FIFA World Cup Qatar 2022: Cyber Threat Landscape
# Table of Contents

**Threat Actors Follow Audiences to the Qatar 2022 FIFA World Cup**  
Background  3  
Cybercriminals and their Motivation  3  
   Financially Motivated Threat Actors  3  
   Hacktivists  3  

**Different Types of FIFA-Themed Cyber Attacks**  
   Cashing Stolen Credit Cards  5  
   Selling Fake Hayya Cards  6  
   Forged Hayya Cards  6  
   Fake Crypto Tokens and Coins  7  
   Phishing and Ticket Sale Scams  8  
   DDoS Attacks  11  
   Betting and Gambling Services  12  

**Recommendations**  
   Recommendations for FIFA Fans  13  
   Recommendations for Participating Organizations  14  

**About CloudSEK**  14
Schedule a CloudSEK demo

At CloudSEK, we predict cyber threats.

Our solutions have relevant use cases for several industries including BFSI. At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface monitoring, Infrastructure Monitoring and Supply chain to give visibility and context to our customer's Initial Attack Vectors.

Interested to know more? Let our CloudSEK experts give you a detailed walkthrough of our platform's capabilities.

Request A Demo
Threat Actors Follow Audiences to the Qatar 2022 FIFA World Cup

The hype and popularity of the FIFA world cup has attracted audiences from across the globe. And this in turn attracts a variety of cybercriminals, who want to exploit the varied fan following, and the organizations participating, to make a quick buck. APT campaigns, phishing, credit card fraud, DDoS attacks, and identity theft are among the threats faced by organizations and audiences. The cybercriminals are motivated by financial gain, ideology, or geo-political affiliations.

This report delves into various Qatar 2022 FIFA World Cup themed cyberattacks, their motivation, impact, and patterns.

Background

Previous large-scale sporting events like FIFA World Cup 2018 and the PyeongChang Winter Olympics 2018 were subject to 25 million and 12 million cyber-attacks per day respectively. For example: The Olympic Destroyer campaign was a devastating cyber attack that impacted the PyeongChang Winter Olympics 2018, and it originated from an advanced APT group.

Along with phishing scams from cyber criminals and advanced attacks from APT groups, the events also face threats from hacktivist groups trying to promote their agenda or bring attention to their cause. The threat of hacktivist attacks cannot be underplayed as recent events around the world have observed an increase in activity from hacktivist groups.

Cybercriminals and their Motivation

Financially Motivated Threat Actors

Cybercriminals motivated by financial gain have resorted to selling fake Hayya cards (FIFA entry permit), match tickets, and even leveraging stolen credit cards to arrange travel and lodging for the game.

Hacktivists

The world cup has attracted the attention of hacktivists groups, who have taken to social media to rally their followers and allies to boycott the Qatar 2022 FIFA World Cup. Messages from groups such as Anonymous, have also been posted on cybercrime forums, to call on other threat actors to support them.

FIFA 2022 Threat Landscape
Hacktivist post asking supporters to boycott Qatar 2022 World Cup

Anonymous
@Anonymousnn3

We #Anonymous join the protest and call on the entire international community to #BoycottQatar2022 over human rights violation. Over 6500+ people has died in 10 years of exploitation and overwork, most of them poor immigrants, at the construction of the 🏟️ in #Qatar. #OpFIFA

FIFA 2022 Threat Landscape

<table>
<thead>
<tr>
<th>Cyber threat actor</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation-states</td>
<td>Geopolitical</td>
</tr>
<tr>
<td>Cybercriminals</td>
<td>Profit</td>
</tr>
<tr>
<td>Hacktivists</td>
<td>Ideological</td>
</tr>
<tr>
<td>Terrorist groups</td>
<td>Ideological violence</td>
</tr>
<tr>
<td>Thrill-seekers</td>
<td>Satisfaction</td>
</tr>
<tr>
<td>Insider threats</td>
<td>Discontent</td>
</tr>
</tbody>
</table>

[Source]
Different Types of FIFA-Themed Cyber Attacks

Cashing Stolen Credit Cards

Telegram channels are offering services to book flights and hotels in Qatar.

Carding groups sell stolen credit card details to carry out illegal and unauthorized transactions. They also provide services to cash out money from these cards, using prepaid gift cards, to cover their tracks. Carding groups could be using FIFA-themed fake sites, such as the one shown below, to collect card details from unsuspecting users, and then use them to book hotel and flight tickets.
Selling Fake Hayya Cards

To attend a FIFA World Cup 2022 game in Qatar, one needs to have a Hayya card, which is essentially a permit document. It must be presented along with the original ticket in order to enter the stadium on game day. Due to the importance of Hayya cards during the world cup, threat actors are selling fake Hayya Cards to unsuspecting fans, who are willing to pay any amount to get one.

Several Telegram channels were found selling Hayya cards for prices ranging from USD 50 to USD 150. To create Hayya cards, the threat actors claim to require the buyer’s valid IDs like passports. And payment is only accepted in Bitcoin.

Apart from losing the money paid to the threat actor’s crypto wallet, the victims also inadvertently share their personally identifiable information (PII), which could be further used to scam them. Threat actors route the money in their crypto wallets via multiple exchanges/ currencies, making it difficult for law enforcement or other agencies to trace or retrieve victims’ money.

