**Multimedia Company DDoS Attack: Incident Report Analysis**

|  |  |
| --- | --- |
| **Summary** | Earlier this week, reports from multiple employees stated that the organization’s network services had suddenly stopped responding. It was then discovered that the network had been disrupted by a flood of ICMP packets. The requests were originating from multiple sources, resulting in a Distributed Denial of Service Attack (DDoS) that created an ICMP flood through an unconfigured firewall. All normal internal network traffic was unable to access any network resources due to the network being overwhelmed with ICMP requests. |
| Identify | The incident management team audited the network devices, firewalls, and access policies involved in the attack to identify vulnerabilities in security. The team found that one of the organization’s firewalls was left unconfigured without any port blocking or IP rules. The resulting outage resulted in a total of 2 hours without any business operations or revenue generating services being available. Any data stored within the network must be compared to backups to identify any damaged or stolen data. |
| Protect | The team has implemented a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification for firewalls, network monitoring software for abnormal traffic patterns, and an Intrusion Detection/Prevention System (IDS/IPS) system to filter suspicious network activity. Additionally, the team will define new baseline configurations for all firewalls to ensure that all firewalls are up to a secure standard. |
| Detect | To detect similar attacks and anomalies that could lead to attacks, the team will use firewall logging tools and an IDS to monitor all incoming network traffic from IP addresses not within the internal network. The team will also consider switching to a Next Generation Firewall (NGFW) depending how much the org would benefit from its features like intrusion protection. |
| Respond | The team has reconfigured firewall and security rules to recognize ICMP floods and similar request flood attacks. The targeted firewall has been reconfigured with strong security rules to match that of the baseline configuration. All security employees have been notified of the cause, response, and results of the attack. We have informed upper management of this event and they will work with content teams to notify customers about the outage. Management will also need to inform law enforcement and other organizations as required by local laws. |
| Recover | The affected server has been reset back to the baseline configuration and is fully functioning. All data or assets related to the server have been confirmed to be reverted to their most recent backups, which should be from the previous night. For future attacks like this, external ICMP requests need to be blocked at the firewall level after confirmation of an ongoing flood. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, when the attack has been resolved, security team members can begin restoring non-critical services, restoring damaged systems, and communicating to organization leadership. |

|  |
| --- |
| Reflections/Notes: |