The DDoS Threat to K-12 Schools

How to Protect Your District from Becoming a Target

Like any other institution or business, K-12 school districts depend on technology to run their operations. On-premise digital assets and mobile devices have played a central role in modernizing education. Unfortunately, there is a downside. Reliance on technology makes K-12 districts a tempting target for cybercrimes, including Distributed Denial of Service (DDoS) attacks.

13% of Education Institutions Experience Ransomware[1]

Education has surpassed healthcare as the most targeted vertical (or sector) by ransomware. Many ransomware attacks occur through email, phising and network vulnerabilities.

The IoT Effect

Worldwide spending on the Internet of Things (IOT) is forecasted to reach **$772.5 billion** in 2018. Software spending will be led by application software along with analytics software, IoT platforms, and security software. Software will also be the fastest growing technology segment with a five-year CAGR of 16.1%.[2]

IDC forecasts worldwide IoT spending to sustain a compound annual growth rate (CAGR) of 14.4% through the 2017-2021 forecast period surpassing the $1 trillion mark in 2020 and reaching $1.1 trillion in 2021.[2]

$772.5 Billion $1 Trillion $1.1 Trillion

IoT Spending
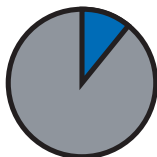
2018   2020   2021
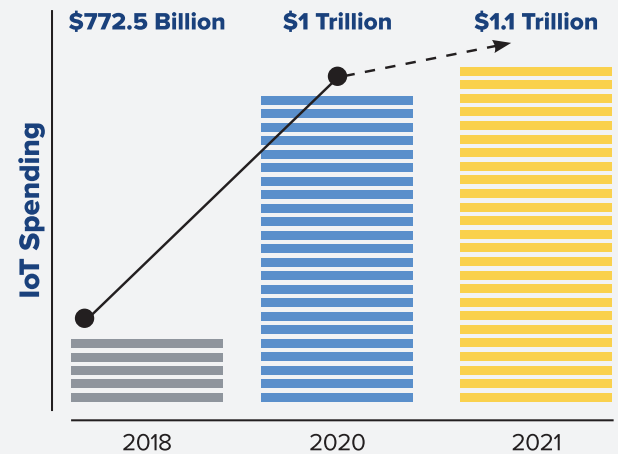
DDoS By the Numbers

The U.S. is the **most** targeted country for DDoS attacks.[3]

1.7Tbps was the **largest attack** in the U.S. to date.[4]

1.8 million DDoS attacks occured in 2017.[5]

DDoS attacks in the U.S. **increased to 23.3%** of the worldwide total in 2017.[6]

30% of DDOS attacks originated from U.S. IP Addresses.[7]

US receives a cyber attack on average **every 3.5 minutes**.[8]

What Makes K-12 Schools an Attractive Target?

Cybercriminals have some favorite targets – healthcare, financial services, retail – but they aren't terribly discriminating when the opportunity arises to disrupt network operations. **Currently, education accounts for roughly a quarter (24 percent)[9] of all DDoS attacks.**

Here's why K-12 and other educational institutions make such an attractive target:

1 School districts rely more and more on **digital networks**.

2 **The increasing volume of traffic** flowing through those networks makes them an attractive target because it also increases the potential for damage.

3 **School districts tend to operate on tight budgets.** Often they lack the same resources as deep-pocket corporations to defend themselves.

4 **Students with a grudge** – or trying to fix a grade or delay an exam – are often behind DDoS attacks.

5 **Schools keep high-value data,** both on students and employees, including Social Security numbers, medical records and other private data.

Attacks on School Districts

The possibility of DDoS attacks against schools is more than academic. It's reality, and has happened multiple times:

- Doug Levin, president and founder of EdTech strategies, has identified more than 330 incidents based on news reports alone.[10]
- Mass school district pays $10K ransom demand after school was hit with ransomware.[11]
- 50,000 student and teacher records exposed at Leon County Schools in Tallahasee, FL.[12]
- Whittier Union High School District was compromised forcing all students to change their passwords for the student information system.[13]
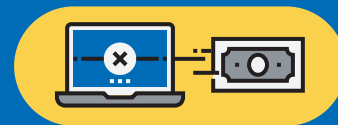
Protect Your Schools

School districts need protection against DDoS attacks. To prevent interruptions to the learning process caused by DDoS attacks, school districts should take advantage of subscription-based services that proactively detect DDoS attacks, alert them when an attack has started, and takes mitigation measures to prevent downtime and foil the attackers. As schools become more and more dependent on technology, DDoS protection is a must. The education of our children is at stake.

Ransomware Too?

Making matters worse, cybercriminals have started to combine ransomware tactics with DDoS.[14] In what is being dubbed as "ransom DDoS" or "RDoS," perpetrators send the target a message demanding payment in bitcoin and threatening to deliver a DDoS attack if the victim refuses to pay. Short-term attacks sometimes accompany the message as a preview of larger action. These attacks so far focus on business, but education is a possible future target.

Sources:

1   https://thejournal.com/articles/2016/09/22/education-sector-now-most-targeted-with-ransomware.aspx
2   https://www.idc.com/getdoc.jsp?containerId=prUS43295217
3   www.statista.com/chart/8281/us-top-source-of-ddos-attacks-in-q4-2016/
4   www.itpro.co.uk/distributed-denial-of-service-ddos/30695/us-firm-fends-off-the-largest-ddos-attack-ever-recorded
5   Arbor Networks
6   Arbor Networks
7   https://www.statista.com/statistics/440582/ddos-attack-traffic-by-originating-country/
8   http://resources.arbornetworks.com/wp-content/uploads/ARBOR_ATLAS_2017Overview_Infographic.pdf
9   www.netscout.com/news/blog/ddos-attacks-school
10 www.scmagazine.com/home/news/government-defense/cyberattack-map-shows-impacted-u-s-school-districts/
11 www.scmagazine.com/home/news/ransomware/massachusetts-school-district-caves-to-ransomware-demand-pays-10000/
12 www.scmagazine.com/home/news/data-breach/breaches-expose-50000-student-and-teacher-records-at-leon-county-schools-more-districts-likely-affected/
13 https://k12cybersecure.com/map/
14 https://securelist.com/ddos-attacks-in-q2-2017/79241/