TLP:CLEAR
PAP:CLEAR

GRANDS ÉVÈNEMENTS SPORTIFS EN FRANCE

ÉVALUATION DE LA MENACE 2023

30 août 2023

Sommaire

Synthèse

Depuis plus d'une décennie, les compétitions sportives internationales majeures font régulièrement l'objet d'attaques informatiques. Ces évènements, en raison de l'intérêt qu'ils suscitent chez des centaines de millions de personnes et des flux financiers importants qu'ils génèrent, constituent une opportunité d'agir pour des attaquants informatiques aux motivations diverses. En effet, ces derniers peuvent chercher à perpétrer des actes malveillants à des fins lucratives, de déstabilisation ou encore d'espionnage. **La Coupe du monde de rugby 2023 (CdM 2023) et les Jeux olympiques et paralympiques 2024 (JOP 2024), organisés en France, pourraient être les cibles d'attaques informatiques de ce type.**

Le **contexte géopolitique**, avec l'invasion de l'Ukraine par la Russie, débutée en février 2022, peut constituer un contexte de tensions favorables à la conduite d'attaques informatiques. Des groupes d'attaquants affiliés à l'un des deux États ou des hacktivistes pourraient chercher à **tirer profit de la couverture médiatique de la CdM 2023 et des JOP 2024 pour promouvoir leur cause et mener des attaques informatiques**. Ces menaces sont à recontextualiser dans le contexte politique national et international dans lequel la CdM 2023 et les JOP 2024 se tiendront.

Si l'ANSSI ne dispose à l'heure actuelle d'aucune information spécifique sur des attaques ciblant la CdM 2023 ou les JOP 2024, **la surface d'exposition de ces deux évènements à des attaques informatiques demeure très importante**. L'organisation et le déroulement d'évènements sportifs d'ampleur nécessitent en effet la mise en œuvre de nombreux systèmes d'information, que ceux-ci appartiennent au pays hôte, aux organisateurs ou à leurs prestataires, sous-traitants, sponsors ou toute autre entité participant d'une façon ou d'une autre à ces évènements. Ces attaques sont susceptibles de perturber de manière substantielle les compétitions sportives d'ampleur.

C'est le cas par exemple de la compromission des systèmes d'information utilisés pour la gestion des infrastructures sportives, des transports, de la distribution d'énergie, ou des contrôles d'accès et de l'impression des billets. Outre la menace potentielle des attaques informatiques pour la sécurité des biens et personnes, celles-ci sont également susceptibles de **ternir l'image du pays organisateur et d'avoir des conséquences négatives sur les retombées économiques pour les organisateurs**(pertes de recettes en termes de billetterie, coût du remplacement de matériel…), les sponsors ainsi que les spectateurs (vol de données ou de fonds). Enfin, la qualité de l'expérience vécue par les spectateurs, téléspectateurs et internautes peut être affectée par la compromission de certains systèmes d'information (impossibilité d'accéder aux stades, fraudes, connexion en Wi-Fi impossible, retransmission télévisée perturbée). **Cette incidence peut aller jusqu'au report ou l'annulation d'épreuves sportives, par exemple en cas de panne d'éclairage ou des systèmes de chronométrage**.

La principale menace identifiée lors de la CdM 2023 et des JOP 2024 est celle à **finalité lucrative**, aussi bien à l'encontre des organisateurs que des athlètes et des spectateurs. Ces derniers peuvent être exposés à des escroqueries, des tentatives d'extorsions ou encore des vols et reventes de données. Les entités organisatrices des évènements sportifs ainsi que leurs prestataires peuvent notamment être ciblés par des attaques par rançongiciel. La durée restreinte des évènements sportifs accroît considérablement la criticité de la continuité des services et donc de la disponibilité des systèmes d'information.

L'existence de **campagnes de déstabilisation**, au moyen de sabotage informatique, d'attaques par déni de service distribué (*DDoS*) [1], de défiguration ou encore de divulgations orchestrées de données (*hack-and-leak*), est également possible. L'édition 2018 des JOP d'hiver de Pyeongchang, en Corée du Sud, a en effet fait l'objet d'une attaque informatique à visée destructrice par le code malveillant Olympic Destroyer, perturbant la cérémonie d'ouverture de l'évènement.

Enfin, il ne peut être exclu que soient menées à l'encontre des nombreuses délégations officielles et des individus intéressés par, ou devant assister à, ces évènements sportifs, des **opérations d'espionnage**.

1. Une attaque informatique ayant pour effet d'empêcher ou de limiter fortement l'accessibilité des sites Internet et des ressources en ligne des entités ciblées, sans porter atteinte à leur contenu.

Introduction

Désignée pays hôte de la Coupe du monde de rugby 2023 (CdM 2023) et des Jeux olympiques et paralympiques 2024 (JOP 2024), la France se prépare à accueillir deux évènements sportifs planétaires. Les JOP 2024 représentent le plus grand évènement, prévoyant de rassembler quatre milliards de téléspectateurs, 13 millions de spectateurs, 30 000 bénévoles et 15 000 athlètes sur 38 sites de compétition [1]. Défi organisationnel et logistique, ces évènements sont également des défis sur le plan de la sécurité informatique. Ces compétitions pourraient en effet faire l'objet, comme des éditions précédentes de ce type de manifestations, d'attaques informatiques [2, 3].

Le périmètre des systèmes d'information pouvant être ciblés par des attaquants apparaît particulièrement large, rendant complexe l'effort de sécurisation de ces évènements face aux attaques informatiques. Toute opération ciblant un ou plusieurs de ces maillons est susceptible de perturber la tenue de ces évènements, *a fortiori* dès lors que certains de ces systèmes d'information peuvent faire l'objet d'interconnexions entre eux permettant aux attaquants de se latéraliser plus facilement. Alors que la CdM 2023 et les JOP 2024 se tiendront bientôt, et sous réserve des évolutions politiques, géopolitiques, sanitaires et techniques à venir, plusieurs menaces contre les systèmes d'information du périmètre peuvent d'ores et déjà être identifiées.

En raison de la haute visibilité et de l'intérêt que des évènements sportifs comme les JOP suscitent chez des centaines de millions de personnes et des flux financiers importants qu'ils génèrent, ces compétitions constituent une cible de choix pour des attaquants informatiques aux motivations diverses. Ceux-ci peuvent chercher à perturber l'activité des entités ciblées, s'enrichir au travers d'activités cybercriminelles ou nuire à la réputation du pays hôte sur la scène internationale.

Les rumeurs d'atteinte à l'intégrité et à la confidentialité des données peuvent avoir des conséquences significatives sur la réputation d'une entité. Par ailleurs, les menaces qui pèsent sur les évènements sportifs ne se limitent pas aux dates de leur tenue, elles peuvent également s'observer en amont et en aval.

Les menaces identifiées ne sont pas spécifiques aux grands évènements sportifs toutefois les conséquences des attaques peuvent avoir une portée plus importante. En effet, la durée restreinte des évènements sportifs accroît considérablement la criticité de la continuité des services et donc de la disponibilité des systèmes d'information.

1. Un contexte qui augmente les opportunités d'attaques

1.1. Une surface d'exposition étendue

La surface d'exposition de ce type d'évènement est très importante. Les acteurs impliqués, allant de la petite et moyenne entreprise à l'État, disposent de niveaux de maturité cyber hétérogènes. De plus, ceux-ci sont potentiellement interconnectés, ce qui soulève des risques de propagation d'attaques informatiques.

L'organisation et le déroulement d'évènements sportifs majeurs reposent sur un nombre important de systèmes d'information (sites Internet, gestion des fournisseurs, billetterie, flux vidéo…) exploités par différents acteurs (Comité international olympique, fédérations nationales, associations…). Les autorités locales disposent également de systèmes dédiés, utilisés notamment par les forces de l'ordre ou les services de secours.

Les épreuves sportives de la CdM de rugby 2023 et des JOP 2024 se dérouleront respectivement sur 9 et 38 sites de compétition [1, 4]. Plusieurs systèmes d'information sont directement impliqués dans le déroulement des évènements sportifs, notamment pour la gestion des infrastructures physiques. Les systèmes de gestion physique ont progressivement été remplacés par des systèmes informatiques, créant une multitude de nouvelles dépendances. L'interconnexion entre les systèmes d'information bureautiques et les systèmes d'information industriels (OT[2]) brouille la frontière entre la sécurité physique et informatique. C'est le cas par exemple des systèmes de gestion technique de bâtiment qui contrôlent les affichages, l'alimentation électrique, la climatisation, les contrôles d'accès, ou encore la vidéosurveillance des infrastructures sportives. Le dysfonctionnement des contrôles d'accès et des caméras de surveillance exposerait les spectateurs à des menaces pour leur sécurité physique.

Outre la menace potentielle pour la sécurité des biens et personnes, des attaques sont également susceptibles de ternir l'image du pays hôte et d'avoir des conséquences négatives sur les retombées économiques pour les organisateurs (pertes de recettes en termes de billetterie, coût du remplacement du matériel…), les sponsors ainsi que les spectateurs (vol de données ou de fonds). Enfin, la qualité de l'expérience vécue par les spectateurs, les téléspectateurs et les internautes peut être affectée par la compromission de certains systèmes d'information (impossibilité d'accéder aux stades, fraudes, connexion en Wi-Fi impossible, retransmission télévisée perturbée).

