# Cybersécurité : à quelles menaces faut-il s'attendre en 2024 ?

*Prompt injection, augmentation des attaques ciblées, avènement du quishing… Zakaria Rachid, CISO de Believe et ex-CISO de Leboncoin.fr, et François Deruty, chief intelligence officer chez Sekoia.io, font le point sur la menace cyber qui plane sur 2024.*

Temps de lecture : minute

*9 janvier 2024*

Appât du gain, pré-positionnement stratégique, hacktivisme, espionnage ou déstabilisation… qu'elles ciblent un État, une entreprise ou un particulier, les cyber attaques ne cessent d'augmenter. Entre 2020 et 2023, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a constaté une hausse de 400 % des actes de cybercriminalité en France. Et les cybercriminels exploitent maintenant l'IA pour perfectionner leurs méthodes et intensifier leurs attaques.

*« L'intelligence artificielle connaît une ascension fulgurante, tandis que l'humain, lui, peine à se libérer de ses biais cognitifs »*, analyse Zakaria Rachid, responsable de la sécurité des systèmes d'information (CISO) de Believe et ancien de Leboncoin.fr. Pour l'expert en cybersécurité, le manque de sensibilisation à l'IA et le peu d'initiative de recherche d'informations par les individus exposent tout un chacun au risque d'une cyber attaque. Ces constats soulignent l'urgence d'une meilleure compréhension de l'IA et d'une culture de la sécurité étendue, afin de renforcer la résilience face aux menaces cyber qui se perfectionnent constamment.

# La compromission via la supply chain

Selon l’expert en cybersécurité, la supply chain représente une cible privilégiée pour les attaques cyber. *« Les systèmes internes des organisations gagnent en robustesse, incitant les cybercriminels à exploiter des canaux transversaux. Les startups, les scale-ups ou les organisations plus traditionnelles, font appel à des fournisseurs ou utilisent des fragments de technologies open source qui ne leur appartiennent pas et qu'elles ne maîtrisent pas entièrement. Les vulnérabilités peuvent résider dans ces maillons faibles, ouvrant des portes dérobées aux cybercriminels. Afin de se prémunir contre de telles menaces, il est impératif d'inclure des clauses de sécurité dans les contrats liant ces organisations à leurs prestataires, exigeant ainsi le même niveau de sécurité que celui appliqué en interne. »*

François Deruty, chief intelligence officer chez Sekoia.io - jeune pousse française spécialisée dans la lutte contre les menaces et le renseignement cyber -, évoque par ailleurs la sophistication croissante des attaques de chaîne d'approvisionnement de niveau deux, où les cybercriminels ciblent les fournisseurs des fournisseurs. *« Les organisations doivent anticiper ces scénarios et renforcer leur cybersécurité à tous les niveaux de la chaîne »*, suggère-t-il.

Zakaria Rachid, souligne notamment qu’un risque majeur plane sur les nombreuses organisations qui intègrent des technologies telles que ChatGPT d’OpenAI ou Bard de Google dans leurs produits, pour la création de chatbots par exemple. *« Un des risques réside dans la possibilité d'une injection de prompt. Ce fut le cas le mois dernier pour Chevrolet dont le chatbot a été détourné pour générer du contenu trompeur et nuisible. En 2024, ce type d'attaque devrait s'intensifier. Outre le chatbot, on peut imaginer des IA compromises qui permettraient d’extraire des infos ou de planifier des actions techniques comme des commandes malveillantes par exemple. »* Zakaria Rachid encourage les organisations à réaliser du

threat modeling à chaque intégration pour contrer ces phénomènes de prompt injection, mais pas seulement. Comme d’autres experts de la cybersécurité, il rappelle que les méthodes assistées par IA, telles que les deepfakes et le clonage vocal, décuplent les chances de succès de l'ingénierie sociale.

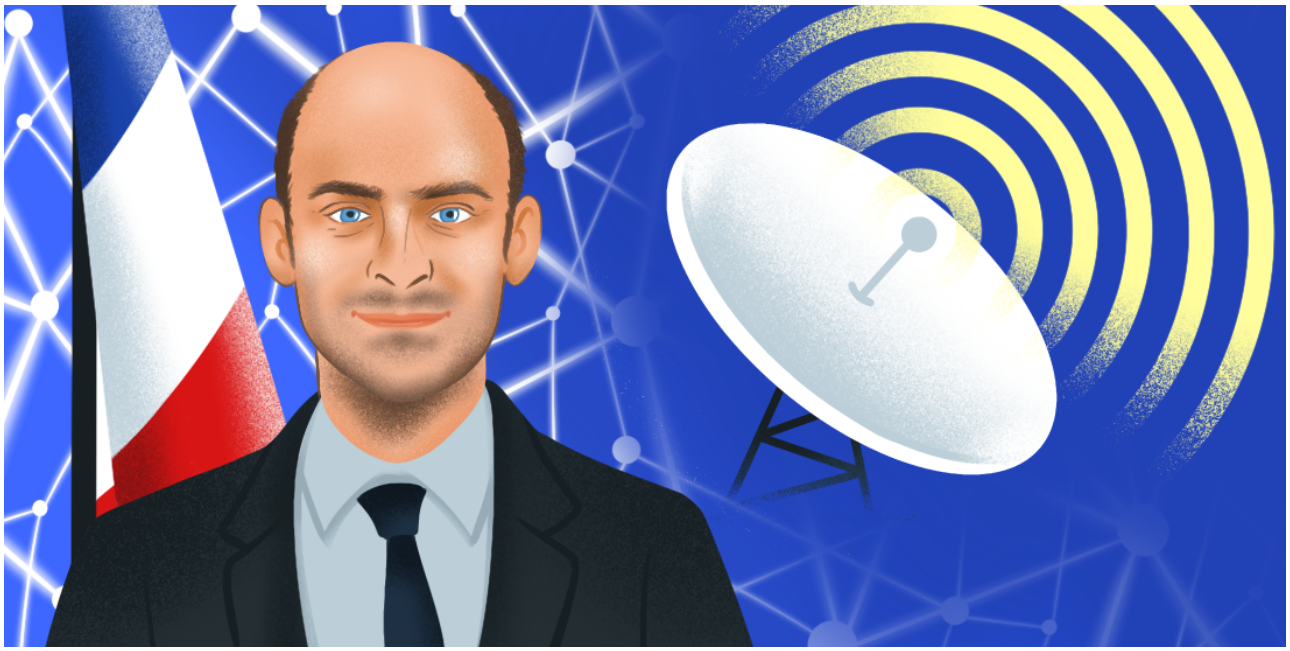
## Attaques ciblées et quishing montent en puissance

Ces techniques d'attaque informatique qui consistent à tromper les individus pour qu'ils divulguent des informations sensibles, telles que des identifiants de connexion, des mots de passe ou des informations financières devraient elles aussi être facilitées par l’IA. *« L’IA permet de collecter et traiter une multitude d’informations sur n’importe qui et de générer du contenu de qualité et très personnalisé. Ces attaques qui, auparavant, ciblaient les VIP vont devenir mainstream »*, explique Zakaria Rachid.

Le Chief Intelligence Officer chez Sekoia.io met en évidence un autre risque émergent lié à la démocratisation de l'intelligence artificielle : le quishing. Une arnaque au faux QR code qui permet au cybercriminel de rediriger la personne qui le scanne vers un site internet qui, bien souvent, à l’air sérieux et officiel, pour qu’elle y rentre ses informations personnelles. *« C’est une menace très efficace. Nous prêtons de plus en plus d’attention aux adresses lorsqu’on juge un mail douteux, mais personne ne vérifie l’URL que génère le QR code une fois scanné et, ici encore, l’IA facilite la massification de faux. »*

Pour François Deruty - qui supervise des activités liées à la collecte, à l'analyse et à l'utilisation de renseignements chez Sekoia.io -, cette nouvelle forme de cybercriminalité souligne la nécessité d’une réflexion profonde sur la sensibilisation à l'IA, la culture de la sécurité et la collaboration étroite entre organisations et prestataires, car seule une

approche globale et proactive pourra véritablement renforcer notre résilience face à ces menaces cyber qui ne connaissent aucune limite dans leur perfectionnement constant.



À lire aussi
Cybersécurité : "Un filtre anti-arnaques doit être déployé d'ici aux JO 2024", selon le ministre Jean-Noël Barrot

JE M’INSCRIS

---

Article écrit par Astrid Briant