



www.veillemag.com

Le magazine des professionnels
de l'information stratégique

Par Jacqueline Sala

Focus Cybersécurité. Septembre 2026. Cyberattaques contre l'État, crise de confiance numérique et vulnérabilités systémiques : la souveraineté à l'épreuve des faits. Yannick Pech

Le mois de septembre 2026 confirme la longue séquence de dégradation du paysage de la cybersécurité en France et en Europe. Fuites de données, attaques contre les administrations et vulnérabilités critiques révèlent les fragilités persistantes des systèmes d'information essentiels. La publication du rapport de l'ANSSI sur le piratage de la DGFIP constitue l'un des faits marquants. Il met notamment en évidence des faiblesses dans la gestion des identités, l'architecture des systèmes et la détection des activités malveillantes...



... Au-delà de cet incident, l'actualité montre qu'il n'est pas nécessaire de disposer d'outils offensifs sophistiqués pour compromettre des infrastructures sensibles. Identifiants légitimes volés, failles connues et dispositifs de surveillance insuffisants peuvent suffire à provoquer des dommages importants. Cette situation témoigne de l'écart sans cesse croissant entre les capacités de protection-détection-réaction et l'évolution de la cybermenace, en particulier à l'aune de la démocratisation des agents d'IA.

FOCUS | DGFIP : UNE ATTAQUE RÉVÉLATRICE DES FRAGILITÉS STRUCTURELLES DE L'ÉTAT

Le 29 septembre, l'ANSSI a rendu public son rapport d'investigation sur les cyberattaques qui ont visé la Direction générale des Finances publiques au cours de l'été. Ce document apporte un éclairage particulièrement instructif sur les conditions de compromission des systèmes des Impôts et sur les faiblesses qui ont permis aux attaquants d'exfiltrer des données sensibles.

Le constat est sévère : l'incident ne résulte pas d'une attaque techniquement sophistiquée, mais de la combinaison de défaillances dans trois domaines essentiels : la gestion des identités, l'architecture du système d'information et la détection des activités suspectes. On pourrait ajouter les lacunes en termes de renseignement sur la cybermenace de la part des ministères hors MINARM

Les investigations ont établi que des identifiants légitimes de plusieurs dizaines d'agents publics avaient été compromis. Selon l'ANSSI, leur

récupération est probablement liée à l'utilisation d'équipements personnels (notons déjà la faille **BYOD** - *Bring Your Own Device*/"Disaster", floutage des activités perso/pro) infectés par des logiciels malveillants de type *infostealer*, capables de dérober des identifiants. Toujours selon le rapport, l'absence d'authentification multifacteur sur deux portails concernés a ensuite facilité l'accès aux ressources sensibles.

L'architecture des systèmes a également contribué à l'incident. Certaines applications étaient accessibles depuis l'Internet ou depuis le réseau interministériel de l'État **sans cloisonnement suffisant**. Cette situation a facilité les possibilités de *latéralisation* (déplacement) entre environnements et a mis en évidence les risques liés aux interconnexions entre administrations.

Enfin, les dispositifs de surveillance n'ont pas détecté les deux principales vagues d'exfiltration. Des signaux suspects avaient pourtant été observés, mais leur traitement et leur corrélation n'ont pas permis d'interrompre les opérations à temps. Les volumes de données extraits auraient dû déclencher des alertes. **Le mot de passe du compte compromis a bien été réinitialisé, mais cela n'a pas permis de supprimer son accès**

