Communications Security
Establishment Canada

Centre de la sécurité des
télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Cyber threat bulletin: Cyber threats to major international sporting events

Canada

About this document

Audience

This cyber threat bulletin is intended for attendees, athletes, government officials and organizations associated with major international sporting events. For guidance on technical mitigation of these threats, consult the [Canadian Centre for Cyber Security's (Cyber Centre) guidance]() or contact the Cyber Centre.

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. You can find more information on the Traffic Light Protocol at the [Forum of incident response and security teams website]().

Contact

For follow up questions or issues, please contact the Canadian Centre for Cyber Security (Cyber Centre) at contact@cyber.gc.ca.

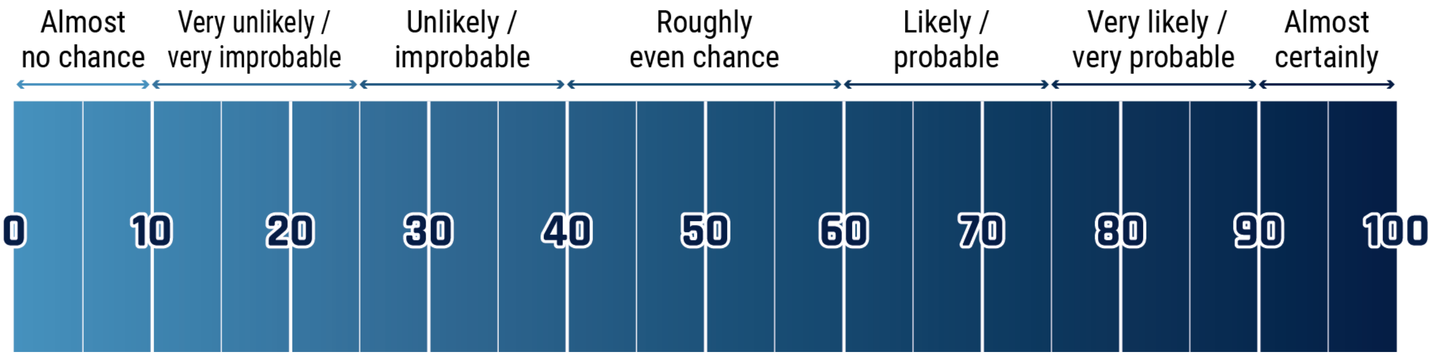
Assessment base and methodology

The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Cyber Centre. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. The Communications Security Establishment's foreign intelligence mandate provides us with valuable insight into adversary behaviour in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The assessments and analysis are based on information available as of December 13th, 2023.

Estimative language guide



Key judgements

- We assess cybercriminals will very likely target large organizations associated with major international sporting events and local businesses around the events through business email compromise (BEC) and ransomware attacks for the purpose of extortion. Cybercriminals will also very likely target individuals associated with major international sporting events, including organizers, attendees and spectators, via phishing emails and malicious websites using these events as lures.
- We assess that hacktivists will likely target major international sporting events with tactics such as website defacements, distributed denial-of-service (DDoS) attacks and hack-and-leak operations. These types of incidents can lead to short- to medium-term service interruptions affecting event organizers, officials and participants.
- We assess state-sponsored cyber threat actors will likely engage in cyber espionage against prominent and high-profile individuals attending major international sporting events to collect foreign intelligence or personal information, and to maintain persistent access when targets return to their home countries.
- We assess that state-sponsored threat actors are unlikely to carry out a major disruptive or destructive attack on major international sporting events in the next year.

Introduction

This assessment examines the cyber threats to Canadians attending major international sporting events in the next year. This includes tourists, government officials and athletes, as well as Canadian organizations involved in organizing, managing, sponsoring and broadcasting events. We assess that the cyber threat to Canadians at major international sporting events in the next year is likely to remain consistent with our assessment but may increase with large or high-profile events such as the Olympics.

