Incident report analysis

Friday, February 16 2024

Shafee Ahmed

Summary	Axiom Apparel was hit with a DDoS (Distributed Denial of Service) attack that knocked out its servers for approximately two hours. The malicious actor was using ICMP packets through an unsecured firewall. The company blocked the problematic ICMP traffic by temporarily shutting down non-essential services to get control again. Then, the team enhanced their network's security with more strict firewall rules, as well as IP verification checks, continuous traffic monitoring with preventative network monitoring software, and an IDS/IPS system in place.
Identify	- The attack type was Distributed Denial of Service (DDoS). - It affected Axiom Apparel's internal network.
Protect	To secure the organization's assets in the future: - consider updating the firewall configuration to not only rate limit ICMP packets, but also implement a comprehensive rule for each type of traffic. - incorporate employee training on recognizing phishing attempts and securing their credentials. - update and patch all systems and software regularly to close any security vulnerabilities
Detect	As new network monitoring software is under way at Axiom Apparel, we should be vigilant in using SIEM tools for real-time analysis of security alerts, as well as

	regularly performing vulnerability scans and pen testing to identify and mitigate potential risks.
Respond	- To contain affected devices, isolate them and/or segment their networks to prevent the spread of attack. - To neutralize, use tools to block malicious traffic and disable any compromised accounts. - For analysis, gather logs from networks, firewalls, IDS/IPS systems, and SIEMs to analyze the attack pattern and origins. - To improve, review the incident response process for any shortcomings.
Recover	To recover immediately, identify critical data and systems that need to be restored first for business continuity. For processes that help the business resume, utilize backups regularly to restore affected systems and data. Review and update the disaster recovery and business continuity plans from the lessons learned from the incident.

Reflections/Notes:

Scenario:

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small

businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.

To address this security event, the network security team implemented:

- A new firewall rule to limit the rate of incoming ICMP packets
- Source IP address verification on the firewall to check for spoofed IP addresses on 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

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.

- Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.

Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.