IMPERVA

CASE STUDY

Keystone RV Stops a Large-Scale DDoS Attack with Imperva Incapsula

Keystone RV Company

Overview

Headquartered in Indiana, Keystone RV is the leading manufacturer of recreational vehicles in North America. The company's brands, including Montana, Cougar, and Outback, are some of the most recognizable names on the highway. Keystone RV, composed of self-described "RV geeks," is poised to ship its five hundred thousandth unit in 2011.

Distributed Denial of Service Attack Cripples Corporate and Partner Websites

Keystone RV maintains both a corporate Website and a partner portal for its ten thousand dealers. In August 2011, the company began receiving reports from dealers saying that its corporate site and its partner portal were unavailable. Mark Widman, Keystone's lead network and security administrator, contacted the company's Web hosting provider and learned that they were suffering from a Distributed Denial of Service (DDoS) attack.

The cause of the DDoS attack was unknown; Keystone had not received a "ransom note" from cyber extortionists, which is a common occurrence with DDoS attacks. And, the company had not perpetrated any actions that would incite cyber vigilantes or political Hacktivists. Keystone appeared to be the random victim of a DDoS attack.

At first, Keystone's Web hosting provider attempted to allocate more Web application hosting resources to the Website. The hosting provider added more Web servers and allotted more application bandwidth. Unfortunately, according to Widman, the hosting provider's "solution fell apart under the attack. We were caught behind the eight ball."

Quick Evaluation and Deployment with Immediate Results

Since the company had not suffered from a DDoS attack before, the security team needed to quickly investigate viable solutions. The security team identified a commercial DDoS defense service and a free offering. The team's IT solutions partner recommended Imperva Incapsula. According to Widman, the security team quickly eliminated the free offering because it couldn't meet Keystone's service guarantees and the initial commercial service that they had discovered was "just too expensive."

Mark Widman contacted Imperva at 4:00 PM on a Thursday afternoon. After supplying Imperva with provisioning information and then updating Keystone's DNS information, the company was able to quickly redirect Web traffic through the Imperva's cloud security infrastructure. By 6:00 PM—two hours later—the Website was up and running and completely protected against the attack.

Keystone RV Company

Customer

Keystone RV Company
Goshen, Indiana

Requirements

- Immediate protection against DDoS attacks
- Accurate application attack prevention
- Easy, affordable solution for hosted Web applications
- Responsive technical support staff

Solution

Imperva Incapsula quickly defeated a DDoS attack targeting the Keystone RV Website and also mitigated several follow-on DDoS attacks.

Bottom Line

- Imperva Incapsula DDoS protection scaled on demand to block a powerful DDoS attack
- As a managed service, Keystone has not had to invest resources or personnel to manage policies
- The Keystone Website is protected against DDoS threats and Web attacks like SQL injection and Cross-site scripting

Imperva Incapsula Foils SYN Flood Attack as well as Follow-on Attacks

Based on information from Imperva, Keystone learned that its Website had been the target of a massive DDoS attack known as a SYN flood. During a distributed SYN flood attack, multiple attack sources send vast numbers of connection requests, known as SYN requests, to the victim's computers in an attempt to overwhelm computing resources. At the height of the attack, Keystone's Web bandwidth usage was over one hundred times greater than typical levels. Imperva Incapsula easily mitigated the DDoS attack through network Denial of Service protection mechanisms. Because Imperva cloud services route traffic through a globally distributed network of data centers, Imperva could scale to handle an attack that exceeded the hosting provider's Internet bandwidth capacity.

Imperva's Security Operations Center (SOC) engineers informed Widman and his team that the majority of the attack traffic was originating from Eastern Europe. Widman worked with the Imperva SOC engineers to restrict access from specific geographic regions while they were under an attack. This measure also helped eliminate undesirable Web requests.

Two days after purchasing Imperva Incapsula, the DDoS attack subsided. However, Keystone suffered two follow-on attacks over the next month. Imperva was able to stop these DDoS attacks as well. After receiving a series of DDoS attacks, Keystone's security team was relieved that their Web applications were safeguarded by Imperva. Widman said, "Imperva has been a lifesaver."

Technical Support Exceeds Expectations

From the outset, Keystone's security team has been impressed by the sales and support staff at Imperva. "Everyone we've worked with has been knowledgeable and responsive." The Imperva SOC manages all aspects of the deployment, including security policy configuration, monitoring, and tuning. When Keystone requests a policy change or enquires about a security alert notification, "Policy changes are performed in less than 45 minutes. Imperva's support engineers have been outstanding."

> *"When we were under attack, our bandwidth went up one hundred fold. Imperva stopped the attack and kept our site up and running. The support team has been great. After provisioning Imperva, we haven't looked back."*
>
> MARK WIDMAN,
> IT AND SECURITY ADMINISTRATOR,
> KEYSTONE RV

Imperva Incapsula Stops Web Attacks, Offers Visibility into Application Activity

In addition to the Imperva Incapsula DDos Protection Service, Keystone also enabled Imperva Incapsula's WAF. So, Keystone's Websites are not only protected against powerful DDoS attacks, but they are also secured against Web application attacks like SQL injection, cross-site scripting (XSS), and directory traversal. Keystone's security team was surprised to learn that both users and bots were attacking the site and attempting to access sensitive data.

Imperva Incapsula DDoS protection not only gives Keystone's security team peace of mind, these services also offer greater visibility into Web application activity. Email alert notifications inform the security team of attacks and abnormal activity. Notifications list the type of threat and the attacker's IP address, Web browser, and geographic location. Keystone's security administrators can also login to the online portal to view additional information such as the targeted URL and the threat pattern that triggered the violation. A high-level dashboard shows security, performance, and configuration information.

With Imperva Incapsula, Keystone is protected against future Web and DDoS attacks. For Keystone, Imperva Incapsula was cost-effective and easy to roll out—Keystone's security personnel just had to complete a short provisioning form and contact the company's DNS hosting provider to update DNS settings. From Widman's perspective, "Every aspect of the service has been stellar."

IMPERVA INCAPSULA