CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

November 17, 2022

FIELDING THREATS:
Cyber, Influence, and Physical Threats to the 2022 FIFA World Cup in Qatar

This report analyzes the threat landscape ahead of the 2022 FIFA World Cup hosted in Qatar that begins on November 20, 2022. The threats analyzed include state-sponsored cyber operations, financially motivated cyber threats, influence operations, and physical security threats. This report will be of most interest to organizations involved in the hosting, running, or sponsoring of the 2022 FIFA World Cup, as well as individuals intending to participate in or attend the tournament.

Executive Summary

Whole-spectrum threats to the 2022 FIFA World Cup in Qatar are largely determined by Qatar's unique geopolitical position on a contentious global stage, with the country enjoying good relations with major powers such as the United States (US), Europe, China, and Iran.

We have not identified any imminent, planned, or ongoing state-sponsored cyber operations linked to known advanced persistent threat (APT) groups targeting the 2022 FIFA World Cup in Qatar or its organizers, sponsors, or associated infrastructure. China, Iran, and North Korea are unlikely to conduct a disruptive attack against the tournament as they lack motivation due to their relations with Qatar, their involvement in the planning and execution of the games, or other national priorities. Nevertheless, state-sponsored APT groups tasked with foreign intelligence collection likely view the 2022 FIFA World Cup as a target-rich environment for cyber espionage and surveillance against foreign dignitaries and businesspersons alike.

Russia is an outlier and very likely harbors a strong set of grievances and thus motivation for targeting the 2022 FIFA World Cup, such as wanting to embarrass Qatar as the host country for siding with the coalition of countries supporting Ukraine's territorial integrity, as well as to retaliate for Russia being banned from participating in the tournament. There is historical precedent for Russia conducting cyberattacks against major sporting events, although Russian APT groups are very likely distracted with Russia's war against Ukraine and are therefore unlikely to conduct a disruptive attack against the 2022 FIFA World Cup. However, we cannot rule out that the Russian government will encourage or otherwise tacitly approve of such attacks conducted by nationalistic Russian hacktivist groups or ransomware operators.

Large international sporting events are also attractive targets for financially motivated cybercriminals. Tournament-related phishing attacks use various lures such as so-called ticket giveaways, free streaming services to watch games, fake betting websites, and tournament-adjacent items like visas and travel, hotel, and restaurant bookings. Other cybercriminal threats include, but are not limited to: fake mobile applications around the event that can distribute malware and harvest user data; sales on dark web markets and shops for counterfeit tickets and compromised credentials; and as above, ransomware attacks that would likely seek to opportunistically target victims based on accessibility, opportunity, and factors such as the ability to pay large ransom amounts.

Iran, China, and Russia's influence activities involving the 2022 FIFA World Cup are primarily being conducted through state-owned media organizations, which emphasize and promote bilateral relations with Qatar. Iran and Russia have also sought to highlight divisions and exacerbate tensions between Qatar and Western countries that have been critical of the tournament being hosted in Qatar due to human rights concerns in the country. Similarly, Iran's "Endless Mayfly" influence operation identified by Citizen Lab in May 2019 involved an instance of disinformation around the 2022 FIFA World Cup, which sought to exacerbate geopolitical tensions between Qatar and other Arab countries following the Qatar diplomatic crisis in June 2017.

Qatar is unlikely to face a major physical security threat during the 2022 FIFA World Cup based on a range of factors including: the country having minimal terrorist incidents in recent years; the decreased capabilities of terrorist groups most likely to target the tournament, including Islamic State in Iraq and the Levant (ISIL) and Al-Qaeda in the Arabian Peninsula (AQAP); Qatar's enhanced security posture, bolstered by security assistance from countries such as the US, United Kingdom, France, Italy, Türkiye, and Pakistan; and Qatar's geographical orientation.

Key Judgments

- Recorded Future has not identified any imminent, planned, or ongoing state-sponsored cyber operations targeting the 2022 FIFA World Cup in Qatar. Nevertheless, state-sponsored APT groups tasked with foreign intelligence collection likely view the 2022 FIFA World Cup as a target-rich environment for cyber espionage and surveillance.
- Russia very likely harbors a strong set of grievances and has the greatest motivation to conduct a disruptive cyberattack against the 2022 FIFA World Cup, and there is historical precedent for Russia targeting major sporting events. However, Russian APT groups are unlikely to conduct a disruptive attack against the tournament due to their preoccupation with Russia's war against Ukraine.
- We cannot rule out that the Russian government will encourage or otherwise tacitly approve of disruptive attacks conducted by nationalistic Russian hacktivist groups or ransomware operators against the 2022 FIFA World Cup. Such attacks can provide plausible deniability for the Kremlin.
- Cybercriminals are launching tournament-related phishing attacks using common lures such as so-called ticket giveaways to collect personally identifiable information (PII) from victims, including financial information like payment card details, or to distribute malware.
- Iran and Russia have sought to highlight divisions and exacerbate tensions between Qatar and Western countries that have been critical of the tournament being hosted in Qatar. And the Iran-aligned group Endless Mayfly historically used the 2022 FIFA World Cup in an influence operation.
- Qatar is unlikely to face a major physical security threat during the 2022 FIFA World Cup, although unmanned aerial systems (UAS) represent a unique disruptive threat that Qatari authorities are working to mitigate with foreign security assistance.

State-Sponsored Cyber Threats

Large international sporting events such as the Olympic Games or the World Cup are attractive targets for cybercriminals and state-sponsored APT groups alike for either financial, disruptive, or espionage purposes. Such events are often years in the making, involve the investment of billions of dollars in infrastructure to support, bring the host country considerable prestige on the international stage, and attract a wide range of spectators, including high-level government officials and businesspersons. As a result, disruption of the event can prove embarrassing for the host government and organizers, while traditional intelligence-gathering-focused cyber-espionage and surveillance activities are likely lucrative given the target-rich environment. To mitigate this risk, travelers to Qatar for the 2022 FIFA World Cup should take additional precautions around their digital communications such as using encrypted communications applications whenever possible, exercising caution when connecting to unknown and public Wi-Fi networks (including in hotels), and considering the use of burner devices for the duration of the trip rather than personal or corporate devices.

As of this writing, we are not aware of any imminent, planned, or ongoing state-sponsored threat activity linked to known APT groups targeting the upcoming 2022 FIFA World Cup in Qatar, its organizers (such as FIFA or the Union of European Football Associations [UEFA]), its sponsors, or associated infrastructure. This includes attacks that may be disruptive or destructive in nature (such as distributed denial-of-service (DDoS) attacks or wiper malware) or more espionage-focused operations. Additionally, we have not observed the establishment of network infrastructure attributed to state-sponsored APT groups intended to facilitate computer network operations against the World Cup or its affiliate organizations or attendees. Similarly, we have not as of this writing found weaponized lure documents for use in spearphishing attacks.

In this section, we review the likely motivators for state-sponsored APT groups' targeting of the 2022 FIFA World Cup, with a focus on the most prominent state-sponsored threat actors — those linked to China, Russia, Iran, and North Korea. Overall, we assess that the Russian government is the most strongly motivated to carry out disruptive attacks against the event, but is very likely focusing its resources on supporting its war against Ukraine instead. And while Iran, China, and North Korea all likely possess the technical capabilities to do so, they are unlikely to pose a disruptive threat to the games as they lack the motivation due to their relations with Qatar, their involvement in the planning and execution of the games themselves, or other national priorities.

China

Chinese state-sponsored APT groups are unlikely to target the World Cup and its affiliates for the purposes of disruption of the event. Nevertheless, those groups tasked with the collection of foreign intelligence, and particularly those falling under the Ministry of State Security (MSS) — China's primary civilian intelligence service — are likely to view the World Cup as a target-rich environment for cyber espionage and surveillance against foreign dignitaries and businesspersons alike. Likely MSS-linked cyber-espionage groups include, but are not limited to, APT10, APT17, APT27, APT40, APT41, TAG-22, RedBravo, and RedDelta.

China and Qatar have enjoyed increasingly close relations in recent years, with Beijing and Doha announcing cooperation on a host of regional and global issues in defense, energy, and economic development, including Qatar's involvement in Beijing's marquee international development project, the Belt and Road Initiative (BRI). Moreover, Chinese companies maintain a considerable presence in Qatar, and the Chinese Railway Construction Corporation in 2016 won the bid to build the largest World Cup venue, the Lusail Stadium, which was completed in 2020.

Significantly, there is no historical precedent for Chinese threat activity groups targeting major international sporting events or sporting bodies, and China has shown more restraint compared to other nations in conducting wide-reaching destructive and disruptive attacks in general. Therefore, while Chinese APT groups have regularly targeted specific organizations and governments ahead of key talks, and Beijing's cyber-enabled monitoring of ethnic and religious minorities domestically and internationally is well-documented, it is unlikely that China poses a disruptive threat to the 2022 FIFA World Cup. This is made even more unlikely due to China's direct involvement in developing the infrastructure to support the event — giving it a vested interest in ensuring that it unfolds smoothly — as well as Beijing's desire to continue to strengthen its relationship with Doha as a major strategic partner in the region.

Russia

The Russian government very likely harbors a strong set of grievances and thus motivation for targeting the 2022 FIFA World Cup in Qatar. Russian activity targeting the event would likely be disruptive in nature, or otherwise seek to embarrass the international entities responsible for organizing the event such as FIFA, UEFA, or international sponsors, both public and private.

Following Russia's invasion of Ukraine in late February 2022, FIFA and UEFA issued a blanket ban against Russian football clubs from competitions, including the upcoming World Cup, in protest of the invasion. Subsequently, the Football Union of Russia abruptly withdrew its appeal of the decision in early April, resulting in the ban remaining in place.

Russian state-sponsored APT groups have a history of targeting international sporting organizations and events beginning as early as 2016, likely in retribution for similar bans of its athletes from participation in major international events, such as the Olympic Games, due to a string of doping scandals. Past Russian state-sponsored activity targeting such organizations includes:

- The Russian Main Intelligence Directorate's (GRU) reconnaissance against the 2020 Tokyo Olympics in an alleged effort to disrupt the event
- Sandworm's disruption of the 2018 Pyeongchang Winter Olympics with the Olympic Destroyer malware
- APT28's hack-and-leak campaign targeting the World Anti-Doping Agency (WADA) and Western athletes' personally identifiable and personal health information (PII and PHI) during the 2016 Rio de Janeiro Summer Olympics
- GRU operators targeting WiFi networks and routers at hotels used by anti-doping officials in Rio de Janeiro and Lausanne, Switzerland, deploying bespoke malware once they obtained access to a host of interest

While Moscow and Doha are engaged both diplomatically and economically with one another, there are signs of significant strain in the relationship, especially since Russia's invasion of Ukraine. First and foremost, Qatar has expressed its support for Ukraine and the territorial integrity of the country along its internationally recognized borders. Moreover, the US formally designated Qatar as a "major non-NATO [North Atlantic Treaty Organization] ally" in March 2022 — a move that is very likely interpreted as signaling Qatar's long-term strategic alignment with NATO and Washington instead of with Moscow. As a result, the Kremlin likely has a particularly strong grievance against Qatar and may view the World Cup as an opportunity to embarrass Qatar's government.

Nevertheless, despite having the motivation to conduct such disruptive attacks against the World Cup and Qatar, the Russian government is very likely distracted with the war in Ukraine, which has turned into a grinding conflict requiring Moscow to marshal as many of the state's resources as possible in an attempt to achieve its strategic aims in the face of Ukraine's staunch armed resistance. It is therefore very likely that Russian APT groups that may otherwise be tasked with disruption of an international event such as the World Cup — especially those aligned with military intelligence such as APT28 or Sandworm, based on historical activity — are instead tasked with prioritizing operations that are directly in support of the war effort in Ukraine.

While we assess it is thus unlikely that established Russian state-sponsored APT groups will conduct such disruptive operations against the World Cup, we cannot rule out that the Russian government will encourage or otherwise tacitly approve of such attacks conducted by nationalistic Russian "hacktivist" groups — such as KillNet or XakNet — or by ransomware operators. Such groups, whether financially or politically motivated, are useful proxy forces that can on occasion further the Russian government's strategic objectives and provide plausible deniability.

Iran

While Iranian state-sponsored APT groups frequently target public and private entities across the Middle East in both destructive and espionage-focused campaigns, they are not known for executing hacktivist-like attacks against international sporting federations. Moreover, due to the strong trade and diplomatic ties between the 2 countries, Iran's participation in the World Cup despite calls for its banning, and due to domestic Iranian instability, it is unlikely that Iran will seek to use cyberattacks to disrupt the games as doing so provides no obvious benefit to the regime and risks upsetting a key regional partner in Qatar.

This does not rule out Ministry of Intelligence and Security (MOIS)- or Islamic Revolutionary Guard Corps (IRGC)-linked espionage activity in-country, however, likely primarily directed against high-profile foreign attendees of the game and dissidents and/or critics of the Iranian regime. Such groups, including APT34 OilRig, APT35, APT39, APT42, and MuddyWater are known to routinely carry out espionage operations against Middle Eastern and Western governments and private sector companies in support of Tehran's economic, political, and military objectives. APT35 has been reported to seek strategic and tactical information and has also undertaken counterintelligence operations at the behest of the IRGC, including in attacks against international conferences and related organizations such as the Munich Security Conference and Think20 Summit in Saudi Arabia. For its part, APT39 has also been reported to focus on counterintelligence and long-term espionage activity with the goals of protecting the regime.

Iran and Qatar have an abnormally close relationship given the latter's membership in the Gulf Cooperation Council (GCC) regional bloc, and Doha carefully balances its alliance with the US and its economic and security ties with Tehran. These ties only strengthened during and following the 2017 Qatar diplomatic crisis in which Doha sought to replace its traditional trading partners — who instituted an embargo against the country — with imports from Iran and Türkiye. Qatar's geographic position in the Persian Gulf, as well as its sharing of the world's largest natural gas field with Iran, induce the 2 to closer relations despite Iranian discomfort with Qatar's hosting of the largest US military base in the region at Al Udeid. Relations between Iran and Qatar have become so cordial that Iran offered — and Qatar accepted — assistance in hosting hundreds of thousands of visitors to the World Cup on the resort island of Kish, offshore of Iran, thus giving Iran an economic and political stake in the success of the games.

Finally, Iran has in recent months been rocked by domestic instability and widespread protests following the death of Mahsa Amini while in police custody. The protests — the largest in over a decade — have turned violent, resulting in the government issuing lockdowns of the information environment within the country and cutting off the internet from the outside world, as well as deploying security forces authorized to use lethal force to quell the unrest. In order to preserve the regime, maintaining and stabilizing the domestic situation is very likely to be the primary task of the Iranian intelligence and security services in the near term. This suggests that little resourcing would likely be devoted to externally oriented cyber operations during the World Cup, even if Iran had the requisite motivation to do so.

North Korea

North Korean state-sponsored APT groups are unlikely to conduct disruptive or destructive attacks against the upcoming 2022 World Cup in Qatar.

There is very limited precedence for North Korea-linked APT groups targeting international sporting events or organizations. In the 1 instance in which this was observed — in a campaign using the fileless malware "Gold Dragon" targeting Olympics-related organizations in the period surrounding the 2018 Winter Olympics in Pyeongchang, South Korea — the campaign appears to have been focused on intelligence gathering, which is consistent with the majority of North Korea state-sponsored cyber campaigns against the South and likely a part of their routine operations.

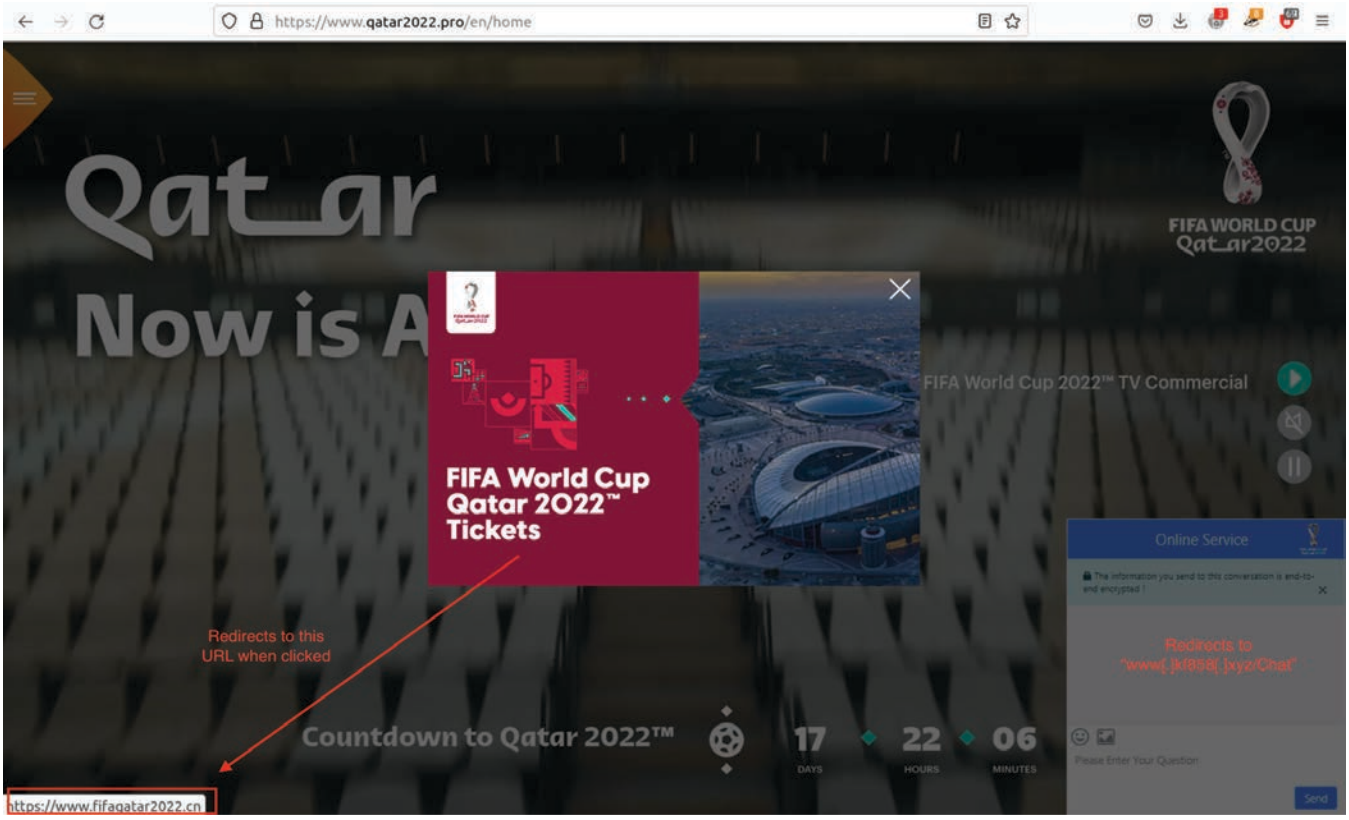


Figure 1: *Example of a typosquat domain impersonating the legitimate qatar2022[.]qa website, with redirects to other suspicious websites (Source: qatar2022[.]pro)*

Moreover, the majority of historical North Korean state-sponsored APT campaigns have been focused on revenue generation for the regime in Pyongyang, which continues to languish under strict international sanctions that limit its access to global markets. These attacks have primarily consisted of compromises of financial institutions, ATM cash-out schemes, or theft of cryptocurrency. Apart from ransomware or other forms of extortion attacks, such as the WannaCry campaign, disruptive or destructive attacks are difficult to monetize and thus are likely of less interest and priority to the regime.

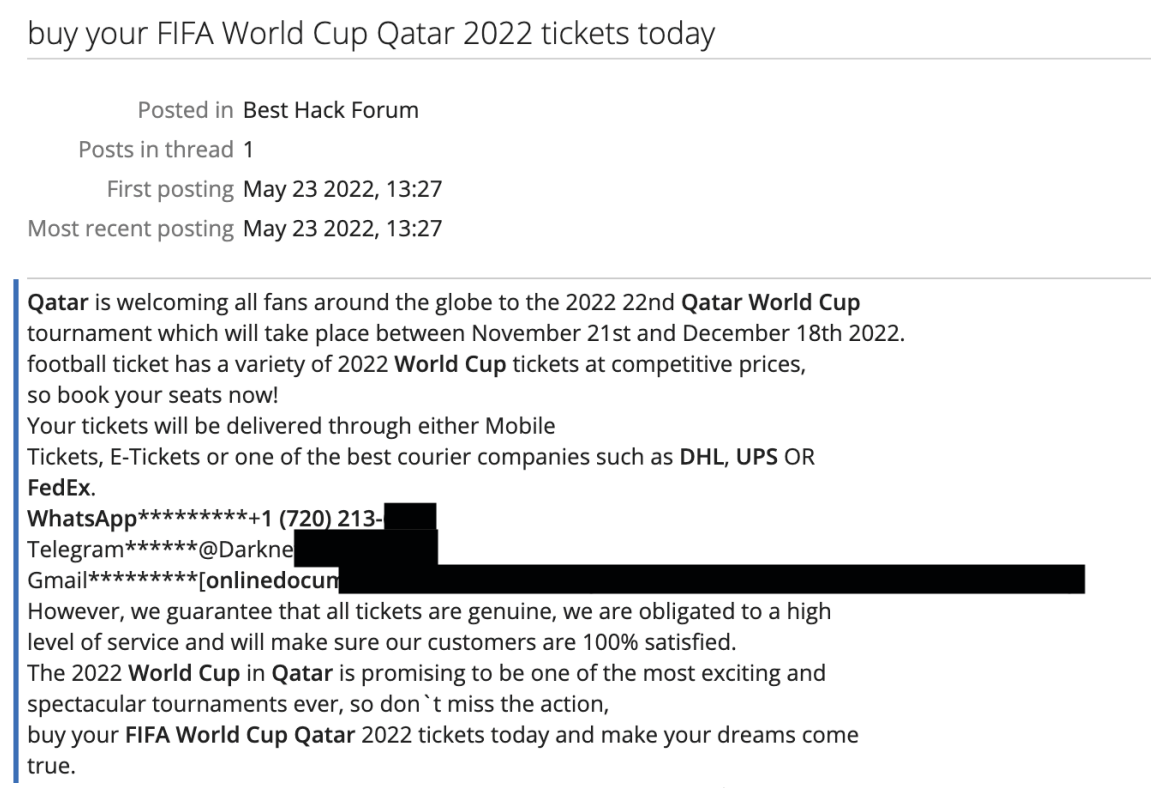
With respect to the 2022 World Cup, North Korea likely lacks the political motivation to engage in disruptive or destructive activity against the games. Pyongyang voluntarily withdrew from World Cup qualifiers in May 2021 likely due to concerns over COVID-19, but unlike Russia was never formally banned from participation by the organizing bodies. Moreover, Qatar has — at least until the imposition of recent United Nations (UN) sanctions that went into effect at the end of 2019 — been host to thousands of North Korean migrant laborers. Many of these laborers were integral to the construction of the venues for the upcoming World Cup games, including the aforementioned Lusail Stadium which was built by a Chinese firm. Overall, Qatar has proven more willing than many governments to continue some form of direct relations with North Korea, and Pyongyang is unlikely to see a benefit to damaging relations via disruptive cyberattacks against the World Cup.

Cybercriminal Threats

As mentioned above, large international sporting events such as the 2022 FIFA World Cup are attractive targets for financially motivated cybercriminals. Cybercriminal threats to the 2022 FIFA World Cup include but are not limited to tournament-related phishing attacks, fake mobile applications around the event that can distribute malware and harvest user data, sales on dark web markets and shops for counterfeit tickets, and threats of ransomware.

Phishing and Fraud

Cybercriminals are leveraging the 2022 FIFA World Cup as a lure in phishing attacks and in other fraudulent activities. Cybercriminals are almost certainly creating fraudulent websites[1] related to the 2022 FIFA World Cup that can be used in phishing campaigns to collect PII from victims, including financial information like payment card details, or to distribute malware.



buy your FIFA World Cup Qatar 2022 tickets today

Posted in Best Hack Forum
Posts in thread 1
First posting May 23 2022, 13:27
Most recent posting May 23 2022, 13:27

Qatar is welcoming all fans around the globe to the 2022 22nd **Qatar World Cup** tournament which will take place between November 21st and December 18th 2022.
football ticket has a variety of 2022 **World Cup** tickets at competitive prices, so book your seats now!
Your tickets will be delivered through either Mobile Tickets, E-Tickets or one of the best courier companies such as **DHL**, **UPS** OR **FedEx**.
WhatsApp*******+1 (720) 213-**[redacted]
Telegram******@Darkne[redacted]
Gmail*********[**onlinedocum**][redacted]
However, we guarantee that all tickets are genuine, we are obligated to a high level of service and will make sure our customers are 100% satisfied.
The 2022 **World Cup** in **Qatar** is promising to be one of the most exciting and spectacular tournaments ever, so don`t miss the action,
buy your **FIFA World Cup Qatar** 2022 tickets today and make your dreams come true.

Figure 2: *Example of a post on a dark web forum advertising 2022 FIFA World Cup ticket sales (Source: Recorded Future)*

Between October 31, 2021 and October 31, 2022, we identified:

- 130 registered typosquat domains of fifa[.]com, 30 of which were created in October 2022 as the 2022 FIFA World Cup draws near
- 143 registered domains that include the terms "Qatar" and "2022", some of which are impersonating the official 2022 FIFA World Cup website, qatar2022[.]qa, such as in Figure 1
- 889 registered domains that include the terms "World" and "Cup"
- 56 registered domains that either include the terms (["FIFA" or "Qatar"] and "Ticket"), or ("World" and "Cup" and "Ticket").

We identified 669 references to 2022 FIFA World Cup phishing campaigns between October 31, 2021 and October 31, 2022. These phishing attacks have targeted both organizations and individuals, though as the tournament approaches, phishing attempts are very likely to focus on targeting individuals. Phishing attacks targeting individuals relate to various components of the tournament, including: tickets to the games (typically so-called "ticket giveaways"); free streaming services for when the tournament begins; betting websites; and tournament-adjacent items like visas and travel, hotel, and restaurant bookings. In November 2021, Kaspersky reported that they detected 11,000 phishing emails between August 15 and October 15, 2021 primarily targeting organizations by inviting bids on contracts to supply goods or services for the 2022 FIFA World Cup, where recipients were asked to pay a commission to participate.

Another attack vector used by cybercriminals is creating fraudulent mobile applications that impersonate legitimate ones, such as the "Hayya to Qatar 2022" mobile application created by Qatar's Supreme Committee for Delivery and Legacy (Apple, Google Play). We identified multiple mobile applications posing as the official 2022 FIFA World Cup application, with thousands of downloads. Although we have not conducted an analysis of these mobile applications, we strongly recommend that individuals only download official 2022 FIFA World Cup mobile applications such as those created by Qatar's Supreme Committee for Delivery and Legacy and by FIFA.

Dark Web Activity

We identified 277 references to the 2022 FIFA World Cup on dark web special-access forums between October 31, 2021 and October 31, 2022. We observed discussions of individuals claiming to be selling tickets to the 2022 FIFA World Cup, as well as other individuals posting in an effort to purchase tickets. We also observed an individual sharing the likely compromised login details of 2 accounts for beIN CONNECT, a state-owned global sport and entertainment network headquartered in Doha, Qatar, with the individual stating "SAVE FOR WORLD CUP".

Another notable post includes an October 4, 2022 post on Cracked Forum by "xAcordx" advertising a malicious .doc exploit file that is claimed to be fully undetectable (FUD) by all antivirus solutions, that "can be sent via Gmail and other popular email providers", and that "downloads and executes any file when ran [sic]". The file is advertised at $600 for a single full FUD build, or $2,400 for the builder allowing unlimited builds with a weekly update to maintain its FUD status. The post advertises many different lures for the document, including "world cup" and "world cup qualifying", demonstrating that the 2022 FIFA World Cup is being used as a lure in malicious documents. The threat actor also includes in their listing a proof-of-concept video that demonstrates the exploit's functionality.

Furthermore, Recorded Future's Identity Intelligence Module identified credential leaks for 14 unique *@qatar2022[.]qa email addresses on both clearnet and dark web sources, including 8 unique email addresses with associated passwords. These credential leaks were included in database dumps including GoNitro Database Dump, Cit0day Dump, ShareThis Data Dump, Zynga Data Dump, Dropbox Credential Dump, and Qatar National Bank Data Dump, while other credentials were stolen through infostealer malware such as Vidar. Credential leaks can be abused by threat actors to obtain initial access into an organization or to perform additional fraudulent activities such as social engineering, spearphishing, and business email compromise (BEC). However, the passwords associated with the email addresses in the aforementioned breaches could be passwords for other websites where the owner used their qatar2022[.]qa email address for a different online service, and are not necessarily the passwords for the owner's email account or corporate network. Using unique passwords for each online service mitigates the risk that leaked credentials can be used by threat actors to access more than 1 online service.

Finally, we identified 269 references to tickets[.]fifa[.]com and hayyar[.]qatar2022[.]qa on dark web shops, specifically Russian Market, Genesis Store, and 2easy Shop. These 2 domains are used to purchase tickets to the 2022 FIFA World Cup, and to apply for a Hayya Card, respectively. All tournament visitors need a Hayya Card to be permitted entry to Qatar, for access to match stadiums, and for free use of public transportation on match days. Visitors applying for a Hayya Card need to provide their personal details. As explained below, these dark web shops sell packages of compromised account details and user logs; cybercriminal actors could purchase compromised account

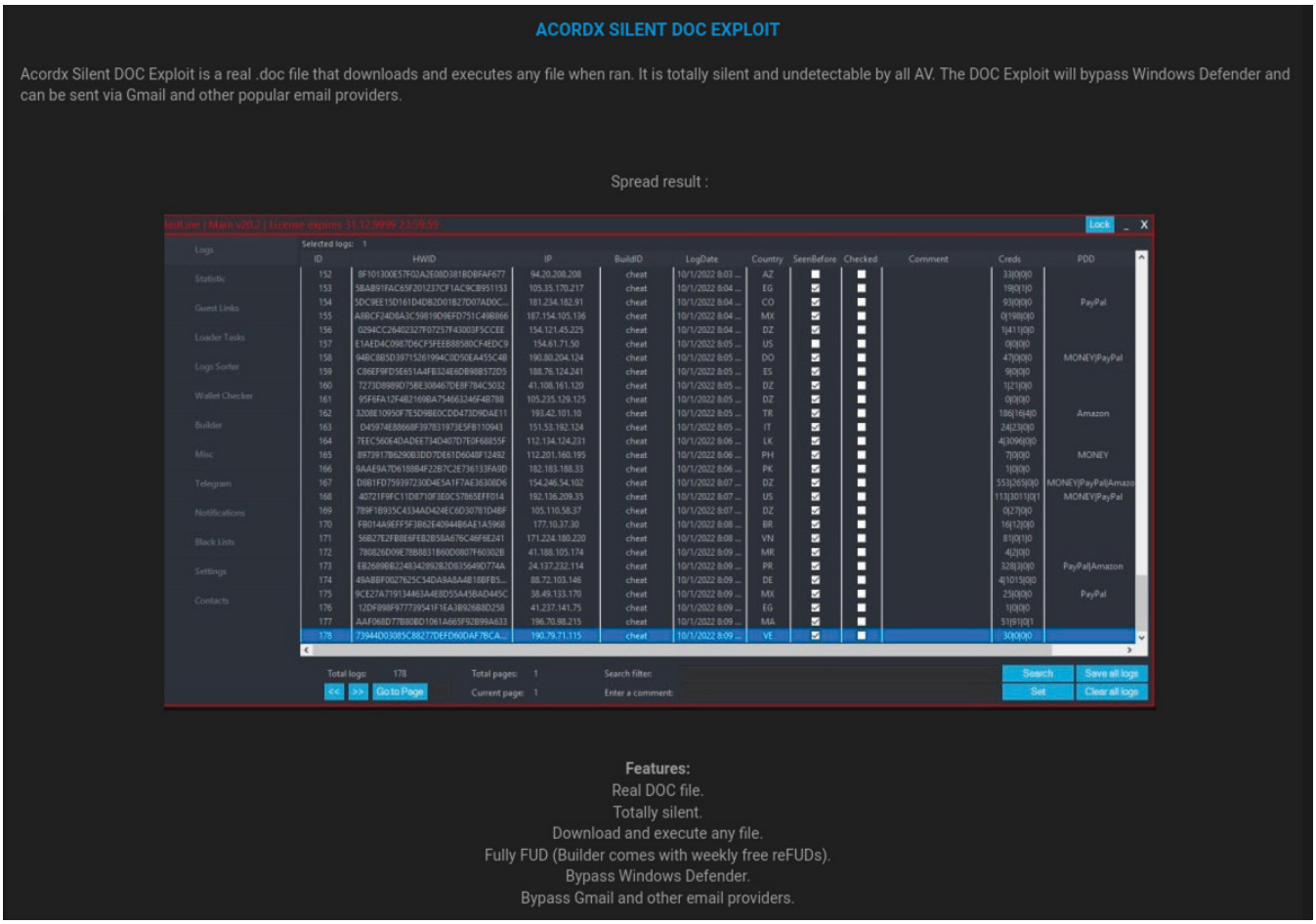


Figure 3: *Exploit with features advertised by xAcordx (Source: Cracked Forum)*

details from these, and other, dark web shops and marketplaces that could lead to greater theft of PII data and possibly match tickets.

- Russian Market is a dark web shop operated by the threat actor RussianMarket that sells dumps, RDP and SSH access, logs, and various account details. Threat actors who purchase credentials typically log in to the accounts and perform malicious activities such as BEC, privilege escalation, and overall online identity takeovers due to extensive information about the source of the credentials and cookies being scraped from victims.
- Genesis Store sells packages of compromised account credentials and associated user data designed to allow threat actors to bypass anti-fraud solutions. Victim data is sold in a single package referred to as a "bot", which includes account credentials, IP address, browser fingerprint (system information), and cookies. After purchasing a bot, the victim data can be imported into a browser plugin called Genesis Security, allowing the attacker to masquerade as the victim to perform attacks such as account takeovers or card-not-present fraud. The price for each bot varies depending on the amount of account credentials, types of accounts, and geographical location of the victim

2easy Shop sells stealer logs harvested from victims infected with infostealers. The prices for logs vary between $3 and $200 per listing and include compromised user logs and accounts from hundreds of organizations worldwide. When compromised data is purchased on 2easy Shop, a buyer typically receives a victim's browser cookie data, browser history, screenshots, general system information about compromised machines, and other data. The compromised account credentials and associated user data are commonly used by threat actors to bypass targeted organizations' defenses and anti-fraud solutions.

Ransomware

We have not identified any specific threats made by ransomware groups demonstrating intent to target the 2022 FIFA World Cup, though we would not expect such conversations to appear in the open. Similar to what we described in our report on Threats to the 2022 Winter Olympics, the 2022 FIFA World Cup may be seen as an attractive target for ransomware attacks given the potential for significant profit, as organizations involved in the tournament will want to ensure the tournament goes as smoothly as possible. Potential targets could include organizations that support the 2022 FIFA World Cup, including those in the transportation, media, healthcare, logistics, and security sectors. However, it is more likely that ransomware operators would seek to opportunistically target victims based on accessibility, opportunity, and factors such as the ability to pay large ransom amounts, as opposed to conducting a large-scale coordinated attack. We have created dozens of Hunting Packages for ransomware families that can be used to detect ransomware samples and behavior.

As discussed above, as a result of Russia being banned from participating in the 2022 FIFA World Cup due to their war against Ukraine and their strained relations with Qatar, we cannot rule out that the Russian government will encourage or otherwise tacitly approve disruptive attacks conducted by nationalistic Russian "hacktivist" groups — such as KillNet or XakNet — or by ransomware operators. Such threat groups, whether financially or politically motivated, are useful proxy forces that can on occasion further the Russian government's strategic objectives and provide plausible deniability. We have previously documented the ties between the Russian state and Russia-based cybercriminals in our report "Dark Covenant: Connections Between the Russian State and Criminal Actors".

Influence Operations

As a result of Qatar's unique geopolitical position, influence operations involving the 2022 FIFA World Cup will likely attempt to "win over" Qatar by emphasizing and promoting bilateral relations while creating and exacerbating tensions between Qatar and the influencer's adversaries. As discussed above, Qatar maintains good relations with Iran and China, and previously had good relations with Russia that have since been strained as a result of Qatar siding with the coalition of countries supporting Ukraine's territorial integrity. Meanwhile, Qatar enjoys good relations with the US, UK, Germany, and many other Western countries. Qatar also offers Europe an alternative to their dependency on Russian gas exports during Russia's war against Ukraine.

Positive Influence

We have observed efforts by Iran, China, and Russia to emphasize their support for Qatar in hosting the 2022 FIFA World Cup and to promote bilateral relations through state-owned media outlets. For example:

- Iran's Mehr News Agency[2] published an article on October 18, 2022 entitled "Iran calls for boosting Tehran-Doha economic cooperation", citing "the readiness of the Islamic Republic of Iran to provide any kind of assistance for holding the 2022 World Cup in Doha".[3]
- China's Global Times published an article on October 24, 2022 entitled "China-Qatar relations exemplified in World Cup preparation, giant panda fostering, joint efforts in energy crisis: ambassador" following an interview with

Qatar's Ambassador to China Mohammed bin Abdullah Al Dehaimi.[4]

- Russia's RT published an article on October 13, 2022 citing Putin's support of Qatar hosting the 2022 FIFA World Cup, stating that Russia is "doing everything we can in terms of transferring [our] experience of preparing for the World Cup", with the Emir of Qatar, Sheikh Tamim bin Hamad al-Thani, responding that "Russian friends have provided great support to Qatar, especially in terms of organization, with the organizing committee of the 2022 World Cup … We thank you for this and we are proud of this relationship".[5]

Negative Influence

Western countries (including Germany, Denmark, France, and others) have been critical of Qatar's hosting of the 2022 FIFA World Cup, citing human rights concerns in the country. This criticism presents an opportunity for adversaries to highlight divisions and exacerbate tensions between Qatar and the West. We have not observed China taking advantage of this opportunity, whereas Iran and Russia have used state-owned media organizations to highlight Western criticism of Qatar. For example:

Iranian state media highlighted multiple examples of Western countries criticizing Qatar due to human rights concerns, including: remarks from Germany's Interior Minister Nancy Faeser[6]; the Netherlands' House of Representatives asking the Dutch government to not send a delegation (though the Dutch government ultimately decided to send a delegation)[7]; German football player Toni Kroos stating that he's against the 2022 FIFA World Cup being hosted in Qatar[8]; and more.

Russia's RT also highlighted multiple examples of Western countries criticizing Qatar due to human rights concerns, including: multiple men's football teams protesting with their football kits[9] [10]; remarks from Germany's Interior Minister Nancy Faeser[11]; reports that some French cities will not be broadcasting the 2022 FIFA World Cup in public areas in protest against Qatar[12]; and more.

Global Research's French-language website, Mondialisation[.]ca, published an article on October 28, 2022 stating that Western countries have launched a campaign to criticize Qatar on "LGBT issues, or the conditions of foreign workers" because Qatar has "not bowed to Western pressure on gas supplies to replace Russian gas".[13] Global Research is a documented pillar of Russian disinformation and propaganda, and has previously "published or republished seven authors attributed by Facebook to be false online personas created by The Main Directorate of the General Staff of the Armed Forces of the Russian Federation, popularly known as the GRU".

- Both Iran's Fars News[14] and Russia's RT France[15] published articles on October 25, 2022 citing the Emir of Qatar, who stated that Qatar has faced unprecedented criticism since winning the bid to host the 2022 FIFA World Cup and that the criticism included "fabrications and double standards that were so ferocious that it has unfortunately prompted many people to question the real reasons and motives behind the campaign".

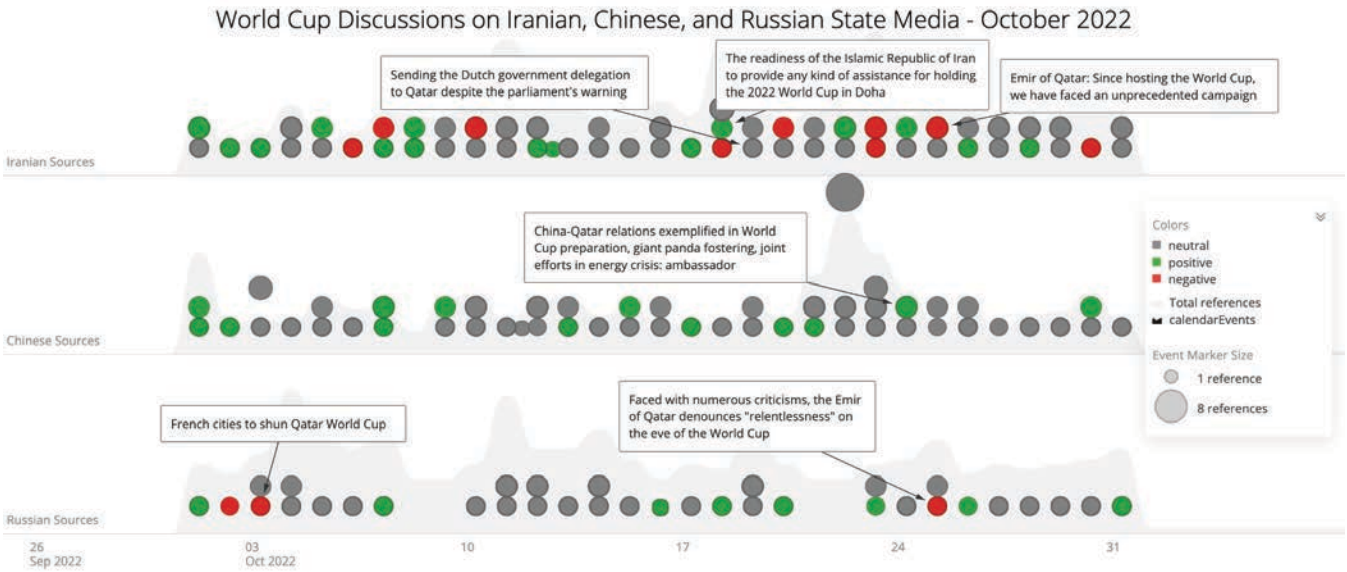


Figure 4: *Sentiment analysis of references to the 2022 FIFA World Cup on Iranian, Chinese, and Russian state media sources (Source: Recorded Future)*

Endless Mayfly

There is a particular precedent in Iran for using influence operations in an attempt to sow discord between Qatar and its international partners and regional neighbors, such as the Endless Mayfly influence operation uncovered by Citizen Lab in May 2019. This influence operation was "an Iran-aligned network of inauthentic websites and online personas" used to amplify geopolitical tensions by spreading false and divisive information critical of Saudi Arabia, the US, and Israel, among others, since at least early 2016.

The Endless Mayfly influence operation included 1 instance of disinformation specifically involving the 2022 FIFA World Cup, namely that 6 Arab countries had asked FIFA to strip Qatar's right to host the FIFA World Cup in 2022. This disinformation attempted to exacerbate geopolitical tensions between Qatar and Arab countries following the Qatar diplomatic crisis in June 2017, whereby Gulf countries and other Arab nations including Saudi Arabia, the United Arab Emirates (UAE), Egypt, Bahrain, and others severed diplomatic relations with Qatar, blaming Qatar for "[embracing] various terrorist and sectarian groups aimed at destabilising the region", including the Muslim Brotherhood, al-Qaeda, Islamic State, and Iran-supported proxy groups within Gulf nations. The 1 instance of disinformation involving the 2022 FIFA World Cup was part of 11 inauthentic articles identified by Citizen Lab that aimed to exacerbate Saudi-Qatar tensions.

Endless Mayfly's disinformation campaign involving the 2022 FIFA World Cup involved the creation of an inauthentic The Local article on July 15, 2017 alleging that 6 Arab countries had asked FIFA to strip Qatar's right to host the 2022 FIFA World Cup. The inauthentic article was hosted on a lookalike domain, telocal-xt3c[.]com, instead of thelocal[.]com. Reuters then published an article on July 16, 2017 citing the inauthentic The Local article, with the heading "Boycott nations demand FIFA strips Qatar of 2022 FIFA World Cup – report".

LONDON (Reuters) - The six Arab countries who last month cut ties with Qatar are reported to have written to world soccer's governing body FIFA to demand it be stripped of hosting the 2022 World Cup because they consider the Gulf state to be a "base of terrorism".

The Swiss website The Local reported that Saudi Arabia, Yemen, Mauritania, the United Arab Emirates, Bahrain and Egypt had collectively written to FIFA asking it to remove Qatar as hosts under Article 85 of the FIFA Code, which allows for such action in the case of emergency.

Reuters has not seen a copy of the letter and FIFA said that their president Gianni Infantino had not received any such document.

Figure 5: *Reuters article citing the inauthentic The Local article involving the 2022 FIFA World Cup (Source: Reuters[16])*

Then, an Endless Mayfly online persona, @Shammari_Tariq, published an article on Buzzfeed Community, which allows for user-submitted content, amplifying the story and citing the inauthentic The Local article and the Reuters article. Another Endless Mayfly online persona, @GerouxM, published a story on Medium reiterating the claim and citing the inauthentic The Local article. Furthermore, after the Reuters article was published, several other media outlets such as Global News, The Jerusalem Post, Bleacher Report, and Haaretz also reported on the story, quickly propagating the disinformation to a wider audience.

Iran has demonstrated a continued interest in leveraging the 2022 FIFA World Cup to sow division and exacerbate geopolitical tensions between Qatar and other countries. For example, an article published by Iran's Mehr News Agency on September 13, 2022 stated that "The Qatari government announced its absolute opposition to the Zionist regime's [Israel's] demand for the opening of the temporary consulate in Doha during the World Cup" after the "Israeli regime had pressured FIFA to put pressure on Doha so that Qatar would accept Tel Aviv's demand"[17].

