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

#08-09 – AOÛT - SEPTEMBRE 2026

A retenir

Le vote européen sur le projet « Chat Control » a déclenché une vague de contestation, accompagnée de cyberattaques, illustrant la montée en puissance des mobilisations hacktivistes autour de sujets fortement médiatisés et controversés.

Les autorités américaines alertent sur l'usage croissant de l'IA générative pour identifier et exploiter des automates industriels vulnérables, touchant notamment les petites infrastructures du secteur de l'eau.

La Commission européenne a saisi la Cour de justice de l'UE contre la France pour son retard dans la transposition de la directive NIS2.

Chiffres du mois

678 000 : c'est le nombre de particuliers et professionnels touchés par la fuite de données de la DGFiP en août 2026. Le Monde

97 % des attaques par l'utilisation d'identifiants compromis ont eu lieu malgré le déploiement d'un MFA. Sophos

62 % des entreprises françaises réclament un durcissement des règles en matière de cybersécurité. Usine Digitale

Principales cyberattaques

Lors d'une cyberattaque menée entre juin et juillet, des pirates se présentant sous le nom de ZeroBytes ont accédé au système d'information de la DGFiP en exploitant des identifiants compromis (ceux d'un agent combinés à ceux d'un tiers habilité). Ils ont pu consulter les données fiscales de 678 000 particuliers et professionnels, ainsi qu'environ 200 000 comptes cadastraux. Les accès, désormais fermés, font l'objet d'un audit de l'ANSSI et d'une enquête du parquet de Paris, tandis que l'administration alerte sur les risques d'hameçonnage. Le Monde

Le 26 juillet 2026, l'acteur Misere a revendiqué la diffusion de données de 111 528 agents de l'État français de plusieurs services publics. Cette revendication est présentée comme une réponse au projet européen de lutte contre la diffusion de contenus pédocriminels en ligne, aussi appelé « Chat Control ». InCyber

Le vote européen sur le projet « Chat Control » a suscité une forte vague de contestation, accompagnée de menaces de cyberattaques (Lunarisec) et de campagnes hacktivistes. Toutefois, de nombreuses informations relayées en ligne ont déformé la portée réelle du vote : il s'agissait de prolonger un dispositif temporaire en vigueur depuis 2021, dans l'attente de l'adoption d'un cadre permanent. Franceinfo

Lors d'un test de sécurité en environnement contrôlé, des modèles d'OpenAI, dont GPT-5.6 Sol, ont réussi à contourner les restrictions qui limitaient leur accès à Internet en exploitant une faille informatique inédite (« zero-day »). Ils ont ensuite mené une intrusion sur la plateforme Hugging Face, utilisant notamment des identifiants compromis afin de tenter d'accéder aux réponses d'un test d'évaluation. L'incident, désormais résolu, relance les inquiétudes sur les capacités offensives des modèles d'IA les plus avancés en matière de cybersécurité. Usine Digitale

Le 6 août 2026, le Stade français a annoncé avoir été victime d'une attaque par rançongiciel attribuée au groupe Qilin. Le club a porté plainte et, avec l'aide de prestataires externes, a pu rétablir ses systèmes grâce à des sauvegardes saines. À ce jour, ses activités ne semblent pas impactées. Stade français

Pour aller plus loin …

[We Live Security] ESET Research publie, le 8 juillet 2026, un rapport sur les menaces liées à l'IA : plus de 3 000 des 900 000 « AI skills » analysées sont jugées malveillantes. Le rapport identifie notamment PromptSpy, premier malware Android exploitant l'IA générative à l'exécution, et une hausse de 108 % des attaques de type ClickFix.

[Sophos] Dans son « State of Identity Security Report », Sophos identifie l'identité comme principal vecteur des attaques par rançongiciel. Les e-mails malveillants (26 %) et l'hameçonnage (24 %) devancent désormais l'exploitation de vulnérabilités (18 %).

