CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 4, 2024

Hurdling over Hazards: Multifaceted Threats to the Paris Olympics

Physical security threats — including terrorism, violent extremism, civil unrest, and disruptive protests — pose the greatest risk of harm and disruption to the 2024 Paris Olympic Games.

State-sponsored actors are likely to escalate cyber-espionage and influence operations to gather information on targets and amplify narratives critical of France, NATO, and Israel, respectively.

The Paris Olympics and supporting entities will attract the attention of hacktivist collectives, and cybercriminals are expected to extort ransomware payouts and conduct Olympic-themed scams.

Executive Summary

The 2024 Paris 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 makes the Paris Olympics a target for those seeking to cause ideologically motivated harm or disruption, enrich themselves through criminality, or embarrass the host nation on the international stage. Insikt Group identified the following high-priority threats to the 2024 Paris Olympic Games based on an assessment of a broad range of past attacks, existing identified threats, and the general geopolitical context. Overall, we assess that physical security threats — including terrorism, violent extremism, civil unrest, and disruptive protests — pose the greatest risk of harm and disruption to the 2024 Paris Olympic Games.

- **State actors will likely escalate espionage and influence operations behind the scenes:** The international prestige associated with Olympic Games glory (as well as France's North Atlantic Treaty Organization [NATO] membership) is likely to restrain state-sponsored cyber disruption. Behind the scenes, however, state-sponsored actors are likely to escalate espionage operations, potentially using Olympic-themed lures or infrastructure to gather information about targets of interest. Influence operations networks based in Russia, Iran, and Azerbaijan are also likely to work overtly and covertly to amplify narratives critical of France, NATO, and Israel.
- **Criminals will use the Paris Olympics to go for (your) gold:** We expect to see cybercriminals take advantage of the pressures facing a host city to extort ransomware payouts against the government, hospitality, transportation, logistics, and healthcare sectors. In addition, Olympic-themed phishing lures and scams will almost certainly target businesses and attendees alike. Entities involved in Olympic operations should make extra efforts to raise awareness of phishing and prioritize the patching of high-risk vulnerabilities exploited by threat actors mentioned in this report.
- **Hacktivists will very likely attempt cyber disruptions to protest support of Ukraine and Israel:** With active conflict ongoing in Europe and the Middle East, hacktivist groups will almost certainly try to leverage the international attention on the Paris Olympics by conducting generally nuisance-level disruptive cyberattacks. While most hacktivists do not have the capability to cause an actual impact on events, a few groups with purported ties to the Iranian government have been more effective in carrying out disruptive "hacktivist" attacks. Organizations should be prepared for heightened distributed denial-of-service (DDoS) activity, website defacements, and potential wiper malware disguised as a ransomware attack.
- **Heightened security measures will limit opportunities for terrorists and violent extremists:** Islamic State (IS) and al-Qaeda supporters in Europe almost certainly intend to target the Paris Olympics, as reflected by the French government raising the country's terrorism threat assessment system (Vigipirate) to its highest possible level, but the event's extensive security footprint will very likely mitigate the probability and impact of a successful attack. Nevertheless, public reports of a foiled attack can have a psychological impact on attendees of the Paris Olympics and disrupt the Games. Event organizers should monitor online forums and messaging

applications popular with al-Qaeda and IS to identify potential attack vectors and suggested targets.

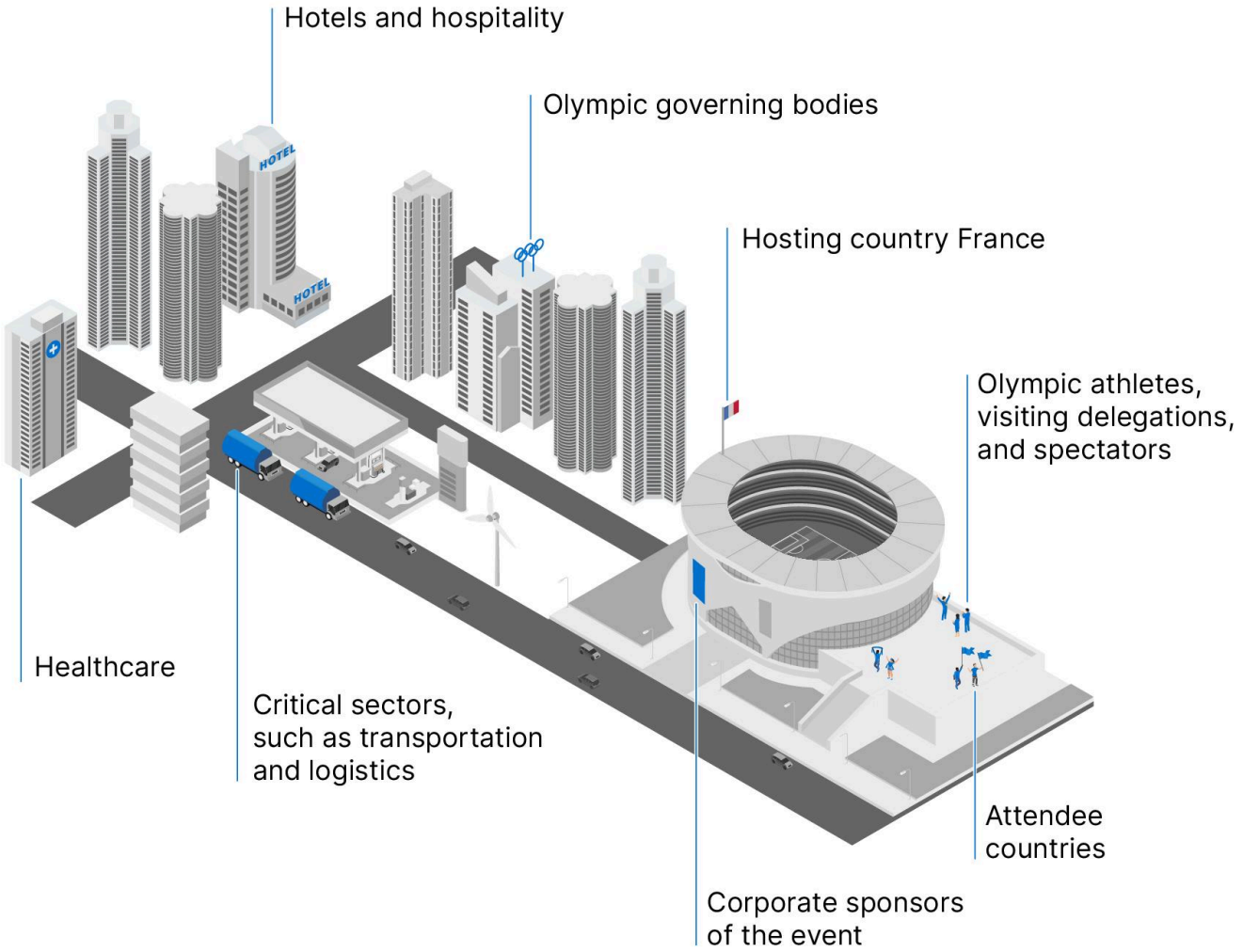

Figure 1: *Targets of threat activity during the 2024 Paris Olympic Games (Source: Recorded Future)*

While we expect the most likely cyber disruptions to come from hacktivists or criminal groups seeking attention or profit, respectively, geopolitical developments could shift the threat landscape to make a significant event more likely. Developments in Russia's war against Ukraine — such as a deterioration of Russia's battlefield position or a significant rise in French lethal aid to Ukraine — could trigger escalatory action from Russian state-sponsored or hacktivist proxy groups. Similarly, events related to the Israel-Hamas conflict that cause uproar, particularly ones that coincide with the running of the Paris Olympics, risk turning disruptive protests into violent riots and could increase motivation for cyber or physical attacks against French or Olympic infrastructure from hacktivists, terrorists, violent extremists, or state proxy groups. We recommend closely monitoring for increased tensions in Europe and the Middle East to anticipate increased risk of cyber or kinetic attacks.

Key Findings

- Russia, China, and Iran are likely to leverage Olympic-themed phishing lures or infrastructure to carry out espionage activities during the Paris Olympics. Insikt Group assesses that Russia is the most likely of those three to attempt to carry out a disruptive or destructive cyberattack due to its past targeting of the Olympic Games and ongoing grievances against France, NATO, and the International Olympic Committee (IOC); however, this activity will likely be restrained by France's NATO membership.
- North Korea also likely lacks the requisite motivation to target the Olympics directly and almost certainly remains primarily interested in revenue generation for the regime. Nevertheless, North Korea is increasingly strategically aligned with Russia, as demonstrated by its material support for Russia's war in Ukraine, and this alignment may introduce the risk of false-flag or proxy cyberattacks.
- The Paris Olympics and supporting organizations will very likely attract the attention of hacktivist collectives — including Russia-nexus, Iran-nexus, and Palestine-nexus groups — as a result of France's support to Ukraine and Israel. Activity will likely consist of opportunistic attacks such as high-volume, low-impact DDoS attacks and website defacements that adopt pre-existing hacktivist campaign brands (such as "#OpFrance" and "#FuckNATO").
- Ransomware groups and the adjacent criminal ecosystem (such as initial access brokers and infostealers) almost certainly see the 2024 Paris Olympic Games as a lucrative opportunity and are likely to take advantage of the pressures faced by relevant local sectors, including hospitality, transportation, and government, to carry out cyberattacks.
- Russian, Azerbaijani, and Iranian influence operations are very likely to leverage the international attention on the Paris Olympics to amplify narratives critical of or embarrassing to France.
- Terrorists and violent extremists are almost certainly plotting to carry out violent attacks, though the extensive security infrastructure in place for the event will make a successful mass-casualty attack very unlikely.
- A significant array of protest groups — including environmental activists, pro-Palestinian supporters, farmers, and labor union members — will almost certainly seek to attract attention to their causes by disrupting the 2024 Paris Olympic Games. While these protests will likely be mostly peaceful and primarily result in moderate impediments to traffic and transportation networks, environmentalist agitators and those opposing Israel's participation in the Paris Olympics are the most likely to engage in forceful clashes with security forces or counter-protesters.

***Figure 2**: Multifaceted threats to the 2024 Paris Olympic Games (Source: Recorded Future)*

State-Sponsored Cyber Threats

The Olympic Games, as well as other large-scale international sporting events, are attractive targets for state-sponsored advanced persistent threat (APT) groups engaged in cyber-espionage or disruption operations. These events attract significant numbers of attendees, including high-profile government officials and businesspersons, making the event a target-rich environment for espionage-motivated threat actors. Moreover, hosting a successful event affords a significant amount of international prestige, meaning that any disruption to the event can prove highly embarrassing for the host government and organizers. As a result, state-sponsored threat groups have targeted the Olympic Games or affiliated organizations in the past in the pursuit of differing national objectives or used Olympics themes in espionage campaigns.

Insikt Group, as of this writing, is not aware of imminent, planned, or ongoing state-sponsored threat activity linked to known APT groups targeting the upcoming 2024 Paris Olympic Games, its organizers (such as the International Olympic Committee [IOC]), sponsors, or other entities. We cannot rule out, however, limited activity closer to the date of the opening ceremony (July 26, 2024), whether it be the registering of malicious Olympic-themed domains or Olympic-themed lure documents and spearphishing emails that may be staging for state-sponsored attacks.

A significant factor moderating the likelihood and risk tolerance for governments with a potential interest in disrupting the Paris Olympics via cyberattack is the hosting of this year's Olympic Games in France, a key NATO member. In 2022 following the onset of Russia's full-scale invasion of Ukraine, NATO officials made an announcement that the alliance had determined that cyberattacks could theoretically trigger the Article 5 collective security clause of the NATO charter. As a result, any government weighing the benefits and risks of carrying out such an operation must account for the possibility of undesirable escalation, reducing the likelihood of severely disruptive cyberattacks by state-sponsored APT groups.

In this section, we review the likely motivators for APT groups' targeting of the upcoming Paris Olympics, with a focus on the most prominent state-sponsored threat actors — those linked to Russia, China, Iran, and North Korea. We conclude that Russia almost certainly has the greatest motivation and capability to launch disruptive attacks against the event, but it will need to weigh the risk of further damaging relations with France and prompting a NATO-led response. China, Iran, and North Korea are unlikely to possess significant motivation to disrupt the Olympic Games but have their own foreign or domestic security reasons to either conduct espionage during the Paris Olympics or opportunistically make use of Olympic-themed infrastructure and lures.

Russia

The Russian government almost certainly has both the intelligence-driven requirements and requisite motivation to launch state-sponsored cyber-espionage and/or disruption operations against the Paris Olympics. Moreover, Russian APT groups have in the past demonstrated both the capability and intent

to carry out such attacks against international sporting events and organizers, including the Olympics, on multiple occasions.

Moscow almost certainly harbors significant grievances against the French government and the IOC for their stances on Russia's war against Ukraine and the treatment of Russian athletes, respectively. For its part, France, under the increasingly outspoken President Emmanuel Macron, has proven a staunch ally of Ukraine in its defense against Russia's invasion. France has and continues to provide Kyiv with significant amounts of military equipment and aid, advocates for continued support from NATO allies, and in February 2024, inked a ten-year bilateral security agreement with Ukraine. Most recently, President Macron angered the Kremlin by articulating a willingness to deploy French troops to Ukraine in an undefined future contingency in order to prevent the country from capitulating to the Russian military, which could put France in direct military conflict with Russia. Finally, Paris mayor Anne Hidalgo has been quoted as saying that Russian and Belarusian athletes "were not welcome" at the upcoming Olympic Games.

Additionally, in response to Russia's invasion of Ukraine, the IOC banned the Russian Olympic Committee outright and determined that Russian and Belarusian athletes would compete in the Paris Olympics as neutral parties rather than representing their home countries, stripping them of the international prestige gained from their athletes medaling in the event. Russia has reacted strongly to both the IOC's sanctions against it and French officials' statements, with Russian Foreign Ministry spokesperson Maria Zakharova stating that the IOC has "slipped into racism and neo-Nazism" and calling on the event to be relocated out of France as a result.

While Insikt Group has not, as of this writing, observed indications of preparations for Russian APT attacks against infrastructure or organizations associated with the upcoming Paris Olympics, Russia has a long history of targeting international sporting organizations and the Olympics themselves in retribution for similar bans against its athletes' participation, including:

- 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 OlympicDestroyer malware
- BlueDelta'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 of 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

Due to the above set of grievances with both the host country, France, and the IOC, Moscow likely sees substantial gain in targeting the upcoming Olympic Games in some form, be it through disruption of the event itself and/or heightened espionage activity against those in attendance or associated organizations. Despite this, however, Moscow's calculus in determining whether or not to carry out

destructive or disruptive attacks is likely to be moderated by a 2022 NATO declaration that cyberattacks against a member state could be eligible for triggering the Article 5 collective security clause of the NATO charter.

The Kremlin has the option of relying on Russian cybercriminals or pro-Russia hacktivists, to disrupt the Paris Olympics while maintaining plausible deniability, or instead focusing on its influence operations that seek to discredit and undermine the Games. Alternatively, Russian APT groups could launch a disruptive attack, possibly under the guise of a hacktivist front. For example, BlueDelta's false flag compromise of French television network TV5 Monde in May 2015 disrupted the network's broadcasts for three hours and BlueDelta acted under a false persona, calling itself the Cyber Caliphate and claiming allegiance to the Islamic State. This type of attack could disrupt some broadcasting of the Paris Olympics and cause reputational and financial damage to the broadcaster, in addition to being part of a cyber-enabled influence operation that has an immediate psychological impact on athletes and attendees concerned about the safety of the event and subsequently tarnishes the Games.

Given both past behavior as well as what is known of tasking remits, the Russian APT groups most likely to be engaged in disruptive operations against the Paris Olympics are assessed to be Sandworm (APT44, Seashell Blizzard) and/or BlueDelta (APT28, Forest Blizzard, Fancy Bear), while BlueBravo (APT29, Cozy Bear, Midnight Blizzard) and Turla (Secret Blizzard, Venomous Bear, Waterbug) are most likely to be tasked with traditional cyber-espionage or hack-and-leak operations.

China

While Beijing maintains a formidable cadre of sophisticated state-sponsored APT groups, it is very unlikely to deploy these capabilities to disrupt the upcoming Paris Olympics. Unlike their Russian counterparts, there is no historical precedent for Chinese APT 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 in general, despite recent evidence of likely pre-positioning within critical United States (US) infrastructure by Volt Typhoon.

Despite some key differences, such as stances on the war in Ukraine, France and China currently enjoy relatively stable and positive diplomatic and economic relations. President Macron and other high-ranking French officials recently traveled to China on state visits, and Chinese president Xi Jinping visited France in early May in advance of the Paris Olympics. Moreover, President Macron previously declined to participate in an international boycott of the 2022 Beijing Olympics — a move that broke with many of France's allies and was viewed favorably by Chinese officials. Finally, the Olympic Games are a source of significant national pride for China, as its athletes routinely medal well in the Olympics, and are expected to win the most medals in the Paris Olympics alongside the US. As a result, China's launching of disruptive attacks that jeopardize either the current positive trajectory of French-Chinese relations or China's own success in the Paris Olympics is very unlikely.

Nevertheless, those groups tasked with the collection of foreign intelligence, and particularly those under the Ministry of State Security (MSS) — China's primary civilian intelligence service — are likely to

engage in some level of opportunistic cyber-espionage operations against select attendees or Olympic-affiliated organizations, or to use the Olympics as themes for either malicious domains or lures. While we have no indications of such campaigns at this time, based on previous targeting patterns, these threat groups may include, but are not limited to:

- RedBravo (APT31, Violet Typhoon, Judgement Panda)
- RedDelta (Twill Typhoon, Mustang Panda)
- RedHotel (Charcoal Typhoon, Aquatic Panda, Earth Lusca)
- RedGolf (APT41, Brass Typhoon, Wicked Panda)
- APT40 (Gingham Typhoon, Kryptonite Panda, Leviathan)
- TAG-88 (APT15, Nylon Typhoon, Vixen Panda)

Iran

Despite substantial tensions in the French-Iranian relationship, such as France's late-2023 decision to retain sanctions against Iran's nuclear program, France's continued support for the dissident group the Mujahedeen Khalq Organization (MKO), and Paris's complicated approach to the ongoing Israel-Hamas conflict, Iran is unlikely to seek to disrupt the Paris Olympics via destructive or disruptive cyberattacks. Such attacks would not only risk potential escalation with the NATO bloc during a period of already heightened regional tensions, and contradict Iran's signals of a desire to de-escalate with Israel, but may also result in the imposition of additional sanctions on an already struggling Iranian economy.

Iranian APT groups have not been previously identified launching destructive cyberattacks or cyber-espionage intrusions against the Olympics or organizations associated with sporting federations. Moreover, Iranian athletes are still scheduled as of this writing to compete in the Paris Olympics under the Iranian flag, despite calls from some critics of the Iranian government to ban them due to the regime's human rights abuses.

This does not, however, preclude Iranian APT groups from leading espionage intrusion attempts against organizations supporting the Paris Olympics or people attending them. At least four known Iran-nexus threat actors — Charming Kitten (Mint Sandstorm), APT42, MuddyWater (TEMP.Zagros, Mango Sandstorm, Static Kitten), and APT34 OilRig (Twisted Kitten, Cobalt Gypsy) — maintain intelligence and counterintelligence requirements that could lead them to launch cyberattacks against organizations and individuals attending the 2024 Paris Olympics.

For example, contracting entities associated with Charming Kitten have been reported to seek strategic and tactical information and have also undertaken counterintelligence operations at the behest of the Islamic Revolutionary Guard Corps (IRGC), including in attacks against international conferences and related organizations such as the Munich Security Conference and Think20 Summit in Saudi Arabia.

Groups like APT34 OilRig, APT42, and MuddyWater routinely carry out operations (1, 2, 3) against Western and Middle Eastern governments and private sector companies in support of Tehran's economic, political, and military objectives. In the context of the Paris Olympics, these operations are

most likely to be directed against high-profile foreign attendees of the event and dissidents and/or critics of the Iranian regime. Due to significant threats emanating from infiltration, subversion, and anti-Iranian government activity, it is likely that APT34 OilRig and MuddyWater will be involved in counterintelligence operations at the behest of their sponsoring government agency — the Ministry of Intelligence and Security (MOIS).

Apart from traditional state-backed cyber-espionage groups, pro-Iranian "hacktivist" groups with nebulous ties to the regime — such as Fatemiyoun Electronic Team, CyberAv3ngers, Pink Sandstorm (BlackShadow, AGRIUS), and Soldiers of Solomon, just to name a few — may use the Paris Olympics as an opportunity to launch hacktivist attacks against the French government and private businesses. In such a scenario, it is likely that groups like the Fatemiyoun Electronic Team will adopt an anti-Israeli stance (as they have since the October 2023 war) to launch attacks against French businesses.

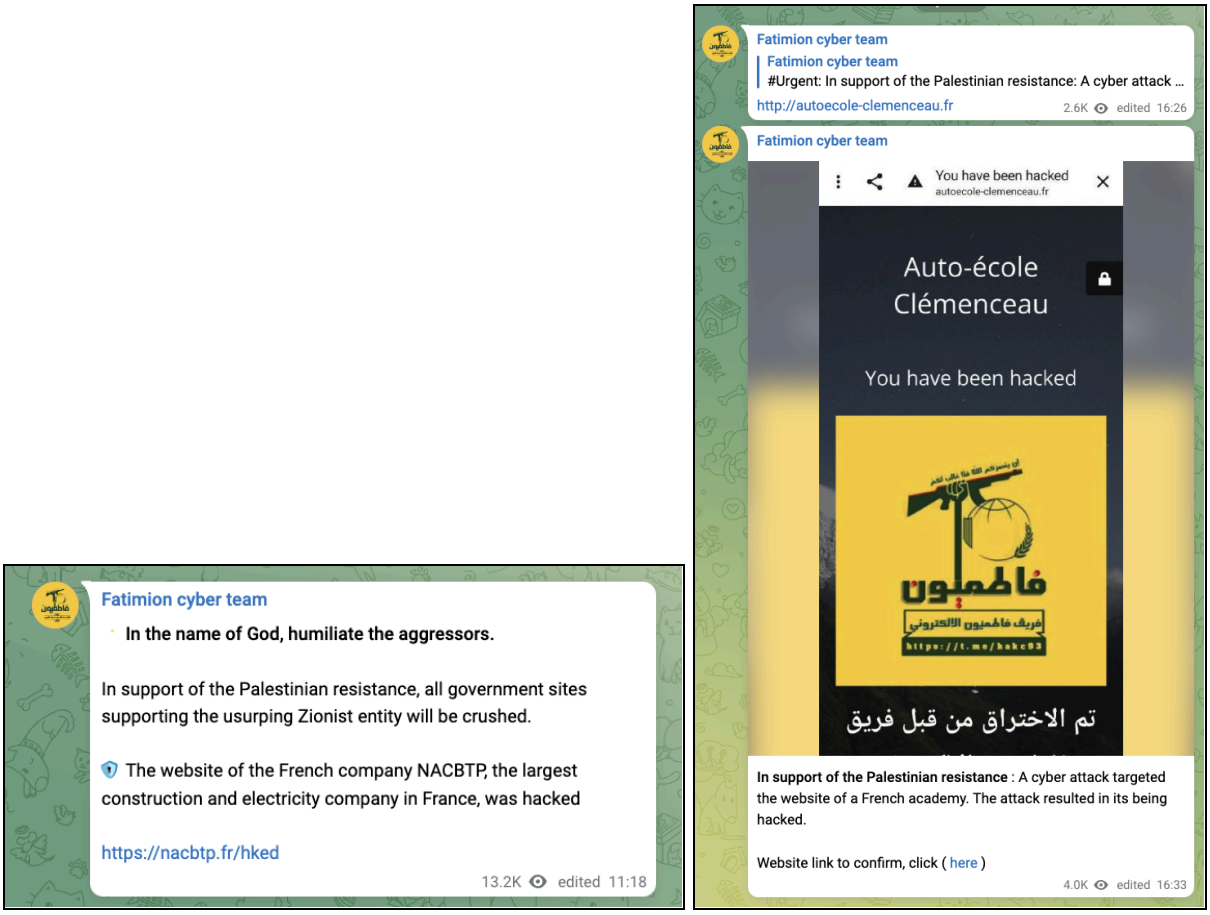

Figure 3: *Claims identified via the Fatemiyoun Telegram channel indicate the group attacked French organizations as part of its anti-Israeli operations (Source: Telegram)*

North Korea

Although North Korea and France lack formal diplomatic relations and France is a supporter of sanctions on Pyongyang, North Korean state-sponsored APT groups are unlikely to conduct disruptive or destructive attacks against the upcoming Paris Olympics.

The 2024 Olympics will mark Pyongyang's return to the Olympics following the country's withdrawal from the 2020 Tokyo Olympics during the COVID-19 pandemic and its subsequent IOC-imposed ban on participation in the 2022 Beijing Winter Olympics. While North Korea only generally sends a small contingent of competitors to the Olympics, as one of the only international events that North Korea is regularly involved in, its athletes' participation is a significant source of national pride and pro-regime propaganda; as a result, the government has an interest in Paris Olympics remaining uninterrupted.

Further, there is very limited precedent for North Korea-linked APT groups targeting international sporting events or organizations. There is one instance in which such targeting was observed — in a campaign using the fileless malware "Gold Dragon" targeting Olympic-related organizations in the period surrounding the 2018 Winter Olympics in Pyeongchang, South Korea. This malware was subsequently attributed to APT37 (Cloud Dragon, Scarcruft) based on code overlap with other known North Korea-nexus malware. The campaign was likely focused on intelligence-gathering, which is consistent with the majority of North Korean state-sponsored cyber campaigns against South Korea and likely a part of North Korea's routine intelligence operations.

The majority of North Korean state-sponsored APT campaigns focus on revenue generation for the regime and consist of compromises of financial institutions, ATM cash-out schemes, or the targeting of cryptocurrency exchanges. Apart from ransomware or other forms of extortion attacks, such as the WannaCry campaign, disruptive or destructive attacks are difficult to monetize and, thus, are likely of less interest and priority to the regime.

North Korea's increasingly close relationship with Russia, however, adds a layer of uncertainty and the possibility for false-flag or proxy attacks similar to the Olympic Destroyer attacks against the Pyeongchang Olympics. That incident was eventually attributed to the Russian APT group Sandworm, but the group attempted to frame North Korea for the attack. There are at least two plausible scenarios in light of the emerging North Korean-Russian strategic alignment:

- North Korean APT groups launch destructive or disruptive attacks directly against the Paris Olympics at the behest of Russia, with both sides calculating that France and its allies would struggle to mount a significant diplomatic, economic, or military response to the incident given the international sanctions and restrictions already in force on North Korea and hesitancy to escalate.
- Russian APT groups launch such attacks against the Paris Olympics themselves and once again attempt to frame North Korea, similarly assessing that potential blowback would be minimal due to the plausible deniability afforded by a false-flag attack.

At this time, there is no indication that such dynamics are at play, and given North Korea's involvement in this iteration of the Olympic Games, it is unlikely that Pyongyang would be willing to play an active role without Russia offering something significant (such as assistance with satellite or ballistic missile development, economic aid, and so on) in return for their involvement.

Cybercriminal Threat Activity

Ransomware Threats

Owing to its complex, high-profile, and international characteristics, the 2024 Paris Olympic Games presents an ideal opportunity for financially motivated cybercriminals to commit ransomware attacks. Companies involved in the event will be under significant pressure to maintain uninterrupted service and less prone to tolerate any downtime of core infrastructure that can disrupt proceedings and damage reputations. Ransomware threat actors could use the situation to their advantage, leveraging companies' urgency to quickly restore operations to extort high ransom payments. Considering that ransom payments have been steadily decreasing since the latter half of 2023, with fewer victims choosing to pay, there likely is a strong appetite among extortionists to seek high-leverage targets — with the Paris Olympics offering such opportunities.

Although the targeting of an Olympic committee by ransomware is not unprecedented, we believe it is more likely for ransomware threat actors to target organizations that support the Paris Olympics instead of the IOC or the International Paralympic Committee (IPC). We believe that sectors such as transportation and logistics, healthcare, hospitality, and public service — rather than the event itself — will all come under additional pressure in the months leading up to and throughout the duration of the Paris Olympics — as Paris welcomes fifteen million expected tourists. Speaking to this assessment, these and other critical sectors routinely fall in the crosshairs of ransomware threat actors, with French government, transportation, and healthcare organizations having been routinely claimed as victims on ransomware extortion websites since the beginning of 2023 (**Figure 4**).

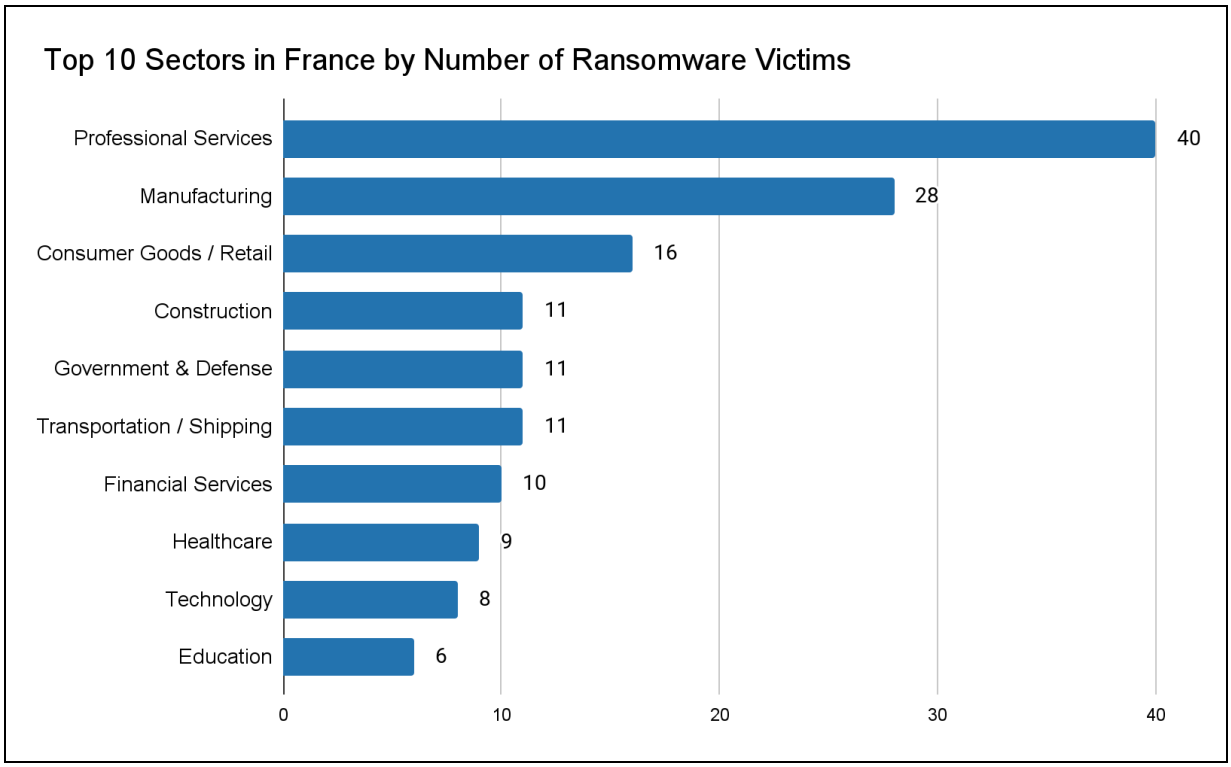

***Figure 4**: Top ten sectors ransomware threat actors targeted in France since the beginning of 2023 (Source: Recorded Future)*

Successful ransomware intrusions targeting the Paris Olympics or organizations supporting the event will degrade the availability of information technology (IT) systems and lead to data breaches — as part of "double extortion" attacks, whereby ransomware threat actors threaten to disclose stolen information as additional leverage. That said, it is also possible such attacks will be accompanied by additional extortion methods that seek to damage the reputation of the Paris Olympics, incur financial losses for participating organizations, and cause widespread panic among observers. For instance, it is not uncommon for ransomware threat actors to pair data encryption and exfiltration with DDoS attacks, website defacement attacks, "doxxing", executive harassment, and other public-facing attacks, to impose further reputational harm and pressure victims.

Depending on factors such as a target's security posture, threat actors' sophistication, data sensitivity, and legal and reputational fallout, ransomware intrusions can have varying consequences for victims. These can range from temporary disruptions and easily recoverable data encryption to severe outcomes like permanent data loss and a complete halt of critical business operations. Recent incidents involving companies in sectors such as healthcare, hospitality, and logistics, including in France, showcased some of these more detrimental scenarios:

- On April 25, 2024, the French city of Gravelines reported suffering a ransomware incident that forced its operations to revert to pen and paper for at least one week. Gravelines's officials also reported disruptions to municipal services, such as its city hall, Centre Communal d'Action Sociale, media library, and equestrian center, due to mitigation measures undertaken to contain

and remediate the incident.

- In mid-April 2024, the French medical institution Hospital Simone Veil (CHC-SV) disclosed that it suffered a cyberattack that forced staff to revert to pen and paper, cancel non-urgent procedures, and transfer some patients to nearby hospitals. Although we did not identify any ransomware group claiming the attack, the broad disruption experienced by CHC-SV aligns with what is commonly observed in the wake of ransomware intrusions. In December 2022, for example, the André-Mignot teaching hospital in Versailles shut down phone and computer systems and transferred six patients from its neonatal and intensive care units to other healthcare facilities after falling victim to ransomware.

- In early April 2024, US hospitality chain Omni Hotels & Resorts suffered a cyberattack that significantly disrupted the availability of reservation, hotel room access, and point-of-sale (POS) systems. The incident was subsequently claimed by the Daixin ransomware group, which threatened to leak stolen information if not paid a demanded ransom.

- In early October 2023, US freight transportation provider Estes Express suffered a cyberattack that affected communications systems and prevented the company from correctly tracking and tracing freight. In early November 2023, LockBit claimed the attack, adding Estes Express to its extortion website and leaking information allegedly stolen from the company's systems.

We note, however, that the level of disruption to the Paris Olympics will almost certainly vary based on the critical role played by the targeted organization, and there is almost no chance of a complete halt of the Paris Olympics due to a single intrusion or a large and coordinated campaign. This is because many aspects underpinning the Paris Olympics' correct functioning are separate from one another, meaning that if a key partner or company supporting a function adjacent to the Paris Olympics, such as hospitality, is forced to slow down operations due to ransomware, this is unlikely to affect the overall proceedings. Additionally, we do not anticipate seeing large and coordinated ransomware operations. While some ransomware groups favor "big game hunting", targeting organizations with financial thresholds to extort high sums of money, ransomware threat actors remain largely opportunistic in their targeting rationale, pursuing low-hanging fruit.

Initial Access Brokers

The 2024 Paris Olympic Games represent an opportunity for financially motivated cybercriminals, including initial access brokers (IABs). IABs are specialized threat actors that sell remote access to compromised corporate networks on dark web forums and via private communication channels, which in turn can be used to conduct account takeovers (ATOs), data theft, and espionage operations, as well as propagate malware infections — including ransomware. Common initial access methods include corporate virtual private networks (VPNs), remote desktop protocol (RDP) services, Citrix gateways, web applications and content management systems (CMS), and corporate webmail servers. IABs may obtain these methods by utilizing a range of tactics, techniques, and procedures (TTPs) including infostealer malware or purchasing infostealer logs from automated dark web shops (such as Russian

Market and 2Easy Shop), credential stuffing, phishing, and RDP brute-force attacks, some of which are discussed further below.

We expect the increased appetite among ransomware operators for high-leverage targets, such as key organizations that support the Paris Olympics, to create an increased incentive for IABs to successfully obtain remote access to those entities.

Top-tier forums, such as Exploit and XSS, are popular platforms where IABs advertise initial access methods to prospective buyers. Initial access advertisements typically adhere to a standard format where the name of the victim organization is withheld or obscured while other details related to the victim are provided for the buyer's benefit — such details can include the victim organization's country, annual revenue, or industry sector, the type of access being offered, user rights available (for example, domain admin or Workgroup admin), and more. Since the victim organization's name is obfuscated, it is often not possible to definitively identify the victim organizations from forum posts. However, monitoring dark web forum posts and Insikt Group threat leads related to organizations in France — as well as relevant industries — can provide additional details about the types of initial access methods that are being sold on dark web forums.

From January 1, 2024, to April 29, 2024, Insikt Group produced 17 threat leads related to advertisements of initial access methods for French entities, and 14 threat leads related to relevant industries, including sports, entertainment, and hospitality. The types of listings that were advertised include access to RDP services, web shells, file transfer protocol secure (FTPS), and a customer relationship management (CRM) system with administrator privileges. At this time, Insikt Group is not able to identify if the organizations and companies targeted by these threat actors are involved in the Paris Olympics; we will include any additional details, including the name of the victim, that we are able to gather from proprietary sources when possible.

Infostealers and Credential Leaks

Compromised credentials, either harvested via information stealer ("infostealer") malware or dark web data dumps, is the primary way for cybercriminals to obtain initial access into a targeted organization. We assess that the volume and value of credentials affecting the Paris Olympics will likely increase in the months preceding the event, to meet threat actor demand. From January 1, 2024, to April 29, 2024, we identified approximately 624 references to compromised credentials on dark web shops and marketplaces affecting domains associated with the 2024 Paris Olympic Games — including *olympics[.]com*, *paris2024[.]org*, and *paralympic[.]org*, among others. At this time, we cannot determine whether the victims of these infostealer infections are employees of the IOC or IPC. In one instance, we identified compromised credentials affecting an email account associated with a Paris Olympics domain. This account is likely related to a current employee, but we cannot confirm this. Compromised email accounts associated with IOC or IPC employees could result in social engineering, business email compromise (BEC), spearphishing, and other attack vectors that could allow a threat actor to move laterally across networks and within organizations.

Phishing and Scams

As highlighted in our 2020 Tokyo Olympics and 2022 Winter Olympics reports, phishing and smishing will almost certainly be popular attack vectors used by cybercriminal threat actors to disseminate credential- and personally identifiable information (PII)-harvesting malware via traditional email and SMS messages. Similar to our previous findings, these phishing and smishing messages will include "use of urgent language in emails, the impersonation of executives or vendors, and the use of malicious websites posing as vendors or ticketing systems". Although detection of phishing-related activities across criminal-related sources has been limited over the last four months, we have observed typosquat registrations of Olympic Games domains and we anticipate an increase in Olympic-themed phishing campaigns and scams as the beginning of the Paris Olympics approaches.