Dans ce contexte, il convient de préciser que de plus en plus de services numériques (Wi-Fi public, application mobile…) sont proposés aux spectateurs et téléspectateurs des évènements sportifs d'ampleur afin de maximiser leur expérience. Athlètes, organisateurs et spectateurs utilisent également dans le cadre des compétitions sportives un nombre grandissant d'objets connectés. Certains outils informatiques sont ainsi employés dans le cadre des épreuves comme moyen d'aide à l'arbitrage ou au chronométrage. Enfin, un grand nombre de systèmes d'information sont également utilisés par des acteurs privés qui accueillent du public en dehors des épreuves sportives (transports, hôtels…).

1.2. Un contexte géopolitique et national à observer

Les contextes géopolitiques, politiques et sanitaires sont susceptibles d'avoir une incidence sur la sécurité informatique des grands évènements sportifs.

L'invasion de l'Ukraine par la Russie, débutée en février 2022, peut constituer un contexte de tensions favorables à la conduite d'attaques informatiques. La participation de la Russie aux JOP 2024 demeure incertaine et les prises de positions des pays participants exposent l'évènement à des cyberattaques par mesure de représailles. L'Ukraine, soutenue par plusieurs pays, menace de boycotter les JOP si les athlètes russes et biélorusses y participent sans bannière neutre [5, 6]. D'un autre côté, le maintien de l'exclusion de la Russie dans le contexte de l'invasion de l'Ukraine pourrait exposer les JOP 2024 à la conduite d'attaques ayant pour but de nuire à la réputation du pays hôte et de perturber le déroulement de l'évènement. En effet, l'exclusion de la Russie des JOP en 2018 en raison des accusations de dopage des athlètes a, selon les gouvernements américain, britannique et canadien, probablement

2. L'OT (*operational technology*) désigne la technologie d'exploitation, elle a en charge les systèmes d'information industriels.

motivé des attaques à des fins de déstabilisation par les groupes d'attaquants liés au renseignement militaire russe (GRU) [7, 8, 9].

Le contexte politique et social français, au moment des épreuves sportives, peut également avoir une incidence sur de potentielles attaques à des fins de revendication politique.

L'épidémie de Covid-19 a également mis en évidence les potentiels effets d'une crise sanitaire sur la tenue de grands évènements sportifs. Ce contexte a eu une incidence sur la nature et l'étendue de la surface d'attaque des JOP de Tokyo (2020) et de Pékin (2022). Dans le premier cas, l'absence de spectateurs étrangers et les paiements par carte bancaire privilégiés aux transactions en liquide ont modifié la surface d'attaque et les opportunités des attaquants [10, 11]. Dans le second cas, la vente des billets a été écourtée et le nombre de spectateurs a été restreint [12, 13]. L'évaluation de la menace est donc susceptible d'évoluer en fonction de ce facteur avant la CdM 2023 et les JOP 2024.

2. Attaques à des fins lucratives

La popularité des grands évènements sportifs attire une large audience. Cela représente un contexte favorable à la conduite d'attaques à des fins lucratives par des acteurs cybercriminels très divers. Cette menace, au regard de l'activité cybercriminelle de ces dernières années, apparaît particulièrement élevée.

2.1. Escroqueries ciblant les spectateurs

Les spectateurs pourraient être la cible de tentatives d'escroquerie bien avant la tenue des Jeux olympiques et paralympiques. Des attaquants ont par le passé exploité l'opportunité de l'ouverture de la billetterie des grands évènements sportifs pour créer de faux sites leur permettant de collecter des données personnelles et bancaires [14, 15, 16]. L'ouverture progressive de la billetterie des JOP 2024 à partir du mois de décembre 2022 constitue une opportunité d'agir pour les cybercriminels [17, 18, 19].

Les grands évènements sportifs comme les JOP sont le théâtre de campagnes d'envoi de courriels indésirables qui visent à vendre des billets contrefaits. Ces campagnes peuvent être aussi utilisés à des fins d'hameçonnage, car ces évènements attirent l'attention d'un large public. L'hameçonnage demeure l'un des vecteurs de compromission privilégiés des attaquants. L'utilisation d'une marque, d'un logo ou d'un slogan immédiatement reconnaissables et liés à un grand évènement multiplie leurs chances de convaincre les victimes de cliquer sur un lien ou d'ouvrir un fichier malveillant afin de les escroquer.

Des attaquants pourraient recourir à la création de faux sites Internet ou de fausses applications afin de réaliser des gains publicitaires, commercialiser des contrefaçons ou récupérer des informations sur les spectateurs ou les athlètes comme cela a été le cas lors de la Coupe du monde de football en 2022 [20, 21, 22]. À ces mêmes fins, des sites légitimes pourraient également être compromis pour rediriger les utilisateurs vers des domaines contrôlés par les attaquants (technique du « point d'eau »).

À titre d'exemple, lors de la Coupe du monde de football au Qatar en 2022, de faux sites Internet aux couleurs de l'évènement ont été recensés, servant à collecter des données de carte de crédit réutilisées pour réserver des billets d'avion et des chambres d'hôtel ou encore vendre de fausses cartes Hayya [3], sans lesquelles les spectateurs ne pouvaient pas accéder aux stades [20, 21].

Les cybercriminels peuvent exploiter des vulnérabilités associées au système d'exploitation des distributeurs automatiques de billets (DAB) afin d'extraire des billets, ou bien les piéger physiquement (*skimming* [4] et *jackpotting* [5]) afin de récupérer les numéros et empreintes de cartes bancaires. Ces techniques peuvent également être appliquées aux terminaux de points de vente dans les commerces et dans une certaine mesure aux sites de commerce en ligne. En effet, les DAB représentent des cibles d'opportunité pendant des évènements de grande échelle au cours desquels les volumes de transactions financières croissent significativement. La compromission de DAB proches des sites accueillant des évènements sportifs a pu être observée lors de grandes compétitions internationales similaires [3, 23, 24]. Les conséquences de ces attaques restent toutefois aujourd'hui limitées. L'adoption générale de la technologie EMV [6] pour les terminaux de point de vente a fortement limité les possibilités d'attaques massives.

Ces attaques, même si elles portent atteinte à la confidentialité des données personnelles et bancaires des spectateurs, n'ont pas d'incidence sur les systèmes d'information des grands évènements sportifs. Toutefois, elles peuvent avoir des conséquences réputationnelles sur l'organisation et le pays hôte.

3. La carte numérique Hayya rassemblait un permis d'entrée dans l'État du Qatar et le billet de match permettant aux spectateurs d'accéder au stade lors de la Coupe du monde de football en 2022.

4. Les attaquants placent un lecteur capturant la bande magnétique de la carte de crédit pendant qu'une caméra ou un faux clavier capture le code pin.

5. Les attaquants compromettent le module de contrôle du DAB à distance pour retirer de l'argent sans qu'il soit prélevé sur le compte des clients de la banque.

6. Europay, Mastercard et VISA. Technologie sécurisée permettant le chiffrement systématique des données de cartes bancaires au sein des terminaux de point de vente.

En cas de compromission ou de suspicion de compromission, les particuliers peuvent contacter Cybermalveillance, qui fait de l'assistance et de la prévention en sécurité numérique : https://www.cybermalveillance.gouv.fr/

2.2. Tentatives d'extorsion

2.2.1. Rançongiciels

La fréquente utilisation de rançongiciels dans le cadre d'attaques à but lucratif ces dernières années laisse penser que ce type de codes malveillants pourrait être utilisé en amont ou pendant la CdM 2023 ou les JOP 2024. Ces attaques pourraient perturber le déroulement des évènements sportifs devant se tenir en France en 2023 et 2024 par exemple en affectant les organisateurs ou sponsors, mais également les athlètes participants ou ainsi que certains services de l'État.

L'hypothèse d'un ciblage volontaire est peu probable. Néanmoins, les cybercriminels sont susceptibles de conduire un ciblage opportuniste. Ainsi, on observe depuis le début du conflit ukrainien des prises de position de groupes cybercriminels patriotiques opérant au service de motivations lucratives et politiques [25].

En janvier 2019, l'AS Saint-Étienne a été victime, *via* le ciblage du stade Geoffroy-Guichard, d'une attaque par rançongiciel. Le principal préjudice a été le blocage, pendant plusieurs jours, des échanges de courriels des employés avec l'extérieur ainsi que l'indisponibilité de la billetterie du club et du Musée des Verts. Au-delà de l'interruption des services, ce type d'attaque occasionne des pertes financières en raison de l'absence de recettes et du coût de la remédiation [26].

En 2020, un club majeur de la Ligue anglaise de football a subi une attaque par rançongiciel. Les attaquants ont demandé 400 Bitcoin (3,8 millions de dollars américains au moment des faits) en échange de la clé de déchiffrement. Suite au chiffrement des systèmes d'information, les comptes courriel du club étaient inaccessibles et le système de vidéosurveillance et les tourniquets du stade ne fonctionnaient pas, ce qui a failli entraîner l'annulation d'un match. D'après le NCSC-UK, le vecteur de compromission aurait été un courriel d'hameçonnage ou l'exploitation d'un accès à distance du réseau de vidéosurveillance pour rebondir vers le réseau bureautique. Cette attaque montre l'importance du cloisonnement des systèmes d'information bureautiques et de sécurité, qui aurait pu ralentir la propagation [27, 28].

