# ERT Threat Alert

## 2016 Summer Olympics: In The Crosshairs

**July 15, 2016**

## Background

As the 2016 Summer Olympics approach, the cyber community turns its attention to the crowds and target-rich environment created by this high profile sporting event. Over 500,000 attendees to Rio De Janeiro are expected to consume record breaking connectivity volumes. This enormous demand will pose a security challenge for service providers as the 2016 Summer Olympics have the potential to be one of the most vulnerable sporting events in modern history and will provide cyber criminals with numerous opportunities.

## Possible Threats

Cyber criminals focus on identity theft by deploying malicious software designed to harvest and steal personal information. Technologies designed to enhance the spectator experience also poses challenges. Internet Service Providers (ISP), sponsors, online merchandise stores, gambling websites, hotels, and even federal and city administration networks are potential targets. Each has a different threat scenario based on the vector of attack.

1. **Denial of Service**
   Considering the high volumes of traffic service providers will cope with, it would not take a sophisticated attack to take an ISP down - a massive DDoS attack via a reflective method in combination with the natural peak of traffic may suffice. Denial of service attacks can be generated via a botnet network. In addition, a determined group of hackers can leverage multi-vector techniques combining network floods with various low and slow attacks (such as SlowHTTP POST, Pyloris, Torshammer, etc.) and even encrypted attacks (such as renegotiation or THC SSL). These attacks can be launched against any of the potential targets listed above.
2. **Application attacks**
   Hacktivists and criminals will launch application attacks like SQL injections in an attempt to steal Olympic data. Information on the attendees, sponsors, or athletes can be quickly monetized or used to post publicly in an attempt to shame the Olympics for a social or political reason. Criminals will also use fake applications and websites to target patrons. Hackers will use attack vectors like Cross site scripting against vulnerable webpages associated with the games so they can inject a client-side script into the user's browser.
3. **Skimmers**
   Criminals will be deploying skimmers on ATMs and Point-of-Sale systems all over Rio de Janeiro. It allows hackers to record the ATM user information and later sell it in the dark market. The larger the crowd, the higher number of victims.
4. **Rogue access points**
   As part of their preparations, hacktivists and cyber criminals have already assessed access points and their vulnerabilities across Rio de Janeiro. They will be using access points to target unsuspecting tourists by choosing a similar name to a trusted network.
5. **Mobile device compromise**
   The threat of a targeted attacks on high profile visitors.
   - Juice-jacking – Malicious charging stations used to write malware on a device while charging.
   - Evil twins – A common MITM tactic using malicious access points that has the same name as legitimate access points. Once connected, malware can be injected onto devices or its traffic can be inspected.

Visitor devices could be targeted by cyber criminals. Fake charging stations or access points can quickly allow an attacker to gain root access into a device. Once infected, devices can perform tasks like record audio and video, take photos, send text messages, open webpages, steal user data, delete files, launch denial of service attacks via HTTP floods, and perform web injections.

## Targets

- International Olympic Committee
- Carriers & Service Providers
- Olympic sponsors
- Media
- Venues

## How to Prepare

Technology can provide a more immersive and rewarding experience for fans, but also create problems and security risks for those managing the event. The Brazilian government and businesses associated with the Olympics should understand the risk and their exposure. Here are suggestions for both attendees and those hosting the 2016 Summer Olympics in Rio de Janeiro.

### Effective Enterprise DDoS Protection Considerations

- 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.

### Protection from SQL Injections and Web Application Vulnerabilities:

- Shortest time from deployment to a full coverage of OWASP Top-10.
- Continuously adaptive protection – recognizing and patching application changes in real time.
- Combination of positive and negative security models for a minimal false-positives rate.
- Automatic and real time generation of policies to protect from zero-day, unknown attacks.
- IP-agnostic device fingerprinting - having the ability to detect attacks beyond source-IP using by developing a device fingerprint that enables precise activity tracking over time.

### Mobile Device Security Tips for Travelling Individuals and Visitors:

- Carry a clean device if possible
- Leave unnecessary devices and documents at home
- Back up your device before you go if it's not a clean phone
- Ensure your phone is updated with the latest operating system
- Disable Bluetooth when not in use
- Disable Wi-Fi when not in use
- Use the verified Wi-Fi when device is in use
- Use VPN
- Change your passwords before and after your trip
- Have RFID shields to protect RFID cards
- Be careful when using ATMs – Understand how to spot and avoid card skimmers gathering card data at stadium ATMs.
- Exercise caution when presented with pop ups while browsing.

- Avoid Olympic related scams delivered via email.

**Network Security Assessment Tips for Olympic Venue Operators:**
Radware recommends that stadium operators review their network between events and inspect networks as necessary in order to defend the threats presented during the Olympics.

- Ensure hardware is up to date
- Regularly patch devices in the stadium
- Conduct audits of the network between games
- Access Control List (ACL) – Filtering network traffic
- Use load balancing for traffic distribution
- Have network and application protection to detect, mitigate and report

## 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.