



Prolexic Mitigates Layer 7 Attacks for Options Trading Firm and Delivers Immediate ROI

In May, two large U.S. online options trading firms received e-mails demanding nearly US\$60,000 from anonymous DDoS attackers. If they didn't pay up, the attacks would continue, potentially costing the firms tens of thousands of dollars if their trading platforms became unavailable for an extended period. After reporting this threat to a government agency, the companies were referred to Prolexic.

Company A had a strong in-house technical team who had been able to fend off previous attacks and prevent its web site from going offline – at least at first. "Our team was doing a pretty effective job and the attacks weren't affecting our business," says the company's chief technology officer (CTO). "But as the attacks continued, the attacker began to change vectors and signatures more frequently. To continue our defense, we saw that we would have to go deeper into our application stack to make coding changes and that posed a high risk to the stability of our site. Obviously, we didn't want to do that."

Faced with an increasing number of more sophisticated attacks, both companies realized that they needed outside help. Company A selected Prolexic while Company B sought out DDoS mitigation services from a large Internet services company.

Prolexic DDoS mitigation experts were able to stop the latest attack within one hour as soon as Company A's network traffic starting flowing through Prolexic's globally distributed scrubbing centers. The company's web site remained online and available to traders while Prolexic experts fought the attack behind the scenes. In contrast, it was a full 48 hours before the Internet services company was able to overcome the latest attack for Company B. As a result, its web site was unavailable during that period – resulting in a damaged brand reputation and lost revenues.

Prolexic's mitigation strategy

It was immediately apparent to the Prolexic technicians that encrypted Layer 7 attacks were being used. Using proprietary tools and techniques, Prolexic was able to stop the latest attack in minutes, eliminating the risk of the attacker hacking into the company's primary trading platform, a scenario that would have been devastating for both the business and its customers.



> Company under attack

A leading online options trading firm in the U.S.

> Type of DDoS attack

Encrypted Layer 7 attacks from multiple geographic locations

> Prolexic mitigation strategy

Use Prolexic's proprietary tools and techniques to block on-going attacks

> Time to mitigation

One hour

"Prolexic gave us a very complete report with a variety of graphics that helped us understand where the attack came from and how it was done."

While encrypted Layer 7 attacks pose a significant and growing threat to companies worldwide, they are no match for Prolexic. The company's proprietary tools enable technicians based at its Security Operations Center (SOC) to decrypt Layer 7 traffic "on the fly". As a result, the Prolexic team was able to identify the attacker's bot signatures, which originated primarily from locations in Asia and Eastern Europe. In addition, they were able to respond immediately to the attacker's changing tactics with real-time monitoring of Layer 7 traffic.

"Prolexic provided us with a complete list of the attacking IP addresses so that we could follow up with the FBI and try to catch the offenders," says the CTO. "Prolexic gave us a very complete report with a variety of graphics that helped us understand where the attack came from and how it was done."

Prolexic's report uncovered more than 65,500 IP addresses used in the attack. Prolexic was also able to pinpoint the geographic locations of the botnets, ranging in size from as few as 9 machines to 35,500. Other key data gathered by the Prolexic team included attack types (GET Flood and SSL GET Flood), bits per second, packets per second, and connections per second (as many as 16,000 per second throughout most of the attack).

The company's CTO was so impressed with Prolexic's expertise and responsiveness he called the other options trading firm that was still under attack – a competitor – and recommended they use Prolexic.

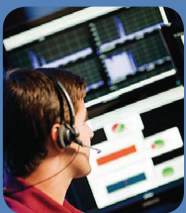
"It's not unusual to see attackers turn their attention and launch intensified attacks on other companies in the same industry once they see that their primary target's traffic is now routing through Prolexic," says Paul Sop, CTO at Prolexic. "Attackers know that we're on the front lines protecting our clients against even the largest and most complex Layer 7 attacks so they move to easier targets."



Staying protected with Prolexic

Online financial services companies in particular must ensure the stability of any or all of the web sites under their domain – especially when the financial resources of its customers are at stake. Today, Prolexic's customer remains protected against Layer 7 DDoS attacks without having to make changes to its application and network infrastructure. In addition, the company will never have to wait 48 hours or longer for attack mitigation like its competitor did.

"What we've learned is that even if you have some DDoS mitigating skills in house, it's not worth the risk of making significant changes to your infrastructure to fend off Layer 7 attacks," says the CTO. "There's always the possibility of making an application change and taking down your site yourself. So from a quality assurance perspective, we know that bringing in a proven DDoS expert like Prolexic is our best defense against Layer 7 attacks."



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.preventia.co.uk or call us on 01273 83 33 00