corero
FIRST LINE OF DEFENSE

JAGEX DROPS THE WARHAMMER AGAINST DDOS WITH CORERO

SUMMARY

INDUSTRY
Online gaming

CHALLENGE
DDoS attacks lead to system slowdown or in some cases outages in service for players in the performance-sensitive online gaming industry. Jagex needed a solution to handle the frequent, intense DDoS attacks it was encountering in its five data centres in the United States and Europe, without causing any disruption to customers' gaming experiences. With attackers changing their DDoS attack techniques in rapid fashion, Jagex required a solution that could automatically detect these emerging attacks and mitigate in real-time, immediately eliminating the DDoS challenge to their sensitive environment.

SOLUTION
Corero's SmartWall® Threat Defense System, SecureWatch® Analytics and SecureWatch® PLUS service

RESULTS
Up to 95% of DDoS attacks are absorbed completely with zero impact on player experience whatsoever.

KEY BENEFITS
- Attacks are blocked before they can cause disruption to players' gaming sessions
- DDoS mitigation is automatic and in real-time, eliminating costly human analysis and configuration of countermeasures
- Jagex's reputation and revenue streams are enhanced when customers have full and continuous access to online games
- Utilizing the SecureWatch PLUS service, Jagex and Corero work together to constantly fine tune the solution to adapt in a dynamic and evolving threat environment

Cambridge based Jagex Games Studio is a multi award-winning games developer and publisher of popular gaming communities like Runescape and War of Legends. With 450 staff onsite serving more than 3 million unique users per month, it is the largest independent games company in Europe and has built a global reputation for developing hugely popular, accessible, free-to-play games along with providing an unbeatable community experience for millions of players around the world. Jagex operates five major datacentres in the US and Europe in order to keep its global online communities running 24/7. Possibly more so than other industries, online gamers are extremely sensitive to system performance and responsiveness. Such a demanding customer base makes it imperative to the business that these communities remain available and online, otherwise Jagex risks losing customer confidence and, ultimately, revenue.

CHALLENGE

The Internet driven business understands that revenue generation relies heavily on system and service availability, and the impact of DDoS attacks can be incredibly costly when systems, applications or platforms fall victim to attack. This is especially true of the online gaming industry where any downtime equates to a drop in visitors. Jagex had been experiencing an increase in attacks for a number of reasons; including banning a small number of known DDoSers, which prompted more attacks, attacks driven for pure attention seeking purposes and those looking for bragging rights. While each of these motivations may seem like small time nuisances to a business that relies on player accessibility, they pose a serious challenge to game availability that is actually the lifeblood of the organisation.

In addition, extortion attempts targeting Jagex were starting to become more commonplace. One instance saw bad actors taking to Twitter, threatening to take down the site unless Jagex paid their ransom requests. Extortion wasn't always the primary driver for DDoS attack activity; some extremist gamers threatened the company with DDoS unless they succumbed to making changes to the game itself. These instances are nothing new to the industry, but illustrations of what Barry Zubel, Head of IT at Jagex, and his team deal with on a day to day basis.

"These days, it is ridiculously cheap to hire a botnet to be used in a DDoS attack," Zubel said. "It's a never-ending race for us to keep up with the kind of capacity attackers can easily get hold of- it costs us a lot more to keep up, and costs attackers very little to execute DDoS attacks."

In fact, historically the average bandwidth needed for Jagex to operate daily and fulfil its consumer obligations is only half of one percent of the total capacity of the datacentres. While that may seem like an excessive overage, these are the infrastructure decisions Internet-facing businesses have been faced with when keeping up with the DDoS threat in order to meet consumer demands and remain competitive in the marketplace.

Zubel also knows that it's not solely about the large, volumetric DDoS attacks - sub saturation attacks that probe the network in attempt to uncover weak spots in security defenses make up the majority of DDoS attacks on

Jagex. "We currently see 300-400 non-critical attacks on our infrastructure per month, and that's being conservative," Zubel explained. "For the IT personnel, that could mean ten or more call outs per day for a 24/7 service, which of course also meant paying staff around the clock."

