SPAFINDER
THE GLOBAL SPA & WELLNESS RESOURCE

Prolexic Restores Peace of Mind to Spafinder.com with Fast DDoS Attack Mitigation

At Spafinder.com visitors can view numerous wellness articles or find wellness and spa providers where they can redeem gift certificates or points earned. While the chairman and CEO thought it unlikely that the company's web site would be attacked, he was proactive and had put in place a DDoS mitigation solution provided by its hosting company. This was a defensive move to protect the site against any attacks that might be launched during the company's busiest time of the year – the fourth quarter – when holiday sales usually generate a significant percentage of Spafinder's annual revenue. "We can't afford to go down at holiday time," says Spafinder's Chairman and Chief Executive Officer, Pete Ellis.

Unfortunately, when it really counted – during an attack – the mitigation solution provided by the hosting company did not live up to expectations. "The solution from our hosting company was supposed to monitor any spikes in traffic and be able to isolate and divert the traffic to limit our exposure to an attack. We found out that the protection they were offering us was like a 1960s car alarm. It did nothing for us except give us false peace of mind."

> Company under attack

Spafinder, a global online resource for spa and wellness services and products

> Type of DDoS attack

A randomized series of Layer 4 and Layer 7 attacks

> Prolexic mitigation strategy

Prolexic's proprietary tools and real-time monitoring by Prolexic technicians

> Time to mitigation

Within minutes after traffic began flowing through Prolexic's mitigation network

When the attack started, Spafinder's 24/7 call center was flooded with complaints that customers could not access the web site to view wellness content, redeem gift certificates or spend rewards points. Ironically, the call center agents needed to access the web site to respond to customer requests, but they could not since the site was down. All they could do was take the customers' names and numbers and promise to call back.

"In addition to generating revenue through our site, we also get about 30,000 customers coming to the site looking for places to spend their certificates or rewards," Ellis says. "The attack was a double whammy on our sales and on customer service, as well."

When the hosting company could not mitigate the attack after trying for about four hours, Ellis realized that he needed a more experienced DDoS mitigation company. He called the CEO of another wellness product company that had been attacked earlier for advice.

"I could see that the attack could go on for days or longer if I didn't do something immediately," Ellis says. "On the recommendation of the CEO of our strategic partner, I called Prolexic, and our site was up and running at full capacity by 6 a.m. the next day."

Prolexic's mitigation strategy

Prolexic technicians began mitigating the attack around 2 p.m. As they began the provisioning process, they realized that the hosting company's DDoS mitigation tool was causing some issues.

PROLEXIC
DDoS Attacks End Here.

They also discovered that one of Spafinder's servers was not operating properly. The Prolexic technicians teamed up with Spafinder's IT staff and the hosting company's technicians to troubleshoot and resolve both problems.

"Prolexic went above and beyond to help Spafinder ensure that their network would integrate properly with ours," says Neal Quinn, vice president of operations at Prolexic. "Even though we experienced a few external issues, we were still able to work with all parties to restore accessibility to their web site the same day."

The Spafinder web site became accessible to customers as soon as Prolexic was able to route the site's traffic through its globally distributed scrubbing centers. Spafinder was able to service a percentage of its normal daily volume of customers that evening and gained full capacity by early the next morning.

Although Spafinder's hosting company had told Ellis that this was a very sophisticated DDoS attack that was difficult to mitigate, Prolexic technicians immediately recognized it as a combination Layer 4 and Layer 7 attack – a common type that they had dealt with many times before. In addition, using a combination of Prolexic's proprietary mitigation tools and real-time monitoring, they were prepared to counteract every move the attacker made over two days of randomized attacks.

"As we deployed our mitigation tools and real-time monitoring, the attack would trickle down to almost nothing, and then another wave of attacks with a different signature would start," Quinn says. "The attack actually spanned two days after we began mitigation because the attackers changed the signature every time they realized we were successfully blocking the attack. Finally, they gave up after they realized that Prolexic could identify and block whatever they could send at us."

