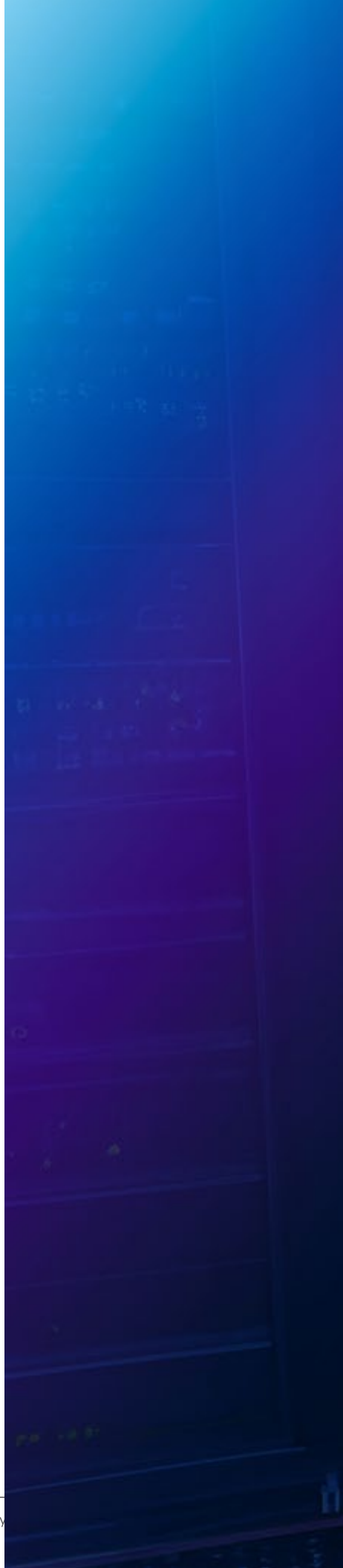
Cyberincidents et Renseignements : 2024

Bilan d'exercice des équipes Intervention en cas de cyberincident et Renseignements sur les cybermenaces de KPMG au Canada

Mars 2024

kpmg.ca/fr

Contents



01 Introduction

Le paysage de la cybersécurité continue d'évoluer, les menaces, de se complexifier, et les méthodes d'attaque, de changer. Comme les tactiques se raffinent, les entreprises doivent s'adapter pour se défendre contre l'exploitation des vulnérabilités émergentes.

Le présent rapport fait une analyse approfondie des menaces réelles auxquelles les sociétés canadiennes ont fait face en 2024, en plus de brosser un portrait prospectif pour 2025. Conçu par les équipes de Réponse aux incidents, de Renseignements sur les cybermenaces et de Gestion des vulnérabilités de KPMG au Canada, il contient des renseignements importants et des perspectives éclairées pour aider les organisations à renforcer leurs moyens de défense.

Il convient de noter que les renseignements contenus dans le présent rapport font état d'expériences et d'incidents réels survenus en 2024. Bien que les descriptions des événements soient exactes, les renseignements sur les victimes ont été modifiés.

02 Intervention en cas d'incident

Sommaire

Aperçu des préoccupations liées à la cybersécurité

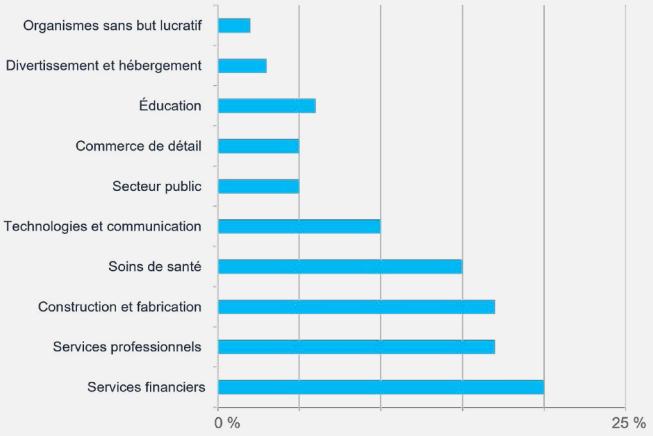
En 2024, les sociétés canadiennes ont subi des pressions accrues des autorités de réglementation, des commissaires à la protection de la vie privée, du public et de leurs actionnaires pour accroître leur cybersécurité. Toutefois, le paysage changeant des menaces a rendu cette tâche de plus en plus difficile, car les attaquants exploitent les vulnérabilités plus rapidement que les sociétés arrivent à les corriger en ciblant les maillons faibles des chaînes d'approvisionnement et en contournant les moyens de défense mis en place par des tactiques sophistiquées.

KPMG a observé l'effet domino des attaques par rançongiciel – une seule atteinte à la sécurité peut perturber les activités de partenaires, de fournisseurs de services et de secteurs d'activité tout entiers. Les cyberattaques ciblant les organisations des secteurs manufacturier et financier ont augmenté, puisque les acteurs des menaces profitent des dépendances opérationnelles et des environnements riches en données pour amplifier leurs répercussions. En outre, chaque cyberincident présente un risque pour les identités. Les cyberincidents et les vols d'identité sont étroitement interreliés, puisque les premiers servent souvent de passerelles pour les crimes axés sur l'identité.

TransUnion, une agence d'évaluation du crédit offrant des services de surveillance au Canada, aux États-Unis, au Royaume-Uni, en Inde, à Hong Kong (RAS – Chine) et en Afrique du Sud, a dévoilé certaines des tendances qu'elle a observées sur le paysage canadien des menaces et des vols d'identité connexes.

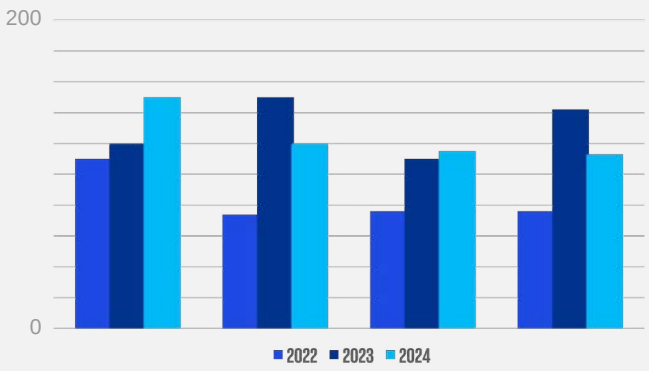
Selon TransUnion, le secteur qui se procure le plus couramment des services de protection de l'identité et qui exerce la plus importante surveillance à ce chapitre est celui des services financiers.

Violations de données survenues en 2024 par secteur



Source : TransUnion

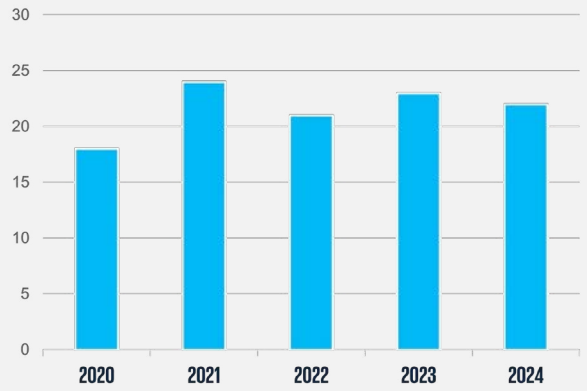
Nombre de violations de données par trimestre



Conformément aux observations de TransUnion, la section Menaces importantes et statistiques ci-dessous, indique une croissance du nombre d'atteintes à la sécurité, malgré leur baisse générale vers la fin de 2024.

Source : TransUnion

Comparaison d'une année sur l'autre de la durée moyenne des abonnements (en mois)



En raison de la multiplication des brèches et des menaces subséquentes aux identités et aux renseignements personnels, la durée moyenne des abonnements aux services de surveillance d'identité de TransUnion se situait entre un et deux ans.

Source : TransUnion

Observations importantes

Hausse de l'exploitation des failles des pare-feu

Depuis le début de 2024, les équipes de Réponses aux incidents et de Renseignements sur les cybermenaces de KPMG ont répertorié des vulnérabilités ciblant divers produits de pare-feu. Elles ont ainsi déterminé que les acteurs de menace préféraient cibler les appareils périphériques connectés pour accéder à l'environnement d'une entreprise. En 2024, il y a eu une hausse marquée de l'exploitation des vulnérabilités des pare-feu; les acteurs de menaces s'évertuent à repérer ces vulnérabilités et à exploiter celles-ci avant que les correctifs soient déployés. La leçon à tirer est claire : l'utilisation d'un dispositif de sécurité périphérique, à elle seule, ne suffit pas. Étant donné que les cybercriminels exploitent les vulnérabilités à grande échelle, les sociétés canadiennes doivent se tourner vers des stratégies de défense proactives, la surveillance en continu, l'utilisation de correctifs fondés sur des renseignements sur les cybermenaces, et les contrôles de sécurité multiniveaux pour se défendre efficacement contre les menaces qui évoluent rapidement.

Les rançongiciels continuent de frapper durement la couche de virtualisation

Les pirates informatiques attaquent de plus en plus les hyperviseurs, surtout les hôtes ESXi et VMware. Cette approche leur permet de contourner les outils de défense traditionnels installés et leur permet de chiffrer la totalité des environnements informatiques d'un seul coup. L'équipe de Réponse aux incidents de KPMG a remarqué plusieurs incidents de type rançongiciel où les malfaiteurs ont réussi à accéder à l'environnement des hyperviseurs et aux machines virtuelles protégées par chiffrement. En changeant de méthodes, les acteurs de menaces ont maximisé leur effet moyennant un effort minimal, et à paralyser efficacement des activités commerciales essentielles grâce au chiffrement simultané de plusieurs machines virtuelles.

L'adoption de telles méthodes souligne le besoin urgent de mettre en place de meilleures mesures de sécurité pour protéger les couches de virtualisation. Le problème est généralisé, car les outils de détection et de réponse (EDR) actuels sont incapables d'assurer cette protection. Les sociétés qui se fient à VMware et aux autres hyperviseurs sur le marché doivent instaurer des contrôles compensatoires pour sécuriser leur infrastructure, comme des mesures de gestion des accès et des privilèges qui servent à protéger les données de connexion des comptes, tout comme des mesures d'isolement pour assurer la gestion, et de robustes stratégies de sauvegarde pour réduire les risques d'interruption complète des activités. Les stratégies déployées doivent évoluer pour aller au-delà de la protection des points terminaux et assurer la sécurité des éléments fondamentaux de l'infrastructure de TI.

Utilisation malveillante des outils de réponse aux incidents et d'enquêtes numériques et des logiciels open source libre

L'équipe de Réponse aux incidents de KPMG a aussi observé que les pirates se servaient de plus en plus de logiciels open source ainsi que d'outils de réponse aux incidents et d'enquêtes numériques commerciaux pour passer inaperçus, extraire des données sensibles et prolonger leur accès aux environnements compromis. Ces utilitaires d'enquêtes open source ont été fréquemment utilisés à mauvais escient pour des activités telles que l'extraction de données de connexion, l'analyse de mémoire et l'établissement d'une porte dérobée, ce qui permet aux attaquants d'agir avec la plus grande discrétion tout en s'intégrant aux activités légitimes d'exploitation de la sécurité.

Ce changement de tactiques rend la tâche difficile aux équipes de sécurité qui cherchent à repérer les mauvaises utilisations des outils de détection. Pour régler efficacement ce problème, les entreprises ne doivent pas uniquement surveiller les menaces traditionnelles; elles doivent aussi faire les suivis pour lesquelles ces outils sont utilisés. Il ne suffit pas de savoir que ces programmes sont exécutés; il est également essentiel de comprendre le contexte dans lequel ils le sont, ainsi que le quand, le comment et le pourquoi.

Sans la mise en place de mesures appropriées, les acteurs de menaces continueront d'exploiter les propres outils des victimes, et garderont une longueur d'avance sur l'échiquier de la cybersécurité.

Attaques par force brute, reconnaissance réseau après les heures ouvrables et masquage par RPV

Les acteurs de menaces ciblent constamment les environnements informatiques au moyen d'attaques par force brute, et ce, souvent tard dans la nuit, tôt le matin ou lors des longs week-ends, c'est-à-dire aux moments où les équipes de sécurité sont moins susceptibles de détecter l'activité suspecte en temps réel.

