Radware Cybersecurity Alert

FIFA World Cup

November 14, 2022

The FIFA World Cup in Qatar is just days away and with COVID restrictions lifted, football fans will no doubt head en masse to attend the first World Cup held in the Middle East. The expected crowds, use of emerging technologies and attention the World Cup always creates will present security challenges for Qatar, FIFA organizers, partners, sponsors, service providers, athletes and attendees.

Radware researchers assess with moderate confidence that the 2022 FIFA World Cup in Qatar will experience similar attacks to those that targeted the Olympics games in Korea and Japan.

Background

Since the last world cup in 2018, which was hosted by Russia, the threat landscape has evolved significantly. This year's world cup in Qatar will run from November 20th until December 18th. It's usually held in May and June, but this year's is scheduled for November due to the intense heat in the Middle East. Thirty-two countries will compete in 64 matches held in eight different stadiums in 5 Qatari cities. The largest stadium, Lusail Iconic Stadium, is capable of holding 80,000 spectators.

For the last decade, Qatar has faced intense criticism and cyberattacks related to bid corruption, and the treatment of workers involved with the construction of the stadiums. Adding to the challenging atmosphere surrounding the World Cup, Russia has been banned from participating in the World Cup due to due to its invasion of Ukraine, state-sponsored threat targeting of anti-doping agencies, and interference with prior Olympic Games. As a result, there is an escalated risk of Russian and foreign interference by threat actors as the event approaches.

Venues

- Lusaka Iconic Stadium
- Al Bayt Stadium
- Stadium 974
- Al Thumama Stadium
- Khalifa International Stadium
- Education City Stadium
- Ahmad bin Ali Stadium
- Al Janoub Stadium

Radware Cybersecurity Alert

FIFA World Cup

November 14, 2022

Potential Targets

- FIFA
- Government of Qatar
- Athletes
- Partners
- Sponsors
- Spectators
- Carriers/ISPs
- Contractors
- Media/Journalist
- Hotels/Hosts

Attack Vectors

PHISHING

Phishing is an attempt to obtain sensitive information, such as usernames, passwords, credit cards or access-protected resources by leveraging malicious emails designed to appear as originating from a trustworthy source. These attempts are sent to everyone in the company or designed to target critical associates (spear phishing) specifically. Once someone becomes a victim of a phishing attack, the attacker will typically drop information stealers to harvest valid credentials. It's expected that phishing emails targeting FIFA organizers, the Government of Qatar, athletes, partners, sponsors, spectators, and service providers will leverage some form of World Cup related messaging, ticket offering, or misinformation designed to harvest data and undermine the integrity of the event.

MALICIOUS DOMAINS

Malicious domains are registered domains designed for malicious intent. Users are typically directed to these sites via ads for fake giveaways or tickets on social media, emails or popups. Malicious domains look to hijack the names of cities, venues, or events to trick users via typo squatting into entering their credentials by spoofing the content of the intended website. Due to the hype generated by the FIFA World Cup in Qatar, it's expected that cybercriminals will be looking to profit off those searching for tickets in the resell market or looking to stream out-of-market games.

DENIAL-OF-SERVICE

Considering the high volumes of traffic service providers will cope with during the World Cup, 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. Even a simple network spike might appear as a DDoS attack. Denial-of-service attacks can easily be generated via botnets such as Mirai or Meris, open resolvers such as DNS and NTP servers, or from a single server. Many DDoS mitigation solutions are rate-based and will drop traffic above a certain threshold. Behavioral algorithms will distinguish between attack and legitimate user traffic more accurately and detect unknown attacks with minimal false positives. It is important to remember the most Denial-of-Service are designed to undermine the targets integrity versus causing long term outages, as seen in the **recent attacks against US critical infrastructure.**

APPLICATION ATTACKS

Cybercriminals will launch application attacks like SQL injections, password cracking, cookie poisoning, cross-site scripting, and session high jacking to steal data from spectators and event organizers. Criminals will also use fake applications and websites to target patrons to gain access to valid credentials. Information on the attendees, sponsors, or athletes can be easily monetized or used publicly to undermine the World Cups' integrity.

Reasons For Concern

The FIFA World Cup in Qatar will create a platform for cybercriminals to spread propaganda, generate profits, and create disruption. To make matters worse, in the post-covid era, it has become increasingly easier for cybercriminals and the average citizens to carry out disruptive attacks. Toolkits, attack services, and initial access are widely available for purchase across the internet, and as a result of the growing cyber conflict in Eastern Europe, attack techniques have improved.

Most cybercriminals at significant sporting events focus on identity theft by spreading malicious software designed to harvest and steal personal information before the World Cup. During the World Cup, connected devices designed to enhance the spectators' experience, such as Wi-Fi, Bluetooth, and other digital services, are often exploited to harvest personal identifiable information(PII).

One of the biggest concerns for network operators surrounding large-scale sporting events such as the FIFA World Cup in Qatar is protecting networks and applications that support multiple stadiums. Broadcast networks, industrial control systems, operational networks, and other related systems are all considered at risk following the Russian state-sponsored cyberattacks that targeted anti-doping organizations and the opening ceremonies of the 2018 Winter Olympics.

Radware Cybersecurity Alert

FIFA World Cup

November 14, 2022

Common Attacks

- Compromising unsecured and vulnerable access points
- Deploying evil twins or fake cell phone towers
- Spreading malware via phishing or malicious domains
- Data mining using fake pop ups, text messages or spoofed websites
- Denial-of-service attacks on critical applications
- Information stealers aimed at harvesting spectators data

Several organizations associated with the FIFA World Cup in Qatar have already been targeted by hacktivist in recent months with attack vectors ranging from simple defacements to network outages caused by Denial-of-Service attacks. These attacks are aimed at spreading a message or causing short lived outages designed to undermine the integrity of the World Cup. Currently, the hacktivist group Anonymous is launching cyberattacks against Qatar and FIFA in an attempted to remove the Iranian soccer team from the World Cup as a result of violent protest in the country.

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 directly and indirectly involved with the FIFA World Cup in Qatar should understand the risks.

How Attendees/Users Can Prepare For The FIFA World Cup

- Ensure your devices are updated with the latest operating system
- Disable Bluetooth and Wi-Fi on your device when not in use
- Only use the official event Wi-Fi and use a VPN when possible
- 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 FIFA related scams delivered via email or on social media

Event Operators: How To Prepare For The FIFA World Cup

Radware recommends that operators review their network between events and inspect networks when necessary to defend against threats that are specific to the FIFA World Cup in Qatar.

- 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 Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

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 RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.