   - Configure automated alerting for unusual TCP patterns
   - Review and update firewall rules

Long-term Recommendations

1. **Infrastructure Improvements:**
   - Consider cloud-based DDoS protection services
   - Implement redundant server architecture
   - Review network capacity planning
   - Deploy load balancers
2. **Process Improvements:**
   - Develop incident response playbook for DDoS attacks
   - Conduct regular DDoS simulation exercises
   - Implement automated attack detection
   - Establish stakeholder communication protocols

Appendix: Technical Details

Network Traffic Analysis

```
Protocol: TCP
Destination Port: 443
```

```
Attack Duration: 47.8 seconds
Packet Type: SYN
Window Size: 5792
Sequence Number: 0
```

Mitigation Effectiveness

Post-implementation monitoring showed: - Successful blocking of attacking IP - Recovery of normal service operations - No residual system impact - Restored access for legitimate users

---

Report prepared by: Zayn AK Security Analyst*