LevelBlue

CUSTOMER STORIES / STATE AND LOCAL GOVERNMENTS

# State and Local Governments Protected with LevelBlue DDoS Defense

## Overview

A US state and local government became the targets of volumetric DDoS attacks, which overwhelmed their websites and networks, limiting daily operations. The hacker group Anonymous Sudan claimed they were executing these attacks for political reasons to create awareness of the conditions in the country. This case study discusses how LevelBlue assisted the government agencies in mitigating the attacks and protecting against future denial-of-service attacks.

## Introduction

A large US state and one of its largest cities became the targets of a 41-hour carpet-bombing volumetric DDoS attack, which overwhelmed their bandwidth, disrupting operations for days. The agencies depended on the Internet for website operations across the state and the city, including policing, licensing, taxing, and permitting. 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 a 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.

**Solution**

- LevelBlue Distributed Denial of Service (DDoS) Defense

**Challenges:**

- Agencies became the victims of volumetric carpet-bombing DDoS attacks.
- Hundreds of random destinations were attacked during the siege and were flooded with phony traffic to knock them offline.
- There were intermittent disruptions to the websites of multiple state agencies that were initially widespread across state services.
- At the local level, a city dealt with a network interruption that caused service issues for several days. The attack affected transactions involving licensing, taxing, permitting, and policing, such as verifying if a vehicle was stolen or if someone had an outstanding warrant.

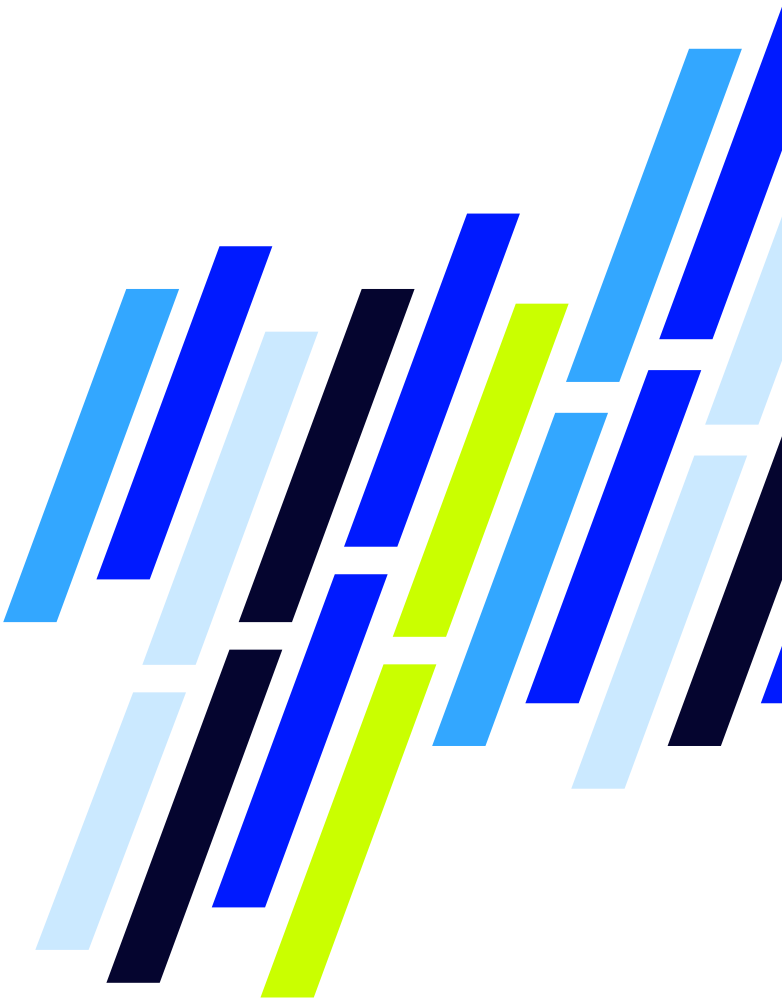
LevelBlue alerted the customers of the attacks and took proactive action to begin mitigation. The governments had LevelBlue DDoS Defense services in place. Therefore, the LevelBlue platform automatically initiated mitigation by rerouting 200 Gbps of traffic to six scrubbing centers in less than 5 minutes. The attacks were initially widespread across state services, and those effects were diminished throughout the day as LevelBlue employed multiple techniques to counter the denial-of-service attack. These techniques included rate limiting, UDP amplification countermeasures, DNS protections, TCP SYN protection, TCP/IP packet validation, and other customer-specific countermeasures.

LevelBlue

## Results/Highlights

**LevelBlue provided the state and city governments with solutions that met the challenges they were facing:**

- Prompt investigation of the incident, including the deployment of IT system engineers specializing in DDoS who investigated multiple DDoS attack vectors
- Incident response mitigation within five minutes, and the customer was back online and stable within 45 minutes
- Close collaboration with the customer during the attack
- After-hours support during the peak 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.**