Background

Worldwide gaming leader Blizzard suffered a major DDoS attack on April 13th 2016, denying players of World of Warcraft, Diablo 3, StarCraft 2 and Hearthstone from playing these online favorites. The hacktivist group The Lizard Squad claimed responsibility (see Figure 3). Following a series of threats issued via Tweeter, Lizard Squad used their powerful stressers to take down the servers of Blizzard's online gaming platform, in addition to hacking the company's corporate email server (see Figure 2). Once Blizzard restored service, the Lizard Squad tweeted "more to come." The Lizard Squad is the same group who has taken down Sony PlayStation and Microsoft Xbox in the past, as well as other gaming services.

Coincidently, this attack happened a week after Blizzard closed a popular pirate server used by numerous gamers and fans. Though not explicitly correlated, **gaming companies should keep in mind fighting privacy includes another dimension: cyber revenge.**

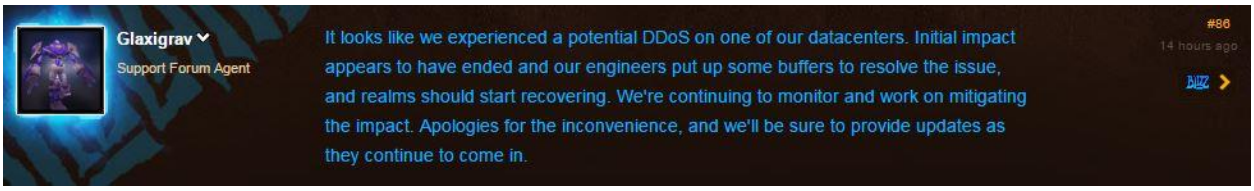


Figure 1: Blizzard acknowledges the attack on their support forum

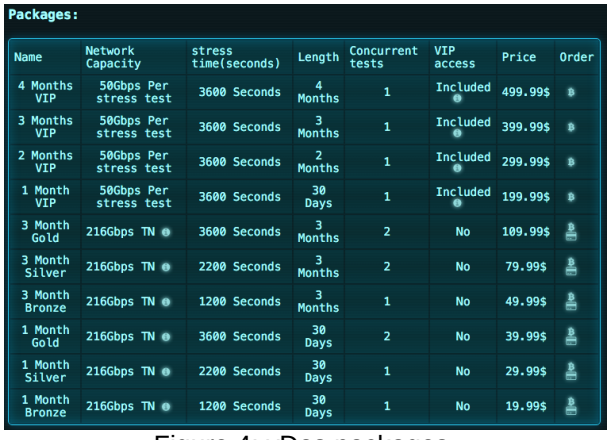
Figure 2: Lizard Squad member tweets an image of a blizzard.com email account

Figure 3: Attack timeline

Attack Methods and Tools

Lizard Squad members have owned and operated a number of stresser services for years. Most recently, they have been observed using vDos[i] and Shenron[ii]. These services offer a number of powerful attack methods that can exceed 200Gbps. The tools offer additional services and such as portmapping, VPNs, IP spoofing and amplifications for DNS and NTP connections.

These tools are available for hire. Prices range between $19.99 and $200 for one month's access. Each package includes a specific attack time ranging from 20 to 60 minutes and offer access to their shared network power of 216Gbps. Private VIP packages guarantee 50Gbps in attack strength (see Figures 4 & 5). Such attack volumes challenge the protections most businesses currently have implemented.