Forged Hayya Cards

There is also considerable chatter among threat actors, on cybercrime forums, regarding various methods to forge or hack FIFA services. Threat actors are also sharing hacking techniques that purportedly allow one to register for a Hayya card without a valid FIFA ticket number, for free. The technique is based on brute forcing the ticket number based on an alleged ticket number pattern that the threat actor shared: “300 and 4 random digits”.

FIFA 2022 Threat Landscape
Fake Crypto Tokens and Coins

Given that Crypto.com is an official FIFA sponsor and Binance has partnered with Cristiano Ronaldo to promote soccer-themed NFTs, threat actors are piggy-backing on this hype to sell fake “World Cup Coin” and “World Cup Token” by promoting them as limited edition cryptocurrency. However, most of these purported coins don’t exist. Yet, the promise of high returns and the novelty factor, lure crypto investors, enthusiasts, and collectors, to fall for these scams.
Phishing and Ticket Sale Scams

Since the FIFA world cup is a popular event, the demand for tickets far exceeds the supply. To exploit this gap between the supply and demand, scammers have set up websites that sell fake tickets.
The phishing sites ask users to sign up, and after collecting their PII, it redirects users to a payment page. After the payment is successful, users don’t receive tickets. In some cases, even the payment gateway is fake and is designed to steal banking information. Threat actors employ techniques such as fast flux, botnets, and reverse tunnel services to ensure that the fake sites are not detected and taken down.

There are even Telegram channels that claim to provide ticket availability checking services. They then notify users when tickets are available, and direct them to list phishing domains to book tickets.
FIFA World Cup Tickets Hunter

A telegram bot to notify you when a ticket is available on the FIFA WC Resale Platform.

Subscribe on Telegram

NOTE: Each message comes with the direct link to fifa.com's match webpage to quickly book tickets. Alternatively, you can visit fifa.com manually when you receive channel notifications for a match and book the tickets. Just make sure you do it quickly because tickets get sold as soon as they get listed on the resale platform.

A website offering service to check for tickets automatically

FIFA 2022 Threat Landscape
DDoS Attacks

Threat actors and hactivists claim to have launched DDoS attacks on Qatar based entities such as qatargas.com and moci.gov.qa. They have also shared proof that the sites that they have targeted are offline due to their attacks. These attacks are being shared on social media under the hashtags: #OpQatar, #OpFIFA, and #OpWorldcup.

Social Media Posts by Hacktivists announcing DDoS attacks on FIFA & Qatar

FIFA 2022 Threat Landscape
Social media posts by hacktivist group Anonymous announcing DDoS on Qatar government websites

<table>
<thead>
<tr>
<th>Websites Targeted by Hacktivists</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.mofa.gov.qa">www.mofa.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.motc.gov.qa">www.motc.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.qe.com.qa">www.qe.com.qa</a></td>
</tr>
<tr>
<td><a href="http://www.moci.gov.qa">www.moci.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.nas.gov.qa">www.nas.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.sjc.gov.qa">www.sjc.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.psa.gov.qa">www.psa.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.pp.gov.qa">www.pp.gov.qa</a></td>
</tr>
<tr>
<td><a href="http://www.qatargas.com.qa">www.qatargas.com.qa</a></td>
</tr>
<tr>
<td>gco.gov.qa</td>
</tr>
</tbody>
</table>

Betting and Gambling Services

As with elections or other sporting events, gambling and betting on the outcome of FIFA World cup matches is common. Threat actors are leveraging this to:

- Share prediction tips for a price

FIFA 2022 Threat Landscape
- Promote fake betting sites that steal users' money and PII
- Spread gambling apps laced with malware

**World Cup 2022 Betting Tips**

Telegram channel sharing betting tips

**World Cup 2022 Betting Tips**

This is a toughie. I have to give Belgium the top spot because of their quality on the ball. I wouldn't go as far as to put them as top cup-contenders, but are definitely one of the most talented squads there. With the creative brilliance of Eden Hazard and Kevin De Bruyne in the middle, along with the threat of striker Lukaku, this well-rounded, experienced squad will look to bounce back and go further than their 2018 WC semifinal loss to eventual champs France.

**FIFA 2022 Threat Landscape**

Recommendations

**Recommendations for FIFA Fans**

- Buy FIFA tickets and Hayya cards only from the official website.

**FIFA 2022 Threat Landscape**
● Validate the legitimacy of cryptocurrencies before investing in them.
● Don't avail FIFA related services from Telegram or social media.
● Do not share your PII or banking details with unknown persons or websites.
● Don't install applications shared via Telegram, social media, or from third-party app stores.
● Review permissions requested by apps and disable permissions that are not necessary for the app's functionality.
● Be wary of schemes that seem too good to be true.

Recommendations for Participating Organizations

● User load balancers or services like Cloudflare to avoid DDOS attacks.
● Use a firewall and keep your software updated to the latest version.
● Run awareness campaigns to educate fans and users about legitimate portals and websites.
● Real-time monitoring and takedown of phishing sites, fake apps, and copy-cat social media pages.
● Report the findings to relevant authorities who can take action against the threat actors.

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats even before they occur. We combine the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply chain intelligence to provide context to our customer’s digital risks. Our unified dashboard allows customers to triage and visualize all digital threats in one place. We also offer workflows and integrations to manage and remediate the identified threats. To learn more about CloudSEK, visit cloudsek.com.