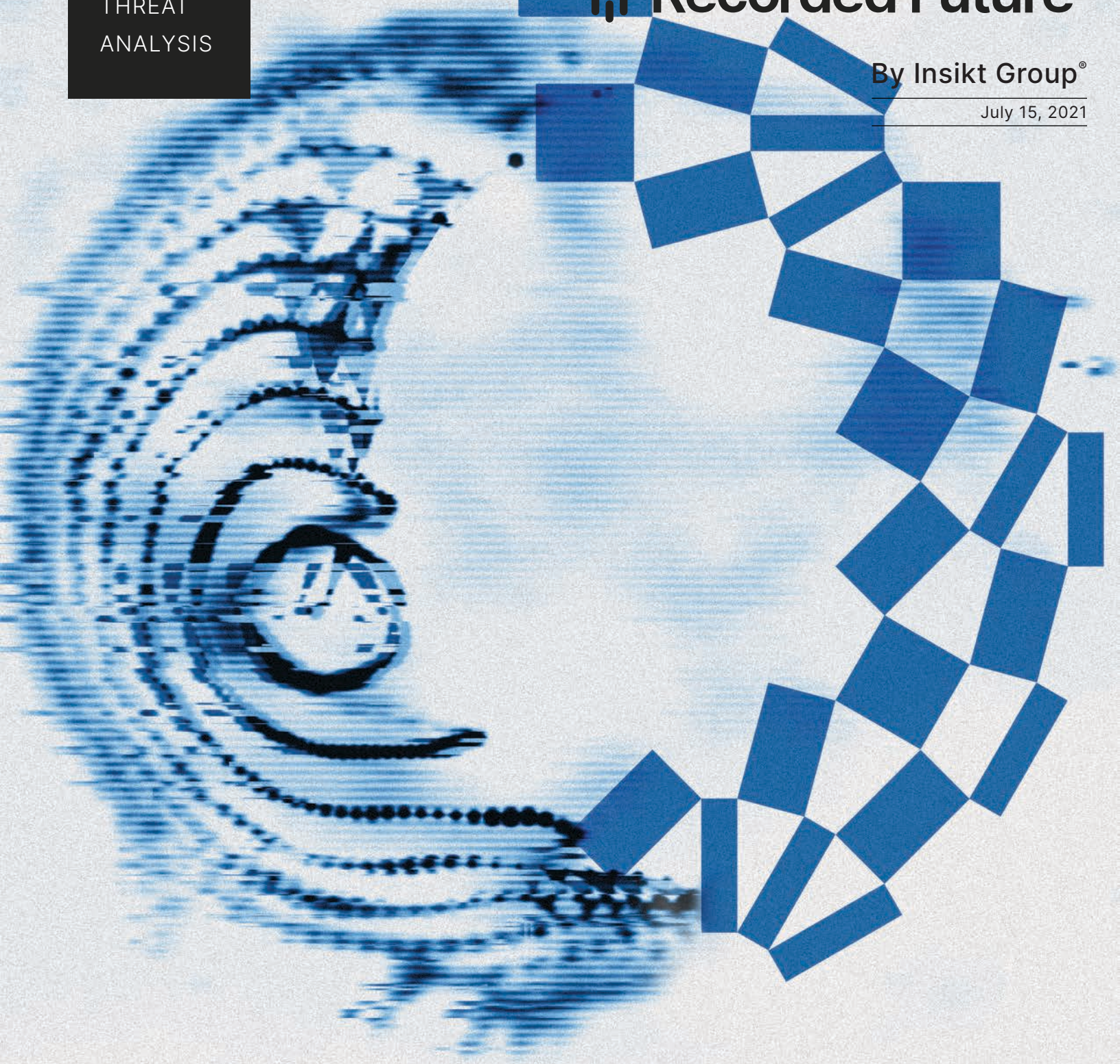
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

July 15, 2021



Threats to the 2020 Tokyo Olympic Games

Recorded Future®

This report synthesizes findings from the Recorded Future® Platform, dark web communities, and open-source intelligence (OSINT) sources to analyze the threat landscape ahead of the 2020 Tokyo Olympics, set to begin on July 23, 2021, after COVID-19 pandemic-related postponements. This report will be of most interest to organizations affiliated with the Olympics organization, Olympic sponsors, or individuals intending to participate or attend the upcoming Olympic Games.

Executive Summary

The Olympic Games are a target-rich environment, drawing athletes from more than 200 nations, worldwide media coverage, and thousands of spectators. The high profile and international nature of the event make the Olympics a target for those seeking to cause politically motivated harm, enrich themselves through criminality, or embarrass the host nation on the international stage. Past Olympics have seen the targeting of the Olympics organization and its partners, such as the World Anti-Doping Agency, from a variety of threat actors.

The upcoming Olympics Games are likely to attract state-sponsored threat activity groups, cybercriminals, and groups motivated by political grievances and regional tensions. Nevertheless, at the time of writing, Recorded Future has not identified any direct threats, planned attacks, or cyber operations against the Tokyo Olympic Games.

