DDoS Attacks Are Already Creating Chaos While Schools and Universities Are Reopening During the Pandemic

It is that time of year, where students of all ages are heading back to school. What's different? COVID-19! Teachers, school administrators and support staff are busy implementing plans to open schools and universities, but this year, they are specifically focused on keeping students safe and healthy in this extraordinary time. To accomplish this, many of the opening plans require some students to remain at home or in dorms at least half the time and attend classes virtually. This requirement alone will vastly increase the overall traffic that will be flowing through a school's network which in turn increases opportunities for bad actors to attack those schools systems' networks to bring them down.

Hard at work behind the scenes are the computers, servers, and infrastructure that support all of the applications that our teachers, administrators, and students depend on throughout the school year. The connectivity and availability of these resources, especially with the students learning from home and the corresponding increase in traffic and potential outages, will prove a critical focus point as the year goes on with the pandemic requirements in place.

Challenge

DDoS attacks are one of the widest ranging threats to an educational institution's information infrastructure. These attacks are very common on the networks of our colleges and universities and are increasingly being seen at high schools across America. Now, with the onset of the pandemic, the increased network traffic due to virtual classroom requirements and VPN usage, these DDoS attacks can have an even greater effect on operations at our educational institutions.

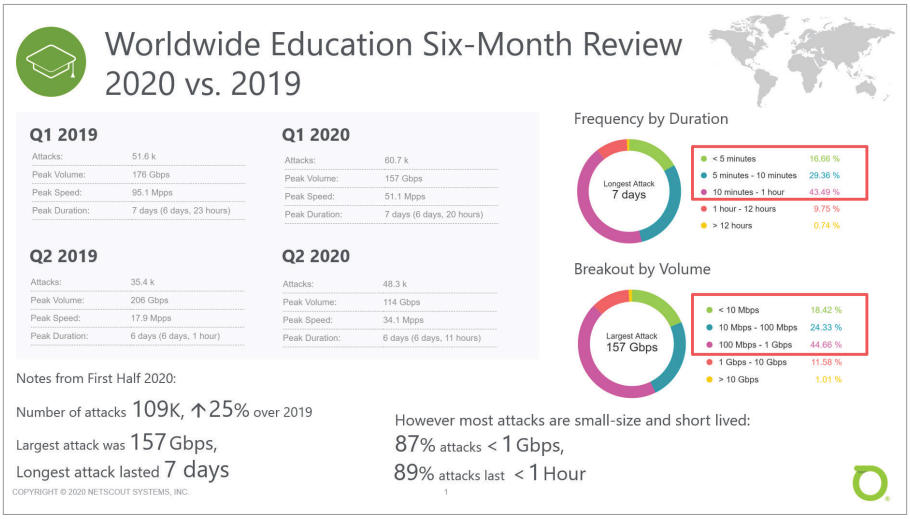
DDoS attacks are attacks against availability – often targeting both network infrastructure connectivity and overall capacity. Network connectivity represents the physical infrastructure of the network itself and how it is interconnected (e.g. routers, switches, firewalls, etc.), while capacity represents the network's ability to reliably present services to users. Connectivity combined with capacity allows for service availability. Impacts to availability can happen when the infrastructure is negatively affected (e.g. a device crashes), or when the capacity of the infrastructure itself is exceeded. Both of these circumstances can happen normally, but can be made to happen at-will through targeted DDoS attacks.

A typical a DDoS attack scenario is when cyber criminals or students overwhelm a network with hundreds of thousands of unnecessary requests or traffic from a multitude and variety of sources, preventing legitimate application requests from being fulfilled and rendering the network, its services and applications unavailable.

Over the past year the NETSCOUT® ASERT (ATLAS® Security Engineering & Response Team) six-month review of worldwide education networks for DDoS activity showed an increase of 25% over 2019, so far.

