Nokia Deepfield Defender helps an online gaming company detect DDoS attacks more accurately and protect its customers

Use case

To remain competitive, online gaming companies need to create cutting-edge gaming content that engages and captivates millions of avid players. Large, webscale gaming companies build excitement by rolling out new releases of their most popular games to worldwide audiences at pre-announced times. This brings millions of players online at the same time to compete for global bragging rights. Winners are determined based on play that lasts hours a day for weeks at a time. Some gaming events feature online finals that bring significant cash prizes to winners.

The peak online gaming hours associated with highly anticipated new releases generate significant traffic surges. They often also attract a surge of distributed denial of service (DDoS) attacks aimed at bringing the gaming company's services down. These DDoS attacks can have a devastating effect on the company's customers and business. Shutting down the attacks without disrupting the service for its customers becomes a mission-critical issue.

Challenge

To handle the increased network load generated by so many online gamers, one webscale gaming company stores its content on multiple servers distributed across several geographically dispersed data centers. During a recent season premiere of a popular game, the company's legacy hardware-based DDoS protection solution failed to detect multiple concurrent, multi-vector attacks that were occurring across its distributed cloud infrastructure. The volume and sophistication of these attacks took one server offline and disrupted service for a very large number of players.

This happened because the company's hardware-based DDoS solution returned a flood of false positives (identifying legitimate traffic flows as DDoS attacks) and false negatives (failing to detect the real DDoS attacks by treating the DDoS traffic as legitimate). This inability to accurately detect DDoS attacks resulted in many 'misfired' or uninitiated mitigation processes, and left many customers without service for hours.

Frustrated gamers saturated the gaming company's call centers, demanding refunds. Others turned to the internet with complaints that aimed to tarnish the company's reputation.

Solution

The gaming company deployed Deepfield Defender to overcome its existing DDoS security challenges and provide protection against a new generation of terabit-scale DDoS attacks. Deepfield Defender detects DDoS attacks as they happen by combining advanced, real-time network analytics focused on DDoS security with unique security-related insight obtained from the internet.

The solution provides DDoS analytics based on advanced heuristics with ratio-based monitoring of IP flows and protocols used for DDoS attacks. These capabilities are enhanced with Deepfield Secure Genome, a unique, constantly monitored and updated database that contains security-related information about of billions of internet endpoints and data flows. It sorts this information into categories and arranges it to create DDoS-related whitelists and blacklists. The result is holistic visibility that can decipher DDoS attacks and all associated flows and allow for precise, real-time mitigation. Deepfield Defender keeps the gaming company's network secure even if an attacker combines many hijacked IoT devices and different cloud servers to create multi-vector, multi-endpoint attacks.

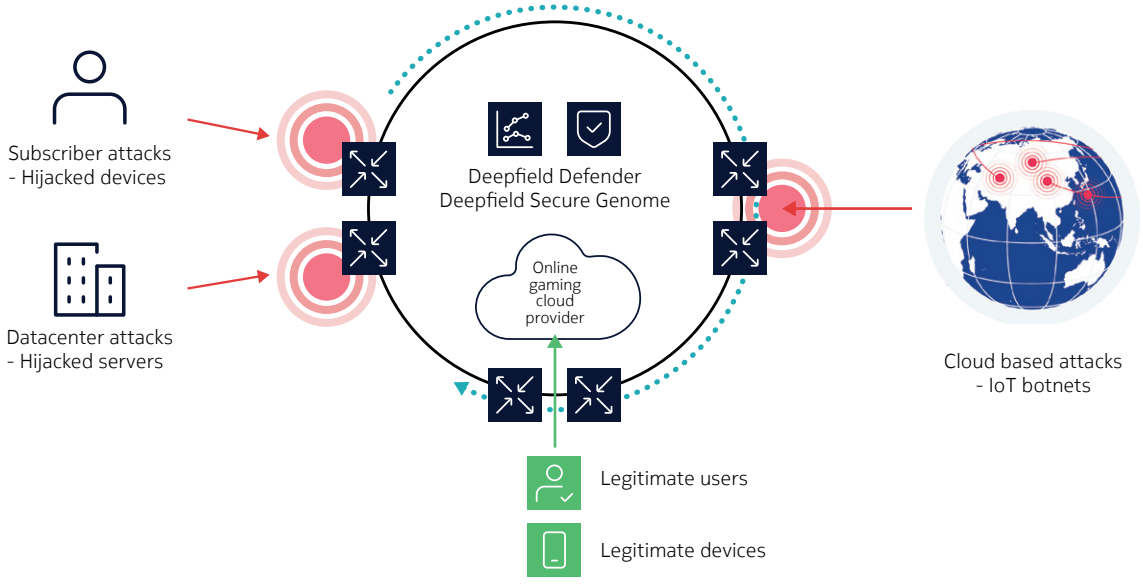
Benefits

Deepfield allows the gaming company to see the composition of every DDoS attack and detect suspicious network activity in real time. The company can use the insight obtained from Deepfield Defender to quickly discard false positives and false negatives. This insight can support efficient mitigation even when attack vectors are changing as the attacks unfold.

With Deepfield Defender, the gaming company has significantly increased its resilience against DDoS threats. It has also neutralized DDoS attacks that accompanied several of its subsequent game releases so that those attacks had no effect on the company's customers. As a result, customer confidence, satisfaction and loyalty have risen dramatically, as has the company's online reputation.

Deepfield Defender detects DDoS attacks in real time by combining advanced network analytics with unique, security-related insight.

Deepfield Defender accurately detects DDoS attacks as they happen



About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID201237 (May)