Physical Threats

Qatar is unlikely to face a major physical security threat during the 2022 FIFA World Cup based on the event's substantive security apparatus and decreased capabilities of global terrorist organizations. An externally directed terrorist attack, while unlikely for reasons enumerated below, would have the greatest potential impact, and unmanned aerial systems (UAS) represent a unique threat vector for targeting attendees and disrupting the event. Qatar has taken steps to mitigate this risk by bolstering its defenses and is receiving security assistance from multiple countries for the duration of the 2022 FIFA World Cup, particularly to defend against any UAS attacks.

Terror Tactics and UAS

Terrorist attacks typically use unconventional methods to inflict casualties, disrupt societies, and damage economies. These tactics vary based on the environment in which the terrorists operate, but have included solo knife attacks, coordinated small arms operations, suicide bombings, vehicle ramming, and UAS, including so-called "suicide drones". The use of UAS represent a potentially significant evolution in terrorist operations since it utilizes commercial off-the-shelf technology readily available in many countries, which can be modified to deploy explosive payloads or perform target reconnaissance. UAS may also be operated beyond line of sight, enabling operators to control them from a place of relative seclusion. More advanced UAS –– such as those reportedly supplied by Iran to the Ansar Allah (Houthis) movement for use against the Saudi-led coalition in

Yemen –– are capable of traveling long distances and could reach Qatari territory. Even unarmed UAS can pose a threat to critical infrastructure, as demonstrated by the standstill created by UAS flying near London's Gatwick Airport in December 2018 and Dubai Airport in 2016 and 2019.

Qatar has faced minimal terrorist attacks in recent years. According to the US Department of State, there were no reported terrorist incidents in Qatar in 2020 (the most recent year they published such data) or 2019. Recorded Future's Geopolitical Intelligence Module did not identify any notable references to terrorist attacks in Qatar in the last 3 years. There have also not been any recent UAS attacks against Qatar. However, the Houthis have used UAS against targets in nearby Saudi Arabia and the UAE in the past few years. For example, the Houthis launched UAS attacks against the UAE as recently as January and February of 2022, and have regularly targeted critical infrastructure in Saudi Arabia including oil facilities and pipelines and airports. Islamist terrorist groups such as ISIL have also used UAS, and the United Nations's top official on counter-terrorism, Vladimir Voronkov, reportedly told the UN Security Council in August 2022 that ISIL "has also significantly increased the use of UAS in the past year, including reported [sic] in northern Iraq".

Terrorist Groups

In June 2017 several Arab countries, including but not limited to Saudi Arabia, the UAE, Egypt, Jordan, and Bahrain, broke diplomatic ties with Qatar, accusing Qatar of embracing "various terrorist and sectarian groups aimed at destabilising the region", including the Muslim Brotherhood, al-Qaeda, ISIL, and groups supported by Iran in Saudi Arabia's eastern province of Qatif. This rupture came after years of similar concerns expressed in the US by Congressional members, Treasury Department officials, and foreign policy experts. Relations between Qatar and its fellow Gulf countries began to be restored in January 2021, and the US government has partnered with Qatari counterparts to stem the flow of terrorist financing on the Arabian peninsula, indicating that Doha is taking steps to address these concerns. Nevertheless, Qatar's unique geopolitical position, as discussed in the Influence Operations section of this report –– particularly its good relations with Iran –– likely contributes to the lack of terrorist attacks that have affected Qatar.

Although an externally directed terrorist attack against the 2022 FIFA World Cup is unlikely, the event does present an opportunity for a symbolic strike against a gathering that represents global cooperation and a relationship between Western countries and Muslim-majority and Arab nations. We note that an attack on the World Cup aligns with historic targeting objectives of the following terrorist organizations and actors:

- **ISIL —** Since the collapse of its caliphate under a US-led military campaign in March 2019, followed by the subsequent death of its founder, Abu Bakr al-Baghdadi, ISIL has endured a steady decline in its operational capacity, but still likely retains the capability to coordinate or inspire an attack on Qatari soil. Although ISIL has not conducted a large-scale external attack outside of the Levant since the 2019 Easter bombings in Sri Lanka, the 2022 FIFA World Cup would likely be a target of interest for the organization. This assessment is based on the high-profile nature of the event, which will draw numerous political delegations from major Western countries that ISIL has attacked previously, as well as threats ISIL has issued against the Qatari government for a number of perceived sins. These grievances include: hosting US and other foreign forces at Al Udeid air base; supporting the Iraqi Awakening Movement; and collaborating with the Iranian government, the IRGC, and Hezbollah (delivered in a May 2020 audio statement by the former ISIL spokesman, Abu Hamza al-Qurashi, and published in an article in a June 2020 edition of Al-Naba). Also, an infographic[18] in the most recent edition of Islamic State Khorasan Province (ISK)'s Voice of Khurasan magazine celebrated the recent death of Doha-based Sheikh Yusuf al-Qaradawi and denounced his service to the "Taghut of the at-Thani's house in Qatar" –– using the same derogatory term that ISK reserves for the Taliban, its primary antagonist in Afghanistan.
- **AQAP —** AQAP represents the Al-Qaeda branch that is most capable of conducting an operation targeting the 2022 FIFA World Cup, although operational limitations imposed by Yemen's intractable civil war very likely will reduce AQAP's ability to launch such an attack. As noted by a recent UN Security Council report, despite battlefield setbacks in recent years, AQAP remains a serious threat in Yemen and seeks to reconstitute its ability to conduct international operations. However, the realities of fighting a multifront war against the Houthis, Saudi-led coalition forces, and members of the Islamic State's Yemen affiliate have required AQAP to retrench significantly. Aside from 2 attacks in 2019, occurring in Saudi Arabia and the US, the group has focused its operations on targets within Yemen –– indicating that the World Cup presents an unlikely target.
- **Lone Wolves —** Despite not sending a significant number of foreign fighters to Iraq and Syria during the rise of ISIL's self-declared caliphate (and thus having a limited rate of returnee extremists), Qatar contends with an elevated risk of domestic violent extremism; a lone wolf

attack targeting the World Cup is thus a possibility, although such an event is unlikely. In 1 social media study conducted in 2014, 47% of Qatar-based social media posts about ISIL expressed positive sentiment, a significant deviation from the much lower percentages found across Europe and the Middle East. Although the US Department of State believes Qatar is making strides in addressing violent extremism, its most recent country report pointedly observed that state-supported intolerance, sectarianism, and violence is still found in textbooks and disseminated through media.

Security Defenses

Qatar has enhanced its own security in the lead-up to the 2022 FIFA World Cup. The government plans to use its own drones to enhance surveillance and security patrols, and the Qatari government reportedly deployed 32,000 government security forces and 17,000 private security forces during a 5-day security exercise across the country in October 2022, indicating the scale of Qatar's security defenses. Furthermore, Qatar is receiving security assistance from multiple countries for the duration of the 2022 FIFA World Cup, including:

- The US: the US made a number of commitments "to strengthen Qatar's event security, port security, screening, contraband interdiction, and risk management capabilities", such as helping Qatar "to identify air passengers linked to terrorism and trafficking of narcotics, weapons, currency, and people". The New York Police Department also met with Qatar's police forces to exchange expertise. More recent memorandums of understanding have been signed between the US and Qatar on defense cooperation around the 2022 FIFA World Cup.
- The UK: the Royal Air Force (RAF) and Royal Navy "will support Qatar with military capabilities to counter terrorism and other threats to the tournament" including "maritime security support from the Royal Navy, advanced venue search training, operational planning and command and control support, and further specialist advice".
- France: France is sending around 220 police officers to provide "high-level expertise and specialised logistical support". The officers primarily consist of anti-drone policing, in addition to bomb-disposal experts, sniffer dogs, anti-terror police, and police offers specialized in tackling football hooliganism. Other French support reportedly includes "a BASSALT anti-drone system that detects and identifies incoming drones" and an E-3F Airborne Warning and Control System (AWACS) aircraft.
- Italy: the Italian Air Force is "deploying a Counter-Unmanned Aerial Anti-Drone Task group to further support the Qatari Armed Forces' defense" against UAS, with Italian armed forces troops being stationed in the country during the tournament.
- Türkiye: Türkiye is providing 3,000 riot police, 100 special operations police, 50 bomb specialists, and 80 sniffer dogs and riot dogs to Qatar.
- Pakistan: Pakistan is sending an army contingent to provide security during the tournament.
- Jordan: Jordan expressed its willingness to assist with security at the 2022 FIFA World Cup, with reports stating that as many as 6,000 ex-Jordanian soldiers were hired into security jobs for the tournament, some of whom have allegedly returned to Jordan after a salary dispute.

