Major US online gaming company mitigates sophisticated DDoS attack with Comcast Business.

Advanced capabilities paired with a tested cybersecurity response and strategy save a large US online gaming organization significant business downtime and financial losses.

Situation

- The online entertainment and gaming industries are proliferating; there are many alternatives, and competition is fierce.
- If web properties are unavailable to customers, the competition is only a few clicks away.
- For an online gaming company, any downtime in the company's digital infrastructure can impact the customer experience and results in direct, sizable revenue losses.
- Therefore, its network, servers, and applications are critical to its day-to-day operations and long-term revenue opportunities.

Challenge

- A major online gaming company in the licensed gaming and entertainment industry came under a large-scale, sophisticated DDoS attack, with a peak traffic volume of 400 gigabytes per second.
- The perpetrators deployed sustained, multi-pronged approaches resulting in one of the most significant and most challenging attacks ever seen by Comcast Business, requiring equally sophisticated detection, response, and adaptation capabilities for DDoS attack mitigation.

Solution

- Emergency DDoS Mitigation Service
- Managed Security Services

Results

- With the Comcast Business cybersecurity team's help and expertise, this major online gaming company was able to recover control of its operations in under 72 hours.
- The company avoided prolonged losses in revenue due to downtime.
- Comcast Business' swift mitigation efforts helped to minimized monetary, operational, and reputational damages.

Meeting players wherever they are

A substantial online gaming division and subsidiary of a large American corporation with thousands of employees plays a significant role in the licensed gaming and entertainment industry in the United States and globally. Creating cross-platform and cutting-edge games, it prides itself on crafting and deploying dynamic content wherever its players are across diverse channels and technology.

As the gaming industry continues its tremendous growth, new technologies and connectivity play a crucial role in this success. Any online gaming organization critically depends on its network, servers, and applications for successful daily operations and revenue generation.

Anatomy of a complex DDoS attack

After reviewing firewall and application server logs, this major online gaming company discovered it was under a severe DDoS (distributed denial of service) attack in the late summer of 2022. With a peak traffic volume of 400 gigabytes per second, the incident is one of the largest and most complex multi-vector DDoS attacks seen in 2022 by Comcast Business. In comparison, the most significant attacks ever recorded worldwide have exceeded one terabyte per second.

The DDoS attacks targeted many of our customer's IP addresses and saturated their circuit bandwidth, making its online gaming services unavailable. While the attack targeted a broad range of customer IP addresses, a technique commonly known as "carpet bombing," most malicious traffic targeted a single IP address. Over time, the attacks grew in intensity and became more complex, using combinations of up to 30 different advanced DDoS techniques that generated hundreds of high-severity alerts, including:

- Multiple User Datagram Protocol (UDP) amplification attacks — a standard method used against gaming companies employing the UDP protocol on gaming servers
- Complex Transmission Control Protocol (TCP) attacks
- Randomized UDP and TCP protocols and windows
- SYN flood attacks
- Carpet bombing

COMCAST BUSINESS

Evolving solutions for evolving threats

In the face of a severe attack, the online gaming company called the Comcast Customer Security Assurance (CSA) hotline for help with Emergency DDoS mitigation.

Within minutes of taking the customer's call, Comcast Business' cybersecurity team responded to the incident by implementing the Commercial DDoS mitigation service and taking additional steps, including:

- Customized DDoS mitigation countermeasures
- Geo-blocking controls
- Advanced filter lists to block known Botnet sources
- Traffic shaping restrictions

As Comcast Business initiated different DDoS mitigation countermeasures to defeat the multi-vector attacks, the perpetrators responded by modifying their attack techniques and procedures. For example, while at first the attacks originated from IP addresses in China, they relocated attack resources to the United States after Comcast Business successfully blocked the Chinese botnet. Three days of attacks resulted in a sophisticated cat-and-mouse game between Comcast Business defenders and the DDoS attackers.

Maximizing opportunity, minimizing risk

Following the successful Emergency DDoS Mitigation Services incident response by Comcast Business, this major online gaming company confirmed that all of its applications were up and running as expected, including customer-facing services, internal employee portals, VPN connections, and third-party affiliate systems.

Comcast Business' cybersecurity division sprang into action with remarkable speed and expertise, successfully mitigating the DDoS attack in under 72 hours. This swift response not only prevented substantial revenue loss that would result from downtime, but it also significantly reduced the time required for remediation and protected the gaming company's reputations.

Without a cybersecurity contingency plan and a large-scale partner with sophisticated capabilities such as Comcast Business, many modern enterprises risk more devastating operational and financial damages as connectivity brings both new challenges and new opportunities across industries.

Following the successful Emergency DDoS Mitigation Services incident response by Comcast Business, this major online gaming company's applications were up and running as expected.

© Comcast 2023. All rights reserved. CAS91666-D_9.23