RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Paris, le 25/11/2021

LA MENACE DES ATTAQUES PAR RANCONGICIELS EN FRANCE ET EN ALLEMAGNE VUE PAR L'ANSSI ET LE BSI

Avec le « Common Situational Picture » - rapport franco-allemand sur la menace cyber partagée de part et d'autre du Rhin - l'ANSSI et le BSI dressent le panorama de la menace grandissante des rançongiciels et sensibilisent aux risques et défis qu'ils représentent pour les entreprises et les institutions.

Pour la 4ème édition du « *Common Situational Picture* », l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et son homologue, le Bundesamt für Sicherheit in der Informationstechnik1 (BSI) font le constat d'une recrudescence des attaques par rançongiciels. Entre 2019 et 2020, en France, le nombre d'attaques a augmenté de 255%. Menace informatique la plus sérieuse pour les entreprises et les institutions, par le nombre d'attaques quotidiennes et leur impact sur la continuité d'activité, les rançongiciels visent particulièrement, depuis 2020, les secteurs de la santé et de l'éducation, les collectivités territoriales ainsi que les prestataires de services numériques.

Panorama de la menace des rançongiciels : des tendances inquiétantes

Si initialement les rançongiciels ciblaient les particuliers avec des demandes de rançons peu élevées, de plus en plus de groupes cybercriminels aux ressources financières et aux compétences techniques importantes ciblent des entreprises et institutions de grande taille en capacité de payer des rançons significatives. Ces attaques dites « *Big Game Hunting* » visent des organisations aux activités critiques en France et en Allemagne. Elles affectent leurs réseaux pour générer une interruption de leur activité avec des conséquences économiques, industrielles et sociales importantes : perte d'exploitation, exfiltration de données confidentielles pouvant affecter leur réputation ou des opérations de fusion et d'acquisition, etc.

Le ciblage des cybercriminels se caractérise par une préparation des opérations d'extorsion en amont, parfois plusieurs mois à l'avance et, de plus en plus fréquemment, par un chantage à la divulgation de données sensibles exfiltrées lors de la cyberattaque. Cette méthode qui consiste à annoncer publiquement l'attaque permet d'exercer une pression supplémentaire sur les victimes. En cas de refus d'obtempérer, les cybercriminels publient alors les informations sensibles volées. Dans d'autres cas, ils tentent de les vendre, parfois en les mettant aux enchères.

Certaines attaques par rançongiciel ne peuvent plus être reléguées au rang de simples attaques à but lucratif. En

[1] Office fédéral de la sécurité des technologies de l'information

effet, leur sophistication, leur impact sur les données sensibles de la victime et la perte de continuité des activités les élèvent au niveau des attaques traditionnellement associées à des groupes d'attaquants étatiques. Les rançongiciels peuvent en outre être utilisés pour d'autres motivations que l'extorsion financière, notamment à des fins de protestation, de déstabilisation, de sabotage ou d'espionnage informatique.

Fort de nombreuses années de coopération intense et régulière, le « *Common Situational Picture* » s'inscrit dans la volonté commune de l'ANSSI et du BSI de renforcer la cybersécurité en France, en Allemagne et dans l'ensemble de l'espace numérique européen.

Lutte contre les rançongiciels : une priorité pour l'ANSSI et le BSI

Plus que jamais, la coopération étroite entre l'ANSSI et le BSI revêt une importance décisive.

« Bien plus qu'un simple outil rentable du crime organisé, l'attaque par rançongiciel peut avoir des effets dignes d'actes de sabotage ciblés. Autour de ce type d'attaque se forment des écosystèmes entiers de services et de plateformes. Leur effet ? Toucher n'importe qui, n'importe où. Les grandes entreprises sont particulièrement visées via des attaques dites de *Big Game Hunting*. Nous avons donc besoin d'un effort commun et international afin de continuer à élever le niveau de sécurité informatique au sein des infrastructures économiques, administratives et de santé. Cette coopération avec l'ANSSI répond à ce besoin essentiel », explique Arne Schönbohm, président du BSI.

« Face au volume et à la sophistication des attaques par rançongiciel, l'ANSSI et l'écosystème français sont entièrement mobilisés. A l'heure où la menace se globalise, la coopération internationale s'impose plus que jamais comme une nécessité. Nous devons continuer à travailler aux côtés de nos homologues européens, tel que le BSI, afin de contribuer à la stabilité du cyberespace.» indique notamment Guillaume Poupard, Directeur général de l'ANSSI.

Grâce aux premiers retours d'expérience et afin d'apporter une réponse à la menace par rançongiciels, l'ANSSI et le BSI continuent d'orienter leurs actions selon quatre axes clés :

- Sensibiliser le public sur les attaques par rançongiciel et leurs conséquences.
- Soutenir la collaboration entre acteurs publics et privés, via la certification de produits et services de sécurité, afin de détecter de potentielles vulnérabilités et menaces sur les systèmes critiques.
- Apporter une aide et une assistance immédiate aux victimes en cas de cyberattaques.
- Renforcer la coopération internationale pour permettre le développement d'un cyberespace sûr, stable et ouvert.

Télécharger le rapport

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

Contacts Presse

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

presse@ssi.gouv.fr