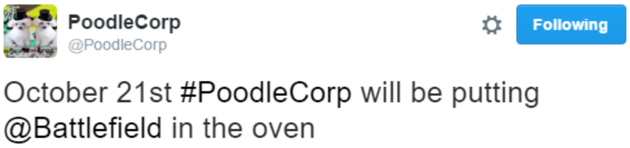
ERT Threat Alert

Game On: Vendors Targeted by Hackers

September 26 2016

Abstract

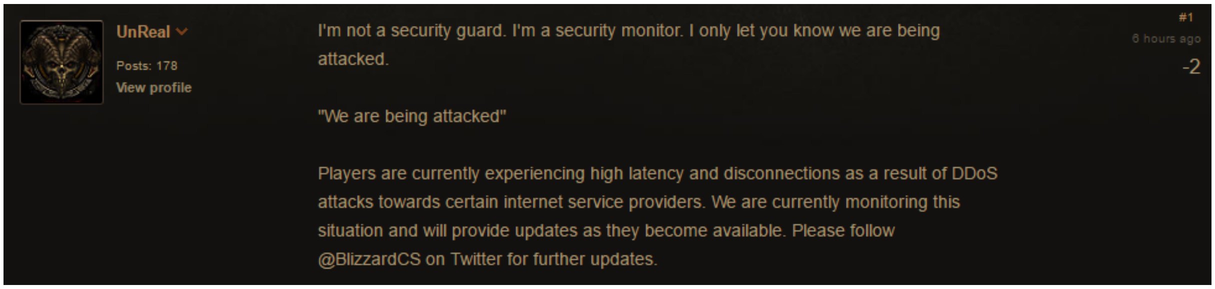
Largescale DDoS attacks have become an everyday occurrence in the gaming industry. Companies are suffering network outages and service degradation causing immediate impact on their brand equity. Case in point: the hacking collective PoodleCorp has committed to launch a DDoS attack in an attempt to ruin the launch of Battlefield 1 on October 21, 2016



October 21st #PoodleCorp will be putting @Battlefield in the oven

Figure 1: PoodleCorp launches attack against Blizzard

There are many reasons this industry is targeted and this alert analyzes a number of these recent incidents as they are becoming more persistent (see Figure 2). The high volume of these attacks not only targets the vendors themselves, but can impact network providers who must contend with potential Internet pipe saturation. Gamers, many of whom are paying customers, remain frustrated.



I'm not a security guard. I'm a security monitor. I only let you know we are being attacked.

"We are being attacked"

Players are currently experiencing high latency and disconnections as a result of DDoS attacks towards certain internet service providers. We are currently monitoring this situation and will provide updates as they become available. Please follow @BlizzardCS on Twitter for further updates.

Figure 2: Blizzard admits being hit by a DDoS attack in August

Background

Hacking and DoS attacks have always been a part of the gaming culture, but recently Radware has documented a dramatic evolution in the DoS attacks directed at the gaming industry. No longer a mere showcase of power, the motivations behind the attacks are becoming more sinister in nature.

Riot Games, EA and Blizzard have all suffered from massive attacks from two DDoS groups, Lizard Squad and PoodleCorp. Since April 2016, Blizzard has experienced over 12 network crippling attacks that have left their user base unable to play their games (see Figure 3).

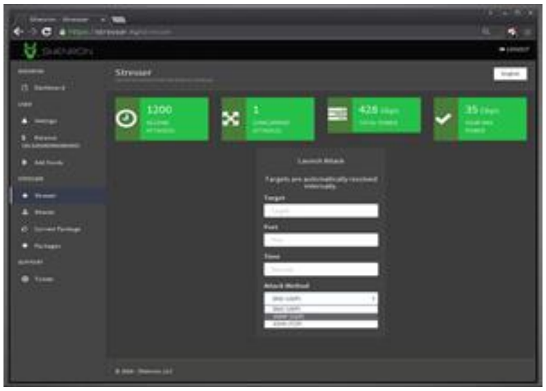
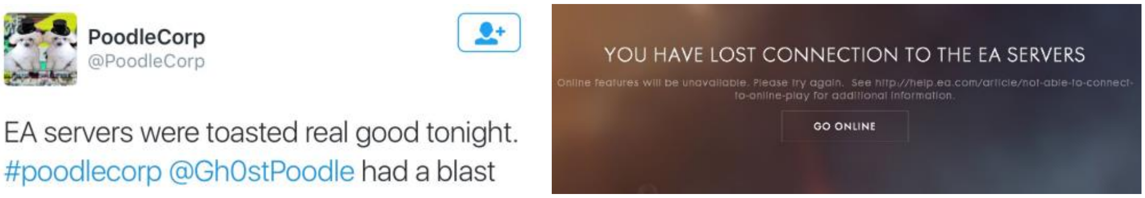


