Cybersecurity Incident Report

Date: July 27, 2024

Incident Type: Suspected SYN Flood Attack

Affected System: Company Web Server

Analyst: Junaid Shakoor

Section 1: Incident Description

On July 27, 2024, at approximately 3:30 PM EDT, an automated alert from our network monitoring system indicated abnormal activity on our web server. Upon investigation, it was discovered that users were experiencing connection timeouts when attempting to access the company website. A review of the server logs revealed a significant spike in incoming TCP SYN requests originating from a single, unfamiliar IP address: 192.168.2.75.

The pattern of traffic strongly suggests a SYN flood attack, a form of Denial-of-Service (DoS) attack designed to overwhelm a server's resources and render it unavailable to legitimate traffic.

Section 2: Technical Analysis

The TCP protocol, used for establishing connections between web browsers and servers, relies on a three-way handshake:

1. **SYN:** The client sends a SYN (Synchronize) packet to initiate a connection.
2. **SYN-ACK:** The server responds with a SYN-ACK (Synchronize-Acknowledge) packet, confirming receipt and agreeing to connect.
3. **ACK:** The client sends an ACK (Acknowledge) packet to finalize the connection.

In a SYN flood attack, the perpetrator sends a massive volume of SYN packets, often with spoofed source IP addresses, without ever completing the handshake. This forces the server to allocate resources to track these half-open connections, quickly depleting its capacity and preventing it from responding to legitimate requests.

In this incident, the logs indicate an abnormally high volume of SYN packets from the suspect IP address, far exceeding normal traffic patterns. This inundation of requests overwhelmed the server, causing it to drop legitimate connections and display timeout errors to users.

Impact Assessment:

- **Immediate Impact:** The company website was rendered inaccessible to both employees and customers, disrupting business operations and potentially leading to lost sales and revenue.

- **Employee Productivity:** Employees were unable to access critical resources and sales information, hindering their ability to serve customers.
- **Reputation:** The website outage could damage the company's reputation, particularly if it persists for an extended period.

Mitigation Actions Taken:

1. **Temporary Isolation:** The web server was temporarily taken offline to allow it to recover from the attack.
2. **Firewall Rule:** A rule was implemented on the company firewall to block all incoming traffic from the suspect IP address (192.168.2.75).

Next Steps:

While the immediate threat has been temporarily mitigated, it's important to note that IP blocking is not a long-term solution, as attackers can easily change their IP addresses.

It is recommended that we:

- **Investigate Further:** Analyze network traffic and logs in more detail to gather additional information about the attack and potentially identify the perpetrator.
- **Implement Mitigation Strategies:** Research and deploy more robust defenses against SYN flood attacks, such as SYN cookies, rate limiting, or cloud-based DDoS mitigation services.
- **Monitor for Recurrence:** Maintain heightened vigilance for any signs of recurring or similar attacks.
- **Communicate with Stakeholders:** Inform relevant parties, including management and employees, about the incident and the steps being taken to address it.

I'm prepared to provide additional technical details or answer any questions you may have.

Sincerely,

Junaid Shakoor

717-644-6870

shakoor.junaidre@gmail.com

Security Analyst