THREAT ANALYSIS

Recorded Future®

By Insikt Group®

January 26, 2022

Threats to the 2022 Winter Olympics

Recorded Future®

This report synthesizes findings from the Recorded Future® Platform and open-source intelligence (OSINT) sources to analyze the threat landscape ahead of the 2022 Beijing Winter Olympic Games. The threats analyzed include nation-state cyber operations, financially motivated and hacktivist cyber threats, influence operations, and geopolitical and physical security threats. This report will be of most interest to organizations affiliated with the Olympics organization, Olympic sponsors, or individuals intending to participate in or engage with the upcoming Winter Olympics.

Executive Summary

The hosting of the 2022 Winter Olympic Games in Beijing, China, significantly alters the cyber, information, geopolitical, and physical threats that face the Games. This report analyzes a whole spectrum of threats facing the 2022 Winter Olympics, including state-sponsored cyber operations, financially motivated and hacktivist cyber activity, Chinese state-sponsored influence operations, international geopolitical tensions, and physical security threats including protests.

Recorded Future concludes that Russia, Iran, and North Korea likely lack the motivation to launch disruptive cyberattacks against the 2022 Winter Olympics due to their close geopolitical relationships with China. Instead, Chinese, Russian, Iranian, and North Korean state-sponsored cyber operations are more likely to be conducted according to surveillance and cyber espionage intelligence requirements. We did not observe any notable dark web chatter or statements by ransomware groups expressing intent to target the 2022 Winter Olympics, though we did identify advertisements on dark web markets for the sale of account details related to the volunteer and media portals of the Games. Financially motivated threat actors will almost certainly opportunistically exploit the 2022 Beijing Winter Olympics, particularly with Olympic-themed phishing campaigns, to target a range of victims, including the Games themselves, associated organizations, and individuals attending or engaging with the event. Further, hacktivists will likely target the Games, including corporate sponsors, in response to China's human rights abuses. Corporate sponsors are already receiving significant online criticism for being associated with the Games being hosted in Beijing.

Hosting the 2022 Winter Olympics is an opportunity for the Chinese government to broadcast the successes of China's political and economic system. Accordingly, China's influence operations to promote and support the Beijing Games are mainly positive and target both domestic and international audiences. These influence efforts are paired with a much more negative campaign to defend against criticism of China's human rights abuses. The Chinese government is already conducting widespread domestic censorship of this criticism and is seeking to downplay and discredit the international diplomatic boycott effort. There have also been grassroots calls for physical protests at the Games, primarily in response to China's human rights abuses. The most recent news, however, indicates that the public will no longer be able to attend the Games due to strict COVID-19 measures. Protests taking place in the weeks leading up to the Games will likely intensify as the Games begin.

Key Judgments

- Recorded Future is not aware of any state-sponsored APT activity targeting the 2022 Winter Olympics, associated organizations, or individuals. Similarly, we have not observed any expressed intent to target the Games by ransomware groups or actors on dark web forums, although the potential for a significant profit makes the Games an attractive target for ransomware groups.
- Disruptive Russian, Iranian, and North Korean state-sponsored cyberattacks targeting the 2022 Winter Olympics are unlikely to manifest due to the close relationships those countries maintain with the host nation, China. Instead, Chinese, Russian, Iranian, and North Korean state-sponsored cyber operations at the 2022 Winter Olympics are likely to be driven by surveillance and cyber espionage intelligence requirements.
- It is almost certain that financially motivated threat actors will opportunistically exploit the 2022 Winter Olympics, particularly with Olympic-themed phishing campaigns. We have already observed an Olympic-themed malware sample. Furthermore, hacktivists will likely target the Games, including corporate sponsors, in protest against the Chinese government's human rights abuses.

- The Chinese government has engaged its entire propaganda system in a long-term, coordinated influence campaign to promote the 2022 Winter Olympics and defend against domestic and international criticism while also conducting widespread censorship of such criticism.
- The 2022 Winter Olympics is being used to promote the digital yuan (e-CNY) by making it possible for foreign visitors to use the e-CNY at Olympic venues in Beijing without having a Chinese bank account, likely to build international credibility of China's central bank digital currency as part of a larger effort to boost the international standing of the yuan.
- The Chinese government has sought to downplay and discredit international efforts to boycott the 2022 Winter Olympics to mitigate the reputational effect the boycott poses. There have been grassroots calls for physical protests at the Games, and protests will likely intensify, with calls for protests both in China and worldwide as the Games get underway.

State-Sponsored Cyber Operations

The second Olympic Games of the COVID-19 pandemic era, the 2022 Winter Olympic Games hosted in Beijing, will look similar to the recently concluded 2020 Tokyo Olympic Games, with many restrictions placed on attendees. While the Olympic Games are typically a target-rich environment, with visitors and delegations from all over the world attending, the measures introduced this year to control the spread of COVID-19 include bans on foreign spectators, regular testing requirements for participants, and strict quarantines. These measures, combined with Beijing's hosting of the event, affect the potential for state-sponsored threat activity targeting the Olympic Games itself, associated organizations, and individuals at the event.

In this section, we assess the threats posed by Chinese, Russian, North Korean, and Iranian state-sponsored advanced persistent threat (APT) groups to the 2022 Winter Olympics. As of this writing, Recorded Future is not aware of any APT-nexus activity targeting the 2022 Winter Olympics, associated organizations, or participating individuals, and Insikt Group believes that disruptive state-sponsored cyberattacks against the Games are unlikely to manifest. However, numerous governments, including the host country of China, as well as Russia, North Korea, and Iran, likely all maintain some level of interest in cyber espionage activities surrounding the event.

China — APT Groups and Activity

As the host nation for the 2022 Winter Olympics, the People's Republic of China (PRC; China) has a significant interest in ensuring that the event unfolds smoothly. For this reason, Chinese state-sponsored APT groups are highly unlikely to engage in cyber espionage or disruptive operations against the Olympics themselves, the International Olympic Committee (IOC), or associated entities. Moreover, 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. 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 Winter Olympics.

Nevertheless, China's powerful and well-resourced security services are highly likely to conduct widespread surveillance and cyber espionage against foreign athletes and dignitaries attending the event, with the goal of preventing disruption of the event or for traditional national security-focused goals. This is in the context of the Chinese government's overriding interest in domestic stability, adversarial relations with numerous foreign governments, and the government's sensitivity to numerous controversial issues for which it is frequently criticized internationally, namely human rights abuses and political freedoms in Xinjiang, Tibet, and Hong Kong, as well as the South Chinese Sea disputes and treatment of Taiwan.

Individuals or affiliates of governments, companies, or other organizations that have publicly criticized the Chinese government on "politically sensitive issues" (including but not limited to those previously mentioned) are at enhanced risk for both digital and physical surveillance and monitoring while in the country, including in both public and private spaces, such as hotel rooms and while using public networks. Given the seriousness with which the Chinese government approaches these issues, it is almost certain that such organizations or individuals are being monitored in the run-up to the event and will continue to be so throughout and even after the conclusion of the Olympic Games.

