RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# COMMUNIQUÉ DE PRESSE

Paris, le 11/03/2026

## Panorama de la cybermenace 2025 : la France sous la pression constante d'acteurs d'origines étatique et cybercriminelle

*Après une année 2024 caractérisée par l'organisation et la tenue des Jeux Olympiques et Paralympiques de Paris, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dresse son bilan 2025 dans la dernière édition de son « Panorama de la cybermenace ». Cette année est marquée par une pression qui demeure constante, posée par des attaquants d'origine étatique ou cybercriminelle, agissant tous à l'encontre d'une variété de cibles françaises.*

Au cours de l'année 2025, l'ANSSI a traité, avec différents niveaux de mobilisation, 3 586 événements de sécurité[1], soit une diminution de 18% par rapport à l'année précédente. Cette diminution peut s'expliquer par la tenue des Jeux Olympiques et Paralympiques à Paris, qui avait suscité un pic de signalements – événements sans gravité – entre les mois de mai et d'août 2024. En 2025, 1 366 incidents[2] ont été portés à la connaissance de l'Agence[3]. Malgré l'absence de grands événements sur le territoire français en 2025, cela représente un volume similaire à 2024 (1 361).

Particulièrement affectés, quatre secteurs d'activité concentrent 76% des incidents : l'Éducation et la recherche (34%), les ministères et les collectivités territoriales (24%), la santé (10%) et les télécommunications (9%). Cela confirme la tendance observée depuis plusieurs années, à savoir l'intérêt marqué des attaquants pour ces secteurs.

### Des motivations qui perdurent : espionnage, déstabilisation et extorsion de fonds

A l'instar des précédentes éditions du Panorama, l'ANSSI a encore régulièrement observé, à l'encontre des intérêts français, les activités des modes opératoires attaquants (MOA) réputés liés aux services de renseignement russes ou chinois, à des fins d'espionnage ou de pré-

[1] Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.
[2] Un incident est un évènement de sécurité où l'ANSSI est en mesure de confirmer qu'un acteur malveillant a conduit des actions avec succès sur le SI de la victime. À titre d'illustration, un déni de service avec impact ou la compromission de compte de messagerie rentrent dans cette catégorie.
[3] Il est à noter que ces chiffres correspondent à la vision de l'ANSSI consolidée par les signalements émis par ses bénéficiaires et ne peuvent, par conséquent, être pleinement représentatifs de l'ensemble des événements de sécurité qui touchent les différents secteurs d'activité en France.

positionnement en vue d'attaques ultérieures aux motivations inconnues. De même, l'Agence a constaté le maintien d'une pression de l'écosystème cybercriminel sur les entités françaises.

Dans un contexte de tensions géopolitiques qui s'intensifient, l'effort continu d'acteurs étatiques pour compromettre les réseaux des entités diplomatiques à des fins de collecte de renseignements stratégiques n'a pas faibli. De même, le ciblage d'infrastructures critiques - à l'image de celui des secteurs des télécommunications ou de l'énergie – avec la poursuite des tentatives de sabotage, reste aussi très prisé de ces acteurs. Evoqué fin 2025 dans un état de la menace dédié[4], le ciblage d'environnements mobiles, portant tant sur des équipements personnels que professionnels, témoigne quant à lui de capacités de recherche sophistiquées et d'une volonté d'atteindre un large panel d'utilisateurs.

En 2025, la menace cybercriminelle a perduré avec une augmentation significative du nombre d'incidents relatifs à des exfiltrations de données, et cela malgré un nombre d'attaques par rançongiciel en légère baisse[5]. Sur les 460 événements caractérisés comme possibles fuites de données[6], 42% ont pu être confirmées comme associées à des compromissions avérées, le reste étant soit des fausses revendications, soit du « recyclage » de données provenant de compromissions antérieures. A noter que le vol et la revente de données ne rapportent que quelques milliers d'euros maximum aux attaquants, alors que le coût de la réponse à incidents pour les victimes se chiffre, lui, à des dizaines voire centaines de milliers d'euros.

**Des frontières entre acteurs étatiques et cybercriminels qui s'érodent**

En 2025, l'émergence d'un brouillard technologique et organisationnel – volontairement utilisé comme levier tant par les attaquants étatiques que les cybercriminels – continue de s'installer. Cela résulte à la fois d'un partage de capacités plus prononcé entre ces acteurs, mais également de l'adoption croisée de pratiques qui, jusqu'à présent, caractérisaient davantage certains plus que d'autres. Cette tendance complique de facto le processus d'imputation car elle est associée à la répartition des tâches entre plusieurs acteurs, qui se spécialisent chacun sur certaines phases de la compromission.

Alors que l'ANSSI est obligée de regarder à travers un écran de fumée, les fuites de données ayant touché cette année des opérateurs de MOA réputés étatiques, des entreprises de lutte informatique offensive (LIO) ou des groupes cybercriminels, ont tout de même permis de mieux appréhender leur fonctionnement interne.

Comme les années précédentes, des équipements de sécurité de bordure ont été affectés par de nombreuses vulnérabilités. La compromission répétée de ces équipements a de nouveau

[4] Téléphones mobiles : État de la menace depuis 2015
[5] 128 compromissions en 2025 contre 144 en 2024
[6] Fuites de données signalées à l'ANSSI ou revendiquées par des attaquants

largement mobilisé les équipes de réponse à incident de l'Agence, soulignant de nouveau les multiples enjeux relatifs à la gestion des vulnérabilités.

Si ce constat illustre la nécessité de renforcer les dispositifs de cybersécurité nationaux et européens, notamment par la voie règlementaire, qui est un axe essentiel – avec la transposition de la directive NIS 2 ou l'entrée en vigueur du Cyber Resilience Act (CRA) – la mise en application de socles de mesures de sécurisation basiques reste essentielle et permettrait d'ores et déjà de mieux protéger des milliers d'organisations françaises.

*« L'année 2025 s'est terminée de manière alarmante sur une série d'attaques informatiques contre les infrastructures électriques polonaises, attaques coordonnées et à visée destructive. Cet évènement dresse le spectre du scénario redouté, auquel la France se prépare. Un scénario central dans lequel nous ferions face à une augmentation massive d'ici 2030 des attaques dites « hybrides », dont les cyberattaques constituent un pan majeur, avec des effets concrets voire destructeurs sur nos infrastructures critiques. Ce Panorama 2025 permet de mieux comprendre et d'anticiper ces cybermenaces pour nous doter d'outils efficaces afin de lutter contre leurs effets car oui, la France a les moyens de contrer, décourager ou au moins complexifier grandement la vie des attaquants. »* précise Vincent Strubel, directeur général de l'ANSSI.

**À PROPOS DE L'ANSSI**

Service du Premier ministre placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense en France. Elle a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

cyber.gouv.fr

**Contacts Presse**

presse@ssi.gouv.fr
06 49 21 63 80 / 06 49 87 30 36

Roxane ROSELL
roxane.rosell@ssi.gouv.fr