It became abundantly clear that an alternative to defeating their DDoS challenge was needed after the New Year in 2013, when attackers used NTP reflection attacks in attempt to take down every major gaming site in the world and managed to throw all Jagex datacentres offline simultaneously. With five main datacentres scattered throughout the US and Europe, Zubel realised that the legacy DDoS mitigation solution Jagex was using was not cutting it in terms of performing to specifications. The legacy solution was based on time-consuming reactive policies in an industry that demands proactive defense measures, and the ability to anticipate the adversary's next move. As such, he sought out a solution that would combine DDoS protection that had the capacity to mitigate the demanding volumes and frequency of attack traffic, but also provide sophisticated DDoS event intelligence that would allow him to keep on top of the constantly emerging new threat vectors.

THE SOLUTION

After an initial proof of concept trial in its London datacentre, Jagex made the decision to roll out the Corero SmartWall® Threat Defense System (TDS) in all of its five major datacentres worldwide. The Corero SmartWall TDS is a purpose-built family of network security appliances designed to eliminate DDoS attacks in real-time through on-premises, rapidly scalable high performing deployments. Included with the purchase of SmartWall TDS, is the Corero SecureWatch® Analytics, powered by Splunk. "With Corero, we get the whole package," said Zubel. "Attack vectors are changing all the time, so dynamic protection is important for us. We get more visibility with SmartWall TDS and SecureWatch - it's more than just knowing that we are under attack. Corero has offered us a solution that is an intelligence tool as much as a DDoS mitigation tool." Jagex evaluated other options to solve their DDoS problem as well. Alternative solutions didn't stand up to Corero's SmartWall TDS, based on the effectiveness of their technology. Corero ultimately persevered based on the ability to provide instantaneous mitigation, robust reporting and analytics, and the ability to scale incrementally based on the demands of Jagex's business.

> "We can now absorb roughly 95% of all DDoS attacks made on our systems with zero impact to our services, which means customers are getting a much more seamless experience,"
>
> - Barry Zubel
> Head of IT at Jagex

In addition, Jagex works closely with the Corero Security Operations team via the SecureWatch PLUS Service complimenting and enhancing the internal resources with the knowledge and experience Corero provides.

Zubel highlighted the significance of working with Corero, using the intelligence the solution provides to solve Jagex's DDoS problems. For example, as a result of the lessons learned from the NTP reflection attacks, Corero provided the expertise to help Jagex recognise and set up mitigation for other types of reflection attacks such as SSDP reflection attacks that amplify packets by leveraging a vulnerability in the implementation of the Simple Service Discovery Protocol that is a component of universal plug-and-play (uPnP) in many consumer cable modem and wireless routers, whereby these devices can be coerced into responding to spoofed record requests to deliver a torrent of traffic against a DDoS victim.

"Without the intelligence aspect of the analytics and reporting capabilities through updates via email, or in particularly urgent cases, a phone call, we couldn't identify all of these different sore points. They help us by flagging potential issues and we can discuss what it actually means to the business in order to help prioritise issues and fine tune solutions to problems," explained Zubel.

> "Attack vectors are changing all the time, so dynamic protection is important for us. We get more visibility with SmartWall TDS and SecureWatch - it's more than just knowing that we are under attack. Corero has offered us a solution that is an intelligence tool as much as a DDoS mitigation tool."
>
> - Barry Zubel
> Head of IT at Jagex

THE RESULTS

Now with the Corero SmartWall TDS solution in place, Jagex can absorb any DDoS attack up to 400% of its normal daily capacity and keep all services to users running smoothly without any disruptions. This has led to an immediate decrease in customer-impacting DDoS events and better retention of existing customers.

"We can now absorb roughly 95% of all DDoS attacks made on our systems with zero impact to our services, which means customers are getting a much more seamless experience," said Zubel. "That in itself is a huge result for us."

The unique product design also means that Jagex is able to scale the solution incrementally as it increases the bandwidth within its datacentres. And because the solution comes backed with Corero intelligence, the risk to Jagex's business is reduced and response time is quicker.

"We experience around ten attacks per day," said Zubel. "That could mean costly call outs for IT staff who would have to be available around the clock. Without Corero, we might need to increase head count by 200% or more to deal with the problems and ultimately it still most likely wouldn't be as effective as the Corero solution."

ABOUT CORERO NETWORK SECURITY

Corero Network Security, an organization's First Line of Defense® against DDoS attacks and cyber threats, is a pioneer in global network security. Corero products and services provide Online Enterprises, Service Providers, Hosting Providers and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. For more information, visit www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749 USA
Phone: +1.978.212.1500
Web: www.corero.com

EMEA Headquarters
Regus House, Highbridge, Oxford Road
Uxbridge, England
UB8 1HR, UK
Phone: +44.0.1895.876579