Securing Education's Digital Transformation

The Changing Stakes of Network Security

The digital transformation of education has changed the stakes for security teams. Protecting the networks that support the modern educational institution has become both mission critical and more challenging. And cyber attackers are taking note:

- "The education sector was the industry most affected by Mirai variants during Q3 of 2017, ahead of energy, manufacturing, entertainment, and financial services, according to figures from SecurityScorecard."[1]
- According to 2017 BitSight report 1 in 10 education organizations experienced ransomware on their networks, twice that of Government and almost four times more than Healthcare.[2]
- UK university networks were subject to more than 1,152 recorded intrusions in 2016-17. The number of recorded attacks has doubled in two years.[3]

Educational institutions are unique in that they try to maintain, as much as possible, an open environment with broad external access for the sharing of information. Yet new digital learning tools and student information systems on more platforms, increasing social media connections, extended wifi networks and 1-to-1 or BYOD initia-tives all increase the risk of cyberattack. On top of this, the data processed in recruitment, alumni relations, finance and HR systems – not to mention research – have become more valuable to cybercriminals.

Normal operations can be crippled by Distributed Denial of Service (DDoS) attacks on student services, online testing, or application processes. But DDoS attacks can also aid and abet phishing campaigns, the theft of valuable data, inject ransomware, and cover illicit access to connected systems.

The Weaponization of IoT for Modern-Day DDoS Attack

Sophisticated malware and the exploitation of the Internet of Things (IoT) botnets has resulted in the virtual weaponization of these devices for DDoS attacks. In 2016 LizardStressor malware running on an IoT botnet of 10,000 IoT devices (primarily webcams), generated sustained attacks of over 540Gbps. The Mirai botnet, designed specifically to infect IoT devices, and released 'into the wild' last year, is estimated to have compromised more than half a million IoT devices worldwide and generated attacks in excess of 620Gbps. But run-of-the-mill volumetric attacks are not the only threats from the new breed of botnets. Both of these botnets can launch the equivalent of the modern-day DDoS attack.

The modern-day DDoS attack is frequently a dynamic combination of volumetric, TCP state exhaustion and application layer attack vectors. Volumetric attacks are designed to saturate internet facing circuits. TCP-State exhaustion attacks can target the very defenses, firewalls and IPS, intended to protect against cyber-attack.

INDUSTRY

Education

Challenges

- As education organizations pursue digital transformation they increase threat surfaces and network vulnerability.
- IoT-based botnets are increasingly being used to launch large and complex DDoS attacks – and educational institutions are tempting targets.
- The attackers' aims go beyond network availability to include ransomware, theft of valuable personal data and access to connected systems.
- Misconceptions linger and current protections struggle with increasingly sophisticated DDoS attacks.

Solution

- Arbor's fully managed, intelligently automated, in-cloud and on-premises DDoS protection solutions provide comprehensive protection from modern day DDoS attacks – so you can maintain service availability.
- Leverage Arbor's ATLAS Intelligence Feed to arm all Arbor solutions with global threat intelligence.

[1] theregister.co.uk/2017/11/07/mirai_botnet_sitrep/

[2] forbes.com/sites/kevinmurnane/2016/09/21/its-not-only-about-healthcare-bitsight-reports-ransomware-has-infected-many-industries/#420222e858a3

[3] bbc.com/news/technology-41160385

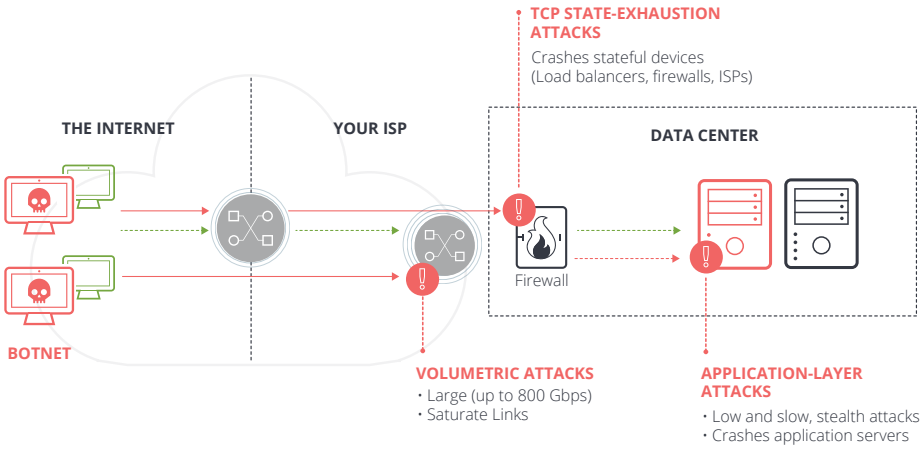

Figure 1: The modern-day DDoS attack is multi-vector.

