

Academic Excellence: Corero's IPS protects Butler Community College networks

Summary

Industry: Education

Challenge: To protect the college networks and end users from incessant outside attacks and control device infections resulting from student practices within the firewall, while maintaining the freedom and flexibility required in a higher learning environment.

Solution: Corero's IPS

Results: Corero Network Security prevented the multitude of attacks from successfully penetrating the college's network perimeter and effectively controlled the internal.

Key Benefits

- Stops advanced threats
- Lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks, malware, spyware, viruses and botnets
- Compatible with cloud-enabled infrastructure

With its main campus in El Dorado, Kansas, and five other community locations, Butler Community College is the second largest community college in the state — and home to the Butler Grizzlies, five-time NJCAA football national champions. Home to more than 13,000 students from around the world, with another 1,200 faculty and employees serving the campus population, the College strives to provide exceptional student-centered learning environments and cultural opportunities that cultivate principled, productive and dynamic communities.

The Challenge

Butler Community College embarked on an ambitious project to deploy a new website designed to reflect the rich tradition of the school and to provide an improved interface for students, faculty and prospective attendees. The new website drew rave reviews from students and staff, and received several awards for its design and navigability. However, it also drew the interest of malicious attackers, who launched a SQL injection attack soon after the launch.

"The new web presence we launched was a strategic component of building the school's brand and recognition and was designed to serve the current campus population while drawing interest from prospective students. No sooner than we had launched, we were faced with a relatively elegant blind SQL injection attack that threatened the entire project," says Philip Pell, chief information security officer at Butler Community College.

The goal of the attack was to inject JavaScript into the website and redirect visitors to download and execute malware from servers in China. The attack was intended to create a fleet of bots out of visitors to the Butler Community College website that could then be used to attack other sites. While Pell and the web services team were able to contain the damage, he soon realized that to minimize future attacks, they needed to go through the more than 8,500 pages online and correctly validate form and API input. To allow the time to correct the code, Pell decided Butler needed a solution that could mitigate ongoing and future attacks while the work took place.

The Solution

Once the initial attack was mitigated, Pell began evaluating intrusion prevention solutions that would serve as one of the perimeter controls in a defense-in-depth security strategy. During his search, he was invited to a Corero Network Security (then Top Layer Security) "Lunch and Learn," in Kansas City, a national program designed by the company to help promote security awareness and provide solutions for the complex security issues facing all organizations.

After the session, Pell decided to include Corero's IPS in an intense bake-off with several competitors.

"[Corero's IPS] was exceptionally responsive. Getting us the demo equipment immediately, sending us a brand new box, which we were able to quickly install over a weekend," says Pell.

After the exhaustive tests were concluded, Pell concluded that Corero's IPS 5500 had something distinct in common with the Butler Grizzlies, the school's national champion football team – both performed head and shoulders above the competition

"The IPS handled all of the attacks with ease. We tested with custom, intentionally vulnerable code to see how each product would perform – it was the only solution to stop all the zero-day attacks," Pell continues. "But most of all, the ease of use in behavior matching and auto-updating stood out above the competition. After the bake-off, it was very easy to pick a winner; in technology, support and overall operational value, the IPS 5500 clearly outperformed all of the competitors. It was an easy choice."

The Results

After selecting Corero, Pell immediately deployed the solution for deep packet inspection of all network traffic and to serve as a firewall on the perimeter. Prior to installing the IPS, the school was experiencing anywhere from 60,000 to 100,000 attacks a day, from older worms such as Morris, Slammer and Sapphire, to zero-day attacks designed to grind the network to a halt. Once the IPS was brought online, all of the inbound attacks were stopped at the perimeter.

The IPS also helped Pell identify and mitigate serious vulnerabilities in the continually evolving threat landscape. Educational institutions have a unique challenge in which attacks are not coming primarily from outside the perimeter. Educational institutions have always faced a larger than average number of threats from inside the network, resulting from the actions of students and faculty.

The practice of sharing media files and downloading programs from websites is popular among students and faculty. This type of user behavior can expose the network to intrusions, worms, viruses, malware and other attacks as well as violating laws such as the Digital Millennium Copyright Act and the Higher Education Opportunity Act. Once introduced into the network, malware can lead to information disclosure or result in the degradation of network performance. Once deployed, the IPS helped Pell identify previously unknown malware attacks that were directly attributable to this type of student and faculty activity.

"We had a number of students whose computers were infected with malware and part of a bot fleet and didn't even know it. Traditionally, if you want to cut down on bots, you need to shut down access to sites and resources," declares Pell. "Because we're a college, we need to be able to protect students without getting in the way of learning in the classroom and living in the dorm room. The IPS prevents spyware and malware from coming into the network, but doesn't prevent students from getting to the sites they need. Malware site blocking has resulted in an immediate, measurable drop in service desk calls."

The zero-day protections provided by the IPS 5500 enabled Butler to free up resources to focus on web projects, and provided the breathing room necessary to stop having to fight emergency brushfires and work on projects that create value for students, faculty and staff.

Additionally, the online reporting capabilities make it easy to update senior management with real-time security status reports, addressing questions about the threat landscape. The easily digestible reports help Pell communicate complex threat information quickly, allowing the team to formulate responses more quickly.

Educational institutions live in a different environment. In most industries, you have absolute control over IT – who can access your network, what's on the machine, what sites they visit – and can knock people off the network when an issue arises. In college settings, however, academic freedom mandates that you're as open as possible.

"Students and faculty come in and have an expectation that their equipment, from iPhones to laptops, will work seamlessly in the network," says Pell. "[Corero] is the only vendor that meets the bill for what we need to accomplish without creating an onerous load on information services or unnecessary restrictions on our student and faculty population. Simply put, it works."

About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprise organizations rely on Corero to protect their critical online assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with offices worldwide. www.corero.com.

Corporate Headquarters

1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
Fax: +1.978.212.1600
www.corero.com

EMEA Headquarters

No.1 Cornhill
London
EC3V 3ND
Phone: +44 (0) 203 427 3407

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.