A high-profile Spanish-language news website with 15 million visits and 58 million page views per month became the target of a devastating DDoS distributed denial of service attack. Some DDoS attackers in Russia had noticed the site and began sending extortion emails and making threatening comments on the website's blogs two months prior to launching a denial of service attack. They demanded “150 bitcoins” or the equivalent of US$2,500 or else they would attempt to bring down the website with a DDoS attack. Management did not respond to these threats in line with company policy and furthermore, the website's hosting company would provide DoS and DDoS mitigation services in the event of any attack.

One Sunday afternoon, a journalist informed the president of the news outlet that the site was down. “Usually when the site is down it is a minor thing and our hosting company takes care of it,” says the co-founder and president. “At first, the hosting company thought it was a faulty router, but later they realized it was a DDoS attack. Unfortunately, the attack was so large that their DDoS mitigation equipment couldn’t stop it. There was nothing they could do.”

The president asked the technicians at the hosting company to recommend some solutions for mitigating the distributed denial of service DDoS attack. They told her to buy some time and get the site back up for a few days by changing site IP addresses. “Someone at the hosting company also told me to just let the attack run its course and take a week off and go on vacation,” she says. “Obviously, that was not an option. We were already offline for eight hours and could not fulfill our live coverage of elections in Colombia, which was a significant news story at the time. Finally, another person at the hosting company said that we should contact a company that specializes in DDoS mitigation and they recommended Prolexic.”

**Prolexic’s DDoS mitigation strategy**

Prolexic technicians quickly determined that the Spanish-language news site was experiencing a Layer 7 DDoS attack of 30 Gbps. They assisted the site’s IT staff in changing its DNS name servers to route all site traffic to servers in Prolexic’s global scrubbing centers, stopping any malicious traffic from reaching the news site. Once the site traffic was flowing through Prolexic’s scrubbing centers, it took about an hour to route the DNS changes to Prolexic.

The DDoS attackers abandoned the attack as soon as they saw that the news site’s traffic was being routed through Prolexic. According to Neal Quinn, Prolexic’s chief operating officer, it is not uncommon for Prolexic to deter attacks.
“Potential attackers can find out when traffic is routed through Prolexic and they typically move on to other easier targets,” Quinn says. “Prolexic can also be viewed as an insurance policy against distributed denial of service attacks and prolonged downtime. When attacks happen, clients can draw upon Prolexic’s mitigation services as needed to ensure ‘business as usual’ and guard against significant financial loss.”

“It took me longer to fill out the contract forms, scan them, and e-mail them back to Prolexic than it took to get our server up and running again,” the president of the news outlet says with a laugh. “It took almost no time. In about a half an hour, the DDoS attack was over.”

The president says that she was surprised that the global news site was so vulnerable to a DDoS distributed denial of service attack and that the hosting company’s DDoS mitigation solution could not mitigate it. Yet she is aware that DDoS attacks are happening more frequently.

“This is happening to other news websites,” she says. “The editor of another site has complained that they have been attacked at least twice over the past six months. The Layer 7 attack is the kind that can really hurt your business and you’re vulnerable all the time.”

Staying protected with Prolexic

“The fact that we had Prolexic in front of us caused the attacker to turn away,” the president says. “The fact is that anyone, from a 15-year-old to professionals, can easily plan and orchestrate a DDoS attack today. My advice would be to be prepared for attacks of the magnitude we experienced and call a professional DDoS mitigation firm like Prolexic to defend your site. We’ve heard sites that are known to be protected by Prolexic don’t get attacked and we’ve seen proof of that.”

About Prolexic: Prolexic Technologies is the world’s largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies, the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.
Ixaris Systems offers businesses and consumers a very flexible and instantaneous way of making and receiving online payments with virtual prepaid cards. The company’s consumer web site, www.entropay.com, enables anyone to open and immediately fund an account to obtain a virtual prepaid Visa card. As the first and now most successful virtual prepaid card introduced in Europe, EntroPay provides consumers with another payment option that is safe, convenient and accepted by millions of merchants worldwide.

Like any online business that experiences success and recognition, EntroPay became a target for DDoS attacks. Three years ago, the site had its first DDoS attack. The attackers sent a ransom e-mail demanding US$15,000 per month from Ixaris management as “protection money.” Management chose to ignore the ransom demand and forwarded it to the relevant authorities. The DDoS attackers followed through on their threat. Although no user data was compromised, the EntroPay site was brought down by a DDoS attack for a considerable length of time, making it impossible for users to create a new prepaid card account or load additional funds to their existing cards. A DDoS attack on EntroPay impacts other B2B sites since multiple URLs are linked by the same underlying application.

“As a financial services provider, the security of our service is of the utmost importance to us, so any attack is something we take very seriously,” says Tim Murfet, chief information officer at Ixaris Systems. “From a commercial standpoint, it is also vital we keep the EntroPay site running 24/7, 365 days a year. When the site is down, we not only miss out on revenue but our brand reputation is affected as well.”

Prolexic’s DDoS mitigation strategy

After the first attack, Ixaris relied on a hardware appliance from its ISP to protect EntroPay from future DDoS attacks. However, this solution failed when EntroPay was hit with another attack. A consultant recommended Prolexic as a DDoS mitigation provider who could quickly and successfully mitigate high volume attacks.

