cloud.google.com /blog/topics/threat-intelligence/cyber-threats-2024-paris-olympics/

Phishing for Gold: Cyber Threats Facing the 2024 Paris Olympics

Mandiant ⋮⋮ 6/5/2024

Written by: Michelle Cantos, Jamie Collier

Executive Summary

- Mandiant assesses with high confidence that the Paris Olympics faces an elevated risk of cyber threat activity, including cyber espionage, disruptive and destructive operations, financially-motivated activity, hacktivism, and information operations.
- Olympics-related cyber threats could realistically impact various targets including event organizers and sponsors, ticketing systems, Paris infrastructure, and athletes and spectators traveling to the event.
- Mandiant assesses with high confidence that Russian threat groups pose the highest risk to the Olympics. While China, Iran, and North Korea state sponsored actors also pose a moderate to low risk.
- To reduce the risk of cyber threats associated with the Paris Olympics, organizations should update their threat profiles, conduct security awareness training, and consider travel-related cyber risks.
- The security community is better prepared for the cyber threats facing the Paris Olympics than it has been for previous Games, thanks to the insights gained from past events. While some entities may face unfamiliar state-sponsored threats, many of the cybercriminal threats will be familiar. While the technical disruption caused by hacktivism and information operations is often temporary, these operations can have an outsized impact during high-profile events with a global audience.

Introduction

The 2024 Summer Olympics taking place in Paris, France between July and August creates opportunities for a range of cyber threat actors to pursue profit, notoriety, and intelligence. For organizations involved in the event, understanding relevant threats is key to developing a resilient security posture. Defenders should prepare against a variety of threats that will likely be interested in targeting the Games for different reasons:

- **Cyber espionage groups** are likely to target the 2024 Olympics for information gathering purposes, due to the volume of government officials and senior decision makers attending.
- **Disruptive and destructive operations** could potentially target the Games to cause negative psychological effects and reputational damage. This type of activity could take the form of website defacements, distributed denial of service (DDoS) attacks, the deployment of wiper malware, and operational technology (OT) targeting. As a high profile, large-scale sporting event with a global audience, the Olympics represents an ideal stage for such operations given that the impact of any disruption would be significantly magnified.
- **Information operations** will likely leverage interest in the Olympics to spread narratives and disinformation to target audiences. In some cases, threat actors may leverage disruptive and destructive attacks to amplify the spread of particular narratives in hybrid operations.
- **Financially-motivated actors** are likely to target the Olympics in various ways, including ticket scams, theft of PII, and extortion against entities during a period of heightened pressure. Capitalizing on interest in the games, threat actors are likely to use olympics-related lures in social engineering operations that are not necessarily targeting the games.

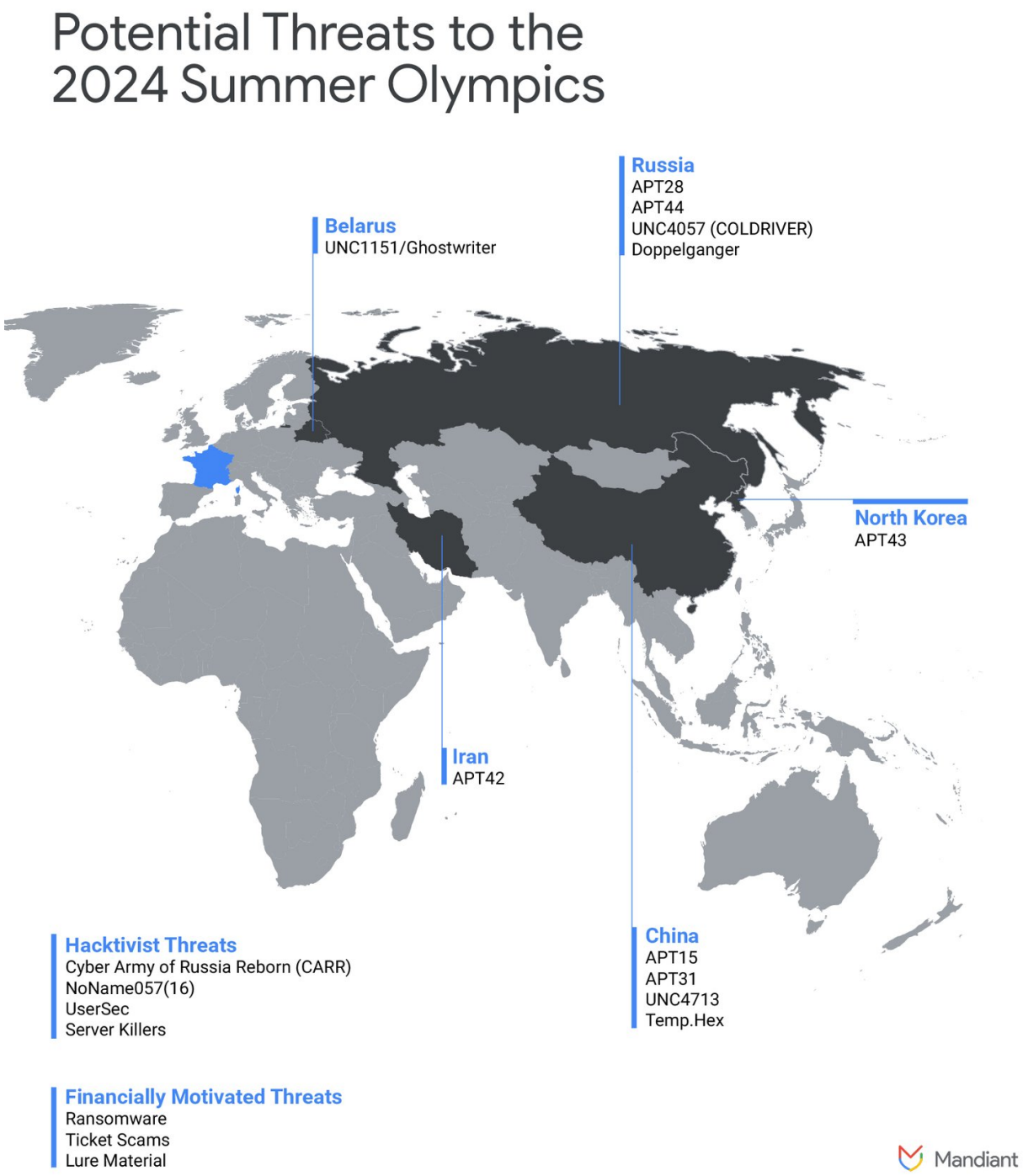

Figure 1: Potential threats to the 2024 Summer Olympics

Olympics-related cyber operations could impact a variety of entities. For some organizations involved in the Games such as sponsors, this could expose them to state-sponsored actors and destructive campaigns that are not typically active in their sectors. Other threats, such as cybercrime and extortion operations, will be more familiar, yet will likely become more prolific and persistent against entities involved in the Games.

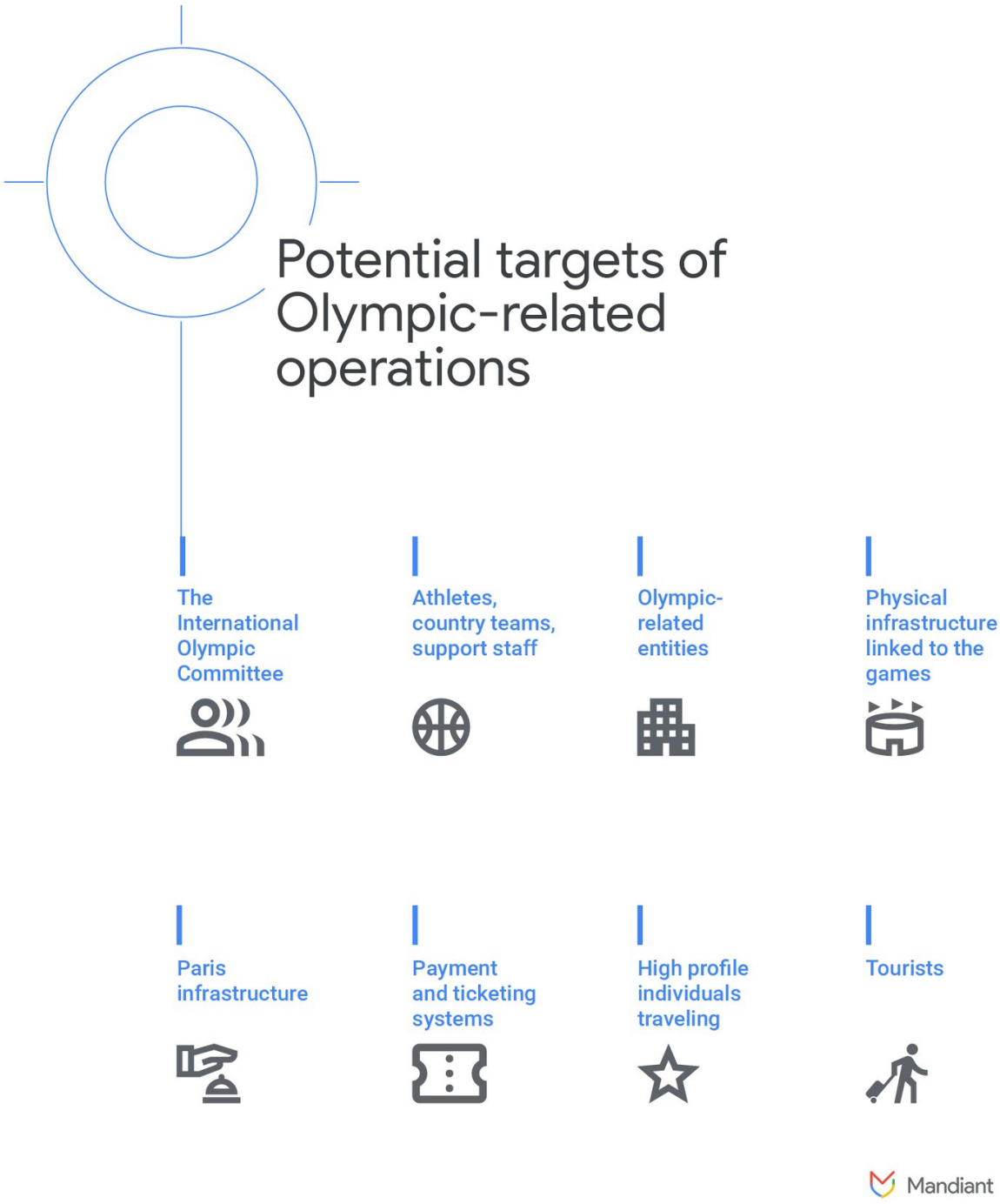

Figure 2: Potential targets of Olympic-related operations

State Sponsored Threat Activity

State-sponsored threats pose the most significant, high severity threat to the Summer 2024 Olympics. Mandiant assesses with high confidence that Russia poses the most severe threat to the Olympics given its repeated targeting of previous Olympic games, its tense relationship with Europe, and recent pro-Russia information operations having already targeted France. Other state-sponsored actors, such as those from China, Iran, and North Korea also pose a risk, albeit to a lesser extent.

Russia

Russian state-sponsored cyber threat activity poses the greatest risk to the Olympics. In addition to intelligence collection activities, Russian operators have demonstrated the capability and willingness to conduct destructive campaigns targeting past Olympics events and hybrid operations in which intrusions support influence campaigns. Mandiant has observed Russian espionage actors conduct cyber threat activity against previous iterations of the Olympic games, disrupting the event itself and undermining the safety and security of organizations related to the Olympics. France may face an elevated risk of Russian cyber threat activity given the country's financial and military support for Ukraine after Russia's invasion in February 2022.

While Russian athletes can compete in the Olympics this year, they will not represent their home country, are unable to participate in the opening ceremony, and must compete as neutral athletes. Russia's perceived grievances at its athletes being once again banned from competing under the Russian flag elevate the threat from Russian cyber attacks compared to other states.

Based on a well-documented history of targeting past Games, Mandiant assesses with high confidence that out of the Russian threat actors we track, APT44 is most likely to target the upcoming games, and the most likely to conduct impactful disruptive, destructive, or hybrid operations in addition to intelligence collection.