This surveillance is very likely to extend to personal mobile devices equipped with special SIM cards offered to foreign athletes that allow circumvention of the Great Firewall while on Chinese telecommunications networks, and the MY2022 Olympic Games app that is required to be installed by all attendees, including members of the press and competing athletes. The MY2022 app collects a range of personally identifiable information, including users' demographic, passport, and COVID-19 health information. Citizen Lab identified that the app has 2 security vulnerabilities

related to the transmission of user data that have not been fixed at the time of this writing and could be exploited by threat actors to steal the aforementioned sensitive information. The Chinese government will almost certainly be able to access data held on the app without needing to exploit these vulnerabilities given that the app is used by foreign visitors to submit required information to the government and is owned by the state-owned company Beijing Financial Holdings Group; therefore, the vulnerabilities are more relevant for criminal threat actors.

Due to surveillance concerns, the Olympic Committees of multiple countries, including the US, the Netherlands, Canada, the UK, and Australia, have advised their athletes to leave personal phones, laptops, and other electronic devices at home and take precautions such as only using burner devices, wiping them of data before arrival and upon departure to Beijing, and to use a virtual private network (VPN) at all times. Similarly, a report by Internet 2.0 warns that an official sponsor of the Games, Chinese cybersecurity firm QI-ANXIN, offers VPN software that harvests a range of data from user devices that could be used to identify users. The report therefore also recommends using a burner device when at the Games. However, we believe it is unlikely that all athletes advised to leave their personal devices at home will do so and that a risk to their data will remain, given that burner phones with good cameras and other features are expensive; athletes will undoubtedly want to post on social media throughout the Games to advertise and attract sponsorship and boost their social media following.

Russia — APT Groups and Activity

Although Russian state-sponsored APT groups have a history of conducting both espionage and disruptive attacks against the Olympic Games and Russia remains banned from formal participation in the Games, the International Olympic Committee (IOC), and associated bodies, we assess that Russia likely lacks the requisite motivation to conduct disruptive operations against the 2022 Winter Olympics. However, cyber espionage campaigns targeting Olympics-associated entities and athletes representing countries with adversarial relationships with Moscow remain likely.

While not formal allies, Beijing and Moscow currently enjoy their closest relationship in decades, as both maintain interests in undermining the existing Western-led international order. While some mistrust in the relationship lingers, the two countries have gone to considerable lengths in recent years to build confidence, holding joint military drills, strengthening economic integration, and cooperating on issues of mutual concern. China's President Xi Jinping has described Russian President Vladimir Putin as his "best friend", and Putin has announced his intention to attend the Games — the first world leader to make such an announcement following the imposition of a US-led diplomatic boycott. As a result, Moscow is highly unlikely to consider its disruption of the Beijing-hosted event as advantageous to its interests.

Russia's lack of motivation to disrupt the event itself, however, does not preclude it from seeking to embarrass or otherwise tarnish the reputation of the IOC, associated bodies, or athletic delegations from adversarial countries due to its continued ban from formal participation under its national flag due to the 2014 Sochi Winter Olympics doping scandal. During previous Olympic Games, Russia conducted both cyber espionage hack-and-leak operations and information operations targeting such organizations or individuals in protest of its ban from participation, which Moscow considers unjust and politically motivated.

Past Russian state-sponsored activity directed against the Olympics or associated entities include:

- 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 during the 2016 Rio de Janeiro Summer Olympics
- GRU operators targeting wireless networks (WiFi) 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

Iran — APT Groups and Activity

Iranian APTs have not been previously identified launching destructive cyberattacks or cyber espionage intrusions against the Olympics or organizations associated with sporting federations. Tehran likely lacks the grievances of states such as Russia and North Korea — both barred from formal participation — against the IOC, which might otherwise induce it to conduct cyber operations against the event. As of this writing, Iran is not banned from the event and enjoys unprecedentedly close relations with China, which would likely be put at risk by such operations.

This does not, however, preclude Iranian APTs from leading espionage intrusion attempts against organizations supporting the Olympics or people attending them. Iranian domestic politics

have been rife with politically motivated sporting controversies, including the boycotting of the Olympic Games and sporting competitions involving athletes from Israel, as well as those involving female athletes and supporters. Iran has already denounced the US-led diplomatic boycott of the 2022 Winter Olympics.

At least 2 known Iran-nexus threat actors, APT35 (Charming Kitten and Phosphorus) and APT39 (Rana Intelligence Computing Company and Chafer), are reported to maintain intelligence and counterintelligence requirements that could lead them to launch attacks against organizations and individuals attending the 2022 Winter Olympics.

APT35 has been reported to seek strategic and tactical information and has also undertaken counterintelligence operations at the behest of the Islamic Revolutionary Guard Corps (IRGC). APT39 has also been reported to focus on counterintelligence and long-term espionage activity with the goals of protecting the regime. APT39 would most likely be responsible for penetrating anti-Iranian government networks that may attempt to use the 2022 Olympic Games as an opportunity to engage with Iranian athletes, their teams, and government representatives. As such, facilities hosting Iranian athletes are at increased risk of targeting. APT39 has previously been linked to counterintelligence and surveillance operations, as well as targeted intrusions against government networks, travel, and the telecommunications sectors at the behest of the Ministry of Intelligence and Security (MOIS). This threat actor group, and those conducting similar operations, is likely tasked with tracking Iranian athletes and diaspora community members, activists, and Iranian dissidents.

North Korea — APT Groups and Activity

While North Korea maintains sophisticated capabilities for cyber operations and disruption, Pyongyang also likely lacks an incentive to target the 2022 Winter Olympics with disruptive attacks due to the risk of jeopardizing its relationship with China, on which Pyongyang largely relies for economic stability and security guarantees. North Korea recently announced that it would not be attending the 2022 Winter Olympics but "give[s] full support" to China.

There is limited historical precedent for North Korean APT groups targeting major international sporting events of organizations. The only precedent is that in February 2018, McAfee detected fileless malware, dubbed Gold Dragon, which was used to target Olympics-related organizations. This malware was subsequently attributed to APT37 based on code overlap with other known North Korea-nexus malware. However, the IOC in September 2021 suspended the country from participation in the 2022 Winter Olympics after it declined to participate in the delayed 2020 Tokyo Olympics due to concerns over COVID-19, citing a violation of the IOC charter. Similar to how Russia's ban from participation in international sport has motivated state-sponsored attacks on Olympics-associated entities and individuals, Pyongyang's ban may drive similar behavior from North Korea-nexus APT groups in protest of their ban. This activity, though, is unlikely to be disruptive to the event itself and may take similar forms to Russian-backed operations, such as hack-and-leak or information operations.

Financially Motivated and Hacktivist Cyber Activity

Dark Web Activity

Dark Web Chatter

Recorded Future did not observe any evidence of direct threats, planned attacks, or cyber operations targeting the 2022 Beijing Winter Olympics among dark web sources and underground forums. Nevertheless, we believe it is almost certain that financially motivated threat actors will opportunistically exploit the 2022 Beijing Winter Olympics.

