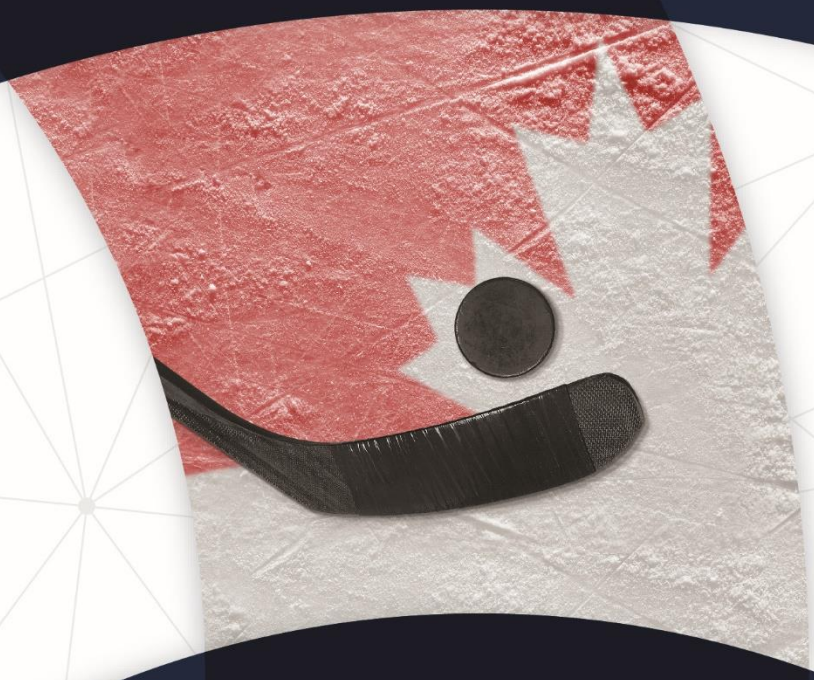
Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada



CENTRE CANADIEN POUR LA
# CYBERSÉCURITÉ

# Bulletin sur les cybermenaces : cybermenaces visant les grands événements sportifs internationaux



Canada

# À propos du présent document

## Auditoire

Le présent bulletin sur les cybermenaces s'adresse aux spectatrices et spectateurs, aux athlètes, aux représentantes et représentants de gouvernements et aux organisations associées aux grands événements sportifs internationaux. Pour obtenir des conseils sur des mesures techniques pour atténuer ces menaces, consultez les conseils du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) ou communiquez avec le Centre pour la cybersécurité.

La mention TLP:CLEAR doit être utilisée conformément aux règles et aux procédures applicables à la diffusion publique lorsque le risque prévisible d'une utilisation abusive est faible ou négligeable. Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:CLEAR peut être distribuée sans aucune restriction. Pour obtenir de plus amples renseignements sur le protocole TLP (Traffic Light Protocol), prière de consulter le site Web du Forum of Incident Response and Security Teams (en anglais seulement).

## Coordonnées

Prière de transmettre toute question ou tout enjeu relatif au présent document au Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à contact@cyber.gc.ca.

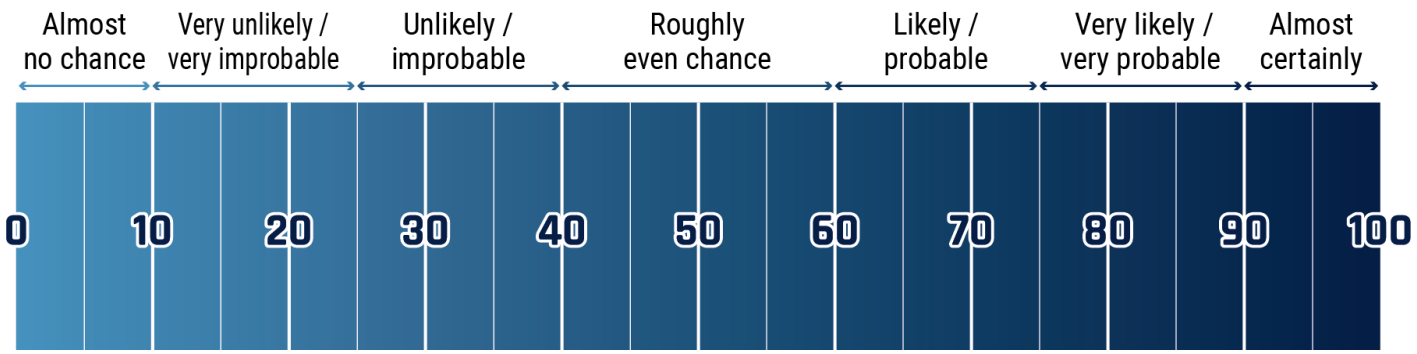
## Méthodologie et fondement de l'évaluation

