



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Date : 23 septembre 2026

N° 3033/ANSSI/SDO/NP

Nombre de pages : 20

Rapport d'incident – Septembre 2026

Actes malveillants observés sur le système d'information de la
Direction générale des Finances publiques entre mai 2026 et
août 2026

TLP:CLEAR

AVERTISSEMENT

UTILISATION DU RAPPORT

L'objectif de ce document public est une présentation de la chronologie des activités illégitimes ayant été observées sur les systèmes d'information de la direction générale des finances publiques (DGFIP) entre mai 2026 et août 2026, ainsi que l'identification de mesures qui auraient pu permettre la détection et/ou la prévention de ces actes.

Toute utilisation totale ou partielle du présent rapport à d'autres fins que son but de sécurité et de transparence est proscrite.

COMPOSITION DU RAPPORT

Une synthèse exécutive est proposée en première partie.

Les enseignements, l'analyse des défaillances observées font l'objet de la seconde partie.

Le troisième chapitre tire les conclusions de cette analyse et présente les actions de remédiation devant être implémentées pour assurer que le même chemin de compromission ne puisse plus être exploité.

La description détaillée des événements et des mesures d'endiguement réactives qui ont été prises par la DGFIP sont exposées en annexe de ce rapport.

Sauf précision contraire, les heures figurant dans ce rapport sont exprimées en UTC+2.

Afin de garantir la sécurité des personnes, le document a été anonymisé et les informations sensibles ont été masqués en vue de la diffusion publique de cette version.

Table des matières

1. Synthèse exécutive	4
2. Enseignements.....	6
2.1. Compromission de comptes	6
2.2. Détection des comportements.....	7
2.3. Filtrage et segmentation réseau.....	8
2.4. Supervision ANSSI.....	8
2.5. Coordination interministérielle.....	8
3. Mesures de remédiation	10
Glossaire des acronymes.....	13
Annexes	15
Annexe 1 : Chronologie des évènements.....	15

1. Synthèse exécutive

Le 12 août 2026 à 13h50, l'acteur Zerobytes revendique sur un forum en ligne, le vol de données appartenant à la plateforme impots.gouv.fr, sous la responsabilité de la Direction générale des Finances publiques (DGFIP). L'ANSSI notifie l'entité le même jour à 16h32. Le 13 août au matin, Zerobytes publie le détail des données volées, qui concernent près de 353 000 particuliers et 252 000 professionnels, obtenues à partir d'un outil de gestion de la relation avec les usagers de la DGFIP.

Les investigations montreront, par la suite, que l'exfiltration s'est produite sept semaines auparavant, et qu'elle a été précédée de plusieurs semaines d'exploration sur des applicatifs de la DGFIP, entre autres, initiée depuis le Réseau Interministériel de l'État (RIE). Les accès de l'attaquant lui ont été possibles grâce au vol, sur une période de trois mois, de plusieurs dizaines d'authentifiants appartenant à des agents légitimes de la DGFIP, probablement compromis *via* des logiciels espions (de type *infostealers*) sur des ordinateurs non administrés par la DGFIP, et à la compromission d'un autre ministère ayant donné accès au RIE à l'attaquant.

Le 13 août 2026, une nouvelle revendication du même acteur est publiée concernant les données cadastrales détenues par la DGFIP. Les investigations de la DGFIP mettront en évidence que la compromission du poste d'un géomètre-expert au sein d'un cabinet privé a permis de contourner la double authentification par messagerie, puis l'accès et l'exfiltration des données entre le 27 juillet 2026 et le 8 août 2026.

Finalement, aucune de ces exfiltrations n'a été détectée, ni par les moyens de supervision de la DGFIP ni par ceux de l'ANSSI, révélant certaines lacunes dans la supervision des systèmes d'information (SI) de la DGFIP.

Les mesures d'endiguement prises immédiatement, notamment les coupures des accès agents et partenaires au portail ayant permis ces exfiltrations, ont entraîné des impacts significatifs sur des services de la DGFIP et d'entités partenaires.

La compromission des SI de la DGFIP n'est pas la conséquence d'une attaque sophistiquée, mais de l'exploitation de faiblesses dans trois domaines :

- **L'identité** : la fuite d'identifiants de connexion fréquente et consécutive à l'utilisation d'appareils personnels, couplée à l'absence d'authentification forte sur deux portails dont l'un donnant accès à des ressources sensibles sur le RIE, offre une chaîne d'exploitation triviale aux attaquants ; le filet de sécurité mis en place par la DGFIP que représente la veille sur les compromissions de comptes a démontré son intérêt mais ne permet pas, à lui seul, de réduire suffisamment le risque (délai de traitement, non-exhaustif).
- **L'architecture** : des applications sensibles [REDACTED] sont accessibles depuis le RIE sans cloisonnement, augmentant leur exposition et ouvrant un

risque de latéralisation depuis des ressources d'organismes tiers (comme cela a été le cas depuis le ministère de l'Éducation nationale).

