JOP Paris 2024 et risques cyber : *l'été de tous les dangers ?*

by cymbioz

RP | INFLUENCE | DIGITAL

Jeux olympiques de Tokyo

450 millions de tentatives d'attaques avaient été repérées par l'opérateur télécoms japonais **NTT.**

Jeux olympiques de Paris

3 milliards d'événements cyber attendus d'après **Franz Régul, RSSI JOP 2024.**

étatiques

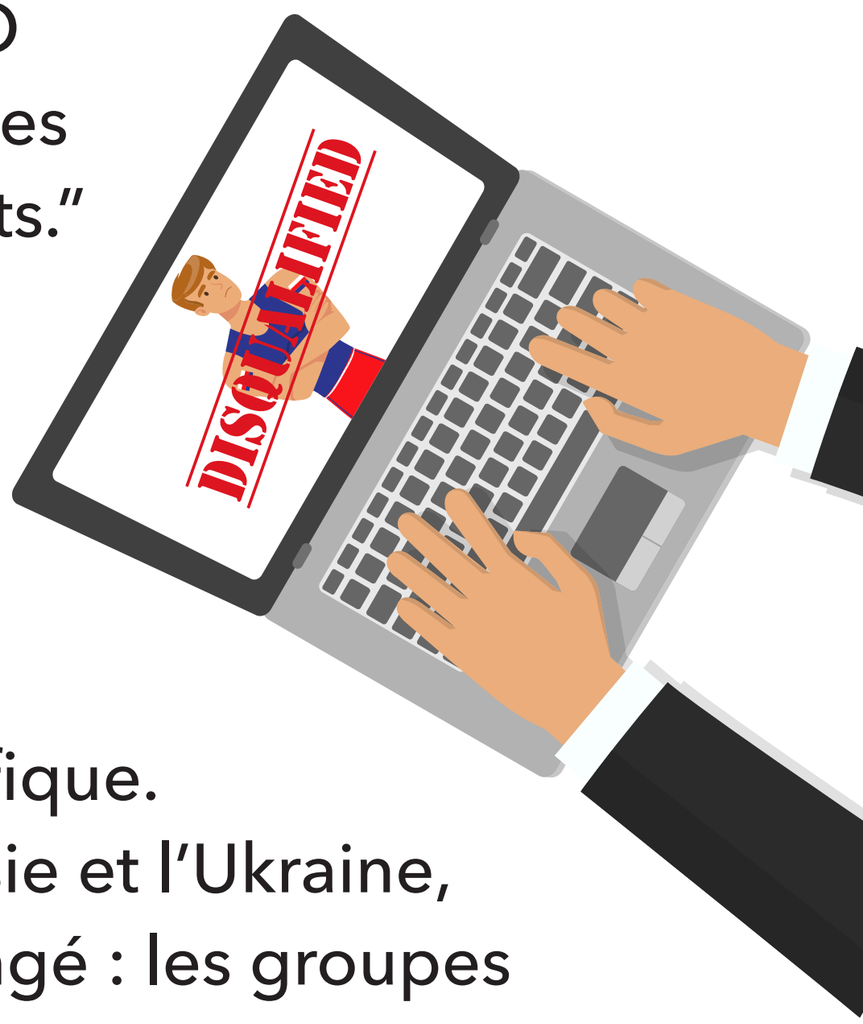
“**L’impact réputationnel d’une crise est majeur, d’ailleurs c’est un prétexte des hacktivistes pour cibler les JOP.** En effet, s’il y a un problème de diffusion, 4 milliards de téléspectateurs potentiels peuvent être touchés donc l’impact est énorme.”

Guillaume Tissier **Directeur du Forum InCyber Europe**

Attaques

“Les JOP **sont souvent utilisés comme des scènes politiques**. L’exclusion de la Russie des JO de Tokyo 2022 et les déclarations politiques d’athlètes en sont des exemples marquants.”

Martin Kraemer **Expert en sensibilisation à la cybersécurité chez KnowBe4**



“Les JOP s’ouvrent dans un contexte spécifique. Depuis le début de la guerre entre la Russie et l’Ukraine, le paysage cyber a considérablement changé : les groupes géopolitiques malveillants affiliés à un État ou non sont désormais mieux entraînés et plus organisés, **notamment avec l’arrivée de Télégram qui permet de garantir l’anonymat complet**, le chiffrement et l’utilisation de groupes sans limitation de membres”.

