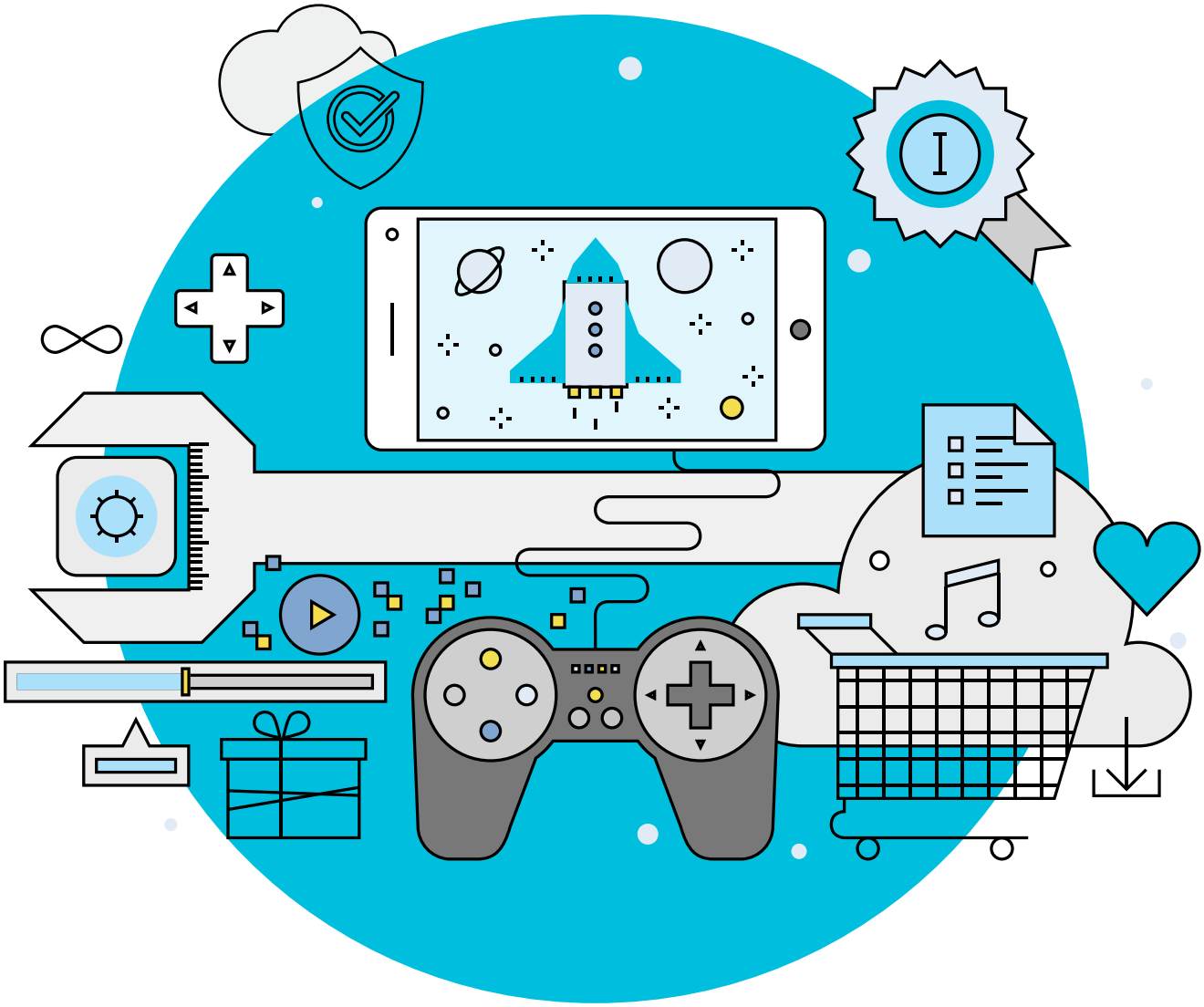
Alibaba Cloud
aliyun.com

Combating **Online Gaming** Vulnerabilities with **Cloud Security**



Index

01 The Online Gaming Landscape

Online games have been around since the 1970s. Over the years they have proliferated to include single and multiplayer games played on mobile devices and tablets through the Internet. Multiplayer games are popularly referred to as Massively Multiplayer Online (MMO) games, and are also the most played category of online games. These include role-playing, strategy, and first-person shooting MMOs.