- **La détection** : Pendant l'incident, le SOC de la DGFIP ne supervisait pas le portail ADER, utilisé par l'attaquant pour exfiltrer les informations E-Contact ; aucun mécanisme n'a corrélé les signaux suspects (connexions nocturnes, volumes anormaux, adresses IP malveillantes, *scraping* industriel). Les solutions de détection au niveau applicatif doivent être améliorées pour mieux identifier les accès suspects. [REDACTED]

[REDACTED]
[REDACTED] En l'absence de règles spécifiques à cette menace, elle n'a pas été en mesure de voir ces comportements suspects.

Un plan d'action prenant en compte les défaillances exploitées a été défini pour la DGFIP. Celui-ci couvre notamment les axes suivants :

- Renforcer la supervision de la DGFIP et élargissement de la couverture à l'ensemble des applications métier ;
- Limiter l'exposition des identifiants de connexion et implémentation de l'authentification forte ;
- Réduire la surface d'attaque et l'exposition des ressources métiers sur les réseaux tiers incluant la mise en place de seuils applicatifs sur les données pouvant être accédées.

Ces chantiers ne pourront aboutir qu'avec un appui de toute la chaîne métier en charge des différents applicatifs, de la hiérarchie du ministère de l'action et des comptes publics et de l'interministériel. Ces chantiers peuvent utilement alimenter le plan d'action permettant de décliner opérationnellement la feuille de route de sécurité numérique de l'État

2. Enseignements

2.1. Compromission de comptes

Au vu de la chronologie des évènements sur la période (cf. annexe 1), le premier élément notable est le volume de comptes pour lesquels l'attaquant dispose de couples identifiant/mot de passe. Aucune tentative d'attaque par force brute ou *credential stuffing* n'a été identifiée, ce qui signifie que l'attaquant disposait de mots de passe pour ces comptes (pouvant être valides ou expirés).

Si les traces montrent que le SOC de la DGFIP procède à la réinitialisation des mots de passe lorsqu'il détecte des compromissions ou que son prestataire lui en notifie, cette situation présente des risques et des faiblesses :

- A partir d'un vol d'identifiants de connexions, l'attaquant a été en mesure de se connecter à distance à des applicatifs de la DGFIP exposés à des tiers et d'accéder à un large volume de données sensibles. Cela est contraire aux principes de résilience et de défense en profondeur.
- La veille effectuée par le prestataire de la DGFIP ne peut vraisemblablement couvrir toutes les plateformes de revente. Aussi, il est à prévoir que des comptes compromis ne soient pas identifiés et donc pas remontés au SOC de la DGFIP. Néanmoins, cette veille est une boucle de rattrapage pertinente.
- La chronologie partagée par la DGFIP montre qu'il existe une période de temps difficilement compressible entre la compromission des comptes et la réinitialisation des mots de passe par le SOC. Cette fenêtre de temps est suffisante pour qu'un attaquant accède à un applicatif métier et débute une exfiltration.
- Des investigations plus larges doivent impérativement être faites à chaque fois qu'un compte est compromis afin d'identifier d'éventuels accès illégitimes sur la période d'exposition. Compte tenu du volume de comptes compromis, l'analyse systématique des activités par le SOC de la DGFIP est très chronophage et ne peut être assurée de manière exhaustive. Les sessions attaquantes du 23 juin et 24 juin 2026 montrent une limite du périmètre supervisé à cette date : le mot de passe du compte utilisé a été réinitialisé et les accès PIGP contrôlés mais l'exfiltration opérée via le RIE n'a pas été identifiée.
- Il est supposé que la compromission d'un tel volume de comptes provienne de l'utilisation d'appareils non administrés par la DGFIP pour accéder aux ressources métiers (notamment des appareils personnels pour les identifiants permettant l'accès au portail ADER ou ceux d'organismes tiers pour les identifiants permettant l'accès au portail APEX). La réinitialisation des mots de passe suite à la compromission de ces comptes ne peut être efficace que si l'appareil sur lequel le compte a été compromis est également nettoyé (ce qui

ne peut être garanti sur l'ensemble des équipements notamment lorsqu'il s'agit d'organisations externes).

Par ailleurs, l'absence d'authentification multifacteur, en particulier sur le périmètre PIGP (pour les comptes d'agents DGFIP), et ADER permet la réutilisation immédiate des identifiants compromis par les attaquants, sans mesure palliative efficace. De même, le cas de l'exfiltration via le portail APEX à partir de la compromission de l'ordinateur d'un géomètre-expert montre que les solutions d'authentification multifacteur implémentées (OTP envoyé par email) sont insuffisantes.