Hacktivism

The 2024 Paris Olympic Games and associated supporting organizations — including corporation sponsors — will very likely attract attention from hacktivist collectives, given the current geopolitical climate that has resulted in a resurgence of hacktivism in the past two years. Hacktivists are largely ego-driven threat actors of low credibility whose alleged attacks frequently cause greater reputational damage than actual service disruptions or long-term impacts on targeted domains or entities. France has historically been targeted with DDoS and website defacement attacks via larger collaborative hacktivist campaigns such as #OpFrance, which dates back to 2015, and the pro-Russian hacktivism campaign #FuckNATO, which originated in 2022. While these pre-established hacktivist campaigns are not directly intertwined with the Paris Olympics, we assess that Russia-nexus or Palestine-nexus hacktivist groups may leverage these existing campaigns and hashtags to publicize or amplify any attack targeting France preceding or during the Paris Olympics. As hacktivism is an ideologically reactionary cyber threat, hacktivist groups and collectives may claim responsibility for DDoS or website defacement attacks targeting France in response to French laws, regulations, sporting restrictions, or evaluations of their home countries' team performance that are perceived by these groups to be "Russophobic", "anti-Palestine", "pro-Israel", or "Islamophobic".

Pro-Russian Hacktivist Groups Targeting France

Pro-Russian hacktivists will likely regard hacktivist activity targeting France and the Paris Olympics as a proportionate response to the increasing isolation of Russia and Belarus from international sporting events and France's support of Ukraine. In 2017, the IOC banned Russia from the PyeongChang 2018 Winter Olympics amid an ongoing doping scandal. Despite this ban, the IOC allowed 168 Russian athletes to compete as "Olympic Athletes from Russia". Similarly, in 2023, the IOC banned Russian and Belarusian athletes from competing as official representatives of their retrospective states but will allow Belarusian and Russian citizens to compete as "neutral athletes" who participate "without an accompanying national flag or anthem" at the Paris Olympics. Pro-Russian hacktivists, such as NoName057(16), Russian Cyber Army, UserSec, Dark Storm Team, Anonymous Sudan, Killnet, and 22C, have historically cited various geopolitical events that they perceive as "anti-Russian" as the catalyst for their DDoS or website defacement campaigns. Using the Recorded Future Intelligence Cloud, we

observed the following notable instances of pro-Russian hacktivist activity targeting France over the past year:

- On March 11, 2024, the French government confirmed that a series of DDoS attacks of "unprecedented intensity" had targeted multiple French government ministries. Insikt Group reported on March 12, 2024, that pro-Russian hacktivist group Anonymous Sudan claimed responsibility for attacks on the French Interministerial Directorate of Digital Affairs, impacting over 17,000 IP addresses and devices and over 300 domains. We note that Anonymous Sudan's alleged DDoS activity has declined significantly since March 2024 and that the group has not claimed responsibility for any DDoS attacks or posted on its main Telegram channel since March 19, 2024, or on its backup channel since March 12, 2024.

- Between March 11 and March 12, 2024, pro-Russian hacktivists NoName057(16), Russian Cyber Army, UserSec, and 22C claimed responsibility for a series of DDoS attacks on specific French entities:
    - Électricité de France (EDF): The largest operator of nuclear power plants, essential for energy production and distribution
    - The City of Bordeaux: A city in southwestern France known for its wine industry, and a hub for aerospace, digital, and logistics sectors
    - Région Normandie (Normandy Region): An administrative region in France known for its history, agriculture, manufacturing, and key trade ports
    - Conseil Régional de Guadeloupe (Regional Council of Guadeloupe): Manages Guadeloupe, a French Caribbean region, overseeing education and infrastructure essential for its development

- In addition to the aforementioned alleged hacktivist campaigns, NoName057(16) has historically posted content antagonizing French president Emmanuel Macron. For example, the group shared an AI-generated meme that critiqued President Macron's masculinity on its Telegram channel on March 14, 2024.

Middle Eastern-Nexus Hacktivist Groups Targeting France

Following Hamas's October 7, 2023, attack on Israel and the ensuing Israel-Hamas conflict, the IOC has faced backlash and allegations of inconsistency over the participation of Israeli athletes in the 2024 Paris Olympic Games. The inclusion of Israeli athletes and France's support for Israel is very likely to trigger retaliatory hacktivist activity by pro-Palestinian groups, with the IOC, French government entities, and corporate sponsors of the Paris Olympics that are viewed as being pro-Israel likely to be primary targets.

We have observed several notable instances of Middle Eastern-Nexus hacktivist groups targeting French government entities during the past year, as detailed below. Although most groups are assessed to have low credibility and a tendency to overstate the impact of their attacks, they will almost certainly view the Paris Olympics as an opportunity to gain notoriety while simultaneously spreading fear,

uncertainty, and doubt. As such, we anticipate an uplift in Middle Eastern-Nexus hacktivist activity directed against French and Olympic-linked entities preceding and during the Paris Olympics. This is expected to remain largely limited to high-volume, low-impact DDoS attacks and website defacements targeting the IOC, partnered organizations and Olympic sponsors, and French government bodies.

Turk Hack Team

Turk Hack Team (THT) has an established history of targeting French government entities. On June 22, 2023, the group claimed responsibility for a DDoS attack targeting France's visa passport official website. More recently, on February 6, 2024, THT claimed responsibility for a series of DDoS attacks targeting La Poste, the largest postal service in France. The attacks were launched as part of the group's #OpFrance campaign, which aims to disable critical infrastructure and public services in France in response to the government's expressed support for Israel. The next day, on February 7, 2024, the group claimed responsibility for DDoS attacks targeting Crédit Agricole, reportedly affecting its mobile applications and online banking systems.

AnonGhost Indonesian

AnonGhost Indonesian is a Southeast Asian hacktivist group that has historically supported the Palestinian territories. On October 16, 2023, AnonGhost Indonesian announced its intention to conduct "takedown, leak and mass defacement" attacks targeting the governments of Israel, the US, France, Germany, and India. The campaign was allegedly launched against countries that support Israel, which AnonGhost Indonesian described as "the cursed nation". Shortly after the announcement, on October 17, 2023, AnonGhost Indonesia claimed to have conducted a "mass takedown" of 173 French websites. Despite expressing the intention to paralyze critical infrastructure, the attacks appeared to have had minimal impact. Separately, on October 29, 2023, the group claimed to have accessed databases belonging to France and Brazil. We believe that these claims are fabricated or exaggerated and that the data shared in these instances are recycled from publicly available databases that were previously compromised.

Garnesia Team

Garnesia Team (Cyber Garuda Indonesia) is a self-proclaimed pro-Hamas hacktivist group that is allegedly Indonesia-based. The group frequently collaborates with Southeast Asian hacktivist groups such as the GANOSEC Team, Team Insane Pakistan, and Mysterious Team Bangladesh (MTB) to target entities in India, Israel, or countries that openly support Israel. On August 30, 2023, Garnesia Team claimed responsibility for DDoS attacks targeting the French Ministry of Justice.

Mysterious Team Bangladesh

Between August 30, 2023, and August 31, 2023, MTB claimed responsibility for a series of DDoS attacks targeting government and critical infrastructure entities in France. Notable targets included the website for the French Ministry of Education, the media outlet News France, the National School of Civil Aviation, and several French airport websites, including Paris, Lille, Toulon-Hyères, and Strasbourg. Although the airports of Paris and Lille appeared unaffected, the websites of Toulon-Hyères and Strasbourg experienced outages for several hours. The group also took down the Paris Cité University website, which has over 50,000 students. The attacks formed part of the group's #OpFrance campaign,

launched in response to the government's perceived interference in Niger and Senegal, specifically its support for the Senegalese government and the possibility of military intervention in Niger. The group also expressed criticism of the French government's decision to ban women from wearing abayas in schools.

LulzSec

On February 9, 2024, LulzSec, claimed responsibility for a DDoS attack targeting the French National Assembly (*assemblee-nationale[.]fr*). On that same day, several members of the pro-Palestine hacktivism collective The Cyber Operations Alliance (C.O.A), consisting of Lulzsec Indonesia, Jambi_Cyber_Team, Garnesia Team, Toxcar_Cyber_Team, Garuda_From_Cyber, StarsX_Cyber_Team, Ketapang_Gray_Hat, Islam_Cyber_Team, Moroccan_Black_Cyber_Army, Hacktivist_Jatim, Ghost of Palestine, GBAnon17, Garuda Anon Security, Bandung Cyber Team, Jakarta Ghost, Hizbullah_Cyber_Team, and IXP666SECTEAM, among others, claimed responsibility for a DDoS attack targeting Orano Group, a uranium producer owned by the French government (*orano[.]group[.]fr*). We could not independently verify these attacks and we assess these groups as having low credibility as they have frequently claimed responsibility for DDoS or website defacement attacks that did not occur or had minimal impact.

R00TK1T ISC

On December 28, 2023, R00TK1T (aka R00TK1T ISC) expanded its targeting to include France and claimed responsibility for targeting the French cosmetics giant L'Oréal but did not provide proof of its alleged attack or even specify what type of attack allegedly occurred. On January 12, 2024, R00TK1T shared a file that it claimed contained compromised data that it breached from the French fire security company Mondialisol (*mondialisol[.]com*). The threat actor did not specify when the database was breached or what type of information was compromised.

Malign Influence Operations

State influence actors are conducting malign influence operations related to the 2024 Paris Olympic Games, using the event as a target of opportunity to reinforce longstanding influence operations and advance corresponding geopolitical objectives. Advanced influence actors sponsored by or aligned with Russia, China, Iran, or Azerbaijan are, at a minimum, using the Paris Olympics to fuel pre-existing malign influence narratives at varying degrees of scope and scale. Common malign influence themes observed related to the Paris Olympics include references to the Russia-Ukraine war and the Israel-Hamas conflict, with narratives centering around Israeli and Russian athletes' participation in the event.

Russia

Russia has and will almost certainly continue to attempt to undermine the Paris Olympics through multiple ongoing malign influence operations, including campaigns active since at least 2023. Russian attempts to discredit the 2024 Olympics are very likely viewed as a proportionate response to perceived hostile activity toward Russia from France and the IOC, as discussed earlier (1, 2). On April 4,

2024, French president Emmanuel Macron told French reporters that Russia-linked actors are "without a doubt" conducting malign influence operations aimed at undermining the 2024 Paris Olympic Games.

Observed malign narratives emanating from Russian sources suggest that France is unprepared to host the Olympic Games, that the Olympic Games pose a significant European safety and security risk, and that the IOC has politicized the Olympic Games with an unfair, anti-Russia bias.

On March 1, 2024, Jean-Noël Barrot, the secretary of state for European affairs in France, told French television station TF1 that the national "bedbug panic" in the fall of 2023 was amplified by social media accounts "of Russian inspiration or origin" and accounts "linked to the Kremlin". Barrot stated that the accounts sought to link the arrival of Ukrainian refugees to the spread of bedbugs throughout Paris and other major French cities, heightening fears of unsanitary conditions ahead of this summer's Paris Olympics. According to French media, French intelligence services concluded that there was a link between Russia-aligned actors and the bedbug panic, but Barrot's statements are the first time a French official had confirmed this publicly.

On March 6, 2024, Reliable Recent News (RRN), an information and malign influence portal managed by two Russian companies, Social Design Agency and Structura National Technologies, published an article suggesting that public confidence in France's ability to host the Olympics was "diminishing" by highlighting various reported "organizational problems".[1] [2] [3] For example, the article cites fewer admissions to observation sites, restrictions on attendance for the opening ceremony, and the state of the Seine River as a "color… [that] leaves something to be desired". The article also notes the Paris police strike over wages and pensions as a security risk, stating that "The police do not expect anything good from the Olympic Games". A separate article from March 28, 2024, argued that "nobody is interested in such Olympic Games", claiming local officials are "forced to distribute free tickets" to garner public interest in the event.[4] The article adds that "a growing number of French people" are concerned about corruption, citing salary increases of senior managers of the Paris 2024 organizing committee.

International audiences, and particularly audiences in France, are almost certainly the target audiences for Russian attempts to erode support for the Paris Olympics. Russian domestic audiences are very likely a secondary audience of Kremlin propaganda targeting the Olympics. Among domestic audiences, the Kremlin very likely looks to reaffirm its view that Russia's exclusion from the Paris Olympics is rooted in anti-Russian bias, as well as legitimize Russia's Friendship Games as a pro-Russian Olympic Games alternative, which are planned to be held in September 2024 for the first time in 40 years. In public statements, Kremlin officials have called the Russian Olympic Committee's (ROC) ban from the Paris Olympics "discrimination", and "politically motivated", and have categorized the IOC's ban on Russian

[1] French authorities have connected RRN to its amplification of Stars of David stencilings across Paris, a suspected Russian influence and intimidation operation.
[2] Social Design Agency and Structura National Technologies are two Russian companies attributed to malign influence operations worldwide, including Doppelgänger. RRN has also been linked to the Doppelgänger operation.
[3] *https://rrn[.]media/fr/la-ceremonie-douverture-des-jo-sera-reduite/*
[4] *https://rrn[.]media/fr/de-tels-jeux-olympiques-ninteressent-personne/*

athletes from participating in the opening parade as "destruction of the idea of Olympism"[5]. Following the IOC's ban of the ROC in October 2023, Russian president Vladimir Putin called the Olympics a "tool of political pressure against people who have nothing to do with politics", further suggesting the IOC conducted "racist, ethnic discrimination" against Russia.[6]

Russia is very likely to use multiple, if not all, of the known overt and covert "pillars" of its disinformation and propaganda ecosystem, as defined by the US Department of State, to promote malign propaganda and other influence content intent on undermining the 2024 Paris Olympic Games. The most overt influence activity from the Kremlin against the Paris Olympics will very likely include Kremlin-aligned statements issued by high-ranking officials in the Ministry of Foreign Affairs, the Kremlin Press Office, the Presidential Administration, and the Foreign Intelligence Service (SVR). It is very likely that these statements, as well as other Kremlin-aligned propaganda talking points against the Paris Olympics, will filter through state-sponsored media outlets, including RT, Sputnik News, TASS, and RIA Novosti. Furthermore, it is very likely we will observe at least some degree of covert influence activity against the Paris Olympics by Russian influence assets, from coordinated inauthentic behavior (CIB) to promote Kremlin propaganda against the event to inauthentic news coverage of the event from existing networks, such as the extensive Doppelgänger operation.

China

China will likely conduct limited influence operations targeting the Paris Olympics, broadly focusing on pro-China messaging. China has previously used its influence apparatus to support and defend its hosting of the 2022 Beijing Winter Olympics, particularly following international boycotts against China's human rights abuses in Xinjiang, and to promote tourism and Chinese culture. However, diplomatic and cultural exchanges between France and China, discussed above, remain a likely deterrent to negative messaging targeting the French government. In addition, 2024 is the inter-government "Franco-Chinese year of cultural tourism", further discouraging Chinese negative messaging targeting France and its hosting of the Olympics due to the empirically negative impact disinformation can have on tourism.

[5] The IOC suspended the ROC in October 2023 following Russia's illegal annexation of Ukrainian territories, which was ruled as a breach of the Olympic Charter.
[6] *https://tass[.]ru/sport/19061381*

Figure 5: *Global Times cartoon promoting Chinese tourism during the 2022 Beijing Winter Olympics (Source: Social Media)*

For the Paris Olympics, China's influence objectives are likely centered around defending its athletes against doping accusations, and as a result are more likely to target US doping agencies and the IOC than French authorities. For example, on April 21-22, 2024, state-sponsored news outlets Global Times and Xinhua both published articles criticizing US Anti-Doping Agency (USADA) CEO Travis Tygart for accusing the World Anti-Doping Agency (WADA) and China Anti-Doping Agency (CHINADA) of turning a blind eye to doping accusations levied against 23 Chinese swimmers.[7] [8] China will likely restrict itself to using only its overt influence apparatus for pro-China messaging during the Olympics. However, if tensions with the US, USADA, or other doping agencies were to escalate, covert influence networks remain an increasingly important tool for Chinese influence operations and could be used to spread negative messaging targeting China's perceived adversaries.

Iran

Iran will very likely continue to conduct limited malign influence operations related to the Paris Olympics based on its demonstrated intent to do so and historically observed influence activity specifically targeting sporting events, such as the Iran-aligned network Endless Mayfly influence operation involving the 2022 FIFA World Cup.[9] Iran's opportunistic influence activities related to the Paris Olympics likely support Iran's ongoing efforts to undermine Israel's actions against Hamas by attacking Israel's reputation on the global stage.

Observed malign narratives emanating from Iranian sources include allegations that countries who support Israel — in the context of participating in the Paris Olympics — are complicit in alleged war crimes in Gaza and that providing support to Israel is akin to supporting the oppression of Palestinians.

[7] *https://www.globaltimes[.]cn/page/202404/1310966.shtml?id=12*
[8] *https://english.news[.]cn/20240421/0a8ff59c2ab44e8883653a9bf6aacbad/c.html*
[9] Endless Mayfly was an Iran-aligned network of inauthentic websites and online personas used to spread false and divisive information primarily targeting Saudi Arabia, the United States, and Israel.

[10] [11] Additionally, Iranian state media has contrasted Israel's participation in the Paris Olympics with the suspension of the ROC and athletes from Russia and Belarus during the 2022 Olympic Games, compared Israel to the historical apartheid in South Africa, and claimed Israel is using the Yarmuk Stadium sports complex located in Gaza City as a torture and execution center.[12] [13] [14] The primary target audience for these narratives is likely individuals and organizations moderately susceptible to actively opposing Israel's participation in the Paris Olympics.

Iran will likely employ a combination of influence TTPs in conducting malign influence related to the Paris Olympics, such as using overt state-owned media outlets — including Supreme Leader Ali Khamenei's official website (*khamenei[.]ir*) and Press TV (*presstv[.]ir*) — as well as covert outlets such as NewsPic (*newspic[.]org*), to publish content calling for an international ban on Israel's participation in the event.[15] [16] As an example, NewsPic has published an almost certainly edited artificial intelligence (AI)-generated stock photo provided by *vecteezy[.]com* to support the aforementioned malign narratives, as demonstrated in **Figure 6.**[17]

Figure 6: *Screenshot of a poster published by NewsPic; the image above the text was identified as a stock image provided by vecteezy[.]com that was edited with text to support the aforementioned malign narratives (Source: NewsPic[18])*

[10] *https://english.khamenei[.]ir/news/10221/Definite-accomplice*
[11] *https://english.khamenei[.]ir/news/10228/Gaza-is-about-the-oppression-of-the-Palestinians-and-their-power*
[12] *https://twitter[.]com/PressTV/status/1757871227555782892*
[13] *https://www.presstv[.]ir/Detail/2024/01/11/718013/Israel-staring-at-Paris-Olympics-ban-for-killing-Palestinian-athletes*
[14] *https://www.presstv[.]ir/Detail/2024/02/20/720425/campaign-ban-israel-intl-sports-competitions-gets-impetus*
[15] *https://twitter[.]com/PressTV/status/1757871227555782892*
[16] NewsPic is assessed by Insikt Group as likely operationally affiliated with IUVM Archive. Insikt Group has historically assessed IUVM Archive as very likely affiliated with the International Union of Virtual Media (IUVM), which was sanctioned by the US Department of the Treasury in 2020 for attempting to influence elections in the US.
[17] *https://newspic[.]org/israels-olympic-suspension-amid-war-crimes/*
[18] *https://newspic[.]org/israels-olympic-suspension-amid-war-crimes/*

Notably, the Boycott, Divestment, and Sanctions (BDS) movement and Democracy in Europe Movement 2025 (DiEM25) currently have respective stand-alone campaigns and petitions calling for the suspension of Israel-affiliated athletes and teams from participating in international sporting events.[19] Based on Iranian state media referencing and directly quoting content affiliated with the BDS movement and DiEM25-specific campaigns, Press TV and other overt Iranian influence assets will very likely continue seeking opportunistic amplification of individuals and organizations external to Iran actively opposing Israel's participation in the 2024 Olympics.