The online gaming culture has however faced sizeable criticism for fostering what is seen as an aggressive environment that has potential links to violence, cyber-bullying, and racial hate. Online games also face social criticism as they are highly addictive, and are even known to lead highly immersed gamers to abandon interacting in the real world.

Despite criticism, online gaming and especially MMOs have grown rapidly into a multi-billion dollar industry. Major MMOs are essentially a business enterprise in itself, the success of which depends on multiple stakeholders, including players, game creators, and investors.

While the lifetime of single player games typically ranges from several weeks to several months, successful multiplayer online games can last for years, with new players joining the game years after its release. The online shooter game Counter-Strike, for instance, was released in 1999 and remains to this day one of the most popular shooting games on the Internet. The perpetual success of the game has come despite the multitude of competing games in the shooting genre.

Online games along with related services, including distribution platforms, share characteristics similar to those of online banking and finance websites, and other typical web-based organizations. The common denominator is that the gaming industry faces the same challenges that other industries have faced in the past. Primary concerns include availability of gaming software and hardware infrastructure during traffic periods, defense against cyber-attacks, and information security. DDoS-attacks and database breaches are the two most common recurring attacks that MMOs, game distribution platforms and networks face today.

This whitepaper explores the security landscape for the online gaming industry, including the history of security threats, modern categories of attacks, as well as the motivations for attackers. We cover the traditional response of gaming companies to counter security threats and discuss what needs to be done to keep attackers at bay. Finally, we consider Alibaba Cloud Gaming Solutions for gaming companies, along with the unique advantages of these solutions.

02 Why Security is Important to Online Gaming

The online gaming industry is expanding rapidly each year. Projections on the MMO market reveal potential for the industry to reach USD$31 billion in total value in 2017, up from USD$24.4 billion in 2014.

Such phenomenal growth is not without its perils, as cyber criminals, hackers, and scammers seek potential opportunities to exploit the industry and steal revenue. Alarming for game providers is the fact that the same procedures used to hack online banks and healthcare records work for hacking into online games. As per a report by Statista, in the second half of 2016, 57 percent of DDoS attack traffic globally was directed at the gaming industry. What's more, the gaming industry has been slower than other industries to acknowledge the serious threat of cyber-attacks, leaving many games exposed and at the mercy of attackers. With high growth in the user base of online games, the need to adequately secure online virtual worlds has become imperative for the livelihood of the industry.

To explain the long-term success of MMOs, one needs to understand player psychology. Players remain loyal to an online game while it is safe and successful. This is where cheating can prove to be a huge deal-breaker for both players and games, as it affects user retention. For gamers, it's hard to enjoy the game if other players are known to be cheating. An unfair playing field achieved through illegal means can kill the average player's interest in the game. Players can be made to feel betrayed and are more likely to quit and move on to another game. Thus, one of the key challenges for gaming companies is dealing with anything that provokes unfairness and exploits vulnerabilities in the game's architecture. Maintaining a sense of justice and fairness is essential to encouraging continued involvement in the game.

2.1 Architecture Vulnerabilities

As a consequence of managing a vast user base of game players, gaming providers are forced to deploy complex architectures. MMOs rely extensively on sophisticated software, built on massive distributed client-server architectures, to deal with the real-time interaction of thousands of concurrent users. These games have no choice but to push the limits of software technology.

The biggest developmental challenge for World of Warcraft, for example, is sharing in-game information (about players, levels, and various other features) with hundreds of thousands of client programs running all at once. When a standard server processes a high number of simultaneous requests in real-time, the probability of a DDoS attacks is greater. This can be a serious threat, as DDoS attacks can cost companies on average an estimated USD$40,000 per hour, as per the Incapsula Survey: What DDoS Attacks Really Cost Businesses.

Compromised game servers can have severe consequences for gamers, as well as for developers. The prime concern for gamers is their personal systems being at a risk when connected to insecure game servers. Hackers, for example,

can breach and take control of a user's personal system by exploiting network vulnerabilities. Hackers use this access to attack other systems, install malicious software and gain access to data on the compromised system. The damage in such instances is not restricted to the user's game account, as the attacker can corrupt or potentially delete the user's online presence as well.

For developers, compromised game servers can result in an indefinite crashing of the game. This adversely affects the gaming company's brand value and erodes consumer confidence in its services.

