ERT Threat Alert
2020 Summer Olympics
March 12, 2020

Abstract

With over 7.8 million tickets for sale, the 2020 Summer Olympics in Tokyo, Japan will bring even larger crowds than the 2016 Summer Olympics in Rio De Janeiro, Brazil.

The expected crowds, the use of emerging technologies and the attention generated around the 2020 Summer Olympics will present security challenges for Olympic organizers, partners, sponsors, suppliers, service providers and attendees. Over the last decade, there have been numerous cybersecurity-related events aimed at those involved with the Olympics. Some of these events were recently highlighted in the Cyber Threat Alliance's (CTA) 2020 Summer Olympic Threat Assessment.

Radware researchers assess with moderate confidence that the 2020 Summer Olympics will see similar attacks to the ones that targeted the 2016 Olympic games.

Background

The 1964 Summer Olympics in Tokyo were the first games to be broadcast in color. Since then, the Olympics have altered how we view sporting events. The 2020 Summer Olympics will deliver new breakthrough in technology with the widespread deployment of 5G networks, 3D athlete tracking and 8K broadcast resolution.

The 2020 Summer Olympics will be one of the most technologically advanced sporting events in history. Spectators won't just be presented with a series of smart stadiums. They will be presented with one of the most connected cities in the world and a glimpse into how technology will influence future sporting events. Spectators will be able to interact with human support robots or ride in an autonomous taxicab. There will also be a variety of multimedia technologies and digital devices deployed for streaming content, providing viewers around the world with immersive and interactive experiences.

Providing spectators with additional connectivity and technological innovations is always a double-edged sword. While connectivity provides a better user experience, additional technology and innovation can create a larger attack surface for cybercriminals.

During the opening ceremonies of the 2018 Winter Olympics, the world witnessed what a cyberattack could look like on a large, connected environment. While spectators were attempting to access the stadium for the opening ceremonies, a piece of malware named "Olympic Destroyer" began knocking official Olympic websites offline, causing service degradation for the stadium's wireless network that disrupted the broadcast of the event. A single piece of malware was able to globally disrupt the games and further strain geo-political tensions.

Radware researchers assess with moderate confidence that the 2020 Summer Olympics will face comparable security challenges and see attacks like the ones that targeted the 2018 Winter Olympics. Because of the larger digital landscape in Tokyo and hype surrounding the 2020 Olympics, we expect to see organizers, partners, sponsors, suppliers, service providers and attendees targeted by both nation-state actors and cybercriminals.

Figure 1: Olympic Venues[1]

Venues

- Olympic Stadium
- Tokyo Metropolitan Gymnasium
- Yoyogi National Stadium
- Nippon Budokan
- Imperial Palace Garden
- Tokyo International Forum
- Kokugikan Arena
- Ariake Arena
- Ariake Gymnastics Centre
- Olympic BMX Course
- Ariake Tennis Park
- Odaiba Marine Park
- Shiokaze Park
- Seaside Park Hockey Stadium
- Sea Forest Cross-Country Course
- Sea Forest Waterway
- Canoe slalom venue
- Dream Island Archery Field
- Olympic Aquatics Centre
- Tokyo Tatsumi International Swimming Center
- Baji Koen
- Musashino Forest Sport Centre
- Tokyo Stadium
- Saitama Super Arena
- Asaka shooting Range
- Kasumigaseki Country Club
- Makuhari Messe International Convention Complex
- Enoshima Yacht Harbour
- Izu Velodrome
- Izu Mountain Bike Course
- Sapporo Dome
- Miyagi Stadium
- Saitama Stadium
- International Stadium Yokohama
- Olympic Village
- IBC/MPC Tokyo International Exhibition Center

Official details about each stadium can be found on the Olympic venues webpage.

Potential Targets

- International Olympic Committee (IOC)
- Carriers
- Service Providers
- Sponsors
- Partners
- Suppliers
- Subcontractors
- Media
- Journalist
- Hotel
- Venues
- Athletes
- Spectators

[1] https://tokyo2020.org/

Attack Vectors

Phishing

Phishing is an attempt to obtain sensitive information, such as usernames, passwords and credit cards, or access protected resources by leveraging malicious emails designed to appear as if they originated from a trustworthy source. These attempts are either sent to everyone in the company or designed to specifically target key associates (spear phishing). Once someone becomes a victim of a phishing attack, the attacker will then have the sensitive information required to gain access to certain systems. It's expected that phishing emails targeting Olympic organizers, partners, sponsors, suppliers, service providers and attendees will leverage Olympic-related messages, offers for tickets or leverage COVID-19-related content.

Malicious Domains

Malicious domains are registered domains designed for malicious intent. Users are normally directed to these sites via ads for fake giveaways or tickets on social media via email or popups. Malicious domains look to hijack names of cities, venues or events to trick users via typo squatting into entering their credentials by spoofing the content of the original website. More advanced forms of malware contain domain-generating algorithms (DGAs) to evade solutions based on signatures or blacklisting. Due to the hype generated by the 2020 Olympic games, it's expected that cybercriminals will be looking to profit off those searching for Olympic tickets in the resell market.