Poussons la réflexion : en prenant en compte toutes ces informations, le rapport ne mentionne pas – il faut le deviner implicitement – ce qui s'est réellement passé. L'inefficacité de la réinitialisation du mot de passe du ou des comptes incriminés, même si la MFA avait été activée, est le signe évocateur que le **principal vecteur d'attaque a reposé sur l'achat en ligne par Zerobytes de logs d'infostealers** où ont été repérés les identifiants desdits fonctionnaires. Or, comment opère un *infostealer*, héritier des plus anciens malwares baptisés *keyloggers* (qui enregistraient les frappes de clavier sur les machines infectées) ? **Le principal avantage des infostealers** tels que Raccoon, Lumma ou Redline **est de capturer** non seulement des mots de passe et autres DCP, mais avant tout **les cookies de sessions de navigation** (ou « jetons d'authentification ») (1*) . Ainsi, plus besoin de connaître les identifiants et contourner au besoin l'authentification multifactorielle, puisque ces informations sont contenus dans lesdits cookies. Imparable, même avec une hygiène informatique élémentaire (la destruction systématique des cookies et des données de site par exemple) : **dès lors qu'on ne révoque pas spécifiquement la session concernée (côté serveur), les cookies associés permettent d'outrepasser l'identification**. En effet, l'accès reste légitime car authentifié.

Mais alors, quelle est la solution pour se prémunir de ces attaques ? Google a lancé en avril 2026 un protocole sur son navigateur Chrome, le **Device Bound Session Credentials** (DBSC) pour protéger les cookies de session, mais il semble que la technologie soit encore artisanale. Mozilla l'a rejetée pour Firefox car l'association estime, d'une part, qu'elle **ouvre une autre surface d'attaque** en contournant des dispositifs de sécurité des navigateurs (*flags* http-Only, secure, same-site, etc.) ; d'autre part, que le protocole **réduit le risque sans l'éliminer** (fenêtre temporelle encore possible de vol, du moins si l'appareil est directement infecté par l'*infostealer*) et ne justifie donc pas sa complexe implémentation au prisme du rapport coût/bénéfice actuel.

(1*) Selon une analyse NordVPN de 2026, les cookies de session représentent 4,6 fois plus de données volées dans les logs d'infostealers que les mots de passe, fichiers et cartes bancaires combinés.

Les meilleures contre-mesures aux vols de cookies de session.

Contrôle	Effet
Révocation serveur (logout (utilisateur), admin (révocation manuelle), IdP (le fournisseur d'ID révoque via SSO)	Invalide la session à la source
Délais courtsd'expiration/d'inactivité	Réduit la fenêtre d'exploitation
Device binding/liaison à l'appareil (ex : DBSC de Chrome V.146, avril 2026 (TPM Windows, Secure Enclave (MacOS/iOS), TEE pour Android (comme Samsung Knox ou Google Titan sur Pixel...)). Pour l'heure Chrome est le seul équipé.	Le cookie est lié à une clé privée dans le TPM <i>Trusted Platform Module</i> , nom générique indiquant l'inscription du cookie, chiffré, dans une puce matérielle/le <i>firmware</i> de l'appareil). Même exfiltré, il devient inutilisable sans l'appareil d'origine
Détection d'anomalie d'authentification (IP, géolocalisation, empreinte digitale...)	Détecte l'usurpation depuis un autre appareil
Renforcement MFA sur actions sensibles	Force une re-vérification même sur une session active

Au bilan, et au-delà des données fiscales dérobées de 678 000 personnes physiques et morales, l'affaire constitue un révélateur des limites de la sécurité numérique de l'État. Elle rappelle que la protection d'une infrastructure ne dépend pas uniquement de la robustesse de ses équipements ou

de la sophistication de ses outils de défense. Elle repose également sur la maîtrise des identités, la segmentation réseau, la surveillance des usages et la capacité à réagir rapidement aux signaux d'intrusion. **Autrement dit, à mettre en œuvre une défense en profondeur**

Certes, l'ANSSI préconise dans son rapport la généralisation de l'authentification forte, la proscription de l'utilisation d'équipements personnels pour accéder aux ressources professionnelles sensibles (risque BYOD), le renforcement de la supervision et une meilleure maîtrise des volumes de données consultables — donc le cloisonnement. Mais il faut donc ajouter **la gestion des sessions avec des moyens techniques de révocation automatique implémentés côté serveurs**