Key Judgments

- State-sponsored threat actors likely pose the most significant threat to the Olympic Games and Olympics-affiliated entities based on their sophisticated capabilities as well as ongoing disputes between various states and the International Olympic Committee (IOC) or associated bodies.
- Given coordinated cyber campaigns targeting previous Olympic Games and affiliated organizations linked to Russian threat activity groups, as well as the current dispute between the IOC and Russia over the country's eligibility to participate in international sporting events, Russian APT groups are likely the most motivated to target and disrupt the upcoming Tokyo Olympics. APT groups linked to other nation-states, such as China, North Korea, or Iran, either lack historical precedence for targeting such events or are assessed to lack the requisite motivation to do so in the case of the Tokyo Olympic Games.
- Ransomware likely poses the greatest threat to Olympics-nexus organizations from the cybercriminal perspective. On June 25, 2021, various newspapers in Japan reported that the Japanese Olympic Committee (JOC) was affected by ransomware in April 2020. Ransomware operators are likely to view the Olympics and associated entities as attractive targets, as downtime of core infrastructure and services are unlikely to be acceptable during the Games; as a result, victim organizations may be heavily incentivized to quickly pay ransoms to restore normal operations.
- State-sponsored propaganda and disinformation outlets are engaging in initial influence activities against the Tokyo games to generate controversy and undermine the event as unpopular, unsafe, or unfair. These narratives are likely to continue throughout the event.
- Recorded Future has not observed any direct physical threats aimed toward the Tokyo Olympics or the athletes themselves. The ongoing COVID-19 pandemic and associated restrictions on international guests in Japan likely reduces the opportunity for such attacks to take place. The Olympics are a common venue for political protest, and widespread opposition to the games in Japan due to the ongoing COVID-19 pandemic in the country is likely to inspire domestic protests. None of the protests thus far observed, however, have been violent.

Cyber Operations Targeting the Olympics Since 2018

Russia

APT Threat Groups and Activity

Russian advanced persistent threat (APT) groups have previously conducted destructive cyberattacks and cyber espionage targeting several organizations with a nexus to the Olympics and international sport. Past targets have included the World Anti-Doping Agency (WADA), the US Anti-Doping Agency (USADA), the Canadian Center for Ethics in Sports (CCES), the International Association of Athletics Federations (IAAF), the Tribunal Arbitral du Sport/Court of Arbitration for Sport (TAS/CAS), the Fédération Internationale de Football Association (FIFA), and French multinational information technology service Atos.

Russian state-sponsored cyber groups were observed targeting the 2018 Winter Olympics, and according to US and UK authorities in 2019, Russian actors have already conducted reconnaissance efforts against officials and organizations involved in the Tokyo 2020 Olympics. This activity was likely related to Russia's banning from the Games for its doping activities; Russia has been banned from competing as a nation in international athletics since 2015. In December 2020, Russia was banned from fielding a national team in the next 2 Olympics, as well as any world championship sporting event for the next 2 years.

APT28 and Sandworm, each associated with Russian Main Intelligence Directorate (GRU) Units 26165 and 74455, respectively, are linked to past targeted intrusions against Olympics-related organizations. The nexus between these military intelligence units and sports is unclear; however, there is a longstanding relationship between the Russian military and Olympic sports, with the Ministry of Defense overseeing elite Russian sports clubs during the Soviet era. The largest Russian sports club is the Central Army Sports Club (CSKA) Moscow, which has claimed at least "1,058 medals were won by CSKA athletes at the Olympic Games, including 463 Olympic gold medals". Therefore, the loss of national pride following the country's bans from participation likely at least in part drives Russian cyber activity against international sporting events and organizations.

For its part, APT28 was active around the time of the 2016 Rio Olympics when the group conducted an influence operation employing pseudo-hacktivist front groups to dump drug-testing files from Olympic athletes that were likely stolen during intrusions into the World Anti-Doping Agency.

Sandworm was active during the 2018 PyeongChang Winter Olympics, conducting destructive malware attacks that disrupted the IT infrastructure of the games in South Korea during the opening ceremony. A malware variant known as Olympic Destroyer was used to target major telecommunications and IT providers as part of targeting the Olympic Games in PyeongChang prior to December 2017. Researchers from Talos and Crowdstrike discovered that Olympic Destroyer was used to disrupt the Olympic Games opening ceremony on February 9, 2018. Sandworm delivered the Olympic Destroyer malware, described by Kaspersky as a "destructive self-modifying password-stealing self-propagating malicious program". Their research indicated that Olympic Destroyer was delivered via spearphishing emails with attached documents containing embedded Powershell scripts that, when executed, installed backdoors on targeted hosts associated with the Olympic Games, including local venues, the Pyeongchang2018[.]com server, and Atos — an IT services provider. Subsequent reporting, sourced to unnamed US officials, suggested that the attack was a "false-flag" operation by Russian GRU actors seeking to make it appear as if North Korea were behind the attack by using North Korean IP addresses and a faked rich header.

North Korea

APT Threat Groups and Activity

Due to North Korea's non-participation in this year's event as well as various internal pressures, including the COVID-19 pandemic and a worsening food shortage, it is unlikely that North Korea will seek to disrupt the Tokyo Olympics. However, for internal propaganda purposes, it is likely that North Korean state media, which is closely controlled by the regime, will doctor photos and fabricate articles of their athletes winning gold medals.

Nevertheless, North Korean threat groups have a limited history of targeting Olympics-nexus organizations. In February 2018, McAfee detected a fileless malware, dubbed Gold Dragon, which was used to target Olympics-related organizations. The first Gold Dragon variants that McAfee observed in the wild in South Korea appeared in July 2017. The original Gold Dragon malware had the file name "한글추출.exe", which translates as "Hangul Extraction" and was seen exclusively in South Korea. While initially no attribution to North Korea was made, in August 2018 McAfee released a comparison of North Korean malware where code overlaps between Gold Dragon and NavRAT were detailed. Various reports in 2018 mentioned that NavRAT is likely linked to North Korean APT Group123 (also tracked as APT37).

In November 2020, Cybereason published details regarding the similarities in URL patterns and infrastructure used by Gold Dragon and several other malware linked to Kimsuky, another North Korean state-sponsored threat group. Kimsuky has historically targeted individuals and experts in various fields, think tanks, and government entities in South Korea, Japan, and the United States, as well as universities with biomedical engineering expertise.

China

APT Threat Groups and Activity

There is no historical precedent for Chinese threat activity groups targeting major international sporting events or sporting bodies. China has also shown significantly more restraint compared to other nations in conducting wide-reaching destructive or disruptive attacks. Therefore, while Chinese 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 Olympic Games at this time.

However, Japan remains a major focus of Chinese cyber espionage efforts both through threat activity groups affiliated with China's principal civilian foreign intelligence service, the Ministry of State Security (MSS), and its military intelligence apparatus, the People's Liberation Army (PLA) Strategic Support Force (SSF), due to the regional proximity between the two countries.

Recorded Future tracks several Chinese groups (detailed below) with a strong Japan focus that could lead them to conduct intelligence-gathering operations targeting Olympic officials and sponsors. Furthermore, athletes or individuals who may seek to use publicity associated with the Olympics to shed light on purported human rights abuses within China, such as that of Uyghur Muslims in Xinjiang, are more likely to be individually targeted for monitoring and surveillance purposes. The main Chinese APT groups with a Japan focus are the following:

- APT10, also known as Stone Panda, CVNX, MenuPass, POTASSIUM, and Red Apollo, is a Chinese state-sponsored threat group that has been active since approximately 2009. The group, composed of private contractors who operate through a series of front companies, operates on behalf of Tianjin State Security Bureau, a provincial bureau of China's MSS. While APT10 has always had a focus on Japan, the group has also targeted organizations globally. However, post-US government indictment, the group has become even more regionally focused, with all recently published activity specifically targeting Japan-linked private sector organizations.
- Tick, also known as Bronze Butler, has historically used custom malware variants to target defense, aerospace, chemical, and satellite industries, primarily focused on organizations with head offices in Japan and subsidiaries in China. In April 2021, Japanese news sources reported that the group is linked to PLA-SSF Unit 61419 located in Qingdao. Tick is suspected of having close links to Tonto Team, another Chinese group which both targets Japan and has been linked to the PLA, specifically the Shenyang Military Region Technical Reconnaissance Bureau. While the groups have distinct tactics, techniques, and procedures (TTPs) and targeting profiles, they have been identified sharing capabilities. In early 2020, Tick Group was linked to a historical intrusion disclosed by the Japanese multinational Mitsubishi Electric.
- A 2020 JPCERT report observed the use of WINNTI malware in targeted attacks reported around August 2020. In previous years, various Japanese security researchers (1, 2) also observed the use of the WINNTI malware variants all the way from 2013 to 2020. WINNTI (aka HIGHNOON) is a longstanding backdoor and rootkit that has been historically used by multiple APT groups, including APT17 and APT41.
- Numerous reports from Japan's Computer Emergency Response Team (JPCERT) indicate that Blacktech, also known as Palmerworm and Temp.Overboard, was highly active in 2017 and 2018 targeting Japanese corporations, with recent reporting indicating the group's continued activity. BlackTech was also named in a 2019 breach against the major Japanese multinational Mitsubishi Electric, the same organization subsequently targeted by Tick. The same Japanese sources also link BlackTech to a military unit based in Wuhan; however, the group has not currently been attributed to a specific PLA unit.

Iran

APT Threat 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. This does not, however, preclude Iranian APTs from leading espionage intrusion attempts against organizations supporting the Olympics or people attending them. Of the major Iranian threat activity groups, APT39 would most likely be responsible for penetrating anti-government networks that may attempt to use the Olympics in Japan 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.

Iranian domestic politics have been rife with politically motivated sporting controversies. These have included the boycotting of the Olympic Games and sporting competitions involving athletes from Israel, as well as those involving female athletes and supporters. The use of thematic lures linked to the Olympics has also not historically been part of observed Iranian APT tactics. However, the potential for Iranian APT groups to expand into the sporting realm is elevated in particular with regards to Iranian domestic political activity, and in relation to other Middle Eastern sporting and Olympic federations.

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 2020 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.

According to an October 28, 2020 Microsoft report, APT35 led an espionage campaign masquerading as conference organizers for the Munich Security Conference and Think20 (T20) Summit in Saudi Arabia. Microsoft's Threat Intelligence Center (MSTIC) assessed that the primary goal of this campaign was the targeting of high-profile individuals attending the security conferences, including ambassadors and senior policy experts. During the operation, APT35 sent spoofed email invitations to former government officials, policy experts, academics, and leaders from non-governmental organizations (NGOs). The emails used near-perfect English and included invitations to remote sessions to assuage fears of travel during the COVID-19 pandemic.

While Recorded Future has not detected any APT35-linked activity that would signal an intent to target the Japanese government, the host city, or any organization linked to the planning of the Olympics, APT35 would likely demonstrate the same TTPs as in past campaigns in their use of Olympic-themed lures to target conferences and events that are either occurring before, during, or after the Olympics. This also includes the targeting of researchers, political, policy, and diplomatic officers attending conferences.

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 maintaining similar operations, is likely to be tasked to track Iranian athletes and diaspora community members, activists, and Iranian dissidents.

Open source reporting has also indicated that intra-governmental targeting has also occurred, whereby members of the IRGC led targeted intrusions against cabinet members of President Hassan Rouhani. While there is no direct link between APT39 and the Olympics, such instances of past targeting reveal the increased likelihood of surveillance against Iranian government officials who may attend the Olympics.

Financially Motivated Cyber Threats

Criminal Targeting

Recorded Future has not identified direct threats, planned attacks, or cyber operations against the Tokyo Olympic Games among dark web and underground forums, with posts referencing the Olympics found primarily on the following underground forums: Club2CRD, Omerta, Korovka, Verified, and the Honker Union of China. The majority of the relevant posts found on these sources are related to such topics as:

- News media citations and reposting
- Advertisements and sales of pharmaceuticals/ medications
- Sales of compromised login account credentials related to the Olympic Games and affiliated Olympic organizations
- Mentions of the Olympics in filenames leaked on ransomware extortion websites

A further 2 dark web marketplaces were observed selling information related to the 2020 Olympic Games: Genesis Store and Russian Market.

Genesis Store: Recorded Future identified references to the 2020 Olympic Games on Genesis Store, a dark web market that sells victim information in a format that the group refers to as "bots". Bots include combinations of victim account credentials, browser fingerprints, IP addresses, and session cookies. All 20 browser logins discovered on the Genesis Store were related to tokyo2020[.]org, the website of the organizing committee. One subdomain appears to be dedicated to the Japanese volunteers of the 2020 Tokyo Olympics.

Russian Market: Recorded Future also found references listed in connection with the 2020 Tokyo Olympic Games on Russian Market, a shop operated by the threat actor "RussianMarket" that sells dumps, RDP and SSH access, logs, and various account details. Similar to the Genesis Store, Russian Market contains various website logins to "tokyo2020[.]org". Gaining access to these credentials would allow threat actors who buy them to log into the accounts and perform malicious activity such as business email compromise (BEC), privilege escalation, and an overall online identity takeover of the legitimate credential holder.

This is due to the fact that the sets of credentials typically have extensive information about the source of the credentials and cookies scraped from the victim.

Ransomware Threats

Ransomware likely poses the greatest cybercriminal threat to Olympics-nexus organizations. On June 25, 2021, various newspapers in Japan reported that the Japanese Olympic Committee (JOC) was affected by ransomware in April 2020.

Recorded Future has not observed chatter or indicators suggesting that ransomware operators are specifically targeting Olympics-related organizations at this time. However, as ransomware operations are generally opportunistic in nature, and due to the high-profile, international nature of the games, such organizations are likely to be attractive targets for ransomware operations. The downtime of core infrastructure and services is unlikely to be acceptable during the games; as a result, the victims are likely to be induced to pay ransoms and restore normal operations quickly.

Recorded Future examined ransomware extortion websites since January 2020 and identified 35 references to 2020 Olympic Games-related entities posted on Corporate Leaks, an extortion website managed by Nefilim ransomware operators. The website is used to post the name or domain of victims infected with Nefilim ransomware, along with a sample set of data stolen from the victim network. Analysis of the content posted on Corporate Leaks indicated that the Olympic Games-related documents were likely a part of an attack against Luxottica Group, an Italian eyewear conglomerate and the world's largest eyewear company, which was hit by a ransomware attack in September 2020. We identified the following Tokyo Olympic-related documents published by the Nefilim ransomware operators:

- 24532 2020-01-13 11:08 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics\MOTOGP Simulation (WHSL).xlsx
- 758183 2020-01-13 11:09 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics\Tokyo Olympic + Mugello 2020 - TH.pptx
- 0 2020-01-14 03:39 LUXOTICA_other_part_8\2020 Marketing Plans\Mugello + Tokyo Olympics

Threats to Olympic Infrastructure

The 2020 Olympic infrastructure faces threats from several sources, including both cyberattacks and physical threats. We believe that as the opening date for the Olympics approaches, there will likely be an increase in phishing attempts made against Olympics employees, partners, vendors, and customers. Additionally, Olympic planners and policymakers should be alert to commonly used techniques involving distributed denial of service (DDoS) attacks, website defacements, domain typosquatting, and spearphishing attacks.

Phishing Attacks

Particular vigilance against phishing attacks is warranted, as this has been a common vector for APT and other threat groups to target Olympic infrastructure during past games. These phishing attacks can lead to malware infections, causing loss of data as well as physical damage to Olympic properties.

We identified approximately 721 references to Olympics-related phishing events in the last 3 months. While threat actor attribution for phishing events is difficult, we observed common themes in the structure of the phishing messages, such as the use of urgent language in emails, the impersonation of executives or vendors, and the use of malicious websites posing as vendors or ticketing systems. It is likely that the overall goals of these phishing emails were to install malware on targeted networks and to gather user credentials that could be used for more targeted attacks.

The 2020 Tokyo Olympics was affected by a May 2021 compromise of the ProjectWEB platform. ProjectWEB is a Japanese cloud-based enterprise collaboration and file-sharing platform launched in the mid-2000s and is broadly used today by Japanese government agencies. In the intrusion, an unknown threat actor was able to access ProjectWEB and obtain at least 76,000 email addresses, proprietary information, and email system settings. The attackers then gained access to Japan's Ministry of Foreign Affairs and Tokyo's Narita International Airport through ProjectWEB and stole air traffic control data, flight schedules, and information on business operations.

On June 2, 2021, the Japanese government's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) confirmed in a statement that the compromise had exposed data of some 170 people who participated in a cybersecurity drill ahead of the Olympic Games. The leaked data included the names and affiliations of people from 90 organizations involved in hosting the Olympics, according to a Japan Times article. However, the ProjectWEB intrusion was likely a supply chain attack to steal information from various Japanese organizations as opposed to a targeted attempt to compromise the Olympics, with the main users of the ProjectWEB platform being Japanese government agencies.

DDoS and Website Defacements

A primary threat to previous Olympics ,such as those in PyeongChang and Rio de Janeiro ,was DDoS attacks performed

by hacktivist groups .However ,Recorded Future has not identified organized hacktivist groups announcing their intent to target 2020 Olympics infrastructure at this time.

Past campaigns include the 2016 Anonymous campaign #OpOlympicHacking ,which has been the most widely noted in regards to targeting the Olympic Games .The aforementioned campaign saw hacktivists using social media channels to organize coordinated DDoS attacks ,discuss vulnerabilities within targeted networks ,and announce the results of campaigns. These attacks were not limited to Olympic-related websites, but also affected companies related to the Olympics such as sponsors ,hosting cities ,and governmental websites.

However ,our data and analysis indicate that ,similar to research conducted by others over the past year ,chatter surrounding hacktivist attacks has been in steep decline since a peak between 2015 and .2016 The number of large enterprises susceptible to SQL injection attacks or DDoS floods has decreased ,likely due to more mature website structures and the use of DDoS protection services like Akamai and Cloudflare. Although some hacktivist actors are highly skilled ,more often than not many members of a hacktivist organization are novices and rely upon simple and outdated tools and techniques that are easily defeated by competent network defenders.

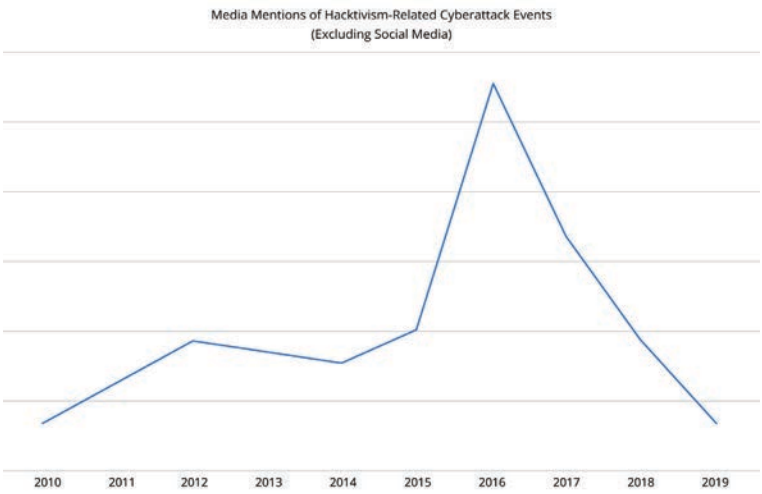


Figure 1: Media mentions of hacktivism-related cyberattacks, 2010–2019 (Source: Recorded Future)

Hacktivist groups rely on media attention to spread their message, and disruptive cyber activities during the event will receive immediate press attention, as observed during the 2018 PyeongChang Olympics. For example, various Iranian hacktivist groups have historically launched targeted website defacement attacks against international football teams, either in support of a local Iranian team competing in international competitions or in support of Iran's national football team. Such attacks have been committed by members responsible for the ALFA TEaM's AlfaShell and have targeted a host of international and regional football sporting organizations.