According to NETSCOUT Arbor's 13th Annual *Worldwide Infrastructure Security Report* (WISR 2018), 48% of respondents an experienced a multi-vector DDoS attack. That's up 20% from prior year. Arbor's WISR also noted a 30% increase in the number of application-layer DDoS attacks. A 'low and slow' application layer attack presents just as much risk as an 800 Gbps volumetric attack. To be effective a DDoS attack only has to saturate the bandwidth of your internet connection.

Making matters worse, sophisticated DDoS botnets now conduct massive phishing operations, deliver ransomware, or help gain entry to other, connected systems. They can be used as cover for multi-part, long-running attack campaigns targeting valuable information.

DDoS attacks have, and continue to evolve concurrent with the digital transformation of education. Security teams face a challenging truth: the open, interconnected systems essential to operating today's educational institution brings more risk.

In 2017, DDoS was used to help penetrate the networks of four Miami-Dade school district networks. Their goal was to find their way into government organizations, "...for some way to slip into other sensitive government systems, including state voting systems."

Reassessing Your Risk from a DDoS Attack

Common misconceptions about what constitutes effective DDoS protection plague proper risk analysis. For example:

- Firewalls, load balancers, WAFs and IPS are not designed to protect against all DDoS attacks. These stateful devices are themselves vulnerable to TCP state exhaustion DDoS attacks – and routinely fail during attacks. According to NETSCOUT Arbor's 13th annual WISR 51% of Enterprises reported their firewalls/IPS failing during a DDoS attack.
- Most on-premises protection can be easily saturated given DDoS attack techniques such as reflection/amplification or IoT botnets for hire. Even though 88% of attacks are less than 2 Gbps, these can still overwhelm most internet circuits.
- ISPs are best positioned to stop large volumetric DDoS attacks – but they struggle to detect smaller, application layer attacks. 74% of attacks last for less than 30 minutes. Automation is vital for effective on-premises protection.

Now is the time for educational institutions to reassess their risk of DDoS attacks and re-evaluate their protection strategies.

The Florida Department of Education experienced a DDoS attack preventing students throughout the state from taking the test for three days. "...we've seen more attacks the past few years than we ever have, and they occur during the periods of time when we are testing." Deborah Karcher, District CIO

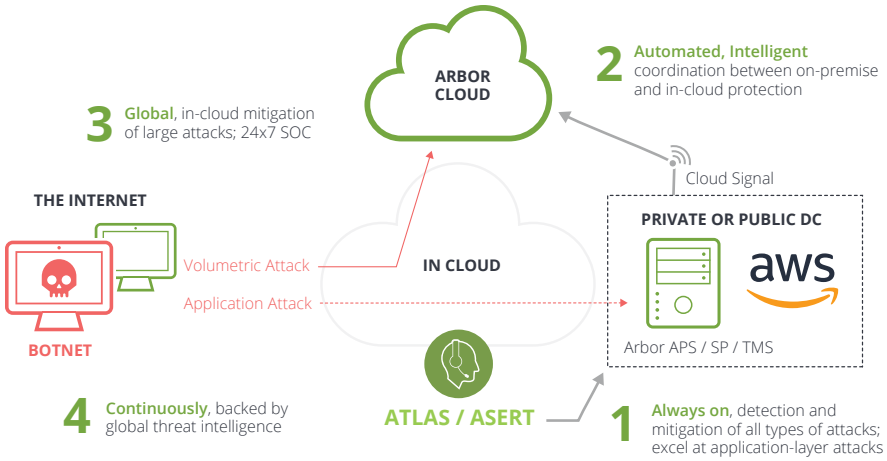

Figure 2: Unified, intelligently, automated DDoS protection products and services: armed with global visibility and actionable threat intelligence.

Protecting your Network and On-Line Requires Intelligently Automated, Layered DDoS Protection

To stop today's DDoS attack industry best practices, recommend a layered, automated protection strategy backed by continuous, timely threat intelligence.

Arbor's DDoS Protection solution offers a fully integrated, intelligently automated combination of in-cloud and on-premise DDoS attack protection products and/or services:

- Arbor APS to stop In-line, always-on, installed in private or hosted data centers (e.g., Amazon Web Services), in front of firewalls and key communication gateways; can automatically stop in-bound network, application-layer and TCP-state exhaustion attacks.
- Cloud Signaling™ to automatically and intelligently link to Arbor Cloud, in-cloud mitigation before on-premise protection and internet circuits are overwhelmed by large attacks.
- Arbor Cloud 24/7 SOC to automatically mitigate volumetric attacks upstream before on-premises gateways and security systems are overwhelmed.
- ATLAS Intelligence Feed to continuously feed all mitigation options to stay protected from the latest threats (e.g., Mirai botnet derivatives).