2.2 Virtual Theft

Inside the virtual worlds of MMOs, players accumulate numerous items that have significant value within the game. Players can trade virtual resources such as money (in-game currency), and other products and items integrated into the gameplay. Players can buy resources with real currency in order to boost their performance or experience within the game. Games with thousands of users are thus hosting virtual gaming economies worth millions of dollars. Note also that a connection exists between the virtual economy of the game and the real world economy. In fact, there are companies that make millions of dollars each month by ensuring the monetization of gameplay, through currency exchange and the sale of virtual items. As a result, it is possible to monetize illegal activities such as cheating and hacking to acquire virtual items. Hackers, upon gaining access to a user's account, can then do as they please with the virtual resources they have wrongly acquired.

2.3 Personal Information

In today's digital world, it is common for gamers to link game accounts to their personal email address and other contact details. Gamers use their personal banking information too, to make purchases within the game. For gaming providers it is thus essential to preserve and secure sensitive personal data. While some large-scale MMO franchises are in a strong position to secure user information, the existing client-server architecture of other game providers faces severe challenges. Inadequate security is exacerbated by the fact that MMOs tend to have in-game scripted activities as part of the gameplay that occur on the client-side. These actions do not place any restrictions on the speed and number of times the user can repeat them. Such freedom has led to the creation of a large community of underground black hat hackers. These groups subsequently target game players' credentials. Once they break past the game's hardware and software security protection, MMOs are powerless to stop the hackers from possessing entire databases containing players' confidential information. A recent such case effected South Korean company Eyedentity Games, who's MMO Dragon Nest was hacked along with two years worth of stolen player data.

03 Online Gaming Security Threats and Concerns - A Closer Look

Common gaming security threats that online games face today stem from their distribution platform. Take for example Steam, a leading online gaming distribution platform. As a multi-OS platform owned by the company Valve, this gaming market comprises of thousands of games and millions of active members. Steam has suffered from an increasing number of malware attacks, with attackers hacking into millions of user accounts. As per an official report released by Steam data associated with approximately 77,000 Steam accounts per month lands in the hands of hackers and cyber criminals. Common gaming security threats that online games face today stem from their distribution platform. Take for example Steam, a leading online gaming distribution platform. As a multi-OS platform owned by the company Valve, this gaming market comprises of thousands of games and millions of active members. Steam has suffered from an increasing number of malware attacks, with attackers hacking into millions of user accounts. As per an official report released by Steam data associated with approximately 77,000 Steam accounts per month lands in the hands of hackers and cyber criminals.

MMOs that feature online competitive action are dependent on real-time interactions, both player-to-player and player-to-game. Such functionality requires instant response times and absence of latency. A delay of even a millisecond in the execution of a user's request can disrupt the gaming experience. Game availability is of paramount importance to gaming companies for ensuring customer satisfaction. This however makes game providers easy targets for cyber-attacks.

The following section examines in greater detail the most critical security threats and concerns for gaming companies.

3.1 DDoS Attacks

3.1.1 Introduction

A Distributed Denial of Service (DDoS) attack aims to overload a game server with a high volume of requests that it cannot handle. The attacker typically uses multiple computers or DDoS bots to send overwhelming requests, in the hope that the server either slows down to an intolerable level or crashes.

3.1.2 Objective and Impact

The objective and impact is game paralysis. In other words, the game breaks down and is unavailable to players. Game paralysis is an immense problem for gaming companies as the downtime caused by such attacks is not only frustrating for users but also causes irreparable harm to the company's reputation. Gaming enterprises can lose out on millions

in revenue from suspension of the game's services. If the game fails to be up and running again quickly, gamers will lose interest and abandon the game altogether. In fact, gaming servers are one of the most frequent targets for DDoS attacks. The legacy World of Warcraft server Elysium, for example, was hit with six simultaneous DDoS attacks that totally crippled its services.

3.2 Phishing and Spoofing

3.2.1 Introduction

Phishing is used to retrieve information, while spoofing refers to impersonating another party and deceiving users to take actions they wouldn't otherwise make. Spoofing in gaming is typically committed through an email where the impersonator mimics the email design and layout of the game provider, tricking the gamer into believing it is an official mail. Users are then manipulated into clicking fake URLs, or are directed to fake websites.