La durée restreinte des évènements sportifs accroît considérablement la criticité de la continuité des services et donc de la disponibilité des systèmes d'information. Si des attaquants parviennent à chiffrer des réseaux critiques au bon déroulement des épreuves sportives, la pression exercée sur la victime pour rétablir la continuité de l'activité est accrue et peut l'inciter à payer une rançon.

L'ANSSI déconseille cependant de payer les rançons. En effet, le paiement ne garantit en rien le déchiffrement des données et peut compromettre le moyen de paiement utilisé (notamment carte bancaire) [29].

Même en l'absence d'une compromission de son système d'information, l'activité d'une entité est susceptible d'être perturbée par un incident affectant un tiers. Une cyberattaque peut ainsi avoir des effets de bord sans interconnexion entre les victimes. En mars 2019, un gestionnaire de parking canadien a été victime d'une attaque menée au moyen du rançongiciel Dharma. Un parking de 1000 places à Ottawa, permettant d'accéder à plusieurs infrastructures dont le Stade Place Toronto-Dominion (TD), a été affecté par cet incident. Pendant deux jours, les barrières du parking étaient levées et son accès était gratuit [30, 31]. Au-delà des pertes financières, ce type d'incidents soulève des problèmes d'accès maîtrisés et sécurisés aux infrastructures sportives.

L'activité d'une entité est également susceptible d'être perturbée en raison de la compromission d'un prestataire. Celle-ci peut également être un vecteur de compromission vers une victime finale. **Ce type d'attaque, nommé attaques *via* la chaîne d'approvisionnement (*supply chain attack*) met en exergue l'importance de la maîtrise de son système d'information et de ses interconnexions**.

2.2.2. Chantages au DDoS et à la divulgation de données

La CdM 2023 et les JOP 2024 pourraient également faire l'objet d'attaques par déni de service avec demande de rançon, appelées chantages au déni de service distribué (DDoS). À l'instar des rançongiciels, ce type d'attaque exploite le levier de l'indisponibilité des services afin de faire pression sur la victime. Les chantages au DDoS sont susceptibles de cibler certains sites officiels de la compétition, de ses sponsors ou encore de la ville d'accueil de la compétition [32].

En septembre 2021, VoIP.ms un opérateur de voix sur IP (*Voice Over Internet Protocol* ou *VoIP*) canadien a subi un chantage au DDoS par des attaquants semblant usurper l'identité du groupe cybercriminel REvil. Cette attaque a eu pour conséquence d'importantes perturbations des services de téléphonie sur IP fournis par l'opérateur, affectant l'ensemble de ses clients et l'indisponibilité de son site Internet. Les attaquants ont diffusé des messages sur les réseaux sociaux ajoutant une pression supplémentaire afin d'inciter la victime à payer la rançon. **Les effets sur la réputation et la criticité de la continuité de l'activité sont ainsi des leviers communément employés par les attaquants afin de faire pression sur les victimes dans le cadre de chantages à la divulgation et de maximiser leurs chances de collecter une rançon** [33].

Des attaquants pourraient réaliser des chantages à la divulgation d'informations, acquises dans le cadre d'une compromission précédente ou supposée de leurs systèmes d'information, à l'encontre de prestataires en profitant par exemple de la crainte des entreprises de voir leurs données personnelles et celles de leurs clients divulguées. Des attaques pourraient également être menées par pur opportunisme en profitant de la tenue de grands évènements sportifs pour mener des attaques de manière non ciblée, mais qui pourraient cependant affecter les prestataires par effet de bord.

2.3. Monétisation des données dérobées

Les données des participants aux évènements sportifs peuvent être la cible d'acteurs cybercriminels aux motivations lucratives.

Le vol et la vente de données à caractère personnel revêtent une importance continue au sein de l'écosystème cybercriminel. L'accumulation de données personnelles librement accessibles ou dérobées permet aujourd'hui aux groupes d'attaquants de reconstituer et de vendre des identités numériques ou des accès cohérents.

Au-delà de l'atteinte portée à la confidentialité des données des victimes et à la réputation des entités chargées de les sécuriser, ces données peuvent servir à mener d'autres types de compromissions.

En juillet 2021, les identifiants de spectateurs et de bénévoles des JOP 2020 ont été mis en vente sur un forum cybercriminel suite à un incident affectant le Comité olympique japonais. D'après ce dernier, la fuite de données n'était pas le résultat d'une intrusion, mais d'individus ayant entré par inadvertance leurs informations sur des sites d'hameçonnage [34, 35].

Les espaces publics hors des infrastructures olympiques peuvent également être la cible de cybercriminels. Les voyageurs arrivant à l'étranger cherchent souvent une connexion Wi-Fi gratuite, ce qui représente une opportunité pour des cybercriminels, surtout lorsqu'il y a une forte concentration de personnes durant un évènement sportif majeur. Lors des JOP de Rio en 2016, l'éditeur de sécurité Kaspersky avait estimé que près d'un quart des réseaux Wi-Fi figurant autour du Comité olympique du Brésil, du parc olympique et des stades n'étaient pas suffisamment sécurisés [36, 16]. La compromission des services Wi-Fi permet aux attaquants de capturer des informations personnelles nécessaires à la conduite de fraudes comme l'identité, l'adresse ou encore les données bancaires des victimes.

3. Attaques à des fins de déstabilisation

Les grands évènements sportifs sont susceptibles de faire l'objet d'attaques à des fins de déstabilisation, notamment du fait d'un contexte géopolitique dégradé. Comme d'autres pays hôtes par le passé, la France pourrait être ciblée par des acteurs étatiques et des hacktivistes aux motivations politiques ou idéologiques cherchant à déstabiliser, discréditer le pays hôte ou perturber la tenue des épreuves sportives. La visibilité accrue de ces évènements amplifie les conséquences des attaques.

3.1. Actions de sabotage informatique

Le sabotage se traduit par la destruction logicielle ou matérielle d'équipements informatiques, entraînant éventuellement une perte de données en l'absence de sauvegarde, la perte de service sur une durée indéterminée et des coûts de réparation ou de remplacement pouvant être très importants.

Des puissances étrangères pourraient se livrer à des actes de sabotage à l'égard des systèmes d'information de la CdM 2023 et des JOP 2024 afin de discréditer l'image de la France et de réduire les retombées économiques positives de ces évènements. Ce risque n'est pas théorique puisque plusieurs tentatives de sabotage ont ciblé dans le passé des évènements sportifs à l'étranger, dont les Jeux olympiques.

L'édition 2018 des JOP d'hiver à Pyeongchang (Corée du Sud) a fait l'objet d'une attaque informatique à visée destructrice au moyen du code de sabotage (*wiper*[7]) Olympic Destroyer, perturbant notamment la cérémonie d'ouverture de l'évènement. Cette attaque a conduit à l'indisponibilité du site Internet des JOP, de l'impression des billets, de la connexion Wi-Fi, du système de vidéosurveillance, de certains affichages dans le stade et de la retransmission en perturbant les flux vidéo. Les serveurs d'hôtels locaux ont également été touchés [37, 38]. Cette attaque a été attribuée publiquement par le NCSC-UK au renseignement militaire russe (GRU) [39]. Elle s'inscrit dans le contexte du scandale du dopage des athlètes russes en juillet 2016 qui a valu depuis à la Russie et ses athlètes des interdictions d'ampleur variée de participer aux compétitions sportives internationales [40].

Les systèmes d'information des grands évènements sportifs ne sont pas uniquement la cible d'attaques informatiques durant leur tenue. Des attaquants sont susceptibles de les cibler en amont, notamment dans la perspective de perturber leur déroulement. En octobre 2020, les autorités britanniques ont rendu publique l'existence d'opérations de reconnaissance visant certains systèmes d'information des organisateurs, services logistiques et sponsors des JOP de Tokyo, qui ont eu lieu aux mois de juillet et août 2021. Selon le gouvernement britannique, cette campagne a été conduite par une unité du GRU spécialisée dans les opérations de sabotage et à l'origine du *wiper* Olympic Destroyer. Cette unité aurait employé le mode opératoire réputé russe SANDWORM mais les informations à la disposition de l'ANSSI ne lui permettent pas de le confirmer ou de l'infirmer [37, 39].

En juillet 2021, un *wiper* distribué au moyen de leurres reprenant le thème des JOP de Tokyo a été observé par l'éditeur de sécurité FORTINET. Toutefois, le code malveillant ne disposait pas de fonctionnalités d'auto-propagation, ni de moyens de rendre le système inopérable. Les informations disponibles ne permettent pas d'identifier précisément les victimes de cette campagne, néanmoins, les leurres étaient rédigés en japonais et reprenaient le thème des JOP de Tokyo [41].

D'après les informations disponibles en sources ouvertes, les Jeux olympiques de Tokyo et de Pékin n'ont pas subi d'attaque informatique ayant perturbé leur déroulement.