Event organizers increasingly rely on information systems and networks to organize, secure and broadcast the events. At the same time, participants and attendees are using new technologies to travel, connect, communicate and consume information online about the events. We assess that major international sporting events are compelling targets for a variety of cyber threat activities, including cybercrime, hacktivism, state-sponsored cyber espionage, and state-sponsored disruptive or destructive cyber attacks. Threat actors are likely to exploit the events' global profile, the large amounts of athlete and attendee information being collected and stored, and the financial value of event-related activities.

Cybercrime

We assess cybercriminals will very likely target large organizations associated with major international sporting events and local businesses around the events through business email compromise (BEC) and ransomware attacks for the purpose of extortion. Cybercriminals will also very likely target individuals associated with major international sporting events, including organizers, attendees and spectators, via phishing emails and malicious websites using these events as lures.

Targeting organizations

We assess that cybercriminals are very likely to target large organizations, such as government organizations and large corporations involved in or sponsoring sporting events, for extortion. Such organizations generate large amounts of personal and financial information through their operations that cybercriminals can attempt to sell through dark web marketplaces or use in follow-on targeted fraud and scams. Smaller businesses may not normally be targeted by cybercriminals to the same extent as larger organizations. However, we assess that their proximity to major international sporting events very likely makes them more desirable as targets for extortion. This is especially true for those in the travel and hospitality sectors. They experience an increase in traffic due to the events, thus increasing the amount of sensitive information they store.

Cybercriminals defraud victims using BEC, a social engineering tactic in which cybercriminals trick victims into transferring funds to a criminal-owned account by impersonating executives or trusted third parties.[2]

Ransomware is a common tool used by cybercriminals to extort their victims. Ransomware blocks access to a computer system by encrypting systems or data while demanding payment from the victim in exchange for the decryption keys. Loss of access to key systems or data can directly interfere with an organization's ability to function. Ransomware attacks also frequently include additional forms of extortion, such as threats to publicly release stolen data.[3] Ransomware can cause significant reputational damage and financial losses for organizations due to loss of productivity and the cost of recovering from an attack. It can also compromise the personal information of employees and customers.

Business email compromise used to target Premier League team

The United Kingdom's National Cyber Security Centre (NCSC) reported an incident where the email account of the managing director of a Premier League football club was compromised via a spear-phishing email. While monitoring the email account, the cybercriminals learned of a forthcoming money transfer of almost one million pounds to another football club and used their access to convince the other club to redirect the transfer to their own account.

Fortunately, the attacker's account had previously been flagged for fraud and the transfer was not completed.[1]

In 2020, an English football club suffered a ransomware attack that encrypted nearly all their devices, rendering their email, security cameras and turnstiles unusable. The club refused the cybercriminal's demand that they pay a 400-bitcoin ransom, approximately $3.8 million USD at the time. According to NCSC, the operational disruption cost the club several hundred thousand pounds.[4]

Targeting individuals

We assess that cybercriminals will very likely target individuals associated with major international sporting events, including organizers, attendees and spectators, via phishing emails and malicious websites using these events as lures. Topical event-related lures may include promises of discounted merchandise, free event tickets or access to a livestream of the events. Cybercriminals also employ search engine optimization (SEO) poisoning to take advantage of people searching for products and information related to major international sporting events. For example, during the 2021 Olympics in Tokyo, there were many instances of event-themed SEO poisoning, usually from webpages posing as television broadcast schedules or streaming pages. These sites prompted users to enter personal information to access event broadcasts. Additionally, they made users complete fake authentication pages (CAPTCHAs) to keep up the illusion of legitimacy. One webpage posing as a television broadcasting schedule also tricked users into allowing browser notifications, then spammed them with malicious advertisements.[5]

Search engine optimization poisoning

SEO poisoning is a tactic used to make malicious sites appear higher in search engine results related to a thematic lure, like a sporting event, to make them appear legitimate. Malicious sites are tagged with keywords or phrases associated with the target theme (such as the Olympics). Bots can artificially increase a site's click through rate to improve the site's search result ranking, among other methods.[6]

SEO poisoning is an attractive technique for cybercriminals because higher placed search results appear more credible, which can increase the number of clicks, and hence victims, it receives.

