National Conference on Research Challenges and Opportunities in Digital and Cyber Forensics
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 4 | Issue 11 | ISSN : 2456-3307 (www.ijsrcseit.com)

A Survey on Distributed Denial of Service Attacks in the Online Gaming Industry

Sanjana A, Medha Vinod
ISE Department, NHCE, Bangalore, Karnataka, India

ABSTRACT

In this digital era, threats in the cyber world has exponentially risen and has resulted in a huge number of cyber-attacks all over the world. One of the most notorious cyber-attacks is distributed denial of service (DDoS), which is a subclass of denial of service (DoS) attacks. DDoS attacks are a standard tactic used to make a service/server unavailable to its users. These attacks involve hackers sending large amounts of traffic to overwhelm and disable a targeted system with a flood of internet traffic. According to several reports, online gaming industry has become the biggest victim or target to DDoS attacks. This paper provides a systematic survey on the various DDoS attacks taking place in the gaming industry. This paper also provides an analysis of the trends of these attacks, counter measures and factors affecting it and vulnerabilities. Through this analysis, we can identify the prior vulnerabilities faced by online gaming and ensure a more successful defense against these threats in the future. Thereby it will help in providing a secure and efficient medium for online gaming.

Keywords : DoS, DDoS Attacks, Online Gaming Industry, Safer Medium, vulnerabilities

I. INTRODUCTION

DoS (Denial of Service) attack is a cyber- attack with spiteful user aimed to render a host computer or other device unavailable to its authorized users by disturbing the device's normal operation. DoS attacks is usually practice of overwhelming or a targeted machine with requests until normal traffic is not able to be processed, resulting in denial-of-service for the users. A DoS attack uses a single computer to launch the attack. A DDoS (distributed denial-of-service) attack is a malicious attempt that tries to disrupt the regular traffic of a targeted server, service or network by overwhelming the target or its contiguous infrastructure with an overflow of Internet traffic. DDoS attacks are more complex as compared to DoS attacks as they involve a large range of devices, increasing the intensity of the attack. Being attacked by one computer is not the same as being attacked by a botnet of a large number of devices. One of the fields affected by DDoS is the gaming industry.

There are different ways by which these attacks affect users. The first is providing the access to lager multiplayer games where there can be only limited which then waits until the developer agrees to the demands of the attacker. On the other side, the game may harm the reputation of the company with limiting player access Similar kind of attacks are initiated by rival businesses or even by overly addicted fans looking to boost their game by harming each other. These can be commenced by the passionate community members observing to punish a developer or publisher for wrong business practices. However, some engage in these attacks to signify their lashing out towards content changes in an online game or even due to the fact that the individual player has been debarred from a game for a certain reason.

II. DDOS ATTACKS IN ONLINEGAMING INDUSTRY

Online gaming industry has been a victim to Distributed denial of service (DDoS) attacks for so many years. Based on several reports from the industry and present trends, the prevalence of DDoS attacks is multiplying exponentially and online gaming servers are the number one target for DDoS assaults [1]. According to [2], this cyber-attack keeps happening on a daily basis for several online gaming websites and servers. These attacks spike prominently during holiday seasons, the summer and spring seasons. A recent report published by Akamai [3], It was observed that 3,072 distinct DDoS attacks in the gaming industry was published in the report present by Akamai [3], between the time span of July 2019 and June 2020.

A. *Infamous DDoS Attack Incidents in Online Gaming*

The most common type of DDoS attack for video games or online games is the network layer attack in which the defenders target your network infrastructure itself. Two popular hacktivist collectives "Lizard Squad" and "Poodle corp." are infamously known for their DDoS attacks on popular online video games like Nintendo, League of Legends, few games in Blizzard networks and also on PlayStation, Xbox.

Some of their attacks are :

1) *Christmas 2014 attacks on PSN and Xbox Live :* Hacking group Lizard Squad threatened formerly to take gaming down the services on Christmas. And on 25th of December, 2014 (Christmas Day), Lizard Squad demanded to have DDoS attack on the Network PlayStation and Xbox Live. Later, distributed denial of service (DDoS) attack took credit on Xbox Live that left tens of thousands of users unable to connect to the service [4]. Their servers were down for several hours and had their cyber-security teams trying to bring them back up. Using a recently discovered malware variant, it was found that these hackers turned household routers into so-called "stresser" tools, which was used to flood the networks with bogus traffic, finally made the service unavailable for legitimate gamers [5].

1) League of Legends DDoS: Servers of the game League of Legends were taken offline with a DDoS attack on 18th August 2014, Later Lizard Squad claimed this to be their first attack [4].
2) Destiny DDoS: 23th November 2014, Lizard Squad claimed they attacked and took down Destiny servers with a DDoS attack [4].
3) Xbox Live DDoS: 1st December 2014, Xbox Live was apparently attacked by the infamous Lizard Squad. Numerous users attempting to connect to use the service would be given the 80151909 error code [4].
4) Sony's PlayStation Network DDoS: In 2011, the PlayStation Network was compromised by sony, which was not noticed by the security breaches of that user accounts, Qriocity and Sony Online Entertainment because distributed denial of service attacks was used as a distraction to make their services unavailable. It was later unveiled that the nearly 77 million users account information on the was been stolen by the hackers by PlayStation Network and Qriocity A week later, it was the acknowledged by the company that the Sony Online Entertainment gaming service had also been breached, affecting an additional 24.6 million users. More than 101 million legitimate user accounts have been compromised. The user names, addresses, email

addresses, dates of birth were included in the data stolen [6]. Lizard Squad claimed the responsibility of the PlayStation Network disrupted via a DDoS attack, 24th August 2014 and again reclaimed 8th December 2014[4].

5) Battlefield 1: Online gamers of a new beta of the video game Battlefield 1 saw their activity disrupted after an alleged distributed denial of service (DDoS) attack knockout the servers of games company Electronic Arts (EA). In 2016, Poodle Corp launched repeated attacks against EA, Blizzard and Riot Games. These hacktivist collectives sold DDoS attacks services and was in a form of advertisement that often partake in stunt hacking. They would also try to intentionally ruin launches of specific and often popular titles, like Battlefield 1 [7].
6) Blizzard: Blizzard Entertainment, an American Video game company which has released several video games like Call of Duty (CoD), Overwatch, World of Warcraft (WoW) has been a victim several times to DDoS attacks over the years. First in April 2016, Blizzard's World of Warcraft: Legion launch faced a cyber-attack. According to Blizzard Entertainment, a distributed denial of services (DDoS) assault caused high latency issues and disconnections during the launch of their new expansion. DDoS attack was a small scale assault, but still managed to take down all the servers of the game during the expansion launch of World of Warcraft: Warlords of Draenor. The hacker group Lizard Squad claimed responsibility for the attack at the time [8]. Later that same year their game servers "Battle.net" was taken down for a span of two hours with players not being able to connect to the game's servers. In August 2017, Over the years, Blizzard's server "Battle.net" has become a victim to several DDoS attacks. The most recent attacks were on June 2020. One of their popular online game "Call Of Duty: Modern Warfare and Warzone" was attacked and the servers were down [10].
7) Final Fantasy XIV : Popular online game Final Fantasy XIV has been dealing with an advanced and persistent DDoS attack. A recent DDoS attacks had flooded the Square Enix's networks, which resulted in an intermittent service degradation and disconnection for over a month [11].
8) Ubisoft : Ubisoft was faced with a series of DoS and DDoS attacks that resulted in service degradation and disconnection that had impacted several major online titles including Rainbow Six Siege and Ghost Recon. Ubisoft issued a statement regarding those attacks stating, DDoS assaults is a common threat for almost all online video games and their service providers. In addition to the outages at Ubisoft, NCSoft released Master X Master, a Multiplayer Online Battle Arena (MOBA) game. NCSoft suffered from several DoS attacks that resulted in users experiencing high level latency and dropped connections [11].
9) Pokémon GO: A group of hackers called "Poodle Corp." had claimed responsibility for a distributed denial of service (DDoS) attack that had down taken the servers of insanely popular augmented reality game Pokémon GO offline [12].
10) Under *application layer attack:* the Mirai botnet was one of the scariest DDoS attack in the history. The couple of Students originally created the Mirai botnet to disable Minecraft servers and later was manipulated to launch the largest-ever DDoS attack [13]. The Mirai botnet had compromised more than 600,000 devices at its peak, creating a DDoS tool magnitudes greater than anything the internet had seen before and was capable of crippling huge parts of it [14].

A. *TRENDS OF DDOS ATTACKS IN ONLINE GAMING*

Akamai has observed since July 2019 that 3,072 distinct DDoS attacks in the gaming industry, making it the largest target DDoS across the net [3].

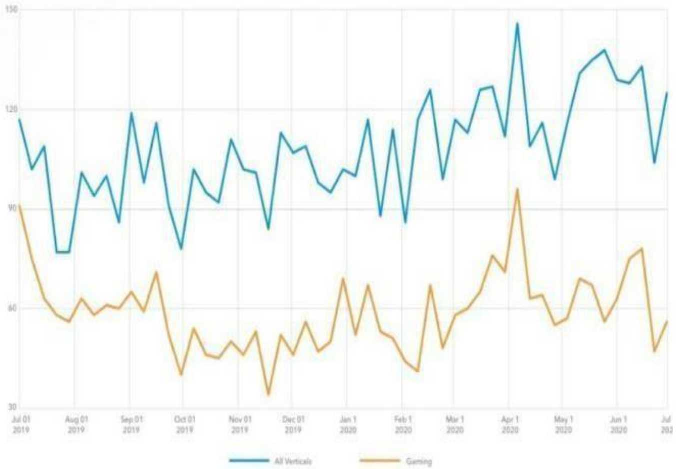

Fig.1 Weekly DDoS Attack Events [3]

DDoS attacks are consistent, occurring particularly in gaming. In 2016, Mirai botnet which was responsibility for a large number of DDoS attacks that created havoc on internet. Several countries like Russia, Turkey and Netherlands are notoriously known for their strong existences in underground forums for DDoS services which is used for targeting mainly gaming.

DDoS Attacks Events by mitigation Outcome are given below, Gaming vs. Rest of the services from July 2019 to June 2020[3].