In fine, l'enjeu dépasse le seul cas de la DGFIP : il concerne la capacité de l'administration française à garantir la confidentialité des informations qui lui sont confiées. La confiance dans les services publics numériques repose sur cette exigence. À mesure que les démarches administratives, fiscales et sociales se dématérialisent, une défaillance de sécurité peut engendrer des conséquences qui dépassent largement le périmètre technique de l'organisme touché. Ce qui interroge par exemple sur le déroulé calendaire de la **généralisation de la facturation électronique**, passée au forceps, alors qu'un moratoire aurait été clairement le bienvenu.

L'ÉTAT FRANÇAIS FACE À UNE VAGUE DE COMPROMISSIONS : LA RÉPONSE S'ORGANISE

Le cas de la DGFIP n'est pas un incident isolé. Le mois de septembre a vu plusieurs révélations concernant des administrations et des organismes publics, confirmant que la protection des données de l'État est devenue un enjeu transversal.

Le 1er septembre, le gouvernement a d'ailleurs engagé le dispositif interministériel **REACTIV** (Réponse et action interministérielle face aux violations de données), destiné à renforcer les capacités d'intervention de l'ANSSI face aux compromissions de comptes et aux exfiltrations. Le dispositif prévoit une mobilisation plus rapide des compétences techniques, un appui renforcé aux ministères et une coordination de crise centralisée.

Le rapport de situation publié le 30 septembre fait état de 99 violations de données signalées à l'ANSSI depuis le 1er août, dont 67 confirmées et 32 encore en cours de traitement. Ces chiffres témoignent de **l'ampleur du travail auquel les équipes de réponse aux incidents sont confrontées** même s'ils ne permettent pas, à eux seuls, de mesurer l'évolution globale de la menace.

Plusieurs incidents illustrent cette exposition. Une **vulnérabilité critique de la plateforme Metabase**, utilisée pour l'analyse et la visualisation de données, a notamment été exploitée contre plusieurs instances de l'administration. Comble du comble, **le périmètre touché a inclus des environnements de la propre ANSSI et de la Direction interministérielle du numérique (DINUM)**, soulignant la difficulté de protéger durablement des outils techniques utilisés par les organismes chargés de la sécurité numérique eux-mêmes (attaque par rebond/par point d'eau).

D'autres compromissions et revendications ont concerné des services publics, des plateformes administratives et des données associées à des dispositifs d'aide ou de formation. Le Service national universel (SNU) a notamment fait l'objet d'une revendication de fuite portant sur plusieurs centaines de milliers de comptes, tandis qu'une violation affectant l'Agence de services et de paiement a exposé les données de bénéficiaires du dispositif « Coup de pouce énergie ».

La multiplication de tels incidents interroge la capacité de l'État à maîtriser l'ensemble de sa surface d'attaque. **Les systèmes d'information publics reposent sur des applications à la fois anciennes et récentes, des prestataires multiples, des échanges interministériels et des outils parfois déployés sans supervision homogène.** Chaque dépendance supplémentaire crée un risque qu'il convient d'identifier, de documenter et de maîtriser. Il faudrait dès lors tout mettre à plat, ce qui paraît irréaliste étant donné l'état de nos finances publiques et les chantiers politiques en cours. Se pose toujours la question de la vision stratégique. Empiler des briques sans logique relève du bricolage permanent.

La réponse ne peut donc se limiter à la correction des vulnérabilités après leur exploitation. Elle suppose la **prévention à travers une politique de sécurité cohérente à l'échelle de l'État**, intégrant la **gestion des identités**, le **cloisonnement des systèmes et des réseaux**, la surveillance et l'amélioration continue et la capacité à imposer des **mesures préventives** (proactives) et **correctives** (rapides) aux administrations concernées.

