PÃ©kin 2022 : une cible de choix pour les cybercriminels
Internet
PostÃ© par : JulieM
PubliÃ©e le : 11/2/2022 13:00:00

En raison de la pandÃ©mie de COVID-19, le nombre de spectateurs autorisÃ©s Ã assister aux Jeux dâ□□hiver de PÃ©kin a Ã©tÃ© restreint.Â

Les touristes Ã©trangers, habituellement prÃ©sents sur place lors de ces Ã©vÃ©nements, seront donc tributaires des rÃ©seaux sociaux et des services de streaming pour suivre les manifestations sportives.

Cette dÃ©pendance accrue Ã lâ□□Ã©gard des infrastructures numÃ©riques donne aux cybercriminels lâ□□occasion de perturber ces services en recourant Ã de nombreuses techniques, notamment les attaques par dÃ©ni de service distribuÃ© (DDoS) ou les attaques par ransomware.Â

Câ□□est pourquoi, le FBI a Ã©mis un avertissement, afin de sensibiliser au risque que les cybercriminels puissent prendre pour cible les Jeux dâ□□hiver de PÃ©kin.

Richard Hummel, ASERT Threat Intelligence Lead chez NETSCOUT estime que cette menace, pouvant affecter la diffusion en direct de cette manifestation sportive de portÃ©e mondiale par le biais dâ□□attaques DDoS, doit Ãªtre prise au sÃ©rieux et rappelle lâ□□importance pour toutes les Ã©quipes impliquÃ©es dans cet Ã©vÃ©nement de travailler ensemble afin de protÃ©ger les rÃ©seaux.

Â« Les Ã©vÃ©nements sportifs mondiaux, tels que les Jeux dâ□□hiver de PÃ©kin, ont toujours occupÃ© une place de choix sur la scÃ¨ne internationale, en mettant en valeur non seulement lâ□□excellence des athlÃ¨tes prÃ©sents, mais aussi le pays hÃ´te.Â

Toutefois, un Ã©vÃ©nement aussi mÃ©diatisÃ© sâ□□accompagne dâ□□un certain nombre de risques, parmi lesquels figure la cybersÃ©curitÃ©.

Ces manifestations modernes nÃ©cessitent en effet une infrastructure numÃ©rique de grande envergure, depuis les tÃ©lÃ©communications et la diffusion vidÃ©o, jusquâ□□Ã la notation, dÃ©sormais numÃ©rique des Ã©preuves, et les mÃ©dias sociaux.Â

Toutes ces activitÃ©s dÃ©pendent fortement de lâ□□accÃ¨s Ã internet. Câ□□est dâ□□autant plus vrai cette annÃ©e avec la limitation de spectateurs physiques Ã cette Ã©dition des Jeux dâ□□hiver, qui augmente ainsi la dÃ©pendance au numÃ©rique, faisant de lâ□□Ã©vÃ©nement sportif une cible de choix pour les cybercriminels.

Partant du constat que les rÃ©centes Ã©ditions des Jeux dâ□□Ã©tÃ©, il est important dâ□□en tirer des leÃ§ons pour 2022.Â

Les Jeux de Londres en 2012 avaient par exemple fait lâ□□objet dâ□□attaques DDoS rÃ©pÃ©tÃ©es et nourries, dont une menace dâ□□attaque de 40 minutes sur le systÃ¨me dâ□□alimentation du site central qui a nÃ©cessitÃ© lâ□□affectation une allocation dâ□□importantes ressources pour assurer le maintien des circuits Ã©lectriques.

Lâ□□objectif Ã©tait vraisemblablement de perturber la cÃ©rÃ©monie dâ□□ouverture. Les Jeux de

Rio de Janeiro en 2016 ont Ã©galement vu des organisations associÃ©es Ã lâ□□Ã©vÃ©nement visÃ©es par une attaque DDoS Ã grande Ã©chelle.

Tout au long de la pandÃ©mie, une augmentation des attaques DDoS ciblant les fournisseurs de services internet et des attaques qui perturbent la supply chain de la connectivitÃ© au sens large ont Ã©tÃ© constatÃ©es.

Il ne serait donc guÃ¨re surprenant que des attaques similaires se produisent lors de cette Ã©dition des Jeux de PÃ©kin, dans le but de causer un maximum de perturbations.Â

Par ailleurs, lâ□□un des principaux secteurs verticaux qui a vu des augmentations significatives du nombre dâ□□attaques est celui de lâ□□Ã©dition et de la diffusion sur Internet, qui regroupe un grand nombre de services de diffusion en continu et de solutions de vidÃ©oconfÃ©rence qui figureront sans aucun doute parmi les principaux outils utilisÃ©s lors des Jeux dâ□□hiver.

Câ□□est pourquoi, une Ã©troite collaboration entre les organisateurs et les Ã©quipes techniques est indispensable pour garantir le bon fonctionnement de cette nouvelle Ã©dition et des prochaines. Â»

Pour sâ□□en prÃ©munir et assurer le bon dÃ©roulement de cette nouvelle Ã©dition, lâ□□ensemble des parties impliquÃ©es dans lâ□□organisation de ces Jeux devront impÃ©rativement collaborer Ã©troitement avec les entreprises de tÃ©lÃ©communications et les fournisseurs de services Internet, souvent en premiÃ¨re ligne des cyberattaques Â».