

Piratage Fédération Française de Tir Où en est-on?

Les tireurs français s'inquiètent du piratage de leurs infos personnelles, pillées en octobre sur le site de la Fédération Française de Tir: quels sont les risques encourus? Et que faire?

Les faits remontent au matin du 20 octobre dernier, date à laquelle une faille de sécurité a été identifiée dans le système de gestion des licences de la Fédération Française de Tir à laquelle nous sommes tous obligatoirement affiliés. Des mesures de protection ont été rapidement mises en place, mais cette cyberattaque a conduit à la fuite des données personnelles des membres de la FFTir: numéro de licence, état civil, adresse postale, adresse électronique et numéro de téléphone. Aucune donnée personnelle de santé ou bancaire n'est concernée, selon la FFTir.

Les données concernant les armes détenues ou les râteliers numériques ne sont pas davantage concernées, puisqu'elles se situent ailleurs, sur le Système d'Information sur les Armes (SIA), système d'enregistrement des armes gouvernemental dont on espère qu'il a fait dans la foulée l'objet de mesures de protection renforcées, même si, par définition, le voleur a toujours un temps d'avance sur le gendarme.

À la suite à cet incident, la FFTir s'est appuyée sur une sauvegarde du samedi 18 octobre 2025 pour rétablir le service sur ITAC. Aussi, les créations et renouvellement de licence, ainsi que toutes demandes effectuées sur ces plateformes entre le 18 et le 20 octobre ont été à refaire. La première mesure de sécurité mise en place par la FFTir a consisté à invalider les QR codes des licences piratées qui venaient d'être renouvelées pour l'année 2025-2026. Les tireurs sportifs ont été priés de revenir sur EDEN pour télécharger à nouveau leur licence, frappée d'un nouveau QR code, et de mettre à jour leurs documents sur le SIA. Une procédure simple



Le 20 octobre dernier les informations stockées sous ITAC ont été piratées.

et rapide. Cette attaque s'inscrit dans un mouvement plus général qui a ciblé plusieurs fédérations sportives en 2025. Elle est due à l'exploitation d'une faille de sécurité chez le prestataire en charge des espaces licences. Prestataire auquel la FFTir pourrait légitimement demander des comptes, qui pourraient, par exemple, prendre la forme d'une ristourne ne serait-ce que symbolique sur le tarif de la prochaine licence.

Combien de tireurs sportifs seraient concernés?

Dans un premier temps, l'ensemble des tireurs actifs, à jour de leur licence semblaient concernés. Mais depuis peu on a vu apparaître sur le net des extraits de l'annonce, si tant est qu'elle est vraie, du pirate qui vend ces données sur le darknet. Contre la somme de 10000 € en bitcoins il propose de vendre plus d'un million de comptes piratés sur les serveurs d'ITAC/EDEN. Soit les tireurs actifs, mais aussi ceux qui ont été un temps, inscrits à la FFTir et qui ont arrêté de prendre leur licence.

Que dit la FFTir?

La FFTir travaille activement au renforcement de la sécurité de ses systèmes d'information. Elle doit lancer un audit complet de son infrastructure afin de renforcer sa capacité à lutter contre les cyberattaques. C'est bien le moins.

Sur le fond, elle est pieds et poings liés. Les autorités en charge de l'enquête, telles que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la brigade de lutte contre la cybercriminalité (BL2C), lui ont interdit de communiquer sur les éléments de cette affaire qui pourraient parasiter leurs investigations. Mais ce silence est mal perçu par certains tireurs sportifs qui n'en mesurent pas l'intérêt.

Que dit le ministère?

Le Service central des armes et explosifs (SCAE) s'est longtemps abstenu de tout commentaire. Mais il a finalement adressé une note à tous les tireurs sportifs inscrits au SIA et donc détenteurs d'armes de catégories B ou C.

Cette note confirme qu'aucune donnée contenue dans le SIA relative aux armes détenues n'est concernée par les éléments



Le hacker a piraté près d'un million de comptes, ceux de tireurs actifs, mais aussi ceux d'anciens licenciés.

L'UFA est rapidement intervenue pour proposer la mise en place d'une double authentification pour accéder au SIA.

qui ont corrompu ITAC et que les données personnelles qui pourraient être usurpées ne permettraient pas l'accès à un compte SIA. L'Union Française des amateurs d'Armes (UFA) était intervenue rapidement pour proposer une double identification pour autoriser l'accès au SIA d'un tireur enregistré. En conséquence, le SCAE a fait savoir par le biais de cette note que les tireurs doivent être attentifs aux messages que le SIA pourrait leur adresser. Une demande de validation leur sera envoyée si une modification de leurs informations personnelles venait à être engagée. Il conviendrait alors de la refuser si la modification n'était pas de leur fait.

Une presse surmotivée

Cette situation, qui préoccupe les tireurs sportifs de façon légitime, est d'autant plus anxiogène que la presse

quotidienne, d'ordinaire mois diserte sur le sujet, en parle ici à qui mieux mieux. Écrite, électronique ou télévisuelle, la presse cite moult exemples de tentatives de cambriolage imputées à des malfaiteurs renseignés grâce au piratage.

