



UEFA Champions League Final

| Event Assessment |

Introduction

The Champions League football tournament, which takes place across Europe, culminates with the Final in Istanbul on June 10, 2023. Violence during the early rounds of the tournament is ubiquitous, with visiting fans often engaging in street clashes with security forces and locals. This form of violence has surged with the number of matches increasing and the advent of ticketless fans traveling across Europe to be part of the atmosphere despite not attending the match. The final match is usually immune to such levels of violence, as it is typically held in a neutral venue with the majority of tickets going to football officials, local politicians, and celebrities. The security force budget is normally higher during the finals as well. However, the 2022 Final saw violent clashes between fans and security officials patrolling the stadium. UEFA officials initially blamed ticketless fans attempting to force their way into the final for the security issues that caused the match to be delayed; however, subsequent investigations showed that security and ticket processing issues at the stadium were to blame. Nevertheless, to avoid a repeat of the ticketing issues, UEFA has introduced an electronic ticketing system. While this could alleviate the issue of ticketless fans attempting to enter the match, it increases the array of potential cyber issues for the match. High-profile sporting events, especially multi-day ones like the Champions League Final, are already prone to scams involving impersonations. There will now be the added risk of fake ticket websites and applications attempting to lure in ticketless fans or tricking fans with tickets into downloading malicious apps or files.

There are also a number of other factors with which visitors will have to contend. Turkey is coming off a tense election that culminated on May 28 with the reelection of President Recep Tayyip Erdogan by a narrow margin. The Erdogan victory has significantly diminished the risk of a security threat at the stadium. Critics predicted Erdogan would challenge the election outcome if he lost, and there were rumors that UEFA was preparing an alternative venue for the Final—particularly in the event Erdogan challenged the vote. Despite his victory, there are still concerns that political opponents could use the match to highlight anti-Erdogan sentiment. This could take place across the city, which voted in favor of the opposition. There could also be pro-Erdogan events, which have been frequent since May 28. Given that there will be Champions League-related events from June 8–11, security and cyber-related risks will be extended before and after the Final.

Key Threats



Physical protests related to recent elections are possible.



A new electronic ticketing system could be targeted by malicious actors.



This is a possibility of clashes between fans of each team.



Accommodations, sponsor, and betting scams could also be issues based on previous events.



Security during the Final will be tight, increasing the risk of clashes between police and fans.



Viewing events outside the stadium are a major security risk.

Key Findings

- Fans in certain areas have a recent history of clashes with opposition fans ahead of major matches.
- There have been previous acts of violence at bars and in proximity to stadiums during early rounds of the Champions League.
- Tournament organizers were concerned about possible violence related to Turkey's election impacting the match.
- Fundraising related to a recent earthquake will feature at the Final and could be targeted by scammers.
- Impersonation websites and mobile apps related to accommodations or sponsors are likely.
- A new electronic ticketing system and enhanced security protocols will be in place in light of issues with entering the stadium at the 2022 Final.



Physical Security Issues

UEFA will introduce new security procedures for the 2023 Final. The organization was heavily criticized for its approach to the 2022 Final in Paris, during which thousands of fans were constricted in slow-moving queues that posed serious safety risks. Additionally, supporters of certain teams were treated as inherent security risks and subject to harsh treatment by police, including tear gassing. [1]

Changes for the 2023 Final include an increased number of safety and security personnel, greater intelligence capabilities, and enhanced accessibility for fans with disabilities. There will also be a greater emphasis on fan inclusivity. Finally, attendees will be provided with electronic tickets only to avoid the confusion over potential fake paper tickets that occurred in 2022. [2] Despite the ticketing issue changes, there remains a risk from unticketed fans visiting Istanbul. During the 2022 Final, thousands of supposedly ticketless supporters were initially blamed for attempting to rush the stadium, as had happened at other football events at the time. While the allegations were ultimately proven unfounded, the risk of unticketed fans causing disruptions in proximity to the event is still high.

In terms of crime, Istanbul is considered a relatively safe city to visit. The city is a global tourist destination, with over 16 million foreigners visiting in 2022 alone. [3] According to a survey published in 2016, nearly 85 percent of Turks rank the national police as the most reliable government institution. [4] Nonetheless, instances of petty crime such as pickpocketing are not uncommon, especially in lower-income neighborhoods and tourist hotspots, and Turkey's ongoing cost-of-living crisis could spur an increase in such crime. At the 2022 Final in Paris, multiple fans were mugged, threatened, or assaulted as they left the game. [5] While organizers likely have plans in place to avoid a similar situation this year, attendees should maintain awareness of their surroundings before and after the event.

