RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 24/01/2023

UN NIVEAU ÉLEVÉ DE CYBERMENACES EN 2022

Dans son « Panorama de la cybermenace 2022 », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) fait état des grandes tendances de la menace cyber ayant rythmé 2022. Les tendances observées l'année précédente se sont confirmées et ce malgré l'intensification du conflit russo-ukrainien et de ses effets dans le cyberespace.

Avec un niveau général qui reste élevé, l'ANSSI constate que cette menace touche de moins en moins d'opérateurs régulés et se déporte sur des entités moins bien protégées. Si le nombre d'attaques par rançongiciel portées à la connaissance de l'ANSSI a diminué, la menace d'espionnage informatique demeure prégnante, ayant de nouveau fortement mobilisé les équipes de l'agence.

Des objectifs principaux qui demeurent le gain financier, l'espionnage et la déstabilisation

Après une accalmie lors du premier semestre, la menace cybercriminelle et plus spécifiquement celle liée aux rançongiciels a connu un regain d'activités fin 2022, se maintenant alors à un niveau élevé. Cette menace cybercriminelle touche particulièrement les TPE, PME et ETI (40 % des rançongiciels traités ou rapportés à l'ANSSI en 2022), les collectivités territoriales (23 %) et les établissements publics de santé (10 %). Plus furtif qu'auparavant, le cryptominage, qui permet de générer des fonds importants, réinvestis par les acteurs malveillants pour acquérir de nouvelles capacités, ne doit pas non plus être négligé.
A l'image de l'année précédente, la menace d'espionnage informatique est celle qui a le plus mobilisé les équipes de l'ANSSI. Près de la moitié des opérations de cyberdéfense de l'agence en 2022 impliquaient des modes opératoires associés en source ouverte à la Chine. Répétées, ces intrusions démontrent une volonté soutenue de s'introduire dans les réseaux d'entités françaises stratégiques.
L'invasion russe de l'Ukraine a généré un contexte favorable à l'augmentation d'actions de déstabilisation en Europe. L'ANSSI a observé des attaques par déni de service distribué, par sabotage informatique ainsi que des opérations informationnelles s'appuyant sur des compromissions de systèmes d'information. Si les attaques par sabotage se sont jusqu'à présent relativement limitées à l'Ukraine, l'évolution du conflit et ses conséquences économiques appellent à une vigilance particulière, notamment dans le secteur de l'énergie.

Des faiblesses persistantes sans cesse exploitées

Les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données continuent d'offrir de trop nombreuses opportunités aux attaquants. Le recours au *cloud* et l'externalisation de services auprès d'entreprises de services numériques, lorsqu'ils ne s'accompagnent pas de clauses de cybersécurité adaptées, représentent une menace sérieuse.
Bien que le nombre d'attaques ciblant la chaine d'approvisionnement ou *supply chain* en 2022 ait quelque peu baissé, cette tendance reste forte et souligne un risque systémique.
Enfin, les correctifs sur les vulnérabilités découvertes ne sont pas suffisamment appliqués à temps par les organisations, laissant alors le champ libre aux attaquants pour les exploiter.

Des attaquants toujours plus performants

Comme déjà observé précédemment, différents profils d'attaquants continuent à user d'outils et de techniques similaires. Cette porosité complexifie la caractérisation et l'imputation des activités malveillantes. Les attaquants étatiques s'inspirent des méthodes cybercriminelles et utilisent de plus en plus de rançongiciels à des fins de déstabilisation dans le cadre d'opérations de sabotage informatique.
Le ciblage des attaquants évolue, cherchant désormais à obtenir des accès discrets et pérennes aux réseaux de leurs victimes avec la compromission d'équipements périphériques (pare-feu ou routeurs). Ce ciblage périphérique se retrouve également dans le type d'entités compromises et confirme l'intérêt des attaquants pour les prestataires, les fournisseurs, les sous-traitants, les organismes de tutelle et l'écosystème plus large de leurs cibles.

Des solutions pour y faire face

Face à ces menaces, les établissements privés comme publics se doivent de prendre conscience du risque cyber à son juste niveau en adoptant les bonnes mesures pour se protéger. Afin de se prémunir des menaces les plus courantes, l'application rigoureuse d'une politique de mise à jour et du guide d'hygiène informatique, une sensibilisation régulière des collaborateurs et le développement de capacités de détection et de traitement d'incident sont indispensables. Des recommandations sont disponibles sur le site de l'ANSSI et l'actualité opérationnelle et les alertes cyber sont accessibles sur le site du CERT-FR.

Par ailleurs, la transposition de la nouvelle directive *Network and information system security* (NIS 2) en droit français au deuxième semestre 2024, au plus tard, va permettre d'élever le niveau de cybersécurité de milliers d'entités, allant de la PME aux entreprises du CAC40, sur a minima 18 secteurs d'activité.

« Ce Panorama de la cybermenace met en lumière une menace cyber qui s'est maintenue à un niveau élevé en 2022. Alors que la France se prépare à accueillir des événements majeurs tels que la Coupe du monde de rugby en 2023 et les Jeux olympiques et paralympiques de Paris en 2024, nous devons renforcer la vigilance et la responsabilité de chacun, pour faire face tous ensemble à cette menace. » déclare Vincent Strubel, directeur général de l'ANSSI.

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 assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

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

www.ssi.gouv.fr - presse@ssi.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 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

Roxane ROSELL
roxane.rosell@ssi.gouv.fr
06 49 21 63 80

presse@ssi.gouv.fr