Leurs campagnes bombardent les portails d'authentification de tentatives rapides de saisie de mot de passe, en changeant les données de connexion de façon cyclique jusqu'à ce qu'une connexion valide soit établie. De façon similaire, les activités de reconnaissance réseau s'intensifient après les heures ouvrables; les adversaires cherchent à trouver des ports ouverts, des services mal configurés et des données de connexion vulnérables de façon à préparer le terrain en vue d'une compromission plus loin dans le système.

Pour mieux camoufler leurs activités, les acteurs de menaces ont accru leur utilisation d'adresses IP canadiennes pour masquer leur véritable origine et se faire passer pour des utilisateurs légitimes. En mettant à profit les services de réseau privé virtuel (RPV) et les hôtes compromis du Canada, les attaquants arrivent à contourner les politiques de sécurité fondées sur la géolocalisation et à se fondre dans le trafic courant, ce qui rend leur détection par les équipes de sécurité encore plus difficile.

Principales leçons et recommandations

Voici les principales leçons que certains de nos clients ont tirées d'une brèche de sécurité informatique.

Rétention des journaux : une déficience persistante

La rétention des journaux demeure une lacune importante, puisqu'elle figure dans les constats d'environ la moitié des enquêtes réalisées par KPMG en 2024. Les journaux critiques, tels que les journaux d'événements Windows, les journaux de trafic réseau et les alertes des outils de sécurité, ont souvent été omis ou effacés, ce qui limitait la visibilité.

Il est fortement recommandé, pour pallier à cette lacune, d'opter pour des solutions centralisées de journalisation, telles que les outils de gestion des informations et des événements de sécurité, pour assurer l'exhaustivité de la collecte de journaux, l'entreposage à long terme et la surveillance proactive et, ultimement, pouvoir détecter plus efficacement les menaces et répondre aux incidents avec plus d'efficience.

Exercices de simulation

Comme les cybermenaces gagnent en complexité, les entreprises doivent redoubler d'efforts et chercher des stratégies novatrices pour garder une longueur d'avance et maintenir un système assez robuste pour se défendre contre les attaques potentielles.

La simulation de cybermenaces de KPMG se veut un exercice structuré où sont reproduits de véritables cybermenaces et scénarios d'attaque. L'objectif premier consiste à évaluer et à rehausser l'efficacité des mesures et des processus de sécurité d'une entreprise, ainsi que sa capacité à réagir en cas d'incident. En reproduisant les tactiques, les techniques et les procédures (TTP) de réels pirates, ces simulations aident les sociétés à repérer les vulnérabilités, à valider l'efficacité de leurs moyens de défense et à augmenter leur capacité à faire face aux cybermenaces.

En 2024, KPMG a tenu son premier Défi simulation de cybermenaces, auquel plus de 150 entreprises ont participé. Ces dernières ont ainsi bénéficié d'une plateforme unique pour tester leur cyberrésilience dans un environnement de compétition et de collaboration. Apprenez-en plus sur le Défi simulation de cybermenaces de 2025 à venir pour découvrir comment les grandes entreprises préparent leur cyberdéfense de demain.

Gestion des correctifs

La non-actualisation du matériel informatique et des logiciels demeure l'une des principales causes des cyberincidents. D'ailleurs, nombre d'enquêtes effectuées en 2024 ont été amorcées en raison de vulnérabilités non corrigées

dans des systèmes désuets. Les acteurs de menaces continuent d'exploiter les faiblesses connues que les organisations ne règlent pas et qui laissent leurs systèmes essentiels vulnérables. Pour atténuer les risques, les entreprises doivent se doter de stratégies de gestion proactive des correctifs qui devraient inclure des évaluations périodiques des vulnérabilités, la mise à niveau prioritaire des systèmes essentiels et le déploiement automatisé de rustines. La correction des vulnérabilités en temps opportun se veut l'un des moyens les plus efficients de se défendre contre les attaques évitables.

Angles morts de la gestion des actifs

La gestion inefficace des actifs s'est révélée une vulnérabilité importante dans environ 30 % des enquêtes menées par l'équipe de Réponse aux incidents de KPMG en 2024. Plusieurs entreprises n'ont pas toute la visibilité souhaitable sur leurs environnements informatiques, ce qui les empêche de repérer les comptes inconnus, les appareils non gérés et les systèmes factices. Ces angles morts ont fourni aux acteurs de menaces des occasions d'infiltrer les systèmes et d'y garder une menace persistante avancée (MPA) active sans être détectés. Pour supprimer cette vulnérabilité, les organisations doivent utiliser des processus continus et centralisés l'inventaire des actifs et faire des audits périodiques de l'ensemble des comptes, des appareils et des systèmes.

Lacunes des solutions EDR et des outils de gestion des informations et des événements de sécurité

En 2024, les enquêtes de l'équipe de Réponse aux incidents de KPMG ont révélé que la couverture incomplète des solutions EDR et l'absence d'outils de gestion des informations et des événements de sécurité constituaient des vulnérabilités significatives dans le système de sécurité des entreprises. De nombreuses sociétés comptaient des points terminaux sans agents EDR, ce qui a permis aux acteurs de menaces d'exploiter les vulnérabilités et de se déplacer latéralement au sein des réseaux de façon à perpétuer leurs attaques.
Parallèlement, une majorité des victimes de rançongiciel n'avaient pas installé d'outil de gestion des informations et des événements de sécurité et, si elles l'avaient fait, elles n'y versaient pas leurs journaux critiques ou elles établissaient des périodes de rétention trop courtes pour permettre la réalisation d'enquêtes. Les équipes de sécurité ont donc été incapables de voir les indicateurs précoces d'une attaque. Certains ont déployé un outil de gestion des informations et des événements de sécurité uniquement pour archiver leurs journaux, sans le configurer pour qu'il intègre tous les journaux pertinents. Ces lacunes affaiblissent les systèmes de défense, mais pire encore, elles invitent carrément les attaquants à exploiter les systèmes non protégés.

Les organisations doivent prioritairement déployer des outils EDR sur tous leurs appareils pour avoir une pleine couverture, les configurer adéquatement pour qu'ils intègrent toutes les données nécessaires et conservent les journaux à long terme. Toute solution inférieure à cette approche laisse le champ libre aux attaquants qui pourront œuvrer sans se faire détecter.

Les entreprises qui n'ont pas les ressources pour gérer le déploiement d'un outil de gestion des informations et des événements de sécurité ou exploiter un centre opérationnel de sécurité (COS) devraient songer à confier leurs services de détection et de réponse gérées (DRG) à une tierce partie. Les services DRG sont souvent assortis d'ententes de niveau de service (ENS) et offrent aux entreprises une tranquillité d'esprit à l'égard de leur situation en matière de sécurité.

Inutilité des sauvegardes quand elles sont inaccessibles

Dans la plupart des enquêtes que KPMG a menées pour des victimes de rançongiciel, les sauvegardes avaient été chiffrées ou supprimées par les attaquants. La récupération des données était donc devenue impossible.

Certaines victimes pouvaient compter sur des sauvegardes hors ligne, mais, faute de pouvoir retrouver leur mot de passe, elles n'ont pas pu y accéder. D'autres, qui croyaient leurs sauvegardes intactes, ont réalisé trop tard que leurs processus de mise à jour ou de mise à l'essai étaient inadéquats.

Une sauvegarde ne peut être plus efficace que la capacité d'une entreprise à la restaurer. Par conséquent, les sociétés doivent élaborer une stratégie de sauvegarde bien définie qui comprend des tests périodiques, une gestion efficace des données de connexion et des solutions d'entreposage par couches (qui devraient inclure des sauvegardes en ligne, hors ligne et immuables).

Sensibilisation à la sécurité et préparation

Dans le domaine de la cybersécurité, la technologie n'agit pas seule. Votre personnel, vos processus et vos moyens de défense doivent aussi être résilients en cas d'attaque. Souvent, les entreprises se croient en sécurité jusqu'à ce qu'un incident se produise et qu'elles peinent à réagir. La sensibilisation à la sécurité ne doit pas être faite uniquement au moyen de modules de formation et de simulations d'hameçonnage. Il est important que les sociétés testent rigoureusement leur système de défense à l'aide d'exercice de simulation, de tests de type « Red Team » et de tests d'intrusion pour déceler les faiblesses avant les attaquants.

