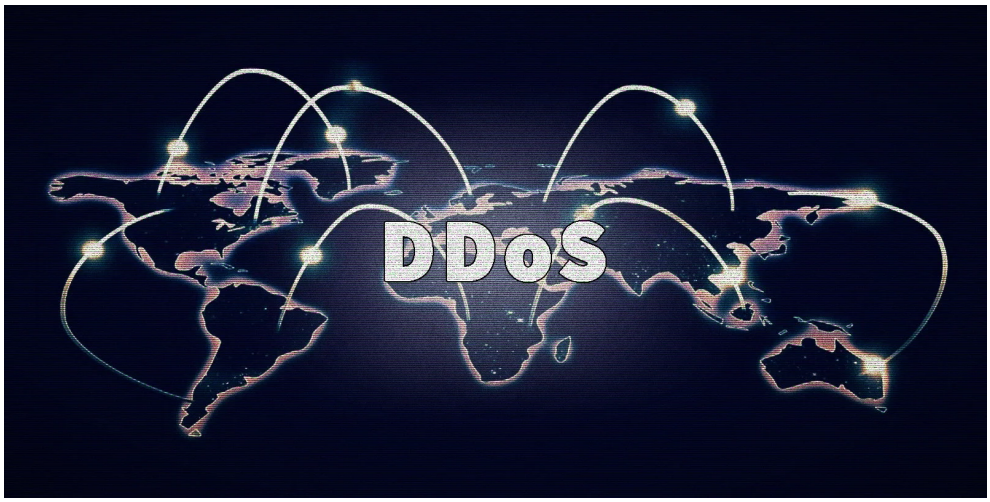
Bandwidth.com is latest victim of DDoS attacks against VoIP providers

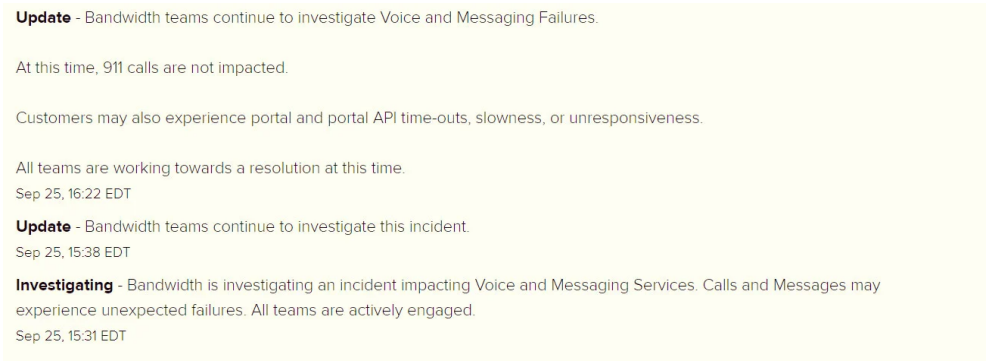
By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** September 27, 2021 09:07 PM **0**



Bandwidth.com has become the latest victim of distributed denial of service attacks targeting VoIP providers this month, leading to nationwide voice outages over the past few days.

Bandwidth is a voice over Internet Protocol (VoIP) services company that provides voice telephony over the Internet to businesses and ers.

Services. Calls and Messages may experience unexpected failures. All teams are actively engaged," reported Bandwidth on their status page (https://status.bandwidth.com/).



Beginning of the outage messages reported by Bandwidth.com
Source: BleepingComputer

Since then, Bandwidth has been providing frequent status updates detailing outages affecting voice, Enhanced 911 (E911) services, messaging, and access to the portal.

As Bandwidth is one of the leading telephony providers for US voice over IP companies, many other VoIP vendors reported outages over the past few days, including Twilio (https://status.twilio.com/), Accent (https://www.accentvoice.com/cloud-status/), DialPad (https://status.dialpad.com/), Phone.com (https://status.phone.com/), and RingCentral (https://status.ringcentral.com/).

While it has not been confirmed if these outages are related to Bandwidth's service disruption, all of the above carriers stated that another upstream provider has caused their outages.

> *"The upstream provider has indicated that service has returned to normal operation. We will continue to monitor this situation and report any new information as it becomes available. Customers should be prepared for potential impairments of inbound services within 12-16 hours as the potential exists for this DDoS attack to return. We will not close this issue until services have returned to the normal operation for a period of 72 hours." - Accent's status page (http://www.accentvoice.com/cloud-status/).*

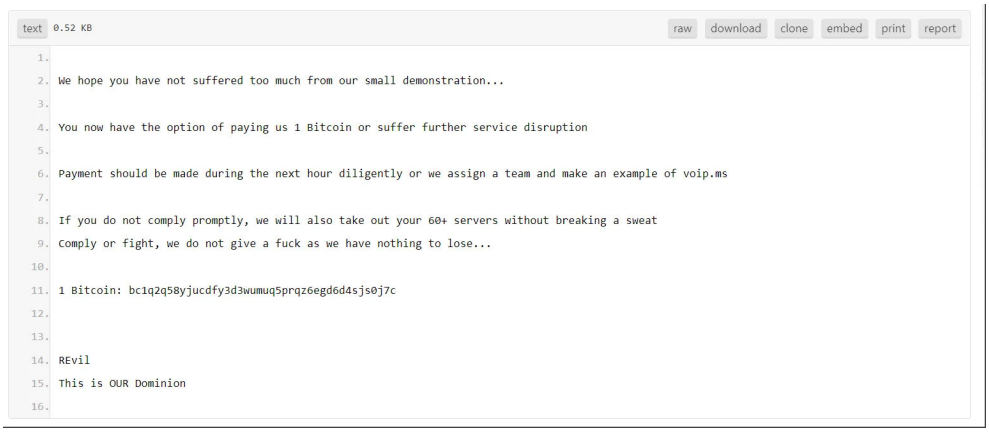
Twilio initially told BleepingComputer that they were not affected by Bandwidth's attack, but their status page states that they had issues with Bandwidth today.