2.2. Détection des comportements

Les sessions d'exfiltration menées par l'attaquant n'ont pas été détectées en temps réel par les mécanismes de contrôle implémentés sur les applicatifs métiers ni sur les équipements de sécurité de la DGFIP. Certains paramètres sont communément utilisés pour détecter un comportement suspect dans une connexion réseau :

- La volumétrie d'informations échangées lors des connexions (11Go entre le 22 et 25 juin, 3Go entre le 21 et 23 juillet) n'a pas levé d'alerte.
- Le nombre de requêtes par utilisateur sur une plage temporelle n'est pas considéré : la technique de *scraping* utilisée par les attaquants impose de devoir initier autant de requêtes que de pages accédées. Au vu du nombre de fiches accédées, le volume de requêtes associées a dû être important. Des mécanismes de *rate-limiting* sont généralement utilisés pour bloquer un nombre trop important de requêtes ou même prévenir d'une tentative d'attaque par force brute.
- Les adresses IP des connexions initiées ne sont pas analysées (connexions depuis des adresses de VPN, depuis des adresses localisées en Inde et pour plusieurs catégorisées comme malveillantes). Par ailleurs, certaines adresses IP ont été utilisées pour se connecter à des comptes connus comme compromis à plusieurs semaines d'intervalles. L'association d'une adresse IP avec un compte compromis peut être utile pour rehausser le caractère suspect d'un comportement.
- Les heures de connexion des utilisateurs ne sont pas interprétées (connexions nocturnes identifiées).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Ces paramètres pris individuellement ne permettent généralement pas d'identifier des comportements suspects sans générer d'importants volumes de faux positifs, néanmoins la corrélation de plusieurs d'entre eux aurait pu permettre de lever des alertes.

L'absence de supervision sur le portail ADER ne permet pas de corréliser des activités malveillantes avec le reste du SI ou en provenance du RIE suite à un signalement d'un autre ministère. Le déploiement de la supervision [REDACTED] doit être accéléré afin de donner de la visibilité au SOC de la DGFIP.

La gestion des droits utilisateurs sur les applicatifs internes n'a pas été étudiée pour la rédaction de ce rapport, néanmoins, les sessions d'exfiltration orchestrées à partir de comptes non-privilegiés mettent en évidence que ces comptes avaient accès à un volume important de données. Ce point pourra être potentiellement adressé lors de l'audit organisationnel de la phase 2.

2.3. Filtrage et segmentation réseau

Plusieurs accès illégitimes identifiés proviennent du RIE [REDACTED], à partir de localisations n'ayant pas de besoins apparents d'accéder à des infrastructures de la DGFIP. La segmentation réseau, qui permet de restreindre l'accès aux seules populations et zones logiques qui en ont le besoin, apparaît alors comme trop permissive. Un filtrage plus fin des accès réseau entre ministères et au sein du RIE doit également être engagé [REDACTED].

2.4. Supervision ANSSI

La supervision de l'ANSSI n'a pas permis de détecter les activités des attaquants pour plusieurs raisons :

- L'ANSSI ne dispose pas de supervision applicative sur ce périmètre. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED];
- Les acteurs malveillants utilisaient des comptes légitimes pour accéder aux applications et la supervision réseau de l'Agence n'a pas permis de les voir ;

Cependant, le volume cumulé de requêtes que l'attaquant a dû générer pour orchestrer l'exfiltration de donnée aurait dû déclencher des alertes.

2.5. Coordination interministérielle

La chronologie des événements fait état de l'usage par l'attaquant du RIE afin d'accéder au portail ADER de la DGFIP. L'utilisation du RIE lui a été rendue possible à cause de la compromission d'infrastructures appartenant au ministère de l'Éducation nationale elles-mêmes raccordées au RIE.

A la date de la première vague d'exfiltration depuis le portail ADER, le ministère de l'Éducation nationale mène d'ores et déjà, conjointement avec l'ANSSI, une réponse

à incident sur son périmètre. Des traces de tentative de latéralisation sur d'autres organisations de l'État disposant d'un accès au RIE, en nombre, ont alors été identifiées.

Sans qu'il soit possible de retracer avec précision les dates d'extraction des marqueurs techniques et des victimes potentielles, il est raisonnable de préciser que le délai d'analyse de ces marqueurs et leur partage auprès des organismes connectés au RIE aurait dû être réduit à son minimum afin d'éviter un risque de latéralisation. De manière complémentaire, des mesures de blocage de flux au niveau du RIE auraient pu limiter les possibilités d'exfiltration, mais une cartographie plus fine des flux légitimes au sein du RIE est un prérequis à l'opérationnalisation de telles mesures.

3. Mesures de remédiation

Afin d'assurer que le même chemin de compromission ne puisse être emprunté de nouveau, par le même acteur ou un nouveau, un ensemble de mesures correctrices doit être considéré. Il est important de mentionner que seul un audit complet (déjà prévu suite à cet incident) sur le SI ou les applications concernées par l'incident permettra d'identifier avec exhaustivité les vulnérabilités exploitables. Ainsi, les recommandations à suivre ne se limitent pas à la chaîne de compromission constatée mais peuvent aussi traiter d'autres faiblesses constatées.