Les exercices réguliers de chasse aux menaces devraient être une priorité pour détecter de façon proactive les signes de compromission au lieu d'attendre de recevoir des alertes. Les interventions en cas d'incident ne devraient pas être un processus réactif. Il faut essayer des approches, les peaufiner et les tester. Grâce à cette préparation, en cas de brèches, les équipes de sécurité ne travaillent pas à l'aveuglette. Elles exécutent plutôt un plan d'intervention qui a été adéquatement mis à l'épreuve. Si votre entreprise n'a pas testé ses moyens de défense dans un scénario du monde réel, elle se trouve déjà désavantagée par rapport aux attaquants qui évaluent et exploitent constamment les faiblesses.

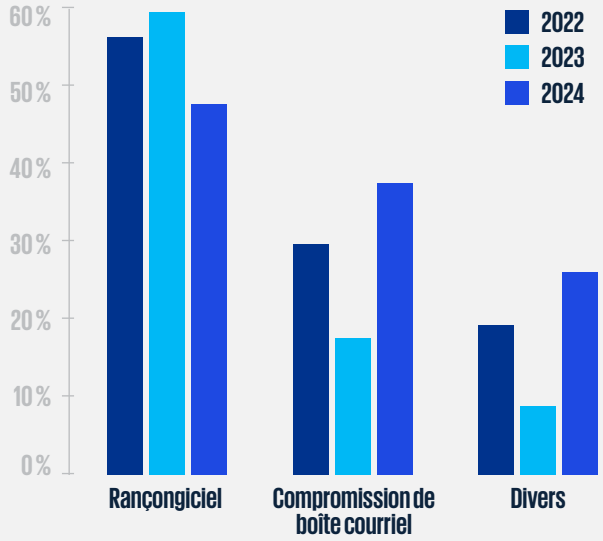
Cyberincidents

Menaces importantes et statistiques

Les rançongiciels et les compromissions de boîte courriel demeurent les cybermenaces auxquelles les entreprises canadiennes font le plus fréquemment face. La preuve, 46 % des enquêtes de KPMG en 2024 portaient sur des attaques par rançongiciel, et 32 %, sur des incidents de compromission de boîte courriel.

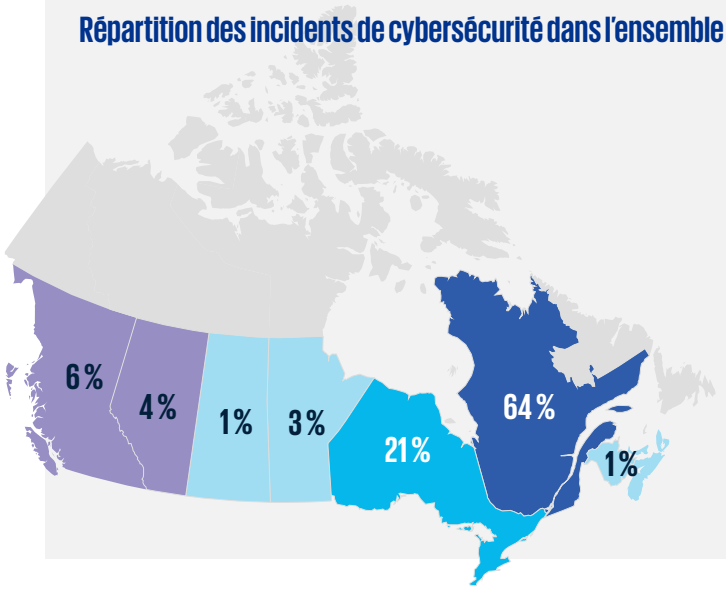
Même si les cas de rançongiciel sont en baisse par rapport à 2023, où ils représentaient 77 % des enquêtes, la sophistication des attaques s'est accrue. En effet, les acteurs de menaces ciblent de plus en plus les hyperviseurs pour fragiliser les entreprises et contourner les contrôles de sécurité. Pour leur part, les incidents liés aux compromissions de boîte courriel se sont intensifiés, passant de 15 % en 2023 à 32 % en 2024. Cela serait dû à l'utilisation, par les acteurs de menaces, à des techniques de contournement du processus d'authentification à deux facteurs et l'utilisation d'adresses IP canadiennes pour se dissimuler dans les activités légitimes. Initialement, ces attaques ciblaient de hauts dirigeants, les équipes des finances et les fournisseurs, car elles devaient servir à manipuler les paiements et à voler les données de connexion, entraînant souvent d'importantes pertes financières et des perturbations opérationnelles considérables. D'autres types de cyberattaques, comme les accès non autorisés et les menaces internes, sont passés à 22 %, comparativement à seulement 8 % en 2023, ce qui met en évidence la hausse de la diversification des méthodes utilisées.

