RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 27 février 2024

PANORAMA DE LA CYBERMENACE 2023 : UN NIVEAU GLOBAL DE CYBERSÉCURITÉ À ÉLEVER POUR FAIRE FACE À UNE MENACE ACCRUE

Dans son « Panorama de la cybermenace 2023 », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) fait état d'un niveau de la menace informatique en constante augmentation, dans un contexte marqué par de nouvelles tensions géopolitiques et la tenue d'événements internationaux sur le sol français. À l'heure où les attaquants ne cessent de s'améliorer et de saisir toutes les opportunités, l'ANSSI appelle plus que jamais à une meilleure application des recommandations de première nécessité.

Un regain net du niveau de la menace cyber pesant sur la France

En 2023, l'espionnage s'est maintenu à un niveau élevé avec une augmentation significative du ciblage des individus et des structures non gouvernementales qui créent, hébergent ou transmettent des données sensibles. Parmi les tendances nouvelles de l'espionnage, l'ANSSI a constaté une augmentation des attaques contre des téléphones portables professionnels et personnels visant des individus ciblés, ainsi qu'une recrudescence de celles réalisées au moyen de modes opératoires associés publiquement au gouvernement russe contre des organisations situées en France.

Les attaques informatiques à des fins d'extorsion se sont également maintenues à un niveau élevé en 2023, comme en témoigne le nombre total d'attaques par rançongiciel portées à la connaissance de l'ANSSI, supérieur de 30 % à celui relevé sur la même période en 2022. Une recrudescence qui rompt avec la diminution observée par l'agence dans son précédent Panorama de la cybermenace. En 2023, 3 703 évènements de sécurité[1] (contre 3 018 en 2022) ont été portés à la connaissance de l'ANSSI dont 1 112 concernaient des incidents[2] (contre 832 en 2022).

Par ailleurs, dans un contexte géopolitique tendu, l'ANSSI a constaté de nouvelles opérations de déstabilisation visant principalement à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation. Si les attaques par déni de service distribué (DDoS) menées par des hacktivistes pro-russes, aux impacts souvent limités, ont été les plus courantes, des activités de prépositionnement visant plusieurs infrastructures critiques situées en Europe, en Amérique du Nord et en Asie ont également été détectées. Ces dernières, plus discrètes, peuvent néanmoins avoir pour objectif la conduite d'opérations de plus grande envergure menées par des acteurs étatiques attendant le moment opportun pour agir.

« Si les attaques à but lucratif et les opérations de déstabilisation ont connu un net regain en 2023, c'est encore une fois la menace moins bruyante, qui reste la plus préoccupante, celle de l'espionnage stratégique et industriel ainsi que du prépositionnement à des fins de sabotage, qui a le plus mobilisée les équipes de l'ANSSI », déclare Vincent Strubel, directeur général de l'ANSSI.

Des attaquants qui s'améliorent, profitent des faiblesses techniques et saisissent toutes les opportunités

De manière générale, l'année 2023 a montré des évolutions notables dans la structure et les méthodes des attaquants. Ces derniers perfectionnent leurs techniques afin d'éviter d'être détectés et suivis, voire identifiés. Il apparaît notamment que des modes opératoires cybercriminels pourraient être instrumentalisés par des acteurs étatiques pour conduire des opérations d'espionnage. De plus, l'écosystème cybercriminel profite aujourd'hui d'outils et de méthodes diffusés largement pour cibler des secteurs particulièrement vulnérables.

Malgré les efforts de sécurisation engagés dans certains secteurs, les attaquants continuent de tirer profit des mêmes faiblesses techniques pour s'introduire sur les réseaux. Ainsi, l'exploitation de vulnérabilités « jour-zéro » et « jour-un » reste une porte d'entrée de choix pour les attaquants, qui profitent encore trop souvent de mauvaises pratiques d'administration, de retards dans l'application de correctifs et de l'absence de mécanismes de chiffrement.

Enfin, les grands événements prévus en France en 2024, et en premier lieu les Jeux olympiques et paralympiques (JOP) de Paris, pourraient offrir aux attaquants des opportunités supplémentaires d'agir. De même, des attaquants pourraient également être incités à s'introduire et à se maintenir sur des réseaux d'importance critique, dans le cadre de tensions internationales. Un risque d'affrontement stratégique entre grandes puissances n'est également pas à exclure.

« L'un des grands enseignements de ce Panorama de la cybermenace 2023 est qu'il n'est désormais plus possible de prendre du retard en matière de cybersécurité, face à des attaquants de plus en plus persévérants », estime Vincent Strubel.

L'ANSSI toujours plus mobilisée pour élever le niveau global de cybersécurité du territoire français

L'ANSSI appelle les organisations françaises à une meilleure application des recommandations indispensables telles que le développement de capacités de détection, la mise en place d'une stratégie de sauvegarde des systèmes d'information, ou bien encore l'élaboration de plans de continuité et de reprise d'activité. Par ailleurs, le suivi régulier des publications du CERT-FR sur les menaces et les vulnérabilités les plus courantes s'impose comme une ressource indispensable pour atteindre le bon niveau de cybersécurité.

En 2024, l'ANSSI sera en grande partie mobilisée sur la cybersécurité des JOP, pour lesquels l'agence a défini, en coopération avec les différents services de l'État impliqués, un dispositif renforcé de veille, d'alerte et de traitement des incidents de sécurité informatique.

Enfin, pour assurer la protection de la Nation dans les années à venir et faire face à la recrudescence constante des menaces et à l'amélioration continue des attaquants, l'ANSSI entend s'appuyer sur l'entrée en vigueur cette année de la directive NIS 2, qui permettra de réguler plusieurs milliers de nouvelles entités et de renforcer progressivement leur sécurité informatique. De plus, l'agence entend continuer à apporter son soutien aux opérations internationales visant à démanteler des réseaux cybercriminels, à l'image de celle menée à l'encontre du groupe QakBot en 2023.

« Le développement constant de la menace et des attaquants démontre la nécessité pour l'ANSSI de faire évoluer sa manière de travailler, en collaborant notamment avec de nouveaux acteurs, afin de mieux organiser et de renforcer la cybersécurité française », conclue Vincent Strubel.

1 : Un évènement de sécurité est un évènement porté à la connaissance de l'ANSSI et qui a 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 malveillantes avec succès sur le système d'information de la victime. A titre d'illustration, un déni de service avec impact ou la compromission de compte de messagerie rentrent dans cette catégorie.

À PROPOS DE L'ANSSI

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

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75007 PARIS 07 SP
cyber.gouv.fr

À PROPOS DU CERT-FR

Par le biais du CERT-FR, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) assure ses fonctions de centre de réponse à incident cyber (CSIRT) national et gouvernemental. Le CERT-FR est le point de contact privilégié aux plans national et international pour tout incident cyber affectant la France. Il assure une permanence de ses missions H24 7j/7.
www.cert.ssi.gouv.fr

Contacts Presse

presse@ssi.gouv.fr
06 49 21 63 80

Roxane ROSELL
roxane.rosell@ssi.gouv.fr

Leïla LEGRAND
leila.legrand@ssi.gouv.fr

Victor PLOUÉ
victor.ploue@ssi.gouv.fr