Hacktivist activity

We assess that hacktivists will likely target major international sporting events with tactics such as website defacements, distributed denial-of -service (DDoS) attacks and hack-and-leak operations. These incidents can lead to short- to medium-term service interruptions affecting event organizers, officials and participants.

Major international sporting events provide an opportunity for hacktivists to widely promote their messaging on domestic issues, environmental causes or international conflict situations. The motivation for hacktivism can vary depending on the event's location, both with respect to the wider geopolitical landscape and domestic issues in that host nation. For example, the anti-government protests in France regarding controversial changes to the minimum pension age[7] is likely a motivation for domestic hacktivism against the 2024 Paris Olympics. Internationally, French support for Ukraine has also motivated pro-Russian hacktivist groups to target the French government, including by defacing the websites of the French National Assembly, Children's Parliament[8] and Senate.[9]

Major international sporting events have been targeted by hacktivists in the past. For example, the 2016 Rio Olympics were targeted by the hacktivist collective "Anonymous". The group capitalized on the increased global attention to the event to protest the Brazilian government. They used DDoS attacks to take down state websites, including that of the Brazilian Ministry of Sports. They also targeted Brazilian sporting organizations with hack-and-leak operations, including the Brazilian Triathlon Confederation and the Brazilian Confederation of Modern Pentathlon.[10] Similar hacktivist activity occurred during the 2014 World Cup where Anonymous carried out DDoS attacks on other state websites, like that of the Brazilian Intelligence Agency and the Ministry of Justice, and on some of the event's sponsors, like The Emirates Group and Hyundai.[11]

State-sponsored cyber espionage

We assess state-sponsored cyber threat actors will likely engage in cyber espionage against prominent and high-profile individuals attending major international sporting events to collect foreign intelligence or personal information, and to maintain persistent access when targets return to their home countries. Canadians considered to be high-profile attendees include:

- government officials
- heads of delegations
- heads of sporting organizations with connections to the government
- representatives of partnered private organizations
- anti-doping program officials
- diplomatic staff

Artificial intelligence (AI) surveillance and the Paris Olympics

In 2023, France became the first country in the European Union to legalize AI surveillance. Initiated for the Paris 2024 Olympics, the legislation covers the use of AI for all large gatherings (over 300 attendees) in the country.[12] According to the French government, the algorithmic video surveillance technology will focus on detecting suspicious movements, behaviours and objects, but will not include facial recognition. The number of devices needed to monitor an event as large as the Olympics would likely increase the cyber threat surface. Furthermore, the audiovisual information collected by these devices is typically stored in cloud-based systems hosted by the vendor. If a vendor's security is vulnerable, sensitive data could be compromised.[13]

In 2021, Verkada, a security-as-a-service company, was compromised. Cyber threat actors gained control over their customers' smart cameras equipped with cloud-based machine vision and AI,[14] thus giving them access to customers' sensitive audiovisual data. Cyber security researchers demonstrated that attackers had the potential to use their access to the Verkada cameras to inject fake footage, preventing camera operators from accurately surveilling an area.

We assess state-sponsored cyber threat actors will likely engage in cyber espionage against high-profile organizations to collect sensitive personal and business information. These high-profile organizations could include government organizations, partnered private organizations and anti-doping organizations.