Prolexic identified the IP addresses of the top ten sources of the DDoS attacks, which included Kazakhstan, Belarus, Peru, and the United Arab Emirates. "I don't think that these attackers were after any kind of financial gain," Ellis says. "On the Internet, hackers are now doing things just to prove they can do it. I think the attack on Spafinder just got someone a 'merit badge' but that doesn't lessen the damage they did to our revenue and customer service."

Staying protected with Prolexic

Since Prolexic mitigated the August 18 DDoS attack, Spafinder has not experienced another – a common occurrence once attackers see that a site is protected by Prolexic. With fourth quarter holiday sales season approaching quickly, Spafinder is gearing up for site traffic that will generate a significant percentage of total yearly revenues. A DDoS attack during the holidays would be a disaster, but now Spafinder is well prepared against that threat with Prolexic.

"If Prolexic had approached me with their solution six months ago without ever having been attacked, I would have said that Spafinder is not the type of company to have this type of problem," Ellis says. "But the reality is that we do 20 percent of our business online with 50 percent of that revenue coming in the fourth quarter. If there were any interruption to business at that time, it would cost us millions of dollars. Now I have no doubt that I need a solution from Prolexic, and it also makes me want to put protective measures in other areas of our business."

Ellis notes that it was easy to do business with Prolexic. "I felt that everybody wanted our business, from the company president on down," Ellis says. "Everyone was extremely responsive."

Ellis also has this advice for CEOs who believe that their companies aren't on an attacker's radar. "I never would have thought that we needed DDoS protection," Ellis says. "At the end of the day, the proliferation of attacks on all types of companies is becoming more serious. Now that it's happened to Spafinder, I say you have to have a DDoS mitigation solution from a company like Prolexic, especially if you have any type of e-Commerce platform."

Prolexic Fights Off Massive Layer 7 DDoS Attack for Global Fragrance and Beauty Products Retailer

In June, a DDoS attack was launched on the complex, image-heavy web site of a leading global retailer of women's fragrances and beauty products – a company that also reported more than US$350 million in online sales. On the day of the attack, customers who attempted to visit the popular, trendy site saw only a blank page that would try to load over and over again for a long period of time. Finally an error message would appear instead of the expected colorful array of lipstick, eye shadow, and blush. In addition to losing the potential revenue from those site visitors – some industry analysts estimate that 24 hours of downtime for a major e-Commerce site can reach US$30 million – the online retailer also risked losing brand equity in a competitive business. Customers spread the news on Twitter that the web site was out of service, and rumors started that perhaps the company itself might be out of business.

> Company under attack

Popular online retailer of many unique brands of fragrances, makeup, and other beauty and bath product lines

> Type of DDoS attack

A stealth, randomized Layer 7 attack disguised as a bandwidth attack

> Prolexic mitigation strategy

Use proprietary tools for Layer 7 attack mitigation and the expertise of Prolexic's operations team to monitor traffic patterns and thwart the attacker's countermoves in real time

> Time to mitigation

The retailer's website was back online within 5 minutes from when Prolexic service was engaged and remained online despite frequent changes to the attack

The retailer fought back at first using the resources of two major service providers that provided a basic level of DDoS mitigation. However, the nature of this Layer 7 DDoS attack was too complex and its volume was too large for those companies to mitigate. The retailer called Prolexic on a Thursday, but had to wait until Monday to get approval to proceed from its corporate management and legal teams. As a result, the retailer's site was offline for a damaging 72 hours.

Prolexic wasn't surprised to get that call. Several days before the retailer was attacked, Prolexic had been contacted by two other companies in the fragrance and beauty industry whose sites were under a similar Layer 7 attack. Both companies immediately engaged Prolexic, whose operations engineers were able to mitigate the attacks in about 5 minutes. As a result, their sites were back online and ready to process weekend sales.

