CYBER THREAT BRIEF:

Anomali Labs

The 2018 FIFA World Cup

Background

Russia will host the 2018 FIFA World Cup from 14 June to 15 July 2018 at 12 different venues throughout 11 host cities, and thousands of foreign visitors are expected to travel to the games. With major sporting events increasingly targeted by physical and cyber threats, we believe that FIFA and their affiliates, spectators, athletes, officials, or other attendees are likely to be confronted by a range of security risks such as protests/demonstrations, hooliganism, financial fraud, and to a lesser extent hacktivism, terrorism, and cyber espionage.

Physical Security Concerns

Terrorism
(Severity: High | Likelihood: Medium)

In advance of the 2018 FIFA World Cup, Islamic State (ISIS-ISIL) supporters have published multiple videos and posters on Telegram calling for terror attacks to take place at the event. These videos and posters represent an eight-month long violent propaganda campaign in which ISIS supporters such as Al-'Adiyat,[1] alTaqwa Media Foundation, and Wafa' Media Foundation[2] threaten to employ a variety of attack methods. Some of these methods include the beheadings of popular football players and team managers, bombings[3] within and near stadiums hosting the World Cup, and the urging of lone wolf-initiated[4] vehicular attacks, shootings, and stabbings. This rhetoric is consistent with ISIS supporters taking advantage of the global sporting events popularity to garner media attention for their cause[5]. The Russian government has released several public statements identifying terrorism as their number one security threat and concern leading up to the World Cup. ISIS is opposing Russian President Putin's support for Syrian President Bashar Al-Assad in his government's fight against ISIS. Several media reports have covered the increased security operations against suspected domestic terrorist cells such as the April 2018 raids of 16 locations by the Federal Security Services (FSB) to arrest members of the "Krasnoyarsk jamaat" group. Anomali Labs assesses with high confidence that ISIS and its supporters will almost certainly continue

1 https://www.memri.org/tv/pro-isis-video-threatens-attacks-world-cup-shows-russian-sochi-stadium-in-flames
2 https://ent.siteintelgroup.com/Chatter/is-supporters-amplify-threats-and-incitement-against-2018-fifa-world-cup.html
3 https://twitter.com/ToreRHamming/status/1006891446794932226/video/1
4 https://twitter.com/ToreRHamming/status/999637706937454594
5 https://eng-archive.aawsat.com/theaawsat/news-middle-east/isis-threatens-rio-olympics-2016

to release posters and videos inciting attacks on the 2018 World Cup; however, we assess with moderate confidence that these incitements combined with the increased Russian security measures will likely not result in a physical act of violence within close proximity to the matches.

Football Hooliganism (Severity: Low | Likelihood: High)

The FIFA 2018 World Cup in Russia will be exposed to a significant risk of violence from ongoing rivalries between opposing hooligan groups. A particular group of interest is the Russian ultra-nationalists or "Russian Ultras" who gained notoriety during the UEFA Euro 2016[6] championships in France for their rioting and clashes with English football supporters. Another concern reported by media outlets is racial and homophobic harassment[7] near the sporting event carried out by Russian Neo-Nazis and Russian Hooligans against domestic and foreign visitors during the matches. A third area of concern is the possibility of Russian Ultras seeking retribution against Polish supporters over the March 2018 destruction and removal of Red Army soldier[8] statues and memorials by the Polish government. However, Russian law enforcement agencies have a strong interest in protecting sporting venues, fan zones, and commercial and touristic areas from hooliganism to prevent tarnishing the overall success of the event. According to multiple press reports[9], the Russian Interior Ministry, the Federal Security Services (FSB), and local authorities have created and regularly updated a blacklist of 1,200 known or suspected Russian hooligans who are banned from attending events and conduct visits to influential individuals to warn them against violent outrages during the matches.

Protests / Boycotts (Severity: Low | Likelihood: High)

There are a number of issues from gay rights abuses to war crimes that have been highlighted by protesters ahead of the 2018 World Cup. Given the international media coverage on Russia and the matches, this provides aggrieved groups a stage for raising public awareness of the alleged offenses committed by

Figure 1. *Pro-ISIS media unit "al-Adiyat" shared a video on June 13, 2018 via Telegram displaying drone surveillance of Sochi Stadium in Russia where explosions are taking place*

Figure 2. *Pro-IS media group poster released on Telegram on May 15, 2018 instructing supported on how to target "infidels" inside and outside stadiums during the 2018 FIFA World Cup*

Russian President Putin and his administration. Some of these grievances focus on:

- **Political Prisoners.** Ukrainian film director and Russian political prisoner, Oleg Sentsov, is currently the focus of campaigns directed at the global football community. There are several appeals to release him, and a global rally was planned on June 1st and June 2nd to support and raise awareness of Ukranian political prisoners.

6 https://www.theguardian.com/football/2016/jun/11/euro-2016-french-police-tactics-raise-fears-of-more-clashes-with-england-fans
7 https://www.mirror.co.uk/sport/football/news/russian-football-hooligans-warn-gay-12609624
8 https://www.express.co.uk/news/world/974205/world-cup-2018-russia-ultras-hooligans-poland-violenc
9 https://www.aljazeera.com/indepth/features/russian-football-hooligans-face-crackdown-world-cup-180410083901797.html

Information can be found under hashtag #FreeSentsov.

- **Discrimination.** "Boycott the 2018 World Cup" is a Twitter account under the handle @CupBoycott, which provides the following reasons for boycotting: Racism in Russian football, discrimination of LGBT people, corruption of Putin and FIFA, ongoing Ukraine crisis, doping in Russia, MH17 and the Skripal poisoning. The account appears to be similar to @18BoycottRussia which was set up a lot earlier to try to prevent Russia from hosting the event.
- **Syrian Conflict.** The Human Rights Watch (HRW) called on world leaders to boycott the opening ceremony of the World Cup soccer competition in Russia unless Russian President Vladimir Putin takes steps to protect Syrian civilians.
- **Animal Welfare.** A petition to prevent the killing of stray animals ahead of the World Cup.

There was a protest held in Kiev on June 14th[10], it remains to be seen whether any further action will take place during the event.

Cyber Threat Landscape

Nation-State Actors (Severity: High| Likelihood: Medium)

A large body of security vendor reporting has previously described nation-state actors leveraging major sporting events as a means for intelligence collection using event-themed subject lines and lure documents for spear-phishing email campaigns. The primary targets have been adversarial governments and militaries, international sporting organizations, and event affiliates such as partners, sponsors, and supporters. Anomali Labs does not have current intelligence on planned or active operations by nation-state actors; however, as they have done this in the past, there is a medium likelihood they will do so again.

Cybercrime (Severity: Medium | Likelihood: High)

The 2018 World Cup provides cybercriminals with a massive audience primed for social engineering attacks such as phishing and SMS-ishing. The World Cup offers plentiful opportunities for luring unsuspecting fans into installing malware onto their devices, disclosing sensitive information (e.g. user credentials, payment card data), or falling victim to a number of other nefarious scams. Historically, international sporting events served as a means for cybercriminals to deceive users with World Cup-, ticketing-, prize giveaways-, promotional ad-themed phishing emails, malware-infected faux event "live streaming" websites, and World Cup-themed rogue and malicious mobile applications. Recently, Kaspersky Labs[11] and ESET Security[12] detected a spike in the number of phishing pages in May and June 2018 appearing during match ticket sales as well as Football- and World Cup-themed spam emails mimicking official FIFA pages and sites allegedly from partner companies. In February 2018, several vendor and researcher blogs detailed an Adidas-themed WhatsApp scam[13] where users received messages offering them 2,500 pairs of shoes in celebration of Adidas' 93rd anniversary. Interestingly enough, scammers repeated this tactic to conduct a similar Adidas-themed WhatsApp scam in June 2018[14]; however, this incident involved an IDN homograph[15] attack by sending an image with an embedded link to scam site "www[.]adıdas[.]de/no.html" that substitutes the letter "i" in Adidas with a short vertical line.

Additional cybercriminal tactics involve exploiting vulnerable infrastructure near World Cup hosted venues and tourist locations such as hotels, restaurants, and shopping centers. According to Kaspersky Lab research[16], 7,176 of approximately 32,000 public Wi-Fi networks in FIFA World Cup 2018 host cities do not use traffic encryption. During the 2014 Brazil World Cup and 2016 Rio Olympics, security researchers discovered multiple fake wireless networks distributed

10 https://www.rferl.org/a/ukraine-russia-fifa-sentsov/29290688.html
11 https://securelist.com/2018-fraud-world-cup/85878/
12 https://www.welivesecurity.com/2018/06/06/fake-fifa-world-cup-themed-lotteries-giveaways/
13 https://www.express.co.uk/life-style/science-technology/917335/WhatsApp-scam-warning-fake-message-Adidas
14 https://www.welivesecurity.com/2018/06/14/phishing-anniversary-free-50-month-subscription/
15 https://capec.mitre.org/data/definitions/632.html
16 https://www.kaspersky.com/about/press-releases/2018_wi-fi-hot-spots-in-world-cup-cities-have-cybersecurity-issues

throughout the city, many presumably setup to compromise users. Hence, we believe that cybercriminals will exploit these potential weaknesses and employ tactics such as establishing rogue Internet access points or hotspots and compromising hotel and public WiFi networks in order to steal personally identifiable information (PII) and financial data. We also believe that cybercriminals will employ tried-and-true tactics such as ATM skimmers and compromising Point-of-Sale (PoS) systems to commit financial fraud.

Hacktivism (Severity: Medium | Likelihood: Medium)

Fancy Bear

The Russian state-affiliated hacktivist group known as "Fancy Bear" has been actively targeting sporting bodies and anti-doping organizations as retaliation for the banning of Russian athletes during the 2018 Pyeong-Chang Winter Olympics following the state-sponsored doping scandal leading up to and including the Sochi 2014 Winter Olympics[17]. In August 2017[18], Fancy Bear released documents from the World Anti-Doping Agency (Wada) that revealed 150 players were caught doping in 2015 for substances such as cocaine, methamphetamine and amphetamine and 25 players were given exemptions by FIFA to take banned medicines during the 2010 World Cup. In the latest case[19], Fancy Bear continued their public disclosure campaign releasing documents in May 2018 allegedly obtained from the Swedish Sports Conference claiming that the vast majority of Swedish top athletes suffer from asthma and used terbutaline to treat it, which effectively treats the respiratory disease by expanding lung capacity and increasing fatigue resistance, giving them an essential advantage to athletes competing in high endurance events like cross-country skiing and the biathlon in 2018 Winter Olympics. We strongly believe that the purpose behind the public leaks of confidential files and email correspondence is an attempt by the Russian Government via their faux persona to deflect attention from the scandal relating to Russian athletes' use of banned substances and an attempt to discredit and tarnish the image of Olympic regulatory

Figure 3. *Tweet by Fancy Bear on August 22, 2017 announcing the disclosure of Wada and FIFA related doping incidents*

bodies and Western nations due to their alleged corrupt and hypocritical practices. Although there is no current reporting on Fancy Bear's intention to target FIFA and their affiliates or the World Cup participants with public leaks, Anomali Labs suspects the possible leakage of confidential files would be a measure employed during the matches to deflect any negative sentiment toward the Russian Government or the Russian national football team.

Anonymous Collective

Unlike the previous 2014 Brazil World Cup, there is a noticeable decline in hacktivists targeting the 2018 Russia World Cup[20]. We have yet to witness Anonymous Collective launch distributed denial of service (DDoS) attacks, website defacements, and doxing attacks against World Cup entities like they did in 2014. We are aware of at least one ongoing hacktivist operation, #OpRussia,[21] that is mainly focused on targeting the Russian Government and Telecommunications providers to denounce the enactment of the November 2017 Russian law[22] regulating the use

17 https://www.nytimes.com/2016/05/13/sports/russia-doping-sochi-olympics-2014.html
18 https://twitter.com/FancyBears/status/899936881659453440
19 https://www.fancybear.net/pages/saga-about-doping.html
20
21
22

