INCIDENT REPORT | 005 | ICMP ATTACK

DETAILS

Cloudo Media
Cause: DDoS due to ICMP flood
Duration: 2 hours

Cloudo Media was at the end of a DDoS attack due to a flood of ICMP packet requests targeting the internal network. DDoS attacks, like this one, will sometimes successfully disrupt business activities and client services.

- Logs indicated that the internal network was affected by a constant barrage of ICMP packet requests.
- This disrupted business and customers were not able to reach the company’s main platform for uploading content.
- Logs indicated that the DDoS attack originated from an unconfigured firewall on an office computer.
- This firewall did not have a basic configuration for blocking specific DDoS attacks via organization controls.

RESPONSE

To stop the disruption, a block from the organization's web service was issued to future ICMP traffic. Because of this incident, the cybersecurity team implemented strict firewall rules, IP spoofing detection, stronger network monitoring, and stronger intrusion detection systems.

- The security team decided that it would be best to provide some training and re-education to everyone within the organization.
- The security team received proper management and communication training.
- Other teams received additional instruction on security rules and procedures.
- Other teams were made aware of new rules and procedures.
- New firewall rules were implemented within a simple guide explaining on how to check them and issued to every user email address. 100% completion.
- After looking at logs, firewall rules were redesigned to be more strict.
- The IDS were improved for detecting more real-time threats, which took configurations made specifically focused on ICMP flood threats.