ERT Threat Alert
2018 FIFA World Cup
June 7, 2018

Abstract
Cybercriminals and hacktivist are getting ready to disrupt the digital experience during 2018 FIFA World Cup™*. Russian authorities, sponsors, service providers, and even stadium networks, are expected to be targeted throughout the months of June and July via a variety of methods for both personal gain and cyber-vandalism.

Background
As the 2018 FIFA World Cup approaches, Radware's Emergency Response Team (ERT) team turns its attention to the crowds and target-rich environments created by high profile sporting events. This year, Russia will host the 21st FIFA World Cup. This marks the first time that the World Cup has been held in Europe since the 2006 World Cup in Germany. This is also the first time the World Cup has been hosted in a Eastern European country. A total of 64 matches will be played in twelve stadiums across eleven Russian cites, with the final match taking place on July 15th in Luzhniki Stadium, Moscow.

The 2018 FIFA World Cup brings large crowds to Russia, not only creating a huge demand for connectivity, but also a serious security risk for FIFA organizers, partners, sponsors, suppliers, and service providers that must be able to protect themselves and stadium networks against the threat of network- and application-attacks. The enormous demand creates a challenge of distinguishing between a flash crowd and a DDoS attack.

Threats
1. **Data Theft**
   Hackers, whether their motives are political, social, or financial, can take advantage of public networks (transportation hubs, cafes, and the stadium networks) at the FIFA World Cup to steal personal data such as usernames, passwords, credit card information or to use the event to spread malware or propaganda.
2. **Nation-State Cyberattacks**
   Recently, Russia was blamed for the cyberattacks that took place during the opening ceremonies at the 2018 Winter Olympics in PyeongChang, South Korea[1]. It was also reported by the Security Service of Ukraine that the recent Russian botnet, VPNFilter[2], was being staged to attack the UEFA Champions League match in Kiev, Ukraine[3] before being dismantled. Radware does not have intelligence on a planned nation-state attack, but we suspect that the World Cup may attract adversaries of Russia to launch attacks.
3. **Hacktivism**
   The FIFA World Cup involves large monetary investments. Key brands are sponsoring the event, and by placing themselves front and center, become potential targets.

Case Study
One of Radware's customers was a sponsor of the 2016 UEFA European Championship. Throughout the tournament, this organization suffered 175,000 web-based attacks against its network and 4 large DDoS attacks. All were mitigated without generating any false-positives and zero false-negatives.

[1] https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.fb210591879e
[2] https://blog.talosintelligence.com/2018/05/VPNFilter.html
[3] https://ssu.gov.ua/ua/news/1/category/2/view/4823#.HAqT76ut.dpbs

Blocked	100.00 % (175,533)
URL Access Violation	47.28 % (82,984)
Server Information Leakage	25.79 % (45,274)
Predictable Resource Location	6.95 % (12,192)
HTTP RFC Violation	5.80 % (10,179)
File Upload Violation	5.45 % (9,575)
Path Traversal	3.05 % (5,345)
Code Injection	2.19 % (3,840)
SQL Injection	1.42 % (2,496)
Server Misconfiguration	1.30 % (2,279)
Other	0.78 % (1,369)

Figure 1: Distribution of web-attacks against Radware's customers during the month of the 2016 UEFA European Championship

