

# Online Gaming Site Security Is a Sure Thing with Corero's IPS

## Summary

**Industry:** Online gaming

**Challenge:** Immediately, to thwart extortionists threatening DDoS; long-term, protect the company against attacks that could quickly drive away customers

**Solution:** Corero's IPS/DDoS Defense solution

**Results:** The online gaming company enjoys comprehensive, on-premises protection against DDoS and other malicious attacks, enabling network security and uninterrupted business continuity.

## Key Benefits

- Stops advanced threats out of the box
- Outstanding performance; lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks, malware, spyware, viruses and botnets
- Compatible with distributed networking architecture

*An online wagering site handles thousands of predominantly sports-related online wagers daily. While the visitors are from around the world, most originate in the United States and Western Europe. Customers are able to place wagers on sports events as well as participating in other games of skill and chance, such as poker and blackjack, via the Internet. As part of an increasingly disturbing trend among similar offshore sites, this wagering site was recently targeted by a cyber-threat:*

"We'll take your network down unless US\$30,000 is wired to a foreign country within a week."

Many threatened sites have chosen to pay the ransom rather than suffer the attack. This site decided to put Corero Network Security's [formerly Top Layer Security] DDoS Defense technology in place to protect it from this and future threats and avoid the "payer" tag in the industry.

## The Challenge

For the most part, typical users of online wagering sites have little loyalty and do not build up equity with a particular site. For this reason, providing rapid response, quick payout and very good service are essential to ensure customer retention. It is essential to the bottom line that the site remains available and responsive at all times, particularly during times of increased wagering such as weekends and high-profile sporting events. Highly organized criminal blackmailers target these organizations, and seem to understand the business well. They have devised attacks with a well-considered economic and technical approach, and their timing demonstrates a keen understanding of this particular industry's metrics.

As is typical, the perpetrators initially unleashed a warning attack against the site to provide credibility for their threat. These initial attacks are typically SYN Flood based, sufficiently controlled so as not to take the site down, but significant enough to alert the site owner that the threat is serious. With the Thanksgiving holiday weekend approaching (a time of very active online wagering) a peak revenue period for the site was in jeopardy. The attack was followed with a demand threatening a full attack unless a ransom was wired to their intermediary within 24 to 48 hours. The attackers seemed aware of several important things:

- Typical mitigation solutions would cost approximately twice the amount demanded
- Deploying traditional measures would take longer than the attack window
- A peak time of revenue generation was imminent
- Existing in-place technology would not provide the level of protection necessary to thwart the attack

The attackers take a carefully planned approach that puts them in a position likely to be paid off – setting their ransom just high enough to make it worthwhile, but not so high that victims consider implementing a technology solution that would be, in the short term, costlier in time and money.

Generally in the online wagering community, these attackers have the reputation of keeping their word; that is, when paid off they will forgo an attack and move to a different target. There is, of course, a risk in paying the demands – one risks being marked as a “payer”, getting a reputation for responding favorably to such demands, leaving oneself open to further attacks by other groups. Another gaming site initially refused to pay, was attacked mercilessly and is now on a “monthly payment plan.”

The potential for lost revenue is huge. For many online businesses, short outages do not drive the customer base away in droves. However, with online wagering sites, the ability to bet immediately and in real-time is essential, especially with the highly volatile nature of the “line” or “spread”, which can vary in real-time depending on the value of wagers placed. If a wager cannot successfully be placed at the site of choice, the bettor will immediately place their bets at another online site. Generally, these are customers will not return, so future revenue from them is also lost. Unfortunately, many wagering site owners make the mistake of thinking it worthwhile to pay the ransom and move on with their business uninterrupted – but that is a very temporary and dangerous approach.

In this instance, the site administrator ignored the payment requests while seeking security solutions. The SYN Flood attacks designed to slow the system continued, with the hours before the promised “full attack” ticking away.

## The Solution

The company had to install a solution in very short order; they needed protection immediately and did not have the time for proper planning and analysis. Corero’s DDoS Defense technology is inherently designed with enough flexibility that it can be installed immediately and fine-tuned while installed and active.

The initial installation was completed rapidly, and fine-tuning and configuration of the solution by emergency support brought in was accomplished in two hours.

Prior to the peak transaction period, the DDoS Defense solution performed optimally, dropping malicious packets from the warning attack and passing legitimate traffic. The SYN flood attacks ceased their effectiveness. When they failed to receive their ransom, the attackers unleashed their full attack on Thanksgiving morning. The site administrator contacted the 24x7x365 Support Center and a support engineer logged into the system to monitor the appliance. The appliance was performing admirably, fending off the furious attack, which consisted of distributed SYN Floods and UDP Floods. The appliance was able to keep the gaming site up and operational. However, the criminals seemed to be monitoring the site for the effectiveness of their attack. When they realized they were not

having an impact, they switched their attack methodology to other modes of attack, including ICMP floods.

These attackers are quite adaptive, using a full range of attacks including:

- Distributed SYN Floods (up to 50 MB/second)
- Single-source SYN Floods (using multiple servers)
- UDP Floods
- NB-Gets
- ICMP Ping Floods
- UDP Fragment Attacks

## The Results

The wagering site has not experienced any downtime due to malicious attacks since installing the Corero solution. Corero has improved network reliability and availability dramatically, enabling rapid processing of online wagers and improving the bottom line, with little worry about additional attacks. Not willing to be at the mercy of these criminals, and understanding that attacks could evolve further, the technical team at the wagering site took this unfortunate event as an opportunity to insulate their network infrastructure and implement a comprehensive security strategy that includes proactive, always-on intrusion prevention with Corero’s IPS.

The IPS has performed very well, not only protecting against the known attacks but also bringing a number of previously undiscovered attacks and exploratory probes to the team’s attention. Additionally, Corero’s IPS goes beyond blocking to provide detailed visibility into all types of attacks such as attack origins, attack types, and also facilitated comprehensive reporting and extensive logging (for law enforcement purposes.)

A critical unsung benefit beyond the elimination of malicious traffic is the reduction in load on the servers managing the wagering applications. No longer does the Web server need to sift through extraneous packets. This greatly reduces the strain on the Web server, improving both efficiency and throughput. This solid operation keeps customers satisfied and returning to the site for their wagering. Corero’s solution has not only provided reliable protection for the site’s network infrastructure, but is actively protecting the site’s bottom line.

## About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprise organizations rely on Corero to protect their critical online assets against risks associated with network-borne cyberthreats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with offices worldwide. [www.corero.com](http://www.corero.com).

---

### Corporate Headquarters

1 Cabot Road  
Hudson, MA 01749  
Phone: +1.978.212.1500  
Fax: +1.978.212.1600  
[www.corero.com](http://www.corero.com)

### EMEA Headquarters

No.1 Cornhill  
London  
EC3V 3ND  
Phone: +44 (0) 203 427 3407

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.