Teneo®

A New Arena for Cybersecurity: The Olympic Games

June 2024

As much as the Olympics are about uniting the world and promoting excellence, respect and friendship, the Games have also, unfortunately, become a rich target of opportunity for cyber threat actors. While it may not be immediately obvious, almost every facet of the Olympic Games today has a nexus to technology and the Internet.

In decades past, governments, their host cities and corresponding arenas prepared for potential terrorist or physical security attacks. Today, cybersecurity has moved to the forefront of preparation in large part due to outcomes from the 2018 Winter Olympics in PyeongChang, South Korea and the 2020 Summer Olympics in Tokyo, Japan. As the world gears up for the Paris 2024 Summer Olympics, namely the July 26 to August 11 Olympics and August 28 to September 8 Paralympics, significant cybersecurity measures are underway to prevent disruption so that the producers, athletes and spectators can focus on what matters most – the Games.

This article analyzes cybersecurity events and learnings surrounding prior Olympic events, critical focus areas today for Paris and the French government as they plan for Summer 2024, and how organizations and spectators alike can stay vigilant as the Games begin.

PyeongChang 2018

In 2018, Russian state-sponsored cyber threat groups APT28 (also known as Fancy Bears or Fancy Bears Hack Team) and Sandworm orchestrated multiple cyberattacks against Olympic entities and events. These actions were conducted in response to the ban imposed on Russian athletes from participating in the 2018 PyeongChang Games.

Background

In early January 2018, Fancy Bears purportedly disclosed the correspondence of International Olympic Committee (IOC) officials and that of investigator Richard McLaren, known for his independent report on allegations of state-sponsored doping in Russia commissioned by the World Anti-Doping Agency (WADA). Through the disclosed emails and blog posts, APT28 aimed to highlight the existence of power struggles and divisions between various sporting organizations, including the IOC, WADA and national anti-doping agencies in the West, throughout the U.S., Canada and Europe. As part of its agenda, APT28 also aimed to propagate the narrative that the U.S. and Canada sought to undermine Europe's leadership in the Olympic movement and assert political dominance over English-speaking nations. This campaign amplified such beliefs through social media platforms like Twitter (X) and by publishing on fake news websites.

At the February 2018 PyeongChang Winter Olympics opening ceremony, network services were disrupted by the malware dubbed “Olympics Destroyer.” The Wi-Fi network, crucial for transmitting photographs and news coverage, experienced a sudden outage. Concurrently, the official Olympics smartphone app, which stored fans' tickets and vital transport details, ceased to function, leading to disruptions for some attendees attempting to enter the stadium. Additionally, broadcast drones were unable to operate and internet-linked televisions intended to display ceremony images across venues became non-functional. The cybersecurity industry and law enforcement agencies have attributed the attack to the Russian state-sponsored group Sandworm. It is interesting to note that a particular effort was made by the adversary to pin the responsibility on North Korea by inserting deceptive fragments within the code.

Tokyo 2020

The 2020 Tokyo Olympics, held in 2021 due to the COVID-19 pandemic, faced significant cyber threats both before and during the event. Cybersecurity was a major concern for the organizers, given the history of cyberattacks on previous Olympic events and the high-profile nature of the Games. In October of 2020, the UK government’s National Cyber Security Centre (NCSC) reported that Russia’s military intelligence unit, or GRU, had conducted cyber reconnaissance on various officials and organizations associated with the 2020 Olympic and Paralympic Games before the events were postponed to 2021.

Background

The Tokyo Organizing Committee and Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) undertook extensive preparations to safeguard the Games, including: detailed risk assessments associated with the Games considering past Olympic cybersecurity incidents; setup of a dedicated cybersecurity team; collaboration with international partners; execution of multiple crisis simulation exercises to prepare for potential cyber incidents; and coordination with private cybersecurity firms like NTT Corporation to build additional resilience into the Games. The FBI warned in July of 2021 that "malicious activity could disrupt multiple functions, including media broadcasting environments, hospitality, transit, ticketing or security."

Subsequent to the Games, in October, 2021, NTT Corporation reported that "the total number of security events that were blocked during the Games, including unauthorized communications to the official website, was 450 million. During the Games, unauthorized communications targeting vulnerabilities in terminals were observed, but NTT responded by blocking the communications." Andrea MacLean with Wireside Communications described the situation as follows: "Cybercriminals certainly saw the Games – and its related supply chain – as a high-value target with low downtime tolerance. After all, crime follows opportunity. And with connected stadiums, fan engagement platforms and complete digital replicas of sporting venues and the events themselves becoming the norm, there's plenty of IT infrastructure and data to target – and via a multitude of components."

Geopolitical Tensions Potentially Stoking Flames This Year

State-sponsored attacks may pose the highest risk of all. After the 2022 invasion of Ukraine, the IOC banned Russian athletes from competing for their country, potentially fueling cyberattacks on the Games. In response to the ban, Russia will host the second "World Friendship Games," a multi-sport international event. It is likely that, to promote its own event and create disruption and distraction to the Paris Olympics, Russia will carry out cyberattacks targeting the Paris Games. Misinformation campaigns aimed at tarnishing the Games' reputation, including accusations of abuse, unfair treatment, physical danger, cheating, corruption and ecological issues may likely occur. In addition, there is a moderate to low possibility of sabotage and tampering attacks, such as scores or results manipulation, to undermine trust in the Games.

Hacktivist activities (acts perpetrated to further a social or political agenda) by threat actors have notably increased over the past year and the upcoming Paris Olympics presents an attractive event to propagate these types of messages. Disruptive attacks, primarily Distributed Denial of Service (DDoS) attacks or even ransomware events, are expected to be carried out by pro-Russian and anti-Israeli actors. Pro-Russian hacktivists are likely to target the Games in response to the ban from 2020, while anti-Israeli groups may focus on conveying their message to further amplify their voices. It is important to note that certain state-sponsored actors use hacktivism to mask their attacks.

Separately, cybercriminals see an easy opportunity to create scams, with fake promotion offers, ticket passes, hospitality reservations and public services. Since the beginning of the year, more than 1,000 domain names have been purchased with the word "Olympic." Teneo Risk's cyber analysts suspect that many of these domains are malicious and will be used for fake websites and

phishing attacks. Given the importance of infrastructure availability and access to data during the Games, these threats pose significant concerns, not only for event organizers and participants, but also for all surrounding organizations associated with the event.

Teneo's Risk Advisory team assesses that while China, Iran and North Korea are capable of hostile cyber activities, Russia is the primary threat actor. France has been a repeated target of Russian cyber aggression for its role in NATO as well as the war in Ukraine. In March of this year, Russian-speaking hacktivist group Anonymous Sudan claimed responsibility for highly disruptive DDoS attacks aimed at a range of French government ministries. As recently as May 21, a local Internet service provider in New Calcedonia was flooded with traffic intended to saturate and disrupt Internet access in advance of President Macron's trip to the archipelago. The responsible IP addresses appeared to originate from Russia.

Paris 2024 Preparations

The Paris Olympics will be the largest event ever organized in France. The French government, in collaboration with international bodies and cybersecurity experts, has implemented a multi-faceted approach to ensure the cybersecurity of the Paris Olympics. Through strategic planning, technological innovation, public-private partnerships and continuous monitoring, they aim to protect the event from potential cyber threats and ensure its smooth and secure execution. The French National Agency for the Security of Information Systems (ANSSI) has been at the forefront of building the national cybersecurity framework, working closely with other national and international bodies. As part of this, ANSSI has developed a robust set of guidelines and protocols tailored specifically for the Olympics, focusing on critical infrastructure, data protection and incident response. In its 2023 Panorama of the Cyber Threat briefing, ANSSI notes that "large events offer attackers additional opportunities to act. In fact, they require the implementation of many information systems – often interconnected and sometimes created for the occasion – by a multitude of actors with heterogeneous security levels. Attackers can take advantage of this extended exhibition area to monitor or extort the organizers and participants. They are also likely to exploit media coverage to tarnish the image of the host country, or even disrupt the progress of the event."