Venues & Hosting Cities

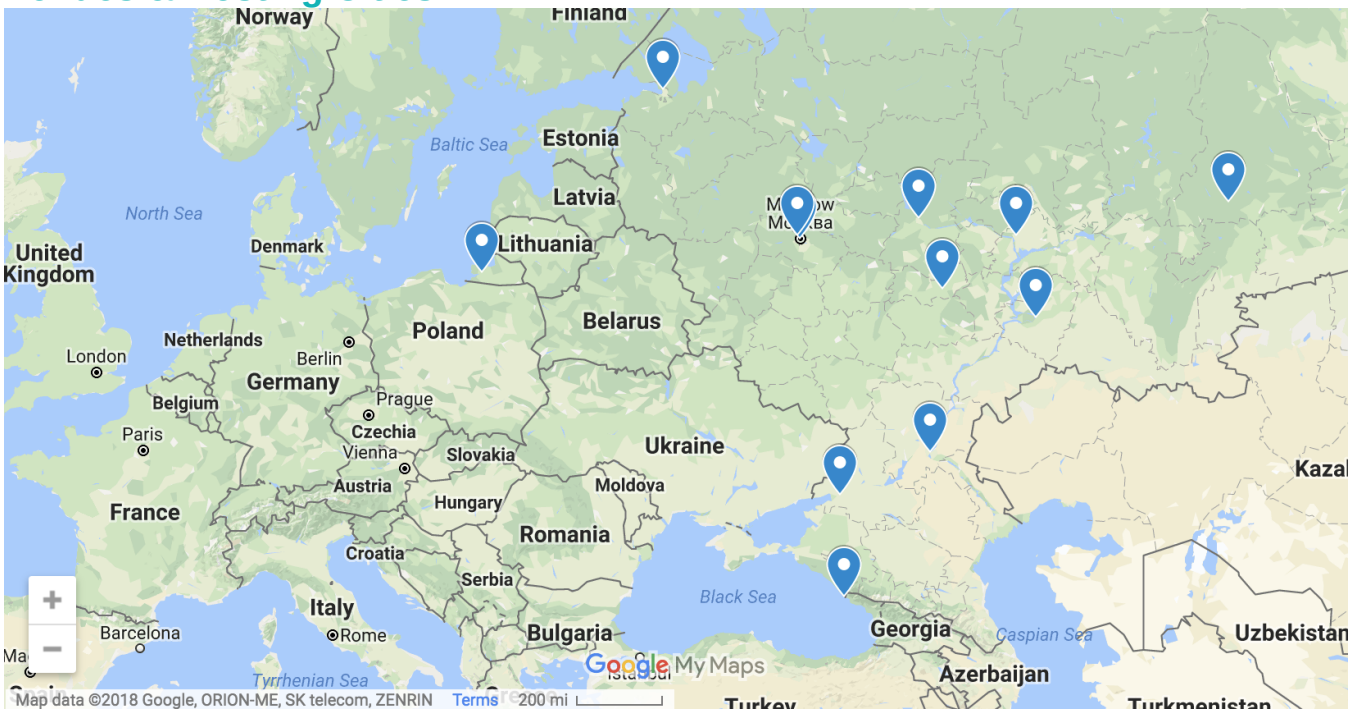

Figure 2: Source: http://www.stadiumguide.com/tournaments/fifa-world-cup-2018/

- Luzhniki Stadium in **Moscow** - Seats 81,000
- Otkritie Arena in **Moscow** - Seats 45,360
- Krestovsky Stadium in **Saint Petersburg** - Seats 68,134
- Fisht Olumpic Stadium in **Sochi** - Seats 47,659
- Cosmos Arena in **Samara** - Seats 44,918
- Kazan Arena in **Kazan** – Seats 45,379
- Rostov Arena in **Rostov-on-Don** - Seats 45,000
- Volgograd in **Volgograd** - Seats 45,568
- Nizhny Novgorod Stadium in **Nizhny Novgorod** – Seats 44,988
- Mordovia Arena in **Saransk** – Seats 44,442
- Central Stadium in **Yekaterinburg** - Seats 35,696
- Kaliningrad Stadium in **Kaliningrad** - Seats 35,212

Targets

The following are the partners, sponsors and supporters – as stated on the FIFA World Cup website – that are considered under threat. It is possible that more organizations will be added when the World Cup starts.

- FIFA
- Stadiums/Venues
- Carriers & Service Providers
- FIFA Partners
    - Adidas
    - Coca-Cola
    - Gazprom
    - Hyundai-Kia
    - Qatar Airway
    - VISA
    - Wanda Group
- FIFA World Cup Sponsors
    - Anheuser-Busch InBev
    - ViVo
    - Husense
    - McDonald's
    - Mengniu Dairy
- Supporters
    - Alfa-Bank
    - Alrosa
    - Rostelecom
    - Russian Railways
    - Yadea

Reasons for Concern

Radware's ERT and researchers are currently assessing the threat landscape of the 2018 FIFA World Cup. Most cybercriminals and hacktivist will be focused on identity theft by spreading malicious software designed to harvest and steal personal information. Often, the technologies designed to enhance the spectators' experience, such as Wi-Fi, Bluetooth and other digital services, are exploited to harvest this information from attendees.

One of the biggest concerns at the 2018 FIFA World Cup will be protecting critical applications and networks that support the event. **Broadcast networks, industrial control systems, civil-service networks** are considered systems that are at greatest risk.

Attack Vectors

Phishing

A digital attempt to obtain sensitive information from a victim by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent out to everyone in the company or designed to specifically target key associates. Once an associate falls victim to these the hacker will then have the sensitive information required to gain access to certain systems.

Malicious Domains

Malicious domains are registered domains designed for malicious intent. Users are normally directed to these sites via fake giveaways for tickets promoted on social media. Bad 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.

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, combined with the natural peaks of traffic, may

be enough to cause service degradation. Denial-of-service attacks can be generated via an IoT botnet such as Mirai. Hackers can leverage multi-vector techniques by combining network floods with various low and slow attacks and even encrypted distributed DoS attacks to cause an outage. A consumption spike might appear as a DDoS attack. Many DDoS mitigation solutions are rate-based and will drop traffic above a certain threshold. Behavioral algorithms make an accurate distinction between attack and legitimate user traffic and also instantly detect unknown attacks at a minimal false-positive rate.

Application Attacks
Hacktivists and criminals will launch application attacks like SQL injections, password cracking, cookie poisoning, cross-site scripting^, and session high jacking in an attempt to steal FIFA and spectator data. Information on the attendees, sponsors, or athletes can be quickly monetized or publicly used. Criminals will also use fake applications and websites to target patrons.
^ *Cross-site scripting against vulnerable webpages - injecting a client-side script into the user's browser.*

Remote Code Execution
In an RCE attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.

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.

Network Security Assessment Tips for FIFA World Cup Venue Operators, Sponsors and Supporters
Radware recommends that stadium operators review their network between events and inspect networks as necessary in order to defend the threats presented during the FIFA World Cup.

- Ensure hardware is udpated
- 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

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

Under Attack and in Need of 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.

*FIFA, World Cup 2018, Russia 2018, 2018 FIFA World Cup and all related logos are trademarks of FIFA or its affiliates