There will be three official fan parks for events related to the Champions League. The first will be a family friendly "Champions Festival" that will be open from June 8-11, 2023, at the Port of Yenikapi in southern Istanbul. This will include a concert and games along with other activities. There will be another "fan village" in the immediate vicinity of the Ataturk Stadium, which will include separate zones for each set of fans. However, only ticketed fans can attend—unlike the festival, which is available to all. [6]

Fallout from Turkey's Election

President Erdogan's reelection is unlikely to cause major unrest in or around Istanbul. Erdogan won the election runoff on May 28 by a narrow margin, and opposition candidate Kemal Kilicdaroglu has not contested the results. Voters in Istanbul generally support Turkey's opposition, which may increase the likelihood of anti-Erdogan sentiment throughout the city. However, this is unlikely to lead to significant disruption.



Turkey's Presidential Candidates Kemal Kilicdaroglu and Recep Tayyip Erdoğan
Source: The Guardian

Assessment:

- UEFA organizers have introduced measures to streamline security proceedings in response to criticism of last year's Final.
- Istanbul is considered generally safe, but the threat of petty crime such as pickpocketing and robbery will be elevated during the event.
- President Erdogan's election victory is unlikely to cause significant unrest.

Recommendations:

- Obey security personnel and follow posted signage to reduce the chances of overcrowding at bottlenecks.
- Maintain situational awareness throughout Istanbul and avoid flashing cash when purchasing from vendors, if possible.
- Report thefts to police immediately.
- Avoid vocal displays of support for the defeated Turkish opposition or antagonism towards the Erdogan government.

FOOTNOTES

[1] <https://apnews.com/article/uefa-champions-league-final-security-review-14c7fb26e080767ea48941920ce37d>
[2] <https://www.uefa.com/insideuefa/news/0281-170c1cdd39d-1ba3e64490b5-1000-uefa-announces-measures-to-enhance-safeguards-for-supporters/>
[3] <https://www.statista.com/statistics/346671/istanbul-number-of-foreign-tourist-arrivals/#-text=In%202021%2C%20the%20number%20of%20in%202022%20at%2016%20million>
[4] <https://www.dailysabah.com/politics/2016/08/17/police-force-most-reliable-institution-in-eyes-of-turkish-public-report-says>

[5] <https://www.marca.com/en/football/champions-league/2022/05/30/62951ec2268e3ec2188b4568.html>
[6] <https://www.manchestereveningnews.co.uk/sport/football/football-news/champions-league-final-screen-istanbul-26980885>



Protest Risk

As with any high-visibility sporting event, the risk of protests is high. Climate activists have attempted on-field demonstrations at previous Champions League finals and may do so again. [7] Groups such as Extinction Rebellion, Just Stop Oil, and Greenpeace have repeatedly shown a willingness to crash high-profile events and cause considerable disruption in an effort to communicate their message.

Protests inside the stadium are possible. In previous rounds, Manchester City fans have booed during the Champions League anthem played at the beginning of each match, reportedly because of a two-year Champions League ban on Manchester City for financial irregularities that was overturned in 2020. [8] Inter Milan fans have also protested at other recent matches leading up to the Final over what they say are unfair ticketing allocations; this has included unfurling banners against UEFA. [9] Both sets of fans will be given 20 percent of the tickets, with the rest going to dignitaries and shareholders. Protests by aggrieved supporters are possible inside and outside the match, but their ability to bring in contraband like banners will be limited.

Turkey's government could also be the target of protests. President Erdogan has been criticized for imprisoning political dissidents and journalists on dubious charges. There is a risk that political opponents could stage protests at the venue against his May 28 reelection. However, so far the largest post election rallies have been by Erdogan supporters. These have included celebratory rallies at parks, bus stops, stadiums, and other designated locations which could cause some travel disruptions if held during the event. [10]

Assessment:

- There is a high likelihood of some form of protests or dissent during the match.
- A symbolic protest inside the stadium, like booing the anthem or holding a banner, is possible.
- Protests are unlikely to cause physical disruptions around the venue.
- Protests related to the recent election are possible in Istanbul and would be the most likely source of physical violence.

Recommendations:

- Avoid expressing a position on the recent elections or participating in political marches or protests.