7. Un type de code malveillant dont l'objectif est d'effacer les données du disque dur de la victime.

3.2. Une caisse de résonance pour les attaquants cherchant à amplifier leurs revendications

Des acteurs malveillants pourraient chercher à profiter de la CdM de rugby ou des JOP 2024 afin d'exploiter la couverture médiatique des évènements sportifs au profit de leur cause et afin de promouvoir leur action. Certains groupes pourraient lancer des attaques par déni de service distribué (DDoS) afin de perturber la disponibilité des services ou détourner l'attention d'autres attaques en cours. Ces attaques peuvent être conduites par des attaquants réputés étatiques ou des attaquants moins sophistiqués comme des groupes hacktivistes.

En 2016, la mouvance hacktiviste ANONYMOUS a été à l'origine d'attaques à l'encontre des autorités brésiliennes et des JOP de Rio en 2016, afin de dénoncer les inégalités économiques et sociales qui entouraient ces derniers. Ces attaques se sont déroulées en deux phases, une première ayant entraîné l'indisponibilité de sites Internet avec des attaques DDoS, la seconde consistant en la divulgation de données personnelles et financières de fédérations sportives brésiliennes [42].

Dans le contexte de la Coupe du monde de football au Qatar en 2022, le coût écologique et les violations des droits de l'Homme ont été des thèmes récurrents d'attaques. Des hacktivistes ont revendiqué des attaques par DDoS ciblant des entités qataries, comme les ministères des Transports et de la Communication et ont publié des preuves de l'indisponibilité de leurs sites Internet accompagnées des *hashtags* #OpQatar, #OpFIFA et #OpWorldCup [21]. Ce type d'attaque peut engendrer une indisponibilité de durée limitée et des pertes financières mais ses conséquences réputationnelles sont difficiles à évaluer.

Les contextes géopolitiques tendus sont propices à la conduite d'attaques à des fins de déstabilisation afin de nuire à l'adversaire. L'invasion russe en Ukraine débutée en février 2022 a déclenché une résurgence d'opérations hacktivistes pro-russes et pro-ukrainiennes.

Ainsi, depuis le mois de février 2022, des groupes hacktivistes mènent régulièrement des attaques liées à cette actualité géopolitique. Ces attaques ciblent régulièrement l'Ukraine mais leur ciblage s'est étendu aux pays de l'Union européenne qui soutiennent l'Ukraine. Selon l'éditeur de sécurité MANDIANT, une partie de ces groupes opère indépendamment du régime russe mais certains seraient des couvertures ou agiraient en coordination avec les autorités russes [43]. Le ciblage d'entités françaises, déjà constaté, est à envisager en représailles potentielles aux futures actions et prises de position de la France à l'égard de la Russie ou en soutien à l'Ukraine [44].

L'évolution des pratiques de visionnage des épreuves sportives, à travers la retransmission en *streaming* (diffusion en flux continu) sur Internet, offre aux attaquants des opportunités supplémentaires de cibler les grands évènements sportifs. En effet, afin d'augmenter la visibilité des évènements sportifs, les organisateurs se tournent de plus en plus vers des supports en ligne comme les sites de *streaming*, les applications et les réseaux sociaux afin de diffuser leurs contenus. Les services de *streaming* peuvent rencontrer des perturbations nuisant à la qualité de l'expérience des spectateurs, par exemple sous la forme d'attaques DDoS [45, 46, 47, 48].

Lors d'un match opposant les équipes de l'Ukraine et du Pays de Galles pendant la Coupe du monde de football 2022, la plateforme ukrainienne de *streaming* Oll.tv a ainsi été victime d'une attaque ayant perturbé sa transmission et redirigé les utilisateurs vers une chaîne de propagande pro-russe [45, 46]. La direction de la plateforme a attribué l'attaque à des attaquants russes sans toutefois fournir davantage d'informations.

Si la probabilité d'attaques informatiques par des hacktivistes dans le cadre de grands évènements sportifs est élevée, les conséquences techniques de ce type d'opérations demeure néanmoins limité. **Ces attaques conduisent généralement à une indisponibilité temporaire des services affectés mais peuvent avoir des effets réputationnels et financiers notables**.

3.3. Compromission et divulgation de données

Des attaquants peuvent conduire des attaques de type *hack-and-leak*, consistant à compromettre un système d'information et à diffuser tout ou une partie de contenu sensible.

Le sport contribue au rayonnement d'un pays à l'international. Ainsi, l'exclusion d'athlètes et de responsables olympiques de grands évènements sportifs peut motiver des actions de représailles. En septembre 2016, l'Agence mondiale antidopage (AMA) a confirmé avoir été victime d'une fuite de données confidentielles relatives à 41 athlètes ayant participé aux JOP de Rio. Ces données ont révélé des résultats de tests anti-dopage et des dossiers médicaux d'athlètes dont le contenu pouvait nuire à leur carrière. Selon l'AMA, cette attaque aurait été conduite par des attaquants réputés russes en réponse aux publications de l'agence révélant un système de dopage institutionnalisé dans le monde du sport russe [49, 50]. Ces révélations ont conduit à l'exclusion d'athlètes russes des compétitions sportives internationales [49, 51].

En décembre 2016 et novembre 2018, plus de 18,6 millions de documents relatifs au fonctionnement des instances internationales de football ont fait l'objet de divulgations, communément appelées « Football Leaks » [52]. Les données ont été obtenues au moyen de compromissions de systèmes d'information, mais les détails de ces accès malveillants ne sont pas connus en sources ouvertes. Ces révélations ont dévoilé des mécanismes d'évasion fiscale, des soupçons de fraude, de corruption et de dopage. Elles ont ainsi nui à l'image des entités et des individus impliqués.

La compromission d'un réseau social, la publication de messages compromettants ou d'une messagerie portent atteinte à l'image de l'entité ciblée et à la confidentialité des données des utilisateurs. Les réseaux sociaux sont une partie centrale des stratégies de communication de toute entité. Ces comptes sont nécessaires pour construire une marque, générer de nouveaux revenus et opérer une partie de la gestion de la relation clients. Des tentatives de prise de contrôle de comptes de réseaux sociaux d'entités impliquées dans l'organisation de la CdM 2023 et des JOP 2024, afin de diffuser des revendications ou des messages politiques, sont probables. Les comptes du réseau social X (anciennement Twitter) officiels du comité international olympique (CIO) et de plusieurs organisations sportives ont été compromis en février 2020 par le Collectif OurMine [8]. Les membres de ce dernier ont revendiqué agir afin de dénoncer le manque de sécurisation de sites très fréquentés et où sont stockées des données personnelles [53, 54]. Ces attaques démontrent que des comptes d'importantes institutions sportives demeurent vulnérables à des attaques de niveau technique limité mais ayant des conséquences médiatiques et réputationnelles notables.

Des attaques perpétrées par un individu agissant seul et pour des motifs personnels peuvent également cibler des entités sportives et avoir une portée déstabilisatrice. En novembre 2021, le forum de l'Olympique Lyonnais a été victime d'un vol de 38 500 dossiers d'utilisateurs, sans que les mots de passe aient été dérobés. L'attaque a été revendiquée par un supporter de l'Olympique de Marseille [55].

8. Groupe formé en 2014 et réputé pour son ciblage de réseaux sociaux de célébrités et de sites Internet d'entreprises populaires afin de faire la promotion de leurs services et d'inciter les victimes à augmenter leur sécurité informatique. Le groupe opèrerait depuis l'Arabie saoudite [53].

4. Attaques à des fins d'espionnage

4.1. Attaques ciblées

Si les évènements sportifs ne constituent pas, à première vue, une cible privilégiée de campagnes d'espionnage, ceux-ci réunissent dans un même pays, voire une même ville, de nombreuses personnalités politiques, dirigeants et collaborateurs d'entreprises. Ces individus constituent des cibles de choix pour des services de renseignement étrangers qui pourraient tenter de profiter de leur présence sur le territoire national afin de compromettre leurs appareils nomades, et *in fine* les réseaux de leurs institutions ou sociétés d'appartenance. En effet, la CdM 2023 et les JOP 2024 sont également des évènements diplomatiques internationaux. Les attaques à des fins d'espionnage ne sont toutefois pas susceptibles de perturber directement le déroulement des grands évènements sportifs. Néanmoins, la révélation d'activités d'espionnage pourrait, même indirectement, avoir une incidence sur leur tenue.

Les lieux d'hébergement mais également les systèmes d'information des infrastructures sportives (comme le Wi-Fi des stades), pourraient en particulier être ciblés. Des groupes d'attaquants se spécialisent dans la compromission de réseaux publics dans l'objectif de dérober des données. En effet, certains groupes conduisent des attaques ciblant les réseaux Wi-Fi d'hôtels afin de collecter les données personnelles de cadres supérieurs [56]. Les grands évènements sportifs, rassemblant des millions de visiteurs, représentent ainsi une opportunité d'agir pour ce type d'acteurs malveillants.

Il ne peut être exclu que la tenue de ces évènements sportifs soit exploitée afin de mener des campagnes d'espionnage à l'encontre des autorités publiques françaises. En effet, les thèmes de la CdM 2023 et les JOP 2024 pourraient être utilisés dans des campagnes d'hameçonnage ciblant les autorités françaises, et ces évènements pourraient être utilisés comme prétexte par des attaquants pour mener des opérations de lutte informatique offensive contre l'État français.

