RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 09/03/2022

UNE ANNÉE 2021 MARQUÉE PAR LA PROFESSIONNALISATION DES ACTEURS MALVEILLANTS

Dans son "Panorama de la menace informatique", l'Agence nationale de la sécurité des systèmes d'information (ANSSI) revient sur les grandes tendances ayant marqué le paysage cyber en 2021 et souligne des risques d'évolution à court terme.

Alors que la généralisation des usages numériques - souvent mal maitrisés – continue de représenter un défi pour les entreprises et les administrations, l'agence observe une amélioration constante des capacités des acteurs malveillants. Ainsi, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37% entre 2020 et 2021 (786 en 2020 contre 1082 en 2021, soit désormais près de 3 intrusions avérées par jour).

Des cyberattaques nombreuses aux finalités diverses : gains financiers, espionnage, déstabilisation, sabotage, …

Alors que les années 2019 et 2020 avaient été marquées par une explosion des rançongiciels, cette menace s'est stabilisée, à un niveau néanmoins très élevé, entre 2020 et 2021, avec 203 attaques traitées contre 192 en 2020. Entitées touchées en premier lieu par les rançongiciels, les TPE, PME et ETI représentent 34% des victimes en 2021 (+53% par rapport à 2020) et sont suivies par les collectivités (19%) et les entreprises stratégiques (10%).

Ces attaques à finalité lucrative qui ont occupé le devant de la scène médiatique ne doivent pas occulter les campagnes d'espionnage et de sabotage, particulièrement préoccupantes. Les opérations d'espionnage informatique restent en effet la principale finalité poursuivie par les attaquants réputés étatiques et constituent l'essentiel de l'activité traitée dans le cadre des opérations de cyberdéfense conduites par l'ANSSI. Cette menace concerne autant les acteurs institutionnels que les acteurs privés.

Le ciblage d'infrastructures critiques est également une préoccupation majeure. Certes, les cybercriminels réduisent leur ciblage d'infrastructures critiques afin de gagner en discrétion et de moins s'exposer à des mesures répressives des Etats. Toutefois, le ciblage d'infrastructures critiques par des acteurs de niveau étatique continue, plus particulièrement dans le cadre de tensions géopolitiques exacerbées.

Enfin, l'ANSSI constate que de plus en plus d'actions de déstabilisation débutent par des compromissions informatiques. Ces dernières permettent ainsi d'exfiltrer des documents qui peuvent être divulgués en l'état, voire modifiés pour déstabiliser une organisation, une personnalité exposée ou encore un État. 39 divulgations de données à des fins de déstabilisation ont été signalées à l'ANSSI en 2021.

De failles de mieux en mieux exploitées

Malgré les publications sur les vulnérabilités découvertes, les organisations qui n'appliquent pas à temps les correctifs restent trop nombreuses. Cela laisse le champ libre aux attaquants pour les exploiter. L'année 2021 a connu une explosion du nombre de vulnérabilités 0-Day exploitées, utilisées en majorité par des acteurs présumés étatiques mais également par quelques groupes cybercriminels.

Les attaques ciblant la chaine d'approvisionnement (*supply chain*), continuent de croître, avec plus de 24 attaques documentées, entre janvier 2020 et juillet 2021, d'après l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Constat partagé par l'ANSSI qui a traité 18 compromissions affectant des entreprises de service numérique (ESN) en 2021 contre 4 en 2020. Ce ciblage accru des fournisseurs de services numériques présente des risques nouveaux puisque leurs outils numériques peuvent devenir des vecteurs de propagation rapide d'une cyberattaque et entraîner des compromission en cascade.

Les nouveaux usages numériques comme le Cloud sont également exploités par les cyberattaquants. La crise sanitaire ayant accéléré son usage dans les secteurs public et privé, l'utilisation généralisée du Cloud augmente mécaniquement le niveau de menace et la surface d'attaque. En effet, des défauts de sécurisation des données sont encore trop souvent constatés dans l'activité opérationnelle de l'ANSSI.

Enfin, la multiplication des divulgations de données facilite la conduite de nombreuses attaques informatiques. En effet, les données exfiltrées contiennent fréquemment des données d'authentification sur des systèmes d'information et fournissent donc une porte d'entrée idéale aux attaquants opportunistes. Le renforcement de la cybersécurité de ces données doit donc être une priorité.

Des attaquants de plus en plus performants

Dans le domaine de la cybercriminalité, la spécialisation et la professionnalisation des attaquants s'explique notamment par les gains financiers accumulés. Un véritable écosystème cybercriminel aux ressources considérables s'est ainsi progressivement constitué et perfectionné, ce qui lui permet de conduire des attaques sophistiquées. Aussi, les cybercriminels adoptent maintenant les modes opératoires habituels des attaquants réputés étatiques : préparation minutieuse de leurs opérations, persistance sur les réseaux des victimes, recherche de ressources d'intérêt, exploitation de vulnérabilités inconnues (ou 0-Day) ou connues mais dont les correctifs n'ont pas encore été appliqués sur les systèmes des potentielles victimes.

Quant aux cyberattaquants réputés étatiques, leurs compétences ne cessent de se développer, tout comme leur furtivité. En effet, pour mieux dissimuler leurs actions, les attaquants réputés étatiques s'inspirent directement des méthodes cybercriminelles en s'appropriant des codes et outils, traditionnellement utilisés à des fins lucratives tels que des rançongiciels ou des logiciels d'hameçonnage. Outre une rationalisation des coûts, cela permet aux Etats de nier de façon plausible toute implication.

Cette convergence des méthodes et outils utilisés par plusieurs profils d'acteurs malveillants complexifie la caractérisation précise des activités malveillantes et limite donc les possibilités d'imputation à des acteurs identifiés.

Enfin, le développement de capacités par les entreprises privées spécialisées participe directement à l'amélioration des capacités offensives d'acteurs n'ayant pas les moyens de les développer en interne ou ne souhaitant pas s'exposer directement. Cette mise à disposition de capacités avancées participe ainsi à la hausse générale du niveau de menace en multipliant ses sources et en favorisant un ciblage décomplexé.

Devenus l'affaire de tous, les cyberattaques n'épargnent aucun secteur d'activité. Tous les acteurs, qu'ils soient publics ou privés ont la main sur tous les outils pour y faire face : mettre en œuvre les mesures de cybersécurité adaptées, élever leur niveau de vigilance, sensibiliser leurs collaborateurs aux risques et s'exercer à la réaction en cas d'attaque. Afin d'endiguer les cyberattaques et de protéger leur activité et leurs données, il est, plus que jamais, essentiel que les organisations consentent les investissements, humains et financiers, nécessaires à leur sécurisation.

« *Ce panorama met en lumière une menace complexe, professionnelle, aux intentions hétérogènes et en perpétuelle évolution. Notre travail de sensibilisation et d'accompagnement, auprès des entreprises et des administrations, a pour objectif d'élever, au sein de toute la Nation, la prise en compte du risque cyber au juste niveau, ce qui n'est pas encore le cas. A l'aune d'évènements majeurs tels que les élections qui se tiennent de cette année et des tensions internationales actuelles, la responsabilisation et la vigilance accrue de toutes les parties prenantes est indispensable pour faire face à cette menace.* » commente Guillaume Poupard, 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 - communication@ssi.gouv.fr

Contacts Presse

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

presse@ssi.gouv.fr