Additionally, since June 2022, Iran has increasingly conducted cyber-enabled influence operations and, since 2016, has demonstrated the operational capability to use CIB networks on social media to amplify influential content. Insikt Group has not identified any instances of Iran employing cyber-enabled influence operations or CIB directly targeting the Paris Olympics; however, Iran very likely retains the capability to do so.

Azerbaijan

Insikt Group has identified further CIB emanating from a previously identified Azerbaijani-linked influence network targeting the 2024 Paris Olympic Games. The French government agency Vigilance and Protection Against Foreign Digital Interference (VIGINUM) first identified the network in November 2023 seeking to undermine France's capacity to hold the 2024 Paris Olympic Games, and connected the network to individuals associated with the New Azerbaijan Party (YAP), the current Azeri presidential party.

We identified likely inauthentic mainstream social media activity criticizing the Paris Olympics using hashtags such as #BoycottParis2024 and #BoycottParisOlympicGames. The same accounts use profile pictures likely stolen from stock image websites and typically portray French citizens. The posts included cheapfake and AI-generated images blending scenes from Paris, the Olympic logo, and pests with the caption "Punaises de lits, rats, moustiques-tigres..." ("bedbugs, rats, and tiger mosquitoes").

Several of the social media accounts identified by Insikt Group demonstrate historical activity consistent with findings from VIGINUM and France24, which investigated a broader influence operation by Azerbaijani assets denouncing France's "neocolonialism", using hashtags such as #neocolonialism, #macron, and #Azerbaijan.

Accounts involved in the recent activity targeting the Paris Olympics had previously amplified the Baku Initiative Group (BIG), a likely front for Azerbaijani influence operations. BIG claims to be a non-governmental organization representing an alliance of pro-independence movements in French overseas departments and territories, such as the People's Union for the Liberation of Guadeloupe (UPLG) and Kanak Socialist National Liberation Front (FLNKS). The organization regularly amplifies communications from these political movements on its social media accounts and two websites (*dub[.]az* and *bakuinitiative[.]com*) with content in French, English, Russian, and Azeri.

[19] *https://diem25[.]org/petition-suspend-israel-from-international-sports/*

Observed influence activity is likely tied to a deterioration in French-Azerbaijani relations following an Azerbaijani offensive in Nagorno-Karabakh in September 2023. Azerbaijani president Ilham Aliyev's YAP has previously been accused of using CIB networks on Facebook in 2021 and 2020 to sway domestic political opinion and target independent or exiled Azeri journalists. As French-Azerbaijani relations continue deteriorating, this broader influence operation will likely continue supporting independence movements in French overseas departments and using inauthentic assets to undermine the French government ahead of the 2024 Paris Olympic Games.

Physical Security and Protests

The 2024 Paris Olympic Games — held in a major world capital repeatedly targeted by international terrorist groups and homegrown violent extremists, recently subject to waves of violent protests — very likely represents the most challenging physical security threat landscape for an Olympic Games since the 2012 London Olympic Games. The locations and venues that will host key elements of the Paris Olympics, most notably the planned opening ceremony on the Seine and the Stade de France, are almost certainly at heightened risk of an attack by terrorists or violent extremists. Anarchists and other actors motivated by a range of ideologies represent less significant physical security threats, but will likely seek to leverage the global spotlight on the Olympics to attract attention to their causes through disruptive protests, demonstrations, and confrontations with security forces.

French authorities have invested billions of dollars to secure the Paris Olympics, which will entail an estimated 67,000 private security personnel, military, and police officers, and the deployment of advanced technologies for surveillance and to combat the threat of unmanned aerial vehicles (UAVs or "drones"). To bolster its domestic resources, France has sought external assistance from a wide range of global partners, including the provision of geospatial intelligence and private-sector communication outreach from US government agencies. The expansive security apparatus established for the Paris Olympics will very likely reduce, but not eliminate, the possibility of a successful terrorist attack or disruptive protests.

Terrorism and Violent Extremism

Terrorists and violent extremists — particularly IS and al-Qaeda supporters in France and neighboring European countries — will almost certainly continue to plot and incite violent attacks targeting the Paris Olympics, although the event's extensive security footprint will very likely mitigate the probability of a successful attack. On March 24, 2024, the French government announced it had raised the country's terrorism threat assessment system (Vigipirate) to its highest possible level, "Attack Emergency", which signals that the threat of a terrorist attack is considered imminent. Three factors almost certainly underlie the heightened risk of terrorism to France during the Paris Olympics:

- The increase in jihadist radicalization and mobilization in Europe following the outbreak of the Israel-Hamas conflict

- The renewed focus of IS's branch in Afghanistan, IS Khorasan Province (ISKP), on planning, guiding, and inciting external operations following the March 22, 2024, terrorist attack at the Crocus City music hall in Moscow, Russia
- An ongoing campaign by IS-affiliated media outlets and the group's supporters to promote terrorist attacks against sports stadiums in Europe — including venues that will be used during the Olympics

Insikt Group has not observed information indicating that other violent extremist threat actors beyond IS and al-Qaeda supporters intend to conduct terrorist attacks against the Paris Olympics. According to French security services and government sources, the bulk of the terrorist threat plots targeting the country in recent months have emanated from IS and ISKP supporters, a dynamic that is almost certain to continue in the lead-up to the event. French police have already arrested one IS supporter — a 16-year-old from the town of Marignier — who allegedly planned to conduct an attack on the Paris Olympics using an explosive belt. In the months prior to the group's claimed attack in Moscow, the French security services claimed to have disrupted several attacks linked to ISKP, according to March 25, 2024, statements from the French president and prime minister.

IS almost certainly seeks to target the Paris Olympics to demonstrate its external operations capabilities and replicate the organization's historic attacks in France. IS propaganda has especially focused on urging its supporters to recreate the November 2015 series of terrorist attacks in Paris that included a suicide bombing at the Stade de France — the main venue for the 2024 Paris Olympic Games. However, due to the pervasive security footprint established prior to the Paris Olympics and complex logistical, financial, and operational difficulties, IS is very unlikely to successfully carry out a sophisticated, centrally coordinated attack involving multiple operatives, on the same scale as the 2015 Paris attacks.

In lieu of a large-scale plot, IS has incited its supporters in France, Belgium, Germany, and other Western European countries to conduct attacks targeting the Paris Olympics through its media products. This effort is almost certain to result in individual IS supporters attempting or plotting to conduct low-sophistication, lone-actor attacks targeting the Paris Olympics; while these attacks are more likely to be carried out successfully, they are also likely to result in limited casualties and have limited impact. In recent months, ISKP-linked media outfits such as al-Azaim Media, as well as numerous online IS support groups and unofficial media outfits, have engaged in a campaign promoting terrorist attacks against European sporting events and venues — including the 2024 Paris Olympic Games. While much of this propaganda has focused on promoting standard, low-sophistication TTPs for IS-linked attacks — such as stabbings, vehicular attacks, attacks with incendiary devices, and improvised explosive devices (IEDs) — certain publications have called for IS supporters to maneuver explosive-laden unmanned aircraft into sports stadiums while events are underway.

***Figure 7**: March 30, 2024, infographic from an unofficial, pro-IS online media source inciting attacks against the 2024 Paris Olympics (Source: Recorded Future)*

Israel-Hamas Conflict

Incidents of terrorist- or violent extremist-targeted physical attacks against Israeli, American, or Western European athletes, fans, and other personnel attending the Paris Olympics involving affiliates of the Iran-backed "axis of resistance" — particularly Iran's IRGC, Hezbollah, and supporters of Palestinian foreign terrorist organizations (FTOs) residing in Europe — are very unlikely but within the realm of possibility. These activities would almost certainly be motivated by the Israel-Hamas conflict and the recent kinetic escalation between Israel and Iran. To varying degrees, these groups have demonstrated an interest in external operations outside the Middle East, as well as capacities for conducting terrorist attacks or extraterritorial assassinations.

These groups would likely view the Paris Olympics as an attractive venue to conduct an attack due to its international profile, although Insikt Group has not identified any information indicating that these groups are planning to conduct violence at the event. Nevertheless, the threats are not without historical precedent — at the 1972 Summer Olympic Games in Munich, Germany, the Palestinian militant group Black September killed two Israeli athletes and took nine others hostage from the Olympic Village, later killing the hostages during a failed exfiltration attempt.

The IRGC, in recent years, has repeatedly demonstrated its intent to conduct extraterritorial assassinations. While these plots mainly targeted Iranian dissidents, the IRGC notably plotted to assassinate US officials following the death of its commander, Qassem Soleimani, in a January 2020 US strike in Iraq. Similarly, the IRGC is likely to target Israeli officials and public figures following the April 1, 2024, Israeli military strike that killed IRGC brigadier general Mohammad Reza Zahedi in Syria. Hezbollah, through its Islamic Jihad Organization, has also plotted attacks against US targets and Israeli citizens overseas. In March 2024, Italian police arrested three affiliates of the Palestinian FTO al-Aqsa Martyrs Brigades, who were reportedly planning to conduct attacks in Western Europe.