4.2. Attaques *via* la chaîne d'approvisionnement

Les manifestations sportives font intervenir plusieurs centaines d'entités aux systèmes d'informations parfois interconnectés entre eux les exposant particulièrement aux attaques *via* la chaîne d'approvisionnement (*supply chain attack*). Ce type d'attaque consiste à compromettre un tiers, comme un fournisseur de services logiciels, afin de cibler la victime finale.

En mai 2021, FUJITSU, une société japonaise d'équipements et services informatiques, a révélé avoir été victime d'un accès non autorisé ayant exposé les données de ses clients *via* ProjectWEB, sa plateforme de partage de données. Les JOP 2020 ont été affectés par cet incident, car les données personnelles d'environ 170 personnes appartenant à 90 entités prenant part aux exercices cyber du Comité d'organisation de Tokyo 2020 ont été dérobées. D'après les médias japonais, l'attaque aurait été conduite par le groupe d'attaquants CIRCUIT PANDA, réputé chinois, mais cette information n'a pas pu être confirmée par l'ANSSI [57]. La multitude de victimes et de renseignement stratégique collecté suggère que le ciblage des JOP faisait probablement partie d'une campagne d'espionnage plus large des clients de FUJITSU. En effet, les attaquants ont notamment dérobé 76 000 adresses mail d'employés et de contractuels du ministère japonais du Territoire, des Infrastructures, des Transports et du Tourisme [58, 59].

5. Recommandations

Les recommandations suivantes visent à éclairer le lecteur afin de bâtir une défense et à se prémunir des menaces détaillées précédemment. Ces recommandations ne sont pas exhaustives et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré. Ces recommandations portent sur les thèmes suivants :

- la sensibilisation ;
- les postes de travail ;
- l'infrastructure ;
- l'administration du système d'information ;
- le maintien en conditions de sécurité ;
- la journalisation et de la détection.

5.1. Sensibilisation

R1

Communiquer de manière régulière

Organiser des sessions de sensibilisation régulièrement afin de responsabiliser les utilisateurs, les administrateurs et les exploitants du système d'information. Les objectifs majeurs sont de mettre l'accent sur les enjeux de cybersécurité et de transmettre les bonnes pratiques à adopter face à une situation de cyber malveillance.

En particulier :

Pour les utilisateurs, administrateurs, et exploitants du système d'information (SI), communiquez les précautions suivantes :

- ne pas ouvrir les messages dont la provenance ou la forme est inconnue, car il pourrait s'agir d'une tentative d'attaque (ex rançongiciel) ;
- se méfier des extensions de pièces jointes douteuses (ex : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk…), et qui peuvent contenir des codes malveillants ;
- être vigilant face aux URL visitées depuis le poste de travail ;
- ne pas connecter sur son poste de travail une clé USB trouvée par hasard, car celle-ci pourrait être compromise par un logiciel malveillant.

Pour les administrateurs de SI, il est important d'axer la communication autour des thèmes suivants : :

- les administrateurs représentent des cibles particulières pour les attaquants de par la nature de leurs missions et les accès et les secrets d'authentification dont ils disposent ;
- de ce fait, les administrateurs doivent protéger leurs moyens et leurs ressources encore davantage avec un niveau de vigilance et de sécurité supplémentaires par rapport aux utilisateurs **[cf. notamment les recommandations du paragraphe 5.4]** ;
- les administrateurs doivent agir sur la mise en œuvre des bonnes pratiques d'administration et d'architecture sur les SI dont ils ont la charge ;

R2

S'exercer régulièrement

En complément des sessions de sensibilisation, il est nécessaire de mettre en place des exercices adaptés pour accroître la vigilance des utilisateurs, des administrateurs et des exploitants.

En particulier :

Pour les utilisateurs, administrateurs et exploitants du système d'information, mettez en pratique les exercices sur les attaques suivantes :

- hameçonnage par messagerie électronique ;
- hameçonnage par support USB ;
- ingénierie sociale

Pour les administrateurs, et exploitants du SI, mettez en pratique le scénario suivant :

- intrusion sur le SI (exemple : de l'intérieur ou depuis l'extérieur du SI).

R3

Pratiquer une veille active sur les menaces

Afin de rester informés sur les menaces émergentes et d'adopter les mesures de sécurité nécessaires à la bonne anticipation de la menace, il est important pour les directions des systèmes d'information et tous les acteurs impliqués dans la cybersécurité des entités, de mener une veille active sur le site du CERT-FR ou tout autre site permettant de suivre l'évolution des menaces en matière de cybersécurité **[Pour aller plus loin 01]**.

5.2. Poste de travail et terminaux mobiles

R4

Sécuriser les postes de travail et les terminaux mobiles des utilisateurs

Mettre en place des mesures organisationnelles et techniques permettant de sécuriser les moyens informatiques mis à la disposition des utilisateurs, des administrateurs et des exploitants. L'objectif est de réduire la surface d'attaque du système d'information et donc de limiter le risque de compromission **[Pour aller plus loin 01]**.

En particulier :

- les moyens informatiques confiés aux utilisateurs sont réservés à un usage professionnel ;
- les utilisateurs ne disposent pas de droits d'administration ;
- les périphériques de stockage utilisés sont chiffrés, y compris le stockage amovible ;
- les risques liés à l'utilisation de support amovible sont traités ;
- les mots de passe stockés sur les systèmes sont protégés, les mots de passe sont complexes **[Pour aller plus loin 02]** ;
- les accès à Internet (Web/mails) transitent par les passerelles d'accès de l'entreprise, qui mettent en œuvre des filtrages pour se prémunir des codes malveillants et opérer une supervision de sécurité.

5.3. Protection du système d'information

R5

Cartographier le SI

Recenser tous les éléments constitutifs du système d'information. L'objectif de la cartographie du SI est de connaître l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle.
La cartographie doit permettre de représenter le système d'information sous forme de vues : l'écosystème métier, applicatif, logique, physique **[Pour aller plus loin 03]**.

R6

Restreindre au strict besoin les services numériques exposés à Internet

Afin de réduire la surface d'attaque du SI et ainsi d'en avoir la maîtrise, il est recommandé :

- d'identifier et limiter l'ensemble des services numériques (applications métiers, services d'infrastructure) nécessitant une interconnexion à Internet (en distinguant les flux entrants et les flux sortants) ;
- de dissocier les accès Internet des accès aux services critiques de l'entité ;
- de forcer les interconnexions identifiées à passer au travers d'une passerelle Internet sécurisée.

R7

Déployer une passerelle Internet sécurisée

Afin de protéger le SI interne des menaces d'Internet, il est recommandé de construire la passerelle de la manière suivante **[Pour aller plus loin 04]** :

- rendre incontournable la passerelle Internet sécurisée pour les flux entrants et sortants du système d'information ;
- mettre en œuvre des pare-feux après le routeur d'accès Internet et devant le SI interne pour constituer une ou plusieurs zones démilitarisées (DMZ) ;
- déployer des services applicatifs de relais dans la ou les DMZ.

R8

Segmenter et filtrer au sein du système d'information

Afin d'éviter la propagation d'une attaque, il est recommandé de segmenter et cloisonner le SI en plusieurs zones de sécurité homogènes (par sensibilité, criticité ou autres critères métier). En complément, des dispositifs de filtrage réseau (pare-feu) doivent être mis en œuvre pour cloisonner les différentes zones du SI (ex : zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, etc.). Ainsi, le cloisonnement sera assuré et les flux entre les différentes zones, maîtrisés.

R9

Sécuriser la configuration des équipements et des logiciels utilisés

L'intégrité des équipements du SI doit être vérifiée et leur configuration doit être durcie au maximum quand cela est possible et maîtrisé.

En particulier :

- n'installer que les services strictement utiles sur les équipements ;
- les configurations des serveurs (physique et virtuel) sont durcies (suppression des mots de passe par défaut, suppression des programmes inutiles, etc.) ;
- l'intégrité des *firmware* et des microcodes installés sur les équipements du SI (serveurs, équipements réseau, postes de travail, etc.) est vérifiée ;
- les accès aux interfaces de gestion matérielle (IDRAC, ILO, IPMI) sont maîtrisés (ex : accessibles depuis un VPN avec une authentification double facteurs s'ils sont exposés sur Internet).

R10

Mettre en œuvre des contre-mesures aux attaques en déni de service

Dans le cas où l'entité expose des services sur Internet, il est recommandé, qu'il s'agisse d'un service souscrit auprès d'un FAI ou géré en propre par l'entité, de déployer une solution de protection anti-DDos **[Pour aller plus loin 05]**.

En particulier :

- Prévoir un mode dégradé pour les activités critiques en cas d'attaque en déni de service.

R11

Mettre en œuvre un contrôle d'accès physique

Afin de protéger physiquement l'accès aux locaux techniques et donc au système d'information, il est recommandé de mettre en œuvre un système de contrôle d'accès physique afin de s'assurer que seules les personnes explicitement autorisées pourront y accéder **[Pour aller plus loin 06]**.

R12

Mettre en œuvre une politique de MCO et MCS pour les SI

Veiller à définir et appliquer une politique de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS) afin de renforcer la sécurité et la stabilité du SI. En priorité, appliquer les correctifs de sécurité sur les équipements et services directement exposés sur Internet, sachant qu'ils sont particulièrement exposés aux attaques cyber.