Once Ixaris IT personnel detected the attack and switched the IP address over to Prolexic’s proxy service, EntroPay was back in business in minutes. After seeing the fast time-to-mitigation provided by Prolexic in an emergency situation, Ixaris management decided to expand its DDoS protection with Prolexic’s PLXrouted service. With this service, DDoS attacks are detected by monitoring on-premise equipment. The traffic-routing service is activated using Border Gateway Protocol (BGP) to on-ramp network traffic to Prolexic’s cloud-based denial of service DDoS mitigation infrastructure.
Most recently, Prolexic has successfully mitigated a number of Layer 4 DDoS attacks against EntroPay, with the largest attack peaking at 700 Mbps. The site has been hit by a wide range of attack types – SYN Flood, ICMP Flood, UDP Flood – of various durations. EntroPay has also experienced attacks characterized by high CPU usage on its routers and several UDP drops on the router’s Access Control Lists (ACLs).

In each case, Prolexic technicians were able to defeat the attackers in just minutes using more than 20 commercial and proprietary mitigation tools and technologies and real-time monitoring of changing attack signatures. Post-attack forensic information also helped Ixaris identify where the attacks originated.

“We like the way that Prolexic can stop attacks immediately when we route the traffic through their servers” says Denise Vella, information security officer at Ixaris. “Also, we’re impressed with Prolexic’s vast experience in DDoS mitigation. They have the industry reputation to prove it.”

**Staying protected with Prolexic**

DDoS attacks on financial industry web sites by sophisticated hacktivist groups have increased dramatically in the early months of 2012, but EntroPay now has the same robust DDoS mitigation defense as 10 of the world’s largest banks – Prolexic. Today, if EntroPay experiences a DDoS attack, the company’s on-call IT personnel are informed immediately and are required to re-route all traffic to Prolexic for mitigation. IT also has access to Prolexic’s 24/7 customer service if any questions or unusual issues arise.

“Prolexic’s customer service is very efficient,” Vella says. “They’re there 24/7 and can address our issues within 5 to 10 minutes in emergency cases. Overall, Prolexic offers excellent service and once our traffic is routed through their network, we’re immediately back in business.”

Murfet compares DDoS protection from Prolexic to a disaster recovery plan that should be regularly tested to ensure that everyone in IT knows how to respond during an attack.

“I recommend having good communication with your DDoS mitigation provider even in non-attack situations and testing the service regularly so you’ll know it will work when you need it,” Murfet says.

“Don’t think that DDoS won’t happen to you, because it will,” Vella says. “If you don’t have the tools in-house, it makes sense to have a DDoS protection service. For a company that requires 100 percent uptime like ours, I would recommend putting a highly experienced DDoS mitigation service like Prolexic in place.”

---

*About Prolexic:* Prolexic Technologies is the world’s largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies, the world’s largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world’s first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.
Prolexic Mitigates DDoS Attacks Against Auction Website

Prolexic's client is a popular online auction site where bidders can purchase name brand new merchandise at steep discounts. Unfortunately, the site became a target for denial DDoS denial of service attackers. Earlier this year, a DDoS attack overwhelmed the site's firewall capabilities and requests were no longer being delivered to the load balancer.

The perpetrators sent a ransom demand for several thousand Euros in exchange for stopping the denial of service attack. Management at the auction site refused to pay. While the site had DDoS mitigation services from its hosting provider, a second attack overwhelmed its resources. The hosting provider nullrouted or “black holed” the auction site in order to avoid collateral damage to its other hosted sites.

“Our site went completely dark,” says the director of technology. “We had been attacked sporadically before, but those were generally smaller DDoS attacks that we could fight off with firewall rules. This time we were down for a total of six hours and we completely lost the opportunity to do business during the attack.”

The site's customers flooded the company's customer service lines with calls and e-mails to complain about the outage. “It’s difficult to put a dollar value on an outage, but it was definitely significant in terms of our reputation,” says the director.

The site's hosting provider recommended Prolexic for DDoS mitigation, among a few others, and after evaluating the levels of protection, Prolexic was selected. “Prolexic responded to our initial request for help with great speed and our site was back online almost immediately,” says the director. “After Prolexic took over, the DDoS attackers never returned.”

Prolexic's DDoS mitigation strategy

Prolexic provided emergency denial of service mitigation service to the site through its PLXproxy service. As soon as the auction site switched its domains over to the Prolexic PLXproxy service the site was back online and ready to accept bids. All traffic to the site was routed through Prolexic's cloud-based global scrubbing centers where Prolexic mitigation experts identified, analyzed and removed the malicious traffic.

Prolexic DDoS mitigation experts quickly identified the malicious traffic as a Layer 3 DDoS attack. They also determined that the attack originated in several Eastern European countries. Prolexic DDoS mitigation engineers used 20 mitigation tools, many of them proprietary, to monitor DDoS activity and counteract the attacker's signature changes on the fly.
“Prolexic responded to our initial request for help with great speed and our site was back online almost immediately.”

**Staying protected with Prolexic**

The director of technology has never uncovered why the auction site was singled out for this large DDoS denial of service attack, even though he knows that other online auction sites have been targeted in the past.

“Prolexic was very helpful throughout the whole DDoS mitigation process,” says the director. “Its engineers immediately answered any questions we had and they fully understood the urgency of our situation. With the site down, we couldn’t serve our customers and time was of the essence.

“Because of the fact that there’s no limit to incoming bandwidth, Prolexic will always help us mitigate whatever type of attack might come our way,” continues the director. “My advice to other online businesses would be to secure DDoS protection. The cost of denying service to a site is shockingly low. Everyone can be a target and anyone can be a potential DDoS attacker.”