Sporting organizations have been targeted by state-sponsored cyber threat actors for espionage in the past. During the 2016 Rio Olympics, Russia-backed threat actors targeted the Wi-Fi networks and routers of a hotel chain used by Olympics officials during the event for reconnaissance. They conducted operations both remotely and on-site, travelling to Rio de Janeiro to gain and maintain persistent access to the networks. While at a hotel in Rio, an International Olympic Committee (IOC) official logged into the World Anti-Doping Agency (WADA) database. Their credentials were then stolen by the threat actors and used, along with other credentials, to export large amounts of information from the database.[15]

These Russia-backed cyber threat actors compromised WADA's systems with the intention to diminish public trust in the organization by exfiltrating and leaking sensitive information. They leaked the personal information of 127 athletes, including their test reports, therapeutic use exemptions (TUEs) and past infractions.[16] The compromise disclosed personal information, undermined public trust in WADA and affected Canadian athletes, including four members of Canada's women's soccer team.[17]

The attack on WADA was almost certainly in retaliation for the organization's support and publishing of "The McLaren Report", an independent report that alleged that the Russian Ministry of Sport had engaged in a coordinated doping scheme. WADA recommended that Russia be banned from the Olympics following the release of this report. Attempts to compromise WADA began shortly after.[18]

Russian athletes are still banned from participating in the Olympics under their country's banner, meaning there is still motive to conduct cyber espionage operations.[19] However, it is unlikely that Russian actors will specifically target high-value Canadians linked to major international sporting events for cyber espionage campaigns or hack-and-leak operations.

Event-associated mobile applications

In 2022, the Beijing Winter Olympics required attendees, press and athletes to download the mobile application MY2022. Users were asked to input personal information including passport details, demographic information and COVID-19 testing history.[20] Similar applications were introduced at the 2022 World Cup in Qatar, acting as a COVID-19 contact tracing tool and as virtual tickets to get into the events.[21]

The University of Toronto's Citizen Lab investigated the MY2022 application, finding that its encryption could easily be bypassed, and some sensitive data stored by the application was not encrypted at all. In addition to taking similar sensitive information, the Qatari apps also had multiple features reminiscent of spyware, including remote access to pictures and video on the device, the ability to read and write to the file system, and the ability to make unprompted calls.

Event-associated applications can act as a useful event information hub for attendees. But when attendees are forced to download them and compelled to provide sensitive personal and medical information, they become a vector for state-sponsored actors to collect information on users.

State-sponsored disruptive or destructive cyber attacks

The Cyber Centre is not currently aware of specific intent by state-sponsored cyber threat actors to target major international sporting events in the next year. We assess it is unlikely that a state-sponsored threat actor will carry out a major disruptive or destructive attack on any major international sporting event in the next year. Despite this, it's important to note that major international sporting events and their associated organizations have been targeted by state-sponsored threat actors in the past. Contributing factors include:

- the cultural and political landscape
- foreign policy

- the opportunity to promote an agenda on the global stage
- a desire for retaliation against the host country

The Russian national team was again banned from the 2018 PyeongChang Olympic games for state-sponsored doping, and some athletes participated under the Russian Olympic Committee (ROC) banner instead. In retaliation to that ban, Russian cyber threat actors hacked Olympic infrastructure during the opening ceremony to disrupt the flow of the proceedings.[22] The attack took down the official Olympic Games website as well as Wi-Fi in the stadium. By disrupting event services,[23] the attackers intended to negatively affect the reputations of the IOC and South Korea.

Russian athletes are currently banned from several international sporting federations following Russia's invasion of Ukraine, including the:

- Fédération Internationale de Football Association
- Union of European Football Associations
- International Ice Hockey Federation
- IOC[24]

In October 2023, the IOC officially suspended the ROC after they decided to claim regional sports organizations in occupied areas of Ukraine, which is a violation of the Olympic Charter.[25] While Russian athletes will still be able to participate, they must do so as neutral athletes, not under their country's banner.[26]

Due to current geopolitical tensions, there is a roughly even chance that major international sporting events are targets for Russian state-sponsored cyber disruption.

Outlook

The high profile and costly nature of major international sporting events make them a prime target for cybercriminals looking to exploit targets of opportunity for profit. They also provide a global stage for hacktivists and state-sponsored actors to gather information and publicly embarrass a target. Although events differ in their size, popularity and host nation, the types of threats they face are consistent across events. Thus, we assess that the threat to major international sporting events is likely to remain consistent with our assessments and unlikely to change over the next year.