Des cambriolages opportunistes chez des détenteurs d'armes, il y en a autant que dans le reste de la population et depuis ce piratage informatique les statistiques des vols ne se sont pas envolées. Il faut rester calme, vigilant et ne pas céder à la paranoïa. Et ne pas oublier que les cambrioleurs amateurs réfléchiront sans doute à deux fois avant de s'attaquer au domicile d'un détenteur légal d'armes.

Une situation dans le flou

Au premier regard, il semblait clair que cette fuite de données pouvait préparer des campagnes de phishing comme on en subit régulièrement depuis des années. Mais l'apparition de copies d'écran de l'annonce du hacker sur le darknet a changé la donne.

Ce message en forme d'annonce propose de vendre en bloc ou à la pièce les données de tireurs enregistrés sur les serveurs d'ITAC.

Il s'agit d'une annonce dont il est difficile de connaître la véracité. S'agit-il du pirate ou d'un usurpateur qui profite de la situation pour vendre des données qu'il n'a pas. Seule l'enquête pourra nous le dire un jour.

En attendant, les coordonnées person-

nelles de tous les licenciés sont dans la nature, et il n'est pas besoin d'être Arsène Lupin pour supposer qu'à toutes ces adresses, des armes et des munitions sont susceptibles d'être trouvées par un monte-en-l'air.

Des tireurs en colère

Si la plupart des licenciés observent patiemment la suite des événements, d'autres ne cachent pas leur mécontentement. Certains ont lancé une pétition contre la FFTir, mais elle n'a rassemblé que quelques dizaines de signatures. D'autres argumentent directement avec raison et pointent du doigt des faiblesses de sécurité connues de longue date que l'on retrouve d'ailleurs dans le SIA, en particulier l'absence de double authentification (MFA).

L'UFA a rappelé récemment, en réponse à de nombreuses demandes dirigées contre la FFTir, que sur le plan strictement juridique, un arrêt de la Cour de Justice Européenne (CJE) daté du 4 mai 2023 précise que pour obtenir réparation, en cas de fuite de données ou de violation du RGPD, la personne concernée doit justifier du préjudice subi.

Ce préjudice doit être la conséquence de la fuite de données. On ne peut donc pas légalement engager d'action préventive sur l'unique supposition, aussi vraisemblable soit elle, que des données pourraient être utilisées à des fins délictueuses.



Langoisse de tout licencié. Se faire ouvrir son armoire forte par une personne malveillante qui aurait récupéré ses données.

En cas d'appel d'individus censés représenter la force publique, demandez identité, grade, service et coordonnées téléphoniques.

Que faire en cas d'appels ou de visites douteuses ?

En cas d'appel d'individus prétendant représenter la force publique, avant toutes choses demandez l'identité, le grade, le service et les coordonnées téléphoniques de la personne qui appelle et faites-lui savoir que vous allez procéder à un appel de contrôle. Il est effectivement possible que de vrais policiers ou des gendarmes cherchent à vous joindre dans le cadre de procédures de demandes d'autorisation d'acquisition d'arme de catégorie B.

Si quelqu'un se présente directement à votre domicile, n'ouvrez pas, demandez les coordonnées de son service pour confirmation et, en cas de doute, composez le 17. Les données qui ont fuité pourraient aussi être utilisées pour des tentatives d'hameçonnage, de phishing, soyez donc particulièrement vigilants aux mails, aux SMS, et aux appels que vous recevez, notamment s'ils vous demandent de fournir des données personnelles ou des informations bancaires et n'ouvrez jamais les fichiers joints dont vous ne connaissez pas la provenance.

Les armuriers qui pratiquent la vente par correspondance sont informés de leur côté qu'ils doivent redoubler de prudence face aux usurpations d'identité qui risquent de se multiplier. ♦

Jean-Pierre Bastié

ENTRETIEN EXCLUSIF!

Un spécialiste de la chasse aux cybercriminels au ministère de l'Intérieur répond à nos questions. Cet expert du Comcyber-MI* qui préfère garder l'anonymat livre un constat inquiétant.

Commençons par les chiffres...

« En cinq ans, la cybercriminalité a progressé de 100 %, et elle continue à croître. Cette progression englobe une cybercriminalité organisée, de plus en plus présente et de plus en plus inventive, et des individus qui sévissent à petite échelle, sur les sites de vente, par exemple. La cybercriminalité organisée pratique aujourd'hui ce que l'on pourrait appeler du taylorisme du crime. Les tâches sont parcellisées, industrialisées, répétées, avec des échanges commerciaux très intenses de bases de données et d'infos sur des forums cybercriminels, ou des messageries chiffrées comme Telegram. Un écosystème économique illicite en pleine croissance.

Que faire face à ce constat ?

