Abstract

As Super Bowl LIII approaches, Radware's Emergency Response Team (ERT) turns its attention to the crowds and the target-rich environments created by high profile sporting events. The Super Bowl, like previous years, will bring large crowds that demand seamless connectivity and that will consume record-breaking volumes this year. Extreme Networks reported that last year's attendees at Super Bowl LII transferred 16.32 terabytes of data with a peak rate of 7.867 Gbps. This enormous demand for connectivity poses a security risk for event organizers, partners, sponsors and attendees.

Figure 1: Super Bowl LIII map / Source: NFL.com

Background

There are few sporting events in the world as significant as the Super Bowl. Last year there was an estimated 103 million viewers and this year advertisers are expected to pay nearly $5 million for a 30-second commercial. Beyond just the game, there is a variety of multimedia technology available to fans, providing a more immersive and interactive experience. These experiences include Super Bowl LIVE, a six-day series of concerts and events in Centennial Olympic Park, and the Super Bowl Experience, an eight-day event full of immersive exhibits and interactive games. Other activities also include the Verizon Experience that will showcase how 5G wireless technology will change the fan experience in stadiums moving forward.

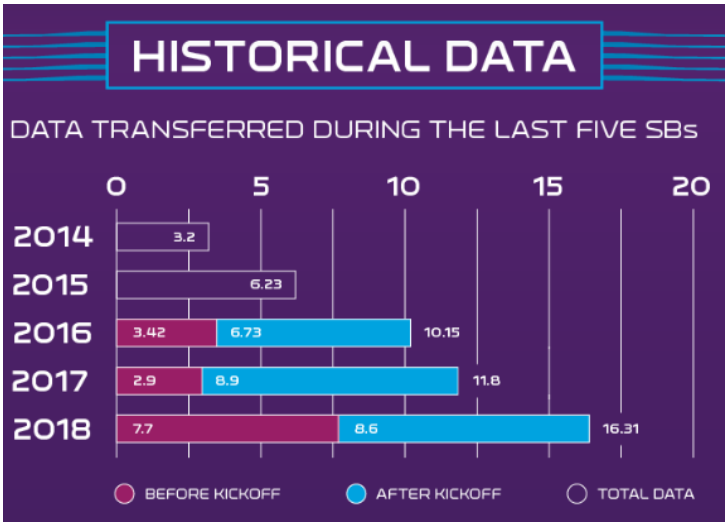

Figure 2: Historical data for the Super Bowl (Source: Extreme Networks)

To ensure attendees have a seamless digital experience, the NFL, Georgia World Congress Center, AMB Sports and Entertainment Group and wireless carriers have made significant investments into the construction of the networks to maintain a high quality of service for the attendees and vendors. The stadium provides 15,000 Ethernet ports, 1,800 access points, and a Distributed Antenna System (DAS) for enhanced cellular coverage from all four major United States cellular carries. The stadium's Wi-Fi is provided by AT&T and consists of two redundant 40GB connections. The stadium also has pulled fiber as close to the access points as possible, terminating in mini intermediate distribution frames (IDF) throughout the stadium. The network gear is from Aruba and Hewlett Packard Enterprise. Others involved with the network include IBM, Corning and ThinkAmp. The stadium also contains 2,000 IPTVs for delivering game content. Mercedes-Benz Stadium also promotes a mobile application. While this application is not as advanced as applications for other stadiums, it does include information about the stadium, news, scores, ordering food for pickup as well as viewing, buying and transferring tickets and parking. These features and networks help ensure fans can watch, eat, share, download and communicate their gameday experience with others.

Figure 3: Wireless AP and DAS

Figure 4: Mini ISFs

Targets

- NFL
- Georgia World Congress Cneter
- AMB Sports and Entertainment Group
- Carriers
- Service Providers
- Sponsors and Partners
- Suppliers and Subcontractors
- Media
- Journalist
- Hospitality
- Spectators

Reason for Concern

Radware's ERT has assessed the threat landscape created by Super Bowl LIII in Atlanta. One of the biggest concerns will surround protecting critical applications and networks that support the event, hosted both locally and in the cloud. Broadcast networks, industrial control systems, civil-service networks, and other related systems are all at risk as well. While there hasn't been a recent attack of scale reported against the Super Bowl, last year we did witness a piece of malware named Olympic Destroyer target and disrupted the opening ceremonies and entry into the 2018 Winter Olympics in PyeongChang.

