dosarrest.com - the real deal

Contributed by Brett Brewer
Thursday, 23 June 2011
Last Updated Thursday, 23 June 2011

I recently had the unpleasant experience of weathering a rather nasty distributed denial of service (DDoS) attack on one of the sites I manage. It's a high traffic site that does many tens of thousands of dollars of business each and every day. Downtime on the site costs a lot of money and makes us look really bad. Earlier this week we received a short, poorly worded email from an anonymous email address informing us that our site was under attack and demanding an unspecified ransom to cease the attack. The attack took the site down early Monday morning and I, along with a few other people, scrambled to find a solution, working with our dedicated server company and Akamai to block the deluge of traffic that had maxxed out the connections on our firewall. This particular type of attack is known as a "SYN Flood Attack". It is very hard to defend against. We tried blocking IP addresses with our firewall and some POS software from Cisco called "Cisco Guard" which proved utterly useless. Akamai tried some other things that took hours to implement and also proved fruitless. In the end, both the dedicated server company and Akamai advised us there was little we could do other than "wait it out". That was simply not an option. By late in the day, we had lost thousands in revenue, not to mention the sinking feeling of utter helplessness at the hands of some asshole "hackers" who we could not hope to track down or identify. We suspected they were in eastern Europe, possibly in Hungary, but that was about all we could deduce. We called the FBI and got a recording and a message about submitting an incident report on their web site. I called CERT's 1-800 number to see if they had any advice or knew who I could report this to and they nearly laughed at me when I told them I'd tried to call the FBI to report it. CERT also directed me to a web form where I could fill out a report, but advised me that most likely nothing would be done. Apparently the WWW in internet addresses really does stand for "Wild Wild West". When it comes to dealing with a DDoS attack, you really are on your own. So what were we to do? Would we pay some unknown stranger an unspecified ransom? Would we wait another day and lose thousands more? Would we hire our own hackers to fight back? Finally as the day was quckly turning to evening and financial losses were piling up, we called one of our business associates who runs an even bigger and more prominent web site and told them what was happening to us and asked if they had any suggestions. They had two words for us....."Call Dosarrest.com", they said. We'd already done some research online looking for solutions and came across dosarrest's web site, but we were hesitant to try them at first. There were dozens of companies out there claiming to be experts in stopping DoS attacks. Some were big, some were small, some had proprietary hardware they would want to sell us to install at our datacenter, some were just services with no explanation of how they would help. But after the recommendation from our business associates, we decided to give dosarrest.com a call. Our associates assured us that when they had gone through a similar situation, they used dosarrest's services and though it wasn't particularly cheap, dosarrest got them back online within an hour or two. We had nothing to lose. Our mounting lost revenue had already cost us far more than dosarrest wanted to get us set up with their service. We made contact with dosarrest's sales rep who told us that depending on how quick we could make the required config changes to our site and DNS, they could have us back online within minutes or at most an hour or two. The sale rep wasn't joking. Within a few minutes of agreeing to the terms of their contract and making our initial paypal payment, their support team had sent us all the required configuration information, set up a proxy server to filter our traffic and were waiting on us to make the needed changes to our web server and dns config. Within the next hour we had completed the DNS and web server updates and our site was back in business. Throughout the process, I emailed their support with questions and had answers within minutes. When I called them, I was quickly connected to a tech-savvy support person who had all the answers I needed. Each time I have contacted them via email since, I have had a response within minutes. I think the longest response time from them was about 20 minutes for a non-emergency email, but usually it's much quicker. In fact, this evening, after several days of running with their service, I made a major update to the web site. About 100 files were changed and out of that 100 files I made 1 mistake in a config file that caused an endless redirect loop on the site. Because I had updated so many files at once, it took about 15 minutes to find my mistake and correct it. When I finished fixing the redirect problem, I checked my inbox to find an email already waiting from dosalert.com support informing me that they had detected that our site was down, had determined that it was not the result of an attack, had added some additional traffic filters as a precaution and were continuing to monitor the situation. It was not an automated message, it was from an actual support person who was actually on top of the situation. I immediately emailed them back to let them know the problem was caused by a stupid mistake on my part and to tell them how impressed I was that they were so diligent in monitoring our site. And then I sat down to write this post. I'm just not used to service this good. We pay a lot of money to our dedicated server company for 24/7 support and though they are often good, they don't come close to the level of service we've gotten from dosarrest so far. In fact, our web server company is supposed to be monitoring our server for downtime too, but I didn't get any messages from them tonight when I took our server down for 15 minutes. Dosarrest was on top of it within a few minutes. My only complaint with dosarrest is that they don't offer dedicated server hosting because I'd probably bite the bullet and go through all hassles to switch to them for that too.

So, in summary, if you are dealing with a DDoS attack on your servers and don't know what to do, call dosarrest.com. Tell 'em Brett Brewer sent you. I won't say they are cheap, but I will say that if your business lives and dies by its web site, there is no substitute for the kind of service they provide. They are the real deal.