incident report

WINDOW

Incident Start: 9/25/2021 2:55 PM ET
Incident End: Ongoing

SERVICES

- Core Voice
- API Voice
- Core Messaging
- API Messaging
- Bandwidth Dashboard and API
- EVS Number Provisioning
- 911 Voice

SUMMARY

- At 2:55pm ET on September 25, Bandwidth received alarms indicating the existence of a critical network-wide incident.
- Bandwidth engineering resources were engaged and identified a very high volume DDoS attack was underway, affecting all Bandwidth data centers and began troubleshooting and recovery efforts.
- Due to the severity of the attack, Bandwidth infrastructure and applications became impaired and Bandwidth customers would have experienced disruption across all services including Voice, Messaging, Number Provisioning and 911.
- Bandwidth implemented DDoS auto-mitigation across the network as the first step towards resolution.
- Secondly, Bandwidth teams blocked affected ports and implemented additional access control lists to mitigate the underlying condition.
- Our engineering and application teams validated the successful recovery of all services and believed the incident had been fully resolved at approximately 6:35pm ET on September 25..
- However, Bandwidth was then targeted three additional times during the following windows:
    - September 26, 10:52am - 2:35pm ET
    - September 26, 5:39pm - 6:40pm ET
    - September 27 8:24am - ongoing

- The signature of the attack changed on subsequent attacks on September 26th, but was less impactful given the work done the previous day.
- However, the attacks on September 27 were across more targeted applications and Bandwidth has had lesser success in mitigating the impact to customers.
- Customers may have observed either a full or partial impairment of the listed services during the recovery of the network.
- Unfortunately, the DDoS threat remains but Bandwidth is continuing to aggressively tackle the malicious activity and mitigate all network and service impacts to the greatest degree possible; both internally and with external partners.

ROOT CAUSE

- On multiple occasions, the Bandwidth network has been the target of a DDoS attack which have resulted in the impairment of infrastructure and applications for customers.

RESOLUTION

- During the first DDoS attack, Bandwidth implemented DDoS auto-mitigation across the network.
- Bandwidth teams then blocked affected ports and implemented more specific access control lists to resolve the first incident.
- However, given the subsequent attacks this incident is ongoing. Bandwidth is marshalling all resources to mitigate impacts to services due to these attacks.

Scott Mullen
Chief Technology Officer