3.2.2 Objective and Impact

The objective of phishing is to extract user's personal information including game credentials or bank details. Meanwhile, spoofing is intended to trick users into downloading malware that can help the spoofer take over their system or erase data. Social media bots are commonly used to track posts left by gamers. Scammers then target users looking for support and direct them to spoofed websites that prompt them to enter their login credentials, thus giving away confidential information. Scammers once duped millions of Facebook users by running a scam asking users to log into Facebook to try out a new fake "dislike" button. The sophistication of the fake Facebook interface led users to enter their Facebook credentials to log in; unaware that they were a part of a major phishing scam.

3.3 Malicious File Downloads

3.3.1 Introduction

Malware is a frequently used tool by scammers to conduct illegal activities. It is a form of invasive software that can gain access and damage a device without the user's consent. Removing the software from the user's systems is inconvenient and time-intensive.

3.3.2 Objective and Impact

Accessing games and especially MMOs tend to be a download-heavy activity, where gamers are required to install files, patches, game updates and third-party modifications. This being the case, attackers can serve gamers fake and files through the use of malware. Malware has serious consequences, as it hacks into a computer and deletes or steals

important files and data. One of the most dangerous malware is Key-logger, a program that records your keystrokes, and collects and sends this information to a third party server. The attackers can subsequently steal login credentials and credit card details. The biggest challenge faced by gamers, in this case, is recognizing malware in disguise, while not missing official updates.

3.4 Social Engineering

3.4.1 Introduction

While not a new concept, social engineering is an ever-increasing threat to the gaming industry. It involves manipulating a user into voluntarily sharing confidential information. Popular online games, especially MMOs host online communities and forums, where gamers talk, chat, and send instant messages during games to discuss strategies and tactics. These communities offer a platform where malicious individuals can use social engineering to defraud people of their game credentials, in-game virtual resources, and credit card details. Bots are commonly used as well to scam players, by offering gift cards in return for users filling out surveys.

3.4.2 Objective and Impact

The prime objective of scammers is to gain access to insecure computers connected to the Internet. Gamers who are looking for suggestions and techniques are easily influenced into sharing their personal information in exchange for advice that can help them improve their game performance.

3.5 Database Breaches

3.5.1 Introduction

With popular MMOs having subscribers in the excess of millions, there is a lot of data that gaming companies need to secure. There have been instances, including in 2011, where several major databases (reportedly up to 77 million users) owned by Sony were compromised by hackers, including but not limited to the databases used for the PlayStation Network.

3.5.2 Objective and Impact

Once hackers get their hands on user's confidential data, nothing, from the gamers in-game account (including all assets and virtual currency collected over time) to personal information is safe. A recent example is the massive South Korean data breach in 2015, which resulted in the arrest of sixteen hackers linked to hacked data of 27 million people, including 220 million private records. According to Forbes, the breach affected approximately 70% of the population

in South Korea aged between 15 and 65. The scale and impact of this attack signals a clear message to gaming companies, that security should not be taken lightly and they must do all they can to ensure data privacy.

04 Psychology and Motivation Behind Attacks

Many reasons exist behind why individuals or groups attack and disrupt the normal play of online games. These include social, financial, emotional, and tactical reasons. For some hackers, the motivation is purely to cheat the game's value system.

Let's examine each of these motivations in further detail.

4.1 Financial

4.1.1 Introduction

Virtual worlds inside many MMOs possess vast sums of virtual resources, which attract hackers and cyber criminals alike. Given the existence of products and services sold for real currency within the game, there are players more interested in embezzling virtual wealth from the game than playing the actual game itself. Dishonest players accumulate real money by generating fake virtual wealth using specialized software that they commercialize, distribute and convert into money.

Criminals have been found to pay hackers to break into the game's security system to extract account details, which they can later sell for profit. For the hackers, they can either sell the stolen account to the highest bidder or sell virtual in-game resources to other gamers. The industry has entire communities that deal in the sale of virtual resources, and gamers offer easy prey for cyber criminals out to make quick money.

4.1.2 Application

Criminals take advantage of confidential user data such as login credentials and bank details to sell on the Internet. External parties often pay top dollar for user databases, and hence criminals and hackers are motivated to conduct these high-level data breaches.

Gaming companies are suffering as well from the increasing rate of DDoS attacks. Once attackers find vulnerabilities in the game software and deployment architecture, they target that game continuously. If the gaming company is unable to upgrade its security system to deal with the attacks, attackers can demand ransom from the gaming company or threaten further disruption. The gaming companies have few options but to pay up, as regular disruption could put them out of business.