An additional mitigating factor decreasing the threat of terrorism to the 2022 FIFA World Cup is Qatar's geographical orientation. Qatar only shares 1 land border with Saudi Arabia and is a peninsula in the Persian Gulf. The border with Saudi Arabia is isolated, has a flat desert topography, and is small enough for security forces to control. While the borders of Bahrain and the UAE are only roughly 10 to 20 miles across the Persian Gulf, these countries, like Saudi Arabia, have cordial relations with Qatar and are not primary incubators of terrorist groups that would seek to target Qatar. A lack of accessible ingress opportunities for terrorist organizations into Qatar, along with Qatar's security defenses discussed above, mitigate (but do not eliminate) the threat of terrorism to the 2022 FIFA World Cup.

Outlook

Qatar's unique geopolitical position on a contentious global stage means it's unlikely that state-sponsored APT groups from China, Russia, Iran, and North Korea will conduct a disruptive attack against the 2022 FIFA World Cup, despite Russia having the greatest motivations for doing so. Instead, nationalistic Russian hacktivist groups or ransomware operators could conduct disruptive attacks against the tournament, which as previously noted can provide the Kremlin with plausible deniability.

Cybercriminal phishing attacks are almost certainly going to continue throughout the 2022 FIFA World Cup tournament, before dispersing after the tournament concludes. It's very unlikely that tournament-themed phishing attacks targeting businesses will continue to use lures that invite victims to bid on contracts or supply goods or services to the tournament given that the tournament begins soon.

It is very likely that Iran and Russia will continue to highlight divisions and exacerbate tensions between Qatar and Western countries that are critical of the tournament being hosted in Qatar, while also promoting their own bileratel relations. Furthermore, Iran, China, and Russia are likely to use the 2022 FIFA World Cup in future influence operations as an example of where the West has sought to impose "Western values" on other countries.

Finally, Qatar is unlikely to face a major physical security threat during the 2022 FIFA World Cup based on the factors explained above. Although Iran, China, Russia are emphasizing and promoting bilateral relations with Qatar through discourse, countries like the US, UK, France, Italy, Türkiye, and others are providing material security assistance to Qatar for the tournament. This security assistance, building on other security cooperation, in addition to the US formally designating Qatar as a "major non-NATO ally" in March 2022, is likely to lead to further security cooperation between Qatar and Western countries.

The sources used in this report are the Recorded Future® Platform and open sources.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.

Endnotes

1 Fraudulent websites include typosquat domains and similar domains. Typosquat domains manipulate the characters in a legitimate domain to create nearly identical domains, often containing a single "typo", such as qatar2o22[.]qa as a typosquat of qatar2022[.]qa. Similar domains are broader and can contain additional keywords, but still intend to deceive the recipient into thinking they are legitimate; for example, ticket-sales-qatar2022[.]com is a similar domain to qatar2022[.]qa.
2 Mehr News Agency is owned by the Islamic Development Organization (also known as the Islamic Propaganda Organization), which is dedicated to the promotion of Islam and the preservation of the ideologies of the Islamic Revolution under the direction of Iran's Supreme Leader.
3 https://en.mehrnews[.]com/news/192618/Iran-calls-for-boosting-Tehran-Doha-economic-cooperation
4 https://www.globaltimes[.]cn/page/202210/1277844.shtml
5 https://www.rt[.]com/sport/564593-putin-message-qatar-world-cup/
6 https://www.farsnews[.]ir/news/14010806000785/%D9%88%D8%B2%D8%A7%D8%B1%D8%AA-%D8%AE%D8%A7%D8%B1%D8%AC%D9%87-%D9%82%D8%B7%D8%B1-%D8%B3%D9%81%DB%8C%D8%B1-%D8%A2%D9%84%D9%85%D8%A7%D9%86-%D8%B1%D8%A7-%D8%A7%D8%AD%D8%B6%D8%A7%D8%B1-%DA%A9%D8%B1%D8%AF
7 https://www.tasnimnews[.]com/fa/news/1401/07/27/2790655/%D8%A7%D8%B9%D8%B2%D8%A7%D9%85-%D9%87%DB%8C%D8%A6%D8%AA-%D8%AF%D9%88%D9%84%D8%AA%DB%8C-%D9%87%D9%84%D9%86%D8%AF-%D8%A8%D9%87-%D9%82%D8%B7%D8%B1-%D8%A8%D8%A7-%D9%88%D8%AC%D9%88%D8%AF-%D9%87%D8%B4%D8%AF%D8%A7%D8%B1-%D9%BE%D8%A7%D8%B1%D9%84%D9%85%D8%A7%D9%86
8 https://www.mashreghnews[.]ir/news/1425851/%D9%85%D9%86-%D9%85%D8%AE%D8%A7%D9%84%D9%81-%D8%AC%D8%A7%D9%85-%D8%AC%D9%87%D8%A7%D9%86%DB%8C-%D9%82%D8%B7%D8%B1-%D9%87%D8%B3%D8%AA%D9%85
9 https://www.rt[.]com/sport/565447-australian-footballers-qatar-world-cup-message/
10 https://www.rt[.]com/sport/519423-qatar-world-cup-deaths-kimmich-germany/
11 https://www.rt[.]com/sport/565580-qatar-summons-german-ambassador-world-cup-criticism/
12 https://www.rt[.]com/sport/564014-french-cities-qatar-world-cup-boycott/
13 https://www.mondialisation[.]ca/pour-avoir-refuse-de-ceder-aux-pressions-occidentales-sur-le-gaz-le-qatar-objet-de-campagne-hypocrite-de-boycott-du-mondial/5672315
14 https://www.farsnews[.]ir/news/14010803000459/%D8%A7%D9%85%DB%8C%D8%B1-%D9%82%D8%B7%D8%B1-%D8%A7%D8%B2-%D8%B2%D9%85%D8%A7%D9%86-%D9%85%DB%8C%D8%B2%D8%A8%D8%A7%D9%86%DB%8C-%D8%AC%D8%A7%D9%85-%D8%AC%D9%87%D8%A7%D9%86%DB%8C-%D8%A8%D8%A7-%DA%A9%D8%A7%D8%B1%D8%B2%D8%A7%D8%B1-%D8%A8%DB%8C%E2%80%8C%D8%B3%D8%A7%D8%A8%D9%82%D9%87%E2%80%8C%D8%A7%DB%8C-%D9%85%D9%88%D8%A7%D8%AC%D9%87-%D8%B4%D8%AF%DB%8C%D9%85
15 https://francais[.]rt[.]com/international/101970-face-nombreuses-critiques-emir-qatar-denonce-acharnement
16 Citizen Lab stated that Reuters later retracted their story, though it remains live on their website.
17 https://en[.]mehrnews[.]com/news/191387/Qatar-rejects-Israeli-request-for-temporary-consulate
18 https://archive[.]org/details/voice-of-khurasan-issue-17/page/2/mode/2up