FUITES DE DONNÉES : UNE MENACE QUI DÉPASSE LE SEUL VOL D'INFORMATIONS

Les compromissions observées le mois passé confirment que **la fuite de données est devenue une finalité à part entière de nombreuses opérations cybercriminelles**. Le chiffrement des systèmes (*ransomwares*) n'est plus systématiquement nécessaire : l'exfiltration d'informations suffisamment sensibles permet déjà d'exercer une pression sur les victimes, de préparer des fraudes ou d'alimenter des marchés clandestins.

En France, les incidents recensés ont touché des organismes publics, des plateformes de services et des entreprises. La Fédération française de handball a fait l'objet d'une intrusion revendiquée une nouvelle fois par le ZeroBytes. Les données potentiellement concernées, relatives aux licences et à la gestion des clubs, illustrent les risques que font peser les compromissions sur des structures dont la fonction première n'est pas la cybersécurité.

D'autres incidents ont concerné des données de bénéficiaires de services publics ou des comptes d'utilisateurs de plateformes administratives. Ces informations peuvent servir à des campagnes d'hameçonnage ciblées, à l'usurpation d'identité ou à des tentatives de fraude reposant sur des informations personnelles authentiques.

La valeur des données ne réside donc pas seulement dans leur contenu brut. **Leur recoupement avec d'autres fuites permet d'enrichir le profilage, de crédibiliser des messages frauduleux et de contourner plus facilement la vigilance des victimes** (hameçonnage). L'exemple de faux documents paraissant très authentiques mais usurpant en réalité l'identité de la DGFIP — portant des **QR codes malicieux (Quishing)** — en atteste.

Cette dynamique renforce l'intérêt des cybercriminels pour les organismes qui concentrent des volumes importants d'informations personnelles, même lorsque leurs ressources financières ou techniques sont limitées. Elle rappelle également que les conséquences d'une fuite peuvent se prolonger bien après la remise en service des systèmes compromis.

VULNÉRABILITÉS CRITIQUES : LES ÉQUIPEMENTS EXPOSÉS RESTENT UNE PORTE D'ENTRÉE PRIVILÉGIÉE

Le mois de septembre a donné lieu à plusieurs alertes de sécurité portant sur des **logiciels et équipements largement déployés** dans les systèmes d'information professionnels.

Le CERT-FR (ANSSI) a notamment signalé des vulnérabilités affectant les solutions SonicWall Secure Mobile Access, Citrix NetScaler, Microsoft Edge, ainsi que différents produits Microsoft, Fortinet et GitLab. Certaines de ces failles peuvent permettre une exécution de code à distance (RCE), une élévation de privilèges (*privesc*) ou une atteinte à la confidentialité des données.

L'alerte concernant Citrix NetScaler ADC et Gateway a particulièrement retenu l'attention, avec des informations complémentaires publiées sur des compromissions et des moyens de détection. Souvent positionnés à l'entrée des réseaux d'entreprise, **ces équipements constituent des points d'entrée critiques lorsqu'ils sont accessibles depuis l'Internet**.

Quant au cas de Metabase, il rappelle qu'une vulnérabilité publiée et corrigée par l'éditeur peut continuer à produire des effets lorsque les mises à jour ne sont pas appliquées rapidement à l'ensemble des instances. La difficulté ne tient donc pas uniquement à l'identification des failles, mais à la **capacité des organisations à connaître précisément leurs actifs** (inventaire, caractérisation), à **hiérarchiser les correctifs** et à **vérifier leur déploiement effectif**.

Ces exemples illustrent les limites d'une approche de la cybersécurité reposant principalement sur la publication d'alertes. Encore faut-il que les organisations disposent d'un inventaire fiable, de procédures de mise à jour opérationnelles et de moyens suffisants pour traiter les vulnérabilités dans des délais compatibles avec leur exploitation par les attaquants.

GÉOPOLITIQUE ET CYBERDÉFENSE : LA RÉSILIENCE NUMÉRIQUE DEVIENT UNE PRIORITÉ STRATÉGIQUE

La cybersécurité reste également un enjeu de souveraineté et de sécurité nationales. Les administrations, infrastructures essentielles et prestataires numériques constituent des cibles dont la compromission peut avoir des conséquences économiques, politiques et opérationnelles.

En septembre, l'ANSSI a renforcé son dispositif d'intervention auprès des services de l'État, tandis que les autorités poursuivaient leurs efforts de sécurisation des réseaux et de coordination interministérielle. Cette mobilisation traduit une évolution de la réponse publique : les violations de données ne sont plus seulement traitées comme des incidents locaux, mais comme des événements susceptibles d'affecter plusieurs organismes et de nécessiter une coordination centralisée.

Parallèlement, le 3 septembre, l'ANSSI et les partenaires du G7 de la France ont publié un **appel à anticiper la transition vers la cryptographie post-quantique**. L'objectif est d'anticiper les conséquences de l'émergence d'ordinateurs quantiques suffisamment puissants (Qubits) pour remettre **en cause la robustesse des mécanismes cryptographiques** actuels.

Si la menace quantique ne constitue pas une urgence opérationnelle immédiate pour l'ensemble des organisations, elle impose tout de même de se préparer avant la rupture technique. Les données **interceptées aujourd'hui pourraient en effet être conservées pour être décryptées demain (attaques à froid)** si les protections employées devenaient vulnérables. Ce que certains services de renseignement ne s'empêchent du reste pas de faire depuis des années déjà (protocole [https...](https://...))

La question de la souveraineté se pose donc à plusieurs niveaux : maîtrise des infrastructures, protection (physique, logique, juridique) et localisation des données, contrôle des dépendances technologiques et capacité à anticiper les ruptures techniques. La résilience numérique ne dépend pas seulement des moyens de défense mobilisés lors d'une attaque ; elle repose également sur la capacité à préparer les transformations technologiques qui modifieront les conditions de sécurité de demain.

INTELLIGENCE ARTIFICIELLE : ENTRE EFFICACITÉ OPÉRATIONNELLE ET NOUVELLES FRAGILITÉS

L'intelligence artificielle fait bien sûr partie de cette révolution disruptive. Cette technologie poursuit du reste sa progression dans les usages professionnels et les pratiques de cybersécurité. Elle permet notamment d'accélérer l'analyse d'événements, d'assister les équipes défensives et de faciliter le traitement de volumes importants d'informations.

Mais ces possibilités s'accompagnent bien sûr de risques désormais bien connus. Les outils d'IA peuvent être utilisés pour industrialiser certaines opérations malveillantes, personnaliser les campagnes de *phishing*, identifier des vulnérabilités *zero day* ou faciliter la recherche d'informations sur des cibles. Dans le même temps, **leur intégration dans les organisations crée de nouvelles questions relatives à la confidentialité des données, à la gouvernance des usages et à la maîtrise des informations transmises aux services externes**

Le développement de ces outils ne doit pas faire oublier les fondamentaux. Une organisation qui ne maîtrise pas ses identités numériques, ses accès, ses applications exposées ou ses flux de données **ne compensera pas ces faiblesses par l'ajout d'une solution d'intelligence artificielle**.

La priorité reste donc de consolider les fondations de la sécurité informatique, tout en évaluant les apports et les risques de ces nouvelles

technologies. L'IA peut renforcer les capacités de défense, mais **elle ne remplace ni la gouvernance, ni l'expertise humaine, ni la responsabilité des organisations** dans la protection de leurs systèmes.

PERSPECTIVES

Septembre 2026 met en évidence un paradoxe désormais difficile à ignorer : alors que les capacités de détection et de réponse aux cybermenaces progressent, les systèmes d'information publics et privés restent exposés à des défaillances fondamentales. L'affaire DGFIP en constitue l'illustration la plus frappante. L'exploitation d'identifiants compromis, l'absence d'authentification forte sur des accès sensibles et les lacunes de supervision ont permis une exfiltration massive sans recours à une technique avancée.

La mise en place du dispositif REACTIV traduit une prise de conscience institutionnelle et la volonté de renforcer la réponse aux incidents. Elle devra toutefois s'accompagner d'une transformation durable des pratiques : maîtrise des identités, cloisonnement des systèmes, segmentation réseau, supervision effective, gestion rigoureuse des équipements et contrôle des prestataires.

Au-delà de la réponse technique, c'est la question de la confiance numérique qui est posée. Les administrations concentrent des données dont la compromission peut fragiliser les citoyens, faciliter les fraudes et affecter la crédibilité des services publics. La souveraineté numérique ne peut donc se résumer à la localisation des infrastructures ou au choix des fournisseurs : elle implique aussi la capacité à protéger effectivement les systèmes et les informations placés sous la responsabilité de l'État. C'est un devoir essentiel vis-à-vis de ses administrés.

Le principal enseignement du mois est finalement moins celui d'une sophistication toujours croissante des attaquants que celui d'un décalage persistant entre la numérisation des organisations et leur capacité à maîtriser les risques qui en découlent. **La cybersécurité devient ainsi un enjeu de gouvernance, de résilience collective et de souveraineté opérationnelle**

RÉSUMÉ

1. **DGFIP : le rapport de l'ANSSI** révèle des défaillances dans la gestion des identités, l'architecture des systèmes et la détection, mais aussi les modes opératoires toujours renouvelés des attaquants.
2. **Administrations publiques: le dispositif REACTIV** renforce la réponse interministérielle, dans un contexte de multiplication des violations de données relevant de la responsabilité de l'État.
3. **Fuites de données** : les compromissions alimentent les fraudes, l'usurpation d'identité et les marchés clandestins, avec des conséquences durables pour les victimes.
4. **Vulnérabilités critiques** : les failles affectant les équipements réseau et les logiciels professionnels imposent une gestion des correctifs plus rapide et plus rigoureuse.
5. **Souveraineté et anticipation** : la résilience numérique repose autant sur la maîtrise des systèmes existants que sur la préparation des évolutions technologiques, notamment post-quantiques et IA.

SOURCES PRINCIPALES

DGFIP, ANSSI et sécurité des administrations françaises

<https://cyber.gouv.fr/actualites/lanssi-publie-le-rapport-dincident-sur-les-cyberattaques-ayant-touche-la-dgfi/>

<https://cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-006>

<https://www.01net.com/actualites/piratage-impots-anssi-revele-vraiment-passe-cyberattaque.html>

<https://www.01net.com/actualites/les-hackers-des-impots-ont-encore-frappe-des-donnees-personnelles-ont-encore-ete-volees.html>

<https://www.01net.com/actualites/suite-piratage-impots-la-cnif-control-fisc-tirer-consequences.html>

Vulnérabilités et alertes de sécurité

<https://www.cert.ssi.gouv.fr/alerte/>

<https://www.cert.ssi.gouv.fr/avis/>

<https://www.cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-002/>

Actualité cyber et veille spécialisée

<https://www.zataz.com/category/actualites/cyber-actualite/>

<https://www.lemondeinformatique.fr>

<https://www.bleepingcomputer.com>

A PROPOS DE L'AUTEUR



Yannick PECH est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, détenteur d'une certification de Pentester junior (eJPT) et de la certification EBIOS Risk Manager de l'ANSSI.

Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur associé au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste à la Compagnie européenne d'intelligence stratégique (CEIS), consultant-analyste au CRR-FR (OTAN-France) et réserviste opérationnel-spécialiste de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie.

KEYWORDS

#Cybersecurity #Cyberattacks #DigitalSovereignty #DataSecurity #DataBreach #Infostealers #CyberDefense #CyberResilience #ThreatIntelligence #AICybersecurity

06/10/2026



Cette newsletter est proposée et diffusée par Veille Magazine - www.veillemag.com
Plan du site |  Syndication | Inscription au site