Denial-of-Service

Considering the high volumes of traffic service providers will cope with during the games, it would not take a sophisticated attack to disrupt an ISP. A massive DDoS attack via a reflective method combined with a spike in network traffic, could be enough to cause service degradation or an outage. Denial-of-service attacks can be generated via an IoT botnet such as Mirai, open resolvers such as DNS and NTP servers, or from a single server. Criminals often leverage multivector attacks by combining network floods with various low and slow attacks and encrypted, DDoS attacks to cause an outage. To make things worse, technologies like 5G and 8K streaming will result in higher volumes of traffic. A network spike at the Olympics might appear as a DDoS attack. Many DDoS mitigation solutions are rate-based and will drop traffic above a certain threshold. Behavioral algorithms will make distinction between attack and legitimate user traffic more accurate and detect unknown attacks with minimal false positives.

Application Attacks

Cybercriminals will launch application attacks like SQL injections, password cracking, cookie poisoning, cross-site scripting and session high jacking to steal Olympic and spectator data. Information on the attendees, sponsors or athletes can be monetized or used publicly. Criminals will also use fake applications and websites to target patrons.

Compromised Access Points – Risk of MITM

Cybercriminals may have already assessed access points across Olympic venues. They will set up fake access points to intercept and manipulate their victims browsing and to steal passwords, credit cards, PII and other sensitive information. A common man-in-the-middle (MITM) tactic using malicious access points is to name a fake access point as the same name of the legitimate access point. Once a user is connected, malware can be injected onto their device.

Reasons for Concern

The Olympics will create a large platform for cybercriminals to spread a message, generate profits or create disruption. To make matters worse, it is easy for cybercriminals to carry out largescale and disruptive attacks in 2020. Toolkits and attack services are widely available for purchase and attack techniques have improved over the last two years.

Most cybercriminals focus on identity theft by spreading malicious software designed to harvest and steal personal information. Connected devices designed to enhance the spectators' experience, such as Wi-Fi, Bluetooth and other digital services, are the ones exploited to harvest information from attendees.

One of the biggest concerns about the Olympics is protecting applications and networks that support the event. Broadcast networks, industrial control systems, operational networks and other related systems, are at risk following the 2018 Olympic cyberattacks.

Mobile devices are also at risk for athletes and viewers. Athletes are targeted for espionage and spectators are targeted for personal information and financial credentials. Connected venues also become a BYOD nightmare for event management and wireless network operators. Open Wi-Fi networks present one of the biggest attack vectors for network and malware-based attacks and are an easy target for cybercriminals.

5G networks have little to no experience with such dense environments as the one proposed by the Olympics because they are relatively new. The attack surface of 5G networks has not been subjected to cyberattacks and could lead to new attack vectors.

Common types of attacks at the Olympics may include:

- Compromising unsecure and vulnerable access points
- Deploying evil twins or fake cell phone towers
- Spreading malware via phishing
- Data mining using fake pop ups, text messages or spoofed websites
- Denial-of-service attacks on critical applications
- Injection attacks aimed at stealing data

Several organizations associated with the 2020 Summer Olympics have already been targeted by phishing attacks. In December of 2019, the 2020 Summer Olympics staff published an alert about an ongoing phishing campaign designed to appear as if it originated from the Tokyo Organizing Committee[2]. Later in the month a second phishing campaign was disclosed after the Special Olympics of New York had its email servers hacked for the purpose of phishing previous donors.[3]

How to Prepare

Technology can provide a more immersive and rewarding experience for fans. It can also create problems and security risks for those managing the networks. Those that sponsor, support or supply the Olympics should understand the risks. Here are suggestions for both attendees and those hosting the 2020 Summer Olympics in Tokyo.

Attendees/Users: How to Prepare for the Summer Olympics

- Ensure your phone is updated with the latest operating system
- Disable Bluetooth on your cell phone when not in use
- Disable Wi-Fi when not in use
- Only use the official event Wi-Fi
- Rent a pocket Wi-Fi device with a local plan
- Always use a VPN
- Have RFID shields to protect credit and identity cards
- Be careful when using ATMs – Understand how to spot and avoid card skimmers
- Exercise caution when presented with popups while browsing
- Avoid Olympic-related scams delivered via email

[2] https://www.cisomag.com/tokyo-2020-authority-warns-against-phishing-emails/
[3] https://www.bleepingcomputer.com/news/security/special-olympics-new-york-hacked-to-send-phishing-emails/

Event Operators: How to Prepare for the Summer Olympics

Radware recommends that operators review their network between events and inspect networks when necessary to defend against threats that are specific to the Olympics.

- Ensure hardware is updated, default passwords are reset and unnecessary services are disabled
- Conduct audits of the network between games
- Scan for rogue access points
- Access Control List (ACL) – Filtering network traffic
- Use load balancing for traffic distribution
- Have network and application protection to detect, mitigate and report attacks

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

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.