CASE STUDY

CART BLANCHE

Eric Hileman calls the combination of VIPRION and BIG-IP software modules that MageMojo is using "the ultimate data center firewall."

Security solutions from F5 Networks help e-commerce hosting provider MageMojo fortify customers' shopping carts following a series of distributed denial-of-service attacks.

At a Glance

COMPANY: MageMojo

HEADQUARTERS: Pittsburgh

EMPLOYEES: 7

BUSINESS: Founded in 2009, MageMojo hosts websites built using Magento, an open-source e-commerce platform. The company, which earned an estimated $1.5 million in revenue in 2013, works with its customers to identify problems in their site configuration and code base and to optimize Magento's features so their online stores deliver exceptionally fast, yet secure service.

TWEET THIS!

Black Friday and Cyber Monday are two of the biggest shopping days of the year. But in November 2012, the staff at Pittsburgh-based e-commerce hosting provider MageMojo learned the hard way that they needed to focus more on security.

That Thanksgiving weekend, a series of distributed denial-of-service (DDoS) attacks flooded MageMojo's network, crippling the company's ability to effectively service its customer base of online-store owners, who rely on that network to complete customer-generated e-commerce transactions.

"The largest of these attacks hit us on Cyber Monday — the worst possible time," recalls Eric Hileman, the company's cofounder. "They didn't just degrade performance; they took our network completely offline for a couple of hours. Our customers lost business — and we lost customers."

MageMojo's once stellar reputation as a provider and manager of Magento Commerce online stores had been tarnished. To restore customers' faith in its abilities, Hileman says, the company needed a dedicated solution that would mitigate future DDoS attacks.

Merchants' Dozen

The PCI Security Standards Council specifies 12 requirements for complying with the Payment Card Industry Data Security Standard (PCI DSS), which applies to any business that stores, processes or transmits cardholder data:

1. **Install and maintain a firewall configuration to protect cardholder data.**
2. **Do not use vendor-supplied defaults for system passwords and other security parameters.**
3. **Protect stored cardholder data.**
4. **Encrypt transmission of cardholder data across open, public networks.**
5. **Use and regularly update anti-virus software.**
6. **Develop and maintain secure systems and applications.**
7. **Restrict access to cardholder data by business need-to-know.**
8. **Assign a unique ID to each person with computer access.**
9. **Restrict physical access to cardholder data.**
10. **Track and monitor all access to network resources and cardholder data.**
11. **Regularly test security systems and processes.**
12. **Maintain a policy that addresses information security.**

SOURCE: Payment Card Industry Security Standards Council

TWEET THIS!

Making Sense of the Marketplace

MageMojo maintains its own network because page load times are an important factor in conversion rates and SEO rankings. Keeping that function in-house allows the company to control all aspects of site performance for its customers.

But the 2012 attacks revealed some weaknesses in the company's core networking equipment, which had been configured for intelligent routing through best path selection and low latency, rather than attack mitigation. Given the packet loss and high latency that resulted, Hileman, his partner and their five-person staff dedicated themselves to researching DDoS mitigation and application-level protection. They ultimately uncovered several potentially helpful approaches:

- **Clean pipes**, through which a dedicated team of IT security professionals in a company or service carrier such as Verizon or AT&T works exclusively on diminishing and eliminating DDoS attacks
- **Third-party mitigation**, a solution in which all traffic passes through a "scrubbing center," where a third-party provider checks it for malware and potential attacks
- **Dedicated DDoS appliances**, which are built specifically to address DDoS mitigation
- **Next-generation firewalls**, which combine web filters, virus scans and firewalling into a single device

Most DDoS protection best practices recommend eliminating firewalls because they are typically a choke point. But as an e-commerce provider, MageMojo must comply with the Payment Card Industry Data Security Standard (PCI DSS), which requires companies to put hardware firewalls in front of public-facing servers. Consequently, removing firewalls wasn't an option.

From their research, the MageMojo team learned that there are basically two types of DDoS mitigation strategies.

