LevelBlue

CUSTOMER STORIES

Federal Agency Protected with LevelBlue DDoS Defense

Solution

- LevelBlue Distributed Denial of Service (DDoS) Defense

Challenges

- A large federal agency became the victim of a volumetric carpet-bombing DDoS attack.
- The attack targeted hundreds of online destinations, flooding the agency's network with false traffic and overwhelming their bandwidth.
- During the attack period, the agency's services were disrupted, including email and virtual private network (VPN) services for remote access.
- The attack also affected the agency's DNS resolution capabilities and took down websites hosted within their network.

Overview

A branch of the federal government became the target of volumetric distributed DDoS attacks, which disrupted daily operations by overwhelming their websites and networks. The hacker group behind the attack was not named. This case study discusses how LevelBlue assisted the government agency to mitigate the attack and help protect against future DDoS attacks.

Introduction

A large federal agency became the target of a 21-hour carpet-bombing (volumetric) DDoS attack, which overwhelmed their bandwidth capabilities. This widespread attack was highly disruptive, discontinuing operations of websites, email, and VPN access across multiple sub-agencies.

The carpet-bombing attack spread indiscriminate assaults over a wide area rather than concentrated attacks on specific targets. The attack vectors consisted of ICMP floods, DNS amplification, Network Time Protocol floods, and fragmented packets.

- ICMP floods overwhelm targets with continuous request packets (pings). This can cause network congestion and prevent legitimate users from accessing network resources.
- DNS amplification occurs when vulnerabilities in DNS servers are exploited to turn initially small queries into larger payloads, thereby increasing the traffic and bringing down the victim's servers.
- Network Time Protocol floods exploit server functionality to overwhelm a targeted network or server with an amplified amount of user datagram protocol (UDP) traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.

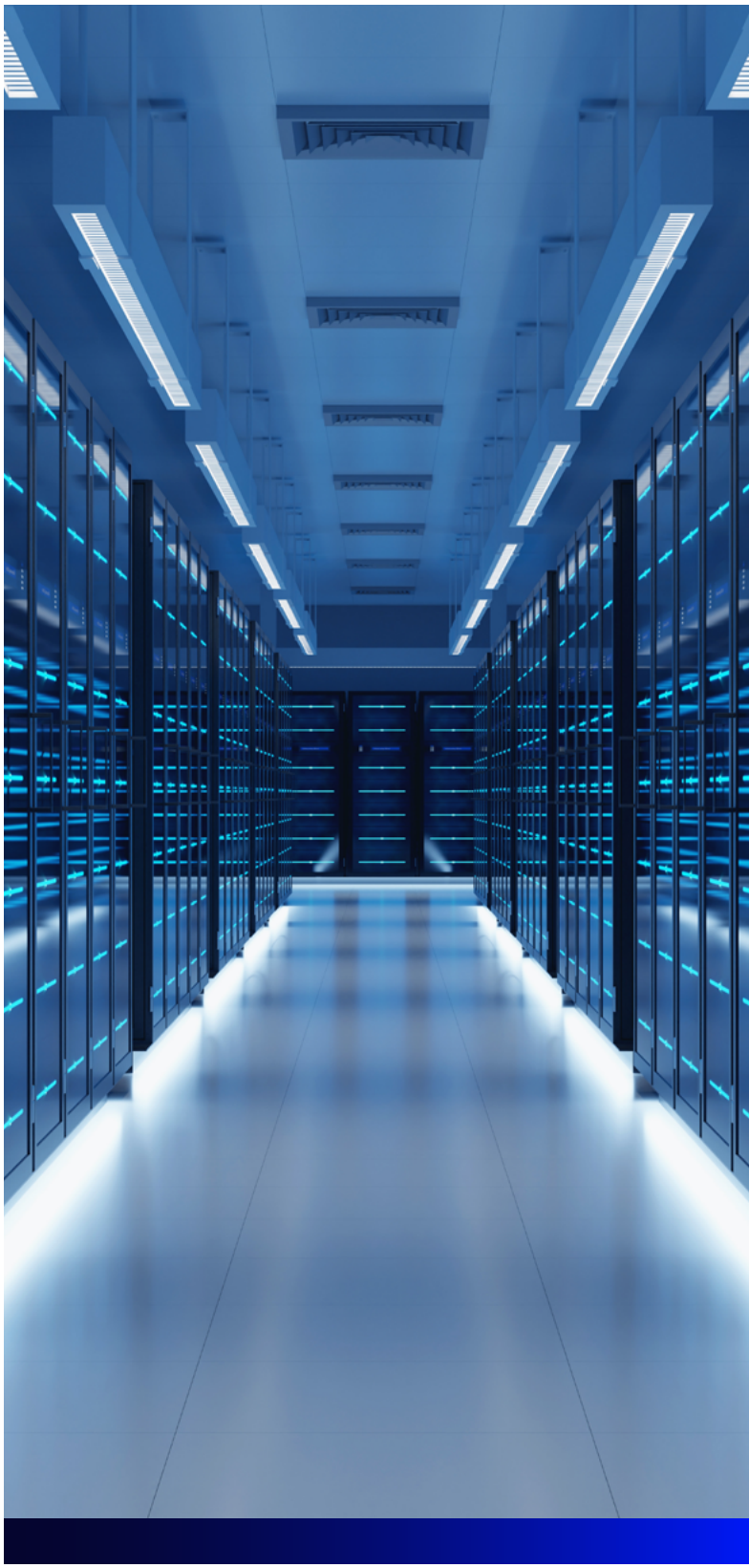
- Fragmented packet attacks happen when attackers take advantage of the process by which IP packets are broken into smaller fragments for transmission. Attackers manipulate these fragmented packet parameters to trigger vulnerabilities or bypass firewall rules, overwhelming a target system and causing it to become unresponsive or crash.

The agency had LevelBlue DDoS Defense services in place, and therefore the LevelBlue platform was able to automatically initiate mitigation by rerouting 250 Gbps of traffic to six scrubbing centers in less than five minutes. LevelBlue also took additional communication measures to maintain constant collaboration with the agency to mitigate the attack. LevelBlue deployed multiple techniques to counter the denial-of-service attack. These techniques included rate limiting, UDP amplification counter measures, DNS protections, TCP SYN protection, TCP/IP packet validation, and other customer specific counter measures. These counter measures progressively reduced the effects of the attack on the agency.

Results/Highlights

LevelBlue provided a large U.S. federal agency with emergency DDoS mitigation service support to quickly mitigate a unique carpet-bombing attack, including:

- Prompt investigation of the incident, including the deployment of IT system engineers specializing in DDoS who investigated multiple DDoS attack vectors
- Immediate incident response mitigation within five minutes, most critical services restored within 90 minutes, and fully mitigated in less than eight hours
- Close collaboration with the customer during the attack
- After-hours support during the peak period of the attack
- 24/7 DDoS protection
- A solution to help with future protection against DDoS attacks



LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.