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise en matière de cybersécurité du Centre pour la cybersécurité. Le rôle que joue le Centre pour la cybersécurité dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, ce qui a contribué à la présente évaluation. Dans le cadre du volet du mandat du Centre de la sécurité des télécommunications touchant le renseignement étranger, le Centre pour la cybersécurité tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. Le Centre pour la cybersécurité utilise des formulations telles que « nous évaluons que » ou « nous jugeons que » pour présenter une évaluation analytique. Les qualificatifs tels que « possiblement », « probable » et « très probable » servent à évoquer une probabilité.

Les évaluations et analyses énoncées dans le présent document sont fondées sur des renseignements disponibles en date du 13 décembre 2023.

## Lexique des estimations



## Principaux avis

- Selon notre évaluation, les cybercriminelles et cybercriminels cibleront très probablement les grandes organisations associées aux événements sportifs internationaux et les entreprises locales qui ont un lien avec ces événements au moyen de compromissions de courriel d'affaires et d'attaques par rançongiciel à des fins d'extorsion. Ils cibleront également très probablement les personnes ayant un lien avec les grands événements sportifs internationaux, y compris les personnes qui organisent l'événement, qui y participent et qui y assistent, par l'entremise de courriels d'hameçonnage et de sites Web malveillants qui utilisent l'événement comme appât.
- Nous estimons que les hacktivistes cibleront très probablement les grands événements sportifs internationaux au moyen de diverses tactiques, comme la défiguration de site Web, les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) et les opérations de piratage et de divulgation. Ce type d'incidents peut entraîner des interruptions de service à court et à moyen terme qui touchent les organisatrices et organisateurs, les représentantes et représentants d'organismes, ainsi que les participantes et participants.
- Nous croyons que les auteures et auteurs de cybermenace parrainés par des États effectueront probablement des activités de cyberespionnage contre des personnes importantes et connues qui assistent à de grands événements sportifs internationaux, et ce, dans le but de recueillir du renseignement étranger ou des renseignements personnels ainsi que de maintenir un accès permanent à leurs cibles lorsqu'elles retournent dans leur pays d'origine.
- Nous estimons qu'il est peu probable que les auteures et auteurs de menace parrainés par des États mènent d'importantes attaques perturbatrices et destructives contre les grands événements sportifs internationaux au cours de la prochaine année.

## Introduction

La présente évaluation examine les cybermenaces visant les Canadiennes et Canadiens qui participent à de grands événements sportifs internationaux cette année. Il s'agit notamment des touristes, des représentantes et représentants du gouvernement, des athlètes ainsi que des organisations canadiennes qui organisent, gèrent, commanditent ou diffusent ces événements. Nous sommes d'avis que les cybermenaces visant les Canadiennes et Canadiens dans le cadre de grands événements sportifs internationaux au cours de la prochaine année resteront comparables à notre évaluation, mais qu'elles pourraient augmenter dans le contexte de grands événements très médiatisés, comme les Jeux olympiques.

De plus en plus, les organisatrices et organisateurs se fient de plus en plus aux réseaux et aux systèmes d'information pour organiser et diffuser ces événements ainsi qu'en assurer la sécurité. En parallèle, les personnes qui participent ou assistent à des événements utilisent les nouvelles technologies pour voyager, pour connecter avec les autres, pour communiquer et pour obtenir de l'information en ligne à propos d'un événement. Nous considérons que les grands événements sportifs internationaux sont des cibles irrésistibles pour un grand nombre d'activités de cybermenace, notamment le cybercrime, l'hacktivisme, le cyberespionage parrainé par un État, les cyberattaques perturbatrices ou destructives parrainées par un État. Les auteures et auteurs de menace exploiteront probablement le profil mondial des événements, la grande quantité d'informations recueillies et stockées sur les athlètes et les spectatrices et spectateurs, ainsi que la valeur financière des activités liées aux événements.

## Cybercrime

Selon notre évaluation, les cybercriminelles et cybercriminels cibleront très probablement les grandes organisations associées aux événements sportifs internationaux et les entreprises locales qui ont un lien avec ces événements au moyen de compromissions de courriel d'affaires et d'attaques par rançongiciel à des fins d'extorsion. Ils cibleront également très

probablement les personnes ayant un lien avec les grands événements sportifs internationaux, y compris les personnes qui organisent l'événement, qui y participent et qui y assistent, par l'entremise de courriels d'hameçonnage et de sites Web malveillants qui utilisent l'événement comme appât.

## Cibler les organisations

Nous évaluons que les cybercriminelles et cybercriminels viseront très probablement les grandes organisations, comme les organisations gouvernementales et les grandes entreprises qui contribuent aux événements sportifs ou qui commanditent ces événements, et ce, dans le but de les extorquer. Ces organisations génèrent une immense quantité d'informations personnelles ou financières par l'entremise de leurs activités, soit des informations que les cybercriminelles et cybercriminels peuvent tenter de vendre sur les places de marché du Web clandestin ou utiliser dans le cadre de fraudes ou d'arnaques de suivi ciblées. Les petites entreprises ne sont pas normalement la cible de cybercriminelles et cybercriminelles au même degré que les grandes organisations. Cependant, en raison de leur proximité aux grands événements sportifs internationaux, nous estimons qu'elles seront très probablement des cibles attrayantes pour l'extorsion. C'est tout particulièrement le cas pour les secteurs du tourisme et de l'hôtellerie. Ces secteurs connaissent une augmentation du trafic en raison des événements, donc une augmentation de la quantité d'information sensible qu'ils stockent.

**Compromission de courriel d'affaires visant une équipe de Premier League**

Le National Cyber Security Centre (NCSC) du Royaume-Uni a signalé un incident dans lequel le compte de courriel du directeur général d'un club de la Premier League a été compromis au moyen d'un courriel de harponnage. Tandis qu'ils surveillaient le compte de courriel, les cybercrimelles et cybercriminels ont pris connaissance d'un prochain transfert d'argent d'une valeur approchant le million de livres sterling à une autre des équipes. Ils ont profité de leur accès pour convaincre l'autre équipe d'envoyer le transfert à leur propre compte.

Heureusement, le compte en question avait déjà été signalé pour de la fraude et il a été possible d'interrompre le transfert.[1]

Les cybercriminelles et cybercriminels fraudent les victimes par l'entremise de la compromission de courriel d'affaires, soit une tactique de piratage psychologique dans laquelle ils incitent les victimes à transférer des fonds vers un compte détenu par une ou un criminel en usurpant des cadres ou des parties tierces de confiance.[2]

Le rançongiciel est l'un des outils couramment utilisé aux fins d'extorsion par les cybercriminelles et cybercriminels. Un rançongiciel empêche l'accès à un système informatique en chiffrant les systèmes ou les données, dont la clé de déchiffrement n'est donnée aux victimes qu'en échange d'un paiement. La perte de l'accès aux principaux systèmes et données interfère directement avec la capacité d'une organisation de fonctionner normalement. Les attaques par rançongiciel présentent également fréquemment d'autres formes d'extorsion, comme la menace de rendre publiques les données volées.[3] Les rançongiciels peuvent nuire grandement à la réputation et entraîner des pertes financières pour les organisations qui en sont victimes, à cause notamment de la diminution de la productivité et du coût de reprise des activités. Ces attaques peuvent également compromettre l'information personnelle des employées et employés ainsi que des clientes et clients.

En 2020, un club de soccer anglais a été victime d'une attaque par rançongiciel qui a chiffré presque tous ses dispositifs, mettant hors d'état les courriels, les caméras de sécurité et les tourniquets à portillons automatisés. Le club a refusé de se soumettre à la demande des cybercriminelles et cybercriminels de leur payer une rançon de 400 Bitcoins, qui équivalait à environ 3,8 millions de dollars américains à cette période. Selon le NCSC, l'interruption des activités a coûté au club plusieurs centaines de milliers de livres sterling.[4]

## Cibler les personnes

Nous croyons que les cybercriminelles et cybercriminels viseront très probablement les personnes ayant un lien avec les grands événements sportifs internationaux, y compris les personnes qui organisent l'événement, qui y participent et qui y assistent, par l'entremise de courriels d'hameçonnage et de sites Web malveillants qui utilisent l'événement comme appât.

Les appâts thématiques en lien avec des événements peuvent notamment promettre de la marchandise au rabais, des billets gratuits ou l'accès à la diffusion en direct de l'événement.

Les cybercriminelles et cybercriminels utilisent également l'empoisonnement de l'optimisation pour les moteurs de recherche pour tirer avantage des recherches que font les personnes pour trouver des produits et de l'information connexes à de grands événements sportifs internationaux. Par exemple, durant les Jeux olympiques de Tokyo en 2021, il y a eu un grand nombre de cas d'empoisonnement de la sorte, généralement par des pages Web qui se faisaient passer pour un site de programmation télévisée ou de diffusion en continu. Ces sites demandaient aux internautes de fournir des renseignements personnels afin d'accéder à la diffusion des événements. De plus, ils demandaient aux internautes de remplir de fausses pages d'authentification (CAPTCHA) afin de préserver l'illusion de légitimité. Une page Web se faisant passer pour un site de programmation télévisée a même incité les internautes à autoriser les notifications sur le navigateur pour ensuite les inonder de publicités malveillantes.[5]

**Empoisonnement de l'optimisation pour les moteurs de recherche**

L'empoisonnement de l'optimisation pour les moteurs de recherche est une tactique qui permet de faire apparaître les sites malveillants plus hauts dans les résultats de moteurs de recherche en lien avec un thème qui sert d'appât, comme un événement un sportif. Ces sites semblent par conséquent légitimes. Des mots-clés ou des phrases en lien avec le thème voulu (comme les Olympiques) sont apposés aux sites malveillants. Entre autres, des robots peuvent faire augmenter artificiellement le taux de clic sur un site, afin d'améliorer le classement du site dans les résultats.[6]

L'empoisonnement de l'optimisation pour les moteurs de recherche est une technique intéressante pour les cybercriminelles et cybercriminels, car les résultats de recherche qui se classent parmi les plus élevés semblent plus crédibles que d'autres, entraînant un plus grand nombre de clics, donc de victimes.

## Hacktivisme

Nous estimons que les hacktivistes cibleront très probablement les grands événements sportifs internationaux au moyen de diverses tactiques, comme la défiguration de site Web, les attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) et les opérations de piratage et de divulgation. Ces incidents peuvent entraîner des interruptions de service à court et à moyen terme qui touchent les organisatrices et organisateurs, les représentantes et représentants d'organismes ainsi que les participantes et participants.

Les grands événements sportifs internationaux représentent une plateforme pour les hacktivistes qui souhaitent promouvoir largement leurs messages sur les enjeux nationaux, les causes environnementales ou les conflits internationaux. Leur motivation varie en fonction du lieu de l'événement lié notamment au paysage géopolitique plus large et des enjeux nationaux de la nation hôte. Par exemple, les manifestations contre le gouvernement en France concernant les changements controversés à l'âge minimal de la retraite[7] représenteront probablement une source de motivation d'hacktivisme national contre les Jeux olympiques de Paris 2024. À l'échelle internationale, le soutien de la France à l'Ukraine a également motivé des groupes hacktivistes prorusses à cibler le gouvernement français, notamment en défigurant les sites Web de l'Assemblée nationale, du Parlement des enfants[8] et du Sénat[9] français.