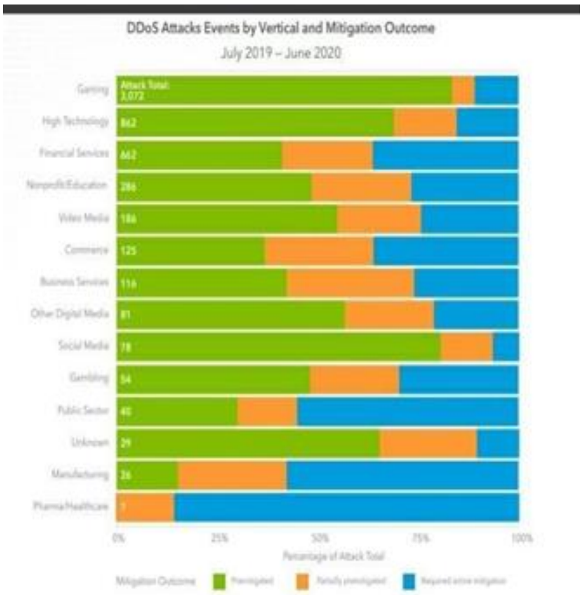

Fig.2 Vertical Outcome

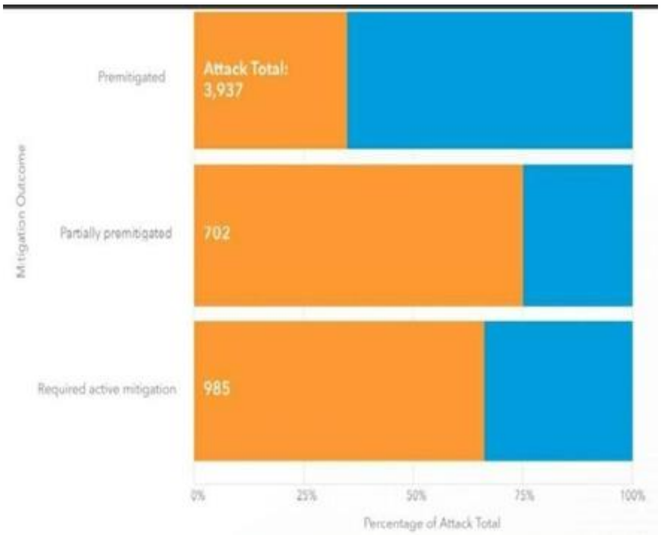

Fig.3 Mitigation Outcome

III. FACTORS CONTRIBUTING TODDOS ATTACKS IN ONLINEGAMING

There are reasons indicating that online gaming industries are targeted more than others, which are [15]:

A. Business Competition

In the world of competitive industries such as online gaming, an attack of DDoS can be used to take down a rival's servers or website.

B. Extortion

Industries like online video games and e- commerce websites are dependent on their online presence and become an easy prey for perpetrators exchange for keeping a specific website online. extorting money.

Hacktivism

Hacktivists commonly target websites related to media, politics or shared sites to protest their actions or ideologies.

C. Vandalism

Cyber vandals, typically random offenders, often attack gaming services or other high profile targets.

D. Nature of Gaming

An advantage is taken over DDoS attack perpetrators gaming and emotion that online gamers have a deep connection for a level or a connection to a specific character in the game. Any interruption in the game may lead to chaos and causing the attackers take advantage of this experience and emotion of these online gamers and twist on the worst to bring about an outbreak.

IV. LOOPHOLES AND VULNERABILITIES

In recent times, the gaming industry has taken DDoS attacks as a considerable margin [17-21].The Hypertext Transfer Protocol (HTTP) does not work neither support the attacks, thereby they are primarily designed or targeted at the network layer.

They explode the server with exponential requests which slows down the servers to the point where the connection ultimately breaks. After a DDoS attack, online gamers are unable to log in and save their data and also the entire storage is wiped lost. Some of loopholes and vulnerabilities are:

A. *Predictable rush hours*

The existing server and network resources are exhausted by DDoS attacks, they are most effective when the resources are already scarce, for instance when a network is being utilized by a large scale of users simultaneously. Sony and Microsoft sold a combined 11 million consoles just before Christmas in the year 2014, which made it easy to expect that their networks would be strapped to their respective limits. During a similar condition, when the reports are depreciation in service due to the sheer volume of regular requests and traffic, then disrupt server/service caused by is much easier for an attacker or hacker to saturation already struggling network infrastructure.

A. *Don’t have to take it offline*

All gamer can conveys that we can’t completely shut down a gaming server to bring it to a halt. Games, especially those featuring multiplayer competitive operations, are completely about instant feedback of users; every additional millisecond between “order given” and “action taken” can severely disrupt the experience of the game. An e-commerce website resulting an attack on a half-second latency might go unnoticed, but a DDoS assault on a Call of Duty server causing the same delay would completely stop all activities. This is not because the server is unavailable, but because it becomes unusable or unstable.

B. *Proprietary Protocols*

Gaming platforms are built on proprietary protocols rather than HTTP, which are custom network protocols built with highest precision in performance. For an application such as a game, it is not easy for it to distinguish between a player and a DDoS bot because there is very little information provided by the online gamers and taken by the game’s developer to differentiate between them.

D. *Single points of failure*

Many applications and online games derived from cloud are managed from a central platforms. When these are taken down by hackers, this causes the entire service to go dark for their legitimate users. In some cases, a DDoS attempt can wreak havoc even if it doesn't succeed in taking the targeted servers completely offline. For instance, mere pressure resulting in slower or more inconsistent performance can ruin the day for an online gamer.

