RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 11/03/2025

Panorama de la cybermenace 2024 : la France doit rester mobilisée et vigilante face à une pression omniprésente des attaquants

Dans son « Panorama de la cybermenace 2024 », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dresse le bilan d'une année marquée par une pression désormais constante posée par, d'une part, la menace systémique que représentent désormais les attaquants cybercriminels, et, d'autre part, la menace posée par les attaquants réputés liés à la Russie et la Chine pour les systèmes d'information les plus critiques de la Nation. Pour y faire face, l'ANSSI appelle l'ensemble des acteurs cyber français à maintenir leur mobilisation et leur vigilance de tous les instants qui ont permis le bon déroulement des Jeux olympiques et paralympiques de Paris 2024 (JOP).

Au cours de l'année 2024, l'ANSSI a traité, avec différents niveaux de mobilisation, 4 386 événements de sécurité[1], soit une augmentation de 15 % par rapport à l'année précédente. Ainsi, 3 004 signalements[2] et 1 361 incidents[3] ont été portés à la connaissance de l'Agence.

Trois principales menaces : cybercriminels, attaquants réputés liés à la Russie et attaquants réputés liés à la Chine

La menace portée par l'écosystème cybercriminel – principalement caractérisée par des attaques visant l'extorsion de rançons, *via* des fuites de données et des attaques par rançongiciel – s'est imposée comme un risque global et quotidien pour toutes les organisations françaises. Parmi les victimes de rançongiciels connues de l'ANSSI, les PME/TPE/ETI (37 %), les collectivités territoriales (17 %), les établissements d'enseignement supérieur (12 %) et les entreprises stratégiques (12 %) ont été plus particulièrement touchés, avec des conséquences souvent très graves sur leur fonctionnement, leur réputation et leur continuité d'activité.

[1] Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.
[2] Les signalements regroupent tous les comportements anormaux ou inattendus pouvant avoir un caractère malveillant ou ouvrir la voie à des usages néfastes à l'encontre d'un SI.
[3] 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 système d'information de la victime. À titre d'illustration, un déni de service avec impact ou la compromission de compte de messagerie rentrent dans cette catégorie.

Une hausse des attaques à but de déstabilisation a également été observée, généralement menées par des groupes dits « hacktivistes »[4] cherchant à attirer l'attention en mettant en œuvre des attaques de faible technicité mais à forte visibilité. Par exemple, les attaques par déni de service (DDoS) contre des cibles françaises ont doublé par rapport à 2023, avec une recrudescence pendant la période des Jeux. Malgré les conséquences limitées de ces dernières, le sabotage de petites installations industrielles a aussi été relevé. Ces attaques représentent une évolution vers une logique de sabotage, pour laquelle une vigilance s'impose.

À l'instar des années précédentes, ce sont les attaques à finalité d'espionnage qui ont le plus mobilisé les équipes opérationnelles de l'ANSSI. Les attaquants réputés liés aux intérêts stratégiques russes ont poursuivi leurs attaques guidées principalement par la recherche d'informations pouvant soutenir leurs efforts militaires ou diplomatiques. De son côté, l'activité associée aux modes opératoires réputés chinois a été particulièrement dense et répandue à des fins de captation de renseignements d'ordres stratégique et économique. Par ailleurs, le ciblage d'opérateurs de télécommunications s'est avéré intense et plusieurs incidents d'importance ont été traités par l'Agence.

Mobilisation et vigilance des acteurs français : l'héritage indispensable des Jeux

L'année 2024 a été marquée par l'organisation des JOP, dont l'exposition médiatique et la surface d'attaque ont constitué des opportunités majeures pour les acteurs malveillants. Cependant, aucune de ces attaques n'a porté atteinte au déroulement de l'événement grâce à la bonne préparation et la grande mobilisation des équipes de l'ANSSI et de l'ensemble de l'écosystème cyber français.

Outre des opportunités conjoncturelles comme les Jeux, les attaquants se saisissent de toutes les faiblesses techniques exposées par les systèmes d'information (SI). Face à ce niveau de sécurité insuffisant, l'Agence enjoint les organisations à durcir et maintenir en condition de sécurité leurs SI afin de réduire la surface d'attaque. En particulier, au regard du nombre et de l'impact des vulnérabilités affectant les équipements de sécurité situés en bordure de SI – qui ont représenté plus de la moitié des opérations de cyberdéfense de l'ANSSI – l'Agence rappelle la nécessité urgente d'appliquer les correctifs de sécurité et ce le plus rapidement possible afin de se protéger d'exploitations opportunistes.

L'ANSSI au cœur d'un collectif, pour une nation cyber-résiliente

[4] Groupes composés de militants numériques utilisant les attaques informatiques afin de promouvoir des causes politiques, sociales ou idéologiques.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

L'année écoulée a conforté l'Agence dans sa volonté de consolider un écosystème relai efficace. En effet, le renforcement des acteurs qui le composent, tels que les centres de réponse à incidents cyber (CSIRT) territoriaux, sectoriels ou ministériels, a déjà permis à l'ANSSI de concentrer son implication sur des attaques ayant des impacts plus critiques.

Face à l'ensemble de ces menaces, la France n'est pas désarmée : les travaux sur le volet cyber du projet de loi Résilience, visant à transposer la directive NIS 2 en France, constituent un pan essentiel de sa réponse. La démarche de co-construction choisie pour cette transposition a permis d'adapter au mieux le texte aux réalités et enjeux des entités afin d'en favoriser son appropriation et sa mise en œuvre.

Enfin, il apparaît indispensable pour l'ANSSI de maintenir la pression sur l'écosystème cybercriminel en poursuivant sa coopération avec les autres services de l'État et les partenaires internationaux. Cette coopération a notamment permis de réaliser des opérations de démantèlement sur l'année écoulée.

« Beaucoup pensaient que 2024 serait une année dramatique pour la cybersécurité française, mais les Jeux olympiques et paralympiques de Paris 2024 ont, au contraire, permis de démontrer que l'ANSSI et notre écosystème était à la hauteur des enjeux cyber nationaux et internationaux. Il serait toutefois malavisé de faire dans l'excès de confiance et de se reposer sur nos lauriers à l'heure où l'intensification des conflits invite plutôt à une mobilisation et une vigilance de tous les instants de la part de tous les acteurs français », conclut Vincent Strubel.

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