HIGHLIGHTS

- DDoS Attacks are Increasing During School Re openings During COVID-19 at Both Universities and High Schools
- Students and Bad Actors Can Both Be Identified Perpetrators
- Federal Funding Can Be Attained for Education Technology While DDoS Mitigation Technology Falls to System Administrators Through Reallocation of Funds Covered by Federal Funding
- Best Practice Mitigation Methodology is Considered to be a Hybrid Multiple Technology Approach



Details

Today many educational institutions are using older networks and legacy hardware and software systems that make it easy to hack. And, unlike corporations with trade secrets and data to protect, many school districts have set up systems to make connectivity even easier. By providing free Wi-Fi in school buildings, these institutions are presenting thousands of opportunities for a hacker to gain access to a school network. The NETSCOUT Threat Intelligence Report, "Global Threat Landscape" for the last half of 2019 says "The frequency of attacks grew by 41 percent in the education sector. The "max" DDoS attack size jumped 58 percent for technical and trade schools specifically and six percent for colleges and universities." DDoS attacks of this magnitude consume all server resources from typical website users.

Students have historically been perpetrators of DDoS attacks on educational system networks. In fact, one of the first DDoS attacks on record was executed by a 15-year-old boy who used the online name "Mafiaboy," and launched one of the first recorded DDoS attacks. This attack occurred In 2000, when Michael Calce (Mafiaboy) hacked into the computer networks of a number of universities and then used their servers to operate a DDoS attack that crashed several major websites, including CNN, E-Trade, eBay, and Yahoo. Student motivation has generally been focused on taking down a server during exams where a student had not prepared or to see and potentially change grades or to show off for classmates.

This is what you need to protect against.

https://www.nbcmiami.com/news/local/student-arrested-in-connection-with-cyber-attacks-on-miami-dade-public-schools/2287613/

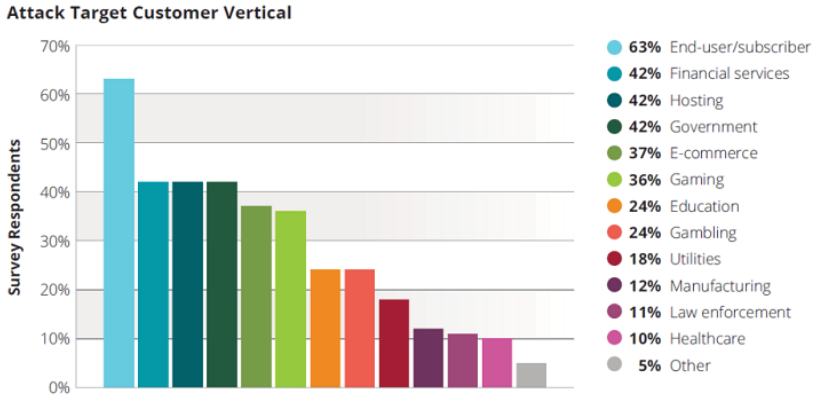


Figure 17 *Source: Arbor Networks, Inc.*

For each month from January to June 2020, the number of DDoS attacks affecting educational online resources increased by at least 350% when compared to the corresponding months in 2019.

https://www.intelligentcio.com/africa/2020/09/15/ddos-attacks-against-educational-resources-increased-by-more-than-350-says-kaspersky

Outside actors use the ease of access to educational institutions networks for more nefarious activities and to leverage items of value on those networks for their activities. A majority of hackers use the easy education network access to commandeer a variety of devices on the network including IoT devices and users personal machines to build Botnet armies to generate DDoS attacks on other targets around the globe. This trend continues today and with the increase in network traffic due to the pandemic, is more intrusive and will cause more damage at our schools and universities.

For example, in Humble, TX., on the first day of virtual learning for the 2020 school year they encountered a DDoS attack. "It was a rough start to the school year at Humble ISD, when the school district's online learning system stopped working. The district launched the school year with all students doing virtual learning to avoid spreading COVID-19. Humble ISD officials say they were hit with a "Distributed Denial of Service" attack around 8 a.m., preventing the students and staff who were actually trying to access their school material from doing so."

In New Palestine, IN., they were enduring a DDoS attack on the school district's internet network which prevented remote learning for two days during the first week of the 2020 school year. "To be unable to offer that right out of the gate is frustrating, especially frustrating knowing that this was a malicious attack on our system and not something of our own doing," said Wes Anderson, CSC Southern Hancock County director of school and community relations.

In Hudson, TX., the ISD's website was down throughout the weekend and Monday during the first week of the 2020 school year after a distributed denial of service (DDoS) attack affected the website's host. "The Hudson ISD website is hosted remotely by a third party, Gabbart, in the AWS cloud," Superintendent Donny Webb said. "The sites hosted by our vendor have been under attack with DDoS causing them to be unavailable. The attacks were off and on for about a week increasing in size, he said.

Funding

Defending against DDoS attacks for educational institutions is usually a mix of solutions or layers of protection spanning the implementation of good network practices to employing third-party purpose-built mitigation software and hardware. These choices are typically driven by budgets since some options are budget friendly and others will cost a great deal more. For many educational institutions during this pandemic, budgets are tight as they will use a majority of their resources to implement reopening plans. The CARES Act (Coronavirus Aid, Relief, and Economic Security) enacted by Congress which allocated roughly $13 billion in the spring provides schools with several different options to spend the money. Educational technology is on that list, and many district IT leaders are expecting to ramp up spending on technology acquisitions, specifically devices and digital curricula to facilitate remote learning and connectivity. Unfortunately, the requirements do not spell out that these funds can be used to secure the availability of the network which is providing the pathway for remote learning.

Another source of funding is the Federal Communications Commission's E-Rate program that covers broadband access at home for students and teachers. In March, the FCC eased its rules for the E-Rate program to allow ed-tech vendors new flexibility to provide schools with improved broadband access. However, most IT Leaders said the federal program that provides discounts to help U.S. schools and libraries improve internet access should also cover home Wi-Fi access for students that need it, to meet the remote-learning needs created by COVID-19. Beside connectivity, IT Leaders identified cybersecurity, mobile devices, and online learning platforms as their next most pressing needs.

Federal funding programs designed to assist with COVID-19 preparations and beyond are rightly focused on connectivity to ensure that every student or teacher working from home has access through broadband or Wi-Fi to the required resources. Protecting the availability of those resources, however, is not an area of focus for this funding so it falls to the IT managers to find the funds. The trend is to use the Federal money to fund the connectivity requirements and reallocate any funds in the budget that were already aimed at the connectivity needed to protect the availability of the network.

Federal funding for educational technology focuses on the building blocks of connectivity to ensure that all students and teachers can participate. Network availability falls to network administrators.

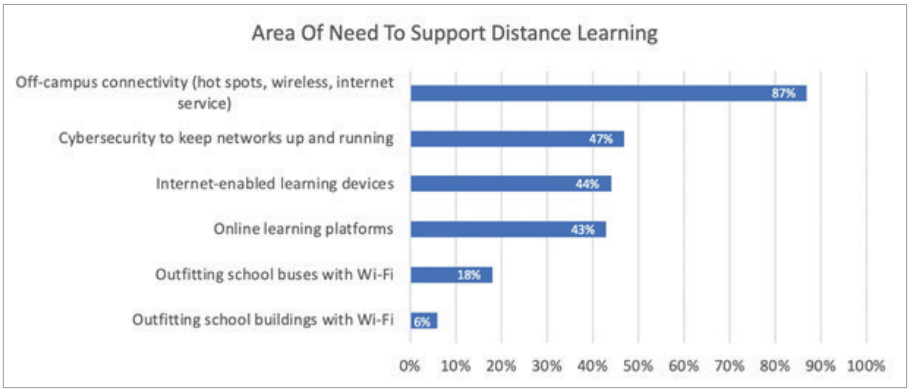


Chart Citation: Writer, D., Rauf, D.[1]

Mitigation

All of the options that protect availability of important educational resources from DDoS attacks can help incrementally, but a hybrid approach of using multiple solutions based on your infrastructure and architecture that has been implemented and deployed by experts in the field, is considered a best practice.

A basic level of protection is to employ sound strategies in the areas of Basic Network Security through user training, implementing a Secure Network Architecture using redundant servers in different geographic locations with automated failover and Securing your Network Infrastructure.

Once the basics are applied, real DDoS mitigation begins with purpose-built DDoS mitigation software or appliances. Many ISPs have this type of software protecting their networks and have services to protect their customers networks. Schools should reach out to their ISPs to see if they offer this service.

For larger educational networks who want to manage their network availability and DDoS mitigations in house, Sightline With Threat Mitigation System (TMS) sitting on the network and employing current infrastructure, (routers and switches) provides traffic visibility, DDoS identification and mitigation that scales.

For smaller institutions Arbor Edge Defense (AED) sits at the edge of the network and provides DDoS identification and mitigation before the traffic enters your network infrastructure.