Many cyber threats can be mitigated through awareness and best practices in cyber security. The Cyber Centre encourages all attendees, athletes, government officials and organizations associated with major international sporting events to take appropriate measures to protect their systems against the cyber threats detailed in this assessment.

Please refer to the following online resources for more information and for useful advice and guidance.

- National Cyber Threat Assessment 2023-2024
- Baseline cyber threat assessment: Cybercrime
- Protecting your information and data when using applications – ITSAP.40.200
- Mobile device guidance for high profile travellers – ITSAP.00.088
- Don't take the bait: Recognize and avoid phishing attacks – ITSAP.00.101

[1] National Cyber Security Centre. "The Cyber Threat to Sports Organisations." July 23, 2020.

[2] Canadian Centre for Cyber Security. "An introduction to the cyber threat environment." October 28, 2022.

[3] Canadian Centre for Cyber Security. "Ransomware playbook (ITSM.00.099)." November 30, 2021.

[4] Shaurya Malwa. "UK football club held to ransom over 400 Bitcoin ($3.8 million)." Decrypt. July 24, 2020.

[5] Trend Micro. "Tokyo Olympics Leveraged in Cybercrime Attack." August 18, 2021.

[6] MITRE ATT&CK. "T1608.006: SEO Poisoning." March 13, 2023.

[7] Angelique Chrisafis. "At least 108 police injured and 291 held in May Day protests in cities across France." The Guardian. May 2, 2023.

[8] Justinas Vainilavičius. "Pro-Kremlin hackers strike French parliament." Cybernews. March 29, 2023.

[9] Digwatch. "French Senate's website taken down by pro-Russian hacktivists." May 5, 2023.

[10] Waqas. "Anonymous DDoS Brazilian Government Websites Because Rio Olympics." Hackread. August 6, 2016.

[11] Nathan B. Thompson, Robert Muggah. "With Anonymous' latest attacks in Rio, the digital games have begun." openDemocracy. August 12, 2016.

[12] Chris O'Brien. "Paris 2024: French Government Approves Controversial AI Video Surveillance." Forbes. March 31, 2023.

[13] Canadian Centre for Cybersecurity. "The Cyber Threat from Supply Chains." February 8, 2023.

[14] Forescout. "'Hack' Highlights The Dangers Of External Access To Data And Devices." March 10, 2021.

[15] Office of Public Affairs. "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations." U.S. Department of Justice. October 4, 2018.

[16] Office of the Privacy Commissioner of Canada. "PIPEDA Report of Findings #2018-006: Breach of the World Anti-Doping database." February 7, 2018.

[17] Thomson Reuters. "Canadian soccer players among latest Olympians to have medical data hacked." CBC. September 19, 2016.

[18] DFRLab. "#PutinAtWar: WADA Hack Shows Kremlin Full-Spectrum Approach." Medium. October 14, 2018.

[19] Eddie Pells. "Nations: No clarity on neutrality, no Olympics for Russia." CBC. February 20, 2023.

[20] Jeffrey Knockel. "Cross Country Exposure; Analysis of the MY2022 Olympics App." The Citizen Lab. January 18, 2022.

[21] Jessica Lyons Hardcastle. "World Cup apps pose a data security and privacy nightmare." The Register. November 11, 2022.

[22] Ellen Nakashima. "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say." The Washington Post. February 24, 2018.

[23] Andy Greenberg. "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History." Wired. October 17, 2019.

[24] Al Jazeera. "Russia-Ukraine war: Which sporting bodies have banned Russia?" March 1, 2022.

[25] International Olympic Committee. "IOC Executive Board suspends Russian Olympic Committee with immediate effect." October 12, 2023.

[26] Claudia Chiappa. "Olympic chiefs ban Russia — but door still open to Paris 2024 for athletes." Politico. October 12, 2023.

CAT. D96-109/2024E-PDF
ISBN 978-0-660-70777-8

Centre de la sécurité des télécommunications
Communications Security Establishment