Incident report analysis

Summary	Today, the client organization experienced a DDoS attack that targeted and compromised our internal network for two hours. During the attack, the client's network suddenly stopped responding due to a flood of incoming ICMP packets. This prevented normal network traffic from accessing the usual network resources. Our team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. From our team's findings, the root cause of the issue is likely due to the unconfigured firewall used by the client's network. The malicious actor(s) used this vulnerability to overwhelm the client's network with incoming ICMP packets.
Identify	The type of attack that caused the client's network to compromise is called the **ICMP flood attack**. This is a type of DoS attack performed by a malicious actor repeatedly sending ICMP packets to a network server. In this case, our team was also able to confirm that multiple devices/servers in different locations were used to flood the target network with unwanted traffic. This means that this was a DDoS attack as well. The entire network was affected and compromised by the attack.
Protect	In order to help prevent an attack like this from occurring in the future, our team updated and patched all of the operating systems used by the client's company. In addition, we configured the firewall rules to limit the rate of incoming ICMP packets, which should help prevent a flood from happening again. Another rule we added was source IP address verification, to ensure that no spoofed IP addresses are sending ICMP packets to the network.

Detect	To detect a future incident similar to this one, our team has implemented a network monitoring software that can detect abnormal traffic patterns within the network. If the network is experiencing any abnormal behavior, our security team will be immediately notified - which allows us to respond quicker. In addition, our team added an IDS/IPS system to filter out some ICMP traffic, based on suspicious characteristics. It will detect and attempt to prevent the traffic from entering the network.
Respond	Our security team responded to the attack by blocking incoming ICMP packets, and stopping all non-critical network services offline. We informed upper management of the issue and its potential cause, and they informed us that they will be informing customers of the breach shortly. Upper management is required by local law to additionally report this incident to law enforcement, and the proper agencies.
Recover	In our recovery from this incident, we first focused on restoring critical network services, so that the network and client's organization could function. We then informed staff of the incident, and let them know that any customer information added around the time of the incident should be checked and reuploaded, just in case. Lastly, we lifted the block on incoming ICMP packets after we had configured the firewall to operate as intended.

Reflections/Notes: