CASE STUDY

University of Guadalajara Proactively Protects Against DNS-Based Cyberattacks with Infoblox

Facts & Figures

- Location: Mexico
- Number of Users: Nearly 300,000
- Industry: Higher Education

Solutions

- DNS security
- Grid
- Internal DDI with BloxOne™ Threat Defense
- External DNS Protection with Advanced DNS Protection
- Reporting and Analytics run in IPv6 branches

Outcomes

- Ability to protect its nearly 300,000 users and their data across all campuses
- Improved network reliability and functionality of DNS services
- Proactively protect the entire network infrastructure against the widest range of DNS-based cyberattacks including DDoS, data exfiltration and malware C&C communications

The Customer: University of Guadalajara

Universidad de Guadalajara, or University of Guadalajara, was founded over two centuries ago in Mexico. It is the second largest university in Mexico with over 290,000 students enrolled in its 442 vocational, high school, undergraduate and graduate academic programs. The campus includes two major university centers located in the metropolitan area of Guadalajara and eight regions of Jalisco, and an office in Los Angeles, California. The university is renowned for its inclusive, flexible and innovative qualities. For example, it is one of the first universities in Latin America to obtain the IPv6 Forum accreditation, and it is currently running voice over IPv6 and web services.

The university's IT team is led by industry expert and Services Operations Coordinator Jorge Lozoya Arandia. He and his team oversee and manage the university's Security Operations Center (SOC) and Network Operations Center (NOC) and all operations of services including cybersecurity, network, infrastructure, servers, backups and more.

"Our IT team's primary objectives are to secure our DNS network-wide and to ensure that our DNS services function…With Infoblox, our team now knows if and when [our network] becomes under attack and is able to mitigate all DNS-based attacks and keep all services up and running."

Jorge Lozoya Arandia,
Services Operations Coordinator, University of Guadalajara

The Challenge

"Our IT team's primary objectives are to secure our DNS network-wide and to ensure that our DNS services function," states Arandia. The university's network has more than 10,000 devices, ERP and financial, student and faculty applications and remote learning services all running on the network simultaneously.

Managing and securing IT application controls with services running on IPv6 has been one of the university's greatest pain points. The team previously relied on the legacy BIND system to manage its network, which kept operational costs high and failed to secure the large network. This legacy solution did include a few layers of cybersecurity, but it lacked a robust DNS security solution.

Elements of a Comprehensive Cybersecurity Strategy

University of Guadalajara has a strong understanding of the nature of the evolving higher education threat landscape. The top threats that the university's IT team experiences include distributed denial of service (DDoS) attacks and insider threats. "Our network is regularly under attack from outside threats and from many devices on our network that are constantly infected. We have a lot of spam, malware and DDoS attacks", Arandia states.

DNS-Based DDoS Attacks, Insider Threats and Proliferation of IoT Devices

"DDoS attacks are among the most common types of threats that I see to our higher learning network", explains Jaime Olmos, Network Operations Center (NOC) manager at the university. DDoS, or distributed denial of service attacks are one of the most powerful weapons on the internet. They can flood DNS servers with malicious requests for example, which can bring down the entire network.

In addition to malware, the users themselves pose some of the most serious threats to the availability and security of the university's massive network. For example, students, faculty, staff and visitors can take part in malicious acts, whether accidentally or deliberately. In addition, they often fail to take reasonable security measures to protect their own sensitive data.

Furthermore, students and other users collectively bring thousands of personal and connected devices onto the university's network each year, such as smartphones, tablets, and laptops and desktop computers. The more devices that enter the university's network, the greater the potential attack surface grows and the more susceptible the network becomes to infections from malware.

Protecting DNS from the Widest Range of Attacks

In order to adapt to the evolving higher education threat landscape and to proactively prevent and protect against such threats as DDoS and other DNS-based threats, the university needed to implement a comprehensive cybersecurity solution that would automatically protect its DNS against the widest range of attacks, in particular DDoS attacks. The university now benefits from the ability to mitigate these attacks and secure its DNS. It also has a central view of attack points and patterns across the entire network, and it continuously monitors and detects DNS-based threats.

"The most important features for the university are network visibility and network availability. The university's IT team is under constant pressure to keep all services that our university's students, faculty and staff use up and running at all times." Arandia continues, "With Infoblox, the IT team now knows if and when it comes under attack and is able to mitigate all DNS-based attacks and keep all services up and running."

Proactively Detecting and Preventing DNS-based Data Exfiltration and Malware C&C Communications

Furthermore, the university is now able to improve user experience such as with internet navigation. "Infoblox and partner Initel also help our team keep users out of contact from C&C malware sites", continues Arandia. The university has not yet begun protecting its users and data from the cloud, but it is planning on demoing the cloud solution in the near future.

Enhanced Network Visibility Stops DNS-Based Attacks in Real Time

In the event of a potential breach, any type of malware poses a serious threat. That's why it's so important to maximize visibility into all devices and services running on the network. The university's IT team must be able to see precisely where threats are occurring on the network, and it must be able to detect and immediately remove all threats.

"When we spoke with the Infoblox team during our interview for this case study, our team detected a breach on our network in real time right during the call," said Alma Ruiz, lead manager of the IT team's SOC and NOC. The Infoblox infrastructure was able to provide Alma and her team real-time cyber threat intelligence data that enabled her to see the threat before it caused any damage and remove it immediately.

Conclusion

Few enterprises in the world have as many users and devices as an average higher education institution, especially University of Guadalajara. The university's IT team has a strong understanding of the threats it is faced with and of the evolving nature of its network infrastructure, and it is well prepared to keep the university's network secure and up and running at all times. Future implementation of an integrated cybersecurity ecosystem solution will help the team enhance visibility, automate processes and respond to threats faster.

For More Information

Learn more about how you can proactively detect malware and protect your users and data via DNS. Visit the Infoblox website or start your free trial of our BloxOne Threat Defense technology today.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com