Historically, high volumes of financially motivated cyberattacks have targeted previous Olympic Games, including the 2020 Tokyo Olympics. NTT Corporation recorded 450 million security events "that were blocked during the [2020 Tokyo Olympic] Games including unauthorized communications to the official website". NTT Corporation's Andrea MacLean stated that this was two-and-a-half times the number of attacks that targeted the 2012 London Olympics. McLean further said that "cybercriminals certainly saw the [2020 Tokyo Olympic] Games — and its related supply chain — as a high-value target with low downtime tolerance" and attacks included "emotet malware", "email spoofing and phishing", "fake websites made to appear as ones associated with the tournament and/or related organizations", and "user authentication errors, such as password spraying attacks".

We identified multiple references in Russian and Chinese on dark web forums regarding a data breach that affected the 2020 Tokyo Olympics, with the references seemingly quoting news articles on the data breach such as Computer Weekly. An anonymous Japanese government official told Kyodo News on July 21, 2021, that the login credentials of ticket purchasers and those that used the volunteer portal had been leaked online. The official stated that the leakage "was not large" and "were likely stolen by unauthorized access to computers or smartphones,

and they were posted on a website that exposes personal information". Indeed, evidence from dark web markets (discussed below) suggests that this risk is likely to affect the 2022 Winter Olympics. Furthermore, threat actors could exploit vulnerabilities in the MY2022 Olympics app to obtain sensitive information, including COVID-19 health and passport information, on those attending the Games, thereby offering another avenue for a potential leak of Olympics-related data.

Dark Web Markets

Recorded Future identified 131 references to the primary 2022 Beijing Winter Olympics domain, beijing2022[.]cn, and its subdomains on dark web sources, specifically the dark web markets Russian Market, Genesis Store, Amigos Market, and 2easy Shop. 125 of these references were to the subdomain vol[.]beijing2022[.]cn, the volunteer application portal used to recruit volunteers for the 2022 Beijing Winter Olympics. As such, it is almost certain that the vast majority of references to vol[.]beijing2022[.]cn on dark web markets relates to the sale of information belonging to individuals that applied to be volunteers at the 2022 Beijing Winter Olympics, similar of the data breach affecting the 2020 Tokyo Olympic Games discussed above.

Russian Market: We identified 93 references to subdomains of beijing2022[.]cn on Russian Market, with no references to the parent domain itself. 89 of these references were to the subdomain vol[.]beijing2022[.]cn, while the other 4 references were to the subdomain media[.]beijing2022[.]cn, which is the "Media Extranet" for the 2022 Beijing Winter Olympics only available to members of the media. 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 business email compromise (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: We identified 2 references to vol[.]beijing2022[.]cn on Genesis Store, with no other references to the parent domain beijing2022[.]cn or additional subdomains. 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.

Amigos Market: We identified 23 references to subdomains of beijing2022[.]cn on Amigos Market, with no references to the parent domain itself. 1 reference was to media[.]beijing2022[.]cn, while the other 22 references were to vol[.]beijing2022[.]cn. Amigos Market is a low-tier shop that sells various compromised data, including RDP and SSH access, and compromised user logs and accounts.

2easy Shop: We identified 12 references to vol[.]beijing2022[.]cn on 2easy Shop, with no other references to the parent domain beijing2022[.]cn or additional subdomains. 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.

Threat actors who purchase credentials or "bots" related to the 2022 Winter Olympics domains mentioned above could abuse them to gain access to information and material only available to the media or volunteers and to the personal information of volunteers.

Ransomware

While we have not seen any specific threats made by any of the ransomware groups to the 2022 Winter Olympics, the potential for a significant profit makes the Games an attractive target for exploitation. A financially motivated threat actor would likely target organizations that support the Olympic Games' supply chain, transportation, media, healthcare, logistics, and security apparatus. Since many of these aspects of the Olympic Games are separate from one another, an attack on one component would be unlikely to disrupt the Games significantly.

For cybercriminals, the lure to attack the 2022 Winter Olympics and associated organizations could be measured by what we saw from high-profile ransomware attacks in 2021. Last year, ransomware gained mainstream media attention for targeting critical infrastructure, which has been the case in the attacks against Colonial Pipeline, JBS, and more recently with several agricultural organizations. However, it is rare for ransomware groups to conduct a large-scale, coordinated

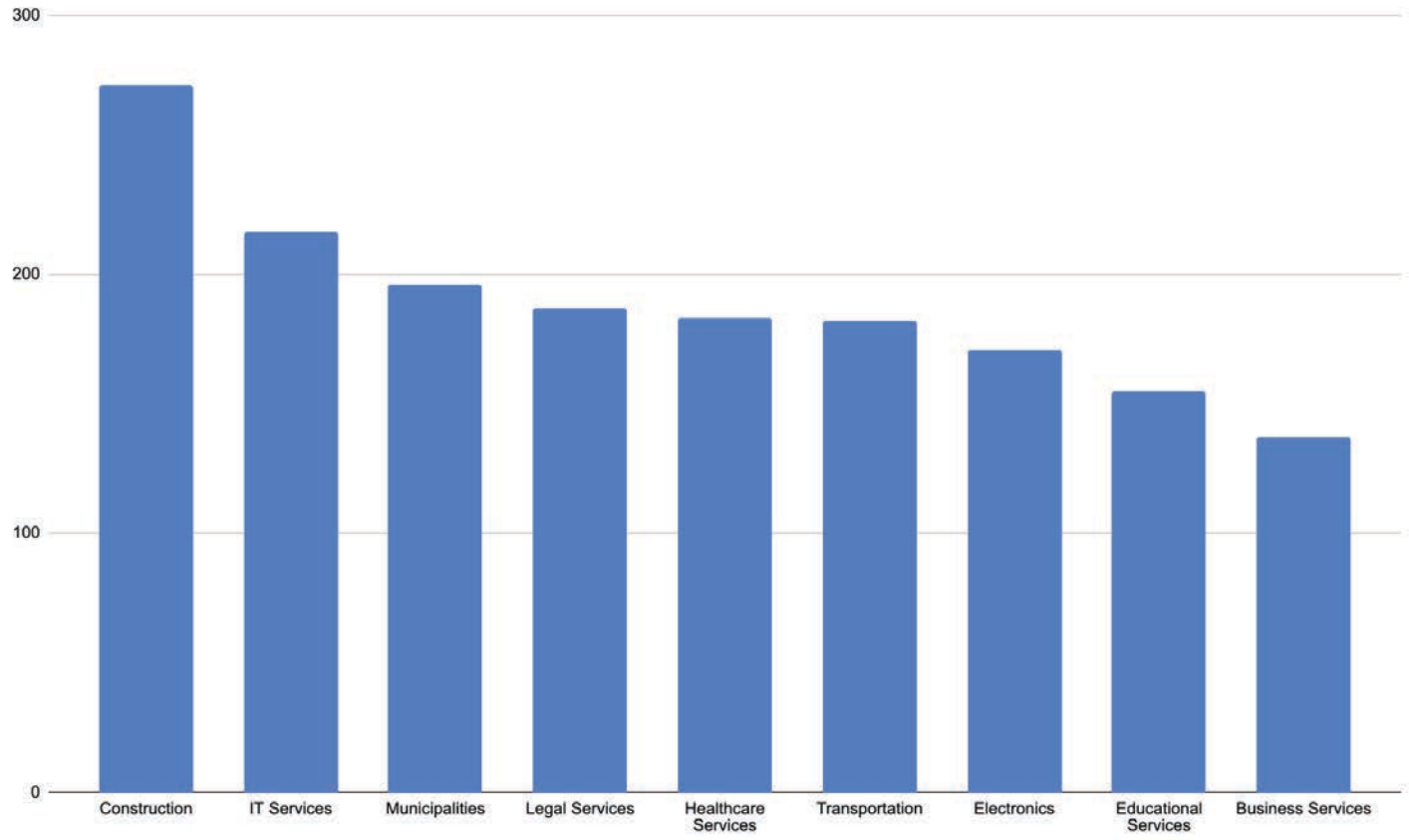

Figure 1: Ransomware victimology showing the top 9 targeted industries in 2021 (Source: Recorded Future)

attack. In reviewing tracking data of ransomware attacks in 2021, Recorded Future analysts believe that ransomware operators and their affiliates are opportunistic and do not typically focus on specific industries or geographic regions, but rather select and pursue organizations based on accessibility, opportunity, and factors such as the ability to pay large ransom amounts. The opportunistic nature of ransomware actors is illustrated in Figure 1, displaying the top 9 most targeted industries.

Other Attack Vectors

Olympic Games-related phishing campaigns targeting employees, partners, vendors, and customers of the 2022 Winter Olympics will very likely increase before and during the event. We have observed a significant number of Olympic Games-typosquat and similar domains being registered, some of which will likely be used in phishing campaigns. Other criminal targeting may involve distributed denial-of-service (DDoS) attacks and website defacements to disrupt, protest, or undermine the 2022 Winter Olympics in response to China's human rights abuses.

2022 Winter Olympic Games-Themed Domains

Recorded Future observed 22 typosquats of the beijing2022[.]cn domain registered over the past year. We further observed 870 similar domains, including the words "Olympic" and ("Games" or "Winter" or "Beijing" or "2022" or "ticket") registered over the past year. At the time of writing, the majority of these domains are parked or benign, although we believe it is likely that a portion of the domains will become active as the beginning of the 2022 Winter Olympics draws nearer and will be used in phishing campaigns targeting the 2022 Beijing Winter Olympics and entities associated with the Games.

We also observed domains being registered in protest of China's hosting of the 2022 Winter Olympics. The domain beijing2022[.]art is being used by the "Chinese dissident artist Badiucao", who created 5 Olympic-themed works of art to depict "the Chinese government's oppression of the Tibetan people, the Uyghur genocide, the dismantling of democracy in Hong Kong, the regime's omnipresent surveillance systems, and lack of transparency surrounding the COVID-19 pandemic". In total, we observed 185 domains including the words ("protest" or "no") and ("olympic" or "beijing") that were registered over the past year. For example, the domain boycottbeijing2022[.]net was registered on April 26, 2021, and was promoted by The Epoch

Figure 2: Homepage of the nobeijing2022[.]org website (Source: nobeijing2022[.]org)

Times as "the global boycott of the 2022 Beijing Winter Olympics website". The Epoch Times is a New York-based, multi-language (mainly Chinese and English) newspaper and media company that opposes the CCP and is known for its far-right views. The Epoch Times promoted the boycottbeijing2022[.]net domain in response to the CCP's "persecution of human rights in Xinjiang, Tibet, Hong Kong and mainland China, as well as threats to Taiwan" in an unsuccessful effort to prevent the 2022 Winter Olympics from being held in Beijing. Another similar protest domain is nobeijing2022[.]org, which seems to be one of the most popular protest domains based on online discussions, is still active as of this writing, and shares statistics on China's "crackdowns against freedom, democracy, and human rights" and encourages people to organize and protest.

Phishing Campaigns

Although Recorded Future observed limited references to other ongoing phishing campaigns related to the 2022 Winter Olympics at the time of writing, the number of phishing campaigns will very likely increase in the run-up to the start of the Games and throughout the event.

Some are campaigns are likely already underway; Recorded Future detected an Olympic-themed phishing document that loads shellcode from a macro[1]. The file name of the sample is "2022冬奥网络安全HW资料.doc", which translates from Chinese to "2022 Winter Olympics Cybersecurity HW Material". The macro code is similar to that of documents built with Cobalt Strike. The file communicates with the command and control (C2) IP address 82.157.186[.]143, which we first observed on June 17, 2021. Shodan indicates that the site contains several vulnerabilities at the time of this publication, including but not limited to an OpenSSH vulnerability CVE-2018-15919 and numerous Apache Server Vulnerabilities, such as CVE-2014-0117, CVE-2015-3185, CVE-2016-0736, CVE-2017-7679, CVE-2018-1283, and CVE-2019-0220. This suggests that the site could have been targeted by external threat activity groups for compromise and use in a campaign or that it may be used as a honeypot. Although its use as such cannot be confirmed as of this writing, Shodan has tagged the IP as a honeypot, with the TCP port 9200 purportedly being flagged as Elastichoney. Based on the malicious activity associated with the infrastructure, it is likely that an ideal target for this lure would be an entity involved in the administration of the Olympic Games (or a partner organization). Attribution for this effort is not yet available given that only open source or non-attributable tooling and techniques have been used as of this writing.

1 Hash: 21ded6b7ab1bfa37aeec8e7f1414b8e7ac0420a2996b84d56901dff8f56c132e

During the 2020 Olympics in Tokyo, Kaspersky analyzed phishing campaigns and found several common and creative themes, including:

- Fake streaming services containing registration pages to harvest credentials followed by a redirection to another page that distributes malware
- Websites trying to sell tickets to the Olympic Games (despite there being no live audiences) and websites offering fake refunds to those who already purchased tickets to harvest payment card and personal information
- Phishing pages impersonating official IOC websites, with some attempting to collect Microsoft Services credentials
- Olympic Games-themed scams luring victims with the chance of winning gifts such as a TV to watch the Olympic Games on and even a so-called Olympic Games Official Token

DDoS Attacks and Website Defacements

The 2022 Winter Olympics and associated organizations, including corporate sponsors, will likely be targets of hacktivist efforts protesting human rights abuses in China. As noted in the "International Efforts to Boycott the 2022 Winter Olympics" section of this report, the hosting of the 2022 Winter Olympics in Beijing is highly controversial, with several countries diplomatically boycotting the Games. At the time of writing, we have observed limited references to hacktivists announcing their intent to target the 2022 Winter Olympics. However, a social media account allegedly belonging to Anonymous Asia reposted a Wall Street Journal article with the headline "Chinese Official Accused of Sexual Assault Played Key Role in Setting Up Beijing 2022 Olympics", and reposted a message from "Students for a Free Tibet" who are campaigning against the 2022 Winter Olympics being held in China. Furthermore, there is a precedent of hacktivists targeting the Olympic Games being hosted in China due to human rights abuses, with hacktivists defacing an official Chinese Olympic Games website during the 2008 Olympic Games in Beijing by changing the headlines of the website into orange to highlight human rights abuses in China.

There has been substantial criticism of corporate sponsors of the 2022 Winter Olympics due to the Chinese government's human rights abuses that we suspect is likely to escalate to a hacktivist effort. Organizations reportedly spend up to $300 million per 4-year cycle to become a corporate sponsor of the Olympic Games, and will run Olympic-themed advertisements and events to generate increased awareness and affinity with their brands. However, the sponsorship relationship results in an exponentially larger attack surface, introducing additional cyber and brand threats. For example, Toyota decided against airing Olympic-themed advertisements during the 2020 Tokyo Olympics, despite being a top sponsor of the Games, almost certainly because of strong domestic opposition to the Games that could harm the Toyota brand.

