CybelAngel

THREAT NOTE

FIFA World Cup Qatar 2022

Preliminary Assessment of the Cyber Threat Landscape for GCC Countries

TABLE OF CONTENTS

Date	25th November 2022
Version	1.0
Author	Mahdi Makke mahdi.makke@cybelangel.com
Classification	TLP:GREEN

On the eve of November 20, 2022 and for the first time in the Arab World, the FIFA World Cup tournament was launched in Qatar. For the hosting country, the organization of the 22nd edition of the world's most popular sports event had an important symbolic significance. This was reflected by the total costs spent on the planification of the tournament that exceeded $200 billion, making this edition of FIFA World Cup, the most expensive in history.

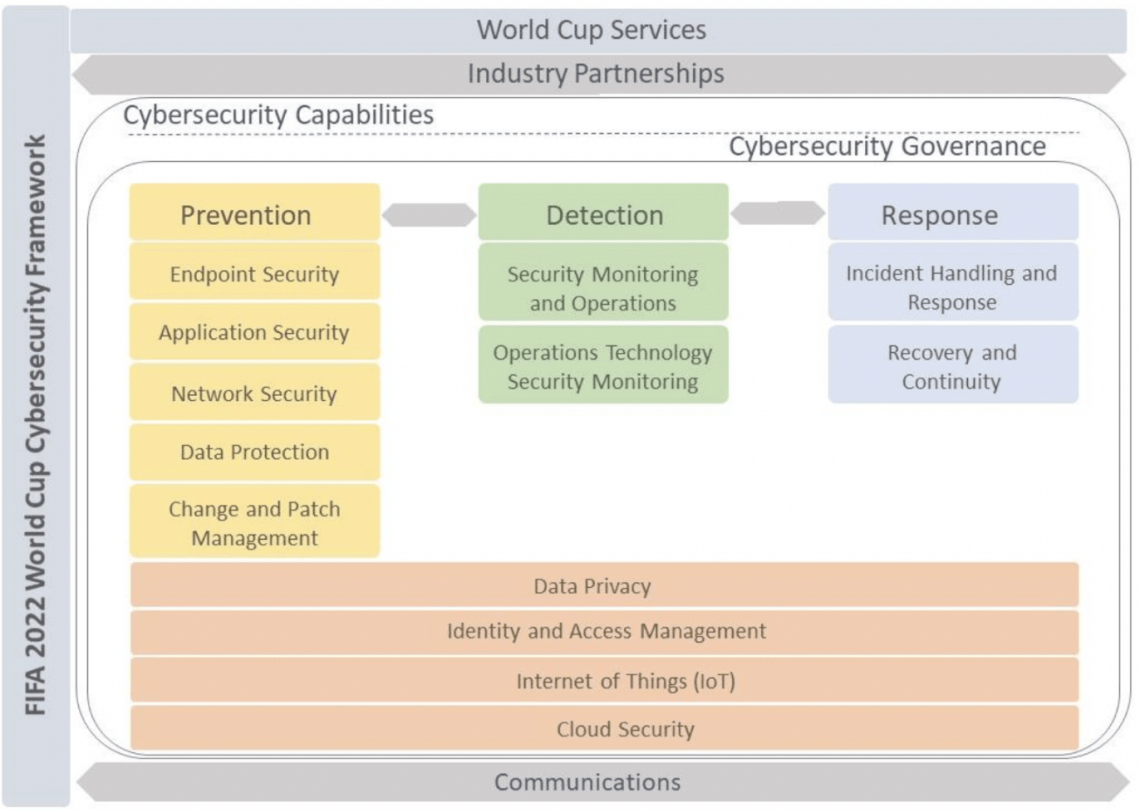
From November 20 to December 18, 2022, global eyes will be focused on this football competition that seems to interest not only the millions of fans and supporters but also multiple malicious actors. In fact, indicators from the past as well as recent developments have shown that this event will represent a breeding ground for cybercriminals. The aim of this report is to assess the cybersecurity threat landscape facing Qatar and the GCC[1] countries as a whole during the FIFA World Cup 2022.

I. Qatar's cybersecurity preparations ahead of the World Cup

Although the majority of Qatar's budget for the World Cup has been allocated to improve the country's infrastructure and logistics, the government has financed an extensive cybersecurity framework. Based on reports published by Tasmu Digital Valley[2], the Qatari government has invested over $1 billion on a plan that specifies a set of cybersecurity policies and procedures. The objective of this strategy is to prevent cyber incidents during the football competition whilst protecting national critical infrastructure supporting the tournament.

[1] The Cooperation Council for the Arab States of the Gulf or Gulf Cooperation Council comprising Saudi Arabia, the UAE, Qatar, Bahrain, Kuwait and Oman.

[2] An innovation cluster and digital ecosystem enhancer platform established by Qatar's Ministry of Communications and Information Technology (MCIT).



Cybersecurity Framework for the 2022 FIFA World Cup Qatar[3]

Compared to the overall costs, the dedicated budget for the cybersecurity ecosystem may seem light. Nonetheless, it highlights the Qatari's awareness of cyber-related risks and digital attacks that tend to become a common practice during popular events. This idea has been emphasized by Mohammad Al-Kayed, the director of cyber defense at Black Mountain[4] that declared: "*If there is anything we have learned about cybercrime from past encounters, it would be that it thrives around major global events*".

[3] Privacy Research Team (2022). *Understanding FIFA 2022 World Cup Cybersecurity Framework*. [online] Securiti AI. Available at: https://securiti.ai/blog/understanding-fifa-2022-world-cup-cybersecurity-framework/

[4] Cybersecurity firm based in the United Arab Emirates.

It is important to note that Qatar followed the footsteps of its GCC neighbors and spent years bolstering cybersecurity safeguards in preparation for the World Cup. Back in 2012 and with funding from Doha, the Interpol set up "*Project Stadia*" to develop effective action plans and implement adequate procedures allowing to properly address the security challenges posed by international sporting events. The aim of this program was to accompany the Qatari authorities in elaborating efficient cybersecurity countermeasures in order to provide a smooth-running and successful event. In March 2022, 8 months prior to the competition's kick-off, a group of global cybersecurity experts was gathered by Interpol in Doha to supervise the final security arrangements.

In addition to Interpol's contributions, several European countries have also partnered with Qatar to provide physical security for this football competition. For instance, the United Kingdom decided to grant counter-terror policing as well as marine security support through the Royal Navy, whereas France has offered to send warning and control systems to track airborne threats. The Italian government deployed a Counter-Unmanned Aerial Anti-Drone Task and stationed troops on Qatari soil; a decision similar to the one taken by Pakistan that also sent an army contingent to provide security. Moreover, it is worth mentioning that Turkey has decided to send 3,000 riot police personnel and Morocco dispatched a team of cyber security experts to Doha[5].

On the Qatari side, and in an attempt to tackle internet security issues, the government established between 2005 and 2006 the Qatar Computer Emergency Response Team (Q-CERT) under the auspices of the National Center for Information Security. In 2013, the National Cyber Security Committee was created to implement the directives of *Project Stadia* as part of the World Cup preparations. This entity was supported by the National Cybersecurity Agency that was founded in May 2021. The latter enhanced the country's cybersecurity capabilities by expanding its partnerships with global players such as Microsoft and Huawei. It also managed to train 25,000 employees in different aspects of information security to address all potential threats linked with the upcoming event.

[5] Mohamed, H. (2022). *How Qatar is planning to ensure security at World Cup 2022*. [online] AlJazeera. Available at: https://www.aljazeera.com/news/2022/10/26/qatar-inks-global-security-partnerships-to-ensure-safe-world-cup

II. Main threats facing the GCC: a diversified panoply of attack vectors

2.1 Security overview on the eve of the World Cup

Before assessing the direct and imminent risks related to the World Cup, Qatar or the GCC, it is necessary to point out that threat actors have kicked-off the event before its official inauguration. In the month leading up to the World Cup, security researchers noted that attackers have leveraged FIFA and football-based campaigns in an attempt to target Arab states. In fact, during the month of October, the volume of malicious emails and phishing attacks was observed to have doubled in the Middle East and North Africa[6].

Cybercriminals took advantage of the event organizers' busy schedule and tried to exploit the human error vector by launching large-scale phishing campaigns. Their objectives ranged from financial fraud to data exfiltration and credential harvesting. Besides mining for sensitive data, the aim of such attacks was also to cause reputational damage for Qatar and the GCC.

2.2 Current cybercriminal threats and challenges

As mentioned previously in this report, major global sporting events represent attractive targets for threat actors and more precisely the financially motivated cybercriminals that exploit two main types of lures during World Cups:

- Tournament-related components: illegal streaming services, fake betting platforms, fraudulent ticket giveaways
- Tournament-adjacent items: e-visa services, flight and hotel bookings as well as restaurant reservations

From a cybersecurity perspective, Qatar and the GCC are currently exposed to a whole spectrum of threats:

[6] Sjouwerman, S. (2022). *World Cup Phishing Attacks Doubled And Will Increase*. [online] KnowBe4. Available at: https://blog.knowbe4.com/world-cup-phishing-attacks-doubled-and-will-increase

Security Risk	Scenario(s)	Occurrence
Phishing Attacks*	Emails impersonating FIFA ticketing office to warn of payment issues	Already Occured
	Fraudulent notifications impersonating the Players Status Department. They contain legal notice regarding delayed legal fees or other administrative issues	Already Occured
	Fake free tickets allegedly offered by Snoonu, the official food delivery partner of the World Cup	Already Occured
Fraudulent URLs*	Customized pages confusingly similar to legitimate websites that ask for login details or banking information of victims	Already Occured
Malwares*	The use of fake mobile applications distributing malware and harvesting user data that is then sold on the Dark Web	Already Occured
	Deployment of banking Trojans, PowerShell backdoors and Remote Access Softwares	
Influence Operations	State-sponsored or hacktivist cyber operations targeting Qatar, GCC countries, sponsors or other associated entities for human rights concerns	Likely
DDOS	Disruptive attacks against websites linked to FIFA, Qatar or GCC states	Possible
Physical Attacks	Violent actions targeting stadiums, fan zones, governmental institutions or participating teams	Unlikely
	Suicide bombing, mass shooting or other forms of terrorism committed by politically/religiously motivated actors	

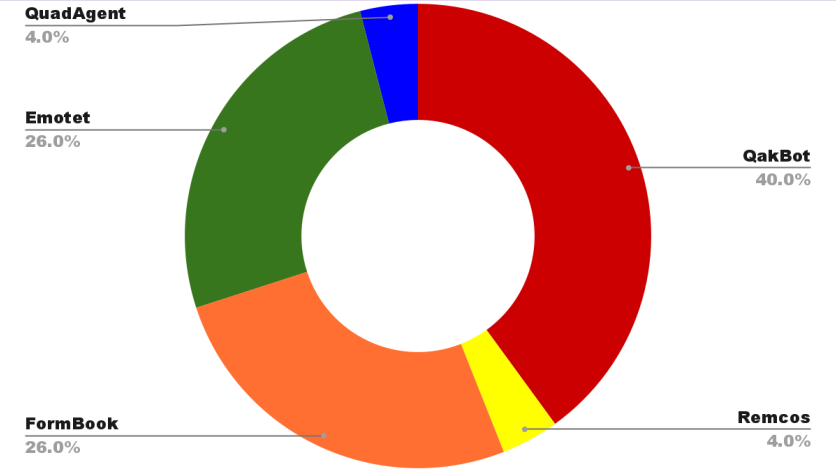
**The occurrence of these security risks has been reported and documented by Trellix*[7]

[7] Kapur, D. and Jain, S. (2022). *Email Cyberattacks on Arab Countries Rise in Lead to Global Football Tournament*. [online] Trellix. Available at: https://www.trellix.com/en-us/about/newsroom/stories/research/email-cyberattacks-on-arab-countries-rise.htm

2.3 Most prolific malwares targeting Qatar & Arab countries

American security company KnowBe4 listed 5 notorious malwares that are at the tip of the on-going cybercrime wave targeting Qatar and Arab Countries. These malwares are used for surveillance purposes and to steal personal and other sensitive data from compromised devices.

Name	Description	Examples of Files Harboring the Malwares
QakBot	Information stealer malware with backdoor capabilities	/
Emotet	Trojan that spreads via phishing email attachments and links	*Bank ABC Islamic Trade Murabaha template Feb 2019.docx*
FormBook	Malware allowing to steal credentials, screenshots and keystrokes	*Mirror UAE stock Cisco.xlsx* *NASDAQ Dividend Data UAE_v3.1.5_Sep2022.xlsb*
Remcos	Remote Access Software used to remotely control compromised devices	*DATE BAY Critical Dashboard with FDD week 42.xlsx*
QuadAgent	PowerShell backdoor that provides unauthorized access and control	/



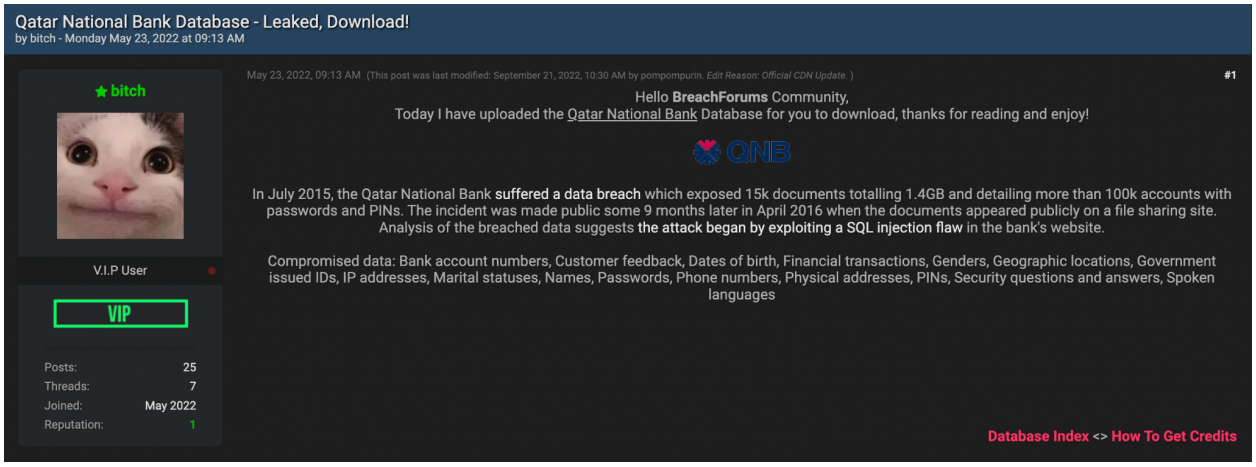
Percentage of attacks in Qatar and the Arab World attributed to the top 5 malware families[8]