Figure 2: Defacement imagery posted by ALFA TEaM members against the Syrian Soccer Federation (Source: tarafdari[.]com)

In large part, attacks such as those committed against the Syrian Football Federation after a 2018 FIFA World Cup qualifying game, or against Bahrain's Football Association (BFA) after a 2022 World Cup qualifier, materialized as hacktivists perceiving a sense of injustice or in response to insults against the Iranian football team or nation. Given the current tensions between Japan and South Korea as well as the political disputes related to the Senkaku/Diaoyu Islands with China, a nationalistic hacktivist campaign out of China in particular targeting Japanese infrastructure is plausible but deemed unlikely given the recent decline in patriotic hacktivism in recent years.

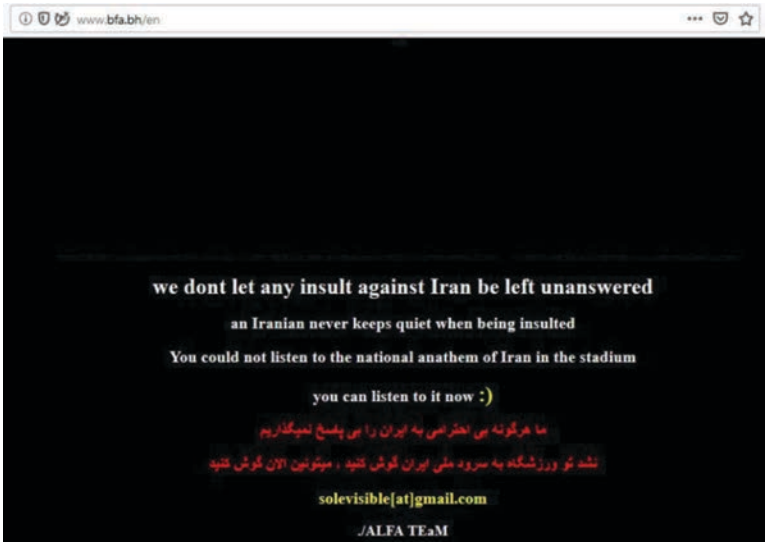


Figure 3: The website of the BFA is defaced by ALFA TEaM after perceived insults heard during the Iranian national anthem at a Bahraini stadium (Source: ILNA News[1])

[1] https[:]//www.ilna[.]news/%D8%A8%D8%AE%D8%B4-%D9%88%D8%B1%D8%B2%D8%B4%DB%8C-7/825013-%D8%B3%D8%A7%DB%8C%D8%AA-%D9%81%D8%AF%D8%B1%D8%A7%D8%B3%DB%8C%D9%88%D9%86-%D9%8

Tokyo Olympics-Themed Domains

Since April ,2021 ,1 Recorded Future has observed the registration of 44 domains that mimic the 2020 Olympics and its branding .Additionally ,we believe that while the majority of these domains resolve to generic domains that are currently parked ,the pages will likely become more active as the start of the games draws nearer.

While no malicious activity was observed at the time of writing, some subset of these domains will likely be used for future malicious purposes closer to the start of the Olympics. A full list of these domains is included in Appendix A.

Non-Cyber Threats to the 2020 Olympics

Information and Influence Operations

Nation-state propaganda and disinformation outlets are engaging in initial influence activities against the Tokyo games to generate controversy and undermine the event as unpopular, unsafe, or unfair.

Before COVID-19 forced the cancellation of the Tokyo games in 2020, the Cyber Threat Alliance (CTA) predicted that disinformation campaigns surrounding the Olympics were "most likely" alongside disruptive cyberattacks. Furthermore, CTA judged that malicious cyber activities "are likely to come in the form of social media or disinformation campaigns rather than direct attempts to compromise a specific organization". This likelihood was further compounded by Russia's Olympics ban, which almost certainly angered the Kremlin and would at the very least compel the state to engage in state-sponsored overt influence activities to undermine the Olympics or athletes competing in the games from other nations.

With the games currently set to occur and with minimal changes in Russia's eligibility to participate (Russian athletes are participating under the Russian Olympic Committee (ROC), not the Russian Federation), we believe that Russian disinformation activities remain likely to materialize.

COVID-19

Since the outbreak of COVID-19, foreign governments, state propaganda and disinformation outlets, and social media have presented false and misleading narratives about the symptoms and the lethality of the virus, treatments and therapeutics, case numbers, and more recently the efficacy of vaccines, as well as legal and moral debates over their use. As we approach the Tokyo Olympics, we believe that COVID-19 will remain a persistent topic of debate in media coverage and will almost certainly serve as a sub-theme of disinformation and propaganda. Broadly speaking, we expect to identify at least isolated false claims both in local Japanese media and abroad regarding regional case counts, variants in the wild, and potentially misleading information about the safety of the local population as athletes from around the world arrive in Japan.

