

Super Bowl LVII

Event Assessment

ZeroFox Intelligence

Super Bowl 2023 Event Assessment

TLP: CLEAR

A-2023-02-03a



Introduction

Super Bowl LVII is slated to occur on February 12, 2023, at the State Farm Stadium in Glendale, Arizona, a Phoenix suburb. The matchup will feature the Philadelphia Eagles and the Kansas City Chiefs. This represents the fourth time that the Super Bowl has been hosted in the Phoenix area; the last time was in 2015. Super Bowl weekend will also coincide with the PGA Tour Phoenix Open in Scottsdale, AZ (about 30 minutes from the Super Bowl location), so the area is anticipated to be saturated with visitors from February 9-13, 2023.

As security preparations for the Super Bowl have progressed, one of the more notable developments has been the inclusion of cybersecurity professionals in those preparations in a much more integrated fashion than previously seen. While no credible cyber or physical threats have been identified prior to the event, this represents the awareness around the impact that a cyber event could have on the Super Bowl, and significant work has been done to prepare for various scenarios should an attack occur.

Betting associated with the Super Bowl is one of the most attractive vectors for targeting by threat actors. This event is anticipated to be the highest betting event in sports history, with wagers expected to be in excess of USD 1 billion. This presents an attractive opportunity for threat actors to obtain significant financial gain through scams and fraudulent mobile apps and websites. Other fraudulent activity identified involves fake accommodations leveraging well-known brands, fake tickets at “too good to be true” prices, and fake apps purporting to stream the game.



Source:
<https://deadline.com/2023/01/super-bowl-lvii-2023-philadelphia-eagles-vs-kansas-city-chiefs-state-farm-stadium-fox-1235243882/>

Key Threats



Nationwide protests, including in Phoenix, have the potential to occur during Super Bowl weekend, although none have been identified.



Super Bowl accommodations are at a premium due to the event size and a coinciding PGA event in the area.



Ticketing scams are common at major sporting events such as the Super Bowl.



Betting is anticipated to be the highest ever on this event, providing a lucrative target for threat actors.



Financially-motivated threat actors will seek to leverage fake Super Bowl-related mobile apps and phishing sites.



Third parties present some of the largest cybersecurity risks to the Super Bowl.

Key Findings

- No credible physical or cyber attack plans have been identified that target Super Bowl LVII.
- Physical security preparedness has also included cybersecurity preparations, as a cyberattack would likely have physical security implications as well.
- Ahead of the Super Bowl, 5G infrastructure has been shored up in order to not only maximize the attendee experience but also to maintain the ability of security and emergency personnel to function.
- Accommodations are sparse and extremely expensive, and scams are present to take advantage of attendees searching for last-minute or cheap accommodations.
- The threat of terrorism during the Super Bowl is currently considered low.
- Betting and ticketing scams are highly likely, as Super Bowl LVII is anticipated to be the largest betting event ever.

SCOPE NOTE ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 5:00 PM (EST) on February 2, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.



Physical Security Preparations

Super Bowl LVII is categorized by the U.S. Department of Homeland Security (DHS) as being of the highest threat level to public safety, and security is expected to be heavy within Glendale, AZ, and the surrounding region. At the time of this report, there were no credible physical threats associated with the Super Bowl; however, attendees and locals need to be aware of possible physical security concerns surrounding the event.

Security preparations have been in progress at the stadium and surrounding areas in Glendale, AZ, for several months now, according to Phoenix's Mayor Kate Gallego.[1] There is a combination of public and private security organizations present, with all levels of public security involved. In addition to securing physical assets like the stadium, roadways, public transportation, and power systems, preparations for the game also include protecting all the IT assets that go into making the Super Bowl happen.

In early 2023, Verizon announced a drastic expansion of wireless connectivity in both Phoenix and Glendale to support, among other things, the government and emergency personnel staffing the game, as well as the fans that will be attending. Along with the wireless connectivity expansions, Verizon is scheduled to bring in a mobile network operations center that has previously been used to assist refugee-processing centers in Virginia and hurricane relief in Florida. The mobile facility, which Verizon calls Tactical Humanitarian Operation and Response, or THOR, is designed to ensure that public safety and emergency personnel maintain their priority status on the 5G network on days when usage will be maxed out, which is possible during the Super Bowl.[2]

The exact physical safety plan will not be publicized, but as has been the case in previous years, will involve collaboration by local, state, tribal, and federal law enforcement agencies. Five local governments are coordinating, along with federal agencies including the Federal Bureau of Investigation; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the Transportation Security Administration; and the Coast Guard.

