Incident report analysis – DDoS Attack

Cybersecurity Analyst

July 30, 2025

Summary	On July 30, 2025, a multimedia company providing web design, graphic design, and social media marketing services experienced a distributed denial of service (DDoS) attack, disrupting its internal network for approximately two hours. The attack involved a flood of Internet Control Message Protocol (ICMP) packets, overwhelming network resources and preventing access to services. The incident management team responded by blocking incoming ICMP packets, taking non-critical services offline, and restoring critical services. The cybersecurity team identified the cause as a malicious actor exploiting an unconfigured firewall to send excessive ICMP pings. Mitigation measures included implementing firewall rules to limit ICMP traffic, verifying source IP addresses, deploying network monitoring software, and installing an intrusion detection and prevention system (IDS/IPS). The attack disrupted business operations, but no data loss was reported.
Identify	The incident was a DDoS attack targeting the companys internal network infrastructure. The attack exploited a vulnerability in an unconfigured firewall, allowing a flood of ICMP packets to overwhelm network resources. Affected systems and components include: Hardware/Systems: Internal network servers, routers, and firewalls handling traffic. Processes/Business Environment: Web design, graphic design, and social media marketing services were disrupted, impacting client-facing operations and internal workflows.

	People: Employees requiring access to internal network resources were unable to perform duties during the attack. The attack originated from an external malicious actor using spoofed IP addresses, highlighting gaps in firewall configuration and IP verification protocols.
Protect	To safeguard assets against future DDoS attacks, the following measures are recommended: Access Control: Implement rate-limiting rules for ICMP traffic and verify source IP addresses to block spoofed packets. Restrict network access to trusted IP ranges for critical systems. Awareness/Training: Conduct mandatory cybersecurity training for employees, focusing on recognizing DDoS attack indicators and secure network practices. Data Security: Encrypt sensitive data in transit and at rest to mitigate risks in future attacks, despite no data compromise in this incident. Information Protection and Procedures: Update firewall management procedures to include regular audits and configuration reviews. Maintenance: Regularly update firewall firmware, network devices, and software to address vulnerabilities. Protective Technology: Deploy an IDS/IPS system to filter malicious traffic and implement network monitoring software to detect abnormal patterns in real time.
Detect	To enhance detection of similar incidents, the following tools and processes are proposed: Anomalies and Events: Deploy a Security Information and Event Management (SIEM) system to aggregate and analyze network logs, alerting IT staff to unusual traffic patterns, such as excessive ICMP requests. Security Continuous Monitoring: Implement network monitoring software to track inbound and outbound traffic, identifying spikes in ICMP or other

	protocol traffic from non-trusted sources. Detection Process: Utilize an IDS to detect unauthorized access attempts and abnormal traffic behaviors. Configure alerts for high-frequency ICMP packets or connections from unverified IP addresses. Conduct regular audits of user account activity.
Respond	A response plan for future DDoS incidents includes: Response Planning: Develop a formal incident response plan outlining roles, responsibilities, and escalation procedures. Include steps to isolate affected systems and reroute traffic. Communications: Notify IT staff, management, and affected employees immediately upon detecting an incident. Communicate with clients if services are impacted, ensuring transparency and regulatory compliance. Analysis: Conduct a root cause analysis post-incident to identify vulnerabilities (e.g., firewall misconfigurations) and trace attack origins using log data and traffic analysis. Mitigation: Contain incidents by isolating affected network segments, blocking malicious IP addresses, and throttling traffic. Temporarily disable non-critical services to prioritize critical system availability. Improvements: Update incident response procedures based on lessons learned, incorporating automated tools for faster containment and regular tabletop exercises.
Recover	To restore operations following a DDoS incident: Recovery Planning: Restore affected systems by restarting services and verifying network integrity. Use backup configurations to restore firewall settings if corrupted. Prioritize critical services for restoration. Improvements: Enhance recovery processes by maintaining redundant network paths and load balancers to minimize downtime. Regularly test backup and restoration procedures. Communications: Inform employees and clients of restored services,

	providing timelines for full operational recovery. Communicate with regulatory bodies if required by local laws.

Reflections/Notes: The DDoS attack highlighted the critical need for robust firewall configurations and proactive network monitoring. Implementing the NIST CSF ensures a structured approach to managing cybersecurity risks, emphasizing continuous improvement. Regular training, updated policies, and advanced detection tools will strengthen the organizations resilience against future attacks. The incident underscores the importance of rapid response and recovery to minimize operational and reputational impact.