> *or as soon as more information becomes available." Twilio's status page (https://status.twilio.com/).*

Bandwidth.com hit with a DDoS attack

Earlier this month, VoIP provider VoIP.ms suffered a catastrophic week-long DDoS attack (https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/) that took down almost all of their services and portals, leaving their customers without voice services.

The VoIP.ms attack was an extortion DDoS attack where threat actors impersonating the ransomware group 'REvil' initially demanded one bitcoin (https://web.archive.org/web/20210918231028/https://pastebin.com/y207gbnR) ($45,000) to halt their attacks but later increased it to 100 bitcoins (https://twitter.com/REvil92457183/status/1439281375937433609) ($4.5 million).



VoIP.ms ransom note
Source: BleepingComputer

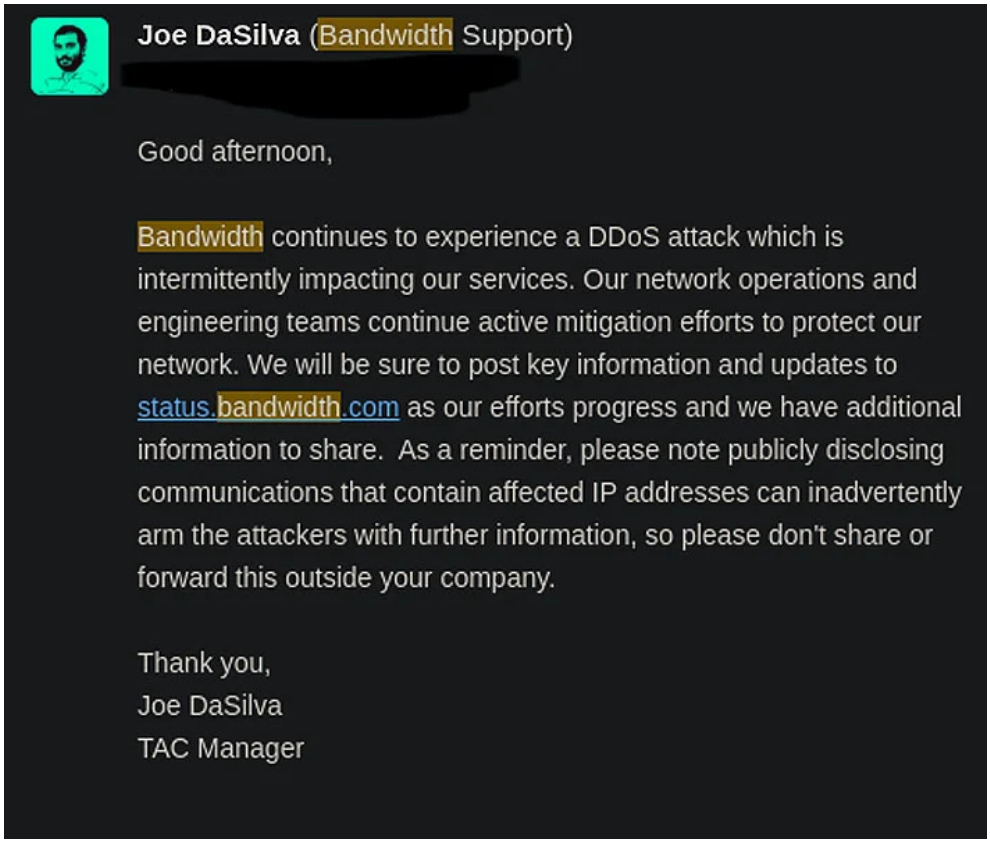
Due to this recent attack, Bandwidth customers immediately suspected that Bandwidth was also suffering from a similar DDoS attack.

As VoIP services are commonly routed over the Internet and require their servers and endpoints to be publicly accessible, they are prime targets for DDoS extortion attacks.

To conduct these DDoS attacks, threat actors will overwhelm servers, portals, and gateways by sending more requests than can be handled and thus making the targeted devices and servers inaccessible to anyone else.

Another customer shared a screenshot on Reddit of a customer support message allegedly from a Technical Assistance Center manager who states that a DDoS attack is responsible for the outages.

"Bandwidth continues to experience a DDoS attack which is intermittently impacting our services. Our network operations and engineering teams continue active mitigation efforts to protect our network," reads a screenshot shared on Reddit (https://archive.is/PmByW).



Source: Reddit

At this time, Bandwidth is reporting that their services are restored, and it is not clear if the threat actors stopped their attacks or were paid an extortion demand.

Unfortunately, it is common for threat actors to briefly halt attacks while they push extortion attempts, so we will not know for sure if the DDoS attack is over until tomorrow.

When we hear back from Bandwidth, we will update our story.

This is a developing story.