Restrictions d'accès aux ressources métiers :

- Les applicatifs métiers doivent faire l'objet d'une politique d'accès plus stricte et clairement définie :
 - Applications à usage interne : elles ne doivent être accessibles que depuis des postes administrés par la DGFIP. Dans ce cas, l'accès à l'application ne doit pas être possible depuis Internet, sauf à travers un VPN dédié aux agents de la DGFIP.
 - Applications à usage externe limité : leur accès ne doit pas être librement possible directement depuis Internet. Il ne devrait être possible de se connecter à l'application que depuis les réseaux internes ou depuis un VPN (site à-site ou point-à-site) pour les partenaires. Une limitation à une liste d'adresses IP sources autorisées est envisageable si les solutions de VPN n'ont pas pu être mises en place. Ce contrôle moindre sur les sources de connexion doit être compensé par des mesures rigoureuses sur les limitations métier dans l'application et sur les mécanismes d'authentification (authentification multifacteur notamment).
 - Applications à usage public : l'accès depuis tout Internet à une application rend difficile la diminution du risque par le contrôle de la source. Des mesures de réduction d'exposition sont tout de même possibles : filtrage sur la base de la source de connexion (géo-filtrage), ou de listes d'interdiction (adresses IP mal réputées, catégories IP non légitimes, etc.). Si bloquer sur le critère de source de connexion n'est pas possible, ce devrait être, au moins, un critère d'alerte pour la supervision. La robustesse de l'authentification doit être d'autant plus renforcée que ces applications sont exposées.
- Plus généralement, les applicatifs doivent systématiquement être mis en supervision dans un SIEM, et des mesures de restriction doivent être appliquées :
 - Application de quotas ; en volume de ressources métiers accédées, en nombre de requêtes ou en volume de données échangées sur une période donnée.

- Protection contre les attaques par injection, à partir de la détection de motifs caractéristiques
- Application de mesures de blocages basées sur la géolocalisation IP (GeoIP) et la réputation IP.

Protection contre les vols d'identifiants :

- L'usage d'appareils personnels pour accéder à des ressources professionnelles doit être proscrit.
- Les appareils professionnels doivent être durcis et suivre les bonnes pratiques de sécurité (application des mises à jour mensuelles, déploiement d'un EDR, Antivirus, VPN *always-on*, etc.).
- Les mots de passe des utilisateurs doivent respecter les bonnes pratiques de sécurité (règles de complexité, etc.).
- L'authentification multifacteur doit être déployée sur tous les applicatifs. Le second facteur doit être résistant à la compromission du premier facteur (par exemple, un one-time password (OTP) distribué par email ne sera pas un choix raisonnable si l'accès à la messagerie est possible à partir d'un unique couple identifiant/mot de passe). Ainsi, on privilégiera des solutions de second facteur à l'état de l'art tels que les *tokens* physiques ou les applications d'authentification. On privilégiera également la livraison du second facteur sur un appareil différent de celui utilisé pour le premier facteur afin de couvrir le risque de compromission de l'équipement (voir mécanismes d'authentification forte dans les exigences fournies par l'ANSSI)
- La sensibilisation des utilisateurs doit être accentuée à plusieurs niveaux :
 - La séparation des usages professionnels et personnels doit être contrainte techniquement et encouragée afin d'assurer que les identifiants professionnels ne sont pas compromis à partir d'environnements non-administrés par la DGFIP ;
 - A la réception d'une notification de compromission de compte, une action de sensibilisation aux bonnes pratiques d'usage des appareils et accès professionnels doit être réalisée auprès de l'agent concerné, conformément à la pratique actuelle.
- Les droits applicatifs des utilisateurs doivent faire l'objet d'une gestion fine, afin d'assurer que chacun d'entre eux ne puisse accéder qu'aux informations dont il doit avoir connaissance pour assurer sa fonction. Des plafonds de consultation des ressources métiers doivent également être implémentés pour limiter l'impact d'un accès illégitime.

Processus de réinitialisation :

- A la réception d'une notification de compromission de compte, la réinitialisation des mots de passe doit s'accompagner d'une analyse de l'activité du compte depuis la date supposée de compromission. Une

cartographie fidèle du système d'information facilitera l'identification des applicatifs exposés.

- En cas de compromission répétée du même compte, une étude approfondie doit permettre d'identifier la cause racine.
- La réinitialisation des mots de passe doit s'accompagner de la révocation des sessions actives sur tous les applicatifs et portails accessibles.
- Afin de renforcer la levée d'alerte suite à des recherches suspectes sur les applicatifs (qui a généré des vrais positifs sur E-Contact comme décrit dans la timeline), la possibilité de déclencher le blocage automatique des comptes pourrait être étudiée.