Additionally, it is likely that COVID-19-related misinformation and disinformation will spread about specific venues, including COVID-19 mitigation procedures (like testing, masks, and other mandates such as vaccines) at both sporting event venues and other high-traffic areas such as the Olympic Village.

Finally, there is a strong chance of targeted false narratives and disinformation targeted at country athlete delegations, such as claims stating that certain athletes or country delegations "brought" a virus variant or were the cause of an internal outbreak that places the public at risk. In 2020, the US military found itself the subject of a false claim produced and amplified by Chinese state officials and official state outlets that suggested that military officials introduced COVID-19 to the Chinese public after the 2019 Military World Games in Wuhan, Hubei province, China, before the first cases of COVID-19 were documented. Chinese authorities have repeatedly reintroduced this conspiracy theory without any supporting evidence.

We have identified Russian state media outlets concentrating on the following themes:

- **The 2020 Tokyo Games are unsafe:** Russian state media outlets have portrayed the Olympic organizing committee as taking a poorly calculated risk amid COVID-19 emergencies in Japan, assessed that the Olympics may be canceled altogether with rising cases, and questioned the event after North Korea elected to not compete for safety reasons.
- **The 2020 Tokyo Games are unpopular with the general public:** Russia Today has extensively covered the Japanese public's lack of support for the games due to COVID-19. Though this sentiment is largely genuine, it is portrayed via sensationalist articles such as "'Olympics kill the poor': Furious Japanese public protest Tokyo 2020 Olympics as calls to cancel Games continue". Likewise, the outlet also alleges that the games are unpopular due to allegations of sexism against the Japanese government and the Olympic Planning Committee. Both Chinese and Russian sources also focus on public opinion polls that suggest a majority of Japanese do not want the games to be held this year.[2]

[2] http://en.people[.]cn/n3/2021/0111/c90000-9807866.html

- **Russia has not been treated fairly by the International Olympic Committee:** Russian state media have strongly criticized and expressed displeasure with WADA's sporting ban in international competition, calling the measures "unjust", as well as a ban on the Russian flag, national anthem, and name at Tokyo 2020, citing Western political pressure. One RT editorial in 2018 called WADA a conduit for "anti-Russian agendas".

Protests and Negative Sentiment

The Olympic Games have historically been used as a platform to amplify voices to current events as well as social causes. Thomas Bach, the President of the International Olympic Committee, received backlash due to his comments that athletes should not use the Olympic Games to stage political protests, such as wearing apparel associated with the Black Lives Matter (BLM) movement. Current events and social causes that are likely to be promoted by athletes and other Olympic Games participants have been highlighted below.

Black Lives Matter and Racial Justice Protests

BLM and the Olympics were in the news together in April 2021 when the IOC confirmed Rule 50 as described in a press release applied to BLM clothing, symbols, or gestures. This also includes, per an IOC-produced document from January 2020, kneeling and raised fists, which also attracted media attention at the time of the document's release. News sites in recent weeks have mistakenly summarized the decision, which included phrasing that appears to indicate that Rule 50 is new for the IOC or that the Japanese government had banned BLM representations specifically. Any BLM or similar demonstration will most likely come from the participating athletes at the Tokyo games. In addition to cautioning against the Tokyo Olympics on the basis of player safety due to COVID, the World Players Association, an athlete's union, stated in recent weeks that it would offer legal support to athletes who are penalized for political gestures. Though there were BLM protests in Japan in June 2020, we believe that protests and demonstrations by attendees, composed of Japanese citizens and residents, would likely focus on general opposition to the Olympics instead.

Uyghur, Hong Kong, and Anti-China Protests

In addition to other possible motivations for protests or disruption of the games, anti-China sentiment related to ongoing controversies about political events in Hong Kong or the treatment of the Uyghur ethnoreligious minority in China may also motivate demonstrations. Already, there are demonstrations and calls to boycott the 2022 Winter Olympics in Beijing over these issues, which will likely dominate narratives in China-related protests.

Domestic Japanese Opposition

In addition to global movements and events, there is also strong domestic opposition in Japan to hosting the Olympics. Recent polling by the Japanese magazine Asahi Shimbun showed that 83% of respondents oppose the Olympics, stating a preference for the games to either be canceled or postponed, with a narrow majority of those preferring the cancellation of the Olympics. This poll resembles similar surveys conducted in Japan in recent months. There have been numerous protests of varying sizes against the protests, primarily near the IOC's Tokyo headquarters. None of these protests has become violent as of the time of writing.

The primary motivation for opposition to the Olympics is fear of worsening the COVID-19 situation in Japan. The most cited additional concerns, per Recorded Future investigations in Japanese-language social media discussions on the topic of the Olympics, are anger at the Japanese government for not obeying Japanese public opinion and environmental damage caused by hosting the Olympics. On the latter, much of this discussion has centered on the Olympic Village. Environmentalist groups seeking to protest or disrupt the Olympics would likely place a higher priority on targeting the Olympic Village as compared to other possible targets given the number of high profile athletes and the Olympic Village being seen as the "heart" of the Olympic Games, though access to and from the Olympic Village will reportedly be closely monitored and restricted by organizers due to COVID-19.