Répartition des incidents de cybersécurité



Source : équipe Réponse aux incidents de KPMG

Répartition des incidents de cybersécurité dans l'ensemble du Canada



Par ailleurs, en 2024, les cyberattaques étaient davantage concentrées au Québec et en Ontario, ce qui cadre avec la plus grande densité d'entreprises et de l'infrastructure critique de ces provinces. En comparaison, les provinces de l'Ouest, comme la Colombie-Britannique et l'Alberta, ont enregistré moins d'incidents, alors que c'est dans le Nord canadien et le Canada atlantique qu'il y en a eu le moins.

Source : équipe Réponse aux incidents de KPMG

Étude de cas no 1

KPMG a accompagné un client pendant une attaque par rançongiciel, où l'acteur de menaces a exploité un outil externe de gestion à distance. Le pirate a réussi à accéder au système à l'aide d'un compte d'administrateur existant, ce qu'il a pu faire en raison de l'absence d'authentification à deux facteurs. Une fois à l'intérieur du système, il a mis en place une porte dérobée et fait passer le trafic par le port 443 et l'intermédiaire d'un service externe fiable pour se garantir un accès continu, même en cas de réinitialisation des données de connexion.

Par la suite, l'acteur de menaces a exfiltré les données, a cartographié le réseau et, à l'aide d'outils de réponse aux incidents et d'enquêtes numériques, a réalisé une image mémoire pour récupérer les données de connexion. Pour ne pas se faire détecter, il a déguisé un outil d'exfiltration de données en modifiant le nom du fichier avant de pousser son attaque et d'accéder à l'environnement ESXi du client au moyen du protocole SSH pour enfin chiffrer les machines virtuelles de l'entreprise. Quand l'attaque a été détectée, des systèmes complets étaient verrouillés, ce qui a paralysé les activités.

Ce cas montre comment les attaquants utilisent des services externes de confiance pour accéder aux systèmes par des portes dérobées furtives et camoufler des outils malveillants afin de ne pas se faire détecter. Sans une grande visibilité du trafic sur le réseau et du comportement des processus, ces menaces peuvent passer inaperçues jusqu'à ce qu'il soit trop tard.

Étude de cas no 2

L'équipe de Réponse aux incidents de KPMG a été appelée à enquêter sur un incident où un acteur de menaces a initialement obtenu accès à l'environnement de développement d'une entreprise, car il n'était pas protégé par les mêmes contrôles que l'environnement de production. Comme l'entreprise ne bénéficiait d'aucune couverture EDR et que son outil de gestion des informations et des événements de sécurité ne surveillait que les systèmes de production, l'attaquant a pu se déplacer impunément jusqu'aux contrôleurs de domaine et aux serveurs de bureau virtuel. L'acteur de menaces a fait de la reconnaissance réseau, cartographié l'infrastructure clé et exfiltré environ 65 Go de données à l'aide de services de stockage infonuagique de grande confiance et gratuits, comme Google Drive et SendSpace. Des données de production se trouvaient dans l'environnement de développement au moment de l'attaque. Pour effacer ses traces, l'acteur de menaces a vidé les journaux des tâches, éliminant du coup les preuves de son intrusion.

Cet incident met en évidence les risques de sécurité souvent négligés que présentent les environnements de développement, surtout quand des données de l'environnement de production y sont utilisées. De tels environnements peuvent servir de passage vers les systèmes et les données critiques d'une entreprise.

Il montre également comment les attaquants abusent des services infonuagiques légitimes pour exfiltrer, en secret, des données et utiliser l'altération des journaux pour effacer toute trace de leur passage. En n'assurant pas une couverture de protection complète à tous leurs environnements, y compris à l'environnement de développement, les sociétés risquent de ne pas repérer les attaques et de ne prendre connaissance des dommages causés qu'après celles-ci.