Another option is to employ an on-demand or always-on cloud scrubbing service like Arbor Cloud to attend to your DDoS Mitigation needs. The Arbor Cloud service can also be used to augment your on-premise mitigation services allowing you to scale your DDoS resilience as needed.

ARBOR PRODUCTS

Arbor Cloud DDoS Protection Products and Services

- A fully managed, tightly integrated combination of in-cloud and on-premise DDoS protection.

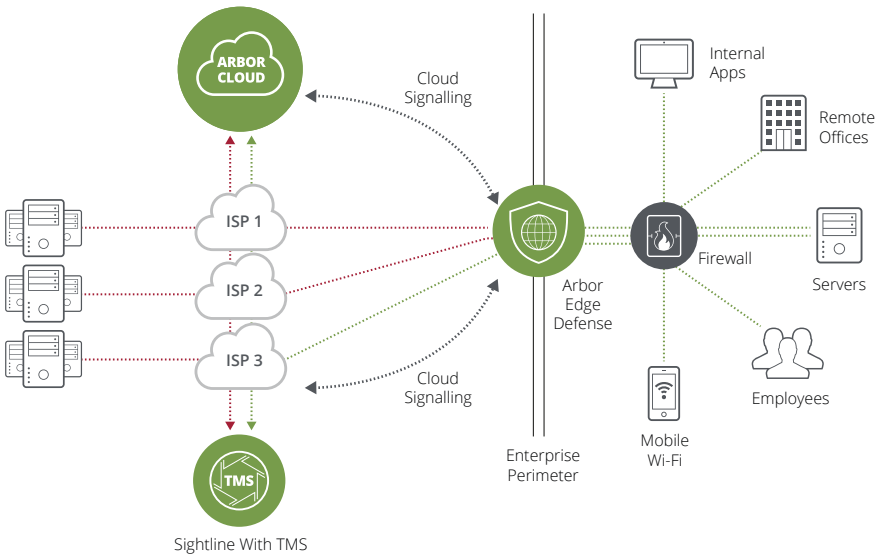
NETSCOUT Arbor Edge Defense

- Always on, in-line, detection and mitigation of DDoS attacks ranging from sub 100 Mbps to 40 Gbps.
- Can stop inbound and outbound DDoS attacks, malware, and C2 communication.

Arbor Sightline + Threat Mitigation System (TMS)

- Arbor Sightline provides pervasive network visibility and DDoS attack detection.
- Arbor TMS provides out-of-path, stateless, surgical mitigation of DDoS attacks as large as 400 Gbps. ATLAS Intelligence Feed (AIF) provides global visibility and threat intelligence continually arming all products and services.

[1] Writer, D., Rauf, D. is a contributing writer with EdWeek Market Brief. (2020, June 26). E-mail drauf@educationweek.org School Districts Banking on CARES Act to Help With Tech Purchases for the Fall. Retrieved September 11, 2020, from https://marketbrief.edweek.org/marketplace-k-12/school-districts-banking-cares-act-help-tech-purchases-fall/



All of these are appropriate forms of DDoS identification and mitigation, however the most effective solution for your network will depend on your specific network architecture and the level of expertise you have in-house. Effective DDoS mitigation and network availability management expertise is the most crucial part of the equation. Arbor Managed Services can provide that you with trained experts who can recommend, implement and manage your solution.

DDoS Attacks and resource unavailability in educational institutions will be the norm for the foreseeable future for three reasons. One is the ease of access due to the connectivity mission of schools combined with the additional network traffic and expanded threat surface from students learning at home. Second is the potential cache of valuable information that can be attained from the systems that universities and schools are required to run. And third is the lure of the variety and volume of devices connected to these networks that can be employed for unpleasant activities. Understanding this should be the impetus behind analyzing what your institution currently has in place to stop the potential attacks, what you need to protect and what you may be missing. The most important factor to analyze is if you have the expertise to implement an effective strategy or do you need to find that expertise.

Recently, attackers have been using the threat of DDoS attacks in extortion scenarios. These attacks have been targeting banks, stock exchanges, travel agencies and currency exchanges. Education institutions will not be far behind.

As is the case with most DDoS attacks, organizations which have adequately prepared to defend their public-facing infrastructure have experienced little or no significant negative impact related to this DDoS extortion campaign.

https://www.netscout.com/blog/asert/high-profile-ddos-extortion-attacks-september-2020

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECSB_027_EN-2001 09/2020