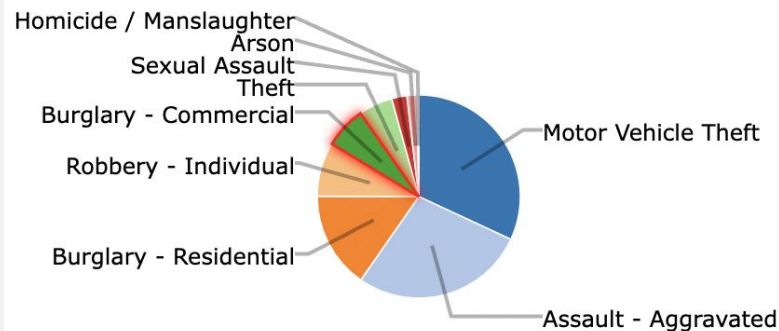
During the January meeting of the Phoenix City Council, it was revealed that the city was expecting 117 bomb technicians and 104 additional explosive device detection canine handlers for the Super Bowl in Glendale and the event's ancillary events in Phoenix, which include concerts, a fan festival, and media events.[3]

Additionally, the Glendale Police Department operates the Real Time Crime Center (RTCC), which uses state and city databases along with Computer Aided Dispatch, ShotSpotter, license plate reader information, and private and public video surveillance systems to accumulate crime intelligence in real time.[4] These tools give RTCC operators the ability to be virtually on-scene prior to the call being dispatched, which allows the operators to supply first responders with critical information about specific incidents, provide situational awareness ahead of officer arrival, and enhance the department's investigative capabilities.

Crime

The areas in and around Glendale, AZ, have some of the highest crime rates in the United States, comparatively. As such, Super Bowl attendees should maintain awareness of their surroundings and avoid situations where they are alone.

As noted below, some of the more common crimes in the area involve Aggravated Assault and Motor Vehicle Theft, which attendees should keep in mind as they travel to and from events.



Source: [hXXps://communitycrimemap\[.\]com/analytic](https://communitycrimemap.com/analytic)

Assessment:

- No credible physical threats have been identified as of the writing of this report.
- Increased security presence, both public and private, will likely assist in handling any criminal activity, as well as deter would-be criminals from committing crimes.
- Physical security preparedness has also included cybersecurity preparations, as a cyberattack would likely have physical security implications as well.
- Ahead of the Super Bowl, 5G infrastructure has been shored up not only maximize the attendee experience but also to maintain the ability of security and emergency personnel to function.
- Criminal activity can be high in the Glendale area, so attendees should maintain awareness of their surroundings and avoid situations where they are alone.

Recommendations:

- Remain with a group when traveling in the Glendale area, especially at night.
- Ensure that vehicles are completely locked with windows up and that valuables are not stored in a viewable area within an unattended vehicle.
- Keep personal belongings somewhere that they cannot be easily pickpocketed.

FOOTNOTES

- [1] [hXXps://fox4kc\[.\]com/news/security-increased-at-state-farm-stadium-ahead-of-super-bowl-lvii/](https://fox4kc.com/news/security-increased-at-state-farm-stadium-ahead-of-super-bowl-lvii/)
- [2] [hXXps://statescoop\[.\]com/phoenix-5g-wireless-infrastructure-super-bowl/](https://statescoop[.]com/phoenix-5g-wireless-infrastructure-super-bowl/)
- [3] [hXXps://www.phoenix\[.\]gov/cityclerk/site/PublicMeetings/230125002.pdf](https://www.phoenix.gov/cityclerk/site/PublicMeetings/230125002.pdf)
- [4] [hXXps://www.glendaleaz\[.\]com/live/city_services/public_safety/police_department/our_community/real_time_crime_center](https://www.glendaleaz[.]com/live/city_services/public_safety/police_department/our_community/real_time_crime_center)



Boycott and Disruptive Activity

The Super Bowl is one of the world's most well-known sporting events. As such, it can also serve as a venue for those looking to garner attention for their causes, such as the Bloodstained Men campaign (an anti-circumcision group), as they know that millions will be watching. Although significant organized protest activity has not been identified targeting Super Bowl LVII, there is always the potential for planned activities to occur unannounced.