Les grands événements sportifs internationaux ont déjà été la cible d'hacktivistes par le passé. Par exemple, les Jeux olympiques de Rio en 2016 ont été ciblés par le collectif d'hacktivistes « Anonymous ». Le groupe a tiré parti de l'attention mondiale accrue sur l'événement pour manifester contre le gouvernement brésilien. Au moyen d'attaques par DDoS, il a fermé des sites Web du gouvernement, notamment celui du ministère des Sports du Brésil. Il a également ciblé des organisations sportives au moyen d'opérations de piratage et de divulgation, notamment contre la Confédération brésilienne de triathlon et la Confédération brésilienne de pentathlon moderne[10]. Des activités semblables ont eu lieu lors de la Coupe du monde de 2014, où le groupe Anonymous a mené des attaques par DDoS contre les sites Web d'autres États, comme ceux de l'Agence

brésilienne du renseignement, du ministère de la Justice et de commanditaires de l'événement, comme le consortium Emirates Group et Hyundai.[11]

## Cyberespionnage parrainé par des États

Nous croyons que les auteures et auteurs de cybermenace parrainés par des États effectueront probablement des activités de cyberespionnage contre des personnes importantes et connues qui assistent à de grands événements sportifs internationaux, et ce, dans le but de recueillir du renseignement étranger ou des renseignements personnels ainsi que de maintenir un accès permanent à leurs cibles lorsqu'elles retournent dans leur pays d'origine. Parmi les personnes présentes venant du Canada, on considère les suivantes comme des personnes importantes :

- représentantes et représentants de gouvernement;
- chefs de délégation;
- dirigeantes et dirigeants d'organisations sportives qui ont des liens avec le gouvernement;
- représentantes et représentants d'organisations partenaires du secteur privé;
- représentantes et représentants de programmes antidopage;
- membres du personnel diplomatique.

Nous estimons que les auteures et auteurs de cybermenace étatiques mèneront des activités de cyberespionnage contre les organisations à haute visibilité, dans le but de recueillir des renseignements personnels et commerciaux sensibles. Ces organisations à haute visibilité peuvent être des organismes gouvernementaux, des organisations partenaires du secteur privé et des organisations antidopage.

Les organisations sportives ont déjà été la cible d'auteures et auteurs de cybermenace à des fins d'espionnage par le passé. Pendant les Jeux olympiques de Rio en 2016, des auteures et auteurs de menace parrainés par la Russie ont ciblé, à des fins de reconnaissance, des réseaux Wi-Fi et des routeurs d'une chaîne hôtelière utilisée par les représentantes et représentantes des Jeux durant l'événement. Ils ont exécuté des opérations à distance et sur place, c'est-à-dire en voyageant à Rio de Janeiro afin d'obtenir et de maintenir un accès permanent aux réseaux. Tandis qu'elle se trouvait à un hôtel de Rio, une personne représentant le Comité international olympique (CIO) s'est connectée à la basse de données de l'Agence mondiale antidopage. Des auteures et auteurs de menace ont volé ses justificatifs d'identité et s'en sont servi, ainsi que d'autres justificatifs, pour exporter de grandes quantités d'informations de la base de données.[14]

**Applications mobiles liées aux événements**

En 2022, les Jeux olympiques d'hiver de Beijing demandaient aux spectatrices, spectateurs, représentantes et représentants des médias ainsi qu'aux athlètes de télécharger l'application mobile MY2022. Les utilisatrices et utilisateurs devaient fournir leurs renseignements personnels, y compris les renseignements sur le passeport, de l'information démographique et les antécédents de test pour la COVID-19.[12] Des applications semblables, servant d'outils de recherche de contacts pour la COVID-19 et de billets virtuels pour accéder aux événements, ont également été utilisées dans le cadre de la Coupe du monde de 2022 au Qatar.[13]

The Citizen Lab de l'Université de Toronto a étudié l'application MY2022 et a conclu que son chiffrement pouvait facilement être contourné et que certaines données sensibles stockées dans l'application n'étaient pas chiffrées du tout. En plus de recueillir le même genre d'information sensible, les applications qatariennes avaient plusieurs fonctionnalités qui rappellent un logiciel espion, notamment l'accès à distance aux photos et vidéos sur un appareil, la capacité de lire le système de fichiers et d'écrire sur le système de fichiers ainsi que la capacité de faire des appels non sollicités.

Les applications liées à des événements peuvent servir de carrefour pratique où trouver de l'information pour les spectatrices et spectateurs. Toutefois, si ces personnes sont forcées de les télécharger et contraintes de fournir des renseignements personnels et médicaux sensibles, les applications deviennent des vecteurs d'où soutirer de l'information sur les utilisatrices et utilisateurs par les auteures et auteurs de menace étatiques.

Ces auteures et auteurs de cybermenace parrainés par la Russie ont compromis les systèmes de l'Agence mondiale antidopage afin d'effriter la confiance du public dans l'organisation en exfiltrant et en diffusant de l'information sensible. Ils ont diffusé les renseignements personnels de 127 athlètes, notamment des rapports de test, l'information d'autorisations d'usage à des fins thérapeutiques (AUT) et des cas d'infractions passées.[15] La compromission a entraîné la divulgation de renseignements personnels, a effrité la confiance du public dans l'Agence mondiale antidopage et a touché des athlètes canadiennes et canadiens, notamment quatre membres de l'équipe féminine de soccer du Canada.[16]

L'attaque contre l'Agence mondiale antidopage représentait presque certainement des représailles contre le soutien et la publication par l'organisation du rapport McLaren, un rapport indépendant alléguant que le ministère du Sport de la Russie a participé à un complot coordonné de dopage. L'Agence mondiale antidopage recommandait que la Russie soit bannie des Jeux olympiques à la suite de ce rapport. Peu de temps après la publication, les tentatives de compromettre l'Agence mondiale antidopage ont commencé.[17]

À ce jour, les athlètes russes n'ont toujours pas l'autorisation de participer aux Jeux olympiques sous le drapeau de leur pays, donc le motif pour exécuter des opérations de cyberespionnage perdure.[18] Toutefois, il est peu probable que des auteures et auteurs de menace russes mènent des campagnes d'espionnage ou des opérations de piratage et de divulgation, dans le seul but de cibler précisément des Canadiennes et Canadiens de grande valeur ayant des liens avec les grands événements sportifs internationaux.

**Surveillance appuyée sur l'intelligence artificielle (IA) aux Jeux olympiques de Paris**

En 2023, la France est devenue le premier pays de l'Union européenne à légaliser la surveillance appuyée sur l'IA. Adoptée en prévision des Jeux olympiques de Paris en 2024, la loi porte sur l'utilisation de la l'IA dans le cadre de grands rassemblements (plus de 300 personnes) au pays[19] Selon le gouvernement français, la technologie de vidéosurveillance algorithmique sera axée sur la détection de déplacements, de comportements et d'objets suspects, mais n'incorpore pas de composante relative à la reconnaissance faciale. Le nombre d'appareils nécessaires pour assurer la surveillance d'une aussi grande envergure que les Jeux olympiques accroîtrait probablement l'exposition aux cybermenaces. Par ailleurs, l'information audiovisuelle recueillie par ces appareils est généralement stockée dans des systèmes infonuagiques hébergés par le fournisseur. Si le niveau de sécurité d'un fournisseur laisse à désirer, des données sensibles pourraient faire l'objet d'une compromission.[20]

En 2021, Verkada, une entreprise offrant des services de sécurité, a été touchée par une compromission. Des auteures et auteurs de cybermenace ont pris le contrôle des caméras intelligentes de la clientèle de l'entreprise, équipées de capacités infonuagiques d'IA et de vision par ordinateur,[21] ce qui leur a donné accès aux données audiovisuelles sensibles de la clientèle. Les chercheuses et chercheurs en cybersécurité ont montré que les personnes à l'origine d'une attaque pouvaient potentiellement se servir de leur accès aux caméras de Verkada pour injecter de fausses séquences vidéo qui empêchent les opératrices ou opérateurs de caméra de surveiller correctement une zone.