Protests leading up to and during the games will likely center around the Japan Sport Olympic Square (JSOS), which houses the offices of the Japanese Olympic Committee (JOC). There have been small protests in recent weeks at the JSOS, and Recorded Future assesses the frequency and size of these protests will grow as the games draw near. Besides housing the JOC, the JSOS also contains the Japan Olympic Museum and sits adjacent to multiple Olympic venues, most prominently the Tokyo Olympics' main venue, the Japan National Stadium.

Figure 4: Image shared on social media planning protests on May 18 in front of the JSOS building (Source: Labornetjp)

Physical Threats

At the time of writing, Recorded Future has not observed any direct physical threats aimed toward the Tokyo Olympics or the athletes themselves. While physical attacks are unusual at Olympic events, they are not unheard of. The opportunities for threat actors to carry out physical attacks on spectators or athletes are likely reduced due to residual COVID-19 restrictions in Japan. Moreover, because of reduced crowd sizes, the potential effect of such attacks is reduced significantly.

Currently, all foreign nationals aside from those with residency status are barred from entering Japan. On June 20, 2021, Tokyo and 6 other prefectures entered into a quasi-state of emergency, which will last until July 11. Officials have since hinted that the imposition of more stringent state of emergency measures remains an option in the lead-up to the Games. The government also announced that it is aiming to allow domestic spectators to attend the Olympic games, although this figure at the time of writing was set to 10,000 people, not including delegates or sponsors.

On May 14, 2021, the Tokyo Organizing Committee of the Olympic and Paralympic Games announced that they would be reducing the number of visiting officials to 90,000 and that "only people who have a role to play, the operational role to play will be in Tokyo". This reduction was aimed toward visitors from the IOC and the International Paralympic Committee (IPC). Additionally, this reduction would also likely affect those associated with international sports federations, media outlets, sponsors, and their guests.

Outlook

Major international events such as the Olympics are prime opportunities for threat actors globally to spy on individuals and organizations of interest, embarrass the host country by disrupting the event, express political stances, or turn a profit through criminal activities. The upcoming 2020 Tokyo Olympic Games are no exception, although the threat landscape for this iteration of the Olympics looks considerably different from those of previous years due to the ongoing COVID-19 pandemic.

While COVID restrictions reduce the likelihood of physical threats and widespread disruptive protests, nation-states, criminals, and hacktivists alike are likely to remain motivated to conduct operations to achieve their various ends. For Russian APT groups, for example, which we believe the most likely state-backed actor set to target the Tokyo Games, disrupting the games is likely to be viewed as just retribution for the country's being banned from participating. For their part, ransomware gangs are likely to view the games as a lucrative target for extortion attacks, as extended downtime of key infrastructure is likely to have highly disruptive effects on the event. Finally, hacktivists, be they patriotic or motivated by particular moral grievances, likely view the Olympics as high-visibility opportunities to express their particular messages, but such activity has been in general decline for several years.

While state-sponsored and even ransomware gang activity is difficult to predict, as the games draw nearer, we expect threat actor chatter around the event to increase, additional typosquat or Olympics-themed domains to be registered and become active in credential-harvesting and malware campaigns, and discussions of planned protests to increase.

Appendix A

A list of the observed Tokyo Olympics-themed domains is provided below:

2021olympic[.]cn
2021olympics[.]jp
2021olympicupdates[.]com
2021olympicupdates[.]live
2021olympicupdateslive[.]com
cancel-olympic[.]tokyo
cxaolympicgames2021[.]org
lost-olympic[.]tokyo
no-olympic[.]tokyo
olympic2020[.]in
olympic2020in[.]tokyo
olympic2021[.]in
olympicgames2021[.]cn
olympicgames2021.co.za
olympicnewstokyo[.]com
olympics2020[.]icu
olympics2020[.]in
olympics2020[.]vip
olympics2021[.]in
olympicsjapan2021[.]in
olympicvirtual2021[.]com
perrigoselfcareolympics2021[.]com
stop-olympic[.]tokyo
summerolympics-2020[.]org
teamnl2020-olympic-paralympic[.]games
the2021olympicgames[.]com
the2021olympicgames[.]org
the2021olympicstokyo[.]com
theolympicstokyo2021[.]com
tokyo----olympics[.]org
tokyo---olympics[.]org
tokyo--olympics[.]org
tokyo-olympicslive[.]com
tokyoolympicplay.blogspot[.]com
tokyoolympicplay[.]com
tokyoolympics[.]org
tokyoolympicsfootballlive[.]com
tokyoolympicsolympics[.]com
tokyoolympicsplay.blogspot[.]com
tokyoolympicsport[.]com
tokyoolympicswaterpololive[.]com
tokyotokyoolympics[.]com
usolympics2020[.]com
usolympics2021[.]com

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.