RÉPUBLIQUE FRANÇAISE

Vie publique
Au cœur du débat public

Cybermenaces : quels sont les risques pour la sécurité informatique en France ?

Publié le 7 mars 2024
3 minutes
Par : La Rédaction

Dans son panorama 2023, l'Agence nationale de la sécurité des systèmes d'information (Anssi) fait état d'une menace informatique qui "continue d'augmenter" dans un contexte de tensions géopolitiques et d'évènements internationaux organisés sur le sol français.

Selon le *Panorama de la cybermenace 2023* , la **Russie**, la **Chine** et l'**écosystème cybercriminel** constituent les **principales menaces sur les systèmes d'information (SI) critiques**, ainsi que pour "*l'écosystème national de manière systémique.*"

Les différents types de cybermenaces

L'**espionnage informatique**, visant à soutirer des données sensibles, s'est maintenu à un niveau élevé en 2023. Des entités travaillant dans des domaines stratégiques et industriels, ou perçues comme proches de l'État français, sont ciblées. Les attaques réalisées "*au moyen de modes opératoires associés publiquement au gouvernement russe*" se sont multipliées.

Les attaques informatiques à des fins d'**extorsion *via* des rançongiciels** ont connu une **hausse de 30% en 2023**, après une baisse l'année précédente. Du fait de la diffusion en *open source* du code source, même des acteurs techniquement peu compétents peuvent se livrer à des opérations représentant une menace importante pour "*des entités particulièrement sensibles aux interruptions de service*" (énergie, santé notamment).

Certaines opérations de **déstabilisation** comme des attaques DDoS (déni de service), ayant pour objectif de "*promouvoir un discours politique*" ou rendre des sites inaccessibles, d'effet limité, ont été attribuées à des hacktivistes prorusses "*très réactifs à l'actualité"*.

Des modes opératoires variés

Le Panorama relève la **recrudescence des attaques contre des téléphones**, privés ou professionnels, ciblant principalement des personnalités publiques et de hauts dirigeants. Bien qu'historiquement liées à des États "*possédant des capacités offensives avancées*", les attaques témoignent désormais d'un essor du marché privé de la surveillance. Des entreprises commercialisent des codes malveillants "*très perfectionnés*" à des particuliers ou des entités privées.

Le **prépositionnement** désigne des tentatives de prise de contrôle d'un réseau pour pouvoir l'éteindre ou le détruire à un moment opportun. Des infrastructures critiques (énergie, transport, télécommunications…) sont ciblées lors d'attaques qui ne sont pas nécessairement détectées.

Les attaquants améliorent leur savoir-faire, mais ils continuent de profiter des **faiblesses techniques des réseaux visés**. Ainsi, si des failles sont toujours exploitées, c'est qu'il est possible de tirer profit des "*mauvaises pratiques d'administration*" (retard de déploiement de correctifs, absence de mécanismes de chiffrement…).