Glossaire des acronymes

- **ADER**
Portail d'accès à certaines applications de la DGFIP au travers du RIE.
- **APEX**
Ce portail est une solution d'accès à des applicatifs externes de la DGFIP à destination de partenaires, notamment les notaires et les géomètre-experts. Il est accessible à partir d'un couple identifiant/mot de passe et d'un second facteur d'authentification qui est un OTP envoyé par email.
- **ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)**
- **Compte-dgfip-**
Les noms des comptes compromis par infostealer sont anonymisés dans la chronologie selon cette dénomination. Les comptes dénommés « compte-dgfip-X » sont des comptes internes des agents de la DGFIP, les comptes dénommés « compte-dgfip-xt-XX » sont des comptes d'agents externes à la DGFIP ayant des accès aux applicatifs de la DGFIP dans le cadre de leur besoin métier.
- **Credential stuffing (bourrage d'identifiant)**
Consiste à réaliser, à l'aide de logiciels ou de façon manuelle, des tentatives d'authentification massives sur des sites et services web à partir de couples identifiants/mots de passe (généralement, une adresse électronique et un mot de passe).
- **CSIRT (Computer Security Incident Response Team)**
Équipe de Réponse aux Incidents de Sécurité Informatique. Il s'agit d'une unité spécialisée dans la gestion et la réponse aux incidents de cybersécurité.
- **DGFIP (Direction générale des Finances Publiques)**
- **E-Contact**
Application de messagerie pour les échanges avec les usagers.
- **EDR (Endpoint Detection and Response)**
Logiciel de sécurité informatique qui surveille en continu les terminaux d'un réseau (ordinateurs, serveurs, mobiles) pour détecter et bloquer les cybermenaces.
- **Infostealer**
Logiciel malveillant conçu pour voler de manière discrète des données des appareils qu'il infecte.
- **OTP (One-Time Password)**

- **PIGP : Portail internet de la gestion publique**

Le PIGP permet aux ordonnateurs, aux comptables des collectivités territoriales et des établissements publics d'accéder à certains services fournis par la DGFIP. Il permettait également aux agents de la DGFIP d'accéder à leur messagerie via un webmail et à des services RH.

- **RIE (Réseau Interministériel de l'État)**

- **Scraping**

Extraction automatique de données sur une application web à l'aide d'un programme informatique.

- **SPDC (Serveur Professionnel de Données Cadastrales)**

- **SIEM (Security Information and Event Management)**

Solution de gestion des informations et des événements de sécurité

- **SOC (Security Operation Center)**

Désigne une équipe centralisée ou une structure dédiée à la surveillance, la détection, l'analyse et la réponse aux incidents de cybersécurité d'une organisation.

- **VPN (Virtual Private Network)**

Annexes

Annexe 1 : Chronologie des évènements

Sources considérées

Grâce aux investigations numériques menées majoritairement par la DGFIP et par l'ANSSI, la chronologie des évènements a pu être déterminée.

Les éléments ayant permis de la reconstituer sont les suivants :

- Les documents issus des analyses de la DGFIP (main courante, chronologie des évènements) ;
- Des journaux d'évènements de la DGFIP ;
- Les notifications de Recorded Future, le prestataire de veille sur les menaces de la DGFIP ;
- Les journaux de flux réseaux ADER/Odin obtenus par le ministère de l'Education nationale ;
- Les publications de FrenchBreaches / Zerobytes (OSINT/CTI).

Il convient de préciser que la DGFIP a complété depuis plusieurs années son dispositif de veille de compromission et revente d'accès de ses utilisateurs auprès des sources de renseignements externes. Ainsi, lorsqu'une compromission d'un compte de son périmètre est détectée ou lui est notifiée (*source : RecordedFuture, Orange Cyber Défense*), le SOC DGFIP procède à la réinitialisation du mot de passe de ce compte (*source : RecordedFuture*), à une recherche d'actions concomitantes et à une sensibilisation de l'intéressé et de son encadrement.

En raison de la diversité des sources, des écarts temporels peuvent apparaître entre celles-ci.

Incident sur l'application E-Contact

- **Premières activités suspectes (mai et juin 2026)**

Entre le **2 et le 8 mai 2026**, plusieurs connexions sur le portail internet de la gestion publique (PIGP) sont enregistrées avec le même compte *compte-dgfip-1*¹ depuis 3 localisations distinctes. Ces connexions sont suspectes car elles sont initiées depuis des adresses IP catégorisées comme malveillantes, géolocalisées en France et en Inde.

Le **7 mai 2026**, le même compte s'authentifie également sur l'application E-Contact à travers le portail ADER. Le mot de passe du compte *compte-dgfip-1* est réinitialisé plus tard ce jour-là, dans le cadre d'un autre incident suivi par la DGFIP (*source : DGFIP*).