R13

Définir une politique de sauvegarde des SI

Afin de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission (par exemple, liés à un rançongiciel), une politique de sauvegarde régulièrement mise à jour doit être définie, appliquée et testée. Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue afin de garantir une restauration en cas d'attaque par un rançongiciel. Au besoin, les sauvegardes doivent être chiffrées afin d'en garantir la confidentialité.

En particulier :

- définir une liste des données jugées vitales pour l'organisme et les serveurs concernés ;
- définir la fréquence des sauvegardes ;
- réaliser des sauvegardes des données critiques et prévoir au minimum une sauvegarde hors ligne (à intervalle régulier) afin de se prémunir des attaques de type rançongiciel ;
- rédiger et tester les procédures de tests et de restauration ;
- rédiger et tester les procédures d'administration et d'exécution des sauvegardes ;
- définir des restrictions d'accès aux sauvegardes.

5.4. Administration du système d'information

R14

Supprimer les accès d'administration exposées directement sur Internet

Dès lors que cela est techniquement possible, il est recommandé de désactiver les accès aux interfaces d'administration, accessibles depuis Internet, afin de réduire au maximum la surface d'attaque du SI. Leur exposition sur Internet facilite le travail des attaquants. De fait, il convient de ne pas les exposer directement et de limiter leur accès strictement aux administrateurs de l'entité (exemple : interface d'administration accessible depuis un réseau d'administration interne dédié, accès aux interfaces depuis un VPN avec une authentification double facteurs).

R15

Administrer le SI depuis un réseau dédié

Les ressources d'administration du SI (ex. : postes d'administration, serveurs outils d'administration) doivent être déployées sur un réseau dédié à cet usage **[Pour aller plus loin 07]**. L'objectif de sécurité est de rendre le SI d'administration le plus sécurisé possible en l'isolant.

R16

Utiliser un poste d'administration dédié et durci

L'utilisation d'un poste d'administration physiquement dédié et durci pour les actions d'administration est recommandée. Ce poste d'administration doit être distinct du poste bureautique et doit faire partie intégrante du SI d'administration. Ce poste d'administration n'a pas d'accès à Internet pour limiter sa surface d'attaque.

5.5. Journalisation et détection

R17

Activer la collecte des journaux d'évènements

Les journaux d'évènements (des composants, des systèmes d'exploitation, des applications, etc.) doivent être activés et collectés. Cela permet d'investiguer les incidents de sécurité *post-mortem*, voire de détecter un incident de sécurité avant que l'attaquant ne parvienne à réaliser son objectif. La centralisation des évènements de sécurité contribue d'une part à sécuriser la collecte des évènements et d'autre part à faciliter les opérations de détection et d'analyse en cas d'incident.

En particulier :

- les évènements utiles aux activités de détection et d'analyse sont identifiés et activés ;
- les évènements sont collectés en fonction de l'évolution du SI et des menaces.

R18

Mettre en œuvre et maintenir des solutions contre les codes malveillants

Des solutions contre les codes malveillants (exemple : antivirus, EDR) doivent être installées sur l'ensemble des serveurs applicatifs, sur les postes de travail et sur les moyens permettant l'interconnexion des SI avec d'autres SI.

R19

Adapter la politique de protection contre les codes malveillants

Des solutions de protection contre les codes malveillants sont indispensables, mais leur déploiement et leur configuration doivent être réfléchis, de sorte qu'elles ne soient pas à l'origine d'un affaiblissement du niveau de sécurité (augmentation de la surface d'attaque, source d'exfiltration de données).

5.6. Références

Pour aller plus loin

01 ANSSI, Cybersécurité pour les TPE/PME en 13 questions, 26 octobre 2022 : https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/
02 ANSSI, Authentification multifacteur et mots de passe, 8 octobre 2021 : https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
03 ANSSI, Cartographie du système d'information, 21 novembre 2018 : https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/
04 ANSSI, Guide interconnexion d'un système d'information à Internet, 19 juin 2020 : https://www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
05 ANSSI, Comprendre et anticiper les attaques DDoS, 20 mars 2015 : https://www.ssi.gouv.fr/guide/comprendre-et-anticiper-les-attaques-ddos/
06 ANSSI, Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, 4 mars 2020 : https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/dispositifs-de-videoprotection/
07 ANSSI, Guide d'administration sécurisée, 11 mai 2021 : https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/
08 ANSSI, Guide d'hygiène, septembre 2017 : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
09 ANSSI, Kit de sensibilisation - Assistance aux victimes de cybermalveillance, 21 janvier 2020 : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation
10 ANSSI, Administration sécurisée des systèmes d'information, 11 mai 2021 : https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/
11 ANSSI, Le nomadisme numérique, 19 octobre 2018 : https://www.ssi.gouv.fr/entreprise/guide/recommandations-sur-le-nomadisme-numerique/

Autres ressources utiles

- CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques), pour l'administration et les opérateurs d'importance vitale et de services essentiels : https://www.cert.ssi.gouv.fr/contact/
- Cybermalveillance, assistance et prévention en sécurité numérique pour les particuliers, les entreprises, les associations, les collectivités et les administrations : https://www.cybermalveillance.gouv.fr/

6. Annexes

Chronologie des principaux incidents ayant ciblé les Jeux olympiques

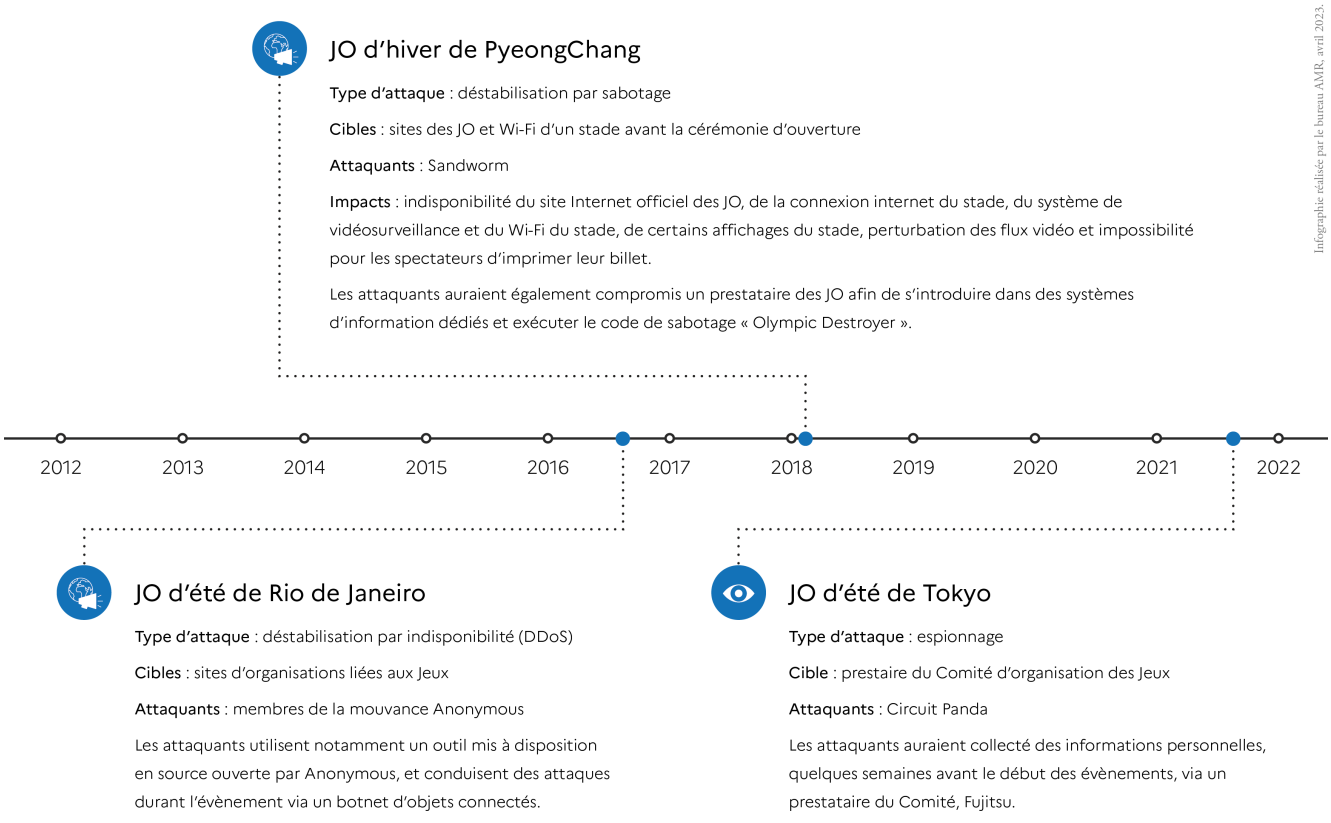

FIG. 6.1.

