La Fédération française de rugby visée par une cyberattaque et un chantage aux données volées

Le groupe de cybercriminels « Play » menace la FFR de dévoiler des informations confidentielles d'ici 5 jours si elle ne paye pas une rançon en échange de ces données.

La FFR a été prise pour cible par des hackers (illustration). LP/Icon Sport/Baptiste Fernandez

Par Romain Baheux avec D.LC

Le 22 juin 2023 à 13h11, modifié le 22 juin 2023 à 14h32

La Fédération française de rugby (FFR) est la cible d'une cyberattaque. Selon les informations de France Info, confirmées par Le Parisien-Aujourd'hui en France, l'instance basée à Marcoussis (Essonne) a été visée par le groupe de pirates informatiques Play. Celui-ci menace de dévoiler des informations confidentielles de la fédération, dirigée depuis une semaine par le nouveau président Florian Grill, si celle-ci n'accepte pas de négocier avec eux d'ici le 27 juin.
« La Fédération Française de Rugby a été la cible d'une attaque informatique durant la nuit du mercredi 7 juin au jeudi 8 juin 2023. Cette attaque a principalement affecté les serveurs de messagerie », explique la FFR dans un communiqué.

Les cybercriminels affirment être en possession de données personnelles d'employés ainsi que de personnes en lien avec la FFR, notamment des passeports. « En termes d'impact, la fédération a été dans l'impossibilité de récupérer les historiques des activités d'une partie des boîtes de messagerie qui ont été chiffrées lors de l'attaque, affirme la fédération. La FFR continue, en lien avec les autorités, à rechercher et analyser les données qui auraient pu être exfiltrées dans le cadre de cette attaque, y compris les e-mails, les contacts et les informations de calendrier. »

« Pas de demande de rançon » selon la FFR

Le groupe Play utilise un rançongiciel, ce qu'a confirmé la FFR, ou « ransomware » en anglais qui correspond à un logiciel malveillant qui vient chiffrer, rendre totalement illisibles, les données d'un ordinateur, d'un serveur ou d'un réseau d'une entreprise ou d'une collectivité locale. « Ils sont connus pour être assez brutaux dans leur demande de rançon alors que les groupes concurrents accompagnent plus leurs victimes pour les faire payer », pointe Maxime Cartan, fondateur de Citalid, une start-up experte en analyse de la menace.

Mais si la cible possède un moyen de restaurer ses sauvegardes et refuse de payer pour retrouver ses « datas », ils actionnent un deuxième levier : la menace de publier les données siphonnées ou de les revendre au plus offrant. « C'est un groupe cybercriminel avec une liste de victimes étendue et mondiale. La France va être particulièrement ciblée car elle accueille des événements sportifs retentissants, ce n'est pas un hasard que l'attaque ait été commise trois mois jour pour jour avant le début d'une compétition », met en avant cet ancien analyste de l'Agence nationale de la sécurité des systèmes d'information (Anssi).

« La FFR n'a pas reçu de demande de rançon à ce jour et ne souhaitera pas y répondre au cas échéant, souligne la fédération. Le service informatique a sécurisé l'ensemble du système et rétabli son fonctionnement. » La Commission nationale de l'informatique et des libertés (Cnil) a été avertie, tout comme la police.

Des institutions souvent ciblées

La fédération, occupée à préparer la Coupe du monde de rugby qui débute dans moins de trois mois en France (8 septembre - 28 octobre), n'est pas la seule à avoir été visée par une cyberattaque récemment. Le centre hospitalier universitaire (CHU) de Rennes a été victime d'une cyberattaque, mercredi dans la soirée. La direction de l'établissement a affirmé que l'offensive numérique n'avait pas eu de conséquences sur la prise en charge des patients.

Partout dans le pays, des organismes publics ou privés sont régulièrement visés par des cyberattaques. En Île-de-France, la prévention face à cette menace a été érigée en « priorité absolue ». Le comité d'organisation des Jeux olympiques 2024 de Paris a inauguré en avril un laboratoire d'experts pour lutter face à ces raids numériques.