Figure 3: Significant Russian Operations Targeting Past Olympic Games

---

APT44 Android Malware Campaign Targeting Users in South Korea Before 2018 Winter Games in PyeongChang

Beginning in late 2017, APT44 (alias FROZENBARENTS) targeted organizations involved in Olympic activities in South Korea. The activity included credential phishing, and distribution of Windows,MacOS, and Android malware. In the Android campaign, APT44 obtained legitimate copies of Android applications popular in South Korea, modified them to add a custom mobile implant, and then published the trojanized apps to the Play Store. The implant, CHEMISTGAMES, was a modular framework designed for gathering data at scale, and included significant automation, abstraction, and specialization for mobile devices. The modular structure of CHEMISTGAMES ensured that the attackers could hide sensitive payloads and reserve them for specific targeted devices.

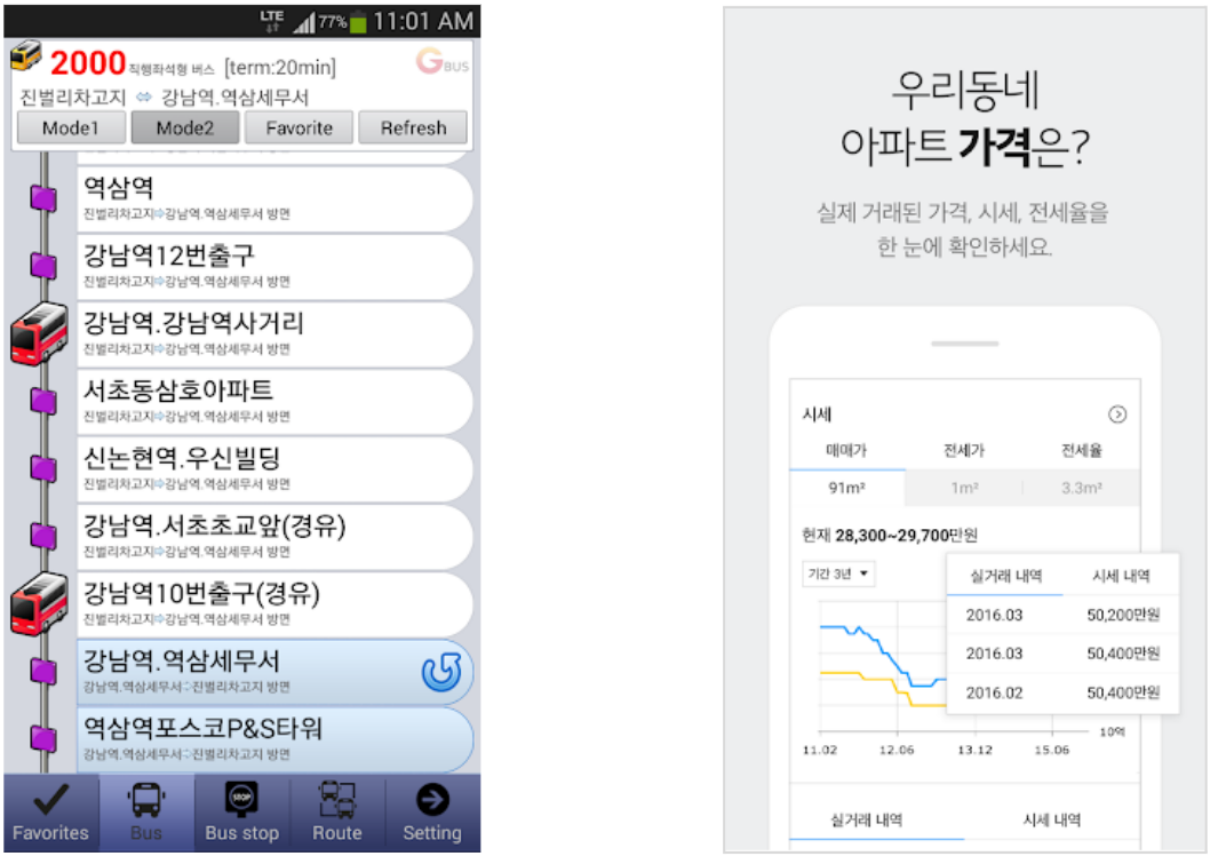

Figure 4: Prior to the Olympics, APT44 modified Android apps popular in South Korea, including a bus timetable app and an app for checking apartment rental prices

Google's Threat Analysis Group (TAG) discovered the Android campaign, developed signatures to protect user devices and block the malware on Play, and banned attacker-controlled developer accounts. Those detections protected users in other APT44 campaigns that attempted to infect users with CHEMISTGAMES, including an attempt to target Ukrainians with a fake webmail app, and domestically-focused campaigns targeting Russian businesses.

Mandiant suggests that UNC4057 (aka COLDRIVER) also poses a risk, despite no previously observed targeting of the Games. The group has conducted both cyber espionage and information operations activity in support of Russia, collecting personally identifiable information (PII) via credential harvesting operations that may support the nation's strategic intelligence priorities, and performing hack-and leak-campaigns to sow discontent in the UK in 2022. This activity cluster may target French organizations

affiliated with the games and high profile individuals from NATO member countries who may be in attendance.

China

Mandiant Intelligence assesses with moderate confidence that People's Republic of China (PRC) sponsored threats pose a moderate risk to the 2024 Paris Olympics. We suggest that APT31, APT15, UNC4713, and TEMP.Hex are most likely to target organizations and individuals related to the event given previous targeting of governments as well as civil society and non-profits in Europe. High profile government officials and senior decision makers attending the event will likely be an attractive target for PRC state sponsored threat actors seeking PII, credentials, or other sensitive information to support their national interests. This creates a heightened risk of spearphishing, credential harvesting, and intelligence collection operations.

While PRC espionage operators have demonstrated a capability and willingness to target operational technology systems, it is unlikely they will leverage destructive or disruptive campaigns targeting the Summer Olympics.

Iran

Mandiant Intelligence assesses with moderate confidence that Iranian state sponsored threats, primarily APT42, represent a moderate to low threat to the 2024 Summer Olympics. We have observed APT42 compromise civil society and non-profit organizations and government entities throughout Europe. Iranian threat actors may leverage the Games, either using the Olympics as lure material or targeting attendees themselves, to support campaigns against these industry verticals. Notably the ongoing conflict in Gaza may impact the frequency and tempo of Iranian intelligence-gathering and information operations activity in the short- to mid-term, with Iranian actors increasing their operations in Israel.

North Korea

Mandiant Intelligence assesses with moderate confidence that North Korean threat actors pose a low threat to the 2024 Summer Olympics. APT43 might leverage information surrounding the Games as lure material for financially motivated operations or potentially as material for social engineering campaigns to build rapport with targets.

Information Operations & Hacktivism

The high profile nature of the Olympics makes the event a popular target for hacktivism and information operations that could capitalize on interest in the Games to conduct high profile operations. Although hacktivists may have limited resources and capabilities, a well-timed disruption could achieve their goals.

Whilst Pro-Russia information operations could be the most prominent ones using Olympics-themed content, campaigns promoting the interests of PRC and Belarus may also use interest in the event to promote various narratives. Hacktivist and information operations actors share many tactics, techniques and procedures, and these groups could also create new personas specifically for their activity related to the Olympics.

Russia

Mandiant Intelligence assesses with high confidence that pro-Russian information operations will pose a frequent, moderate severity threat to the Summer 2024 Olympic Games. We have observed information operations promoting pro-Russia, anti-Ukraine, and anti-Western narratives leveraging the Olympics due to the popularity of the Games. Additionally political retribution for France's pro-Ukraine stance and Russia's ban from competing at the games under their flag may drive information operations activity promoting Russian interests.

- In February 2024 the French Foreign Ministry accused Russia of conducting widespread disinformation campaigns to disrupt the upcoming general election and the Olympics in retaliation for France's support of Ukraine after Russia's invasion in February 2022.
- In April 2024 at the opening of an Olympic swimming venue, French President Emmanuel Macron accused Russia of conducting an online disinformation campaign undermining the safety and security of the upcoming games. Mandiant Intelligence has independently observed pro-Russia activity from campaigns that we track, which appears to be consistent with these claims.

Several pro-Russia hacktivist groups have targeted entities throughout Europe and pose a viable threat to the Summer Olympics, including: Anonymous Sudan, Cyber Army of Russia Reborn, NoName057(16), UserSec, and Server Killers. We judge the threat from pro-Russia hacktivists to be particularly elevated because a number of these groups have publicized destructive attacks or data leaks from Russian state sponsored intrusion activity. Several groups have also demonstrated the ability to disrupt high profile targets with DDoS attacks.

Case Study: Doppelganger

Mandiant Intelligence has observed a network of inauthentic domains and social media accounts across multiple platforms, which we attributed to the pro-Russian information operations campaign publicly referred to as "Doppelganger". These domains have promoted political content in English, German, French, and Italian and circulated narratives aligned with Russian strategic interests, including those related to the Russian invasion of Ukraine.

- Mandiant has observed some narratives targeting the upcoming 2024 Paris Olympics promoted by Doppelganger domains. This has included articles promoting narratives that generally implied that France was not prepared as a host, as well as those that appeared intended to frame the French Government as inadequately prepared for the security risks potentially surrounding the games—particularly those related to Islamic extremism (Figure 3).
- In March 2024 the U.S. Department of Treasury announced sanctions against two individuals and two organizations associated with a Russian information operations campaign which posed as European government entities and media outlets to distribute inauthentic, pro-Russian narratives to European audiences. This activity aligns with the coordinated inauthentic networks of threat activity used by the Doppelganger campaign.