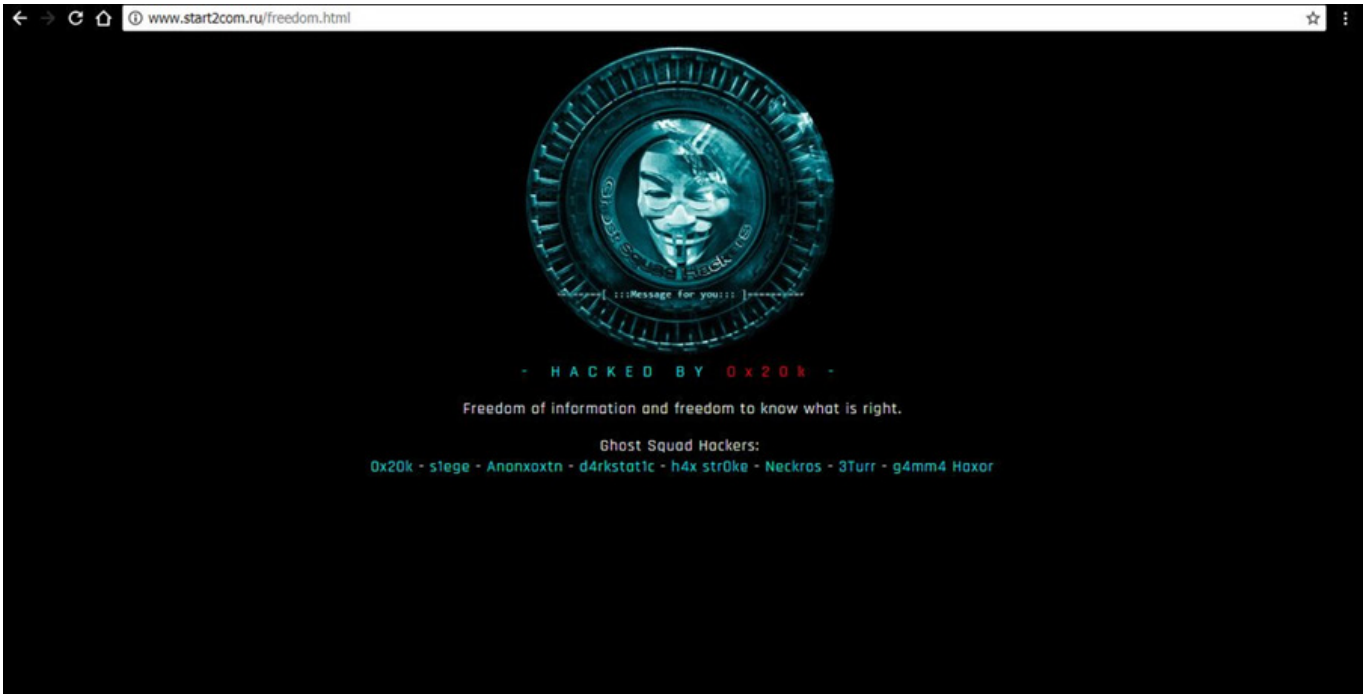

Figure 4. *Website defacement of Russian Telecom Company by GhostSquadHackers, an Anonymous Group affiliate*

of technologies enabling users to search the Internet anonymously such as virtual private networks (VPNs) and proxy servers (anonymizers). To date, we have not observed any credible reporting of hacktivists targeting FIFA, the World Cup, or its affiliates; however, with the global attention on the World Cup, we believe a strong potential remains, albeit unsophisticated and non-persistent, of hacktivists being provoked into action by an unrelated geopolitical, economic, or social issue.

Targets

Aside from the potential targeting of FIFA, the stadiums/venues, and carriers or service providers within the general vicinity of the football matches, we assess with high confidence that FIFA partners, sponsors, and supporters will be targeted by malicious actors seeking to abuse their brands to commit financial fraud or to disrupt online business such as the purchasing of ticketing sales, retail merchandise, and online banking. The following contains a list of known FIFA-affiliated entities obtained from the FIFA 2018 Russia World Cup website:[23]

Figure 5. *2018 World Cup Partners, Sponsors, and Regional Supporters*

FIFA Partners

- Adidas
- Coca-Cola
- Gazprom
- Hyundai-Kia
- Qatar Airways
- VISA
- Wanda Group

FIFA World Cup Sponsors

- Anheuser-Busch InBev
- Husense
- McDonald's
- Mengniu Dairy
- ViVo

23 https://www.fifa.com/worldcup/organisation/partners/

National and Regional Supporters

- Alfa-Bank
- Alrosa
- DIKING
- Experience & Invest
- LUCI
- Rostelecom
- Russian Railways
- Yadea

Conclusion

Overall, Anomali Labs believes that the 2018 World Cup will continue to inspire an increase in physical and cyber activity with an emphasis on hooliganism, terrorist threats, and financial fraud; however, we are unaware of any indications of a high-level physical or cyber event targeting the World Cup as witnessed in the 2018 Winter Olympics with the deployment of destructive malware or the UEFA 2016 riots. We assess with high confidence that jihadists and their supporters will likely continue to release propaganda attempting to incite physical violence at the World Cup. We assess with high confidence that isolated incidents of hooliganism and petty crime will occur but will have a limited impact on the overall matches. We judge with near certainty that cybercriminals will target individuals and organizations affiliated with the World Cup using scam related communications similar to recent phishing activity abusing the Adidas brand name and historical actions employed by financially-motivated actors, previously observed in global sporting events to include the World Cup and Olympics.