Après une année d'accalmie, la menace "cyber" repart de plus belle

Emile Marzolf

Image d'illustration générée par Midjourney.

Ce n'était que partie remise. Après le déclenchement de la guerre en Ukraine en 2022, les cyber-attaquants, très souvent basés en Russie, s'étaient concentrés sur ce conflit, qui avait d'ailleurs provoqué l'éclatement d'un important groupe de hackers russo-ukrainiens : Conti. Le conflit avait conduit à une baisse de 20% des incidents de sécurité signalés en France à l'Agence nationale de sécurité des systèmes d'information, l'Anssi. Deux ans après, les cyberattaques reprennent de plus belle. *"Nous constatons en 2023 une augmentation de la menace en quantité comme en qualité, et dans toutes ses composantes, qu'il s'agisse d'espionnage, d'extorsion de fonds ou de déstabilisation et de sabotage. Les attaquants s'améliorent en termes de capacité, de furtivité et d'agilité",* a résumé le directeur général de l'Anssi, Vincent Strubel, lors d'une présentation du "panorama de la cybermenace" pour l'année 2023. Au total, le nombre d'incidents de sécurité signalés et traités par l'agence a bondi de plus de 30%, pour passer de 832 incidents en 2022 à 1112 l'an dernier. En cause, notamment, la recrudescence des attaques par rançongiciels, après une baisse notable en 2022, qui regrimpent elles aussi de 30%. Ces rançongiciels servent soit à verrouiller les données d'une structure et à ne promettre leur libération que contre paiement d'une rançon, soit à les exfiltrer en menaçant de les publier en ligne, soit les deux à la fois.

Et à ce petit jeu, les collectivités ne sont pas les mieux loties. Elles représentent même désormais 24% des victimes de rançongiciels, juste derrière les petites et moyennes entreprises (34% des victimes, contre 40% en 2022). En 2021, les collectivités ne représentaient que 19% des victimes. Bien qu'ils fassent régulièrement la Une, les hôpitaux ne représentent toujours que 10% des victimes de rançongiciels, comme en 2022. L'Anssi rappelle néanmoins l'importance, pour les établissements de santé, de ne pas négliger leur cybersécurité. *"Le CHU de Brest, qui a pu mettre en œuvre rapidement des mesures d'endiguement, après sa compromission du 9 mars 2023, n'a été pertubé dans son fonctionnement que pendant plusieurs semaines et non plusieurs mois. A Dax, 18 mois après l'attaque, certains systèmes ne sont toujours pas reconstruits",* a donné pour exemple le sous-directeur des opérations, Mathieu Feuillet.

Une nouveauté, par contre, les associations rejoignent la typologie des structures ciblées par des attaquants toujours mieux outillés et organisés. *"Les acteurs du rançongiciel sont plus industrialisés que jamais, aussi bien en termes économiques que de spécialisation", a* expliqué Vincent Strubel, qui n'hésite pas à parler de "fast-foods" du rançongiciel, avec une organisation en franchises, qui contribue chacun à des campagnes massives d'attaques qui visent simplement les plus cibles les plus faciles. Ce qui n'empêche pas les autorités de parvenir à leur mettre des bâtons

dans les roues, comme en témoigne la vaste opération menée en entre plusieurs pays, dont la France, pour mettre à bas l'infrastructure du très actif groupe LockBit. *"Ce types d'actions de démantèlement et de coopérations internationales ont une certaine efficacité pour perturber ces groupes, et faire retomber la pression, au moins pour un certain temps",* a assuré Vincent Strubel, tout en reconnaissant que les hackers sauront rapidement se remettre sur pied, ces-derniers n'étant pas inquiétés par la justice dans leur pays de résidence, comme, au hasard, la Russie.

Opérations d'espionnage et risques de sabotage

Les opérations d'espionnage, dont le traitement occupe toujours la majorité du temps des agents de l'Anssi, restent à un niveau stable mais très élevé, dû notamment au retour en force - juste derrière les acteurs affiliés à Chine - des acteurs affiliés à la Russie *"qu'on avait vus occupés ailleurs en 2022",* a exposé Vincent Strubel. *"L'activité 2023 a été forte, notamment sur les données sensibles de la diplomatie, la défense, et l'industrie"*. Néanmoins les cibles ont quelque peu évolué, avec une attention toujours forte sur les données de l'administration et des entreprises stratégiques, mais aussi, désormais, sur les cercles de réflexion et autres think tank, ainsi que les organismes de recherche. Par ailleurs, les attaquants n'hésitent plus à s'en prendre à plusieurs reprises à la même cible, quitte à devoir exploiter des failles de plus en plus étroites.

Mais ce qui inquiète le plus l'Agence, ce ne sont pas ces opérations d'espionnage, très discrètes, mais la tendance, nouvelle, chez les acteurs étatiques ou para-étatiques, à réaliser des opérations plus sophistiquées de sabotage, par seulement pour espionner ou déstabiliser, mais pour détruire "*aussi bien numériquement que physiquement"* certaines infrastructures critiques. "*Ce que l'on observe en France, ce n'est pas encore du sabotage, mais du prépositionnement, c'est-à-dire la prise en main de certains systèmes et infrastructures, pour y rester et pouvoir déclencher une action le moment venu",* a reposé Vincent Strubel. Le directeur pointe sans ambage l'"*agressivité désinhibée"* des acteurs affiliés à la Russie, désormais prêts à emprunter les méthodes des cybercriminels intéressés par l'argent, pour déstabiliser ou mettre à plat les systèmes d'information de structures stratégiques, publiques ou privées. Et à l'approche des Jeux Olympiques de Paris, l'Agence s'attend et se prépare depuis plus d'un an à ce que la France soit particulièrement visée dans les prochains mois.