## Cyberattaques perturbatrices ou destructives parrainées par un État

Le Centre pour la cybersécurité n'a pas actuellement connaissance d'intentions précises d'auteures et auteurs de cybermenace parrainés par des États de viser de grands événements sportifs internationaux au cours de la prochaine année. Nous estimons qu'il est peu probable que les auteures et auteurs de menace parrainés par des États mènent d'importantes attaques perturbatrices et destructives contre un grand événement sportif international au cours de la prochaine année. Malgré tout, il est essentiel de noter que les grands événements sportifs internationaux et les organisations connexes ont déjà été la cible d'auteures et auteurs de menace parrainés par des États par le passé. Parmi les facteurs contributifs, il y a :

- le paysage politique et culturel;
- les politiques étrangères;
- l'occasion de promouvoir des intérêts à l'échelle mondiale;
- le désir de représailles contre le pays hôte.

L'équipe nationale russe a été de nouveau bannie des Jeux olympiques de PyeongChang en 2018 en raison de dopage parrainé par l'État, et certaines et certains athlètes ont plutôt participé sous la bannière du Comité olympique russe. En représailles de cette interdiction, des auteures et auteurs de cybermenace russes ont piraté l'infrastructure olympique durant la cérémonie d'ouverture afin de perturber le déroulement des événements.[22] L'attaque a mis hors service le site Web officiel des Jeux olympiques, ainsi que le réseau Wi-Fi du stade. L'interruption des services de l'événement[23] avait pour but d'influencer négativement la réputation du CIO et de la Corée du Sud.

Les athlètes russes sont actuellement bannies et bannis de plusieurs fédérations sportives internationales à la suite de l'invasion de l'Ukraine par la Russie, y compris :

- la Fédération Internationale de Football Association;
- l'Union européenne des associations de football;
- la Fédération internationale de hockey;
- le CIO.[24]

En octobre 2023, le CIO a officiellement suspendu le Comité olympique russe après qu'il a décidé de revendiquer des organisations sportives régionales dans les régions occupées de l'Ukraine, une infraction envers la Charte olympique.[25] Les athlètes russes auront toujours la possibilité de participer, mais elles et ils devront le faire sous une bannière neutre, et non sous la bannière de leur pays.[26]

En raison des tensions géopolitiques actuelles, il y a une probabilité presque égale que les grands événements sportifs internationaux soient la cible de cyberactivités perturbatrices parrainées par la Russie.

## Perspective

La grande visibilité et la nature coûteuse des grands événements sportifs internationaux en font des cibles de choix pour les cybercriminelles et cybercriminelles qui souhaitent exploiter des cibles inopinées à des fins lucratives. Elles représentent également une plateforme mondiale pour les hacktivistes et les auteures et auteurs de menace qui souhaitent recueillir de l'information et embarrasser publiquement une cible. Bien que les événements de différentes nations hôtes soient d'envergure et de popularité diverses, les types de menaces qui guettent ces événements demeurent les mêmes. Par conséquent, nous jugeons que les menaces visant les grands événements sportifs internationaux resteront comparables à notre évaluation et qu'elles ne changeront probablement pas au cours de la prochaine année.

Bon nombre des cybermenaces peuvent être atténuées grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de cybersécurité. Le Centre pour la cybersécurité recommande aux spectatrices et spectateurs, aux athlètes, aux représentantes et représentants de gouvernements et aux organisations associées aux grands événements sportifs internationaux de prendre les mesures nécessaires pour protéger leurs systèmes contre les cybermenaces décrites dans la présente évaluation.

Consultez les ressources en ligne suivantes pour obtenir de l'information supplémentaire ainsi que des avis et conseils utiles :

- Évaluation des cybermenaces nationales 2023-2024
- Évaluation des cybermenaces de base liées à la cybercriminalité
- Apprenez à protéger votre information et vos données lorsque vous utilisez des applications (ITSAP.40.200)
- Conseils sur les appareils mobiles à l'intention des voyageurs connus du public (ITSAP.00.088)
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)

[1] National Cyber Security Centre. « The Cyber Threat to Sports Organisations » (en anglais seulement). 23 juillet 2020.

