**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | This multimedia company recently experienced a DDoS attack based on a flood of ICMP packets, which compromised the internal network for two hours until it was resolved. After the investigation of the IT team, we discovered that the malicious actor sent a flood of ICMP pings into the company’s network through an unconfigured firewall, in that way the attacker overwhelmed the network using a DDoS attack. The network security team responded in various ways: updating their firewall with the rule of limit the rate of incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics and sourcing IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. The impact of the attack consists of business disruption, revenue loss and reputation damage. |
| Identify | The company suffered of a distributed denial of service attack (DDoS) exactly it has been an ICMP flood attack. The network started flooding receiving constant and huge amounts of ICMP packets, then the network got overwhelmed and stopped working. This lead to workers and users to be unable to access all the network including all the resources. This attack affected the overall of the productivity and operations of the organization. |
| Protect | The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets, an IDS/IPS system to filter out some of the ICMP traffic based on suspicious characteristics and source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| Detect | In order to prevent this attacks from happening, the network security team implemented an IP address verification on the firewall to check spoofed IP addresses on ICMP packets and a network monitoring software to detect abnormal traffic patterns. |
| Respond | For now on if an attack occurs we will isolate the affected resources (to avoid the spreading), block incoming ICMP packets, stop all non-critical network services offline, and restore critical network services, in that way they will contain the issue. Previously using the network monitoring system should detect any abnormal traffic patterns, and the IDS/IPS system should work filtering out the traffic based on suspicious characteristics. Finally, we will have to update the playbook used in prevention of attacks, in order to get a complete baseline configuration. |
| Recover | When the attack happened, the server and the network went down for several hours, so at this point all the data has to be recovered and the access to the network services too. This type of attacks will be blocked by the updated firewall, then all non-critical network services will be stopped, finally the critical network services will be restored first. If the critical network services were restored, then we will restore the ones that are non-critical bringing them online again. |

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