Prolexic's mitigation strategy

After the beauty product retailer received management's approval to engage Prolexic on Monday, the Prolexic team was ready to mitigate almost immediately. Within five minutes of the network traffic being routed through the Prolexic scrubbing centers, the retailer's site was back online and ready for business.

"These attacks were of a nature we hadn't seen before," says Paul Sop, chief technology officer at Prolexic. "Years ago, we identified an emerging trend where complex Layer 7 attacks were increasing and proactively developed monitoring, alerting, and mitigation tools to address them before they became mainstream. We were ready to block this attack quickly and were able to easily and rapidly bring this retailer's site back online."

PROLEXIC
DDoS Attacks End Here.

"This was one of the larger Layer 7 attacks that we had seen at that point in time."

PROLEXIC
DDoS Attacks End Here.

"The attackers used a DDoS method that made it look like it was only an attack on bandwidth," Sop continues. "But since we had just fought off a similar combination Layer 7 attack just days earlier for the other fragrance companies, our solution for this client was really plug and play. We saw that the attacker was using the same botnet, so we already had the signatures in place to fight the attack."

Using proprietary tools and drawing upon the team's previous experience, Prolexic was quickly able to determine the attacker's strategy:

- Avoid the caching of the retailer's existing DDoS mitigation provider by targeting the back-end application server directly
- Each bot used a low-request-rate to avoid threshold mitigation, easily bypassing commonly used commercial off-the-shelf (COTS) hardware solutions designed to mitigate DDoS attacks
- Employ HTTPS attack components to avoid Intrusion Prevention System (IPS) and most mitigation systems
- Construct queries which peg CPU and overload back-end databases

"This was one of the larger Layer 7 attacks that we had seen at that point in time, and one that reflected a trend we had been watching," Sop says.

"In this case, the attack started with a massive Layer 4 attack with bandwidth to distract from the more insidious Layer 7 attack that is at a lower bandwidth level and harder to detect. That's where Prolexic's experience came in. We knew to expect this combination attack and we looked for it. A DDoS service provider with less experience might take things at face value and miss the real threat."

Prolexic also drew upon its team's expertise in responding to the attacker's countermoves on-the-fly in real time in randomized attacks. When fighting Layer 7 attacks, Prolexic's team knows that there is usually a human attacker at the other end pulling the strings.

"We often see the attacker making offensive moves, and that happened with this cosmetic retail client," Sop says. "Our operations personnel constantly monitored the traffic, noticed any changes, did the pattern recognition, figured out what was new and how to block it. We then applied a new signature block all in the course of a few minutes. We've had to do that as many as 40 times in some cases. There is no automated device on the planet that can react in real time like our operations people can."

Putting on a fresh, confident face with Prolexic

Since becoming a client, the beauty product retailer has relied on Prolexic to protect its e-Commerce web site from future DDoS attacks. Today, just as its customers face the world more confidently using the beauty products it sells, this retailer operates online with confidence, knowing that Prolexic will respond quickly with a proven DDoS solution to keep the site running smoothly should another attack occur. But additional attacks aren't as likely since potential attackers know that this web site is protected by Prolexic. But that doesn't mean they won't try.

"Attackers know when a web site's traffic terminates with Prolexic, so it's not unusual for us to see our customers get attacked about 12 months after the contract is signed, because they want to see if we are still protecting the site," Sop says. "The following year, we had given this retail client an additional 30 days to negotiate a contract renewal. Attackers didn't know this and just 13 days after the supposed contract expiration, they launched an attack out of nowhere that was quadruple the size of the one the previous year. This time the attackers never had a chance to bring this site down for 72 hours again – not with Prolexic on the front lines."

About Prolexic: Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet facing infrastructures for global enterprises and government agencies within minutes. Six of the world's ten largest banks and the leading companies in e-Commerce, payment processing, travel/hospitality, gaming and other at risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com** or call **+1 (954) 620 6002.**