Infoblox

CASE STUDY

Keio Group Protects Japan's Critical Infrastructure with BloxOne® Threat Defense

The Customer

Keio Corporation is a private railway operator in Tokyo, Japan. It is the primary firm within the Keio Group, which is comprised of 54 companies involved in transportation, real estate, retail and other industries. Kenichi Sato and Hiroko Tamura, both holding the title of Group IT Officer-in-Charge, lead the company's IT Management Department at Keio Corporation Headquarters in Tokyo. These IT and cybersecurity experts and industry veterans are tasked with managing and protecting Keio Corporation's growing network and keeping users and passengers safe wherever they are located.

The Challenge – Modernizing to Address Emerging Cyberthreats in Uncertain Times

Keio has been driving a corporate initiative to migrate to the cloud in order to modernize its evolving network and scale for rapid growth. The customer also wanted to accelerate IT system deployment, reduce costs, easily adapt to changes in the external environment and digitize the network via artificial intelligence (AI) and Internet of Things (IoT) solutions. The customer planned its initiatives with a cloud-based cybersecurity solution at the foundation.

Meeting Compliance Standards and Protecting Critical Infrastructure

The business has been planning for logistical challenges in preparation for hosting major global events. Tamura explains, "In the past several years the government has demanded that we meet the highest compliance standards in preparation for hosting the Tokyo Olympics and Paralympics." However, these global events have both been postponed until 2021, and as of May 2020 face potential cancellation. Thus, the enormity of the challenge and the intense uncertainty surrounding the trajectory of current events has put the customer's users and other critical infrastructure businesses in a uniquely risky situation.

KEIO

Company: Keio Corporation

Industry: Public Transportation, Critical Infrastructure

Location: Japan

Initiatives:

- Protect against advanced DNS-based malware threats
- Reduce costs and workloads for IT and cybersecurity teams

Outcomes:

- Simple installation and flexible deployment through a cloud-based solution
- Reliably detect and block threats that were previously difficult to detect
- Protect approximately 6,000 PCs from threats
- Scale for future growth

The Situation - Adapting to the Evolving Threat Landscape

Until recently, the company's cybersecurity strategy and launching of the Keio Security Incident Response Team (SIRT) in 2015 have sufficiently protected against existing threats. However, after further investigating the rapidly evolving threat landscape, the Keio team identified an evolutionary need to migrate to the cloud for a more robust solution that would protect against emerging cyberthreats. The IT team discovered that 88.2 percent of web applications running on the IT team's network had significant vulnerabilities to SEO poisoning and similar threats. According to Sato, "There has been an increasing number of new web-based threats that have been difficult to address with a traditional cybersecurity solution alone. It became necessary to build a more multi-layered defense."

The Solution - Stopping Advanced Threats with a Cloud-Based Solution

Keio needed a solution that would improve DNS-based traffic control and prevent data exfiltration threats via web browsing. After thoroughly testing and comparing options, it chose Infoblox's BloxOne Threat Defense solution. The Keio team cited BloxOne's DNS Firewall, ease of installation, sufficient verification period and ability to minimize false detections as primary selling points. Tamura said, "Since Infoblox offers a cloud-based cybersecurity service, it is easy to deploy to every other company within the Keio Group. It can also flexibly support the addition of new functions and minimize the hardware maintenance and operations costs associated with an on-prem solution."

The company further notes its enhanced ability to improve operational efficiencies with the solution's Reporting and Dossier functions. These functions display a list of links for information related to detected and blocked malware, and for searching websites containing the described information without having to access them. The customer is also benefitting from the solution's use of analytics and machine learning to detect and block the latest threats. Such threats include information leaks through DNS-based attacks, domain name generation algorithms (DGAs), DNS Messenger and fast-flux attacks. In addition, highly accurate detection occurs through linkage of DDI (DNS/DHCP/IP address management), threat information and contextual information. These sophisticated features can then rapidly deal with threats.

> *"Since Infoblox offers a cloud-based cybersecurity service, it is easy to deploy to every other company within the Keio Group. It can also flexibly support the addition of new functions and minimize the hardware maintenance and operations costs and load associated with an on-prem solution...Infoblox staff is very helpful and willing to listen intently to and discuss our requests for new functions and integration with other solutions."*
>
> Hiroko Tamura,
> **IT Management Officer-in-Charge,**
> **Keio Corporation**

"The JPCERT materials were particularly helpful," Sato said. "If malware could not be detected or blocked during the attack stage of delivery, the DNS can be checked again on execution of the exploit, C&C and objective, thus increasing the probability of blocking unauthorized communications that slipped through during the attack stage of delivery." Table 1 presents the interaction of attack stage and content with logs.

Relationship between Attack Stage, Attack Content and Logs

	Attack Stage	Attack Content that can be Detected in Logs	Log Acquisition Target Device
1	Reconnaissance	-	-
2	Weaponisation	-	-
3	Delivery	Sending of emails with malware attached by attackers	Mail server
		Sending of invitation emails and invitations to websites containing malware by attackers	Mail server Web proxy server DNS server
4	Exploit	Callback (communications sent outside the company without going through a web proxy server)	Firewall DNS server
		Callback (communications sent outside the company using protocols such as HTTP and HTTPS)	Web proxy server DNS server
5	Installation	-	-
		-	-
6	C&C	Callback (communications sent outside the company without going through a web proxy server)	Firewall DNS server
		Callback (communications sent outside the company using protocols such as HTTP and HTTPS)	Web proxy server DNS server
		Infectious activity (searching for vulnerable PCs, internal servers, etc.)	Firewall
		Revoking access or permissions to the file server, etc.	AD log Firewall
7	Execution of the purpose	Callback (communications sent outside the company without going through a web proxy server)	Firewall DNS server
		Callback (communications sent outside the company using protocols such as HTTP and HTTPS)	Web proxy server DNS server
		Taking out confidential information (via mail server)	Mail server DNS server

Source: "Using Logs for the Early Detection and Analysis of Sophisticated Cyber Attacks", by the JPCERT Coordination Center
https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf

Table 1: Relationship between Attack Stage, Attack Content and Logs

Measurable Outcomes and a Superior Customer Experience

Keio reports that it has had an exceptional customer experience. According to Tamura, "Infoblox staff is very helpful and willing to listen intently to and discuss our requests for new functions and integration with other solutions."

The customer tested the Infoblox solution over the course of two periods in 2018 and again in 2019. Keio formally decided to install BloxOne Threat Defense for the Keio Group companies in June 2019 and began full-scale operations three months later. As a result, Keio has further enhanced its cybersecurity posture and modernized its network to scale for future growth. It is now proactively protecting approximately 6,000 client PCs and can detect over 50 communications to URLs that had previously not been detected, including the dangerous Emotet download site.

Upon looking to the future, Keio anticipates an increase in remote user activity with the rise of telecommuting. It is planning to further reduce its operation load with automatic identification of suspicious devices and linkage of firewalls and other cybersecurity tools.

For More Information

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