"DDoS attacks are a significant threat to educational institutions, representing one half of all security incidents."

The Arbor Availability Protection System (APS)

- Provides always on, in-line protection from network and application layer DDoS attacks and advanced threats.
- Provides in-bound and out-bound threat identification and mitigation.
- APS mitigation platforms and capacities range from 2U appliances (1 Gbps – 40 Gbps) to virtual machines (sub 1 Gbps).

The Arbor Cloud DDoS Protection Service

- Arbor Cloud is a fully managed DDoS protection service providing up to multi-Tbps of global protection.
- Arbor Cloud Signaling™ providesinstant, intelligent communication between on-premise Arbor APS and Arbor Cloud for comprehensive, layered, DDoS protection.
- ATLAS Intelligence Feed (AIF) continuously arms all Arbor solutions with timely, actionable, threat campaign intelligence.

Arbor ATLAS: Global Visibility and Threat Intelligence

Over the past 16 years more than 400 ISPs have participated in ATLAS, providing Global Visibility and Threat Intelligence to businesses worldwide.

Arbor's Security Engineering and Response Team (ASERT) leverages ATLAS to conduct threat research, help customers mitigate DDoS attacks and create ATLAS Intelligence Feeds (AIF). AIFs continuously arm all Arbor DDoS protection products and services.

Unique, Automated Threat Intelligence

DDoS is frequently part of larger attack campaigns that include the planning of tactics, techniques and procedures (TTPs) long before a victim is even targeted. A campaign is an ongoing set of operations, much of it automated, against well-researched targets. And adversaries frequently circle back – particularly if they have been successful.

The good news is that these techniques and tactics leave a trail. For over 16 years Arbor has had unique visibility into global threats. The ATLAS Intelligence Feed (AIF) is built on data from over 400 ISPs providing global threat intelligence. About one-third of all Internet traffic flows thru ATLAS or an Arbor product. (A current representation of some of this data came be seen on the Digital Attack Map.) ASERT security experts augment this data with additional research and historical perspective. For example, tracing the origins and trajectory of Mirai malware to better determine the 'reputation' of suspect IPs.

The AIF continuously arms all Arbor on-premise and cloud-based solutions with actionable threat intelligence. Timely and embedded AIF threat intelligence helps in the more rapid, automatic – as successful – mitigation of DDoS attacks.

New Methods of Quanitifying Risk

There are a number of risk frameworks, from NIST, ISO, CERT, ISACA, and others. While all recognize the business need to assess risk, they for the most part leave quantification up to the organization. What is clear is a compliance based approach to security is not enough. For example, you could "meet" all the NIST guidelines and still be at significant risk from DDoS or other advanced attacks.

One emerging risk analysis methodology is Factor Analysis of Information Risk (FAIR). FAIR provides for the quantitative measurement, management and communication of information risk in terms of the value to the business. A practical understanding and analysis of information risk in terms of dollars and cents can enable more well-informed business decision making. To see an example of how to conduct a FAIR-based risk analysis of DDoS attack and how different Arbor solutions can reduce the risk refer to the "Additional Resources".

No matter what framework or risk analysis methodology you use, accurate results depend on three things: 1) knowledge of the latest DDoS attacks trends (i.e., size, frequency and complexity); 2) best practices in DDoS defense (i.e., an intelligent combination of in-cloud and on-premise protection backed by continuous threat intelligence) and 3) understanding that not all assets are equal in value and will have a different risk profile.

Summary

Educational organizations continue to undergo significant digital transformation and increased vulnerability to new DDoS attacks. The risks and costs of service unavailability, a data breach, incident recovery and ransomware are greater than ever. More sophisticated tools and techniques in the hands of determined attackers means now is the time to re-evaluate the risks to your operations and assets.

Arbor's intelligently automated, fully integrated in-cloud and on-premise solutions represent the industry's most comprehensive, effective DDoS protection. Easy to deploy and use armed with campaign intelligence from ATLAS, Arbor's complete solution enables you to more efficiently protect your infrastructure and information assets – and better safeguard your institution's bottom-line.

LEARN MORE

Overview of Arbor DDoS Protection Solution
ATLAS Attack Map
FAIR White Paper

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_005_EN-1801 05/2018