In the first, which includes clean pipes and third-party mitigation, a company can keep its existing core network in place and rely on other companies to filter the traffic before it hits the network. Dedicated DDoS appliances and next-generation firewalls fit the second category, requiring adequate upstream bandwidth, plus packet processing in routers and switches to handle the size of the attacks.

"We first looked at clean pipes and third-party mitigation providers," Hileman explains. "They were attractive to us because we could implement them fairly quickly without an immediate substantial investment in our network."

But clean pipes can be prone to false positives, are expensive and use the same dedicated appliances that MageMojo planned to consider anyway, he continues.

Hileman and his team decided that a third-party mitigation provider would be a cost-effective, short-term solution. However, the provider they selected made repeated mistakes. Soon, they realized that using yet another third-party solution would introduce too many additional potential points of failure into MageMojo's network.

"The easy solutions proved to be wrong for us," says Hileman, who adds that the company was prepared to invest in larger upstream connections and new core routers to handle large incoming attacks. "We liked investing in a larger core because it solved the problem of needing more throughput as we grew," he says. "But we needed extremely large firewalls and attack protection for the clients' servers beyond what traditional firewalls alone could provide."

The team next considered dedicated DDoS appliances. Yet, they soon found that the same specialized hardware they were using also was in the next-gen firewall segment, and had fewer features and higher costs. The logical step, then, was to consider next-gen firewalls, but they didn't scale well for speeds faster than 10 gigabits per second. Worse, the DDoS protection they offered would prove useful only for the most common attacks, and their session state tables, though large, were still vulnerable.

What MageMojo needed was a true data center firewall, Hileman explains — a solution that would scale easily and seamlessly beyond 10 gigabits per second; offer high availability with an active/passive standby unit; include Layer 7 inspection and manipulation; come certified by ICSA Labs; and wouldn't allow its session state table to be filled. An examination of traditional firewalls from Cisco Systems and Juniper Networks revealed that even the largest options couldn't scale seamlessly beyond 10Gbps without swapping entire chassis or line cards.

"At this point, we weren't feeling too good about the options," Hileman adds. But then he found CDW Account Manager Jake Jansen through a member of Web Hosting Talk's Colocation and Data Centers forum.

"After speaking with Jake, I felt comfortable working with him on such a large purchase," Hileman says. Although the team had identified the Cisco gear they wanted, they weren't sure what to do about the DDoS equipment they knew they needed. Jansen listened to their needs and tapped CDW's engineers to suggest a few options that MageMojo hadn't previously been aware of or considered.

Hileman wanted to make sure that the $450,000 they ultimately invested in Cisco and F5 Networks equipment was worth every penny, so he put the CDW team through its paces.

"We wanted multiple calls with all the vendors," he remembers. "We wanted as much engineering assistance

DDoS Action Items

Distributed denial-of-service (DDoS) attacks are front of mind again for many organizations following several intrusions on business and government systems by both political hactivists and those who launch such attacks for profit. Jon Oltsik, senior principal analyst for the Enterprise Strategy Group, recommends these best practices for mitigating DDoS attacks.

Understand how today's DDoS attacks differ from those of the past. People still think of DDoS attacks as a Layer 3 or Layer 4 attack on the network. That's no longer true, as the vast majority of attacks today are on applications as opposed to internal networking equipment.

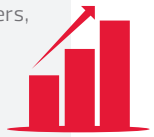
A knowledgeable hacker can take down an application by attacking one workstation with a rogue protocol. But he or she would need a more expensive botnet to launch a DDoS attack at the network layer.

Conduct a networkwide DDoS risk assessment. The goal is to find out where vulnerabilities lie. This includes a careful look at every layer of the network, from the network connections in Layer 3 to the applications in Layer 7.

During the assessment, ensure that the organization's Domain Name System (DNS) servers aren't underprovisioned. Be sure that the DNS servers are properly patched and maintained so they are less vulnerable to an attack. It's also important to thoroughly check firewalls and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) appliances for potential weaknesses.