Adrien Merveille **Expert en cybersécurité chez Check Point**

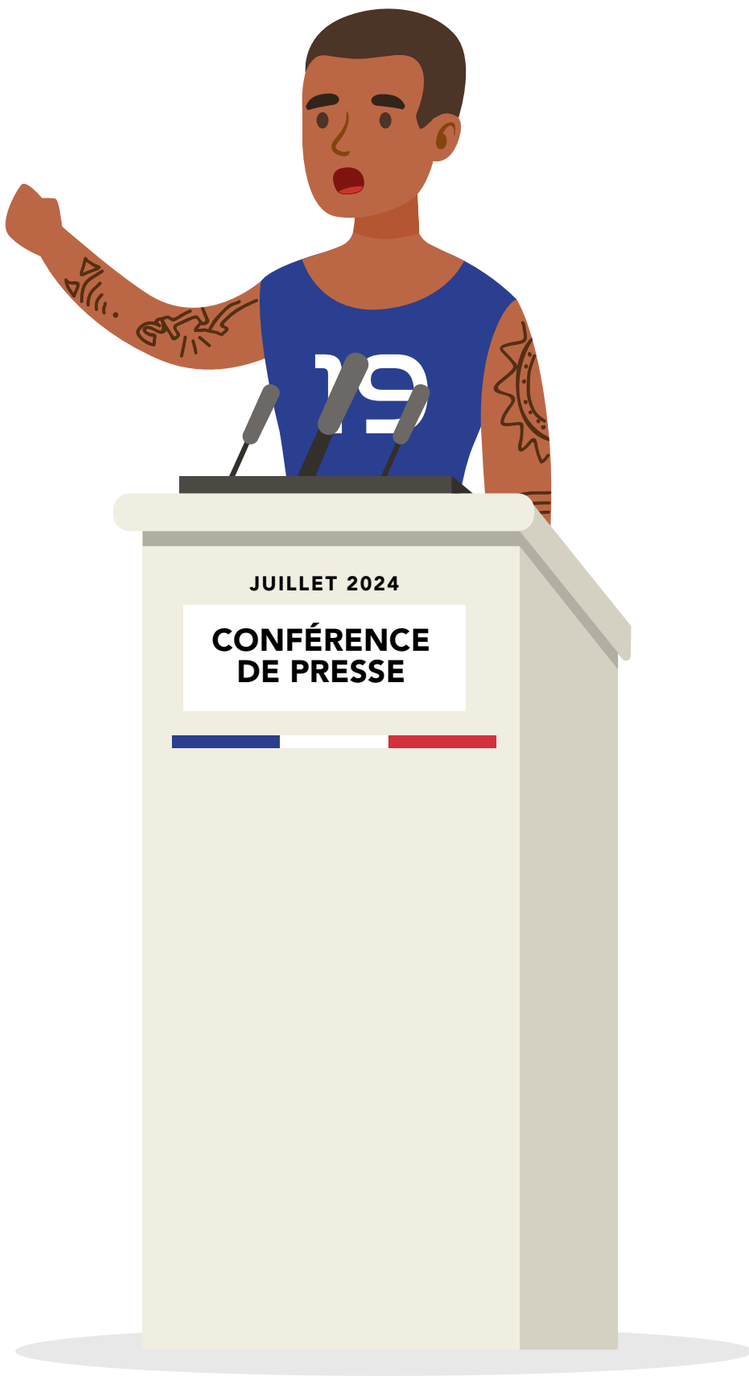
Attaques étatiques

“Les structures les plus critiques pour le succès de l’événement ont fait l’objet d’un encadrement spécifique de l’État et des entités organisatrices. Mais il ne faut pas négliger l’ensemble des autres entreprises, **en particulier celles dont la marque est fortement associée à notre pays**, qui seront certainement aussi la cible des attaques des hacktivistes qui viseront à entacher l’image du pays et créer du “bruit cyber”.”

Charlotte Couallier **CEO et co-fondatrice de Dattak**

“Les OIV sont sur le devant de la scène, elles sont les cibles prioritaires des cybercriminels. L’objectif des cybercriminels est **la déstabilisation de la France via le lancement d’attaques étatiques qui visent à affaiblir le pays sur l’échiquier mondial**, et montrer que la France n’est pas capable d’organiser un événement d’une telle envergure.”

Pierre-Antoine Failly-Crawford
Responsable de l’équipe de réponse à incidents chez Varonis



Cybercriminalité (grand public)

"Un scénario de risque sérieux serait une campagne de **deepfake vidéo démontrant que le POC du système de chronomètres a été piraté**, et que l'affichage des temps réalisés n'est pas fiable, décalé de quelques millisecondes pour chaque épreuve. Sans même lancer l'attaque sur le système, le discrédit serait total, jetant le doute sur la valeur même d'une médaille d'OR."

Marc Béhar **Fondateur PDG de XMCO**

"Des arnaques sont constatées à plusieurs niveaux, comme les **fausses billetteries mais aussi les faux emplacements de foodtrucks et stands proposés à la location** sur des sites olympiques moyennant le versement d'acomptes."

Antoine Pitaud **Expert cybersécurité chez Bitdefender**

Cybercriminalité (grand public)

"Attention à la désinformation, **au traitement médiatique des informations par les médias**".

Michel Van Den Berghe **Président du Campus Cyber**

"Les JOP de Paris sont un terrain de jeu pour les cybercriminels. Les auteurs potentiels de ces cyberattaques sont supposés être animés par des motivations d'enrichissement financier issus d'Etats ennemis. **Leur volonté première n'est autre que de déstabiliser la France, ses institutions et ses infrastructures**."

Ivan Rogissart **Sales Engineer Director, Southern Europe, chez Zscaler**

Entreprises

"À l'aube des Jeux Olympiques de 2024, des adresses de domaine imitant celles de Paris 2024 et liées à un site Web ressemblant à une agence de voyages ont été identifiées. Ce **site Web semble être utilisé pour attirer des victimes et extorquer de l'argent.**"

Colline Chavane **Analyste en menaces cyber chez Sekoia**

"Un **email de phishing usurpe actuellement l'identité de marque de la Région Île de France** et vise directement les collectivités locales au prétexte d'une "coordination efficace avec l'organisation des jeux olympiques de Paris 2024" et d'une mise à jour des protocoles de sécurité."

Romain Basset **Directeur des Services client chez Vade**

"On voit déjà un bon nombre d'attaques DDOS et il est désormais trop tard pour anticiper. **Nous conseillons de prendre une assurance pour la partie DDOS** et préparer un "rétro attaque" sur le même modèle qu'un rétro planning pour débloquer les choses rapidement en cas d'attaque."

Matthieu Dierick **Expert en cybersécurité chez F5**