Field Invasions and Fan Clashes

Football matches experienced a wave of field invasions in 2022 in the run-up to the Champions League Final. That trend has diminished but has not been discontinued in 2023. Several Manchester City fans were given jail sentences for storming the field after they won a title-deciding game in May 2022. The fans were cited for violent attacks on opposing fans, players, and throwing flares. [11] However, security measures in place at the 2023 Final will likely mitigate such risks; in particular, the prospect of the 20,000 vetted Manchester City and Inter Milan supporters storming the field is unlikely given they are a minority in the stadium. Bringing contraband like flares into the stadium is easier, although the heightened security measures inside the stadium should preclude it.

While unlikely, violent clashes between rival supporters cannot be ruled out. Inside the stadium, supporters of both teams will be kept separate. Each team has been given just 20 percent of the tickets, with the remaining 60 percent going to neutrals or dignitaries. [12] However, the risk of clashes between rival fans outside the stadium is much higher. Manchester City fans were filmed fighting rival Liverpool supporters ahead of a semi-final match in the United Kingdom in April 2022. [13] Ahead of a Champions League match in March 2023, fans of German side Eintracht Frankfurt were banned from visiting the Italian city of Naples after both sets of fans engaged in violent activity during a previous match. Frankfurt fans went to Naples anyway and clashed with police. [14] The most likely locations for these sorts of clashes are outside the stadium, where both sets of supporters may mix, or at bars and restaurants, which function as supporter zones to watch the game on television.

Assessment:

- Violence between fans is possible but unlikely.
- Security forces will likely have a low tolerance level for disruptive behavior, which could lead to arrests.

Recommendations:

- Avoid disruptive behavior like excessive drunkenness or perceived antagonism of opposition fans or the police.
- Avoid large gatherings of opposition fans, especially away from the stadium.

FOOTNOTES

[7] <https://bleacherreport.com/articles/2074646-greenpeace-protesters-arrested-at-champions-league-final>
[8] <https://theathletic.com/4524063/2023/05/17/manchester-city-fans-champions-league/>
[9] <https://sempreinter.com/2023/05/24/curva-nord-could-stage-coppa-italia-final-protest-champions-league-final-tickets/>
[10] <https://www.zawya.com/en/world/middle-east/erdogan-says-turks-have-given-him-new-presidential-mandate-r-128tyip>

[11] <https://www.independent.co.uk/news/uk/prime/manchester-city-fans-charged-aston-villa-b2084887.html>
[12] <https://www.uefa.com/insideuefa/news/220-17d4fec484ee-05cab4e5dd-1000-ticket-sales-for-2023-uefa-club-competition-finals-launched/#:~:text=2023%20UEFA%20Champions%20League%20final&text=A%20total%20of%2047%2C200%20tickets,via%20UEFA%20UEFA.com%20ticket>
[13] <https://www.mirror.co.uk/sport/football/news/liverpool-man-city-fans-fight-26726874>
[14] <https://www.opnews.com/article/napoli-frankfurt-fighting-fans-champions-league-778071cf03fbd8ffm3d#f55608d25c>



| Nation-State Activity

Turkey's ties with neighboring Middle Eastern countries have been historically fraught but are improving, lowering the risk of disruptive nation-state activity. Bilateral relations with Israel, Saudi Arabia, and the United Arab Emirates have improved since 2021 after years-long hostility. Turkey is also seeking to normalize ties with Syria, despite backing rebel factions in the country's long-running civil war. [15] The presence of Turkish troops in northern Syria remains a source of tension, but Syria is unlikely to attempt a disruption while normalization talks are ongoing. Similarly, Turkey is engaged positively with Iran, and their mutually good relations with Russia will likely preclude Iranian disruptions at the event. [16] Turkey has remained neutral in the war in Ukraine and serves as an effective mediator between the two sides. Russia in particular approves of this posture and reportedly backed President Erdogan during the election. Therefore, Russian-backed activity that could embarrass or anger Turkey is unlikely.

Because Turkey is a member of NATO and shares close, if not warm, ties with most of Europe, disruptions from European states are very unlikely. Despite decades of hostility, relations with Armenia are relatively warm at the moment and are unlikely to deteriorate in the near future. [17] Turkey has increased its purchase of Russian oil since the invasion of Ukraine but has balanced this by providing weapons and aid to Ukraine's government. [18] It also facilitated the Black Sea Grain Deal, which granted shipping relief to both Ukraine and Russia. Turkey has thus sufficiently pleased both sides to make interventions by either unlikely, though anti-war activists could stage protests at the event.

> Assessment:

- The risk of nation-state activity is low.
- Hostility towards the Erdogan government is more likely to take the form of physical protests by activists rather than efforts to disrupt the match.

| Terrorism Threats

Istanbul has seen terror attacks in the past, including car bombs and suicide bombers, though few have occurred in recent years. Most recently, a bomb detonated in a busy shopping district on Istiklal Avenue in November 2022, killing six people and injuring 81. [19] Turkey's government blamed Kurdish militants operating in Syria, though no group ever claimed responsibility. Prior to that, no attack had taken place since 2017.

Kurdish militant groups remain active but have been put on the defensive by military operations in Turkey's southeast, as well as northern Syria and northern Iraq. President Erdogan's harsh nationalist rhetoric during his presidential campaign may have agitated these groups, who could view disrupting the Final as a way to embarrass the newly-elected president. Turkey's security forces have a long history of countering attacks, however, and tight security will make the success of any planned disruption unlikely. Nonetheless, terrorist activity cannot be ruled out.

> Assessment:

- Terror attacks in Istanbul have become rarer in recent years but cannot be ruled out.
- High security during the Final will make it difficult for threat actors to successfully execute an attack.
- Kurdish political groups could choose to highlight their cause during the final, but those will likely take the form of protests or symbolic gestures like banners held inside the stadium.

> Recommendations:

- Report suspicious activity immediately.
- Follow crowd control directions promptly and do not linger near large groupings of police, who could be targeted by terrorists.

FOOTNOTES

[15] <https://en.mehnews.com/news/200874/Turkey-to-start-normalizing-ties-with-Syria-soon-Cavusoglu>
[16] <https://www.reuters.com/world/turkey-syria-russia-iran-hold-highest-level-talks-since-syrian-war-2023-05-10/>
[17] <https://www.euronews.com/2023/03/24/can-football-help-normalise-relations-between-armenia-and-turkey>
[18] <https://tradingeconomics.com/turkey/crude-oil-imports-from-russia>

[19] <https://www.bbc.com/news/world-europe-63615076>



Cybersecurity Concerns

As one of the most-watched and lucrative events in the world, the Champions League could be a target for both financially and politically-motivated actors. As such, threat actors will almost certainly leverage the game to target fans, organizations, and host entities. Cyber risks will significantly increase for brands and sponsors associated with the match, the two teams participating, and governing bodies that include the local government and UEFA. More so, with major sporting events becoming increasingly digitized, the attack surface for threat actors has also increased. Sophisticated threat actors will almost certainly aim to compromise networks by exploiting vulnerabilities within interconnected stadium systems, including operational technology and Internet of Things (IoT) devices.

One such example was the 2018 Champions League Final that was held in Kyiv, Ukraine. During that final, there was reportedly an effort by Russian cyber actors to cripple Ukrainian infrastructure, with hackers infecting IoT devices—including internet routers and storage devices—with malware called VPNFilter. VPNFilter has a command that renders infected routers, servers, mobile phones, and laptops unusable and could have prevented millions of viewers from watching the game. It is unclear if the attack was done to coincide with that final, but the number of infected devices did increase just ahead of the match on May 29, 2018—with the bulk of them in Ukraine. [20]

Any operational systems with internet connectivity at the Ataturk Olympic Stadium are susceptible to attack. A compromise of an IoT-connected lighting system (CLS) has perhaps the most potential to disrupt the Final. The attack surface of a CLS will depend in large part on the extent to which associated network assets consist of on-premises equipment and software or cloud resources. Of the various broad means of attacking a CLS, tampering (modifying code or data) and elevation of privileges (obtaining unauthorized capability to issue commands) are most likely to result in operational interference of lighting and disruption of the event.

Another potential target for cyber actors will be events related to the earthquake Turkey suffered in early 2023. The final day of the event on June 11 features a benefit concert for victims of the earthquake. Since the earthquake, there have been repeated cyber incidents related to earthquake relief. In the immediate aftermath of the earthquake, supposed Russian hackers disrupted communications between aircraft providing aid to the victims. Likely Russian-backed group Killnet claimed responsibility for the attack because some of the aircraft belonged to NATO. [21] Russian-backed actors would find plenty of ostensibly anti-Russian or pro-Ukrainian targets at the Champions League Final, where shows of support for Ukraine are common. Russian teams have also been banned from the competition over the war. Killnet disrupted the broadcast of the Eurovision 2022 singing competition after Russia was banned and Ukrainian acts won the competition. [22] However, Russia considers Turkey a key ally for political and financial reasons and is unlikely to countenance an attack that could worsen relations.

Social Engineering

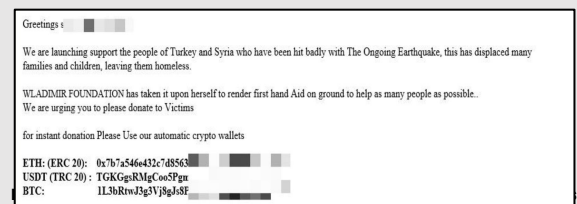
Social engineering poses one of the greatest threats to organizations and spectators participating in the Champions League Final. However, as observed in previous iterations of the final, there is likely to be a spike in tournament-related lures both in the lead-up to and during the event, as threat actors will aim to capitalize on heightened global interest to harvest credentials, deploy follow-on payloads, and conduct financial fraud.

Social engineering campaigns during the 2023 Final are almost certain to vary in complexity from low-level, rudimentary email and SMS-based scams targeting mass audiences to sophisticated spear phishing attacks directed at specific organizations and individuals associated with the Final, such as diplomats, journalists, and high-profile executives. Most lures are very likely to use trademarks from UEFA and tournament sponsors to appear legitimate, as well as attempt to impersonate businesses operating in support of the event, such as hospitality, retail, and travel companies. The most prevalent scams and fraudulent activity observed in previous tournaments include:

- Fake lottery win notifications promising fans last minute tickets or access to celebrities
- Illegitimate accommodation and local experience offers
- Malicious streaming and gambling sites
- Counterfeit ticket and merchandise sites

Because of the new ticketing system, attendees should be on the lookout for alternative ticketing applications or websites, as well as hotel or accommodations impersonations. Fraudulent sites dedicated to betting are also likely. Ahead of the World Cup in Qatar in late 2022, ZeroFox Intelligence identified phishing sites posing as known betting sites; the site fifa-bet365.com masqueraded as popular sports bookie site bet365.com. [23]

In the immediate aftermath of the earthquake, scam donation sites were common; they could resurface from June 8-11 when earthquake aid will again be prioritized. [24]



Source:
<https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-exploit-human-misery-in-earthquake-hit-turkey-and-syria-with-new-online-disaster-scam/>

FOOTNOTES

[20] https://www.theregister.com/2018/07/13/ukraine_vpnfilter_attack/
[21] <https://www.telegraph.co.uk/world-news/2023/02/12/russian-killnet-hackers-disrupt-natos-turkey-syria-earthquake/>
[22] <https://www.euronews.com/culture/2022/05/16/eurovision-2022-russian-hackers-targeted-contest-say-italian-police>

[23] ZeroFox Internal Collections
[24] <https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-exploit-human-misery-in-earthquake-hit-turkey-and-syria-with-new-online-disaster-scam/>

Turkish Cybersecurity Protocols

Western visitors to Istanbul will likely encounter less robust cybersecurity protocols than those with which they are accustomed. This makes data shared while visiting Istanbul vulnerable. ZeroFox has identified repeated instances of the Hydra Market Telegram channel advertising the sale of Turkish usernames, passwords, and phone numbers—mainly obtained by hacking Turkish financial services and government entities. For example, on March 30, 2023, Hydra Market advertised stolen data from Isbank, a small commercial lending bank in Turkey. [25] The same leak also advertised data related to the Free Cause Party, a political party inside Turkey. Hydra Market also claimed to be in possession of data on millions of Turkish citizens from the e-government website of Turkey. On May 26, 2023, Hydra Market reportedly disclosed 135 million records pertaining to Turkish COVID-19 vaccinations as part of a wider dump. [26]

While these data dumps mainly impact Turkish citizens registered with local banks or government institutions, there is also a risk to those who use local mobile money services or have a reason to interact with Turkish government websites. There have been recent hacks of COVID-19 databases used by countries to monitor and administer vaccines that provide hackers with personal information on millions of users. Also visitors who purchase a SIM card are also at risk of having that number compromised later on by hackers. On May 22, 2023, the Baseleak Telegram channel claimed to have information on 116 mobile phone accounts in Turkey.

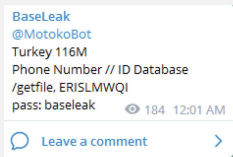


Image from Baseleak leak site claiming access to 116 Turkish mobile phone numbers
Source: ZeroFox Internal Collections

- Assessment:**
 - Turkish cybersecurity protocols are weak and often compromised by financially-motivated cyber actors.
 - Data shared with government entities or financial services institutes could be targeted by hackers after the final.
- Recommendations:**
 - Avoid downloading suspicious mobile apps or visiting unverified websites.
 - Avoid sharing personal data with Turkish government authorities via COVID-19 monitoring apps.
 - Refrain from using mobile money payments, especially for services that you have not used before.

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

[25] ZeroFox Internal Collections
[26] ZeroFox Internal Collections