Civil Unrest and Disruptive Protests

Security measures imposed by French authorities ahead of the Paris Olympics will very likely reduce the ability of protest groups to disrupt the event. Groups protesting the ongoing Israel-Hamas conflict, such as Urgence Palestine, and perceived environmental and social justice impacts of the Olympic Games, such as Extinction Rebellion (XR), represent the most likely actors to directly target the Paris Olympics, organizers, or associated contractors with protests. These groups will also likely hold demonstrations in Paris or near Olympic Games locations to take advantage of global media attention on the event to publicize their causes. Protests over national political issues in France — including strikes and farmers' protests — are unlikely to directly target Paris Olympics organizers or events, but will likely cause incidental disruptions to public transit, major roads, or public services. Actions by these groups are generally peaceful, but some — primarily environmental and pro-Palestine protests — draw hundreds or thousands of participants and have seen clashes with counter-protesters or police, resulting in isolated injuries. Further, environmentalists and farmers' groups frequently adopt highly disruptive tactics, such as blockades of main roads, which will likely impact attendees traveling to events.

Environmental Activists

On January 22, 2024, French interior minister Gérald Darmanin characterized "environmentalist collectives", such as XR, Soulèvements de la Terre, Dernière Rénovation, and Saccage 2024, as most likely to attempt disruptive actions during the Olympics. Based on these groups' historical activity, protests will likely focus on perceived environmental impacts or inequality stemming from preparations for the Paris Olympics. For example, Saccage 2024 advertised a May 1, 2024, anti-Olympic protest march in Paris to Place de la République. This came after protesters gathered in February 2024 at the Olympic Village in Saint-Denis against the construction of 14,000 athlete studios amid a lack of affordable housing in the area. While protests by groups such as XR are typically peaceful, they will likely disrupt public transit and local traffic. However, the French government has taken steps to limit potential disruption to the Paris Olympics, such as by screening volunteers for the Olympics and rejecting those with identified links to environmental groups.

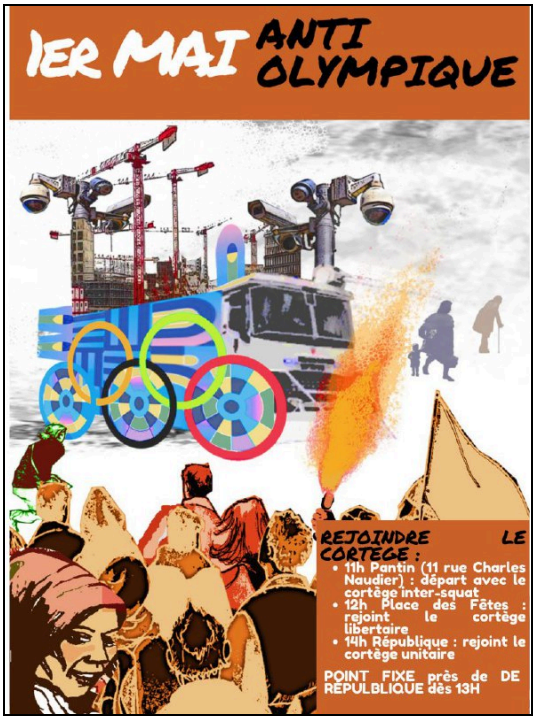

***Figure 8**: April 26, 2024, infographic from Saccage 2024 advertising anti-Olympics march in Paris on May 1 (Source: Recorded Future)*

Pro-Palestine Protests

Protests related to the Israel-Hamas conflict have occurred less frequently in France than in other countries, as French authorities have banned multiple pro-Palestinian demonstrations, citing public order risks. However, on April 26, 2024, large crowds of pro-Palestinian protesters blocked the entrance to Sciences Po Paris after riot police cleared a sit-in the previous day. On March 10, thousands of protesters gathered in Paris to call for a ceasefire in Gaza, organized by Urgence Palestine and supported by the La France Insoumise political party. Pro-Palestine groups will likely increase focus on the Paris Olympics in the lead-up to the event, specifically on the participation of Israeli athletes or private security providers for the event that are linked to Israel's defense industry. For example, the Palestine Saint-Denis Committee planned a protest at the Organizing Committee for the Olympic Games in the Paris suburb of Aubervilliers on April 30, calling for Israel to be banned from the Olympics. Notably, Saccage 2024 shared the protest call on social media, suggesting that pro-Palestine demonstrations will likely receive support from environmental groups.

These protests have been peaceful, but are very likely to draw counter-protesters, and the heightened security presence during the Paris Olympics will likely increase the chances of clashes with law enforcement. Moreover, events related to the Israel-Hamas conflict that cause uproar, such as Israeli strikes that killed aid workers, particularly if those events coincide with the running of the Paris Olympics, risk escalating protests into violent riots. On April 16, 2024, social media posts showed an individual driving a car into a pro-Palestinian Jewish protest outside the headquarters of French

weapons manufacturer Thales Group in Meudon, outside Paris; notably, Thales is one of several private contractors responsible for security at the Olympics.

Farmers' Protests

Since late 2023, farmers' unions have held disruptive protests across Europe, including in France, over European Union and national agriculture and trade policies. In February 2024, two major French farmers' unions, the Fédération Nationale des Syndicats d'Exploitants Agricoles (FNSEA) and the Young Farmers union, lifted week-long roadblocks around Paris after the government offered concessions. However, the FNSEA has called on the government to pass legislation by June, and Coordination Rurale, another major farmers' union, continues to hold protests across France. A perceived lack of progress on agricultural issues before the Paris Olympics and upcoming European Parliament elections in June will likely prompt further protests, causing localized traffic disruptions.

Labor Actions

In April and March 2024, the Confédération Générale du Travail (CGT) and Force Ouvrière, the two largest unions representing state employees, filed notices allowing them to call strikes during the Paris Olympics, with the CGT specifically citing the impact of the Paris Olympics on workers, including bonuses, accommodation, and lack of vacation. Similarly, on April 24, France's civil aviation agency asked airlines to cut flights by 75% at Paris-Orly Airport, by 55% at Paris Charles de Gaulle Airport, and by 45% at most other airports due to an air traffic controllers strike. While the French government will very likely prioritize negotiations or other measures to prevent disruption during the Paris Olympics, the event notably coincides with traditional national vacations, increasing the likelihood of public sector strikes. Such actions will very likely disrupt public transit and personal and business commutes during the Paris Olympics.

Figure 9: *Major protests and civil unrest in Paris from January 1 to April 30, 2024 (Source: Recorded Future)*

Mitigations

The Recorded Future Intelligence Cloud should be used to mitigate the multifaceted threats to your organization resulting from the 2024 Paris Olympic Games.

- Protect against cyber intrusions by gaining comprehensive visibility into your organization's attack surface, prioritizing alerts and automating remediation, accelerating security operations detection and response, tracking the state-sponsored APT and cybercriminal threat landscape and evolving threat actor TTPs, and more.

- Identify infostealer logs and credential leaks related to your organization and monitor IAB advertisements to prevent account takeovers, data theft, espionage operations, and other attacks, including ransomware propagation. Recorded Future's Identity Intelligence can be used to alert you to your organization's credentials that have become compromised.

- Detect references to your organization's brand in relation to the Paris Olympics to uncover potential hacktivist and activist threat activity targeting your organization, and take down domain and brand impersonations that could be used to scam your customers or third parties.

- Monitor the geopolitical environment for events that could alter adversarial countries' intent to conduct cyber intrusions or influence operations against the Paris Olympics.

- Understand France's Country Risk score based on five functional categories: governance & institutions, physical security & travel, cybersecurity, data privacy & surveillance, and supply chain. Travelers should take corresponding necessary precautions when attending the Paris Olympics, such as only using trusted equipment for charging electronic devices.

- Identify real-time physical security and protest events occurring near business facilities during the Paris Olympics using Recorded Future's Facility Risk Event Playbook to protect corporate employees, facilities, and assets.

Recorded Future clients should use the Paris 2024 Olympic Games Intelligence Kit. Recorded Future Intelligence Kits centralize information, including custom advanced queries and Intelligence Cards, based on specific industries or areas of interest.

Outlook

The Olympic Games are a testament to international cooperation, having only been canceled three times in over a century in response to nothing less than world war. This continuity underscores the resilience of, and global commitment to, the event. However, geopolitics have always competed alongside the athletes, and given the current escalation of international tensions and conflicts, the 2024 Paris Olympic Games will be especially fraught.

Insikt Group expects to see increased threat activity as the Paris Olympics draws near, though the combination of advanced preparation, technological solutions, and international collaboration offers a strong defense against these challenges. We recommend monitoring geopolitical developments that may increase motivation for hacktivists, violent extremists, or state proxy groups to carry out a disruptive attack against the Olympic Games. For example, Russian setbacks in Ukraine, the escalation of violence in Gaza, or the spread of conflict to other parts of the Middle East, will change how different threat actors evaluate the costs and perceived benefits of a cyber or physical attack in Paris. The online forums and messaging applications utilized by hacktivists, violent extremists, and state proxy groups should be continuously scrutinized to identify indications of operational planning.

As a result, organizers and associated stakeholders must focus on an adaptive security strategy that takes into account the geopolitical threat landscape as well as the capabilities of various groups. Monitoring the evolution of cyber and influence threat actor TTPs and adoption of new technologies, ensuring robust cyber defenses among all organizations involved in the Paris Olympics from the IOC to public transportation, and fostering international cooperation in intelligence-sharing will be critical to ensuring the seamless running of the Paris Olympics.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

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 threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com