4.2 Social

4.2.1 Introduction

The primary aim for certain hacking groups is to gain attention and showcase their strength. These groups are also known to sell DDoS-as-a-Service software over the Internet. Attacks on games can be used as a marketing stunt and a sales driver for their software solutions.

With gaming being a passionate experience, such interruptions can evoke a strong backlash from users. Hackers can thus achieve their goal of instant online fame from exploiting the emotions of avid game players. A recent DDoS attack on the popular MMO, World of Warcraft, brought the game to a halt in August 2016, delaying its launch, thereby helping the hackers gain instant fame.

Bad blood from games can even spill over into the real world. This is a serious concern for gaming companies as the negative publicity tarnishes the game's reputation.

4.2.2 Application

The behavior of fellow players, especially cheaters in the game, can lead to retaliation. Players may seek out to acquire the personal data of other gamers through hacking to harm or blackmail them. Attackers may even resort to in-game harassment of fellow gamers to force them to quit the game, and then take over their account.

4.3 Emotional

4.3.1 Introduction

Gamers naturally become frustrated if they are unable to progress in the game quickly. They may feel dejected if all of their friends are doing exceptionally well and are ahead in the game's competitive standings. Also, the more popular and addictive the game is, the more keen gamers are to do well. Based on the structure given to the games by developers, it usually takes a long period of sustained play to reach advanced levels of any game and unlock new features.

Not all gamers may wish to progress by grinding through the game and spending real money to buy resources. Instead, they look for shortcuts or unfair means to advance, such as hacking.

4.3.2 Application

Although the majority of gamers are honest, there are gamers who are motivated to cheat and exploit the game's vulnerabilities. There's also potential for gamers to try and take out their frustrations on the game itself, by disrupting the game through hacking or DDoS attacks, in the self-serving aim that no one else enjoys the game. An instance of

this occurred in October 2016, when a disgruntled gamer was alleged to have shut down large parts of the Internet in Europe and the US with an attack on Dyn.

Game providers have the option of implementing a ban on players perceived to be conducting illegal activity. However, this can provoke the banned gamer to resort to hacking to further disrupt the game.

4.4 Tactical

4.4.1 Introduction

Intellectual property theft is a crime in any industry, and gaming is no different. After hacking into a game, attackers can get their hands on the game's source code. The information will enable the attacker to create a new competing game and mimic the hacked game. Any gaming company that suffers from this category of attack might not be able to recover, as the source code will allow gamers to exploit tricks and loopholes in the game, defeating the whole purpose of continuous gameplay to progress to higher levels.

4.4.2 Application

To some degree, there exists a culture around players using DDoS attacks to interrupt and prevent other player's progression within the game. Games frequently have time-based milestones with great rewards, so preventing a major proportion of users from logging in results in a significant competitive advantage. To achieve this, gamers disrupt an entire service, reaping in-game benefits when the game recovers from the attack.

An attack could also be used to direct gamers to a competitor's games. Due to the subsequent disruption and loss of service, many angry and frustrated gamers may switch over to rival games. The loss of revenue from downtime as well as a reduction in the number of gamers can quickly drive a game out of business, thereby achieving the attacker's objective.

05 How Gaming Companies Can Raise the Security Bar

Since their inception, gaming platforms have regularly relied on custom network procedures deployed with performance as the single most important factor to development, with security taking a backseat. As a result, gaming companies often lack sufficient information on how gamers use their services and are unable to distinguish requests that comprise a DDoS attack from an authentic gamer's request. Gaming providers are reluctant to block access to any legitimate gamer, and hence they have lower defenses, thereby allowing access to attackers. As a result, mitigating attacks becomes a difficult and resource-intensive task.

The gaming industry is a relatively new entrant to the cyber security table and still lacks the regulatory controls and standards found in other sectors such as banking and finance. In addition, gaming companies face a major impediment when tackling security threats, and they are partly responsible for this. This is because the focus from a security standpoint has been to counter piracy and intellectual property theft. However, after suffering from long downtimes caused by increasingly frequent attacks (data breaches as well as DDoS attacks), gaming companies have realized the need to deploy advanced security measures.

The first step for gaming enterprises is understanding what makes them vulnerable to attack. Peaks in traffic, for example, exist in gaming usage whereby a very high number of gamers play an MMO concurrently. This commonly happens around holiday season when game providers offer rewards to players. The traffic on game servers can be incredibly high, and latency immediately becomes an issue. This situation can also occur when a gaming company releases a major new update/version, or a new game altogether. In today's digital age, companies make a point of publicizing a new game launch well in advance to generate as much buzz as possible. Traffic consequently spikes after the release of an update or new game.

