IMPERVA®

CASE STUDY



Protecting a Social Trading Platform from DDoS Attacks

How Incapsula protected eToro's trading environment from recurring DDos attacks.

eToro

The Business & Technical Challenge

As an online trading company, eToro operates in a complex environment: through the use of HTTP/HTTPS sites, Flash applications, and proprietary API's (both web-based and application-based), the company processes thousands of transactions every minute. eToro's trading infrastructure is a highly available and redundant environment built to sustain failure and ensure system uptime for all its users worldwide.

In July 2012 the company experienced network DDoS attacks that were causing repetitive availability issues on the trading systems. The company's IT department, together with their hosting provider, attempted to deal with these attacks. This required a significant amount of time and human resources, which shifted focus from other critical system support tasks, despite not fully mitigating the attacks.

Johnathan Assia, CEO: "As the largest social trading community today, with millions of people trading at any given time, our company cannot afford the slightest disruption to our service. We started looking for a solution that could not only mitigate all DDoS attacks, but also handle our multiple environments (HTTP/S, Flash and proprietary API's). Since we process financial transactions, we required a service that would be PCICompliant, but more importantly would be transparent such that it would not impact our traders' user experience even when undergoing a DDoS attack. It was also imperative that we work with a provider that could support us 24x7 and get us setup quickly".

The Solution

With multiple websites, trading systems and proprietary API's, implementing Incapsula had to be done quickly but carefully, to make sure that eToro would not experience any downtime during the process.

Gur Shatz, Incapsula CEO: "As Incapsula has vast experience protecting social platforms, financial companies and online trading systems, we were able to get eToro on the service relatively quickly. We immediately detected that eToro was suffering from both network (Layer 3 & 4) and application (Layer 7) DDoS attacks that were causing system instability.

Once on the service, we were able to absorb all the attack traffic with our network's backbone and filter the applicative attacks too. We relied heavily on our bot detection and progressive DDoS challenge technology, to block 100% of attackers transparently, without affecting any real users."

Website
eToro.com, openbook.etoro.com

Industry
Social Trading

Founded
2007

Registered Users
2.75 million

Number of websites
25

CEO
Johnathan Assia

Company Background
eToro empowers more than 2.75 million users in more than 140 countries worldwide to trade currencies, commodities and stocks through an innovative online and mobile investment platform and an active trading community, with thousands of new accounts created every day.

Results and Benefits

Incapsula is now an important component of eToro's security infrastructure. When under DDoS, traffic is routed through Incapsula for screening, where malicious traffic and DDOS attacks are blocked automatically.

eToro is taking advantage of Incapsula DDoS Protection key benefits, to secure its online properties:

information such as the targeted URL and the threat pattern that triggered the violation. A high-level dashboard shows security, performance, and configuration information.

With Imperva Incapsula, Keystone is protected against future Web and DDoS attacks. For Keystone, Imperva Incapsula was cost-effective and easy to roll out–Keystone's security personnel just had to complete a short provisioning form and contact the company's DNS hosting provider to update DNS settings. From Widman's perspective, "Every aspect of the service has been stellar."

- **Protection against Network and Application Level Attacks**
  Through a worldwide network of multi-gigabit scrubbing centers and bot detection technology, Incapsula provides an on-demand complete protection for both network (Layer 3 & 4) and application level (Layer 7) DDoS attacks.
- **No Annoying Delay or CAPCHA Screens, and Less than 0.1%False Positives**
  Incapsula unique escalated challenge and bot detection technology ensures that while under attack, legitimate visitors are not delayed or denied access to the site and therefore the user experience remains unaffected.
- **24x7 Managed Security Service**
  Incapsula DDoS security team monitors attacks and is available on-demand before, during or after attacks to ensure your site is up and running and performing optimally.

"With Incapsula, we are able to focus on managing our business: the world's largest investment network. Incapsula handles all the network and application DDoS attacks that impact our uptime and availability. When it comes to DDoS attacks, support is one of the most important factors is choosing a service. Incapsula provides us with fantastic 24x7 support. We know that if something goes wrong, they are available. Their experience in protecting financial institutes and online trading companies is clearly apparent, and I'm happy that we have made the right choice."

JOHNATHAN ASSIA, CEO, ETORO

© 2018, Imperva, Inc. All rights reserved. Imperva, the Imperva logo, SecureSphere, Incapsula, CounterBreach and ThreatRadar are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders.