cybernews LIVE

Cyber Threat Landscape

2024 Olympic Games in Paris

Robert J Carloff
CYBER NEWS LIVE Reston VA & Canberra ACT

DROP BEAR
CYBER PRODUCTIONS®

Contents

Opening Statement

This is an independent cyber threat analysis for the 2024 Olympic Games in Paris (Paris 2024). Paris 2024 is scheduled from July 26 to August 11, 2024, with the Paralympics scheduled from August 28 to September 8, 2024. Like previous Olympic games, Paris 2024 is anticipated to encounter numerous cyber threats. This report delves into areas including crypto currencies, cyber threat actors, emerging technologies, scams, social media, sponsors, and supply chain attacks.

Undertaking the cyber threat analysis for the Olympics started to become a passion of mine in 2015 after completing the Cyber Threat Analysis for the 2016 Rio Olympics, where I undertook a leading role in conjunction with industry and government partners. Since then, I have completed every cyber threat analysis for the summer and winter games.

Please share this information widely.

1. Crypto Currency

Crypto currencies, such as Bitcoin, have gained significant traction in recent years as digital alternatives to traditional currencies. However, along with their growing popularity, these digital assets have become targets for various cyber threats. In this section we will provides insights into the cyber threats associated with crypto currencies, including digital currency, digital wallets, and non-fungible tokens.

Crypto currencies, such as Bitcoin, have gained significant traction in recent years as digital alternatives to traditional currencies. However, along with their growing popularity, these digital assets have become targets for various cyber threats. In this section, we will provide insights into the cyber threats associated with crypto currencies, including digital currency, digital wallets, and non-fungible tokens can have an impact on Paris 2024.

Crypto Currency (Bitcoin)

Bitcoin, as the leading crypto currency, is a prime target for cyber threats due to its widespread adoption and high market value. Threat actors may employ various tactics to exploit vulnerabilities in Bitcoin networks, including:

- **Ransomware Attacks:** Cyber criminals leverage Bitcoin's anonymity and decentralization to demand payments in exchange for decrypting encrypted data, evading detection and accountability.
- **Phishing Scams:** Fraudulent websites and emails impersonate legitimate crypto currency platforms to deceive users into revealing private keys or login credentials, resulting in theft of funds from digital wallets.
- **Exchange Hacks:** Cyber attackers target crypto currency exchanges to pilfer digital assets stored in online wallets, causing substantial financial losses for both users and exchanges.

Digital Currency (National Crypto currency in France)

While France has explored the possibility of introducing a national digital currency (Central Bank Digital Currency, CBDC), known as the digital euro, the concept presents its own set of cyber threats:

- **Cyber Espionage:** State-sponsored threat actors may target CBDC infrastructure to gather intelligence or disrupt financial systems, potentially undermining national security, and economic stability.
- **Data Privacy Concerns:** The centralized nature of CBDCs raises concerns about data privacy and security, as large-scale data breaches could compromise sensitive financial information of citizens.

Digital Wallets

Digital wallets, used to store and manage crypto currencies, are susceptible to various cyber threats:

- **Malware Attacks:** Malicious software can compromise digital wallets, enabling threat actors to steal private keys or manipulate transactions, leading to unauthorized fund transfers.
- **Phishing Attacks:** Cyber criminals employ phishing emails or counterfeit websites to deceive users into divulging their wallet credentials, granting unauthorized access to crypto currency funds.

Non-Fungible Tokens (NFTs)

NFTs, which represent unique digital assets such as art, collectibles, and virtual real estate, have recently emerged as a lucrative target for cyber threats:

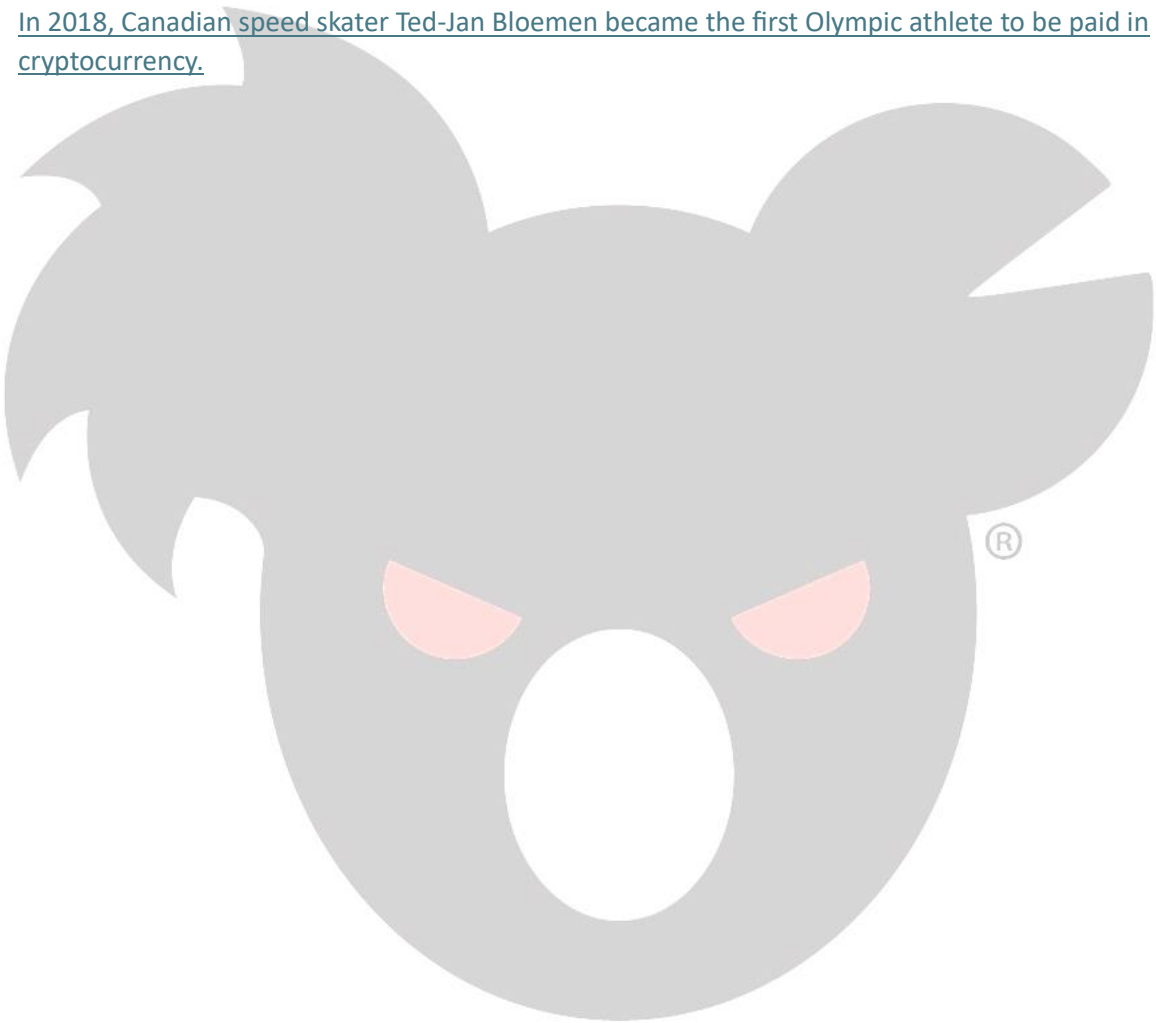
- **Fraudulent Sales:** Scammers exploit the hype surrounding NFTs by selling counterfeit or plagiarized digital artworks, deceiving buyers into purchasing illegitimate tokens.
- **Smart Contract Vulnerabilities:** NFT platforms and marketplaces utilizing smart contracts are vulnerable to coding errors or exploits, potentially leading to theft or manipulation of NFT assets.

Conclusion

As crypto currencies continue to proliferate and evolve, the cyber threats targeting these digital assets are likely to escalate. To mitigate these risks, stakeholders must remain vigilant against emerging threats, implement robust cyber security measures, and educate users about best practices for securely managing and transacting with crypto currencies, digital wallets, and non-fungible tokens. Additionally, regulatory authorities and industry stakeholders must collaborate to establish frameworks and standards aimed at enhancing the security and resilience of crypto currency ecosystems.

Examples

- The 2022 Winter Olympics in Beijing featured crypto as a major part of the event.
- In 2018, Canadian speed skater Ted-Jan Bloemen became the first Olympic athlete to be paid in cryptocurrency.



2. Cyber Threat Actors

2.1 Nation State:

Nation-state and sophisticated cyber threat actors pose significant risks to organisations and governments worldwide. These threat actors are often well-funded, highly skilled, and motivated by political, economic, or strategic interests. They employ a range of tactics, including advanced persistent threats (APTs), social engineering, and zero-day exploits, to infiltrate target networks, exfiltrate sensitive data, and disrupt critical operations. Key characteristics and tactics of these actors can include:

Targeting Trade Secrets and Sensitive Information

Nation-state and sophisticated threat actors frequently target organisations to steal trade secrets, intellectual property, and sensitive information. They employ sophisticated cyber espionage

techniques, such as advanced persistent threats (APTs), to infiltrate networks, exfiltrate data, and gain a competitive advantage. Targeted industries may include technology, defense, finance, and healthcare, among others.

Supporting National Interests

Cyber threat actors affiliated with nation-states frequently conduct their operations with the backing or guidance of governmental bodies, aiming to promote their country's national interests, strategic goals, or geopolitical agendas. Their actions encompass a wide array of tactics, including espionage, sabotage, dissemination of disinformation, and engagement in cyber warfare. These actors often target critical infrastructure, governmental agencies, military establishments, and diplomatic organisations as part of their efforts to achieve their objectives and exert influence on a global scale.

Mitigation Strategies

Enhanced Cyber Security Measures:

To detect and mitigate threats posed by nation-state and sophisticated actors, organisations and governments must implement robust cyber security measures. These measures include network segmentation, encryption, intrusion detection systems (IDS), and endpoint protection solutions. Regular security assessments, penetration testing, and incident response planning are essential to strengthen defenses against evolving threats.

Information Sharing and Collaboration:

Collaboration among government agencies, industry sectors, and international partners is critical for sharing threat intelligence, identifying emerging threats, and coordinating responses to cyber attacks. Public-private partnerships, sector-specific information sharing and analysis centers (ISACs), and international cyber security initiatives facilitate collective defense efforts and enhance resilience against cyber threats.

Regulatory Compliance and Cyber Hygiene:

Compliance with cyber security regulations and industry standards, such as the NIST Cyber security Framework, GDPR, and ISO 27001, helps organisations establish baseline security practices and safeguard sensitive information from unauthorised access or disclosure. Cyber hygiene practices, including regular software patching, user training, and access control, are essential for minimizing vulnerabilities and preventing unauthorized access by threat actors.

Conclusion

Nation-state and sophisticated cyber threat actors pose significant challenges to global cyber security, targeting trade secrets, sensitive information, and critical infrastructure to advance national interests. To counter these threats effectively, organisations and governments must adopt a proactive approach to cyber security, leveraging advanced technologies, collaborative partnerships, and regulatory compliance to enhance resilience and protect against evolving cyber threats.

2.2 Organised Crime:

This report explores the rising threat of financially motivated cyber crime, with a particular focus on the frequent use of social engineering tactics. We will analyse the different methods employed by cyber criminals to achieve their goals and the potential impacts on individuals and organisations.

Financially Motivated Activities:

Cyber crime has become a major concern, driven primarily by financial gain. Cyber criminals employ various tactics to steal money and valuable information, including:

- **Data Breaches:** Hacking into computer systems to steal sensitive data, such as credit card information, personal identification details, and intellectual property.
- **Ransomware Attacks:** Encrypting a victim's data and demanding a ransom payment for decryption.
- **Phishing and Smishing:** Sending fraudulent emails or text messages designed to trick victims into revealing personal information or clicking on malicious links.
- **Online Payment Fraud:** Stealing credit card details or using fake accounts to make unauthorized purchases.

Frequent Use of Social Engineering:

Social engineering is a manipulative tactic used by cyber criminals to exploit human trust and gain access to information or systems. Common methods include:

- **Pretexting:** Creating a false scenario to gain a victim's trust, such as impersonating a legitimate organisation.
- **Baiting:** Offering something enticing, like a gift or prize, to lure victims into clicking on malicious links or downloading malware.
- **Tailgating:** Physically following authorized individuals into secure areas.
- **Quid Pro Quo:** Offering to perform a service or provide information in exchange for sensitive details.
- **Shoulder Surfing:** the act of spying on someone's screen or keyboard while they are using a computer, ATM, or other electronic device, typically in a public place.

Potential Impacts:

Financially motivated cyber crime has far-reaching consequences, impacting individuals and organisations alike. Some potential repercussions include:

- **Financial Losses:** Individuals can suffer financial hardship due to stolen money or identity theft. Organisations may face significant financial losses from data breaches, ransom payments, and fraudulent activities.
- **Reputational Damage:** Data breaches and other cyber attacks can damage an organisation's reputation, leading to a loss of trust from customers and partners.
- **Operational Disruption:** Cyber attacks can disrupt business operations, leading to downtime, productivity loss, and hindered service delivery.

Conclusion:

Financially motivated cyber crime, particularly when coupled with frequent social engineering tactics, poses a significant threat to individuals and organisations. Remaining vigilant, practicing safe online habits, and implementing robust security measures are crucial to mitigate these risks. Organisations should invest in security awareness training for employees to enhance their ability to identify and avoid social engineering attempts.

Recommendations:

- **Individuals:** Be cautious when clicking on links or opening attachments in emails or text messages, even if they appear to be from legitimate sources.
- **Organisations:** Implement multi-factor authentication, regularly update software and security systems, and conduct regular security awareness training for employees.

By staying informed and taking proactive measures, individuals and organisations can better protect themselves from the evolving threats of financially motivated cyber crime.

2.3 Cyber Terrorism

In this section we will examine the growing threat of cyber terrorism, focusing on its politically or ideologically motivated nature and its goal of instilling fear through destructive attacks. We will explore the methods employed by cyber terrorists, potential targets, and the unique challenges cyber terrorism poses compared to traditional terrorism.

Politically or Ideologically Motivated Actions:

Cyber terrorism differs from other forms of cyber crime in its primary motivation. Unlike financially motivated attacks, cyber terrorism aims to achieve **political or ideological goals**, such as:

- Promoting a specific ideology or agenda
- Undermining government authority and public trust
- Disrupting critical infrastructure and essential services
- Influencing public opinion and sparking social unrest

Cyber terrorists are often affiliated with **extremist organisations, hacktivist groups, or lone actors** driven by strong ideological convictions.

Goal to Instil Fear through Destructive Attacks:

Cyber terrorists primarily seek to **instil fear** within a population or government. They achieve this by launching destructive attacks that can cause significant damage and disruption:

- **Disrupting critical infrastructure:** This includes targeting power grids, transportation systems, and communication networks to create widespread chaos and panic.
- **Attacking financial institutions:** Disrupting financial services can cripple the economy and create economic instability.

- **Spreading misinformation and propaganda:** Cyber terrorists can manipulate social media and online platforms to spread false information, sow discord, and erode public trust in institutions.
- **Stealing and leaking sensitive data:** Exposing government secrets, corporate information, or personal data can have a significant impact on national security, individual privacy, and public trust.

The Uniqueness of Cyber Terrorism:

Cyber terrorism presents unique challenges compared to traditional terrorism:

- **Accessibility:** The low barrier to entry makes it easier for individuals or groups with limited resources to launch cyber attacks.
- **Anonymity:** Cyber terrorists can operate anonymously, making it difficult to track down and apprehend them.
- **Global Impact:** Cyber attacks can transcend physical borders, causing widespread disruption and affecting individuals and organisations worldwide.

Conclusion:

Cyber terrorism is a growing threat with the potential to cause widespread damage and disrupt critical infrastructure, economies, and societies. Understanding the motivations, goals, and tactics of cyber terrorists is crucial for developing effective mitigation strategies.

Recommendations:

- **Governments:** Invest in robust cyber security infrastructure, strengthen international cooperation to combat cyber crime, and raise public awareness about the threat of cyber terrorism.
- **Organisations:** Implement robust security measures, conduct regular vulnerability assessments, and educate employees on cyber security best practices.
- **Individuals:** Be vigilant online, practice good cyber hygiene, and refrain from sharing sensitive information on public platforms.

By working together, governments, organisations, and individuals can enhance their collective resilience against the evolving threat of cyber terrorism.

2.4 Hacktivism

In this section we will address the potential threat of hacktivism directed towards Paris 2024. Hacktivism, the use of digital tools and techniques to advance social or political agendas, poses a unique challenge due to its diverse motivations, disruptive tactics, and potential involvement of insiders.

Hacktivism and the Olympics:

The Olympic Games represent a high-profile international event, making them an attractive target for hacktivist groups seeking to:

- **Raise awareness for a specific cause:** Hacktivists may target the Olympics to draw attention to social or political issues they consider neglected by the international community.
- **Disrupt the event:** Launching cyber attacks on critical infrastructure or operational systems could disrupt the smooth running of the Games, generating negative publicity and impacting the event's integrity.
- **Embarrass the host nation:** Hacktivists might target French government systems or Olympic organisers to expose vulnerabilities and undermine public trust in the host nation's ability to secure the event.

Disruptive Attacks and Insider Threats:

Hacktivist attacks often take the form of:

- **Distributed Denial-of-Service (DDoS) attacks:** Overwhelming websites or online services with traffic, rendering them inaccessible to legitimate users.
- **Defacement of Websites:** Altering the visual appearance of websites with messages or images promoting the hacktivist's cause.
- **Data Breaches:** Stealing or leaking sensitive information, such as athlete data, ticketing information, or internal communications.

These attacks can significantly disrupt the Games, leading to operational delays, financial losses, and reputational damage.

A particularly concerning aspect of hacktivism is the potential involvement of **insiders**. Individuals with authorised access to systems may be sympathetic to the hacktivist cause or susceptible to manipulation, making them vulnerable to social engineering tactics. Detecting such insider threats is challenging due to their authorized access privileges.

Varied Motivations and Challenges in Detection:

Hacktivists are driven by diverse motivations, including:

- **Fraud:** Stealing financial resources or personal information for personal gain.
- **Revenge:** Targeting individuals or organisations perceived as having wronged a specific group or cause.
- **Desire for destruction:** Causing widespread disruption and damage, often with an element of anarchism.

This diversity makes it difficult to predict or prevent hacktivist attacks, as they may not follow the traditional financial motivations observed in typical cyber crime. Additionally, the authorised access to insider threats makes their activities harder to detect and raises concerns about potential collusion with external actors.

Recommendations:

- **Enhance cyber security measures:** Strengthen network security, implement robust access controls, and conduct regular vulnerability assessments.

- **Raise awareness and training:** Educate staff, athletes, and stakeholders about cyber threats and best practices for secure online behaviour.
- **Foster international cooperation:** Collaborate with international partners to share intelligence, identify potential threats, and develop coordinated defensive strategies.
- **Monitor social media:** Track online discourse and social media activity to identify potential threats and emerging hacktivist campaigns.

Conclusion:

Paris 2024 is vulnerable to hacktivist attacks, which could lead to significant disruption and reputational damage. Understanding the motivations, tactics, and challenges associated with hacktivism is crucial for implementing effective protective measures.

2.5 Advanced Persistent Threats (APTs)

In this section we examine the potential threat posed by Advanced Persistent Threats (APTs) to Paris 2024. APTs, well-resourced adversaries engaging in sophisticated long-term cyber operations, present a significant risk due to their targeted nature, prolonged access, and potential objectives of espionage, data theft, and disruption.

APTs and the Olympics:

The high-profile nature of the Olympic Games makes them an attractive target for APTs seeking to achieve various objectives:

- **Espionage:** Stealing sensitive information related to Olympic strategy, logistics, athlete data, and intellectual property.
- **Data theft:** Targeting personal information of athletes, officials, and spectators for financial gain or future exploitation.
- **Disruption and destruction:** Disrupting critical infrastructure or operational systems to cause chaos, damage the event's integrity, and potentially influence political or geopolitical agendas.

Examples of APTs known to target major events include:

- **Fancy Bear (Russia):** Linked to cyber attacks against various sporting organisations and anti-doping agencies.

Targeted and Prolonged Network Intrusion:

APTs differ from traditional cyber attacks in their approach:

- **Targeted:** They meticulously research and target specific individuals, organisations, or systems related to Paris 2024.
- **Prolonged:** APTs establish persistent access to networks over extended periods, allowing them to gather intelligence, steal data, or lay the groundwork for future attacks.
- **Sophisticated tactics:** They employ advanced techniques to bypass security defenses, such as social engineering, zero-day exploits, and custom malware.

These characteristics make APTs particularly challenging to detect and mitigate, increasing their potential impact on the Games.

Risks and Potential Impact:

A successful APT attack on Paris 2024 could have significant consequences:

- **Data breaches:** Exposure of sensitive information could damage the reputation of the organising committee, athletes, and sponsors.
- **Disruption of operations:** Compromised critical infrastructure or operational systems could disrupt ticketing, broadcasting, or other essential services.
- **Financial losses:** Data breaches, operational disruptions, and reputational damage could result in substantial financial losses for organisers and stakeholders.
- **Geopolitical tensions:** Depending on the origin of the APT, successful attacks could exacerbate existing geopolitical tensions and international relations.

Conclusion:

The potential threat posed by APTs to Paris 2024 necessitates a proactive and coordinated approach. Understanding their tactics, motivations, and potential targets is crucial for implementing effective risk mitigation strategies.

Recommendations:

- **Enhance cyber security posture:** Implement robust security measures with multi-factor authentication, data encryption, and continuous monitoring.
- **Intelligence gathering and threat sharing:** Foster collaboration with international partners to share intelligence on potential APT activity and emerging threats.
- **Incident response preparedness:** Develop and rehearse comprehensive incident response plans to effectively address potential attacks.
- **Security awareness training:** Educate staff, athletes, and stakeholders on cyber threats and best practices for secure online behavior.

By taking these steps, organisers can significantly reduce the vulnerability of the 2024 Olympic Games to sophisticated cyber attacks by APTs, ensuring a safe and secure event for all participants.

2.6 Cyber Espionage

In this section, we examine the various cyber espionage threats potentially endangering Paris 2024. Building upon past examples such as Fancy Bear's intrusion into anti-doping agencies, the report explores potential avenues for cyber espionage and the evolving landscape of cyber threats, including ransomware, destructive malware, and website defacement. Additionally, the report addresses the challenges posed by emerging technological advancements.

Cyber Espionage: Learning from the Past, Preparing for the Future:

Espionage targeting the Olympics is not a new phenomenon. Cases like Fancy Bear targeting the United States Anti-Doping Agency (USADA) illustrate the potential for cyber attacks aimed at:

- **Stealing confidential information:** This could include athlete training routines, competition strategies, doping test results, and intellectual property related to technology used in the Games.
- **Gaining a competitive advantage:** Leaking stolen information could help competing nations gain an unfair advantage in various sporting events.
- **Undermining trust and integrity:** Successful cyber espionage attacks can damage public trust in the Olympic Games and cast doubt on the fairness of competition.

Evolution of Threats: Beyond Traditional Espionage:

While espionage remains a primary concern, cyber criminals are constantly evolving their tactics:

- **Ransomware:** Attackers could exploit vulnerabilities and encrypt critical infrastructure or data, demanding a ransom for its recovery. This could significantly disrupt operations and lead to financial losses.
- **Destructive malware:** Malicious software designed to destroy or render data and systems inoperable could be deployed to disrupt critical infrastructure, causing delays and operational chaos.
- **Website defacement:** Hackers may target official Olympic websites or those of sponsors, replacing content with messages promoting specific agendas or causing reputational damage.

Emerging Technology Advancements: A Double-Edged Sword:

The use of emerging technologies at Paris 2024, while potentially enhancing the Games, also introduces new attack vectors:

- **Internet of Things (IoT) devices:** The increased use of smart devices for ticketing, access control, and other purposes could create vulnerabilities if not adequately secured.
- **Artificial intelligence (AI):** AI-powered systems used for security, logistics, or athlete performance analysis can be susceptible to manipulation or sabotage.
- **Cloud computing:** Reliance on cloud-based infrastructure for data storage and processing necessitates robust security measures to prevent unauthorized access or data breaches.

Conclusion:

Paris 2024 presents a complex cyber security landscape, with espionage threats combining with evolving tactics and emerging technologies. A comprehensive approach is crucial to mitigate these risks, ensuring the safety, security, and integrity of the event.

Recommendations:

- **Implement robust cyber security measures:** Regularly assess vulnerabilities, enforce strong passwords, and utilize advanced security solutions.

- **Foster international collaboration:** Share intelligence and best practices with other participating countries and international security organisations.
- **Raise awareness and training:** Educate staff, athletes, and stakeholders on potential cyber threats and best practices for secure online behaviour.
- **Embrace secure technology adoption:** Thoroughly assess and implement emerging technologies with robust security protocols to minimize risks.

By recognising these potential threats and taking proactive measures, organisers can ensure Paris 2024 is a safe and successful event, celebrating athletic excellence while mitigating the ever-evolving landscape of cyber security threats.

Examples

- Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban
- Inside Fancy Bear's Arsenal: An Update on the Cyber Tactics of APT28
- Fancy Bear hackers targeted at least 16 athletic organisations ahead of Tokyo Olympics

3. Emerging Technology Advancements

Artificial Intelligence, Machine Learning, and Deepfakes

In this section of the report, we will examine the potential cyber threats posed by emerging technologies like Artificial Intelligence (AI), Machine Learning (ML), and Deepfakes to Paris 2024. While these technologies offer potential benefits such as enhanced security and personalized experiences, their misuse can create significant challenges.

Emerging Technologies and the Olympics: A Double-Edged Sword:

- **AI and ML:** These technologies offer potential benefits:
    - **Enhanced security:** AI can analyse vast amounts of data to identify suspicious activity and potential security threats.

  - **Personalized experiences:** ML can personalize the spectator experience by tailoring information and services based on individual preferences.
- **Deepfakes:** Deepfakes, hyper-realistic synthetic media, pose potential risks:
  - **Misinformation and disinformation:** Fabricated videos or audio recordings featuring athletes or officials can spread misinformation, damage reputations, and sow confusion.
  - **Social engineering:** Deepfakes can be used to impersonate officials in phishing attempts or social engineering scams targeting athletes, staff, or sponsors.

Potential Impacts of Misuse:

Malicious actors could exploit these technologies for various purposes:

- **Disrupting operations:** AI-powered bots could overwhelm ticketing systems or launch Denial-of-Service (DoS) attacks on critical infrastructure.
- **Manipulation and fraud:** Deepfakes could be used to manipulate financial transactions, spread propaganda, or influence public opinion against specific athletes or nations.
- **Erosion of trust:** Widespread use of deepfakes could erode public trust in the integrity of the Games and the authenticity of information disseminated through official channels.

Mitigating the Risks:

Combatting these emerging threats requires a multi-pronged approach:

- **Proactive security measures:** Implement robust AI security protocols to detect and prevent malicious AI applications.
- **Media literacy training:** Educate staff, athletes, and spectators on how to identify and critically evaluate information, especially online content.
- **Public awareness campaigns:** Raise awareness about the potential misuse of AI and deepfakes to promote transparency and encourage responsible use of technology.
- **International collaboration:** Establish collaborative frameworks with international partners to share intelligence and develop joint response strategies.

Conclusion:

While emerging technologies present exciting opportunities for the Olympics, it is crucial to acknowledge and address the potential misuse of AI, ML, and deepfakes. By taking proactive steps and fostering international cooperation, organisers can mitigate these threats and ensure the 2024 Olympic Games are a celebration of athletic excellence and technological innovation while upholding security and integrity.

Examples

- How emerging technologies could shape the 2032 Olympics
- Reflecting on 20 years of technology transformation at the Olympic Games

4. Scams

In section of the report, it examines the potential threat posed by scam lists targeting the excitement surrounding Paris 2024. These scams exploit the public's desire for exclusive access or insider information, often involving fake ticket lotteries, merchandise fraud, and other deceptive practices.

Scams: Capitalizing on Hype

Scams are deceptive marketing schemes that lure victims with the promise of exclusive benefits or scarce resources. The allure of the Olympic Games makes them a prime target for such scams:

- **Fake Ticket Lotteries:** Emails or social media posts advertise non-existent lotteries offering a chance to win Olympic tickets. These scams often involve upfront fees or require victims to disclose personal information.

- **Ticket Resale Fraud:** Fraudulent online marketplaces or social media accounts offer fake or overpriced tickets to the Games.
- **Merchandise Scams:** Websites or social media pages advertise counterfeit or low-quality Olympic merchandise, exploiting the desire for official memorabilia.
- **Accommodation Scams:** Fake listings lure victims into paying for non-existent or overpriced accommodations near Olympic venues.
- **Sports Betting Scams:** Involve fraudulent schemes aimed at deceiving individuals who engage in sports betting activities, typically for financial gain.

Impact on the Public:

List scams targeting the Olympics can have a significant negative impact on the public:

- **Financial losses:** Victims may lose money by paying for fake tickets, fraudulent merchandise, or non-existent accommodations.
- **Identity theft:** Disclosure of personal information through list scams can lead to identity theft and further financial losses.
- **Erosion of trust:** Widespread scams can create a sense of distrust and uncertainty surrounding legitimate ticket sales and merchandise channels.
- **Negative perception of the Games:** The prevalence of scams can tarnish the public image of the Olympics and discourage genuine spectators from participating.

Identifying List Scams:

Several red flags can help identify list scams:

- **Unrealistic promises:** Offers of guaranteed tickets, exclusive merchandise, or deeply discounted accommodations are often too good to be true.
- **Urgency and pressure:** Scammers often create a sense of urgency, pressuring victims to act quickly before the "opportunity" disappears.
- **Poor grammar and typos:** Legitimate organisations typically maintain professional communication standards.
- **Suspicious payment methods:** Requests for payment through unusual methods like money transfers or prepaid cards are indicative of scams.

Recommendations:

- **Public awareness campaigns:** Educate the public on common list scams associated with the Olympic Games and how to identify them.
- **Collaboration with ticketing platforms:** Work with official ticketing platforms to promote secure and legitimate ticket purchase channels.
- **Monitor online marketplaces:** Proactively monitor online marketplaces and social media platforms for suspicious activity and fraudulent listings.
- **Reporting mechanisms:** Establish clear channels for reporting suspected list scams to relevant authorities.

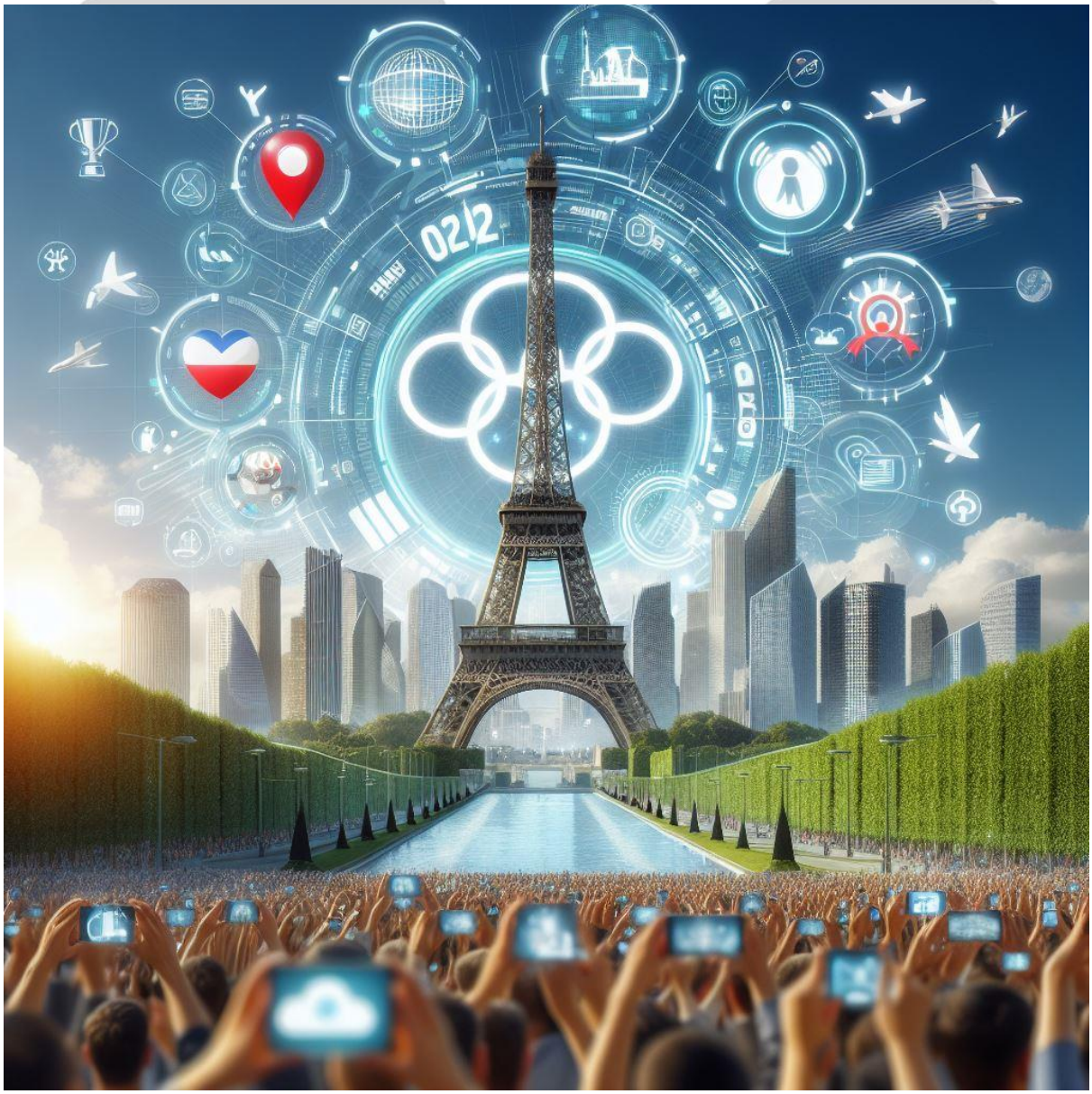
Conclusion:

List scams pose a significant threat to the public and the reputation of the 2024 Olympic Games. By raising awareness, collaborating with relevant stakeholders, and implementing effective reporting mechanisms, organisers can minimize the impact of these deceptive practices and ensure a positive experience for genuine spectators.

Examples

- Top 4 Olympic Games Scams – How to Protect Yourself
- Olympic 2024: tickets already sold illegally on the internet, 44 fraudulent sites identified

5. Social Media



Social media platforms like Instagram, Meta (Facebook), TikTok, and X (formally Twitter) will undoubtedly play a significant role in the 2024 Olympic Games in France. While offering opportunities for engagement and information dissemination, these platforms also present potential cyber threats. This report examines the role of social media in the context of the Games, highlighting both its benefits and the potential threats associated with its use.

Social Media: A Powerful Tool for the Olympics:

- **Engagement and Community Building:** Social media fosters engagement between athletes, fans, and stakeholders, creating a global community around the Games.
- **Information Sharing:** Real-time updates, event highlights, and behind-the-scenes content can be shared instantaneously, keeping audiences informed and excited.
- **Brand Promotion:** Official Olympic accounts and athlete profiles can be leveraged for promoting sponsorships, ticketing, and merchandise sales.
- **Global Audience Reach:** Social media allows for a wider reach, engaging fans across the globe and raising awareness about the Games.

Potential Threats Posed by Social Media:

- **Misinformation and Disinformation:** The rapid spread of unverified information can create confusion, fuel negativity, and damage the reputation of athletes or the Games.
- **Targeted Harassment and Abuse:** Athletes and officials can be subjected to online harassment, bullying, and hate speech, impacting their mental well-being.
- **Fake Accounts and Bots:** Malicious actors can use fake accounts or bots to manipulate public opinion, spread misinformation, or launch coordinated attacks.
- **Doping Rums and Scandals:** Fabricated accusations and rumours regarding doping can spread rapidly on social media, tarnishing athletes' reputations.
- **Ticket Scalping and Fraud:** Social media platforms may be exploited for selling counterfeit or overpriced tickets, leading to financial losses for fans.

The Role of Social Media Platforms:

Social media platforms have a responsibility to mitigate the threats associated with their platforms:

- **Content moderation:** Implement robust content moderation practices to identify and remove hate speech, misinformation, and fake accounts.
- **Promoting media literacy:** Partner with organisers to promote media literacy initiatives, encouraging users to critically evaluate information online.
- **Transparency and cooperation:** Work transparently with the Olympic organisers to address potential threats and ensure responsible use of platforms.

Recommendations for the 2024 Games:

- **Social media guidelines:** Develop clear guidelines for athletes, officials, and stakeholders regarding responsible social media usage during the Games.

- **Monitoring and reporting systems:** Establish efficient monitoring and reporting mechanisms to identify and address potential threats quickly.
- **Partnerships with platforms:** Foster collaboration with social media platforms to proactively tackle misinformation, harassment, and other malicious activities.
- **Media literacy campaigns:** Educate the public on how to identify credible sources, verify information, and report suspicious content online.

Conclusion:

Social media holds immense potential for the 2024 Olympic Games. By acknowledging both its benefits and potential threats, organisers and social media platforms can work together to ensure a positive and secure online environment that celebrates athletic excellence and fosters global unity.

Examples

- How Social Media Changed the Olympics, and What It Means for #Rio2016
- Social Media and the Olympics: A Chance for Improving Gender Equality
- How social media impacts athletes at the Olympics
- The Impact and Role of Social Media at the Olympics

6. Sponsor Matrix

Paris 2024 will rely heavily on sponsorships to support the event. While official sponsors provide vital financial resources, they also introduce an element of risk to the Games' overall cyber security posture. In this section, we will examine the "Sponsor Matrix," identifying potential vulnerabilities associated with official sponsors and outlining strategies to mitigate these risks.

Sponsor Matrix: A Complex Ecosystem:

Paris 2024, involve a multitude of official sponsors across various industries. These sponsors:

- **Provide financial support:** Sponsorship funds fuel the Games' operation and infrastructure development.

- **Enhance brand awareness:** Sponsors leverage the Games' global reach to promote their products and services.
- **Offer technological solutions:** In some cases, sponsors may provide technology infrastructure or services for the Games.

Potential Risks Associated with Sponsors:

- **Supply Chain Attacks:** A cyber attack targeting a sponsor's infrastructure could potentially compromise Olympic systems connected to their services.
- **Data Breaches:** A data breach at a sponsor company could expose sensitive Olympic information shared with them for marketing or logistical purposes.
- **Brand Hijacking:** Malicious actors could exploit a sponsor's brand associated with the Games for phishing attacks or to spread misinformation.
- **Reputational Risk:** Negative publicity surrounding a sponsor's cyber security practices could tarnish the image of the Games.

Mitigating Sponsor-Related Risks:

- **Thorough vetting:** Implement a rigorous vetting process to assess the sponsors' cyber security posture before entering into agreements.
- **Data sharing agreements:** Establish clear data sharing agreements outlining specific information exchange practices and data security protocols.
- **Penetration Testing and Security Audits:** Encourage sponsors to conduct regular penetration testing and security audits of their systems to identify vulnerabilities.
- **Information Security Awareness Training:** Collaborate with sponsors to promote information security awareness training for their employees who handle Olympic-related data.

Sponsor Matrix Considerations:

- **Shared Responsibility:** Emphasize the shared responsibility between organisers and sponsors for maintaining robust cyber security throughout the Games.
- **Incident Response Planning:** Develop a comprehensive incident response plan outlining procedures for responding to cyber attacks that might involve sponsors' systems.
- **Transparency and Communication:** Maintain open communication with sponsors regarding cyber security threats and potential mitigation strategies.

Conclusion:

The "Sponsor Matrix" presents both opportunities and challenges for Paris 2024. By adopting a proactive approach and fostering a collaborative environment, organisers can leverage sponsorships while effectively managing the associated cyber security risks.

7. Supply Chain Attacks

Supply chain attacks, targeting third-party vendors and partners, are a growing threat to large-scale events like Paris 2024. In this section, we will explore the increasing frequency and potential impact of supply chain attacks, highlighting the vulnerabilities they pose to the Games' critical infrastructure and operational integrity.

Supply Chain Attacks: A Rising Threat Landscape:

Supply chain attacks involve compromising a seemingly less secure vendor or partner within an organisation's network to gain access to the main target – in this case, the Olympic infrastructure.

The increasing frequency of these attacks can be attributed to several factors:

- **Expanded attack surface:** Organisations rely on an ever-growing network of vendors and partners, significantly expanding the potential entry points for attackers.
- **Focus on weakest links:** Attackers often target less-resourced vendors with weaker cyber security posture to gain easier access to the main target.
- **Sophisticated techniques:** Attackers leverage increasingly sophisticated tactics like social engineering and zero-day exploits to bypass security measures.

Potential Impact on Paris 2024:

Supply chain attacks pose a significant threat to the 2024 Olympic Games in several ways:

- **Disruption of Critical Services:** Compromised vendors involved in critical services like ticketing, broadcasting, or venue management could disrupt crucial aspects of the Games.
- **Data Breaches:** Attackers may steal sensitive information about athletes, spectators, sponsors, or organisational plans through compromised vendors' systems.
- **Financial Losses:** Data breaches or operational disruptions caused by supply chain attacks can lead to financial losses for organisers and stakeholders.
- **Reputational Damage:** A successful supply chain attack can tarnish the reputation of the Games and raise concerns about security and data privacy.