Figure 3: LizardSquad Shenron Stresser Panel, used to launch April attacks against Blizzard

There are numerous reasons for these attacks, however most can be categorized under the following three categories:

1. **Trolling** – These assaults come at crucial moments when gamers are trying to take advantage of game specials and bonus points. These events have set start and finish dates. When attackers cripple the network during these times, gamers can become upset and take to social media to voice their frustration. By upsetting the users in a critical moment, hackers can harm the reputation of the company.
2. **Retaliation** – Recently, Blizzard banned a large group of users for using automatic triggering and aim bots. In response, these users with the assistance of Lizard Squad, where able to retaliate against the company with a massive DDoS attack.
3. **Thrill and Attention** – These attacks are focused mainly on tournament disruption, booting specific players, stunt DDoS'ing, advertisement (self-promotion)


PoodleCorp
@PoodleCorp

EA servers were toasted real good tonight. #poodlecorp @Gh0stPoodle had a blast

YOU HAVE LOST CONNECTION TO THE EA SERVERS

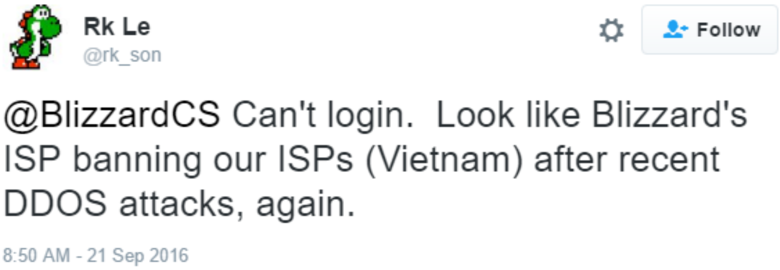
Online features will be unavailable. Please try again. See http://help.ea.com/article/not-able-to-connect-to-online-play for additional information.

GO ONLINE

Figure 4 & 5 – Poodlecorp harasses Electronic Arts

Reasons for Concern

Attacks continue to increase in size. By combining multiple botnets and stresser services in joint operations, these mega DDoS 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 service degradation impacting additional enterprise customers as it consumes the service provider’s resources (see Figure 6). Often times, attackers will aim their attacks directly at an ISP with a PoP near the gaming operator to disrupt traffic.



Rk Le
@rk_son

@BlizzardCS Can't login. Look like Blizzard's ISP banning our ISPs (Vietnam) after recent DDOS attacks, again.

8:50 AM - 21 Sep 2016

Figure 6: During these attack legitimate users find themselves being blocked

Targets

- EA
- Blizzard
- Riot Games

Attack Vectors

Botnet - A collection of compromised computers often referred to as "zombies" infected with malware that allows an attacker to control them using a command and control server. Botnet owners or "herders" control their botnet by means of a covert channel such as IRC (Internet Relay Chat), issuing commands to perform malicious activities such as DDoS attacks, sending spam, and steal information.

How to Prepare

- Improve resilience
- Adopt a threat intelligence process
- Encourage information sharing
- Consider a cloud scrubbing service with a high mitigation capacity (looking ahead – at least 2TB)

Effective DDoS Protection Considerations for Organizations Under Threat

- A hybrid solution combining on-premises detection and mitigation with cloud-based protection for volumetric attacks. It facilitates quick detection, immediate mitigation and prevents Internet pipe saturation.
- Maintaining service availability under attack by choosing a solution that monitors traffic behavior and distinguishes between legitimate users and attack traffic, allowing them in while blocking the malicious packets
- An integrated, synchronized solution that can protect from multi-vector attacks such as network floods, and application layer attacks such as low-and-slow service disruptions or HTTP/S floods.
- A cyber-security emergency response plan that includes a dedicated emergency team of experts and clear actions in the event of attack.

Radware recommends IT crews to monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats when they occur.

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.