In the months leading up to the Super Bowl, there have been some occurrences that have garnered attention. While they have a low probability of resulting in a broader disruption during Super Bowl LVII, they are worth noting. For instance, several business owners in the Phoenix area filed a lawsuit against the city over its implementation of a "clean zone," whereby signage has been restricted in the area around the Super Bowl and must be approved by the NFL in order to be posted.[5] The business owners have argued that this is a violation of free speech and that the restrictions are a hindrance to driving attention towards their business during this tourist-heavy event. A judge ruled that the resolution was unconstitutional on February 2, 2023.[6]

As is typical for sporting events, there are calls on social media for boycott activity towards the Super Bowl due to the teams playing, referees participating, or allegations of rigging by the NFL.[7] At this time, there does not appear to be a coordinated effort that should have a measurable impact on the event.

Fallout from the police-involved death of Tyre Nichols in Memphis continues to generate protests and other demonstrations. On January 28, 2023, a contingency gathered peacefully in downtown Phoenix in support of Tyre Nichols; however, nothing has been identified to date that would indicate a larger-scale event that could impact the Super Bowl.[8] Should additional nationwide events be scheduled, there is the potential for events to take place in the Phoenix area as part of a broader movement.

Assessment:

- Significant planned protest activity during Super Bowl LVII has not been identified to date.
- Boycott activity is unlikely to have a real impact on the Super Bowl, as any calls appear to be decentralized and focus on various topics regularly associated with sports rather than honing in on one specific cause.
- There is a possibility that additional events could be organized in support of Tyre Nichols as part of a broader nationwide movement; however, previous events in the Phoenix area have been peaceful.

Recommendations:

- Should a protest emerge, such activity could draw a response from security personnel or counter-protesters and lead to an escalation in activities.

Terrorism

ZeroFox has identified no evidence of terrorist threats made against the upcoming Super Bowl LVII. Totemic targets of this nature with a global audience and that involve the mass-gathering of spectators represent an attractive target for terrorist actors. While there have been no previous incidents against the Super Bowl, attacks against sporting events and stadia have occurred globally, including in Atlanta in 1996 and in Paris in 2015.

The threat from organized terrorist groups is low. While a number of overseas jihadist terrorist organizations, such as Al-Qaeda (AQ) and the Islamic State (IS), frequently encourage attacks against high-profile targets due to the shock and awe potential, they are unlikely to be able to mount an attack against the Super Bowl directed by core leadership. It is also unlikely that domestic terrorist organizations will seek to target Super Bowl LVII.

Terrorist organization supporter groups and individuals may release "fanboy" media graphics or statements on private platforms threatening an attack. This trend is common with major world events, including holidays, large sporting competitions, or other national celebrations. The greatest threat to Super Bowl LVII comes from individuals galvanized and inspired by this rhetoric targeting the venue or areas where spectators have gathered to celebrate. Lone-wolf attacks are difficult to identify and mitigate due to the limited circle that has knowledge of the attack planning. Following such attacks, terrorist organizations will frequently claim the attack as their own to garner additional publicity and outwardly portray strength. Further investigations later call into question the claimed affiliation.

A terrorist attack would most likely involve the use of easily accessible materials, such as bladed weapons, firearms, or rudimentary improvised explosive devices (IED). ZeroFox Intelligence also notes that the potential for threat actors to use unmanned aerial vehicles, such as drones, is low; the Federal Aviation Administration (FAA) has issued a flight advisory for the times surrounding the Super Bowl, indicating that action could be taken against any Unmanned Aircraft System (UAS) identified.[6] It is also possible vehicles could be used as a weapon to target spectators, related events, or associated facilities in the area surrounding the State Farm Stadium.

FOOTNOTES

- [5] <https://www.12news.com/article/news/community/free-speech-protecting-sponsors-debate-phoenix-super-bowl-clean-zone-nfl/75-23b30367-f816-4383-b400-8e34faaf4aaf>
- [6] <https://www.12news.com/article/sports/nfl/superbowl/judge-rules-phoenixs-super-bowl-clean-zone-resolution-unconstitutional/75-f3b0fe1-8780-4377-9928-41555alc1617>
- [7] <https://www.azfamily.com/2023/01/29/peaceful-protest-phoenix-brings-attention-police-brutality-following-tyre-nichols-death/>
- [8] <https://twitter.com/samueljacobs06/status/1619915901947748352>



Accommodations

The hospitality industry in the Phoenix area has been gearing up for months for Super Bowl LVII by readying their facilities and training additional staff. The PGA Tour Phoenix Open coincides with Super Bowl weekend—the area will be saturated with visitors involved with each event. Phoenix also hosted the Super Bowl and the PGA event simultaneously in 2015 and was able to accommodate the 120,000 plus out-of-state visitors that accompanied those events.[9] However, the 2015 events were pre-COVID-19, and many organizations have not experienced such an influx of visitors since.