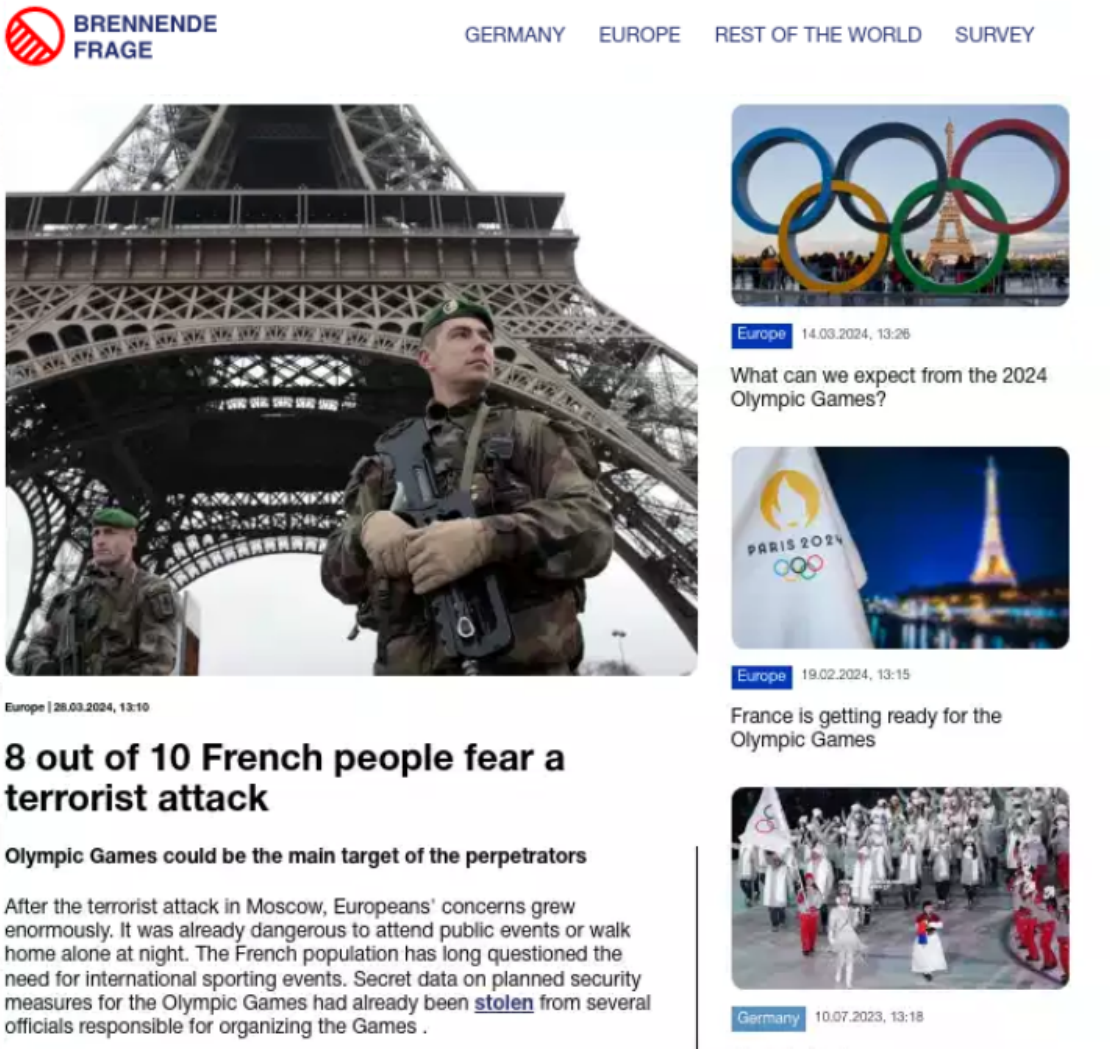

Figure 5: Example of an Olympics-related article published by a Doppelganger affiliated domain

China

PRC information operations will likely leverage Olympic-themed narratives to promote pro-PRC and anti-Western ideologies. Additionally, we anticipate pro-PRC information operations campaigns will likely use the doping scandal surrounding the PRC's swim team as part of their operations to highlight anti-PRC or pro-Western biases.

There is precedent for pro-PRC campaigns commenting on past Olympics.

- Rolling Stone highlighted a PRC-linked operation that masqueraded as a European news outlet "New Europe Observation" to foment discord in European populations using controversial topics such as immigration and the boycott of the Beijing Olympics in 2022. This operation attempted to hire "astroturf" protesters to participate in offline demonstrations and engaged native speakers of English, Russian, and other languages.
- In late 2021 and early 2022, Mandiant Intelligence identified social media accounts that we judge to be part of a pro-PRC information operations campaign dubbed "DRAGONBRIDGE" critiquing the U.S. decision to boycott the 2022 Winter Olympics in Beijing.
- ProPublica highlighted how pro-PRC information operations leveraged bots to promote false narratives surrounding Beijing's 2022 Olympic Winter Games.

Belarus

Mandiant identified UNC1151 and Ghostwriter activity in December 2021 promoting the narrative that Lithuania would boycott the 2022 Beijing Winter Olympics. Lithuania remains a frequent target for Ghostwriter operations and this likely was an opportunity to cause internal unrest leveraging a topical event.

Financially-Motivated Threat Activity

Mandiant Intelligence assesses with moderate confidence that financially motivated actors pose a moderate severity threat to the 2024 Summer Olympics. The amount of financial transactions conducted at the games will likely be an attractive target for malicious actors seeking profit with minimal effort. Cybercrime will likely be opportunistic in nature with the main risks including:

- **Ransomware and extortion operations** have a tendency to target organizations during high-pressure moments, including the hosting of major events. Listings from data leak sites over the last year indicate that France is the fifth most impacted country by ransomware and data theft extortion activity. We observed listings for French organizations posted most frequently on sites for LOCKBIT, 8BASE (aka PHOBOS), NOESCAPE, MEDUSA, and ALPHV. It is also possible that cybercriminal groups that have not been historically active in France will increase their targeting against Olympic-related entities in the runup and during the Games.
- **Ticket scams** often capitalize on interest in major sporting events to sell counterfeit tickets via fake ticket websites. The popularity of the games, growing demand for tickets, and the large amount of financial transactions occurring on third-party ticket platforms could make these systems an attractive target for cybercriminals.
- **Lure material** is often tied to topics of interest within the general public, and we anticipate that threat actors will likely use the upcoming Olympics as lure material for the initial compromise stages of their campaigns. Lures can convince unsuspecting users to engage with malicious material resulting in the distribution of malware.

Risk Mitigation Techniques

Organizations should strongly consider taking proactive measures to reduce the risk of cyber threats associated with the Paris Olympics.