IDC reports that in 2024, France will put roughly $94 million toward cybersecurity to protect the country leading up to and during the Olympics. France and Atos, the worldwide IT partner for the Olympics and Paris Olympics technology partner, are coordinating with cybersecurity experts across the globe to mitigate risk associated with these cyber threats. The Paris organizers, Atos and the IOC are working closely with South Korea's Olympic Games security team to better understand the attacks from 2020. As part of this effort, the collaboration has organized "war games" in which it hires ethical hackers to attack systems in place for the Games and offers "bug bounties" to those who discover vulnerabilities. The IOC has also held trainings for committee members on phishing scams.

Franz Regul, managing director for IT at Paris 2024, notes that "we're expecting the number of cyber security events to be multiplied by 10 compared to Tokyo (in 2021)." Despite that significant statistic, the IOC announced in January of this year that they have full confidence that French authorities will keep the Paris Olympics safe.

Considerations for Organizations and Spectators

In today's geopolitical and cyber threat climate, cyberattack attempts targeting the Olympic Games are guaranteed. However, as seen at the last two Olympic Games, properly-implemented cybersecurity efforts can effectively minimize the risk of a significant impact for viewers and participants.

- As organizations prepare for the Paris Games, it would be prudent to develop offline emergency alternatives for employees, visitors, athletes or other stakeholders to minimize disruptions. This is especially true for those in the Olympics' "supply chain" such as infrastructure providers, media, online applications and platforms supporting the Games, venues and sponsors.
- Crisis management plans and relevant crisis communications response plans should be revised and tested for specific Olympics-focused scenarios impacting access to critical infrastructure, Internet and mobile phone access. Given the importance of infrastructure availability and access to real-time data during the Games, these threats pose significant concerns, not only for event organizers and participants, but also for all surrounding organizations associated with the event.
- Crisis simulation exercises should be underway to help identify potential vulnerabilities and build resilience and redundancy into operations so that executives and boards are prepared to quickly convene and manage a range of crisis scenarios with a particular focus on sustained Internet disruption.
- CISOs and company IT experts should prepare their organizations for traditional cyber threats such as ransomware and DDoS attacks by:
  - Reviewing current asset inventories – especially those assets supporting Olympics and critical infrastructure and ensuring relevant monitoring and alerting functions focused on those assets are calibrated and ready to go for the upcoming events;
  - Ensuring multi-factor authentication (MFA) is deployed across company assets;
  - Reinforcing policies and procedures with employees related to data access and data management;
  - Raising awareness related to the increased probability of Olympics-branded phishing emails targeting employees and social-engineering attempts to steal credentials to gain access to systems.
- Threat monitoring teams should be keenly focused on calibrating social and traditional media and deep/dark web monitoring to address the unique threat environment associated with the Olympics.
- Safety and security teams should also ensure access and connectivity to intelligence reporting from law enforcement and key intelligence agencies to stay ahead of potential emerging issues, warnings or alerts.

Cybercriminals seeking financial gain will likely create scams with fake promotion offers, ticket passes, hospitality reservations and public services, posing some risk to attendees of the Games. All individuals, and especially ticketholders or spectators, should exercise caution when opening emails and links allegedly from the Olympics. Paris 2024 is a fully digitally ticketed event and therefore, Teneo's Risk Advisory team recommends that attendees ensure they purchase tickets through official Olympics websites and ticketing applications. Additionally, they should take snapshots of the official digital ticket images as a backup. The event organizers have already identified fraudsters attempting to scam the public by offering free tickets to the opening ceremony, charging only the

cost of shipping fees. The official website of the Paris 2024 Olympics ticketing office encourages individuals to contact them directly with any concerns related to potential fraud or authenticity of communications by the Olympics by reaching out to the following address: integrityandenforcement@paris2024.org.

To combat mis/disinformation campaigns, organizations should closely monitor and collaborate with social media platforms by establishing protocols to detect and report sources of false information for flagging or removal. For individuals, if something looks suspicious or doesn't seem credible, it is important to fact check before sharing or disseminating content further through corroboration or reporting. Lastly, while the previously mentioned cyberattack threats are most common and expected, this does not rule out the potential for a cyberattack which may cause panic, injury or the potential loss of life. Heightened awareness of the threat landscape and vigilance while present at the Games by everyone will help keep the focus on the primary objective: sports.

For more information, email: Resilience&Intelligence@teneo.com

Author

Courtney Adante
President, Security Risk Advisory
Courtney.Adante@teneo.com

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com