Cybersecurity Incident Preliminary Report

Date: July 27, 2024

Incident Type: Suspected SYN Flood Attack

Affected System: Company Web Server

Analyst:Junaid Shakoor

Incident Summary:

This afternoon, our company website became inaccessible to both employees and customers. Upon investigation, server logs revealed a massive influx of TCP SYN requests originating from a single, unfamiliar IP address: 192.168.2.75. This pattern of activity strongly suggests a SYN flood attack, a type of Denial-of-Service (DoS) attack designed to overwhelm a server and disrupt its normal operation.

Technical Analysis:

The TCP protocol, utilized for establishing connections between web browsers and servers, involves a three-way handshake. A SYN flood attack disrupts this process by sending a flood of SYN packets without completing the handshake, causing the server to exhaust its resources. This is precisely what the logs indicated, with an abnormally high volume of SYN requests originating from the suspicious IP address.

Impact Assessment:

The immediate consequences of this attack were significant:

- Website downtime resulted in potential lost sales and revenue.
- Employee productivity was hampered due to the inability to access critical resources.
- The company's online reputation may have suffered due to the outage.

Mitigation Actions Taken:

To address the immediate threat, the following steps were taken:

1. The web server was temporarily taken offline to allow it to recover.
2. A firewall rule was implemented to block all incoming traffic from the suspect IP address (192.168.2.75).

Next Steps:

While these measures have temporarily mitigated the issue, they are not a long-term solution. Further investigation is required to gather more information about the attack and its source.

Additionally, implementing more robust security measures, such as SYN cookies, rate limiting, or cloud-based DDoS mitigation services, is crucial to prevent future attacks.

Recommendations:

- Conduct a thorough analysis of network traffic and logs to identify the attacker and assess the full extent of the damage.
- Research and deploy appropriate security measures to protect against SYN flood and similar DoS attacks.
- Monitor network activity closely for any signs of recurring or new threats.
- Inform relevant stakeholders, including management and employees, about the incident and the ongoing mitigation efforts.

I am available to provide further technical details or answer any questions as needed.