DOSarrest Internet security

DOSarrest CASE STUDY

DOSarrest restores Virgin Gaming's international gaming community

When people who love to play Xbox 360® and PlayStation® 3 video games want to connect, they turn to Virgin Gaming. At Virgingaming.com console game enthusiasts can set up tournaments and leagues, challenge each other in ladders, and play for cash, points and prizes. Introduced through a partnership with WorldGaming.com, Virgin Gaming provides the secure backend required to facilitate payment and automatically validate results while nourishing a community of gamers of all skill levels from around the world.

WHAT WENT WRONG

On June 11, 2012 at 9:30pm a wave of distributed denial of service attacks was aimed at Virgin Gaming's servers. They have experienced DDoS attacks in the past, but this one was unlike any they had seen before:

- it was more sophisticated than prior attacks;
- it was aimed directly at TCP port 80;
- it was big with over a million unique IP addresses engaged in the attack.

"We've been a big supporter of DOSarrest since we've started using the product and we have recommended the service on multiple occasions."

Ijaaz A. Ullah
Vice President
IT Operations at
Virgin Gaming

It is significant that the attack was aimed directly at TCP port 80 because previous attacks had only targeted UDP port 7. While DDoS attacks are never convenient, when it targets UDP port 7 the port can be blocked relatively easily, effectively turning off the flood of traffic that is pouring into the server and minimizing the effect of the attack. Because UDP port 7 controls a non-essential function, it can be shut down temporarily and end users can continue to access the site.

In this case, however, the attack targeted TCP port 80, which is the same port by which end users access the website. Blocking port 80 would mean shutting down the website. So this was not a viable alternative for mitigating the attack.

As it happened, this particular attack was so large that it overwhelmed Virgin Gaming's ISP's network, and knocked virgingaming.com offline almost immediately. By 4:30am, seven hours into the attack, the traffic reached a volume of 3 Gbps on the ISP's network, and the ISP took the drastic and costly measure of completely blocking the HTTP and HTTPS ports (ports 80 and 443). End users were completely shut out.

CALLING IN THE EXPERTS

Ten hours into the attack with no end in sight, Virgin Gaming convened a working group to discuss strategies for mitigating the attack. It was 7:00am. The working group elected to find a DDoS protection or proxying service. After a couple of hours of research, speaking to colleagues, and soliciting quotes from several providers, the group made the decision to work with DOSarrest. This decision was based on three factors:

- Fastest response to quote request: Within 6 minutes of emailing the DOSarrest sales team a security engineer was on the phone with Virgin Gaming's team.
- Quick resolution guaranteed: DOSarrest promised that within minutes of payment, the proxying service would be engaged.
- Most competitive price: DOSarrest's price was considerably more appealing than that of its competitors.

The ISP agreed to manage the contract with DOSarrest and relay the costs to Virgin Gaming to ensure that the 24 hour NOC would be available to support DOSarrest's efforts if needed.

RESOLVING THE ISSUE

By 10:51am the DOSarrest contract was approved, it was paid for at 11:14am and by 11:35am the Virgin Gaming DNS was updated to point all traffic to DOSarrest's proxying servers, instantly relieving the ISP of the massive traffic of the attack and allowing them to unblock the ports that took the website offline. Virgin Gaming was back online and functioning normally in just over 20 minutes of issuing payment.

From that moment onward Virgin Gaming's traffic doesn't touch the Virgin Gaming servers until it first passes through DOSarrest's scrubbing nodes. Using a variety of proprietary techniques and software augmented by a stellar team of hands-on security engineers, DOSarrest analyzes every bit of traffic and discards what is not legitimate, sending only the clean and legitimate traffic through to Virgin Gaming's servers. Attack traffic is rendered completely useless and has not succeeded in destabilizing Virgin Gaming's site since.

RESOLVING THE ISSUE

Awesome visibility

Since migrating to DOSarrest, Virgin Gaming has access to DOSarrest Security Service, a secure customer panel which displays a variety of charts and graphs of the traffic patterns relating to the Virgin Gaming website. Through this panel the Virgin Gaming team have seen regular DDoS attacks launched against virgingaming.com. But thanks to DOSarrest's service, there is no other indication that the attack has occurred. The website remains online and performing at its usual high standard.

Extreme support

When the operations team needs to contact DOSarrest support they have been met with an unusually high calibre of expertise on the phone. Expert security engineers answer the phones and resolve issues all day, every day.

Rating from 1 – 10

From Ijaaz A. Ullah, Vice President, IT Operations at Virgin Gaming:
"Our operations group loves this service, as it has helped mitigate a significant outage and continues to do so."