MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

Revue de presse des cybermenaces

Centre d'analyse des cybermenaces

#10 – Octobre 2026

A retenir

En septembre, l'ANSSI constate une intensification des attaques liées à des violations de données visant les services de l'État (ministère de la Transition écologique, SNU, ASP). ANSSI

Parallèlement, la compromission de prestataires démultiplie l'impact des attaques (Brevo, Revolut).

En réponse, l'État accélère : dispositif REACTIV de l'ANSSI, mise en examen d'un membre présumé de ZeroBytes, contrôle de la DGFiP par la CNIL.

Octobre est le mois européen de la cybersécurité.

Chiffres du mois

45 % : c'est la part des Français informés d'une fuite de leurs données personnelles en 2026, contre 30 % en 2025, selon le 3e baromètre sur la perception cyber des Français réalisé avec Ipsos Digital.
Cybermalveillance.gouv.fr

14 : c'est le nombre d'incidents transfrontières significatifs signalés en 2025 par les États membres, alors que l'ENISA en avait identifié 322 visant au moins deux États membres en 2024, selon la Cour des comptes européenne. Cour des comptes européenne

Principales cyberattaques

Le 7 septembre 2026, le ministère de la Transition écologique a été ciblé par une cyberattaque. L'attaquant revendique l'exploitation d'une interface de programmation (API) mal configurée et d'une faille de contrôle d'accès (IDOR) : les données de 14 656 contrôleurs et de 8 166 utilisateurs auraient été exfiltrées. Le ministère a renforcé ses mesures de protection et saisi le parquet ; l'ANSSI participe aux investigations. Le Monde Informatique

Le groupe LunarisSec revendique le vol des données d'environ 275 000 comptes de la plateforme du Service national universel (SNU), dont 5 000 comptes de responsables de structures (noms, prénoms, adresses électroniques, numéros de téléphone). Le 18 septembre, le SNU a confirmé une possible fuite ainsi que la création frauduleuse de comptes de responsables. FrenchBreaches

Le portail du dispositif « Coup de pouce énergie » de la Région Île-de-France, géré par l'Agence de services et de paiement (ASP), a fait l'objet d'un accès frauduleux le 27 août 2026. Les avis de paiement exfiltrés contiennent noms, adresses postales, numéros de bénéficiaire, IBAN et montants versés. L'attaquant revendique plus de 143 000 lignes ; l'ASP a informé 108 555 personnes concernées. Solutions Numériques FrenchBreaches

Brevo, plateforme française d'envoi de courriels, a subi deux incidents. Le 9 septembre, un accès frauduleux à son système a permis d'envoyer, depuis le compte de Trezor, un faux message d'alerte de sécurité à 347 000 adresses. Le 14 septembre, une clé API Cloudflare compromise a servi à injecter, pendant environ cinq heures et demie, un faux CAPTCHA de type ClickFix, qui pousse l'internaute à exécuter lui-même une commande malveillante, dans les ressources de Brevo intégrées aux sites de ses clients. Brevo Trezor

L'acteur malveillant ChimeraZ a publié, le 19 septembre, les données de 120 158 clients de l'Armurerie Lavaux : identités, adresses, téléphones et détail des achats d'armes et de munitions. Le pirate présente certaines données comme liées à la FFTir et au Système d'information sur les armes (SIA), sans que rien ne permette d'affirmer que ces systèmes ont été compromis. Ces informations exposent les détenteurs d'armes à des opérations de repérage.
FrenchBreaches

Pendant environ six mois, le groupe IAmNotAVillain aurait obtenu de Revolut les données de quelque 680 clients, dont plus de 100 Français, en adressant de fausses réquisitions depuis un compte de messagerie certifiée (PEC) compromis, attribué à une préfecture italienne. Les données transmises incluent pièces d'identité, selfies de vérification, IBAN et historiques de transactions. FrenchBreaches Security Affairs

Pour aller plus loin …

[Cour des comptes européenne] « Rapport spécial 19/2026 : détection et réponse aux incidents de cybersécurité » - La Cour juge le cadre de coopération de l'UE seulement partiellement efficace : les États membres partagent peu leurs incidents et le système européen d'alerte en cybersécurité n'est toujours pas opérationnel.
Cour des comptes européenne

[ENISA] *« ENISA's view on Cybersecurity in the Frontier AI Era »* - L'agence européenne estime que l'IA de pointe peut ramener à quelques minutes le délai entre la divulgation d'une vulnérabilité et son exploitation, et relève un délai médian de 72 minutes entre l'accès initial et l'exfiltration. ENISA Security Affairs