[8] Glover, C. (2022). Qatar World Cup employees targeted by phishing cyberattacks. [online] Tech Monitor. Available at: https://techmonitor.ai/technology/cybersecurity/qatar-world-cup-cyberattacks-phishing

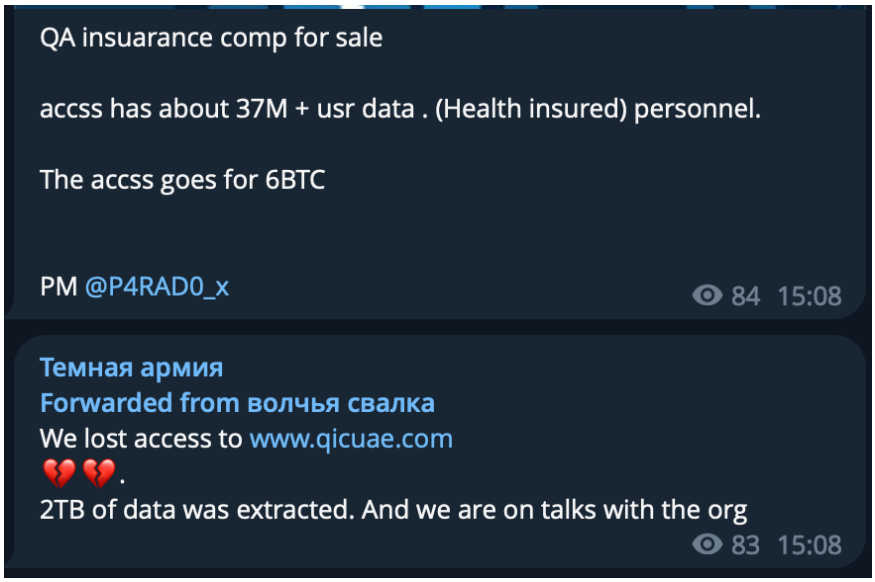
III. Malicious activities linked to Qatar and the GCC: CybelAngel's detections

Given the fact that social engineering attacks are at the core of malicious activities during the World Cup, CybelAngel decided to investigate dark web forums to search for all data that could potentially be used as part of phishing campaigns. The screenshots below taken by CybelAngel aim to provide examples of data that is likely to be used for malicious purposes.

The first sample displays a database that is being sold by a threat actor. It contains credentials (Emails and encrypted MD5 Passwords) of over 179,000 users based in the Arab World. The post was initially shared in April 2022 but it resurfaced by the end of September 2022, less than 2 months before the official kick-off of the World Cup tournament in Qatar.



The second example shows a threat actor sharing 1.4 GB worth of data consisting of old documents linked to Qatar National Bank. The latter suffered a data breach back in 2015 that left exposed personal identifiable information of the bank's customers. Although the leak is more than 7 years old, it has resurfaced on the eve of the 2022 World Cup.



The third case is an extract from a conversation between threat actors on a Telegram channel. A database belonging to UAE Qatar Insurance Company and allegedly containing 2 TB of personal data is put up for sale.

KEY TAKEAWAYS

- During the much-awaited international football tournament, cybercriminals and financially motivated threat actors are expected to leverage every opportunity in an attempt to collect PII from victims.
- Phishing Campaigns and Fraud Schemes represent the two main vectors of attacks which will certainly continue to be used throughout the FIFA World Cup tournament.
- Qatar and the GCC are currently targeted by 5 main malwares that spread through malicious URLs, binaries and email addresses.
- With foreign countries providing material security assistance to Qatar, it is unlikely that the host-country will face a major physical security threat during the World Cup. Nevertheless, influence operations aiming to cause reputational damage for the Qatari authorities due to human rights concerns may happen. This attack vector can be instrumentalized by state-actors, state-sponsored entities and more importantly, hacktivist groups.

THREATS ARE ALWAYS OUT THERE; THAT'S WHY CYBELANGEL IS HERE.

CONTACT US:
marketing@cybelangel.com

CYBELANGEL.COM

Are you exposed? Find out with a complimentary External Exposure Scan!

CLICK OR SCAN

CybelAngel