US politicians have criticized corporate sponsors of the 2022 Winter Games, and as discussed in the "Physical Threats and Protests" section below, so has the No Beijing 2022 protest group. We have also observed social media users tagging corporate sponsors in posts and criticizing them for remaining silent, being complicit, and enabling the Chinese government to conduct human rights abuses while encouraging other social media users to sign online petitions to pressure corporate sponsors of the Games to withdraw their sponsorship. As a result, it is likely that ongoing criticism of corporate sponsors of the Games will escalate to hacktivist activity, such as website defacements, DDoS attacks, and other common hacktivist attacks.

As noted in Recorded Future's report on the 2020 Tokyo Olympic Games, we continue to see a general decline in hacktivism, although hacktivists have defaced Olympic Games websites and launched DDoS attacks during past Olympic Games. Hacktivists defaced the website of the Brazilian Olympics Committee after Brazil's poor performance during the 2008 Olympic Games, and another popular hacktivist campaign that was spearheaded by Anonymous Brasil was OpOlympicHacking prior to and during the 2016 Olympic Games in Rio de Janeiro, which involved DDoS attacks against Brazilian government websites and the leaking of "personal and financial details from various Brazilian sporting associations". Nevertheless, the number of large organizations susceptible to SQL injections, website defacements, and DDoS attacks has decreased due to the use of cybersecurity services such as DDoS protection services.

Chinese State-Sponsored Influence Operations

As the host of the 2022 Winter Olympic Games, the Chinese government has engaged its entire propaganda system in a long-term, coordinated influence campaign to support and defend the hosting of the Olympic Games in Beijing from domestic and international criticism. Influence operations related to the event are primarily positive to promote and support the Chinese government view of China and what the 2022 Winter Olympics represent. Decisions by several countries to diplomatically boycott the 2022 Winter Olympics due to concerns over human rights abuses in China received significant coverage across Western media, which then prompted a surge of defensive reactions from Beijing targeting the boycotting countries. Additionally, China is conducting widespread censorship of criticism internally and will censor broadcasts of the 2022 Winter Olympics on its own internet and news platforms to protect its domestic

and international audiences from being exposed to content its censors deem offensive, controversial, or disreputable.

Propaganda

China is conducting a large-scale, ongoing propaganda campaign around the 2022 Winter Olympics, targeting audiences both domestically and internationally. The campaign has two focuses: promoting positive views of Chinese culture, governance, landscapes, and athletes, and countering criticism from Western media and politicians, dissidents and protesters. This influence campaign can be broken down into 5 parts: the messaging, the influencers, the audiences, the infrastructure used for dissemination, and the tactics of the Chinese government propaganda system.

Messaging

The Chinese government views the 2022 Winter Olympics as a timely opportunity to counter international criticism for human rights abuses and to establish China as a global leader for peace and cooperation and the global leader in the fight against COVID-19. The official motto of the 2022 Winter Olympics is "Together for a shared future", which "represents the power of the Games to overcome global challenges as a community, with a shared future for humankind". Following this sentiment, messaging around the 2022 Winter Olympics is consistently positive and includes slogans such as "The light of the Winter Olympics shines all over the world", and features beautiful photos of Beijing, as well as scenic photos from various geographies in China. The Beijing Organizing Committee for the 2022 Winter Olympics, in collaboration with songwriters, created a theme song for the Games, whose lyrics emphasize the same positive attitude of togetherness: "We all yearn for love, so let's go hand in hand. Together for a shared future, you and I, we can touch the sky".

In addition to the messaging around peace and togetherness, Beijing emphasizes that China is a considerate and safe country working hard to fight climate change and eradicate COVID-19. Through its "zero COVID" policy, China touts itself as the global leader in the fight against COVID-19 and reiterates its benevolence through donations of COVID-19 vaccines, test kits, and personal protective equipment to developing areas of the world. Much of the propaganda related to COVID-19 was initially to counter accusations that COVID-19 originated in Wuhan, China, which PRC officials still deny. However, as the 2022 Winter Olympics nears, the strategy has shifted to positioning itself as the global leader in containing COVID and providing assistance to other countries, which aligns with the overall message of "togetherness". President Xi Jinping's 2022 New Years address sums up this overall messaging: "We will spare no effort to present a great Games to the world. The world is turning its eyes to China, and China is ready."

In contrast to the positive message of "togetherness" is the darker side of China's propaganda: persistent, high-volume criticism of the US and the West and the denial of human rights abuses in Xinjiang. China's government officials mention the US in a negative context hundreds of times each week, on average, on social media. According to the propaganda tracker Hamilton Dashboard, the "United States" (and "US") is the second most mentioned phrase in Chinese state-sponsored social media posts throughout 2021, and the majority of these posts are negative in sentiment, criticizing the US's diplomatic protest as "politicizing the Olympics" and contradicting the "spirit of togetherness" promoted in other messaging. Despite US support for its own Olympic committee and athletes, China portrays the US's diplomatic protest as poor sportsmanship and politicization. Differentiating between the American and Chinese approaches to the Olympics creates an "us versus them" element of identity. The Chinese government uses this tactic to recruit sympathetic partners to their side and to reject the US.

Following the Biden administration's announcement of the US's diplomatic protest to the 2022 Winter Olympics, Chinese government officials flooded social media with harsh criticism and words of condemnation, threatening that "the US will pay a price for their erroneous actions". In a December 7, 2021 press conference, Ministry of Foreign Affairs spokesperson Zhao Lijian stated, "The US has been fabricating the biggest lie of the century about so-called 'genocide' in Xinjiang, but it has long been debunked by facts. Based on its ideological biases as well as lies and rumors, the US attempts to interfere with the Beijing Winter Olympics, which will only expose its malicious intention and lead to greater loss of moral authority and credibility".

Influencers

China's influencers are individuals and organizations that conduct propaganda work on behalf of the Chinese government. Narrative centralization and control is maintained at the highest levels of the CCP and its Central Propaganda Department (中国共产党中央委员会宣传部), where content is dictated and then passed down to state-sponsored media outlets, government officials at home and overseas, sock puppet armies, and proxy actors hired to target specific audiences in other countries. These state-sponsored actors maintain high levels of engagement with audiences all over the world and have played an important role in the spread of pro-China messaging overseas, especially related to the 2022 Winter Olympics.

In November 2021, China's Consulate General office in New York hired a US-based company called Vippi Media to conduct a covert pro-China influence operation in the United States. The $300,000 contract, which was disclosed under the Foreign Agent Registration Act (FARA) on December 13, 2021, details that Vippi Media should hire 5 tiers of influencers, ranging from "nano" influencers (fewer than 10,000 followers) all the way up to "celebrity" influencers (2 million Instagram followers or 2.5 million TikTok followers). The influencers are responsible and accountable for driving viewership, mass awareness, and premium content for the Chinese government to portray positive images and sentimental moments related to Beijing's history, cultural relics, modern life of people in China, and "new trends". Influencers are also encouraged to show "touching moments" of Chinese athletes' preparations for and performances during the 2022 Winter Olympics. Additionally, the contract dictates that at least 20% of posts focus on "cooperation and any good things in China-US relations", highlighting "cooperation" on issues like "climate change, biodiversity, new energy" and "positive outcomes". 10% of the content will promote news and trends directly from the consulate general office. This contract serves as an example of how China is paying to reach younger, more tech-savvy audiences via social media outlets and influencers as proxies to China's government.

Audiences

Beijing strives to reach audiences of all types around the world to "tell China's story well". This effort includes targeting the Chinese diaspora overseas with pro-China and pro-Beijing Olympics messages to limit its reputational damage in environments where it does not have more control over the narrative. Beijing recognizes that young people are especially important in building a foundation for a world more friendly to China and its form of governance. Beijing is focusing its messaging on younger audiences and foreign audiences in an effort to influence public opinion about China, grow acceptance for Chinese culture and governance, further global adoption of its "One China" policy (reinforcing its stance that Taiwan is an inalienable part of China), and convince the global public that it is cooperative and charitable.

Infrastructure

China's primary methods of propaganda dissemination on the 2022 Winter Olympics are broadcast media and online social media platforms. China's most popular state-sponsored broadcast media include China Central Television (CCTV), China Daily, China News Service, People's Daily, Global Times, Xinhua News Agency, China Global Television Network (CGTN), and China Radio International. Recently, we have observed a transition to proxy and fringe news outlets in foreign countries as well, especially in countries where China's Belt and Road Initiative (BRI) projects are taking place. As China's government contracts with foreign media outlets and influencers, it is increasingly capable of controlling the content to reflect its own pro-China, anti-US narratives.

Social media platforms are a vital method for disseminating Olympics-related propaganda, both in domestic and foreign markets. In China, the top social media platforms are Tencent WeChat, Sina Weibo, Douyin, and Tencent QQ. All of these platforms are used widely within China and are subject to censorship under China's laws. Most foreign social media platforms are banned within China. However, Chinese government officials and state-hired "trolls" are allowed access to foreign social media platforms. Most international platforms identify Chinese state-affiliated accounts with a label and ban advertisements from those accounts. Some of the platforms also identify and report malign influence campaigns, including from China.

Tactics, Techniques, and Procedures

China conducts both offensive and defensive influence campaigns to control the messaging about the 2022 Winter Olympics. Beijing's tactics include long-term propaganda strategies such as showcasing a healthy, happy Chinese society, as well as ad hoc incident response campaigns, such as countering US criticism and diplomatic boycotts.

Many of China's influencers build rapport with local communities, adopting languages, clothing, religion, and other cultural identities. Through the shared sense of identity, and sometimes struggle, local audiences are more receptive to hearing the message. For example, the influencers often blame war, upheaval, and local conflicts on Western imperialism and connect with local audiences over a shared sense of wrongdoing by the US or so-called imperialist nations that allegedly intervene in foreign matters. This has helped China's influencers obtain "hero" status in foreign communities and promote China's non-interventionist rhetoric. These tactics have been used over the past year to build relationships between China and foreign audiences in the lead-up to the 2022 Winter Olympics. While the efficacy of these tactics is difficult to gauge, influence operations contracts reveal that the Chinese government does rely on numbers of engagements (likes, shares, comments) to measure the success of these campaigns. In the case of the upcoming 2022 Winter Olympics, China will likely measure its influence operations success by its ability to manage the Olympics without intervention or incident by foreign actors, terrorists, or protesters.

Censorship

Censorship is likely to be the most dangerous form of influence implemented by China during the 2022 Winter Olympics. Efforts by the CCP to censor journalists and human rights groups during the Olympics is likely to pose both an espionage threat and a physical security threat to these individuals and their organizations. The Chinese government stands accused of genocide and invasive surveillance of the Uyghur Muslim population in the Xinjiang Uyghur Autonomous Region of China, which the Chinese government adamantly denies and censors news of. This topic is the primary public relations concern going into the Olympics. A large portion of its state-sponsored influence, both propaganda and censorship, is dedicated to this topic in an effort to maintain credibility as a government and create a positive reputation on the global stage. Additionally, the recent censorship of Chinese tennis Olympian Peng Shuai's allegations against Zhang Gaoli, a former member of the Politburo Standing Committee, the highest-level decision-making body in the Chinese Communist Party (CCP), and her subsequent disappearance, raise concerns about the safety of Olympic athletes who would choose to speak out against the CCP during the 2022 Winter Olympics. This is just one example of a broader trend of "disappearing" celebrities who don't act in line with the Chinese government.

In the lead-up to the 2008 Beijing Summer Olympics, Chinese authorities promised "there will be no restrictions on media reporting and movement of journalists up to and including the Olympic Games" as they prepared for 20,000 journalists from all over the world to arrive in Beijing. However, when the time came, foreign journalists were harassed and threatened, and some domestic journalists were expelled and imprisoned for reporting on restricted topics, such as human rights abuses. The Foreign Correspondents' Club of China documented more than 230 cases of harassment, obstruction, and detention and at least 10 cases of death threats made against foreign journalists in China. 6 Hong Kong broadcasters were expelled from Tibet for reporting on anti-government protests, and over 50 journalists reported obstruction from Chinese government officials for trying to report on the same topic. Chinese freelance journalist Lü Gengsong is still serving an 11-year sentence at Changhu Prison in Zhejiang province for reporting on human rights issues in China during and following the 2008 Beijing Olympics. Despite widespread reporting on these issues, China faced no apparent negative consequences for breaking its commitments to the foreign press, or for punishing local reporters. In July 2008, it came to light that IOC officials made a deal with Beijing to allow the restriction and censorship of websites the Chinese government deemed "sensitive", despite Beijing's promises for free, open internet for attendees and press.

For the 2022 Winter Olympics, Beijing has not made the same type of assurances, and the situation for journalists is even more grim. The Committee to Protect Journalists said in late 2020, there were 47 journalists jailed in China, up from 30 in 2008, making China the "worst jailer of journalists in the world" for the second consecutive year. Also in 2020, 18 foreign journalists were forced to leave China due to "deteriorating diplomatic relations" between China, the United States and Australia. A more recent Reporters Without Borders investigation revealed that at least 127 journalists, ranging from major news outlet employees to local bloggers, are currently being detained in China following a sweeping crackdown to limit free expression. Additionally, in August 2021, Recorded Future discovered a large-scale Chinese state-sponsored influence campaign targeting the British Broadcasting Company's (BBC) network after it exposed that the Chinese government is paying foreigners to spread its propaganda overseas. Beijing is committed to limiting reputational harm done by the press, especially as the Olympics nears.

The CCP now has much more control over the media environment for the 2022 Olympics. With a closed-loop management "bubble" established to protect from COVID-19 outbreaks (covered more in the Physical Threats and Protests section below), the Chinese government needs no other mechanism to control who may enter or exit the COVID-free areas. The Beijing Olympic Committee will likely restrict foreign journalists' movements within the bubble, dictate whom journalists have contact with, and enforce consequences on anyone who may seek to operate outside of China's laws, including reporting on anti-government and pro-democracy protests.

