CASE STUDY

Interval Leisure Group Inc.

“Infoblox offered us a multitude of solutions, from Secure DNS through IPAM, all in one—which is exactly what we were looking for.”

— Sasan Hamidi, CISO, Interval Leisure Group

Profile

The customer:
Interval Leisure Group, Inc. is a leading global provider of non-traditional lodging across a broad spectrum of the vacation industry.

The challenge:
Interval’s Microsoft DNS system didn’t have a centralized or automated IPAM database, and the security team badly needed visibility and reports that would help them analyze security incidents. In addition, the network team—operating in a dynamic environment of aggressive business expansion—needed automation to replace time-consuming and error-prone spreadsheets.

The solution:
- Infoblox DDI
- Infoblox DNS Firewall
- Infoblox Security Ecosystem
- Infoblox Reporting and Analytics
- Infoblox Network Insight

The results:
- More efficient, cost effective management of core network services
- Better command of IP addresses for more rapid detection of infected end points
- An additional layer of protection against advanced persistent threats and malware

The Customer

Interval Leisure Group (ILG) is a leading global provider of non-traditional lodging, encompassing a portfolio of travel, leisure, membership, exchange, resort management, and rental businesses. Interval International and Trading Places International (TPI) offer exchange and travel-related products to more than 2 million member families worldwide. Under license from Hyatt, Hyatt Vacation Ownership markets and manages shared ownership properties and operates Hyatt Residence Club. Vacation Resorts International, VRI Europe, and TPI offer timeshare resort, homeowners’ association, and club management services, while Aston Hotels & Resorts and Aqua Hospitality provide hotel and condominium rentals and resort management. Headquartered in Miami, Florida, ILG has offices in 16 countries and nearly 6,000 employees.

The Challenge

What began as a quest for an automated IP address management (IPAM) system to facilitate forensic investigations into malware became a larger initiative to make several enhancements to network security and to increase network management efficiency as well.

Interval Leisure Group CISO Sasan Hamidi begins by explaining the security requirement. “For the past few years the hospitality industry has been plagued by data breaches,” he says. “It has become a favorite target of hackers because the hospitality industry’s databases are a very rich source of credit-card data and personally identifiable information.” In 2014 alone, he adds, his security operation center correlated over 19 million alerts, 8,500 of which were classified as medium-to-high-threat alerts and opened as tickets for analysis.

But conducting forensic investigation in the legacy environment was taking far too long. “As we all know from some of the big exposures like Target had,” says Hamidi, “time is of the essence. Any delay in detecting infected devices gives malware more time to replicate within your network.” The delays the security team was experiencing using spreadsheets were considerable. Every incident took between two and four hours to diagnose—even more, if analysts tried to identify infected end points—and this was amounting to hundreds of hours. In addition, investigation results were often inaccurate because the IP addresses they pointed to had been reassigned. “It was time to stop putting bandages on top of bandages and to step back and re-architect our environment with Infoblox Secure DNS,” Hamidi says.

When Hamidi started looking for an automated IPAM solution to replace the company’s manual spreadsheet-based system, he soon realized that for IPAM to work the way he wanted it to, it had to function within an efficient Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) environment. Since Infoblox offers the industry-leading solution for integrated
DNS, DHCP, and IPAM (DDI), the Santa Clara, California, based company was a prime candidate. “Infoblox offered us a multitude of solutions,” Hamidi says, “from Secure DNS through IPAM, all in one—which is exactly what we were looking for.” When the network and infrastructure teams were consulted, they saw the potential to improve management efficiency as well, and supported the purchase of an Infoblox solution. “Once an IP address expires, it’s very difficult to determine from logs which addresses are still active and which aren’t,” says Hamidi. “Nobody wants to assign thousands of static IP addresses to end points serviced by DHCP.”

The Infoblox Solution
Infoblox DDI, which integrates DNS, DHCP, and IP address management via a single user interface and a shared database, could address the network team’s concerns, and automated IPAM could greatly accelerate the security team’s task of investigating malware. “We are hoping that Infoblox IPAM can bring order to our environment and enable us to resolve addresses to host names and host names to addresses,” Hamidi says.

Interval also purchased Infoblox DNS Firewall and the Infoblox Security Ecosystem to supplement its FireEye solution for defending against zero-day malware. By integrating with FireEye, DNS Firewall enables Interval to leverage Infoblox DNS-level blocking and device fingerprinting to detect and disrupt APT malware communication and bring additional accuracy to the identification of infected devices attempting to access malicious domains.

The Results
The installation is in progress, and will eventually be rolled out to all of Interval Leisure Group’s subsidiaries. When the deployment is complete, Infoblox DDI running on patented Infoblox Grid™ technology will give Interval state-of-the-art IPAM and automated error checking on the world’s most advanced, highly available, fault-tolerant, and scalable platform. Hamidi sums it up this way: “In an enterprise with a complex network such as ours, supporting thousands of resorts around the world, effective security and efficient network management are both moving targets. But we’re pretty good sharpshooters, and we expect Infoblox to improve our aim even more.”