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

Education has surpassed healthcare as the most targeted vertical (or sector) by ransomware. Many ransomware attacks occur through email, phishing 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%.

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.

DDoS By the Numbers

The U.S. is the most targeted country for DDoS attacks.

1.7Tbps was the largest attack in the U.S. to date.

1.8 million DDoS attacks occurred in 2017.

US receives a cyber attack on average every 3.5 minutes.

DDoS attacks in the U.S. increased to 23.3% of the worldwide total in 2017.

30% of DDoS attacks originated from U.S. IP Addresses.
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.

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.

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.

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.

Sources:
5. Arbor Networks
6. Arbor Networks
13. https://k12cybersecure.com/map/