[2] Centre canadien pour la cybersécurité. « Introduction à l'environnement de cybermenaces ». 28 octobre 2022.

[3] Centre canadien pour la cybersécurité. « Guide sur les rançongiciels (ITSM.00.099) ». 30 novembre 2021.

[4] Shaurya Malwa. « UK football club held to ransom over 400 Bitcoin ($3.8 million) » (en anglais seulement). *Decrypt*. 24 juillet 2020.

[5]Trend Micro. « Tokyo Olympics Leveraged in Cybercrime Attack » (en anglais seulement). 18 août 2021.

[6] MITRE ATT&CK. « T1608.006: SEO Poisoning » (en anglais seulement). 13 mars 2023.

[7] Angelique Chrisafis. « At least 108 police injured and 291 held in May Day protests in cities across France » (en anglais seulement). The Guardian, 2 mai 2023.

[8] Justinas Vainilavičius. « Pro-Kremlin hackers strike French parliament » (en anglais seulement). Cybernews, 29 mars 2023.

[9] Digwatch. « French Senate's website taken down by pro-Russian hacktivists » (en anglais seulement). 5 mai 2023.

[10] Waqas. « Anonymous DDoS Brazilian Government Websites Because Rio Olympics » (en anglais seulement). Hackread. 6 août 2016.

[11] Nathan B. Thompson et Robert Muggah. « With Anonymous' latest attacks in Rio, the digital games have begun » (en anglais seulement). OpenDemocracy. 12 août 2016.

[12] Jeffrey Knockel. « Cross Country Exposure; Analysis of the MY2022 Olympics App » (en anglais seulement). The Citizen Lab. 18 janvier 2022.

[13] Jessica Lyons Hardcastle. « World Cup apps pose a data security and privacy nightmare » (en anglais seulement). The Register. 11 novembre 2022.

[14] Office of Public Affairs. « U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations » (en anglais seulement). Département de la Justice des États-Unis. 4 octobre 2018.

[15] Commissariat à la protection de la vie privée du Canada. « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2018-006 : Intrusion dans la base de données de l'Agence mondiale antidopage ». 7 février 2018.

[16] Thomson Reuters. « Canadian soccer players among latest Olympians to have medical data hacked » (en anglais seulement). CBC. 19 septembre 2016.

[17] DFRLab. « #PutinAtWar: WADA Hack Shows Kremlin Full-Spectrum Approach » (en anglais seulement). Medium. 14 octobre 2018.

[18] Eddie Pells. « Nations: No clarity on neutrality, no Olympics for Russia » (en anglais seulement). CBC. 20 février 2023.

[19] Chris O'Brien. « Paris 2024: French Government Approves Controversial AI Video Surveillance » (en anglais seulement). Forbes, 31 mars 2023.

[20] Centre canadien pour la cybersécurité. « La cybermenace provenant des chaînes d'approvisionnement ». 8 février 2023.

[21] Forescout. « 'Hack' Highlights The Dangers Of External Access To Data And Devices » (en anglais seulement). 10 mars 2021.

[22] Ellen Nakashima. « Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say » (en anglais seulement). The Washington Post. 24 février 2018.

[23] Andy Greenberg. « The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History » (en anglais seulement). Wired. 17 octobre 2019.

[24] Al Jazeera. « Russia-Ukraine war: Which sporting bodies have banned Russia? » (en anglais seulement). 1er mars 2022.

[25] Comité international olympique. « Suspension avec effet immédiat du Comité olympique russe par la commission exécutive du CIO ». 12 octobre 2023.

[26] Claudia Chiappa. « Olympic chiefs ban Russia — but door still open to Paris 2024 for athletes » (en anglais seulement). Politico. 12 octobre 2023.

CAT. D96-109/2024F-PDF
ISBN 978-0-660-70778-5