Faits marquants

Le parquet de Paris a annoncé, début septembre, la mise en examen et le placement en détention provisoire d'un homme de 18 ans, membre présumé du groupe ZeroBytes, pour extraction frauduleuse de données et association de malfaiteurs. Le groupe est soupçonné du piratage de la DGFiP (données de 678 000 usagers d'impots.gouv.fr) et de celui du ministère de l'Éducation nationale. Un second suspect, âgé de moins de 16 ans, a été remis en liberté. L'enquête est confiée à l'Office anti-cybercriminalité (OFAC). Euronews

Un Parisien de 25 ans a été mis en examen pour escroquerie et blanchiment en bande organisée, puis placé en détention provisoire. Entre mai et juillet 2025, il aurait utilisé des adresses électroniques désactivées de la police et de la justice pour se faire passer pour des commissaires ou des procureurs et obtenir des virements vers le Portugal et l'Espagne. Le préjudice est estimé entre 150 000 euros et un million d'euros. L'enquête a été menée par l'Office central de répression de la grande délinquance financière (OCRGDF). Clubic FrenchBreaches

Informations sur la menace

Deux failles critiques du cœur de WordPress ont été corrigées en septembre. La première, baptisée « Click2Shell » et corrigée le 17 septembre par la version 7.1.1, permet, au moyen d'une URL spécialement conçue, d'installer et de prévisualiser automatiquement un thème inactif. La seconde (CVE-2026-87902), corrigée le 22 septembre par la version 7.1.2, permet à un attaquant non authentifié, dans certaines configurations, d'inclure un fichier PHP local et d'exécuter du code à distance ; les premières tentatives d'exploitation ont été détectées quelques heures après le correctif. Le CERT-FR recommande une mise à jour immédiate. WordPress.org CERT-FR Bleeping Computer

Le 28 septembre, le CERT-FR a émis une alerte sur deux vulnérabilités critiques (CVE-2026-88771 et CVE-2026-88772) de Citrix NetScaler ADC et Gateway, des équipements d'accès distant. Exploitées avant la publication des correctifs, elles permettent à un attaquant non authentifié d'exécuter du code à distance ; une preuve de concept est désormais publique. Le CERT-FR demande d'appliquer les correctifs et de rechercher d'éventuelles traces de compromission. CERT-FR

Un dirigeant de Fideuram, filiale de banque privée d'Intesa Sanpaolo, a reçu sur WhatsApp un message usurpant l'identité du directeur général du groupe, puis l'appel d'un faux avocat dont la voix aurait été clonée par IA. Onze faux documents, dont une procuration à la signature contrefaite, ont achevé de le convaincre : 95 millions d'euros ont été virés, dont environ 36 millions restent introuvables. Le parquet de Milan enquête. Cybernews

Anticipation / Réglementation

Octobre est le mois européen de la cybersécurité (ECSM), campagne annuelle de l'Union européenne coordonnée par l'ENISA avec la Commission européenne. En France, la 14e édition du Cybermois, lancée le 15 septembre par Cybermalveillance.gouv.fr avec plus de 2 400 partenaires, porte la campagne « Se cyber protéger, ce n'est pas si bête » : dépliant conçu avec la CNIL sur les violations de données, CyberTour de France (Biarritz, Rennes, Rouen, Lille, Montpellier, Paris) et sensibilisation en gare les 22 et 29 octobre. Cybermalveillance.gouv.fr ENISA

Le 31 août 2026, le Premier ministre a donné 15 jours aux ministres pour appliquer le plan de sécurisation de l'État présenté en avril et doté de 200 millions d'euros. Le 7 septembre, à sa demande, l'ANSSI a mis en place REACTIV (Réponse et action interministérielle face aux violations de données) : l'agence pourra imposer aux ministères les mesures immédiates nécessaires pour protéger les données des citoyens et centralisera la communication technique de crise. ANSSI Le Monde Informatique

Après les intrusions ayant touché près de 700 000 personnes, la CNIL va conduire un contrôle approfondi de la DGFiP, ainsi que de l'ANTS. Une mise en demeure ou une procédure de sanction pourrait intervenir d'ici fin 2026, la CNIL ne pouvant pas infliger d'amende à l'État. FrenchBreaches

Cliquez ici pour vous abonner :