Packages:

Name	Network Capacity	stress time(seconds)	Length	Concurrent tests	VIP access	Price	Order
4 Months VIP	50Gbps Per stress test	3600 Seconds	4 Months	1	Included	499.99$	
3 Months VIP	50Gbps Per stress test	3600 Seconds	3 Months	1	Included	399.99$	
2 Months VIP	50Gbps Per stress test	3600 Seconds	2 Months	1	Included	299.99$	
1 Month VIP	50Gbps Per stress test	3600 Seconds	30 Days	1	Included	199.99$	
3 Month Gold	216Gbps TN	3600 Seconds	3 Months	2	No	109.99$	
3 Month Silver	216Gbps TN	2200 Seconds	3 Months	2	No	79.99$	
3 Month Bronze	216Gbps TN	1200 Seconds	3 Months	1	No	49.99$	
1 Month Gold	216Gbps TN	3600 Seconds	30 Days	2	No	39.99$	
1 Month Silver	216Gbps TN	2200 Seconds	30 Days	1	No	29.99$	
1 Month Bronze	216Gbps TN	1200 Seconds	30 Days	1	No	19.99$	

Figure 4: vDos packages

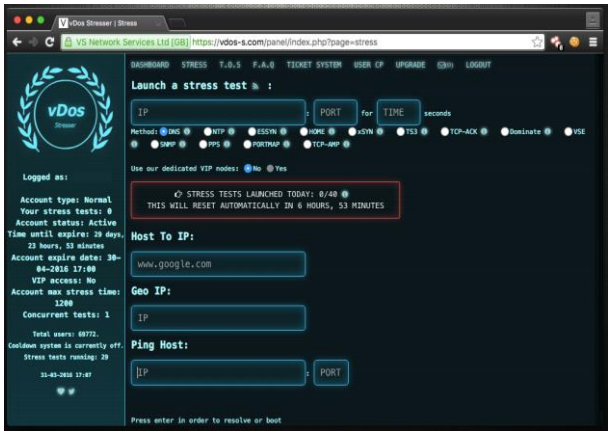


Figure 5: vDos attack panel

Shenron has a very similar pricing structure. Prices range from $19.99 to $999.99 a month for access to their network. Each package also includes a specific attack time depending on which package is purchased. On the lower end, an attack of 1200 seconds can be launched versus 18000 seconds on the high end. Shenron's network strength claims the ability to launch attack sizes up to 500Gbps (see Figures 6 & 7).

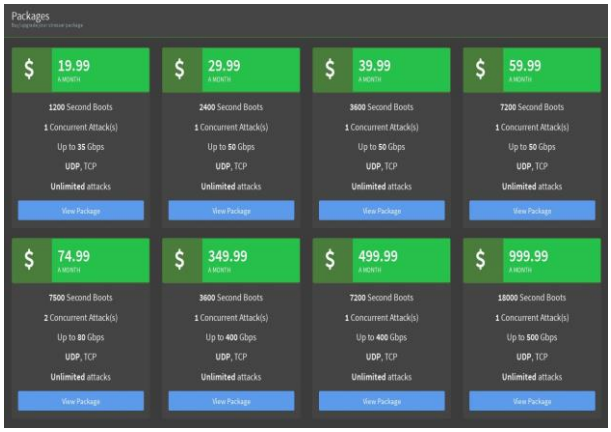


Figure 6: Shenron packages

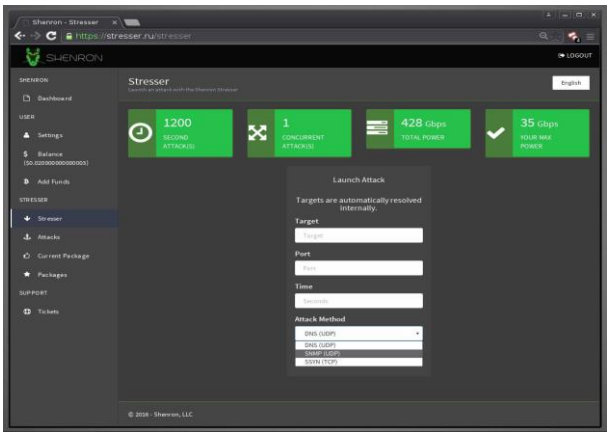


Figure 7: Shenron attack panel

Organizations Under Attack Should Consider

- A security solution that can protect its infrastructure from multi-vector attacks that includes 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 and 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 offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

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.