E. *UDP*

It is very popular among DDoS attackers because it's easy to spoof and is used in almost all DNS amplification attacks, which exploits the vulnerabilities and loopholes in domain name system (DNS) servers. Beyond UDP, several other common attack vectors are SYN Flood, DNS Response, TCP and NTP.

V. CONTROL MEASURES

Most online industry Game developers and the related companies remain the main target for DDoS attacks, which comprises of the large percent of all DoS and DDoS attempts. The Security Operations Command Centre (SOCC) Experts tailor the mitigation controls to detect these attacks and try to eradicate these attacks in the future by conducting live analysis of the internet traffic to determine further improvement . DDoS attack events are found out either by the SOCC or by the targeted organization itself. SOCC records major part of the attack mitigation data [1].

A. *Anti-Malware Software*

It is a rock solid anti-malware software that also monitors your internet connection. The software Anti-malware is used reports of existing malware and bot signatures to identify and block them from infecting your computer. This is only a fraction of the work done, as new kinds of malware will be made the next second and there can only be few people discovering and reporting their signature to the respective companies.

B. *VPN*

Virtual private network (VPN) use certain protocols to basically encrypt the data and send it through servers so the sender and receiver of the data will not be exposed. Several VPN providers like Nord VPN also have specific DDoS attack relief servers which uses a stability check systems to monitor all unusual amount of internet traffic going through the server. Finally distributes it and cover the data in order to minimize the negative effects on the legitimate users [22].

C. *Generic Routing Encapsulation Tunnel*

A generic routing encapsulation tunnel (GRE) is a vital component that ensures that the normal users are not affected by insufficient mitigation measures. A GRE tunnel reduces the network traffic and establishes a high-speed point-to-point connection between the network nodes that will bypass normal routing disturbances [1].

VI. CONCLUSION

Due to very fast advancement in technology, we experience a humungous amount of cybersecurity threats and challenges. The online gaming industry is one industry that has been threatened over the years. This survey paper focuses on DDoS attacks and how these attacks have been affecting the gaming industry over the years. The various loopholes that are used by the DDoS attackers have been discussed, along with the trends of these attacks over the years and the control measures taken to prevent such attacks. With time, there definitely will be an improvement in the research to generate methods that ensure DDoS can be handled effectively the safety of online gaming.

VII. REFERENCES

[1]. DDoS Mitigation,"It's Not a Game: The Ever-Growing Risk of DDoS Attacks on Online Games",Accessed on: September 23rd.[Online].Available: https://www.imperva.com/blog/ddos- attacks-on-online-gaming-servers/

[2]. CAMBRIDGE, Mass., State of the Internet / Security report, Gaming: You Can't Solo Security, Sept. 23, 2020 .Accessed on Sept. 24, 2020.

[3]. [Online].Available:https://www.akamai.com/uk/en/multimedia/do cuments/state-of-the-internet/soti-security-gaming-you-cant-solo- security-report-2020.pdf

[4]. Martin Mkeay,"Gaming, You can't solo Security",Accessed on: September 23rd. [Online]. Available: https://www.akamai.com/uk/en/multimedia/documents/state-of- the-internet/soti-security-gaming-you-cant-solo-security-report- 2020.pdf

[5]. Brian Feldmen ,"Three Minecraft Players Were Behind the Botnet That Took Down a Chunk of the

Internet Last Year",Accessed on: September 24rd. [Online]. Available:https://nymag.com/intelligencer/2017/12/three- minecraft-players-created-the-webs-scariest-botnet.html

[6]. Russell Brandom ,"Lizard Squad used hacked routers to take down Xbox Live and PlayStation Network",Accessed on: September 24rd. [Online]. Available:https://www.theverge.com/2015/1/9/7520415/lizard- squad-used-hacked-routers-to-take-

[7]. Fahmida Y. Rashid ,"Sony Data Breach Was Camouflaged by Anonymous DDoS Attack",Accessed on: September 24rd. [Online]. Available:https://www.eweek.com/security/sony-data- breach-was-camouflaged-by-anonymous-ddos-attack

[8]. "Recent DDoS Attacks on Game Providers Ubisoft and NCSoft",Accessed on: September 24rd. [Online]. Available:https://security.radware.com/ddos-threats-

[9]. attacks/threat-advisories-attack-reports/ddos-assaults-on-gaming- providers/

[10]. Paul Sawers ,"PlayStation Network and Xbox Live DDoS arrest:

[11]. U.K. authorities grab an 18-year-old man",Accessed on: September 24rd. [Online]. Available:https://venturebeat.com/2015/01/16/18-year-old- arrested-over-playstation-and-xbox-ddos-attacks/

[12]. Tom Spring ,"Blizzard Entertainment Hit With Weekend DDoS Attack",Accessed on: September 24rd. [Online]. Available:https://threatpost.com/blizzard-entertainment-hit-with- weekend-ddos-attack/127440/

[13]. Eric Kain"Hit By DDoS Attack — 'Call Of Duty' 'Overwatch' And 'World Of Warcraft' Experiencing Issues",Accessed on: September 24rd.[Online].

[14]. Available:https://www.forbes.com/sites/erikkain/2020/06/02/call- of-duty-modern-warfare-and-warzone-servers- down/#91fa6b77a908

[15]. "Recent DDoS Attacks on Game Providers Ubisoft and NCSoft",Accessed on: September 24rd. [Online]. Available: https://security.radware.com/ddos-threats-attacks/threat- advisories-attack-reports/ddos-assaults-on-gaming-providers/

[16]. Duncan Riley, Inc. ,"Pokemon GO goes down following DDoS attack from Poodle Corp",Accessed on: September 24rd. [Online]. Available: https://siliconangle.com/2016/07/17/pokemon-go-goes- down-following-ddos-attack-from-poodle-corp/

[17]. Akamai Technologies, Inc. ,"Akamai Report Reveals Broad, Persistent Cyber Attacks Targeting Video Game Players and Companies",Accessed on: September 24rd. [Online]. Available: https://www.prnewswire.com/news-releases/akamai-report- reveals-broad-persistent-cyber-attacks-targeting-video-game- players-and-companies-301136183.html

[18]. https://nymag.com/intelligencer/2017/12/three-minecraft-players- created-the-webs-scariest-botnet.html

[19]. Lance Whitney ,"Why certain companies are more heavily targeted by DDoS attacks",Accessed on: September 24rd. [Online]. Available: https://www.techrepublic.com/article/why-certain-companies-are-more-heavily-targeted-by-ddos-attacks/

[20]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[21]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[22]. Paul Sawers ,"PlayStation Network and Xbox Live DDoS arrest:

[23]. U.K. authorities grab an 18-year-old man",Accessed on: September 24rd. [Online]. Available:https://venturebeat.com/2015/01/16/18-year-old- arrested-over-playstation-and-xbox-ddos-attacks/

[24]. Olawale Daniel ,"Online Gaming: Are DDoS Attacks The Biggest Nemesis For Online Gamers?",Accessed on: September 24rd. [Online]. Available: https://techatlast.com/ddos-attacks-online- gamers/

[25]. Noah Gamer ,"Why DDoS attacks target gaming and software companies",Accessed on: September 24rd. [Online]. Available:

[26]. https://blog.trendmicro.com/why-ddos-attacks-target-gaming-and- software-companies/

[27]. Lance Whitney ,"Why certain companies are more heavily targeted by DDoS attacks",Accessed on: September 24rd. [Online].Available:https://www.techrepublic.com/article/why- certain-companies-are-more-heavily-targeted-by-ddos-attacks/

[28]. Hrvoje,"DDOS: THE ENEMY OF ONLINE GAMING AND HOW TO PROTECT YOURSELF",Accessed on: September 24rd. [Online]. Available: https://www.keengamer.com/