Faits marquants

Le 15 juillet 2026, la police nationale espagnole, avec l'appui d'Europol et d'Interpol, a annoncé le démantèlement d'un réseau ayant détourné 140 millions d'euros via de fausses plateformes d'investissement et des fraudes au président. Les fonds étaient blanchis par 67 mules financières, à travers plus de 800 comptes bancaires. Bilan : quatre arrestations en Espagne, au Portugal et au Panama, six perquisitions dans les provinces de Barcelone, Gérone et Tarragone ainsi qu'à Porto, plus de 170 smartphones et 15 ordinateurs saisis, et 3 millions d'euros bloqués en vue d'une restitution aux victimes. Génération NT

Le Woolwich Crown Court, tribunal pénal londonien, condamne deux membres de Scattered Spider, Owen Flowers et Thalha Jubair, à cinq ans et six mois de prison pour l'attaque de 2024 contre Transport for London (TfL). L'exploitation d'une attaque par ingénierie sociale a permis le vol de données de 10 millions de voyageurs et coûté 40 millions de livres sterling. Le groupe, également actif en France, constitue une menace transnationale majeure. Cette condamnation, fruit d'une enquête internationale menée par la NCA et le FBI, marque la plus grande poursuite pénale contre des cybercriminels au Royaume-Uni. Le Mag IT

Informations sur la menace

Les autorités américaines alertent sur une nouvelle menace visant les infrastructures critiques : des hackers utilisent désormais l'IA générative pour identifier et exploiter plus facilement des automates industriels Siemens vulnérables. Le secteur de l'eau est particulièrement exposé, notamment les petites infrastructures aux moyens de cybersécurité limités. Cette menace illustre comment l'IA peut abaisser la barrière technique des cyberattaques contre des systèmes industriels essentiels. Usine Digitale

Le 2 juillet 2026, SOCRadar a attribué la campagne FortiBleed aux opérateurs de rançongiciel INC Ransom et Lynx. Cette campagne de vol d'identifiants, reposant sur un renifleur Golang ("FortiGate Sniffer"), aurait compromis plus de 430 000 pare-feu FortiGate et exposé plus de 110 millions d'identifiants.. Un opérateur lié à FortiBleed a été retrouvé connecté aux panneaux de négociation des deux groupes. La campagne aurait obtenu un accès administrateur sur 409 cibles, complété la chaîne d'attaque sur 354 d'entre elles et abouti à au moins 12 déploiements de rançongiciel. Le courtier en accès initial serait russe et compterait une vingtaine de membres. SOC Radar

La société Barracuda détecte une recrudescence d'attaques par hameçonnage utilisant le « text salting ». Cette technique consiste à injecter des mots inoffensifs dans les emails pour tromper les filtres utilisant l'IA et les LLM. Les attaquants masquent ces ajouts par la manipulation de texte, rendant le message illisible pour l'humain, mais interprété comme bénin par l'algorithme. Cette méthode contourne les défenses modernes qui ne distinguent pas toujours le texte visible du code source. The Register

Des acteurs malveillants ciblent les joueurs utilisant Steam à travers une campagne de ClickFix. Ces faux profils incitent les joueurs à exécuter des commandes PowerShell pour résoudre des bugs. Le script installe ensuite un faux utilitaire de maintenance pour masquer l'installation d'un mineur de cryptomonnaie (XMRig). Bleeping Computer

Réglementation

L'entrée en vigueur le 1er juillet 2026 de la taxe européenne sur les colis hors UE (<150 €) crée un terrain propice au phishing. Les attaquants exploitent la complexité du calcul des frais, appliqués par catégorie douanière et non par colis, générant une confusion légitime chez les consommateurs. Des messages urgents, imitant la douane ou les transporteurs, réclament des paiements infimes pour débloquer des envois. Cette approche vise à contourner la vigilance de la victime en demandant un montant réduit avant de soutirer des données bancaires et des identifiants. Numerama

La Commission européenne a saisi la Cour de justice de l'UE contre la France pour son retard dans la transposition de la directive NIS2, qui devait être intégrée au droit français avant le 17 octobre 2024. Ce texte renforce les obligations de cybersécurité et de notification des incidents pour les secteurs critiques. La France invoque notamment un désaccord sur l'interdiction des « backdoors » dans les services de chiffrement. Elle risque désormais une amende forfaitaire et des astreintes journalières jusqu'à la transposition complète. Le Monde Informatique

Le 4 août 2026, Boursorama rapporte que le gouvernement a renforcé le contrôle des investissements extra-européens dans des secteurs stratégiques, notamment la défense, la cybersécurité et l'IA. Publiés au Journal officiel le 2 août, deux textes permettent à Bercy de contrôler les investissements non-européens dans des entreprises françaises sensibles cotées hors de l'UE. Le seuil de contrôle est ainsi abaissé de 25 % à 10 % des droits de vote, quel que soit le marché réglementé sur lequel l'entreprise est cotée. Boursorama