- Organizations involved in the Games should update their threat profile to account for potentially new threats to which they will be exposed. Intelligence on relevant threat actors can be used to inform detection efforts, insert proactive security controls, conduct threat hunting within a network, and inform cyber risk assessments linked to the Games. It may be helpful to review the following guides for countering DDoS and destructive attacks:
- Organizations that face an elevated threat from ransomware and extortion operations are encouraged to read Mandiant Intelligence's Ransomware Protection and Containment Strategies guide. This provides practical guidance for hardening and protecting infrastructure, identities, and endpoints.
- Security awareness training should highlight the risks of Olympics-related social engineering lures in the runup to and during the Games.

- Organizations and individuals traveling to the Games should consider travel-related cyber risks, such as the elevated risk of public Wi-Fi tampering, scams involving Olympics-related events, and the targeting of VIPs (i.e. government officials, senior decision makers, and business executives).
- Organizations that face an elevated threat of information operations in relation to the Olympics should consider potential brand damage risks and comms mitigation strategies. It may be helpful to review Mandiant's blog post, How to Understand and Action Mandiant's Intelligence on Information Operations.

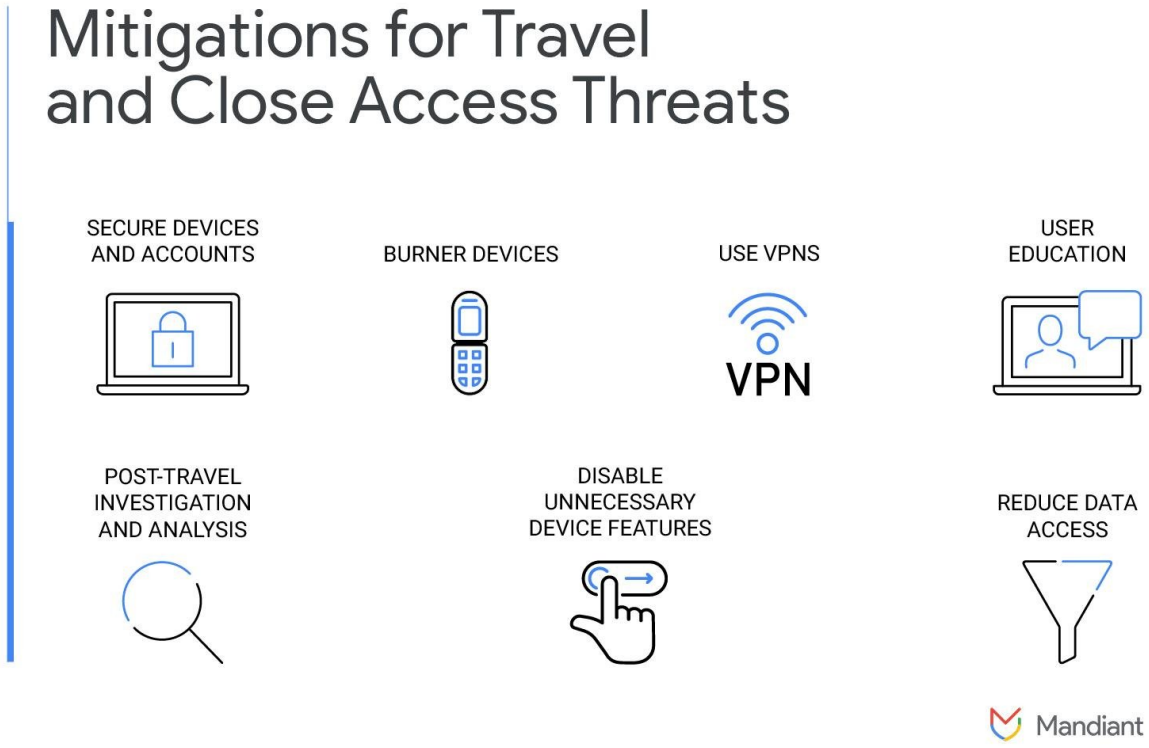

Figure 6: Mitigations for travel and close access threats

Outlook

Despite the variety of Olympics-related cyber threats, the security community is better prepared when compared to previous iterations of the Games. Having observed actors such as APT44 target previous Olympics, we have better insights into the ways the Games could be targeted. This gives defenders an opportunity to build a proactive and tailored security posture.

Posted in

- Threat Intelligence