Abstract
Around the holidays, companies such as Microsoft and Sony typically find their gaming platforms under threat of a cyber knockout; but a new hacktivist group, New World Hackers, isn't playing by the rules. Xbox Live suffered a series of outages over the last week that resulted in millions of worldwide gamers unable to access their service thanks to New World Hackers and its highly powerful stressor service.

Background
Since Sunday, February 14 Xbox Live has experienced a series of outages that have left millions of gamers unable to access their service. Most recently, on Monday February 22, Xbox Live suffered from another service outage that left users unable to play digital games or use services like Netflix and Hulu.

Xbox Live has faced minor outages since the beginning of the year, leaving customers upset and venting on social media. Over the last week, Xbox Live has experienced some of the worse service degradation since the famous Lizard Squad attack on Christmas day 2014. Xbox has confirmed that they are experiencing issues on their status page but have not elaborated on what or who is behind the cause of these outages.

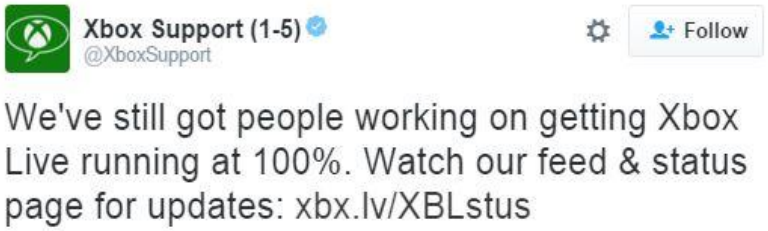

Figure 1: Tweet from Xbox Support on February 14 regarding a service outage

According to analysis by Radware's Emergency Response Team, the hacktivist group New World Hackers is behind one of the outages. They have claimed responsibility for launching two massive DoS attacks against Xbox on February 14 and 22. Recently, The New World Hackers also claimed responsibility for the alleged 602Gbps attack on the BBC[i] and another attack on Donald Trump's mail server. The New World Hackers are using their stressor service, formally known as BangStress, to conduct these large-scale DoS attacks.

Figure 2: New World Hackers claim responsibility for the Xbox outage on February 22

Reasons for Concern

1) **The gaming industry continues to experience attack campaigns constantly**. Upset gamers and hacktivist groups have been persistently targeting the gaming industry. In some attacks, the gaming companies are among a diverse group of targets while others are targeted specifically. 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 a easy and efficient attack, allowing the attacker to cause more damage leveraging fewer resources.

2) **The popularity and use of booter and stressor services is increasing**. These services are now available for hackers and hacktivists to conduct DoS attacks. Booter and stressor services are quite affordable and easily accessible. These tools pose a major concern as the user does not have to have prior knowledge about how a DoS attack works, thus becoming a replacement for LOIC. In addition, many stressor services use *multi-vector attacks* utilizing UDP, NTP, SSDP, SSYN, ESSYN, XML-RPC, Chargen and Dominate protocols.

3) **New powerful stressor services recently released.** Recently, the Lizard Squad has released a new version of their stressor service, Shenron. The New World Hackers have also released their group stressor to the public after the BBC attack. For as little as $20 you can launch 20-minute attacks, but not concurrently, for a month.

In its 2015-2016 Global Application and Network Security Report, Radware predicted the gaming industry to be in center of the 2016 “ring of fire”, with a high likelihood to experience DDoS attacks.

Targets

- Xbox Live

Attack vectors

- Denial of Service
  - New World Hackers
  - Lizard Squad

How to Prepare

Attacks like these are difficult to predict. Steam, Xbox Live, PlayStation Network, along with other gaming companies like ABC game servers[ii] will consistently be the target of DOS attacks. These attacks are designed to cause service outages due to vulnerabilities in server applications or a large amount of traffic aimed at a weak network. Radware offers a full range of solutions to help networks properly mitigate attacks similar to the ones used against Xbox Live. Radware’s DefensePro can help networks with real time, behavioral-based attack mitigation and its Attack Mitigation Services can aid in detection and mitigation via cloud-based volumetric attack scrubbing.

Organizations at Risk Should Consider

- A robust security architecture that actually delivers infrastructure protection from both network and application-based DDoS attacks, as well as from sophisticated web-based intrusions to prevent defacement, information theft and loss of reputation.
- 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 cyber-security emergency response plan that includes an emergency response team of experts and processes in place. Identify areas where a third party's help is needed.
- 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. Maintaining and inspecting your network often is necessary in order to defend against these types of 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.

---

[i] http://www.bbc.com/news/technology-35213415
[ii] https://twitter.com/ABCGameServers/status/701922983208685568