International Geopolitics and Physical Threats

International Geopolitics and China's Digital Yuan

This section discusses international geopolitical tensions surrounding the 2022 Winter Olympics, focusing on human rights-oriented boycott efforts, and analyzes China's efforts to promote the digital yuan (e-CNY) during the Olympics.

International Efforts to Boycott the 2022 Winter Olympics

For the Chinese party-state, hosting the Olympic Games is an opportunity to broadcast the successes of China's political and economic system as well as affirm the country's increasingly prominent position on the world stage — which makes the international boycott effort a potentially serious reputational threat. While reacting to Beijing winning its bid to host the 2022

Winter Olympics, a July 2015 article from state-run press agency Xinhua described the occasion as "another glorious moment in China's history". The article stressed how Beijing becoming the first city in the world to host both the Summer and Winter Olympics "is the supreme honor and glory of the Chinese nation". The piece discusses how Beijing winning its 2008 Summer Olympics bid was a recognition of "the tremendous achievements obtained by China's reform and opening up" and how winning the 2022 Winter Olympics bid represented "the international community's full confidence in the continuous and steady development of China's politics, economy, and society". Likewise, China's President Xi Jinping has repeatedly stressed the importance of Chinese athletes "winning honor for the country" (1, 2, 3), and other similar goals. The Chinese authorities have also linked the 2022 Winter Olympics to China's long-term development goals, further raising the stakes of this year's Games.

The 2022 Winter Olympics have consistently attracted human rights-related pushback, which started with the International Olympics Committee's (IOC) decision in 2015 to award the Olympics to Beijing. The China Director of Human Rights Watch (HRW) described the choice as "a slap in the face to China's besieged human rights activists"; even as early as the 2008 Summer Olympics, HRW asserted that the Games were fueling, rather than alleviating, human rights abuses. However, the boycott movement did not start to gain momentum until the second half of 2018. By October 2018, the primary catalyst for the current boycott movement — China's treatment of the Uyghurs and other ethnic groups in Xinjiang province — prompted 2 United States senators to urge the IOC to relocate the 2022 Olympics.

Throughout 2019, global news outlets, advocacy groups, and non-governmental organizations repeatedly called for the Games to either be moved to a new location or for various parties to boycott them entirely (1,2,3,4). These arguments continued throughout 2020, with more media outlets beginning to take note of the "growing" movement and the debate in other countries becoming more prominent (1,2,3,4). In September 2020, 160 "[Uyghur], Tibetan, Hong Kong and Mongolian rights groups based in Asia, Europe, North America, Africa and Australia" called for the IOC to revoke Beijing's second Games over human rights abuses in Xinjiang, Tibet, and Hong Kong. In February 2021, the number of these groups rose to 180. By February 2021, the grassroots boycott movement had begun gathering momentum among world governments. In the US, for instance, US Congressman Michael Waltz introduced a bill that would have seen the US withdraw from the 2022 Winter Olympics unless it was moved to another country. Likewise, former US Ambassador to the United Nations Nikki Haley urged the Biden administration to boycott the Games. Canada reportedly began evaluating its participation in the 2022 Winter Olympics as well.

On December 6, 2021, the White House announced that the US would not send an official delegation to the 2022 Winter Olympics in Beijing, citing "ongoing genocide and crimes against humanity in Xinjiang and other human rights abuses". US athletes, however, will still attend and will have the full support of the US government. Following the US's announcement, several countries also announced diplomatic boycotts of the 2022 Winter Olympics, including the United Kingdom, Japan, Canada, Australia, New Zealand, Kosovo, and Belgium. Lithuania had announced its diplomatic boycott earlier on December 3. These diplomatic boycotts are part of a broader campaign to put pressure on China over Xinjiang, with other actions including sanctions, export controls, import restrictions, and genocide designations by the US and other countries (1, 2, 3).

Chinese authorities have consistently sought to downplay and discredit efforts to boycott the 2022 Winter Olympics. In reaction to the US's diplomatic boycott, on December 6, Zhao Lijian stated that the US should "avoid politicizing sports" and "stop hyping the so-called 'diplomatic boycott' of the Beijing Winter Games, lest it should affect bilateral dialogue and cooperation in important areas", warning of China's willingness to take "resolute countermeasures". Zhao also claimed that "US politicians keep hyping a 'diplomatic boycott' without even being invited to the Games". The IOC has expressed similar sentiments, with IOC member Dick Pound saying "how could you boycott something to which you were not invited". Pound further cast doubt on the effectiveness of the boycotts, stating "governments can signal their disapproval of whatever the particular Chinese policies may be — whether it makes any difference to the Chinese is anybody's guess. I would say, basically, no". Chinese state media has leveraged Pound's remarks to push back against the boycott effort (1, 2, 3).

China's Promotion of the Digital Yuan

The Chinese government is promoting the digital yuan (e-CNY) at the 2022 Winter Olympics by making it possible for foreign visitors to use the e-CNY at Olympic venues in Beijing without having a Chinese bank account. This is the first time that China's digital currency will be tested with international users. It is likely that this promotion of the e-CNY, particularly trialing the digital currency with foreign visitors, is an effort by the Chinese government to build international credibility in its central bank digital currency (CBDC) as part of a larger effort to boost the international standing of the yuan.

China's central bank, The People's Bank of China (PBOC), announced it was researching a "Digital Currency Electronic

Payment" system in 2014. The Digital Currency Electronic Payment (DCEP) project was officially launched in 2017, establishing China's CBDC; a digital version of the yuan (referred to as DCEP, digital yuan, e-yuan, digital RMB, and e-CNY). The DCEP project is currently in the "Pilot" phase. It was first piloted in 4 cities in April 2020, and has since significantly progressed and expanded across China. At the beginning of 2022, the PBoC launched a digital wallet app for the e-CNY available on China's iOS and Android app stores for members of the public located in Chinese cities partaking in the e-CNY trials, namely Changsha, Chengdu, Dalian, Hainan, Qingdao, Shanghai, Shenzhen, Suzhou, Xian, Xiongan, and, importantly, venues of the 2022 Winter Olympics being hosted in Beijing.

There are likely several motivations behind China's launch of the e-CNY, including:

- Countering the "threat" of a "privately developed 'super sovereign' digital currency" like Facebook's Libra, as evidenced, in part, by the PBoC effectively banning cryptocurrency transactions in China on September 24, 2021
- Allowing for greater insight into how money is flowing in China, "purportedly to manage anti-money laundering and counter-terrorism financing risks", though raising significant data privacy concerns that the PBoC governor responded to in November 2021
- Regaining control over payments currently mediated by private firms such as Alipay and WeChat, instead allowing the PBoC to directly mediate payments and store payment data themselves
- Boosting the international standing of the yuan and beginning a breakaway from a US-centric global financial order, where over 40% of global transactions on SWIFT's international payment systems are denominated in dollars "compared to less than 2% in yuan", in addition to SWIFT international payments complying with unilateral US sanctions

Physical Threats and Protests

In addition to diplomatic boycotts of the 2022 Winter Olympics, there have also been calls for physical protests of the Games, although the public will no longer be able to attend the Games. Athletes have been warned by the deputy director general of Beijing 2022's International Relations Department that they could be punished for "any behavior or speeches that are against the Olympic spirit", such as by canceling the offending athlete's credentials. Similarly, Human Rights Watch has advised athletes "not to speak up" on human rights abuses while at the Games for the sake of their own safety. There have been a small number of grassroots protests in the months leading up to the 2022 Olympics, with many of the protests relating to topics such as human rights abuses in Xinjiang and Tibet or geopolitical tensions such as those between China and Taiwan. As the Olympic Games nears, it is likely that protests will continue to be organized both domestically in China and worldwide.

