**Incident report analysis**

| **Summary** | According to reports, the multi-media-based company fell victim to a DDOS attack, which knocked its internal network offline for roughly 2 hours prior to it being restored to its fully functioning state. Amid the attack, the organization’s network services seized responsiveness upon an abnormal deluge of ICMP packets and consequently, this caused internal users to have trouble accessing network resources. As a response, the companies incident response team chose to block further ICMP packet requests, which basically neutralized any non-essential network functions while prioritizing quintessential services as well. Subsequently, the organization’s security team analyzed the incident and discovered that the superfluous amount of ICMP pings were sent through an inadequately configured firewall to their organizational network from an unfamiliar and malicious source. Unfortunately, this loose firewall configuration provided a window of opportunity for the attacker to bombard their network by way of a DDoS attack. | | |
| --- | --- | --- | --- |
| **Identify** | Our security team has audited their internal network components, access privileges and devices in order to determine possible gaps in their securities. The company's incident response team inspected its ICMP logs relative to the incident and realized that a redundant volume of ICMP pings were transmitted from a suspicious source through a loosely configured firewall in order to overwhelm their network and ultimately compromise its functionality. Evidently, the log data suggests that the inadequately configured firewall was what left their organizational network exposed as well as vulnerable to a DDOS attack. | | |
| **Protect** | Their security team updated their firewall parameters and configurations in order to cap the volume of ICMP packets that are allowed entry to their network within a particular length of time. In addition, the team also deployed both IDS and IPS systems in order to be able to better monitor as well as manage what ICMP packet requests are granted access to their network given their respective IP traits or package contents. | | |
| **Detect** | We also updated the source IP configurations within their firewall in order to distinguish data packets being sent from fraudulent source IPs from those of legitimate ones as well as installed network surveillance programs like wireshark, so that they could maintain keeping a proverbial close eye for anomalies amongst day to day network traffic transmissions. | | |
| **Respond** | Responsively, to combat these cloud security issues we opted to implement security measures like new firewalls to place a cap on the volume of inbound ICMP packets as well as source IP address verifiers in order to distinguish potential incoming packets containing spoofed IP addresses. Additionally, we also decided to integrate SIEM tools as well as network monitoring software to have one central dashboard to keep overwatch for network anomalies and we also implemented both IDS/IPS systems in order to distinguish between illegitimate or legitimate ICMP transmissions. | | |
| **Recover** | The incident management team recovered operational functionality of the companies essential network services, while also halting non-essential services and blocking inbound ICMP packet transmissions. Moreover, we will also restore their networks baseline configurations after rebooting the networking, so that appropriate configurations can be upheld in the future as well as regularly updated to address any future network vulnerabilities or unforeseen threats that may arise. | | |

| **Reflections/Notes**: N/A |
| --- |