



## 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.

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."



### > 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.

*"We often see the attacker making defensive moves, and that happened with this cosmetic retail client."*

"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 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 countermeasures 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.

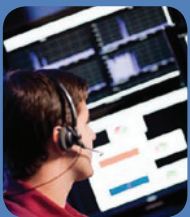
"We often see the attacker making defensive moves, and that happened with this cosmetic retail client," Sop says. "Our operations personnel constantly monitored the traffic, noticed any changes, did the pattern recognition, figured out what was new and how to block it. We then applied a new signature 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. GII 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.preventia.co.uk](http://www.preventia.co.uk) or call us on 01273 83 33 00