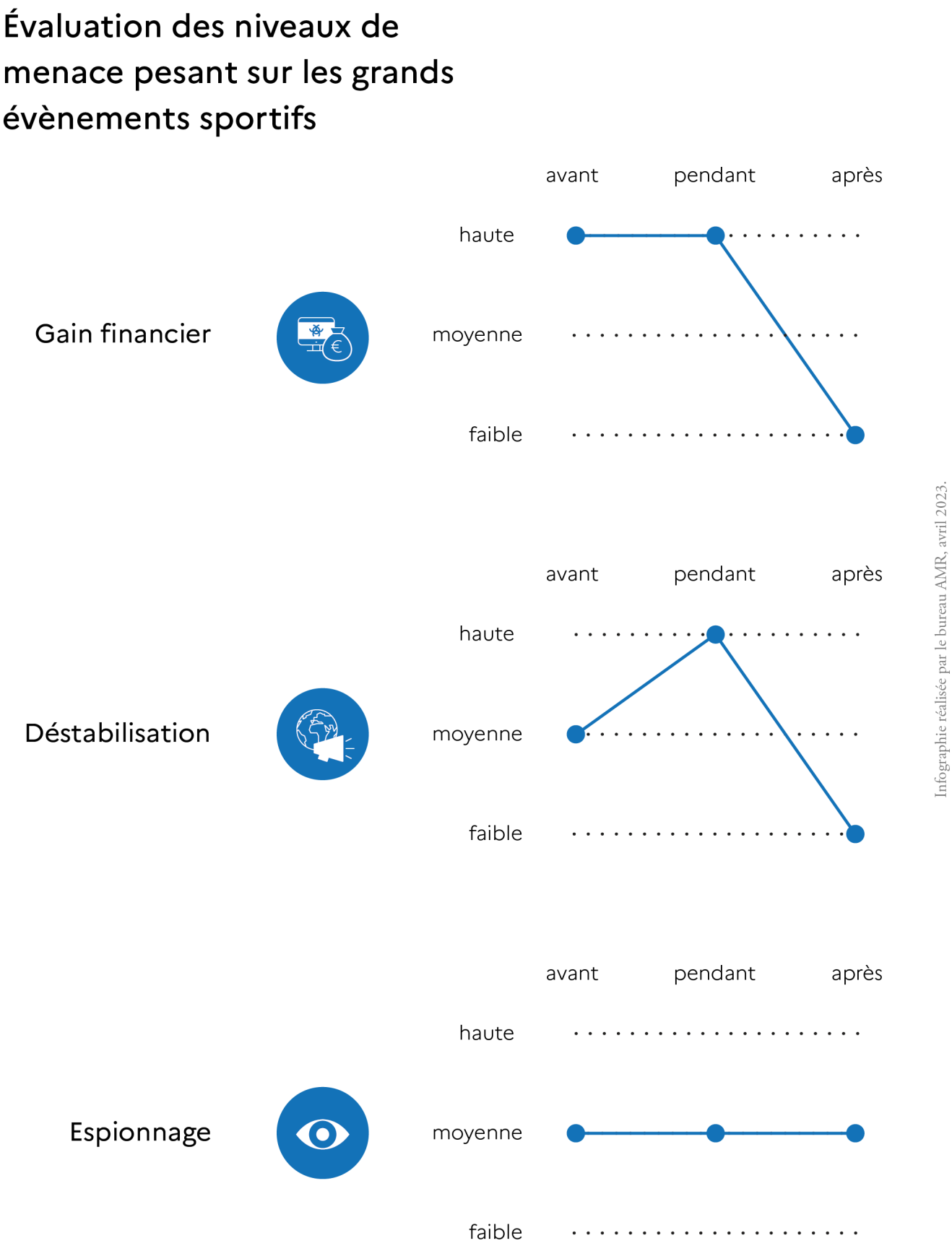
Évaluation des niveaux de menace pesant sur les grands évènements sportifs
avant
pendant
après
haute
moyenne
faible
Gain financier
Déstabilisation
Espionnage
Infographie réalisée par le bureau AMR, avril 2023.

FIG. 6.2.

A. Bibliographie

[1] Paris 2024. *Paris 2024 et ses parties prenantes annoncent le cadre exceptionnel de la Plac...* 20 octobre 2022.
URL : https://presse.paris2024.org/actualites/paris-2024-et-ses-parties-prenantes-annoncent-le-cadre-exceptionnel-de-la-place-de-la-concorde-et-des-champs-elysees-pour-la-ceremonie-douverture-des-jeux-paralympiques-de-paris-2024-7e95-e0190.html.

[2] Cynthia Dion-Schwarz et al. *Olympic-Caliber Cybersecurity : Lessons for Safeguarding the 2020 Games and Other Major Events*. 4 octobre 2018.
URL : https://www.rand.org/pubs/research_reports/RR2395.html.

[3] Cyber Threat Alliance et al. *2020 Summer Olympics Threat Assessment*. 1er janvier 2020.
URL : https://cyberthreatalliance.org/wp-content/uploads/2021/05/CTA-2020-Olympics-Threat-Assessment-Report_rev_Final.pdf.

[4] Rugby World Cup France 2023. *Votre guide des neuf stades de la Coupe du Monde de Rugby 2023*. 8 septembre 2021.
URL : https://www.rugbyworldcup.com/2023/news/626157/guide-stades-coupe-du-monde-de-rugby-2023?lang=fr.

[5] Le Figaro. *Foot : la Russie écartée de l'Euro 2024*. 20 septembre 2022.
URL : https://www.lefigaro.fr/sports/football/euro-2024-la-russie-ne-participera-pas-au-tirage-au-sort-20220920.

[6] AFP et Médiapart. *L'Ukraine menace de boycotter les JO de Paris 2024 si la Russie est invitée*. 26 janvier 2023.
URL : https://www.mediapart.fr/journal/fil-dactualites/260123/l-ukraine-menace-de-boycotter-les-jo-de-paris-2024-si-la-russie-est-invitee.

[7] Le Monde. *Les Occidentaux se coordonnent pour accuser la Russie de cyberattaques*. 4 octobre 2018.
URL : https://www.lemonde.fr/pixels/article/2018/10/04/les-occidentaux-se-coordonnent-pour-accuser-la-russie-de-cyberattaques_5364802_4408996.html.

[8] Ministère de la Défense néerlandais. *Russian Cyber Operation Disrupted - Cyber Security - Defensie.Nl*. 4 octobre 2018.
URL : https://english.defensie.nl/topics/cyber-security/russian-cyber-operation.

[9] Gouvernement britannique. *Minister for Europe Statement : Attempted Hacking of the OPCW by Russian Military Intelligence*. 4 octobre 2018.
URL : https://www.gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence.

[10] USA TODAY. *Tokyo Olympics to Be Held without Fans after New COVID-19 State of Emergency Declared*. 8 juillet 2021.
URL : https://www.usatoday.com/story/sports/olympics/2021/07/08/2021-olympics-fan-not-allowed-attend-tokyo-games-due-covid-19/7899959002/.

[11] Twimbit. *Banking on the Olympics – Japan Speeds towards Digitisation*. 24 janvier 2020.
URL : https://twimbit.com/insights/banking-olypics-japan.

[12] Time. *What We Learned About COVID-19 Rules at the 2022 Olympics*. 21 février 2022.
URL : https://time.com/6149800/beijing-2022-covid-19-olympics/.

[13] NPR. *China Will No Longer Sell Tickets to the Beijing Winter Olympics Due to COVID-19*. 17 janvier 2022.
URL : https://www.npr.org/2022/01/17/1073597684/beijing-olympics-tickets.

[14] Reuters. *Beijing Games Hit by Internet Ticket Scam*. 4 août 2008.
URL : https://www.reuters.com/article/us-olympics-tickets-scam-idUSPEK25562820080804.

[15] The Guardian. *Last Minute Olympics Tickets Too Good to Be True, Which Warns*. 28 juillet 2016.
URL : http://www.theguardian.com/money/2016/jul/28/last-minute-olympics-tickets-scam-warning.

[16] Forbes. *Hackers Go For Gold At 2016 Rio Olympics*. 8 août 2016.
URL : https://www.forbes.com/sites/curtissilver/2016/08/08/hackers-go-for-gold-at-2016-rio-olympics/.

[17] Le Monde. *JO 2024 : plus de 13 millions de billets sont mis en vente, un défi technique et sécuritaire*. 23 décembre 2022.
URL : https://www.lemonde.fr/sport/article/2022/12/23/bugs-fraudes-cyberattaques-le-defi-technique-et-securitaire-de-la-billetterie-des-jeux-de-paris-2024_6155513_3242.html.

[18] Franceinfo. *Paris 2024 : comment les organisateurs ont-ils structuré la billetterie pour faire face aux cyberattaques ?* 15 mars 2023.
URL : https://www.francetvinfo.fr/les-jeux-olympiques/paris-2024/paris-2024-comment-les-organisateurs-ont-ils-structure-la-billetterie-pour-faire-face-aux-cyberattaques_5710715.html.

[19] Le Figaro. *Jeux olympiques : comment Paris 2024 souhaite lutter contre les faux billets*. 30 novembre 2022.
URL : https://www.lefigaro.fr/actualite-france/jeux-olympiques-comment-paris-2024-souhaite-lutter-contre-les-faux-billets-20221130.

[20] Group-IB. *Scammers on the Pitch : Group-IB Identifies Online Threats to Fans at FIFA World Cup 2022 in Qatar*. 29 novembre 2022.
URL : https://www.group-ib.com/media-center/press-releases/scammers-on-the-pitch/.

