La complexité des attaques au rancongiciel inquiète le gendarme français de la sécurité informatique

Gardienne de la sécurité informatique française, l’Anssi tire la sonnette d'alarme à propos des nombreuses attaques au rancongiciel, de plus en plus sophistiquées, détectées ces derniers temps.

Temps de lecture : minute

8 février 2021

Les cyber attaques au rancongiciel - logiciel malveillant d’extorsion qui prend en otage des données personnelles - ne peuvent plus "*être reléguées au rang de simples attaques à visée lucrative*" , prévient l’Anssi, agence nationale de sécurité des systèmes d’information. "*Leur sophistication, leur intérêt pour les données de la victime ainsi que la perte de continuité d'activité qu'elles engendrent les rapprochent d'attaques à visée d'espionnage ou de sabotage mises en oeuvre par des attaquants de niveau étatique*" , souligne cette autorité dans une note technique de 34 pages rassemblant les informations publiquement disponibles sur ce sujet, vendredi dernier.

"*Les attaques à l'encontre d'hôpitaux montrent qu'une attaque par rançongiciel peut avoir des conséquences pour les patients dans le monde réel, en mettant leur vie en danger*" , écrit-elle. Les attaques contre les entreprises de services informatiques font planer le risque d'une "*déstabilisation de plusieurs grands groupes*" , voir d'un "*pan d'activité économique tout entier*" via certaines entreprises-clés, ajoute-t-

elle.

Des rançons de plusieurs millions de dollars

Début janvier, le directeur général de l'Anssi, Guillaume Poupard avait révélé que l'Anssi avait multiplié par quatre en 2021 le nombre de ses interventions dans des entreprises ou institutions frappées par des rançongiciels. Les attaques sont de plus en plus sophistiquées, avec des demandes de rançons se chiffrant parfois en millions de dollars, rappelle la note de l'Anssi publiée vendredi. "*Le montant d'une rançon (du groupe) DarkSide peut osciller entre 200 000 et deux millions de dollars, tandis qu'une rançon (du groupe) WastedLocker peut osciller entre 500 000 et 14 000 dollars*" , selon le document.

Les criminels à l'origine des attaques font partie de réseaux de plus en plus professionnalisés, avec des rançongiciels mis à disposition sous forme de logiciel à la demande (Raas, Ransomware as a Service). Dans ce modèle, l'agresseur a accès "*sous forme d'abonnement ou de partenariat à un rançongiciel, ses infrastructures de paiement et de distribution, ainsi qu'à un ensemble de services de back-office (support technique, interface d'échange avec les victimes...)*" , note l'Anssi.

Article écrit par AFP, avec Maddyness