CloudSEK

Research Paper

FIFA World Cup Qatar 2022: Cyber Threat Landscape

Table of Contents

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

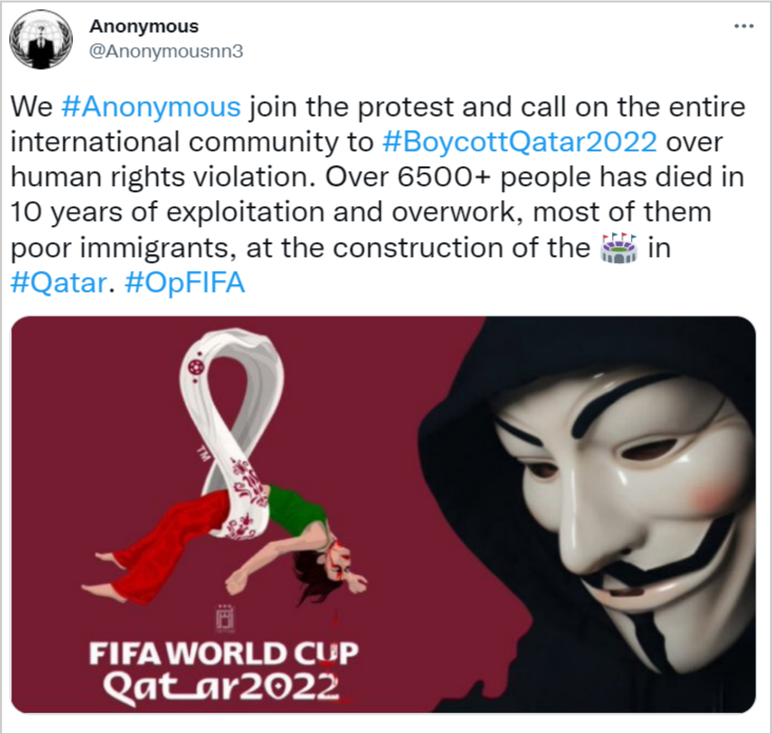
Financially Motivated Threat Actors

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.

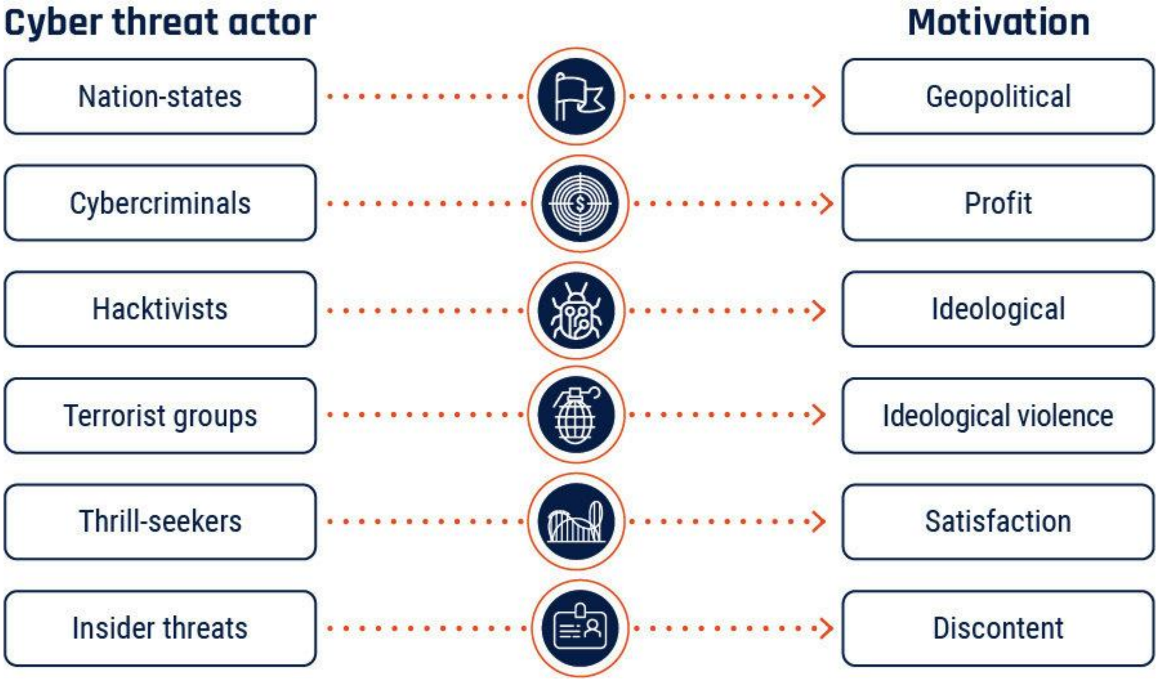
FIFA 2022 Threat Landscape



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

Hacktivist post asking supporters to boycott Qatar 2022 World Cup



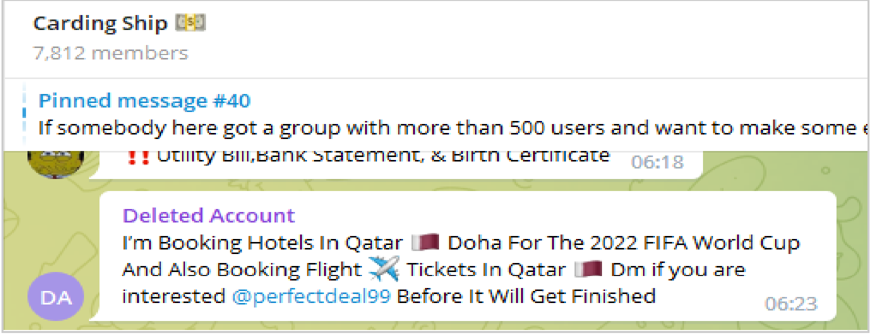
Cyber threat actor	Motivation
Nation-states	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist groups	Ideological violence
Thrill-seekers	Satisfaction
Insider threats	Discontent