[21] CloudSEK. *FIFAWorldCup Qatar2022 : Cyber ThreatLandscape*. 29 novembre 2022.
URL : https://uploads-ssl.webflow.com/635e632477408d12d1811a64/63d39ff76e65a6946876a083_Fifa-Cyber-threat-report.pdf.

[22] ReliaQuest. *Cyber Threats to the FIFA World Cup Qatar 2022*. 10 novembre 2022.
URL : https://www.reliaquest.com/blog/cyber-threats-to-the-fifa-world-cup-qatar-2022/.

[23] Kaspersky. *IT Threats during the 2016 Olympic Games in Brazil*. 13 juin 2016.
URL : https://securelist.com/it-threats-during-the-2016-olympic-games-in-brazil/75045/.

[24] Radware. *2018 Winter Olympics & Threats of Cyber Attacks*. 29 janvier 2018.
URL : https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/2018-winter-olympics/.

[25] Accenture. *Global Incident Report : Threat Actors Divide Along Ideological Lines over the Russia-Ukraine Conflict on Underground Forums*. 14 mars 2022.
URL : https://acn-marketing-blog.accenture.com/wp-content/uploads/2022/03/UPDATED-ACTI-Global-Incident-Report-Ideological-Divide-Blog-14MARCH22.pdf.

[26] Le Point. *L'AS Saint-Etienne victime d'une tentative d'escroquerie par des hackers*. 26 janvier 2019.
URL : https://www.lepoint.fr/sport/l-as-saint-etienne-victime-d-une-tentative-d-escroquerie-par-des-hackers-26-01-2019-2289080_26.php.

[27] NCSC-UK. *The Cyber Threat to Sports Organisations*. 23 juillet 2020.
URL : https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf.

[28] Decrypt. *UK Football Club Held to Ransom over 400 Bitcoin ($3.8 Million)*. 24 juillet 2020.
URL : https://decrypt.co/36579/uk-football-club-held-to-ransom-over-400-bitcoin-3-8-million.

[29] ANSSI. *Publication : Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ?* 1er août 2020.
URL : https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/.

[30] Bleeping Computer. *Ransomware Hits Garage of Canadian Domain Registration Authority*. 28 mars 2019.
URL : https://www.bleepingcomputer.com/news/security/ransomware-hits-garage-of-canadian-domain-registration-authority/.

[31] IT World Canada. *Ottawa Parking Garage System Hit by Ransomware, Entry System Crippled | IT World Canada News*. 28 mars 2019.
URL : https://www.itworldcanada.com/article/ottawa-parking-garage-system-hit-by-ransomware-entry-system-crippled/416389.

[32] Akamai. *Unprecedented Levels of Ransom DDoS Extortion Attacks*. 11 septembre 2020.
URL : https://www.akamai.com/blog/trends/unprecedented-levels-of-ransom-ddos-extortion-attacks.

[33] Bleeping Computer. *VoIP.Ms Phone Services Disrupted by DDoS Extortion Attack*. 20 septembre 2021.
URL : https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/.

[34] Computer Weekly. *Tokyo 2020 Hit by Data Breach*. 26 juillet 2021.
URL : https://www.computerweekly.com/news/252504456/Tokyo-2020-hit-by-data-breach.

[35] The Asahi Shimbun. *Data on Ticket Buyers and Volunteers for Olympics Leaked | The Asahi Shimbun : Breaking News, Japan News and Analysis*. 22 juillet 2021.
URL : https://www.asahi.com/ajw/articles/14401064.

[36] Kaspersky. *Le guide complet des cybermenaces à la mode liées aux Jeux Olympiques*. 20 juillet 2016.
URL : https://www.kaspersky.fr/blog/olympic-games-2016-threats-guide/5868/.

[37] Kaspersky. *Olympic Destroyer : qui a piraté les Jeux Olympiques ?* 26 octobre 2020.
URL : https://www.kaspersky.fr/blog/olympic-destroyer/10084/.

[38] Wired. *Inside Olympic Destroyer, the Most Deceptive Hack in History*. 17 octobre 2019.
URL : https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[39] Gouvernement britannique. *UK Exposes Series of Russian Cyber Attacks against Olympic and Paralympic Games*. 19 octobre 2020.
URL : https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games.

[40] Le Monde. *Dopage : la Russie conteste sa mise au ban du sport mondial*. 27 décembre 2019.
URL : https://www.lemonde.fr/sport/article/2019/12/27/dopage-la-russie-conteste-sa-mise-au-ban-du-sport-mondial_6024192_3242.html.

[41] Fortinet. *Wiper Malware Riding the 2021 Tokyo Olympic Games | FortiGuard Labs*. 26 juillet 2021.
URL : https://www.fortinet.com/blog/threat-research/wiper-malware-riding-tokyo-olympic-games.html.

[42] HackRead. *Anonymous DDoS Brazilian Government Websites Because Rio Olympics*. 6 août 2016.
URL : https://www.hackread.com/anonymous-ddos-brazilian-government-websites/.

[43] Mandiant. *GRU : Rise of the (Telegram) MinIOns*. 23 septembre 2022.
URL : https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.

[44] Numerama. *Des hackers russes s'attaquent à la France pendant le discours de Poutine*. 21 février 2023.
URL : https://www.numerama.com/cyberguerre/1277226-des-hackers-russes-sattaquent-a-la-france-pendant-le-discours-de-poutine.html.

[45] Institute of Mass Information. *Hackers Attack OLL.TV Media Service and Broadcast Russian Propaganda Instead of Football*. 6 juin 2022.
URL : https://imi.org.ua/en/news/hackers-attack-oll-tv-media-service-and-broadcast-russian-propaganda-instead-of-football-i45981.

[46] Story Ukraine. *Russian Hackers Hacked Oll.Tv during 2022 FIFA World Cup Qualifier Ukraine vs. Wales – Ukraine News, Politics*. 6 juin 2022.
URL : https://news.storyua.com/news/23541.html.

[47] The Verge. *FuboTV Was down during a World Cup Semifinal Due to a 'Cyber-Related Incident'*. 14 décembre 2022.
URL : https://www.theverge.com/2022/12/14/23509674/fubo-tv-down-france-morocco-world-cup-semifinal.

[48] SportBusiness. *World Cup Rights-Holder New World TV Hit by Cyber Attacks*. 6 décembre 2022.
URL : https://www.sportbusiness.com/news/world-cup-rights-holder-new-world-tv-hit-by-cyber-attacks/.

[49] Reuters. *Anti-Doping Agency Says Athlete Data Stolen by Russian Group*. 13 septembre 2016.
URL : https://www.reuters.com/article/us-doping-wada-cyber/anti-doping-agency-says-athlete-data-stolen-by-russian-group-idUSKCN11J26T.

[50] World Anti-Doping Agency. *Cyber Security Update : WADA's Incident Response (5 October 2016)*. 5 octobre 2016.
URL : https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response.

[51] Libération. *Dopage d'Etat : un rapport de l'AMA va-t-il priver la Russie des JO ?* 18 juillet 2016.
URL : https://www.liberation.fr/sports/2016/07/18/dopage-d-etat-un-rapport-de-l-ama-va-t-il-priver-la-russie-des-jo_1466924/.

[52] La Croix. *"Football Leaks" : Rui Pinto reconnaît avoir recouru au piratage informatique*. 10 octobre 2022.
URL : https://www.la-croix.com/Lanceur-alerte-pirate-informatique-source-Football-Leaks-barre-2022-10-10-1301236926.

[53] Wired. *Meet OurMine, the 'Security' Group Hacking CEOs and Celebs*. 27 juin 2016.
URL : https://www.wired.com/2016/06/meet-ourmine-security-group-hacking-ceos-celebs/.

[54] Reuters. *Twitter Says Olympics, IOC Accounts Hacked*. 15 février 2020.
URL : https://www.reuters.com/article/us-twitter-olympics-idUSKBN2090SA.

[55] Le Figaro. *Le forum officiel de l'Olympique Lyonnais piraté pour «venger» l'attaque de Dimitri Payet*. 25 novembre 2021.
URL : https://www.lefigaro.fr/sports/football/ligue-1/le-forum-officiel-de-l-olympique-lyonnais-pirate-pour-venger-l-attaque-de-dimitri-payet-20211125.

[56] ZScaler. *New DarkHotel APT Attack Chain Identified*. 16 décembre 2021.
URL : https://www.zscaler.com/blogs/security-research/new-darkhotel-apt-attack-chain-identified.

[57] The Asahi Shimbun. *Hackers Sought Government Data on Nuclear Plants, Olympics | The Asahi Shimbun : Breaking News, Japan News and Analysis*. 31 août 2021.
URL : https://www.asahi.com/ajw/articles/14430219.

[58] Cyber Security Hub. *IOTW : Tokyo Olympics Suffers a Fujitsu-Related Breach*. 6 août 2021.
URL : https://www.cshub.com/executive-decisions/articles/iotw-tokyo-olympics-suffers-a-fujitsu-related-breach.

[59] Recorded Future. *Threats to the 2022 Winter Olympics*. 29 juin 2022.
URL : https://www.recordedfuture.com/threats-2022-olympics-games.

30 août 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité