# ERT Threat Alert
## Recent DDoS Assaults on Gaming Providers
## July 20, 2017


## Abstract
There is nothing new about DDoS attacks against the gaming industry and over the last several weeks there have been a number of assaults launched against a handful of gaming companies. Hacking and DDoS attacks have always been a part of the gaming culture. Unfortunately, largescale DDoS attacks targeting gaming networks and ISPs have become an everyday occurrence. When attacked, companies typically suffer from network outages and service degradation that results in players being disconnected or prevented from accessing game content all together. The attackers can range from in-game competition trying to gain an advantage to an upset user trying to disrupt gameplay. In addition to malicious traffic, companies can also experience natural floods when they release new game titles, expansion packs or in-game content. This often presents a challenge in identifying and blocking bad traffic without blocking legitimate users.


## Reasons for Concern
The gaming industry continues to experience attack campaigns across the world. When game services become unavailable due to a DDoS attack, users are disconnected and millions of gamers around the world, many of whom are paying customers, become frustrated with the company, thereby resulting in reputation damage. DDoS attacks on game servers can also have an impact on network providers who must contend with potential Internet pipe saturation.

In some attacks, the gaming companies are among a diverse group of targets while others are targeted for specific reasons. Part of the appeal of targeting a gaming service is the constant connectivity of its users and availability of a centralized gaming platform that creates a single point of failure. This makes for an easy and often efficient attack, allowing the attacker to cause more damage leveraging fewer resources while gaining more attention.

Over the years, Radware has followed the evolution of DDoS attacks directed at the gaming industry. In 2016 Lizard Squad and Poodle Corp launched repeated attacks against EA, Blizzard and Riot Games. Both groups sold DDoS attacks services and would often engage in stunt hacking as a form of advertisement. They would also try to intentionally ruin launches of specific and often popular titles, like Battlefield 1.

## Recent Attacks
### Final Fantasy XIV
Over the last month[1], Final Fantasy XIV has been dealing with an advanced and persistent DoS attack that has included changing attack vectors[2]. These attacks that have flooded Square Enix's networks, resulting in intermittent service degradation and disconnection for over a month. Square Enix, in a recent statement, confirms that they have experienced a series of attacks from a third party since mid-June. The attacks appear to have started in parallel with the release of the second expansion pack, Stormblood[3], for Final Fantasy XIV on June 16th. These attacks have now transferred from targeting Square Enix's game servers to their upstream providers.

When companies release new gaming titles or expansion packs, there is often a flood of users attempting to access the content. As a result, the flood of legitimate users creates additional stress for gaming

[1] http://na.finalfantasyxiv.com/lodestone/news/detail/943f91bc27073dba50f8e848ce2c73ef704df951
[2] http://eu.finalfantasyxiv.com/lodestone/news/detail/eb864930feb9f294aba73013cc23837b9453797c
[3] http://na.finalfantasyxiv.com/lodestone/topics/detail/7933cb4e7b3a01b4e86dc352c2ac06cca462cfc4

networks. Prior to the release of Stormblood, Final Fantasy relocated their data center[4] to provide better service availability and increased optimization for their users.

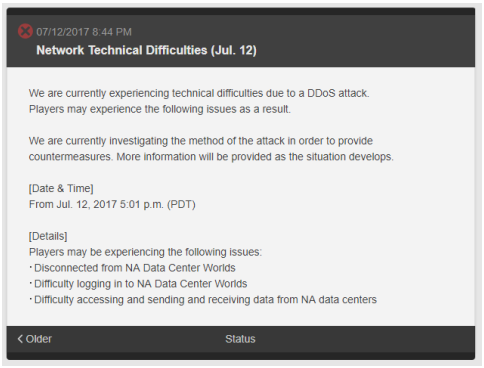


Figure 1: Enix suffering network issues due to a DDoS attack

**Ubisoft and NCSoft**

At the end of June, Ubisoft was faced with a series of DoS attacks[5] that resulted in service degradation and disconnection that impacted several major online titles, including Rainbow Six Siege and Ghost Recon. In a brief update, Ubisoft stated that DDoS attacks are a common problem for almost all service providers. The impact on their networks resulted in users experiencing high latency and limited connection to Ubisoft's game servers. This attack was not persistent like in the case of Final Fantasy XIV, but the attacks did disrupt gameplay for a number of major titles.

In addition to the outages at Ubisoft, NCSoft also saw a round of DoS attacks targeting their game servers. At the end of June[6], NCSoft released, Master X Master, an Multiplayer Online Battle Arena (MOBA) game. NCSoft suffered from several DoS attacks that resulted in users experiencing high latency and dropped connections. Like Final Fantasy XIV, NCSoft was targeted around the same time they released Master X Master.


Figure 2 & 3: Ubisoft and NCSoft acknowledging they have suffered DDoS attacks

## Scope and Volume

Attacks continue to increase in quantity and volume. By combining multiple botnets and stresser services in joint operations, these mega attacks are bound to cause severe damage not only to the gaming operators and their players, but to the network infrastructure providers as well, who will have to absorb (or scrub) these mega DDoS attacks. This disruption ultimately leads to high latency and service degradation

[4] http://forum.square-enix.com/ffxiv/threads/321165-Important-Information-Regarding-North-American-Data-Center-Relocation
[5] http://forums.ubi.com/showthread.php/1695762-Online-Services-Degradation-6-28-17
[6] https://forums.playmxm.com/topic/1844-ongoing-service-impact/

impacting additional enterprise customers as it consumes the service provider's resources. Often times, attackers will aim their attacks directly at an ISP with a PoP near the gaming operator to disrupt traffic.

One of the biggest challenges for mitigating a DDoS attack is distinguishing between legitimate and malicious users. False positives and false negatives can create problems for legitimate gamers. If their traffic is identified as malicious, it results in the gamer experiencing a denial of service, while if traffic from a malicious user is deemed legitimate, it allows them to continue carrying out the attack.

## How to Prepare

An advanced anti-DDoS solution that includes behavioral analysis and challenge responses can allow users to access gaming content during an attack. Rate limiting traffic can prevent floods but will often result in denying service to legitimate gamers. With behavioral analysis, a baseline of application behavior can be established so when an attack is launched the traffic is compared to the baseline, allowing the system to detect and drop suspicious traffic. In addition, challenge response mechanisms can also help prevent malicious traffic from targeting your networks. If the source is suspicious, a challenge will be presented to the source to determine if the user is real or a bot. This method helps prevent unwanted floods from malicious bot traffic.

## Organizations Under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks including protection from network- and application-based DDoS attacks, as well as volumetric attacks that can saturate the Internet pipe
- A hybrid solution that includes on-premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated, web-based attacks and website intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

In addition to Radware products, we recommend that you review your network patch your system according. Maintaining and inspecting your network often is necessary in order to defend against these types of risks and threats.

## Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button".

## Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.