In both cases, game servers are already working at close to full capacity. An effective DDoS attack in such instances is very easy to implement given that the DDoS attack threshold will be comparatively low. Such an attack was carried out on the servers of Battlefield 1 Beta, just one day after its launch.

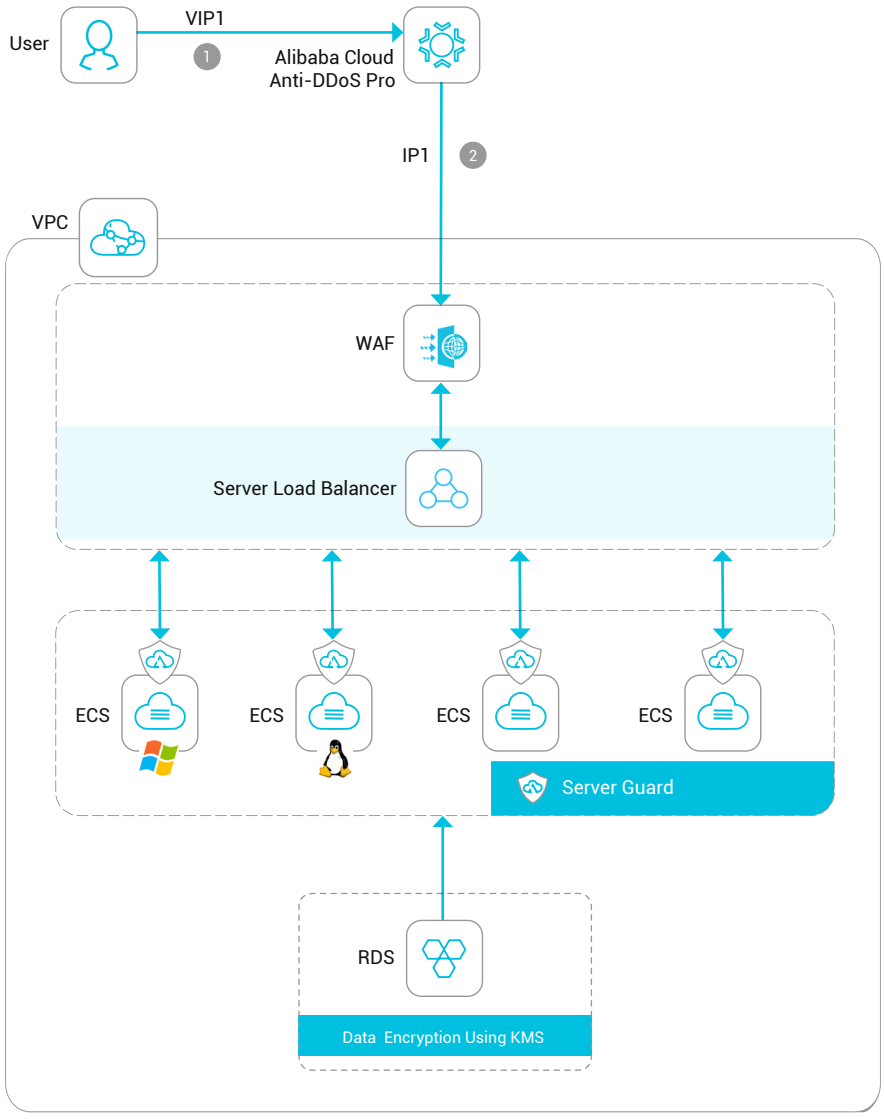
Gaming companies should conduct thorough risk assessments to be able to respond proactively to DDoS attacks. The key here is a change in the mindset of gaming companies and developers towards taking security seriously. Game providers need to pay attention to threats to the gaming environments and create more secure games. Measures for user data protection and two-way user authentication for logins can be helpful. They should also roll out regular security updates to ensure that they keep up with the techniques deployed by attackers.

06 Alibaba Cloud Solutions and Benefits

It's becoming increasingly important for gaming companies to upgrade their security infrastructure to tackle threats posed by cyber criminals. An always-on solution is another need of the hour, as the gaming industry has gamers all around the globe in every time zone.

In a bid to tackle fluctuating demands, gaming companies should invest in solutions that provide scalability on-demand, enabling them to increase their resource pool when traffic is high.