Entre le **22 mai et le 3 juin**, plusieurs tentatives de connexions suspectes (adresses IP catégorisées malveillantes ultérieurement) sur le PIGP sont journalisées sans lever

¹ Tous les noms des comptes ont été anonymisés.

d'alerte. Sur cette période, 3 comptes *compte-dgfip-2*, *compte-dgfip-3*, *compte-dgfip-4* ont été utilisés :

- **13 mai 2026** – Compromission du compte *compte-dgfip-2*
- **16 mai 2026** – Compromission du compte *compte-dgfip-4*
- **17 mai 2026** – Compromission du compte *compte-dgfip-3*
- **22 mai 2026** – Début de connexions suspectes au PIGP avec le compte *compte-dgfip-2*
- **24 mai 2026**
 - Modification du mot de passe de *compte-dgfip-2* par le SOC DGFIP
 - Tentatives de connexions au PIGP de plusieurs comptes à partir de la même adresse IP (*compte-dgfip-2*, *compte-dgfip-3*, *compte-dgfip-4*)
- **25 mai 2026** – Tentatives de connexions au PIGP de plusieurs comptes (*compte-dgfip-2*, *compte-dgfip-3*, *compte-dgfip-4*) à partir d'une même adresse IP, différente de la veille.
- **29 mai 2026** – Tentatives de connexions au PIGP avec le compte *compte-dgfip-3*
- **3 juin 2026** – Fin des connexions suspectes pour le groupe de trois utilisateurs.

Le compte *compte-dgfip-2* a été identifié par le prestataire de veille comme compromis et le SOC de la DGFIP a réinitialisé son mot de passe le jour de la notification (**25 mai 2026**). La compromission du compte *compte-dgfip-3* n'a pas été notifiée par le prestataire de veille. Le compte *compte-dgfip-4* a été identifié comme compromis le **3 juin 2026**, la dernière date de changement de mot de passe est le **12 juin 2026**, soit 9 jours plus tard.

Le **7 juin 2026**, un nouveau compte *compte-dgfip-5* s'authentifie avec succès au PIGP depuis une IP localisée en France. Quelques minutes plus tard, l'attaquant valide l'accès métier sur le portail ADER à partir d'une adresse IP du RIE (adresses *adresseIP_01* et *adresseIP_02*), avec ce même compte *compte-dgfip-5*. Les recherches de l'attaquant sur la messagerie déclenchent une alerte le jour même et le compte *compte-dgfip-5* est réinitialisé le jour même. Ce traitement rate le pivot effectué par l'attaquant entre les portails PIGP et ADER, difficilement identifiable en l'absence de supervision du portail ADER (source : DGFIP).

Le **9 juin 2026**, le centre opérationnel de sécurité des systèmes d'information ministériels (COSSIM) du ministère de l'Éducation nationale informe l'ensemble des CSIRT (*Computer Security Incident Response Team*) des ministères d'un incident sur son périmètre. Le COSSIM partage 17 marqueurs utilisés lors de cette attaque et leur demande d'élever le niveau de vigilance sur les connexions réseau initiées depuis les adresses IP de son ministère au travers du RIE (liste des adresses IP du ministère jointe au signalement). L'adresse *adresseIP_02* y est mentionnée à ce titre.

Le **11 juin 2026**, le COSSIM envoie un nouveau marqueur.

Le **15 juin 2026**, un partenaire informe l'ANSSI de la compromission de 2 comptes de la DGFIP *compte-dgfip-6*, *compte-dgfip-7*. La DGFIP ne répond pas et n'est pas relancée par l'Agence. Les comptes *compte-dgfip-6* et *compte-dgfip-7* avaient fait l'objet d'une notification *RecordedFuture* (source : DGFIP) et ont bien été réinitialisés (le 2 juin et le 9 juin respectivement).

Le **16 juin 2026**, l'attaquant effectue de nouvelles tentatives à destination du PIGP et de ADER : des connexions non authentifiées sont initiées vers le portail ADER à partir du SI du ministère de l'Éducation nationale (source : *ministère de l'Éducation nationale*) tandis que l'attaquant effectue des tentatives de connexions (en échec) depuis *adresseIP_03* avec 6 comptes sur le PIGP *compte-dgfip-2*, *compte-dgfip-3*, *compte-dgfip-4*, *compte-dgfip-8*, *compte-dgfip-9* et *compte-dgfip-10* (source : DGFIP).

- **Premières exfiltrations de données (juin 2026)**

Le **21 juin 2026**, une authentification est réussie avec un nouveau compte *compte-dgfip-11* sur le PIGP depuis internet puis le **22 juin 2026** sur le portail ADER depuis le RIE (adresses *adresseIP_01* et *adresseIP_02*) (source : DGFIP). Il est à noter que les adresses IP à l'origine de ces connexions avaient déjà été utilisées par l'attaquant pour des tentatives d'authentification mentionnées pendant les premières activités suspectes. Au cours de cette session, l'attaquant effectue de la reconnaissance technique. On constate le téléchargement d'une fiche de documentation applicative [REDACTED] (source : ANSSI)

Le **22 juin 2026**, un partenaire informe l'ANSSI de la compromission d'un compte *compte-dgfip-12*. La DGFIP répond le jour même à l'ANSSI avoir réinitialisé ce compte et sensibilisé leur agent (source : ANSSI).

