



Prolexic Answers Late Night Weekend Call to Mitigate DDoS Attack for Foundation Source

It was supposed to be a restful weekend for Gerry Battista, vice president of Information Technology Operations, and his staff at Foundation Source, the nation's largest foundation management firm. On a Friday evening, the network monitoring system sent out an alarm. Pages wouldn't load completely at www.foundationsource.com and the company's clients could not log in to their accounts to make gifts and grants.

"We checked our firewall and saw that there were 6,000 to 7,000 active connections going through it, whereas we usually have an average of 600 connections max when all of our clients are on the site," Battista says. "So we knew that we were under some kind of automated attack."

After further investigation, Battista's IT team confirmed that the site was under a DDoS attack, so they tried to block the attack using their firewall. They also went through a very tedious process of identifying the IP addresses that were making the connections and blocking them one by one. They also tried blocking the IP addresses outside of the U.S., but these measures worked for only a short time. The attack stopped completely a few times during the weekend, but then reoccurred three times stronger than before. At that point, it was evident to Battista that the company's firewall just could not handle the deluge of malicious traffic. The company's ISP was unable to help because it couldn't weed out the malicious traffic without affecting other clients. Battista and his staff began an online search to find a DDoS mitigation vendor – around 9 p.m. on Sunday.

"There are many providers out there who will host your applications in the cloud to provide DDoS mitigation services, but there are very few who will do it while your site is under a DDoS attack," Battista says. "After narrowing down our short list to Prolexic and another provider, we chose Prolexic. We saw that Prolexic had far more experience in successfully mitigating these kinds of attacks. Most of all, Prolexic was the only provider who actually called our operations manager back at 11 p.m. on Sunday night."

Prolexic's mitigation strategy

By noon on Monday, management at Foundation Source had signed the contract to give Prolexic the green light to start DDoS mitigation. Deployment of the Prolexic DDoS mitigation services required minimum involvement on the customer's part, with Battista's IT group only having to make minor changes to the client log-in URL and the URL used for administering client accounts.



> Company under attack

Foundation Source, the nation's largest foundation management firm

> Type of DDoS attack

A series of high packet-per-second GET Flood attacks

> Prolexic mitigation strategy

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

> Time to mitigation

Within hours after engaging Prolexic



"Prolexic's track record as an expert in DDoS mitigation was clearly evident."

As this was an emergency situation and new client for Prolexic, technicians did not have the luxury of profiling and identifying typical site traffic for www.foundationsource.com. Despite this hurdle, Prolexic's Security Operations Center staff were still able to quickly determine that the site was being attacked by a strong and widely distributed GET Flood, develop blocking signatures, and mitigate the attack in minutes as soon as traffic starting flowing through Prolexic's scrubbing centers.

Prolexic's mitigation technicians provided Battista's IT group with several IP addresses to which they would direct the site's DNS. The IT group reconfigured the firewall to allow only Prolexic IP addresses to come through. Prolexic's technicians also monitored the attack traffic 24/7 and immediately countered any changes that the live attacker would make in the attack signature, size, and complexity – something that automated mitigation tools alone cannot do. By 9:30 p.m. on Monday night, the DNS had been fully propagated and the Foundation Source web site was reopened to its clients and the public.

Battista was very happy with the responsiveness of the Prolexic team, as well as the flexibility of the terms of the contract. "The other company on our short list had a more attractive price upfront, but there would be significant costs if we wanted to stay on the service for a set amount of days after the attack," Battista says. "That would have cost us thousands of dollars per day. Prolexic offered us a better deal all around."

Staying protected with Prolexic

Battista notes that the company was fortunate that the DDoS attack occurred on a weekend, when client traffic to the site is less than during the business week. "Our business week was not impacted by the attack and we had plenty of time to try to mitigate the issues," he says. "We also had a workaround plan in place, so our offices could still administer client accounts while we kept the bad traffic blocked. An attack during the week would have been a different story, because having the site inaccessible would have damaged our client relationships."

Foundation Source's relationship with Prolexic is very good, according to Battista. "Everything was top notch with Prolexic," he says. "Their people were very responsive and everyone was kept in the loop throughout the mitigation process. Prolexic's track record as an expert in DDoS mitigation was clearly evident."

Today Foundation Source continues its mission of administering gifts, donations, and grants with DDoS protection from Prolexic. Staying protected is critical to ensuring that the web site will be accessible to its foundation clients who must meet annual regulations for dispersing funds.

"To this day, we have no idea why our web site was attacked," Battista says. "We had never been attacked before, but it can happen to anyone."



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