Keeping in mind the specific requirements of the gaming industry, Alibaba Cloud offers state-of-the-art gaming security solutions incorporating current industry best practices for information security and DDoS defense. The following diagram presents a typical deployment architecture proposed by Alibaba Cloud as part of its gaming solution.



Anti-DDoS Security

Alibaba Cloud's Anti-DDoS service is a cloud-based service designed to resist massive DDoS attacks, as they are a significant threat to gaming companies. Anti-DDoS Pro provides protection to gaming companies by mitigating all categories of malicious DDoS attacks, while at the same time ensuring high availability. Anti-DDoS Pro diverts traffic to the Alibaba Cloud Anti-DDoS scrubbing centers by updating DNS resolution settings (web) or by replacing the original website IP with the anti-DDoS IP provided by Alibaba Cloud. Such maneuvers help in filtering the traffic by blocking all threats identified while forwarding the clean traffic to the original server. The filtering ensures comprehensive DDoS protection for gaming enterprise's entire IT infrastructure.

Customized Security Architecture

Alibaba Cloud VPC gives gaming enterprises the flexibility to build their own cloud architecture in an isolated and secure environment, giving them control over their virtual networking environment. Game providers have the freedom to create subnets, configure network gateways and route tables, and select an acceptable range of IP addresses. This ensures unwanted visitors (IP addresses identified in the past as sources of attacks) have no access to the game. For additional security, gaming companies can separate VPC instances into different security domains using security group features. Another distinct advantage for gaming companies is that all Alibaba Cloud ECS instances integrate Anti-DDoS protection to resist DDoS and other malicious attacks to shield game data and applications.

Web Application Firewall and Server Guard

Web Application Firewall (WAF) and Server Guard are cloud firewall services that help protect core data and empower gaming companies to defend themselves against data breaches. Based on powerful big data capabilities and underlying security, WAF provides protection against web-based attacks, including SQL injections, Malicious BOTs, command execution vulnerabilities, and other common web attacks. WAF filters out a large number of malicious access attempts. This filtering is helpful for gaming companies in dealing with attackers that use DDoS bots, as it gives them the opportunity to set predefined rules that can identify queries generated by bots. Along with Anti-DDoS Pro, WAF directs safe traffic to the game servers and prohibits attacks from progressing.

Alibaba Cloud can enable the Server Guard in every ECS instance for gaming companies. It monitors programs to identify if any single program is burning the server's resources. It sends back an alert to notify the game developer, who can verify if the program is malicious and if so take corrective action.

Deploy Globally

With an international network of 13 international data center regions, including China, America, Europe, Middle East, Asia and Australia, and 530 Content Delivery Network (CDN) nodes across the globe, Alibaba Cloud gaming solutions ensure gaming companies do not suffer from latency issues, irrespective of the location from where gamers are playing.

07 Conclusion

Security is of supreme importance for the online gaming industry. The massively distributed client-server architecture of MMOs can cause multiple loopholes that compromise its security. From the game developer's perspective, it is essential to retain loyal customers who are willing to pay-to-play over extended periods, as long as the game is fair and all players have an equal opportunity to progress within the game. Next, there is the virtual economy within these games, linked inextricably to the real-world economy, which hackers can target for monetary benefits.

Gaming companies have suffered from frequent security attacks due to their traditional perception of security threats, with the focus instead being on safeguarding themselves against piracy. This inclination has made them highly vulnerable to data breaches and DDoS attacks. While other industries now have strict cyber security rules and regulations, the gaming industry still has some way to go in this regard.

Alibaba Cloud offers highly scalable and available gaming security solutions to enable gaming companies to efficiently protect against malicious and debilitating attacks. This solution includes products such as Anti-DDoS Pro, VPC, WAF, and Server Guard to ensure highly advanced security.

It is essential for gaming companies to take heed of possible security threats, as well as prescribed solutions so that they can continue offering a glitch-free and smooth gaming experience to consumers.

References

1. http://www.darkreading.com/vulnerabilities---threats/why-online-video-gaming-will-be-the-next-industry-under-cyber-attack-/a/d-id/1325519

2. http://www.makeuseof.com/tag/security-malware-threats-online-gamers-aware/

3. https://arstechnica.com/security/2008/08/safeguarding-your-virtual-goods-MMO-security-a-mixed-bag/

4. Security in online gaming, Bachelor Thesis Information Science, Rens van Summeren

Alibaba Cloud
aliyun.com