There have also been warnings from organizations such as Airbnb about third parties leveraging their brand name and falsely indicating that they are affiliated.[10] These third parties seek to prey on attendees who are looking for good deals and ultimately scam their victims out of money.

Phishing emails, smishing messages, and direct messages on social media can also be sources of fraudulent accommodation activity and frequently direct recipients to nefarious websites.



Source:

[hXXps://twitter\[.\]com/SUPERBOWLHOTELS/status/1620478033395064880/photo/1](https://twitter.com/SUPERBOWLHOTELS/status/1620478033395064880/photo/1)

Grammatical errors and offers that appear too good to be true are frequent red flags of this type of fraudulent behavior.

> Assessment:

- While the Phoenix area is prepared for the upcoming influx of visitors from both the Super Bowl and the PGA Tour event, last-minute, cheap accommodations are unlikely to be available.
- Scammers will seek to target attendees looking for deals and last-minute places to stay in order to capitalize financially on the event.
- Trademarks of the NFL, Super Bowl sponsors, and event participants are likely to be utilized in scams and illegal activity as a means of adding legitimacy to campaigns.

> Recommendations:

- Ensure that reservations are made ahead of time for attendees in order to avoid the risk of not being able to secure accommodations during the event.
- Always make sure that bookings are done through legitimate apps or websites and not through third parties. As indicated, these third parties are frequently not actually affiliated with legitimate hospitality organizations and are looking to scam victims out of money.

Cybersecurity Threats

While ZeroFox Intelligence did not identify specific plans by threat actors to disrupt the event, because of its visibility, a cyberattack cannot be completely ruled out. As such, cybersecurity has been a large focus by security teams in the lead up to Super Bowl LVII. The state of Arizona's Chief Information Security Officer (CISO) has made efforts to shore up all Super Bowl IT assets, including mobile ticketing apps, streaming media, and cashless transactions with stadium vendors.[11]

Arizona's CISO also indicated that, although extreme efforts have been put forth around cybersecurity for Super Bowl LVII, third parties remain one of the primary cybersecurity concerns.[12] These vendors lie outside of the IT perimeter for Super Bowl security, making it difficult to ascertain their vulnerabilities.

Notably, a ransomware attack targeted National Football League (NFL) team the San Francisco 49ers during Super Bowl weekend in 2022. On the evening of February 12, 2022, the BlackByte ransomware group claimed responsibility for the incident, listing the NFL team as a victim on its dark web leak site.[13] This attack highlighted the value targeting such an organization can bring—particularly to gain notoriety during the largest sporting event of the year.

Mobile applications for the NFL, ESPN, and Fox Sports will likely experience high-volume activity during Super Bowl Sunday as fans stream content throughout the event. Rogue mobile apps may pose a threat to Super Bowl fans attempting to stream the game for free or to bypass restrictions on legitimate applications. To mitigate the risk of cyber threats, Super Bowl LVII attendees and fans must use caution when downloading unverified apps or using services that are not authorized by the NFL and its supporting sponsors. These "rogue" mobile applications are often unregulated; apps hosted on third-party app stores often contain flawed or outdated software that is susceptible to malware attacks or has other known vulnerabilities. Official Super Bowl LVII applications are available for download via the Apple App Store for iOS devices and the Google Play Store for Android devices.

> Forward Look:

- Expect that, in the lead-up and throughout Super Bowl LVII, threat actors will leverage the event as a lure due to the high international visibility of the event.
- Super Bowl third parties remain some of the highest cybersecurity risks to the event, as their IT infrastructure lies outside of the Super Bowl security team's digital perimeter.

> Recommendations:

- Always ensure that mobile apps are downloaded from legitimate app stores, and avoid third-party app stores.

