

A private K-12 academy addresses network security issues to defend against DDoS attacks

Schools can fight off increase in malicious network attacks by partnering with Spectrum Enterprise

During the worst days of the pandemic, most schools in the United States had to take a crash course in delivering education remotely. Even for the schools best-positioned to respond in this crisis, there were some unanticipated problems.

At one private K-12 academy, the problem wasn't that the students and the school lacked the resources to execute the forced remote learning experiment. The problem was that one of the kids had learned how to use the internet in ways the school did not expect, and figured out a way to shut down instruction completely.

The student learned how to schedule and launch Distributed Denial of Service (DDoS) attacks that crippled the school's network and infrastructure, shutting down all instruction, as well as back-office functions like billing, payroll and cafeteria fees. Using easily found and inexpensive scheduled DDoS attacks from a seemingly legitimate web site, and advice from group chats, he could shut down the school whenever he felt like it. And he felt like it for about 160 instructional hours in the spring semester of 2021.

DDoS is a type of malicious attack that overwhelms a network with a massive flood of requests. In 2020, the NETSCOUT Threat Intelligence report counted 4.83 million DDoS attacks in the first half of the year.

The attacks became even more prevalent in 2021, with NETSCOUT reporting an 11 percent increase over the same time period in 2020.¹

The school eventually partnered with Spectrum Enterprise and they have not lost one minute to a malicious attack since then.

The local provider just didn't have the tools to help

At first, the school thought they were just experiencing hardware troubles. Their network had crashed before, as a result of internal wiring issues. But this was different. The school director of information systems explains, "In May, when we began to return students to the classroom, it started hitting us the hardest. At 8:20 AM our internet circuit went down, then it was up after the end of the school day."

The school uses Google Meet for remote learning, as well as for many aspects of in-person classroom instruction. "If a teacher can't connect to Google Meet, they can't start the class, and they can't show the video or use online textbooks," he says. "Further, we can't do billing. We can't do payroll. We can't do anything."

The school had a local provider for internet access. However, they just didn't have the tools or the capabilities to track down the cause of the outages. "The engineers could only work with tools they had,"



A K-12 academy partnered with Spectrum Enterprise and added layers of security to protect its network.

Client profile

Client

Private K-12 academy

Industry

Education

Services

DDoS Protection
Fiber Internet Access

Overview

- As pandemic conditions were easing up earlier in 2021, a K-12 academy decided to return to in-person instruction, after spending months in a virtual learning environment. That's when the DDoS attacks began.
- The K-12 school lost nearly 160 hours of instructional time during these attacks.

Outcomes

- Spectrum Enterprise installed Fiber Internet Access and DDoS Protection.
- When a DDoS attack is attempted, traffic is now routed to a Spectrum Enterprise cloud-based scrubbing center. Malicious traffic is mitigated and legitimate traffic returns to its original route and intended destination.

Why it matters

- The school has not experienced any network downtime since the installation.
- IT resources spent battling the attacks can now be directed towards ongoing improvements in education and educationally relevant technology.



A student had learned how to schedule and launch DDoS attacks that crippled the school's network and technology infrastructure.

he explains. "They did replace their equipment, but the circuit we had with them, they just didn't have any tools on it to really help, really troubleshoot. So they pointed fingers at us, and we pointed fingers at them. Nothing happened, and the DDoS attacks continued."

"It was not a monitored circuit like we have now with Spectrum Enterprise, and so they pointed fingers at us, and we pointed fingers at them. Nothing happened, and the DDoS attacks continued."

—Director of Information Services

Finding the real problem

Eventually, having ruled out internal issues, the two-man IT team at the school knew that it had to be malicious attacks causing the

outages. The team reached out to faculty and asked them to keep their eyes out for any suspicious behaviors.

The request paid off. "A teacher told us that every morning when this one kid opened his Chromebook, the network went down." As it turned out, the culprit was a 12-year-old boy in the school's 9th grade. When the school was fully remote, the student was unsupervised at home. When the school came back to full in-person learning, that was when the malicious attacks really began to ramp up.

"The downside to doing instruction online is that students can't be fully monitored," he explains. "So, when you have a student of a certain skill level suddenly turning in straight A work, with perfect grammar, teachers will notice. When he came back into school full-time, he didn't have the tools that he was using to cheat at home and his grades plummeted. So, he decided to start his DDoS attacks during class time, especially during test times."

The director of information systems used an existing service the school had to determine how the boy was



The school has not experienced any network downtime since the installation of Fiber Internet Access with DDoS Protection.

pulling off the attacks. “We have a subscription service that we use to filter, block and manage over a thousand Chromebooks across the facilities at all grade levels. We noticed he was hitting a site that operated under the guise of a legitimate service that provided attacks against IP addresses in order for IT professionals to stress test their networks. So we paid \$10 to that site for a DDoS attack to last for about 10 seconds. Within minutes, we were able to push a DDoS attack towards our public IP address,” he explains.

That’s when he called a local IT consulting firm. And then the IT firm called Spectrum Enterprise.

Looking forward to no drama

The IT consultants recommended Fiber Internet Access (FIA) with DDoS Protection from Spectrum Enterprise. In July, the director of information systems was given the green light by the school’s board to make the purchases. Before the teachers came back from summer break in mid-August, the solution was up and running. The Spectrum Enterprise team went all in, and delivered two days before the requested deadline date. The school was impressed with

the planning and installation prowess shown by the Spectrum Enterprise team. “They had their installers come through ahead of time. We talked about it, walked through the path. Everything was planned out well, and the two days they were able to shave off the whole process were invaluable.”

“Now, we have FIA from Spectrum Enterprise with a 99.9 percent availability SLA. They’re monitoring our circuit, we know they’re going to reach out to us if they see traffic problems,” he explains. “So far, so good. We haven’t had any successful new attacks. That makes me very happy, because I just wanted a year of no drama.”

“We talked about it, walked through the path. Everything was planned out well, and the two days they were able to shave off the whole process were invaluable.”

—Director of Information Services

The solution allows the director of information systems to focus on other critical aspects of his job. “What I really enjoy is introducing educationally relevant technology, so our teachers will have more teaching tools and resources. Now that I don’t have to spend anywhere near the amount of time I used to looking at our network performance, firewall logs and utilization, I can focus more time on that,” he explains.

1. Netscout, “Issue 7: Findings From 1H 2021 NETSCOUT Threat Intelligence Report,” (Netscout, 2021) <https://www.netscout.com/threatreport>

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America’s largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice. ©2021 Charter Communications. All rights reserved.