Le **23 juin 2026**, une connexion réussie est constatée avec un nouveau compte *compte-dgfip-13* sur le PIGP depuis internet, puis sur le portail ADER depuis le RIE (*adresseIP_01* et *adresseIP_02*). Au cours de cette session, l'attaquant se concentre sur l'application E-Contact (prise d'une capture d'écran) et initie le développement itératif d'outils d'extraction par *scraping* sur celle-ci (source : DGFIP, ANSSI).

Le compte à l'origine de la connexion, *compte-dgfip-13*, est identifié comme compromis par *RecordedFuture* le même jour, dans la même temporalité que les actions de l'attaquant sur le portail ADER (source : DGFIP et *RecordedFuture*).

En parallèle, l'activité de ce compte lève une alerte à cause des recherches effectuées sur le PIGP et entraîne automatiquement la création d'un ticket auprès du SOC DGFIP à 20h50. Le compte se déconnecte à 23h51.

- **Exfiltrations automatisées de données (juin et juillet 2026)**

Le **24 juin 2026** à partir de 04h26, le même compte *compte-dgfip-13*, est exploité pour exfiltrer, pendant une session de plusieurs heures, des données de E-Contact [REDACTED]

[REDACTED]. Cette phase d'exfiltration prend fin le **25 juin 2026** à 02h31 (source : ANSSI/DGFIP).

Le ticket du SOC est traité le **24 juin 2026** à 10h40 via la réinitialisation du mot de passe du compte *compte-dgfip-13*, ainsi que celui de la session du 21 juin du compte *compte-dgfip-11* (source : DGFIP).

Ce traitement, adressant une alerte sur le PIGP, passe à côté de l'activité sur le portail ADER. La réinitialisation n'interrompt pas la session et l'exfiltration en cours qui se poursuivent (source : ANSSI).

Ces activités, entre le **22 et le 25 juin 2026**, se retrouvent dans les investigations du ministère de l'Éducation nationale qui identifie *a posteriori* une connexion volumineuse en données échangées entre le serveur attaquant et le portail ADER (source : ministère de l'Éducation nationale).

- **Activités entre les deux exfiltrations (juin et juillet 2026)**

Entre **mi-juin et fin juin 2026**, l'attaquant effectue des tentatives d'authentification plus nombreuses (l'adresse IP à l'origine de ces connexions ayant déjà été utilisée par l'attaquant au cours des jours précédents). Les tentatives concernent 14 comptes (*compte-dgfip-2*, *compte-dgfip-3*, *compte-dgfip-4*, *compte-dgfip-8*, *compte-dgfip-9*, *compte-dgfip-10*, *compte-dgfip-14*, *compte-dgfip-15*, *compte-dgfip-16*, *compte-dgfip-17*, *compte-dgfip-18*, *compte-dgfip-xt-1*, *compte-dgfip-xt-02*, *compte-dgfip-xt-03*, *compte-dgfip-xt-04*), toutes en échec (source : DGFIP).

Le **29 juin 2026**, un partenaire informe l'ANSSI de la compromission du compte, *compte-dgfip-13*. Il s'agit du compte utilisé pour l'exfiltration de données le **24 juin 2026**, or cette compromission n'était pas connue à cette date et les analyses menées par le SOC de la DGFIP ne l'identifient pas. La DGFIP répond le jour même à l'ANSSI avoir déjà connaissance de ce fait et confirme l'avoir réinitialisé (source : ANSSI).

Le **1^{er} juillet 2026**, la DGFIP est informée par son prestataire de la vente de 2 comptes *compte-dgfip-19*, *compte-dgfip-20*. Le SOC DGFIP réinitialise les mots de passe (source : RecordedFuture).

Les investigations montreront, *a posteriori*, des échecs de connexion sur le PIGP le même jour et le jour précédent avec ces comptes à partir d'une des adresses IP utilisées pour l'exfiltration du **24 juin 2026** (source : DGFIP).

Le **4 juillet 2026**, le COSSIM partage un nouveau lot de marqueurs issus de la gestion de son incident initial.

Le **6 juillet 2026** à 20h18, 4 minutes après la connexion du compte *compte-dgfip-5* sur le PIGP, des recherches suspectes effectuées par l'attaquant sur la messagerie génèrent automatiquement une alerte auprès du SOC (source : DGFIP).

Le **7 juillet 2026**, l'attaquant se connecte sur le portail ADER avec le compte *compte-dgfip-5*. Il télécharge manuellement 2 fiches [REDACTED], possiblement pour vérifier la validité de ses accès.

A 10h10, le SOC réinitialise le compte *compte-dgfip-5*, concerné par l'alerte de la veille (Source : DGFIP)

Le **11 juillet 2026**, 2 comptes *compte-dgfip-4* et *compte-dgfip-7* utilisés par l'attaquant sont en échec de connexion sur le PIGP (source : SOC DGFIP).

- **Seconde vague d'exfiltrations de données (juillet 2026)**

Le **18 juillet 2026**, deux nouveaux comptes sont compromis *compte-dgfip-21*, *compte-dgfip-22* (source : DGFIP et RecordedFuture).

Le **21 juillet 2026**, à 19h49, l'attaquant valide le bon fonctionnement sur PIGP (depuis l'adresse IP *adresseIP_01*) des couples identifiant/mot de passe de cinq comptes dont les deux compromis le **18 juillet 2026** *compte-dgfip-xt-5*, *compte-dgfip-xt-6*, *compte-dgfip-xt-7*, *compte-dgfip-21*, *compte-dgfip-22*. À 19h43, il se connecte également au portail ADER avec *compte-dgfip-xt-6* (source : DGFIP).

Le **22 juillet 2026** à 07h11, l'attaquant se reconnecte avec le compte *compte-dgfip-21*. A 7h28, il relance l'exfiltration automatique de données sur l'application E-Contact (source : DGFIP). [REDACTED]. Cette session prend fin à 11h33.

A 16h20, l'attaquant se reconnecte et recommence son exfiltration jusqu'à 17h16 (source : DGFIP).

Le **23 juillet 2026**, le SOC de la DGFIP détecte des recherches suspectes avec le compte *compte-dgfip-21* (source : DGFIP).

Le **24 juillet 2026**, le SOC traite le ticket de la veille en réinitialisant le compte *compte-dgfip-21* et bloque également l'IP *adresseIP_01* (source : DGFIP).

Ces activités, entre le **21 et le 27 juillet 2026**, se retrouvent dans les investigations du ministère de l'Éducation nationale qui identifie une connexion réseau de 3Go entre le serveur attaquant et le portail ADER (source : ministère de l'Éducation nationale).

- **Revendication et découverte de l'incident (août 2026)**

Le **12 août 2026**, l'attaquant revendique sur un forum [REDACTED] la compromission de la DGFIP et annonce le vol de 678 437 enregistrements (392 867 particuliers, 285 570 professionnels) (source : OSINT/CTI). Cette publication est associée à la session d'exfiltration observée **24 juin 2026**.

- **Mesures d'endiguement (août 2026)**

Le **6 août 2026**, l'ANSSI signale à la DGFIP 2 adresses IP (*adresseIP_01* et *adresseIP_03*) associées à des activités malveillantes, afin d'effectuer une levée de doute sur du trafic suspect à destination de deux portails de la DGFIP. Ce trafic est identifié dans le cadre d'une recherche d'antécédents sur les sondes de l'ANSSI.

Le **11 août 2026**, la DGFIP répond à l'ANSSI avoir identifié des connexions suspectes. Elle indique avoir réinitialisé 5 comptes et avoir mis en blocage les 2 adresses IP partagées.

Le **12 août 2026**, l'ANSSI informe le CSIRT Finances qui prévient le SOC de la DGFIP (*source : ANSSI*).

Le **13 août 2026**, la DGFIP identifie l'accès de l'attaquant depuis le RIE [REDACTED]. Elle désactive l'accès au portail ADER pour les comptes des agents DGFIP et assimilés. Cette mesure est toujours d'actualité et le portail ne devrait pas être réouvert aux identités de ce type (*source : DGFIP*).

Le **18 août 2026**, la DGFIP coupe les accès au PIGP pour les comptes « agents » (les comptes externes utilisés par les partenaires « gestion publique » de la DGFIP pouvant conserver leur accès). Cet accès « agents » est toujours coupé et ne devrait pas être réouvert (*source : DGFIP*).

Incident sur le serveur professionnel de données cadastrales (SPDC)

Le **13 août 2026** à 18h44, l'ANSSI est avertie d'une revendication de la compromission de données issues du SPDC, appartenant à la DGFIP. La revendication mentionne 2 millions de Français concernés et une exfiltration ayant eu lieu le **29 juillet 2026**. D'après l'attaquant, les données contiendraient des noms, dates de naissance, identifiants fonciers, parcelles cadastrales et informations sur les biens détenus. A 20h, le service du haut responsable de défense et de sécurité (SHFDS) de Bercy accuse réception et indique avoir prévenu la DGFIP (*source : ANSSI*).

Le **14 août 2026**, la compromission d'un compte d'un géomètre-expert au sein d'un cabinet privé est identifiée comme la source de l'exfiltration. Celle-ci aurait été opérée à travers le portail APEX dédié à ces partenaires. La possible compromission du poste informatique du géomètre-expert a permis d'outrepasser le second facteur. Le compte a immédiatement été désactivé et l'accès au portail a été verrouillé, induisant un fort impact (*source : DGFIP*).

Le **18 août 2026**, la DGFIP indique avoir désactivé tous les comptes de ce cabinet de géomètre et les avoir prévenus de la compromission probable de leur environnement informatique (*source : DGFIP*).