

Bulletin sur les cybermenaces : accélération des cyberattaques par intelligence artificielle agentive



Communications Security
Establishment Canada
Canadian Centre
for Cyber Security

Centre de la sécurité des
télécommunications Canada
Centre canadien
pour la cybersécurité

Canada

Table des matières

Vue d'ensemble	2
Le signe du changement	3
Pourquoi le Centre pour la cybersécurité avertit les Canadiennes et Canadiens	3
Que devraient faire les organisations	4
Préparer les infrastructures essentielles	5
Signalement des incidents de cybersécurité	6
Ressources utiles	6



Vue d'ensemble

Des changements que l'on anticipait depuis longtemps commencent à prendre forme dans le domaine de la cybersécurité.

L'intelligence artificielle (IA) facilite déjà la détection des failles, le développement de code malveillant et les attaques contre de nombreuses organisations en même temps. Il s'agit de versions de cybermenaces connues plus puissantes que les précédentes. L'IA agentive va plus loin en liant des étapes distinctes d'une attaque et en les menant à bien avec peu de directives humaines.

Des cyberactivités malveillantes récentes menées par Storm-0940 illustrent cette tendance, qui montre l'évolution fondamentale des techniques malveillantes dont peuvent se servir les divers auteurs de menace. Dans ce cas, l'auteur de menace a utilisé un cadre d'IA agentive pour mener à bien et coordonner plusieurs étapes d'une cyberattaque¹. Il a pu chercher des cibles, tester des façons de s'introduire dans les systèmes, explorer des réseaux compromis et rechercher un meilleur accès. Il est parvenu à le faire rapidement, de façon répétée chez un grand nombre d'organisations.

L'évolution la plus importante ne correspond toutefois pas à l'identification d'un auteur de menace ou à la détermination des détails d'une campagne. C'est plutôt l'émergence d'un cadre réutilisable qui aide à mener des cyberopérations à une échelle industrielle.

Les cyberattaques ne sont pas encore entièrement autonomes. Des humains choisissent encore les cibles, fixent les objectifs et supervisent l'opération. Cependant, de plus en plus du travail lié à ces décisions peut maintenant être délégué aux machines. Les responsables de la défense ont dès lors moins de temps pour détecter une attaque et y mettre fin.

¹ L'IA agentive fait référence aux systèmes d'IA qui peuvent planifier et mener à bien une série de tâches avec peu de directives humaines. ARTEX est un exemple de virage en profondeur vers les systèmes d'IA qui peuvent planifier et exécuter de multiples étapes d'une cyberattaque. Plusieurs cadres accessibles au public prennent en charge les tests de sécurité automatiques, et les auteurs de menace abusent également des agents d'IA généraux pour mener des cyberopérations. Ces systèmes varient dans la capacité et le degré d'autonomie, mais la tendance dépasse un seul outil ou une seule campagne. Une plus grande partie d'une attaque peut être déléguée aux machines, qui augmentent le rythme et l'ampleur des attaques et réduisent le délai dont dispose les responsables de la défense pour intervenir.

Le signe du changement

Storm-0940 a utilisé un cadre d'IA agentive appelé ARTEX pour cibler des centaines d'organisations. Dans certains cas, l'activité est passée de la sélection d'une cible à l'obtention d'un accès privilégié aux systèmes infonuagiques en moins de trois heures².

Le cadre a permis de trouver des cibles, de tester des mots de passe et d'explorer les systèmes compromis. Aucune de ces techniques n'est nouvelle. La nouveauté, c'est plutôt la capacité de les lier, de les automatiser et de les répéter contre un grand nombre de cibles.

Storm-0940 donne un premier coup d'œil à la façon dont l'IA transforme les cyberopérations. Les comptes ayant une faible protection, les permissions d'accès excessives, les systèmes exposés, les logiciels non corrigés et les lacunes dans la surveillance demeurent les manières courantes de s'introduire dans les systèmes d'une organisation. L'IA agentive peut aider les auteurs de menace à trouver et à exploiter ces failles plus rapidement et à plus grande échelle.

Pourquoi le Centre pour la cybersécurité avertit les Canadiennes et Canadiens

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) avertit depuis quelque temps que l'IA élimine les obstacles à l'accès aux cyberactivités malveillantes et augmente la vitesse, l'ampleur et la sophistication des cybermenaces³. Les activités rendues publiques cette semaine confèrent un caractère urgent à cet avertissement.

Au fur et à mesure de la croissance des capacités des agents automatisés, les organisations pourraient être confrontées à des attaques qui passent à plusieurs systèmes en même temps. Les machines peuvent agir plus rapidement que ce que nombre de processus et de politiques sont conçus pour gérer. Les décisions qui autrefois donnaient le temps de discuter pourraient bientôt devoir se prendre en quelques minutes.

² Microsoft Security Research et Microsoft Threat Intelligence. [AI-Driven, Large-Scale Nation-State Campaign Using ARTEX Enables Supply Chain Compromise](#) (en anglais seulement). Microsoft Security Blog. Le 21 octobre 2026.

³ Centre canadien pour la cybersécurité. [Évaluation des cybermenaces nationales 2025-2026](#). Gouvernement du Canada. Le 20 septembre 2024. Centre canadien pour la cybersécurité. [Déclaration des organismes de cybersécurité de la collectivité des cinq sur l'évolution des cyberrisques posés par l'IA : pourquoi les dirigeantes et dirigeants doivent agir maintenant](#) Le 22 juin 2026.



C'est particulièrement important dans le cas des infrastructures essentielles. Un incident qui touche un fournisseur de services infonuagiques, un autre fournisseur, un système de gestion des identités ou une technologie opérationnelle peut se propager au-delà de l'organisation d'abord compromise. Il peut perturber les services essentiels et entraîner des dommages physiques et économiques dans divers secteurs. Il s'agit d'un risque pour la sécurité nationale et économique du Canada.

Le Centre pour la cybersécurité priorise la sécurité et la résilience des systèmes numériques les plus importants du Canada, au gouvernement du Canada et au sein des infrastructures essentielles. Il aide également les propriétaires et exploitants d'infrastructures essentielles à se préparer à maintenir les services essentiels en cas de cyberincident grave.

Pour l'instant, la plupart de ces activités sont suffisamment généralisées et tapageuses qu'elles sont détectées par les mesures de cyberdéfense sophistiquées. On estime que les cyberactivités facilitées par l'IA risquent probablement de devenir plus ciblées, moins visibles et plus difficiles à détecter qu'actuellement au fur et à mesure que la technologie s'améliore.

Que devraient faire les organisations

L'IA agentive ne rend pas obsolètes toutes les pratiques de cybersécurité déjà établies. Elle en accroît l'importance.

Le Centre pour la cybersécurité avise depuis longtemps que les Canadiennes, les Canadiens et les organisations canadiennes sont confrontés à un plus grand risque lorsque les pratiques de base de la cybersécurité ne sont pas adoptées de façon uniforme⁴.

Les organisations devraient :

- exiger l'authentification multifacteur résistante à l'hameçonnage pour les administratrices et administrateurs, l'accès à distance et d'autres comptes importants;
- restreindre l'accès accordé aux utilisatrices et utilisateurs, aux applications et aux comptes de service;
- examiner les accès accordés à une partie tierce et les applications infonuagiques partagées;

⁴ Centre canadien pour la cybersécurité. [10 meilleures mesures de sécurité des TI](#). Le 13 janvier 2021. Centre canadien pour la cybersécurité. [Les meilleures mesures pour renforcer la cybersécurité des petites et moyennes entreprises \(ITSAP.10.035\)](#). Février 2024.

- apporter les correctifs rapidement aux systèmes connectés à Internet et retirer les services qui ne sont plus requis;
- conserver les journaux de sécurité et assurer une surveillance pour détecter les connexions inhabituelles, les nouveaux justificatifs d'identité et les changements inattendus dans les accès;
- décider à l'avance qui peut isoler un compte, une application, un réseau ou un service;
- mener des exercices pour pratiquer l'intervention en cas d'incidents qui se déroulent en quelques heures plutôt qu'en jours;
- séparer les systèmes importants et conserver des sauvegardes éprouvées hors ligne ou des sauvegardes protégées.

Ces mesures diminuent les options d'attaque. L'IA amplifie les conséquences des mesures de contrôle faibles et des lenteurs dans les décisions, mais les bases d'une bonne cybersécurité demeurent efficaces.

Préparer les infrastructures essentielles

La prévention seule n'est pas suffisante. Les propriétaires et exploitants d'infrastructures essentielles doivent se préparer à la possibilité que les systèmes importants, les fournisseurs et les communications soient indisponibles ou qu'il soit impossible de leur faire confiance.

Par l'intermédiaire de [l'initiative de Résilience des infrastructures essentielles face à l'intensification des menaces \(RIEFIM\)](#)⁵, le Centre pour la cybersécurité aide les organisations à se préparer en cas de perturbation grave et prolongée causée par des cyberactivités pour qu'elles puissent continuer à fournir les services essentiels aux Canadiennes et Canadiens.

L'initiative de RIEFIM est axée sur trois capacités pratiques, soit :

- isoler les systèmes essentiels;
- exploiter les services essentiels de façon indépendante durant une interruption de grande envergure;

⁵ Centre canadien pour la cybersécurité. [Initiative de Résilience des infrastructures essentielles face à l'intensification des menaces \(RIEFIM\)](#). Le 18 Septembre 2026.

- rebâtir les systèmes touchés à partir de sources de confiance hors ligne.

Les propriétaires et exploitants d'infrastructures essentielles devraient :

- déterminer les fonctions minimalement nécessaires pour protéger la vie et la sécurité ainsi que maintenir les services essentiels;
- établir des procédures claires et préautorisées d'isolation des systèmes essentiels et des connexions externes;
- tester des façons manuelles ou différentes de mener les activités;
- cerner les services qui peuvent être réduits ou être interrompus en cas de crise;
- comprendre leur dépendance aux télécommunications, aux services infonuagiques, aux services publics et au personnel spécialisé;
- conserver hors ligne des copies de confiance des produits essentiels, comme les logiciels, les configurations, les instructions et le matériel de reprise;
- tester la façon dont les systèmes de technologie de l'information et de technologie opérationnelle peuvent être récupérés et examinés avant de les reconnecter.

L'objectif n'est pas de maintenir les activités normales en toute circonstance, mais de protéger la vie et la sécurité, de limiter l'étendue des dommages et de continuer à fournir les services viables minimaux sur lesquels les Canadiennes et les Canadiens comptent en dépit de la capacité réduite.

Signalement des incidents de cybersécurité

Les organisations qui font l'expérience de cyberactivités suspectes ou malveillantes devraient les signaler au Centre pour la cybersécurité par l'intermédiaire de son [portail en ligne](#). Les victimes de cybercrimes devraient également signaler l'incident à leur service de police et au [Centre antifraude du Canada](#), le cas échéant.

Veuillez transmettre toute question ou tout enjeu connexes au Centre pour la cybersécurité à contact@cyber.gc.ca.

Ressources utiles

Consultez les ressources en ligne suivantes pour obtenir de plus amples renseignements, ainsi que des avis et conseils :



- [Évaluations des cybermenaces nationales - Centre canadien pour la cybersécurité](#)
- [Déclaration des organismes de cybersécurité de la collectivité des cinq sur l'évolution des cyberrisques posés par l'IA : pourquoi les dirigeantes et dirigeants doivent agir maintenant – Centre canadien pour la cybersécurité](#)
- [L'intelligence artificielle de pointe \(ITSAP.10.050\) – Centre canadien pour la cybersécurité](#)
- [Les 10 mesures de sécurité en matière d'intelligence artificielle : Introduction \(ITSAP.10.049\) – Centre canadien pour la cybersécurité](#)
- [Initiative Résilience des infrastructures essentielles face à l'intensification des menaces – Centre canadien pour la cybersécurité](#)
- [Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information \(ITSM.10.089\) – Centre canadien pour la cybersécurité](#)
- [Mesures de cybersécurité de base à l'intention des petites organisations \(ITSAP.10.300\) – Centre canadien pour la cybersécurité](#)
- [Objectifs relatifs à l'état de préparation en matière de cybersécurité : Sécuriser les systèmes les plus essentiels – Centre canadien pour la cybersécurité](#)

