Consolidated High School District 230 **Enhances Security with Comcast Business DDoS Mitigation**

COMCAST BUSINESS
BEYOND FAST

Proactive Network Protection Critical for Digital Learning Environment

Elementary, middle and high schools are increasingly reliant on network connected technologies and cloud-based applications to foster modern teaching and learning experiences. From back of house school operations to in the classroom lesson plans, smart devices and internet access play a pivotal role in day to day operations and student engagement.

At Consolidated High School District 230 in south suburban Chicago, three high schools and an administration building form a campus at the frontier of education's technology revolution. All of the more than 8,300 students are provided laptops, facilitating a new era of digital learning and 1 to 1 teaching in every classroom. The over 1,000 faculty and staff are also harnessing technology to support the district's primary mission to cultivate successful schools and successful students.

Innovation as Catalyst for New Threat Vectors

In response to digital transformation trends, District 230 had already begun to address new realities that made network management more complex. Their Wi-Fi network required 3 SSIDs to manage guest, student and private needs with different levels of access permissions, paths to the internet and rate limits for each. Their ecosystem of cloud apps and integrated systems required a great deal of attention to both troubleshoot performance issues and also stay on top of user management.

While the adoption of new technologies had generally brought great benefits to students, teachers and staff, they also expanded the attack surface – a problem top of mind for security professionals in all industries.

"We have seen that DDoS attacks are increasingly commonplace among our peers in education," said Marce Gonzalez, Network Operations Manager for District 230. "Our campus has been the target of more than a dozen attacks in the last four years," said Gonzalez, "and we have come to view as a matter of when vs if the next attack will occur."

These types of attacks can be crippling for schools. Without access to network services, not only does learning stop but important systems and processes for state and federal compliance are jeopardized.

Proactive Solution to Unpredictable Threat

District 230 had experience with other mitigation solutions but was dissatisfied with the significant performance issues caused by requiring network traffic to be directed via a virtual private network to a vendor's scrubbing sites before delivery at the intended destination. In speaking about the switch to Comcast, Gonzalez highlighted, "because of its unique design, there is no latency with the Comcast solution."

D230 was already working with Comcast Business to upgrade their Ethernet Dedicated Internet circuits at each building. The Comcast Business DDoS Mitigation solution, a cloud-based and subscription solution that requires no hardware installation or on-premise management, was easily implemented to compliment the district's multiple 600 Mbps and 1 Gbps Ethernet connections across their campus.

The Comcast Business DDoS Mitigation Service alerts the customer when an attack occurs and helps protect against volumetric or flood, State/TCP Exhaustion, and application layer attacks. Customers also have access to a portal that shows historical activity and attack information.

Situation

- Consolidated High School District 230 in Orland Park, Ill. with three high schools
- More than 8,300 students each with laptops and personal devices
- First-hand experience confronting rising trend of DDoS attacks in education

Challenge

- Increasing reliance on cloud-based systems and applications to manage day-to-day operations
- Growing ecosystem of integrated systems and tools
- DDoS and security attacks on the rise

Solution

- Comcast Business DDoS Mitigation Service
- Comcast Business Ethernet Dedicated Internet (EDI)

Results

- Proactive threat monitoring, detection and mitigation
- Easy to manage solution with no on-premise equipment
- Automated notifications and event information via convenient portal

In speaking of the persistent threat, Gonzalez commented, “We found that attacks were being triggered from inside our network.” He added, “Kids can be creative with technology - our first attack came around finals and shut the school down. Some motives are experimental, or bragging rights, and some more malicious. As we have gotten more sophisticated in our response and tracing the source of the threat, we have had instances where attacks were initiated from within the classroom.”

The tools to carry out a denial-of-service attack are readily available on the Internet. There are also underground communities offering DDoS-for-hire services at relatively low costs. Comcast Business has helped mitigate multiple DDoS attacks on District 230. During an attack, the solution:

1. Detects the DDoS attack fingerprint
2. Drops or rate limits layer 3 and 4 malicious traffic at the edge
3. BGP routes layer 7 traffic to multivendor scrubbing centers
4. Passes clean traffic through a secure tunnel

“I logged into the Comcast Business portal recently and saw that we had another routine attack, but thanks to the Comcast Business DDoS Mitigation Service, our schools didn’t even notice it,” Gonzalez said.

“We have seen that DDoS attacks are increasingly commonplace among our peers in education.”

- Marce Gonzalez
Network Operations Manager
District 230