Multimedia Company DDoS Attack: Incident Report Analysis

Summary	In recent days, numerous staff members reported a sudden cessation of network services within the organization. Further investigation revealed that the network had been compromised by an influx of ICMP packets. These requests originated from various sources, culminating in a Distributed Denial of Service (DDoS) attack that generated an ICMP deluge through an improperly configured firewall. As a result, all standard internal network traffic was unable to access network resources due to the overwhelming volume of ICMP requests.
Identify	The incident response team conducted an audit of the network components, firewalls, and access protocols involved in the attack to pinpoint security vulnerabilities. Their investigation uncovered that one of the organization's firewalls lacked proper configuration, with no port restrictions or IP regulations in place. The ensuing downtime resulted in a total of 120 minutes without any operational or revenue-generating services being accessible. Any information stored within the network must be cross-referenced with backups to identify any compromised or missing data.
Protect	The team has established a new firewall protocol to restrict the influx of ICMP packets, implemented source IP address authentication for firewalls, deployed network surveillance software to detect unusual traffic patterns, and installed an Intrusion Detection/Prevention System (IDS/IPS) to filter out suspicious network activity. Furthermore, the team will establish new standard configurations for all firewalls to ensure they meet a uniform security standard.
Detect	To identify similar attacks and abnormalities that could potentially lead to attacks, the team will employ firewall logging tools and an IDS to monitor all

	incoming network traffic from IP addresses outside the internal network. The team will also evaluate the potential benefits of upgrading to a Next Generation Firewall (NGFW), considering its advanced features such as intrusion protection.
Respond	The team has recalibrated firewall and security protocols to identify ICMP floods and comparable request flood attacks. The targeted firewall has been reconfigured with robust security rules to align with the baseline configuration. All security personnel have been briefed on the cause, response, and outcomes of the attack. We have notified senior management of this incident, and they will collaborate with content teams to inform customers about the service interruption. Management will also need to report the incident to law enforcement and other relevant organizations as mandated by local regulations.
Recover	The affected server has been reset to its baseline configuration and is now fully operational. All data or assets associated with the server have been verified to be restored to their most recent backup, which should be from the previous evening. For future attacks of this nature, external ICMP requests should be blocked at the firewall level once an ongoing flood is confirmed. Subsequently, all non-essential network services should be suspended to minimize internal network traffic. Next, critical network services should be prioritized for restoration. Finally, once the attack has been mitigated, security team members can begin reinstating non-critical services, repairing damaged systems, and relaying information to organizational leadership.

Reflections/Notes:

This incident highlights several crucial areas for improvement in our network security infrastructure.

The unconfigured firewall that allowed the DDoS attack to penetrate our defenses represents a significant oversight in our security protocols. Moving forward, we must implement more rigorous procedures for firewall configuration and regular audits of our network security measures.

The two-hour downtime resulted in substantial operational and financial impacts, underscoring the critical nature of our network services to business continuity. This event serves as a stark reminder of the importance of proactive security measures and the need for a robust, rapid-response protocol for similar incidents in the future. Our incident response team demonstrated commendable efficiency in identifying and addressing the issue. However, the incident reveals the need for more comprehensive network monitoring tools that can detect and alert us to unusual traffic patterns before they escalate into full-blown attacks. The implementation of new security measures, including rate-limiting ICMP packets and deploying an IDS/IPS, should significantly enhance our ability to prevent and mitigate similar attacks in the future. However, we must remain vigilant and continuously update our security strategies to stay ahead of evolving threats.

Lastly, this incident underscores the importance of clear communication channels both within our organization and with external stakeholders. Timely and transparent communication about the outage to our customers and relevant authorities is crucial for maintaining trust and complying with regulatory requirements.