FOOTNOTES

[9] [hXXps://www.azfamily\[.\]com/2023/01/31/businesses-hotels-prepare-large-crowds-during-super-bowl-wm-phoenix-open/](https://www.azfamily[.]com/2023/01/31/businesses-hotels-prepare-large-crowds-during-super-bowl-wm-phoenix-open/)

[10] [hXXps://www.wibw\[.\]com/2023/01/30/airbnb-warns-chiefs-fans-potential-scams-when-booking-stays-arizona](https://www.wibw[.]com/2023/01/30/airbnb-warns-chiefs-fans-potential-scams-when-booking-stays-arizona)

[11] [hXXps://statescoop\[.\]com/arizona-prepares-new-governor-ciso-super-bowl/](https://statescoop[.]com/arizona-prepares-new-governor-ciso-super-bowl/)

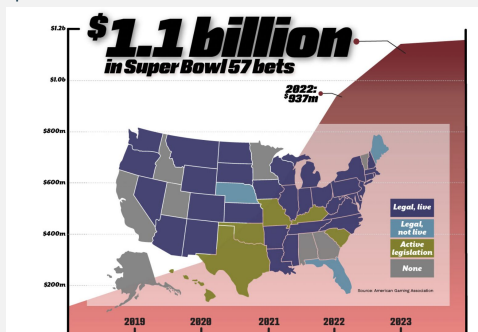
[12] ZeroFox Intelligence, (2022, February 14). Flash Report: LastPass Breach Update. Retrieved from [hXXps://cloud.zerofox\[.\]com/intelligence/advisories/16673](https://cloud.zerofox[.]com/intelligence/advisories/16673)

[13] [hXXps://statescoop\[.\]com/arizona-prepares-new-governor-ciso-super-bowl/](https://statescoop[.]com/arizona-prepares-new-governor-ciso-super-bowl/)



Fraud and Scams

Super Bowl LVII is anticipated to be the most bet-on sporting event ever; bets are predicted to exceed USD 1 billion.[14]



Source: <https://www.playusa.com/2023-usa-super-bowl-betting-projection/>

As such, betting participants make ideal targets for threat actors looking to capitalize on the event. Security researchers have expressed concern over bookmakers' cybersecurity practices as they bring on new participants and store personal data for their customers. An 83 percent increase in traffic is expected for sports betting for the Super Bowl, and concerns center around whether these organizations have invested enough in cybersecurity infrastructure to protect customers—and whether best practices, such as enforcing verifications, have been followed.[15]

Another area of concern for Super Bowl attendees is around ticketing scams. The lowest-price, legitimate tickets are currently selling for around USD 5,300; anything identified online for less is likely a scam, and purchasers should be wary.[16] Arizona's Attorney General has issued a warning about this, encouraging purchasers to stick to trusted sites such as Ticketmaster for their tickets and to avoid purchasing tickets on sites such as Craigslist, where scammers would be much more active.[10] Notably, Super Bowl tickets are mobile-only, so any other ticket-delivery method should be viewed with suspicion.[17]

Assessment:

- In light of the record-breaking betting revenues anticipated during Super Bowl LVII weekend, threat actors are highly likely to attempt to capitalize by exploiting the weak cybersecurity practices of some betting vendors, as well as establishing fraudulent sites to trick new registrants.
- Fraudsters are highly likely to attempt to scam eager fans seeking tickets to the Super Bowl, oftentimes offering tickets at much lower, too-good-to-be-true prices.

Recommendations:

- Utilize betting apps with strong cybersecurity practices, such as Multi-Factor Authentication and verification processes.
- Remain vigilant against deals that appear too good to be true. Given the cost of legitimate tickets currently for Super Bowl LVII, cheaper options are likely attempts by fraudsters to scam purchasers.

APPENDIX: Traffic Light Protocol for Information Dissemination

TLP: RED

HOW IT IS USED

Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW IT IS SHARED

Recipients may NOT share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

TLP: AMBER

HOW IT IS USED

Sources may use TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW IT IS SHARED

Recipients may ONLY share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP: AMBER+STRICT restricts sharing to the organization only.

TLP: GREEN

HOW IT IS USED

Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW IT IS SHARED

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

TLP: CLEAR

HOW IT IS USED

Sources may use TLP: CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW IT IS SHARED

Recipients may share TLP: CLEAR information without restriction, subject to copyright controls.

About ZeroFox

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-a-service leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident, and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers—including some of the largest public-sector organizations, as well as finance, media, technology, and retail companies—to stay ahead of adversaries and address the entire lifecycle of external cyber risks.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400

FOOTNOTES

- [14] <https://www.sportspromedia.com/news/super-bowl-lvii-2023-sports-betting-wagering-nevada-new-york-ntl/>
 [15] <https://cybernews.com/news/fraudsters-ready-to-attack-super-bowl-wagers/>
 [16] <https://www.kwch.com/2023/01/31/booking-last-minute-trip-super-bowl-advice-avoid-falling-victim-scammers/>
 [17] <https://8abc.com/super-bowl-57-tickets-philadelphia-eagles-scams/12761845/>