Conclusion:

Supply chain attacks pose a complex and evolving threat to the 2024 Olympic Games. By proactively addressing this issue and implementing robust mitigation strategies, organisers can create a more secure ecosystem for the Games, protecting critical infrastructure, sensitive data, and the overall integrity of the event.

Mitigating Supply Chain Risks:

Several measures can be taken to mitigate the risk of supply chain attacks:

- **Vendor Risk Management:** Implement a robust vendor risk management program to assess the cyber security posture of all vendors involved in the Games.
- **Contractual Obligations:** Incorporate strong cyber security clauses into contracts with vendors, outlining expectations and compliance requirements.
- **Security Awareness Training:** Extend security awareness training programs to include vendors and their employees handling Olympic-related data.
- **Threat Intelligence Sharing:** Foster collaboration and information sharing among organisers, vendors, and relevant authorities to stay updated on evolving threats.
- **Multi-factor Authentication:** Encourage vendors to implement multi-factor authentication (MFA) for all access points to their systems.

Examples

- Paris Olympics Threatened by Cyberattacks
- Tokyo Olympics becomes the latest victim of the Fujitsu hackers

- Supply chain not to blame for Olympic shortages

Overarching Conclusion

In conclusion, the cyber threat analysis for the Paris 2024 underscores the critical importance of robust cyber security measures in safeguarding the integrity, security, and success of the event. As with any major international gathering, Paris 2024 faces a diverse array of cyber threats, ranging from sophisticated cyber espionage tactics to emerging risks posed by emerging technologies and social engineering scams.

To effectively mitigate these threats, stakeholders must adopt a proactive and collaborative approach, leveraging advanced cyber security technologies, sharing threat intelligence, and implementing robust defense strategies. Additionally, continuous monitoring, regular security assessments, and comprehensive incident response planning are essential components of a resilient cyber security posture.

By remaining vigilant, adaptive, and united in their efforts to combat cyber threats, organisers, government agencies, sponsors, and other stakeholders can help ensure a safe and secure environment for athletes, spectators, and participants alike during the 2024 Olympic Games in Paris.

Appendix

Worldwide Partners

Airbnb https://www.airbnb.com.au/e/olympics

Alibaba https://www.alibabagroup.com/en-US/

Allianz https://www.allianz.com/en.html

Atos https://atos.net/en/solutions/cyber-security

Bridgestone https://www.bridgestone.com/olympics/

Coca-Cola / Mengniu https://www.coca-colacompany.com/ / https://mengniu.com.cn/

Deloitte https://www.deloitte.com/global/en/about/story/impact/deloitte-ioc.html

Intel https://www.intel.com/

OMEGA https://www.omegawatches.com/en-us/

Panasonic https://na.panasonic.com/us/

P&G https://us.pg.com/

Samsung https://news.samsung.com/global/

Toyota https://global.toyota/en/

Visa https://usa.visa.com/

Premium Partners

Accor https://all.accor.com/a/en.html

Groupe BPCE https://groupebpce.com/

Carrefour https://www.carrefour.com/en

EDF https://www.edf.fr/en/the-edf-group/edf-at-a-glance

LVMH https://www.lvmh.com/

Orange https://www.orange.com/en

Sanofi https://www.sanofi.com/en

Official Partners

Groupe ADP https://www.parisaeroport.fr/en/homepage-group

Air France https://corporate.airfrance.com/en

ArcelorMittal https://corporate.arcelormittal.com/

Caisse des Dépôts https://www.caissedesdepots.fr/en

Cisco https://www.cisco.com/

CMA CGM https://www.cma-cgm.com/

Danone https://www.danone.com/

Decathlon https://sustainability.decathlon.com/

FDJ https://www.groupefdj.com/en/a-win-win-for-french-sport/

GL events Group https://www.gl-events.com/en

Ile-de-France Mobilités https://www.iledefrance-mobilites.fr/en

Le Coq Sportif https://www.lecoqsportif.com/

PwC https://www.pwc.fr/

Official Supporters

Air Liquide https://www.airliquide.com/

Airweave https://airweave.com/

Arena https://arenagroup.com/

DXC Technology https://dxc.com/us/en

Egis https://www.egis-group.com/

Enedis https://www.enedis.fr/

ES Global https://es.global/

Eviden https://eviden.com/

Fitness Park https://fitnesspark.fr/

Fnac Darty https://www.fnacdarty.com/en/

Garden Gourmet https://www.gardengourmet.com/

Gerflor https://www.gerflor.com/

RATP Group https://ratpgroup.com/en/

Highfield https://www.highfieldfrance.fr/

Hype https://hype.earth/en

La Poste Groupe https://www.lapostegroupe.com/en

Loxam https://loxam.com/en/

Lyreco https://www.lyreco.com/group/

Miko https://www.unilever.fr/brands/ice-cream/miko/

Mondo https://www.mondoworldwide.com/emea/en/

MTD https://www.mtd.net/

Myrtha Pools https://www.myrthapools.com/en/

OnePlan https://www.oneplanevents.com/

Optic 2000 https://www.optic2000.com/

Ottobock https://www.ottobock.com/en-us/home

Randstad https://www.randstad.com/

Rapiscan Systems https://www.rapiscansystems.com/en

Re-uz® https://re-uz.com/

RGS Events https://www.rgsevents.com/

Saint-Gobain https://www.saint-gobain.com/fr

Salesforce https://www.salesforce.com/fr/

SCC https://france.scc.com/

SLX https://www.slx.co.uk/

SNCF https://www.sncf.com/en

Sodexo Live! https://www.sodexo.com/en/services/sodexo-live

Syndicat des Eaux d'Île-de-France https://www.sedif.com/

Technogym https://www.technogym.com/en-US/

Thermo Fisher Scientific https://www.thermofisher.com/us/en/home.html

Tourtel Twist https://www.beertime.fr/tourtel-twist

VINCI https://www.vinci.com/vinci.nsf/en/index.htm

VIPARIS https://www.viparis.com/en

Westfield https://www.westfield.com/en/france