Implement adequate rules to mitigate a DDoS attack. Tune existing security controls so they're better able to prevent a DDoS attack.

Organizations that use Sourcefire Snort for IDS/IPS, for example, should be aware of all Snort signatures for DDoS. This applies all the way up the stack, including DNS servers, SSL accelerators and application-layer rules.



Calculate an ROI benchmark. It's always best to think of security as an insurance policy rather than a source of cost savings. To calculate a potential return on investment, however, divide the total cost of any security technology deployment by the amount of lost revenue, lost productivity and the cost of remediation in the event of a disruptive DDoS attack.

Don't be afraid to ask for help. If an organization lacks the internal expertise to protect against DDoS attacks, seek outside assistance. Most carriers, such as Verizon and AT&T, have teams that focus on DDoS. Some third-party companies also specialize in mitigating DDoS.

as we could get. To top it all off, our financing fell through at the last minute. But none of this fazed Jake. He always returned emails and calls right away."

Because CDW works with more than a dozen leasing companies, Jansen says he was confident that one of them would come through for MageMojo. "We finally found them a leasing arrangement with Cisco Capital," he explains. "We started the process in November 2012, and the order was placed in March."

25%

The projected percentage of distributed denial-of-service attacks in 2013 that would be application-based

SOURCE: *Arming Financial and E-Commerce Services Against Top 2013 Cyberthreats* (Gartner, January 2013)

Finding Relief Through F5

That order included F5's VIPRION hardware, BIG-IP Local Traffic Manager (LTM), BIG-IP Advanced Firewall Manager (AFM) and BIG-IP Application Security Manager (ASM). Hileman says the combined solutions have both "surprised and relieved" him. "All of our requirements for scalability, performance, redundancy and attack protection have been met," he confirms.

According to Hileman, the F5 VIPRION platform lets MageMojo start small with a single blade, then scale quickly and seamlessly by inserting more blades into the chassis. When the company reaches the maximum vertical scaling by filling a chassis with blades, they can add more chassis and begin scaling horizontally. Multiple chassis can use an active/passive configuration for redundancy.

The VIPRION hardware also offers additional DDoS protection through synchronized (SYN) cookies, a Transmission Control Protocol sequence that offsets a SYN flood, and application acceleration using Secure Sockets Layer offloading. The SYN cookies stop SYN flood attacks — perhaps the most common form of DDoS attack, in which phony packets flood a network and launch an attack. The SSL offloading, meanwhile, significantly improves application performance by using specialized features in the VIPRION hardware to handle the SSL encryption.

The BIG-IP base software contains a connection reaper to ensure that even under the highest attacks, its session state table (the part of the device that keeps track of network connections) is never overwhelmed. The connection reaper also ensures that F5's state table never fills by purging the oldest connections from the state table once it reaches its high-water mark, preventing new connections from being accepted.

The BIG-IP LTM module was selected to provide the load balancing and Network Address Translation features — which route packets from network to network — that MageMojo needed. LTM also includes F5's iRules scripting all the way up to Layer 7, which mitigates many common attacks.

The BIG-IP AFM module was certified by ICSA Labs, thus fulfilling the company's PCI DSS firewall protection requirement. And the BIG-IP ASM module helps the company mitigate Layer 7 application-level attacks. MageMojo also relies on F5's IP Intelligence subscription-based service to block connections from known botnets and other malicious IP addresses.

"The results have been excellent," CDW's Jansen says. "F5 was the perfect solution for MageMojo's needs."

Hileman couldn't agree more, calling the combination of VIPRION and BIG-IP software modules "the ultimate data center firewall."

Together, they offer "all the features of dedicated DDoS protection appliances, with better performance and redundancy," he continues. "It's like a Swiss Army Knife: It can meet any requirement because it's a full Layer 7 proxy, enabling us to maintain PCI DSS compliance while also providing DDoS and application-level protection for our customers."

Jen McKen Photography

TWEET THIS!

CDW® PEOPLE WHO GET IT™