La première réponse consistera à investiguer sur le fonctionnement de la cyberattaque pour en comprendre le mécanisme précis et tenter de localiser et d'identifier ses auteurs. Dans la foulée, nous agissons par anticipation pour éviter les cyberattaques et les escroqueries. Malheureusement, les cybercriminels ont souvent l'avantage de l'initiative. Ils sont nombreux, plus nombreux que ceux qui s'efforcent de les empêcher de nuire. Et contrairement à nous, ils sont transnationaux. Les poursuites transnationales sont soumises à un encadrement juridique strict qui complexifie l'entrave des malfaiteurs. Nous travaillons avec et par l'intermédiaire de procureurs, et toute cette coopération doit se mettre en place. Si ça se passe très bien en Europe avec Euro-pol, dans certains pays non coopératifs, c'est une toute autre affaire. Or, en face, ce sont plusieurs millions de cybercriminels auxquels nous sommes confrontés. Nous constatons aussi une imbrication croissante entre criminalité traditionnelle et cybercriminalité, la seconde faisant profiter la première de ses technologies. C'est vrai dans le domaine des armes, et plus encore dans celui des stupéfiants. La cybercriminalité représente en 2024, près de 400 000 dépôts de plaintes. Mais 400 000 plaintes ne veut pas dire 400 000 infractions, mais plusieurs millions, car bien des citoyens ne déposent pas plainte. C'est pourquoi ont été créées les plateformes de signalement ou de plainte



“En cinq ans, la cybercriminalité a progressé de 100 %”

en ligne Perceval, Pharos ou encore Thésée. Elles ne permettent pas hélas de poursuivre tout le monde, de repérer rapidement les criminels organisés qui procèdent à des campagnes massives d'escroqueries modestes, et font leur chiffre sur le nombre.

Combien d'agents combattent la cybercriminalité en France ?

Plus d'une dizaine de milliers, si l'on compte tous les policiers et gendarmes qui ont reçu une formation de base sur le sujet. À un niveau plus spécialisé, plus technique et plus pointu concernant les enquêtes judiciaires, il existe quatre pôles spécialisés, police (OFAC), gendarmerie (UNCyber), préfecture de police de Paris (BL2C) et DGSI, qui opèrent en coordination.

Piratage de la FFTir: loin d'être un cas isolé

Selon le dernier rapport annuel du ministère de l'Intérieur sur ce sujet, ce sont plus de 17 000 attaques contre des systèmes d'information qui ont été enregistrées en 2024 en France. En tout, 348 000 attaques numériques ont été relevées en 2024, dont 230 000 fraudes à la carte bleue, 222 000 cas de contenus illicites, 107 000 plaintes pour escroquerie via internet. Dans la lutte contre ces infractions, 60 000 personnes ont été identifiées et mises en cause.

Engagez-vous des hackers repentis, comme au cinéma ?

Nous engageons des techniciens chevronnés. Et il peut arriver, mais sous contrôle judiciaire précis et avec des agents ayant reçu l'habilitation, que des enquêteurs procèdent, par exemple, à des achats de produits illicites pour identifier des cybercriminels et les interpeller.

Que conseillez-vous au citoyen ?

De s'informer sur la cybersécurité, par exemple en suivant une formation gratuite en ligne Secnum Académie de l'ANSSI, de se méfier des appels téléphoniques cherchant à se faire passer pour votre banque ou un fournisseur d'énergie, de ne pas cliquer sur des pièces jointes ou liens malveillants d'expéditeurs inconnus, de ne pas télécharger de fichiers piratés potentiellement vérolés (films, logiciels, etc...). Malheureusement, l'intelligence artificielle est également utilisée par les cybercriminels. Les courriels et SMS truffés de fautes d'orthographe et donc assez facilement identifiables partiront de plus en plus au passé. Les attaques seront de plus en plus sophistiquées, de plus en plus crédibles.

Depuis décembre 2024, il existe également le service 17cyber.gouv.fr qui est une plateforme en ligne, équivalente numérique de l'appel 17. Le 17Cyber est destiné à toutes les victimes d'infractions numériques : particuliers, entreprises et collectivités. Fruit d'un travail collectif entre Cybermalveillance.gouv.fr, la police et la gendarmerie, le 17Cyber permet aux victimes de bénéficier d'un parcours adapté en fonction du type d'attaque informatique, de leur prodiguer des recommandations, de les orienter vers un téléservice et, ou encore d'être accompagné par tchat par la police ou la gendarmerie.

Propos recueillis par Marc Schlicklin

*Comcyber-MI: le commandement du ministère de l'Intérieur dans le cyberspace, COMCYBER-MI, coordonne tous les services du ministère de l'Intérieur traitant de la lutte contre les cybermenaces. Il assure la cohérence, la performance et la lisibilité du dispositif global du ministère face aux cybermenaces.



Le ministère de l'Intérieur s'est d'abord abstenu de tout commentaire. Mais le SCAE a finalement publié une note confirmant que le SIA n'avait pas été piraté.