[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 Ship 💵
7,812 members

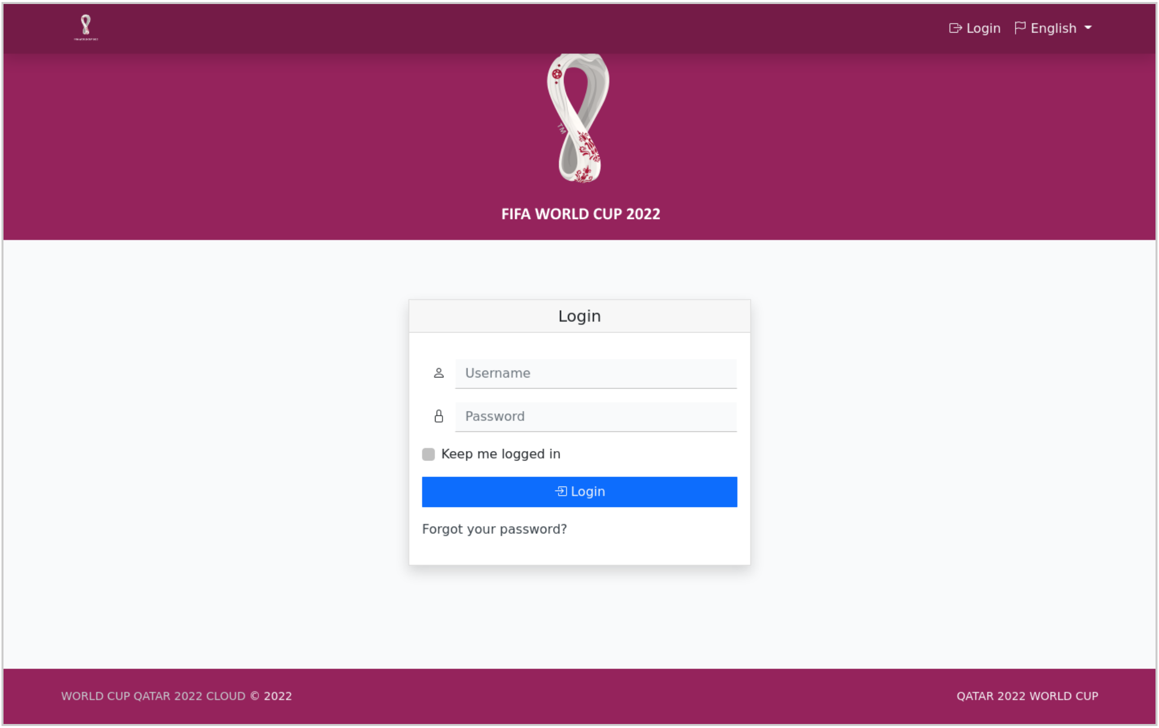
Pinned message #40
If somebody here got a group with more than 500 users and want to make some e

‼️ Utility Bill,Bank Statement, & Birth Certificate 06:18

Deleted Account
I'm Booking Hotels In Qatar 🇶🇦 Doha For The 2022 FIFA World Cup And Also Booking Flight ✈️ Tickets In Qatar 🇶🇦 Dm if you are interested @perfectdeal99 Before It Will Get Finished 06:23

Telegram message offering to book hotel and flight tickets to Doha

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.

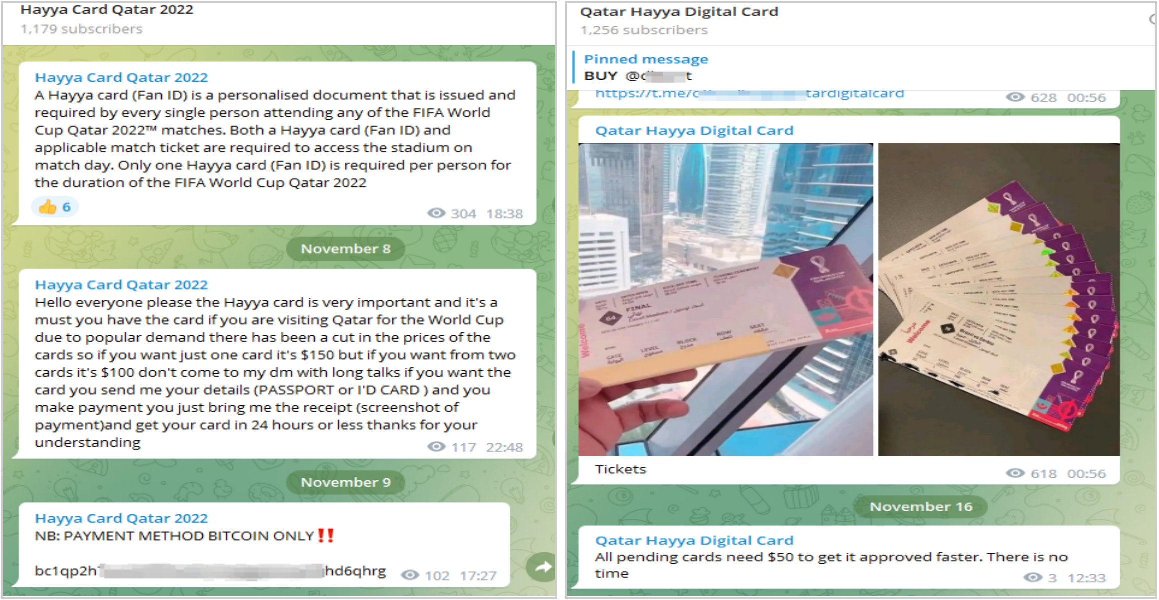


FIFA themed fake site

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.



Hayya Card Qatar 2022
1,179 subscribers

Hayya Card Qatar 2022
A Hayya card (Fan ID) is a personalised document that is issued and required by every single person attending any of the FIFA World Cup Qatar 2022™ matches. Both a Hayya card (Fan ID) and applicable match ticket are required to access the stadium on match day. Only one Hayya card (Fan ID) is required per person for the duration of the FIFA World Cup Qatar 2022
👍 6 304 18:38

November 8

Hayya Card Qatar 2022
Hello everyone please the Hayya card is very important and it's a must you have the card if you are visiting Qatar for the World Cup due to popular demand there has been a cut in the prices of the cards so if you want just one card it's $150 but if you want from two cards it's $100 don't come to my dm with long talks if you want the card you send me your details (PASSPORT or I'D CARD) and you make payment you just bring me the receipt (screenshot of payment)and get your card in 24 hours or less thanks for your understanding
117 22:48

November 9

Hayya Card Qatar 2022
NB: PAYMENT METHOD BITCOIN ONLY‼️
bc1qp2h[redacted]hd6qhrg 102 17:27

Qatar Hayya Digital Card
1,256 subscribers

Pinned message
BUY @c[redacted]t
https://t.me/c[redacted]tardigitalcard 628 00:56

Qatar Hayya Digital Card
Tickets 618 00:56

November 16

Qatar Hayya Digital Card
All pending cards need $50 to get it approved faster. There is no time
3 12:33

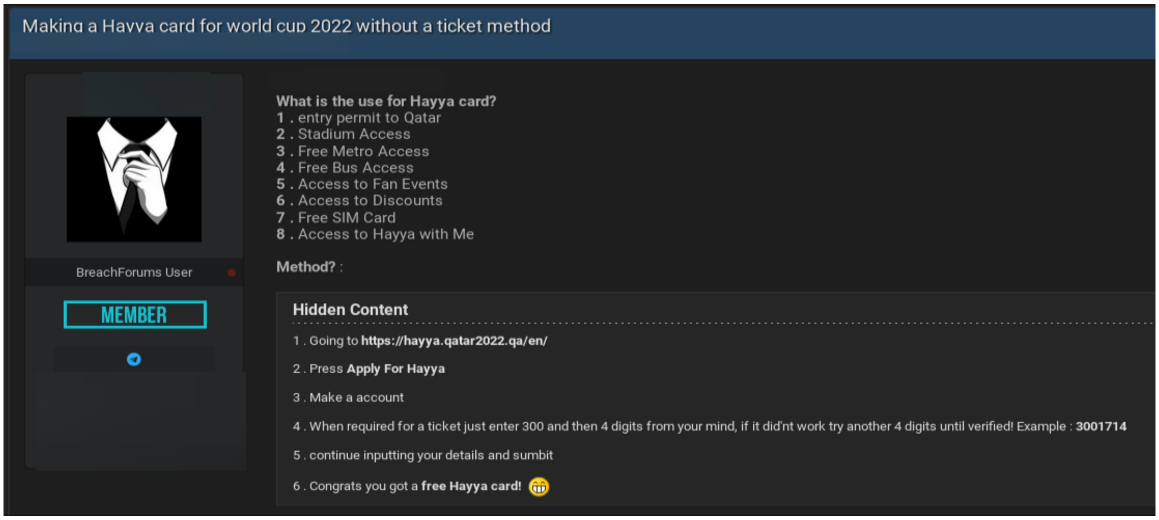
Telegram channels selling Hayya cards

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



Making a Hayya card for world cup 2022 without a ticket method

What is the use for Hayya card?
1 . entry permit to Qatar
2 . Stadium Access
3 . Free Metro Access
4 . Free Bus Access
5 . Access to Fan Events
6 . Access to Discounts
7 . Free SIM Card
8 . Access to Hayya with Me

Method? :

Hidden Content

1 . Going to **https://hayya.qatar2022.qa/en/**

2 . Press **Apply For Hayya**

3 . Make a account

4 . When required for a ticket just enter 300 and then 4 digits from your mind, if it did'nt work try another 4 digits until verified! Example : **3001714**

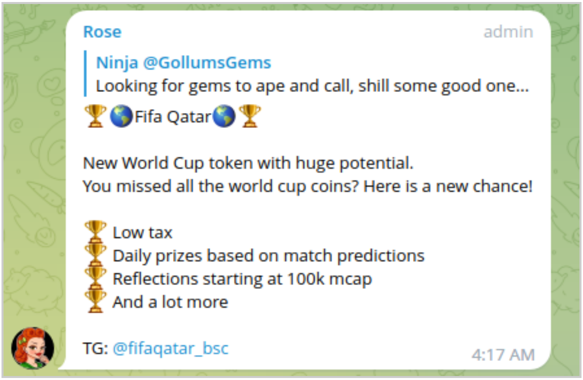
5 . continue inputting your details and sumbit

6 . Congrats you got a **free Hayya card!** 😁

Technique to register Hayya card without a valid ticket

Fake Crypto Tokens and Coins

Given that Crypto.com is an official FIFA sponsor and Binance has partnered with Christiano 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.



Rose admin

Ninja @GollumsGems
Looking for gems to ape and call, shill some good one...

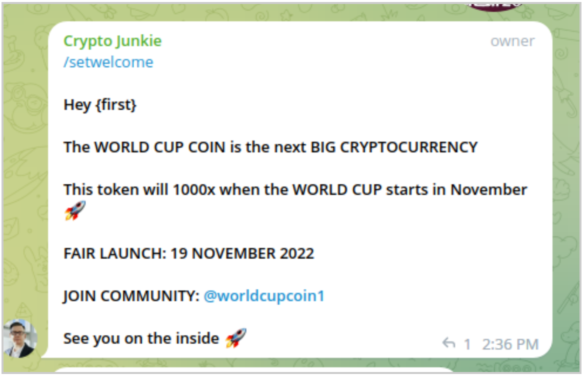
🏆🌎Fifa Qatar🌎🏆

New World Cup token with huge potential.
You missed all the world cup coins? Here is a new chance!

🏆 Low tax
🏆 Daily prizes based on match predictions
🏆 Reflections starting at 100k mcap
🏆 And a lot more

TG: @fifaqatar_bsc

4:17 AM



Crypto Junkie owner
/setwelcome

Hey {first}

The WORLD CUP COIN is the next BIG CRYPTOCURRENCY

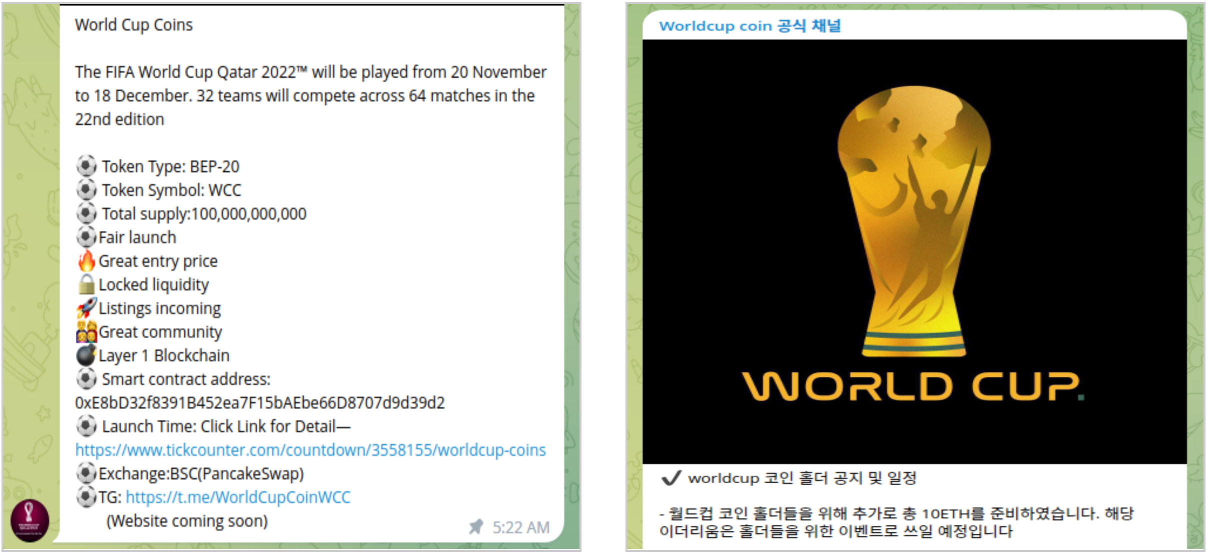
This token will 1000x when the WORLD CUP starts in November 🚀

FAIR LAUNCH: 19 NOVEMBER 2022

JOIN COMMUNITY: @worldcupcoin1

See you on the inside 🚀

1 2:36 PM



World Cup Coins

The FIFA World Cup Qatar 2022™ will be played from 20 November to 18 December. 32 teams will compete across 64 matches in the 22nd edition

⚽ Token Type: BEP-20
⚽ Token Symbol: WCC
⚽ Total supply:100,000,000,000
⚽Fair launch
🔥Great entry price
🔒Locked liquidity
🚀Listings incoming
👨‍👩‍👧‍👦Great community
💣Layer 1 Blockchain
⚽ Smart contract address:
0xE8bD32f8391B452ea7F15bAEbe66D8707d9d39d2
⚽ Launch Time: Click Link for Detail—
https://www.tickcounter.com/countdown/3558155/worldcup-coins
⚽Exchange:BSC(PancakeSwap)
⚽TG: https://t.me/WorldCupCoinWCC
(Website coming soon)

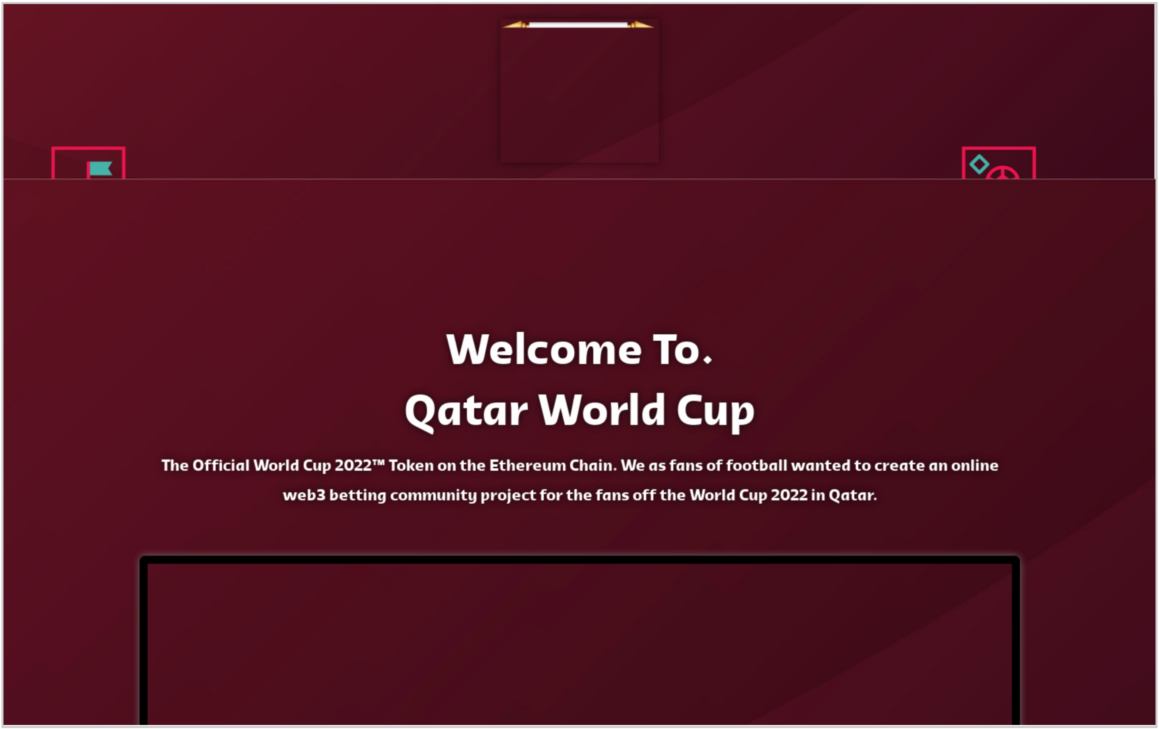
5:22 AM

Worldcup coin 공식 채널

✓ worldcup 코인 홀더 공지 및 일정

- 월드컵 코인 홀더들을 위해 추가로 총 10ETH를 준비하였습니다. 해당 이더리움은 홀더들을 위한 이벤트로 쓰일 예정입니다

Threat actors selling world cup coins and tokens



Welcome To.
Qatar World Cup

The Official World Cup 2022™ Token on the Ethereum Chain. We as fans of football wanted to create an online web3 betting community project for the fans off the World Cup 2022 in Qatar.

Suspicious site promoting crypto token

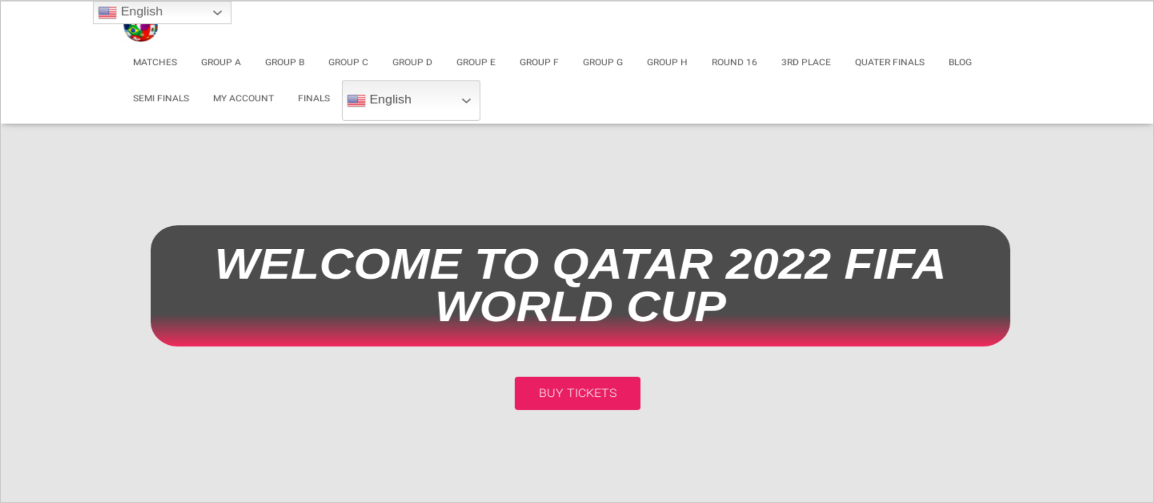
Phishing and Ticket Sale Scams

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.

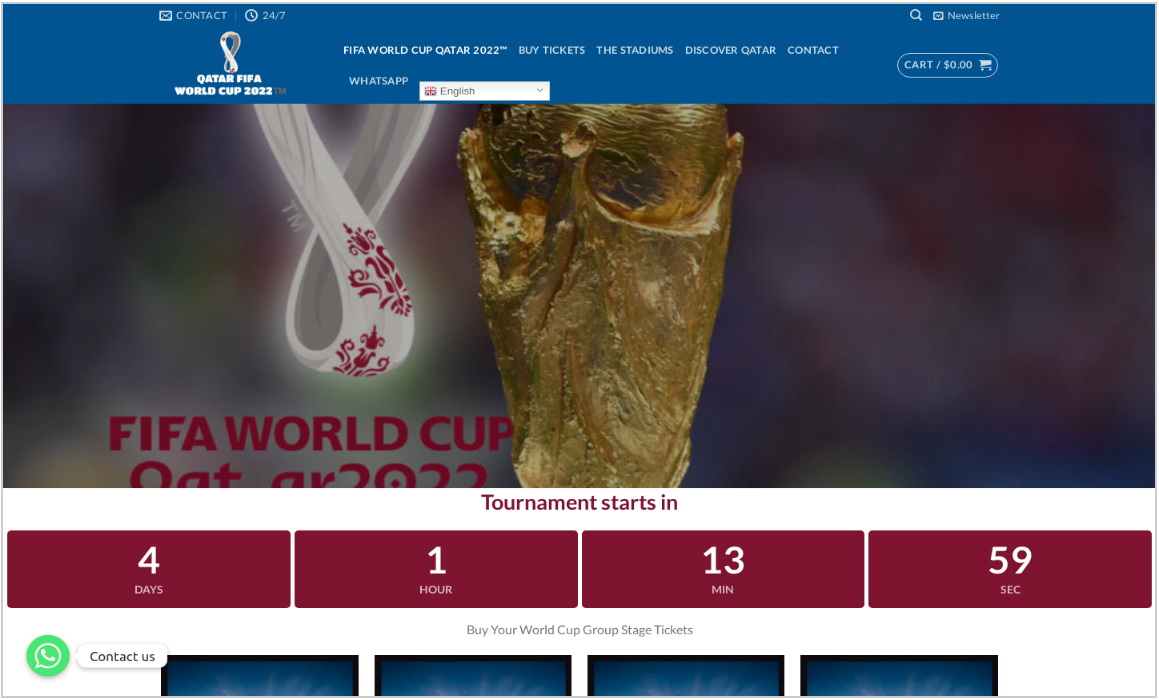
FIFA 2022 Threat Landscape

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.

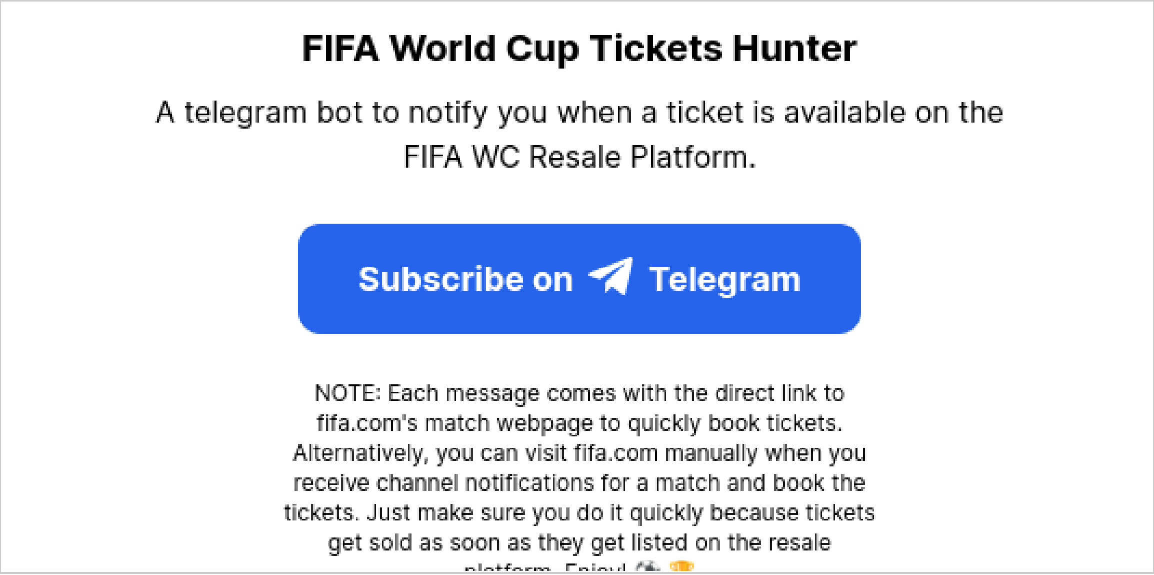


Site offering to sell FIFA World Cup tickets



Site offering to sell FIFA World Cup tickets

FIFA 2022 Threat Landscape

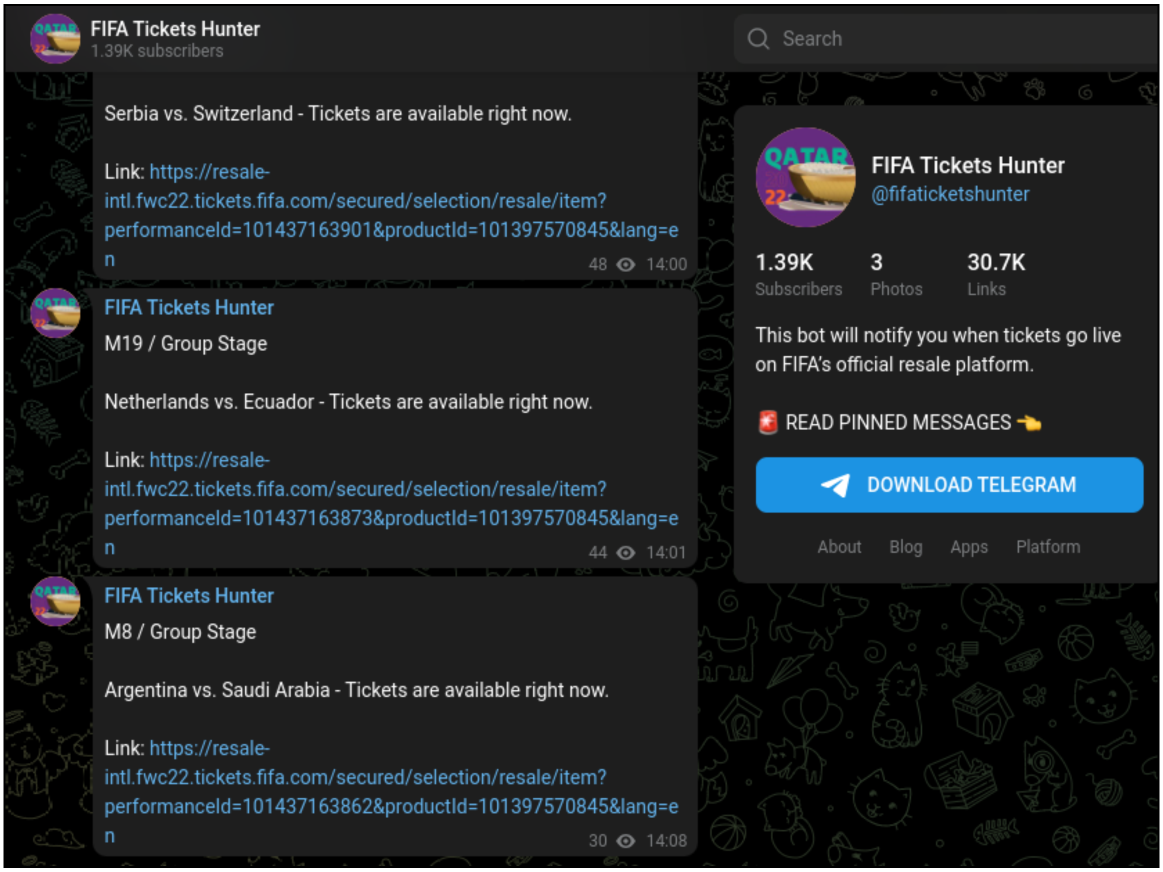


FIFA World Cup Tickets Hunter

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

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. Enjoy! ⚽ 🏆

A website offering service to check for tickets automatically



Serbia vs. Switzerland - Tickets are available right now.

Link: https://resale-intl.fwc22.tickets.fifa.com/secured/selection/resale/item?performanceId=101437163901&productId=101397570845&lang=en

48 14:00

FIFA Tickets Hunter

M19 / Group Stage

Netherlands vs. Ecuador - Tickets are available right now.

Link: https://resale-intl.fwc22.tickets.fifa.com/secured/selection/resale/item?performanceId=101437163873&productId=101397570845&lang=en

44 14:01

FIFA Tickets Hunter

M8 / Group Stage

Argentina vs. Saudi Arabia - Tickets are available right now.

Link: https://resale-intl.fwc22.tickets.fifa.com/secured/selection/resale/item?performanceId=101437163862&productId=101397570845&lang=en

30 14:08

FIFA Tickets Hunter
@fifaticketshunter

1.39K	3	30.7K
Subscribers	Photos	Links

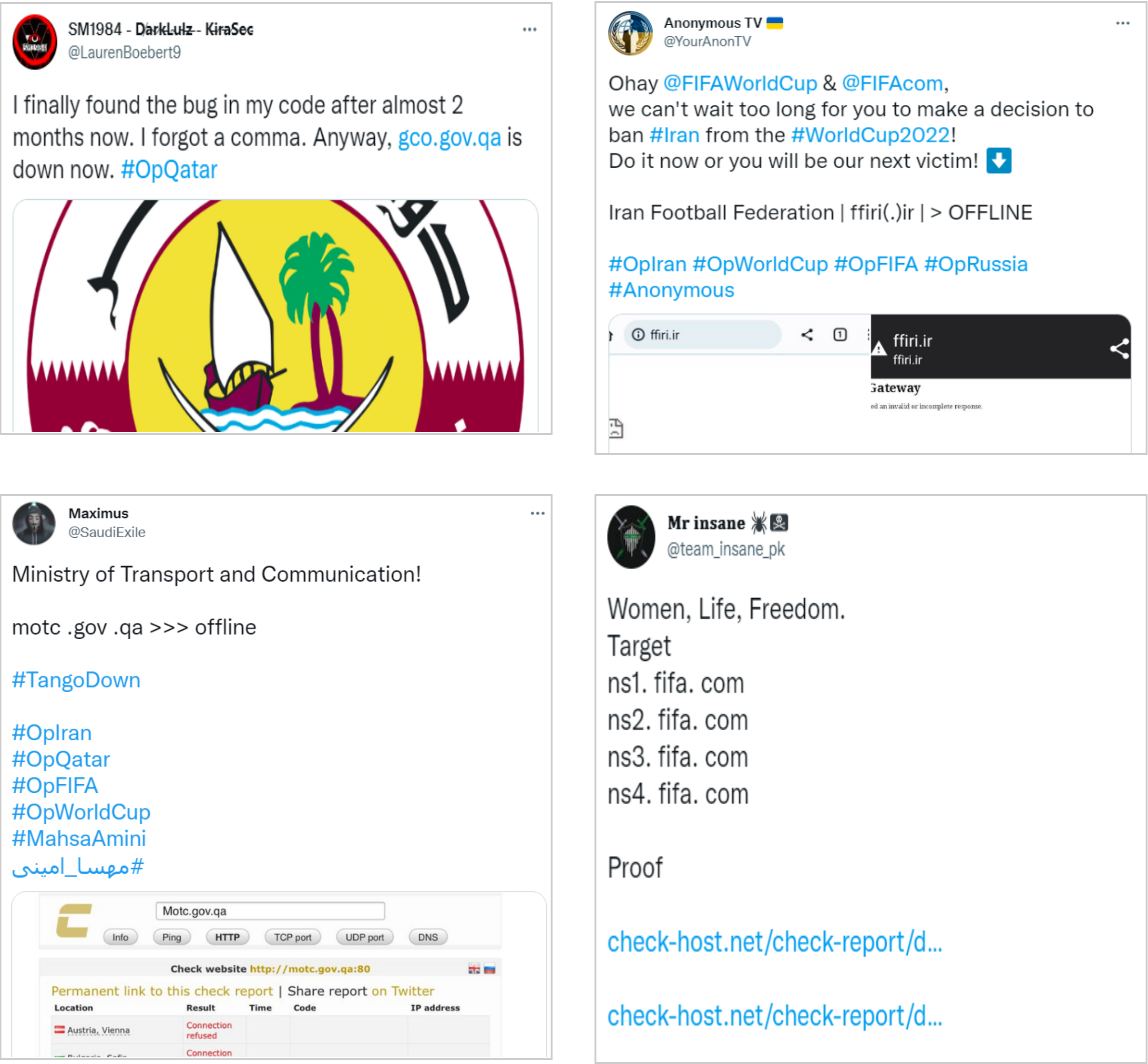
This bot will notify you when tickets go live on FIFA's official resale platform.

🚨 READ PINNED MESSAGES 👈

A telegram bot offering automatic ticket availability checking service

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 their attacks. These attacks are being shared on social media under the hashtags: #OpQatar, #OpFIFA, and #OpWorldcup.



SM1984 - ~~DarkLulz~~ - ~~KiraSec~~
@LaurenBoebert9

I finally found the bug in my code after almost 2 months now. I forgot a comma. Anyway, gco.gov.qa is down now. #OpQatar

Anonymous TV 🇺🇦
@YourAnonTV

Ohay @FIFAWorldCup & @FIFAcom,
we can't wait too long for you to make a decision to ban #Iran from the #WorldCup2022!
Do it now or you will be our next victim! ⬇️

Iran Football Federation | ffiri(.)ir | > OFFLINE

#OpIran #OpWorldCup #OpFIFA #OpRussia
#Anonymous

ffiri.ir
ffiri.ir
ffiri.ir
Gateway
ed an invalid or incomplete response.

Maximus
@SaudiExile

Ministry of Transport and Communication!

motc .gov .qa >>> offline

#TangoDown

#OpIran
#OpQatar
#OpFIFA
#OpWorldCup
#MahsaAmini
#مهسا_امینی

Motc.gov.qa

Check website http://motc.gov.qa:80

Permanent link to this check report | Share report on Twitter

Location	Result	Time	Code	IP address
Austria, Vienna	Connection refused			
Bulgaria, Sofia	Connection			

Mr insane 🕷☠
@team_insane_pk

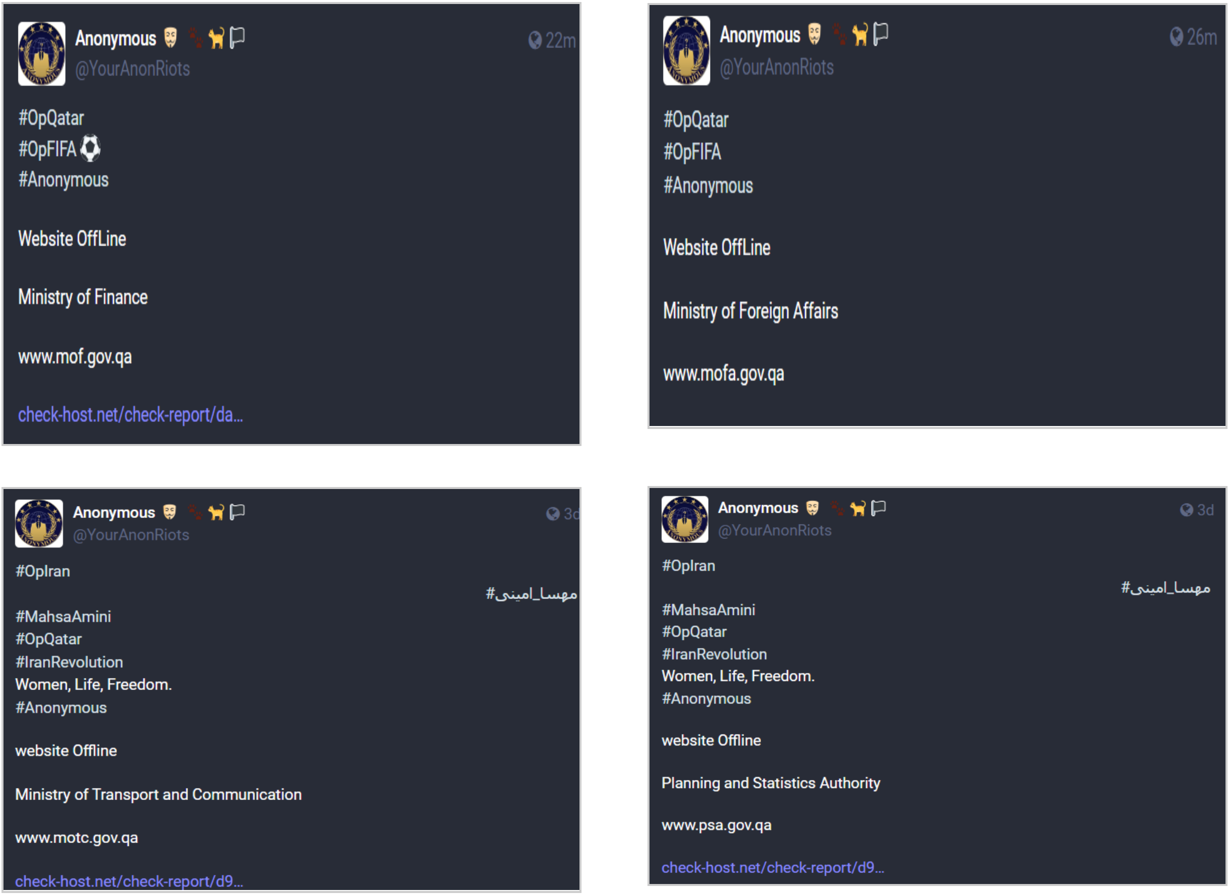
Women, Life, Freedom.
Target
ns1. fifa. com
ns2. fifa. com
ns3. fifa. com
ns4. fifa. com

Proof

check-host.net/check-report/d...

check-host.net/check-report/d...

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



Anonymous
@YourAnonRiots
22m

#OpQatar
#OpFIFA ⚽
#Anonymous

Website OffLine

Ministry of Finance

www.mof.gov.qa

check-host.net/check-report/da...

Anonymous
@YourAnonRiots
26m

#OpQatar
#OpFIFA
#Anonymous

Website OffLine

Ministry of Foreign Affairs

www.mofa.gov.qa

Anonymous
@YourAnonRiots
3c

#OpIran

#مهسا_امینی

#MahsaAmini
#OpQatar
#IranRevolution
Women, Life, Freedom.
#Anonymous

website Offline

Ministry of Transport and Communication

www.motc.gov.qa

check-host.net/check-report/d9...

Anonymous
@YourAnonRiots
3d

#OpIran

#مهسا_امینی

#MahsaAmini
#OpQatar
#IranRevolution
Women, Life, Freedom.
#Anonymous

website Offline

Planning and Statistics Authority

www.psa.gov.qa

check-host.net/check-report/d9...

Social media posts by hacktivist group Anonymous announcing DDoS on Qatar government websites

Websites Targeted by Hacktivists	
www.mofa.gov.qa	www.motc.gov.qa
www.qe.com.qa	www.moci.gov.qa
www.nas.gov.qa	www.sjc.gov.qa
www.psa.gov.qa	www.pp.gov.qa
www.qatargas.com.qa	www.mof.gov.qa
gco.gov.qa	

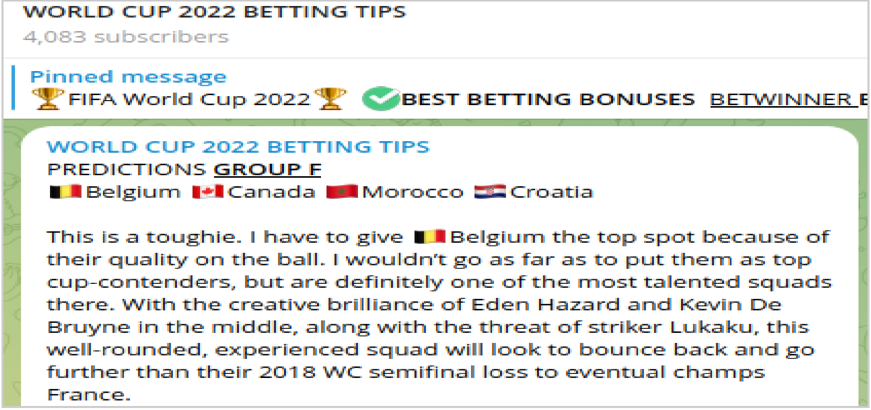
Betting and Gambling Services

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



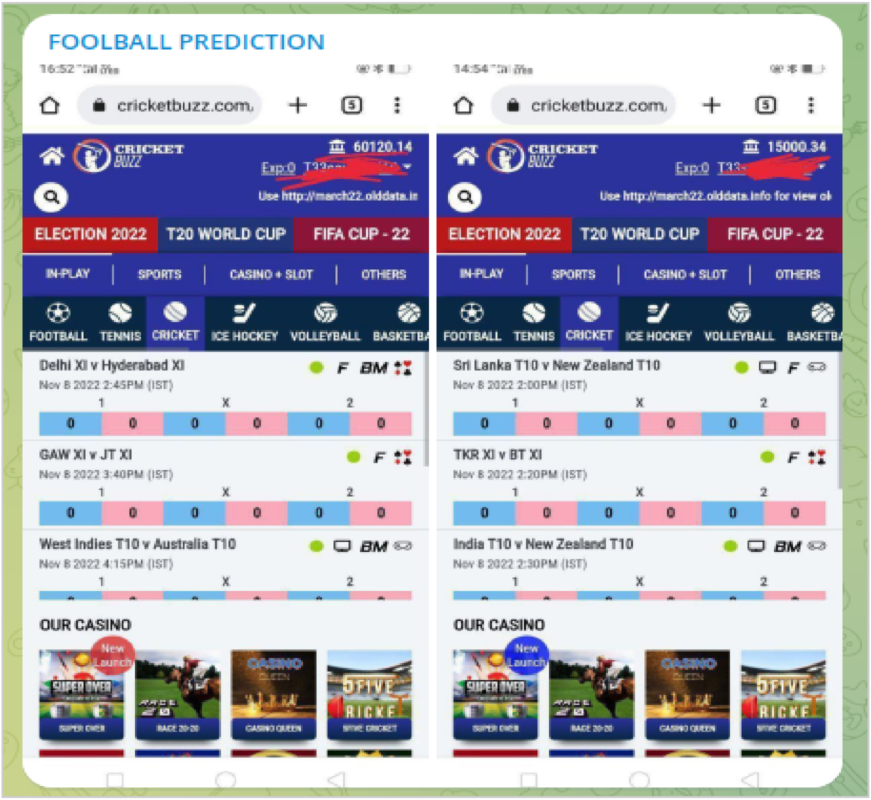
WORLD CUP 2022 BETTING TIPS
4,083 subscribers

Pinned message
🏆FIFA World Cup 2022🏆 ✅BEST BETTING BONUSES BETWINNER E

WORLD CUP 2022 BETTING TIPS
PREDICTIONS GROUP F
🇧🇪Belgium 🇨🇦Canada 🇲🇦Morocco 🇭🇷Croatia

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.

Telegram channel sharing betting tips



FOOLBALL PREDICTION

Telegram channel promoting gambling site

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.