Major sporting events create a platform for cybercrime, though recently most cybercriminals and hacktivist have been focused on identity theft. They do this by spreading malicious software that is designed to harvest and steal personal information. Today's High Density (HD) stadiums, theaters, arenas, and amphitheaters require small cells, Wi-Fi, and DAS deployments to serve their demanding environments. The technologies designed to enhance the spectators' experience, such as Wi-Fi, Bluetooth, and other digital services, are the ones that are often easily exploited to harvest information from attendees.

For Super Bowl LIII, most cybercriminals will focus on identity and financial theft in the days leading up to the game. These attacks will often be baited with promotions for Super Bowl tickets or a trip to Atlanta for the game. Another concern surrounds the current Wi-Fi. The networks name is **'attwifi'** and does not present the users with a login portal. While this makes it incredibly user-friendly, it also makes it easy for malicious actors to deploy evil access points in hopes an unsuspecting fan connects to it and discloses sensitive information.

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 target key associates specifically. Once an associate falls victim to these the hacker will then have the sensitive information required to gain access to specific 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 typosquatting 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.

Compromised Access Points

Risk of MITM attacks. As part of their preparations, hacktivists and cybercriminals have likely already assessed access points and their vulnerabilities across the venues. They will set up fake access points to intercept and manipulate their victim's browsing and to steal passwords, credit cards, PII and other sensitive information. A common MITM tactic using malicious access points is to name a fake access point as the same name of the legitimate access points. Once a user is connected, malware can be injected onto their device.

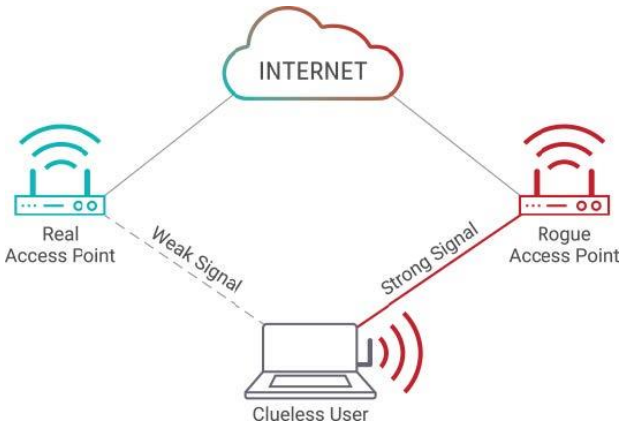

Figure 5: Diagram of a compromised access point

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 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 denial-of-service 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 not only make an accurate distinction between attack and legitimate user traffic but 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, session high jacking, and others in an attempt to steal fan and spectator data. Information on the attendees, sponsors, or athletes can be quickly monetized or publicly used.

ATM Skimmers
Criminals will be deploying skimmers on ATMs and point-of-sale systems in the areas surrounding the stadium. It allows hackers to record the user information and later sell it for profit. The larger the crowd, the higher number of potential victims.

Figure 6: ATM skimmers

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 Super Bowl Operators, Sponsors, and Supporters
Radware recommends that stadium operators, in general, review their network between events and inspect systems as necessary to defend the threats presented in smart stadiums.

- 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

Attendees/Users: How to prepare for the Super Bowl

- 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 official event Wi-Fi when device is in use: **'attwifi'**
    - There will be no portal or advertisements. Join to Connect
- Always use a VPN
- Be careful when using ATMs; understand how to spot and avoid card skimmers gathering card data
- Exercise caution when presented with pop-ups while browsing
- Avoid NFL-related scams delivered via email.

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
- **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

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.