No Beijing 2022

Most protests against the 2022 Winter Olympics have been organized by international groups and center around the reports of human rights abuses and forced detentions of people in the Tibet and Xinjiang regions of China. One group calling for boycotts and protests of the Games is No Beijing 2022, which is organized by 86 grassroots organizations worldwide, including the Students for a Free Tibet and the World Uyghur Congress. The group is composed of Tibetans, Uyghurs, Hong Kongers, Taiwanese, Southern Mongolians, and Chinese rights activists and their supporters. Their website provides resources for those looking to sign up for protests, or organize their own protests using NoBeijing2022's Action Toolkit. They also had a Global Day of Action on January 4, 2022, and had protests planned in North America, Europe, Australia, Argentina, Indonesia, Japan, South Africa, South Korea, and Taiwan. The group is also selling merchandise to help support their cause. Furthermore, the group has publicly criticized various sponsors of the 2022 Winter Olympics (such as AirBnB and Snickers) and is calling upon supporters to message those companies using the #NoBeijing2022 hashtag. The group has also organized previous Global Day of Actions, with the last day being on June 23, 2021, as well as "social media storms" where its members message pre-made phrases from their Action Toolkit toward the IOC, athletes, sponsors, and other vendors of the Olympic Games. Hashtags used by this group include #NoBeijing2022, #Beijing2022, #NoBeijingGames2022, and #BoycottBeijing2022.

Other Protests

Other human rights groups, athletes, and independent organizations have called for the boycott of the 2022 Winter Olympics, with some groups labeling it the "Genocide Games" (#GenocideGames). There were protests at a handover ceremony in Greece in October 2021 after Beijing Games Vice President Yu Zaiqing lit a torch for the Games. The protestors held a Tibetan flag and called for a boycott of the Games due to the suppression of cultural and religious freedoms in Tibet. In December 2021, protestors from the Tibetan Youth Association and Students for a Free Tibet in Europe gathered at a meeting of the International Olympic Committee's headquarters in Lausanne, Switzerland. The protestors demonstrated in the building's lobby, and several chained themselves to the Olympic rings outside of the building.

Another coalition of human rights groups, Boycott Beijing 2022, has called upon athletes, sponsors, and governments to boycott the 2022 Winter Olympics, stating that participating in the Games would be "tantamount to endorsing China's genocide against the Uyghur people, and legitimizing the increasingly repressive policies of the totalitarian Chinese regime". There have also been reports of protests in the US, called "Recover Freeway", that saw banners draped over bridges in California and Colorado. These banners had phrases such as "No Beijing Genocide Winter Olympics" and "End CCP". Furthermore, there are approximately 50 petitions on Change[.]org, a US petition website, as well as dozens of other petitions on social media and other websites, calling for the boycott of the 2022 Winter Olympics.

Chinese authorities have also increased security in the Tibetan regions of Lhasa, Shigatse, Chamdo, Draggo, Ngaba, and Rebkong in the leadup to the Winter Olympics. A December 2021 report by Radio Free Asia, identified that additional security forces were deployed and movements within the region have been restricted. At the time of writing, it is unknown whether similar restrictions and heightened security are being placed upon other regions, such as the Xinjiang Uyghur Autonomous Region.

Olympics Bubble and COVID-19 Travel Restrictions

Due to the ongoing COVID-19 pandemic and China's zero-COVID strategy, the 2022 Winter Olympics will be held in a tight bubble that includes only the athletes, media, and essential personnel, such as volunteers, cooks, coach drivers, and cleaners. While the bubble is designed to contain the spread of COVID-19, similar to the bubble that Japan had for their Summer Olympics, there are concerns that China's bubble will be too strict. The bubble will consist of a closed loop and will begin from the moment people land in Beijing until the time they leave. Unlike the Tokyo Olympics, those in the bubble will not be able to leave and venture into the public and participants living in China will have to quarantine after the Olympic Games. Travel between the 3 game areas will be done via high-speed railway and those in the bubble will be kept in separate carriages. There are concerns among diplomats that they may not be able to offer help to those inside the bubble, if needed. On January 5, China announced that it had started to seal the Olympics bubble and that those participating in, working at, or volunteering with the Games would be in a "closed loop" with no direct access to places outside of the bubble from the date. Athletes and journalists arriving for the Games in the coming weeks will also be in the bubble.

There are also concerns that there will be travel restrictions imposed on the bubble if a COVID-19 case were to emerge. China has locked down several cities, such as northwestern Xi'an and central Yuzhou, in response to a rise in COVID-19 infections. At the time of writing, neither the Chinese government nor the IOC have released their response plans if a COVID-19 infection were to emerge within the bubble.

China has also banned all foreign spectators from attending the 2022 Winter Olympics and more recently canceled plans for any members of the public to be able to attend the Games. The ban on members of the public attending the Games is intended to reduce the spread of COVID-19, but it can also be used to thwart attempts by protestors to disrupt the Games. Furthermore, while historical Olympic Games have had special zones for protestors, the IOC has said that any official protest zones at the 2022 Winter Olympics will depend on local public health measures that are being enforced at the time of the Games. It is very unlikely that there will be a special zone for protestors given that members of the public are now banned from attending the Games. Moreover, given how tight the Olympics bubble is, it is unlikely that there will be protests held by outside groups at the Games, as seen in historical events, and protests of the Games will likely be conducted outside of China (such as the aforementioned instance at the IOC) by international groups.

Outlook

The threat landscape for the 2022 Winter Olympics is vastly different from other recent Olympic Games due to their being hosted in Beijing. Chinese, Russian, Iranian, and North Korean state-sponsored cyber activities are more likely to focus on surveillance and cyber espionage rather than disruption operations; Chinese state-sponsored influence operations are mainly positive in an effort to promote and defend the Games being hosted in Beijing, while censoring domestic and international criticism of China; diplomatic boycotts and grassroots protests are in response to China's human rights abuses.

The threat that is most consistent with those facing previous Olympic Games is that of financially motivated threat actors opportunistically exploiting the 2022 Winter Olympics. Financially motivated threat actors likely pose the greatest cyber threat to a wider range of targets during the 2022 Winter Olympics, including the Games themselves, associated organizations, and individuals interested in the Games. Financially motivated cyber activity that exploits the 2022 Winter Olympics will likely inform the threat landscape for the 2024 Olympic Games in Paris as well, but we expect the threat landscape for the 2024 Games to be significantly different with regards to state-sponsored cyber operations, influence operations, international geopolitics, and physical threats.

Similar to our report on the 2020 Tokyo Olympics, we expect to observe increased threat activity as the beginning of the 2022 Winter Olympics draws near, for example uncovering additional Olympic-themed phishing campaigns and fraudulent domains.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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