**Multimedia Company DDoS Attack :Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | Earlier this week, multiple employees reported network services tied to the multimedia company had suddenly stopped responding and became inoperable. Upon investigation, the network disturbance was caused by a flood of ICMP packets being sent by an attacker. The requests were being sent from multiple sources, implying a Distributed Denial of Service (DDoS) attack caused by an improperly configured firewall. Normal network functionality was lost due to the network being overwhelmed by ICMP requests. |
| Identify | The incident management team reviewed network activity by auditing firewalls, network devices and policies. The team discovered the attack was able to flood the server with TCMP requests through an unconfigured firewall, allowing for open ports that were not blocked, and no IP rules. The outage caused the organization to lose functionality for over two hours, which resulted in a loss of revenue. Any data stored on the network will need to be compared to the baseline image prior the attack. |
| Protect | The security team responded to the incident by implementing new security measures such as a new firewall rule, limiting the rate of incoming ICMP packets. Source IP verification within the firewall was enabled, checking for spooked IP addresses on incoming ICMP packets. Utilization of network monitoring software, which will detect real time abnormal traffic patterns and alert the security team. |
| Detect | The detect future attacks and vulnerabilities that could lead to attacks, the team will begin using IDS to monitor all incoming network traffic from IP addresses that are no associated within the network. The team will use firewall logging, and will consider the use of Next Generation Firewall (NGFW) to maximize security capabilities for the organization. |
| Respond | The security team has reconfigured the current firewall rules, enabling the identification of ICMP floods, and similar flood requests. The firewall was reconfigured to match baseline security configuration. All team members have been debriefed on the incident, including the cause, action taken and the overall results of the attack. Team leaders and management have been informed and will begin to notify customers of the event. Management will need to work with law enforcement as required by local or federal laws. |
| Recover | The affected server has been reformatted back to baseline configurations and has full functionality. All settings and data have been reset back to baseline configuration and restored. To provide continuous safeguarding, ICMP requests originating from external IPs need to be blocked at the firewall level once a flood is identified. Team will communicate the order in which assets and data will be recovered, beginning with critical services then restoring non-critical services and how to proceed with restoring damages. |

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