Analyse propre au secteur

Similairement à l'an dernier, KPMG a observé qu'aucun secteur d'activité n'a été épargné par les attaques par rançongiciel et la compromission de boîte courriel. Toutefois, une tendance marquée semble se dessiner dans le secteur manufacturier, où la fréquence des attaques a augmenté. Cette hausse pourrait être attribuable aux positions plus faibles des entreprises manufacturières en matière de cybersécurité, comparativement aux secteurs davantage axés sur la technologie. De nombreuses entreprises manufacturières sont confrontées à des défis en raison de la désuétude de leur infrastructure, des limites de leurs contrôles de sécurité et de la priorité qu'elles accordent à leur productivité au détriment de leur cyberrésilience. Cette combinaison en fait des cibles attrayantes pour les attaquants motivés.

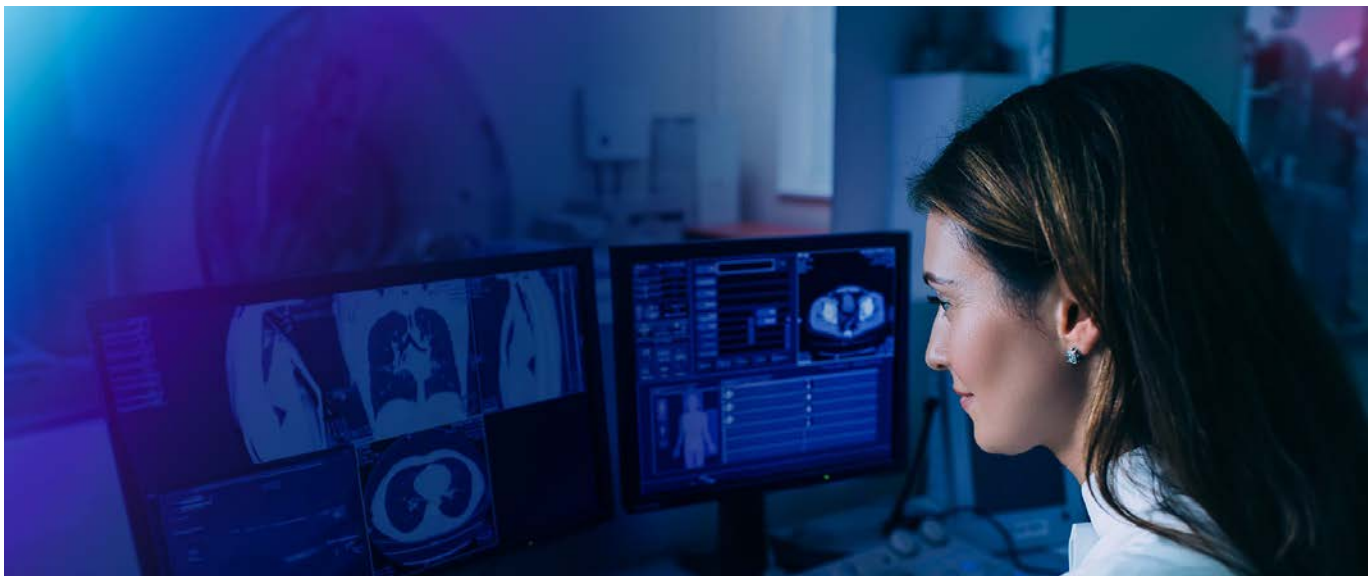
En 2024, KPMG a noté une amplification notoire des attaques de compromission de boîte courriel et des tentatives de fraude bancaire auprès des petites et moyennes entreprises du secteur des services financiers par rapport à 2023. Les acteurs de menaces ont centré leurs efforts sur les courtiers et les propriétaires d'entreprises individuelles des secteurs des finances et des assurances. Ils ont tiré parti de leurs fréquentes interactions directes avec les consommateurs et de leur dépendance au courriel pour échanger des dossiers, des données financières et, dans certains cas, des renseignements bancaires clés. Ces secteurs d'activité ont été particulièrement ciblés par les attaquants qui cherchent à faire des gains financiers faciles.

Tendances

En 2024, selon les constatations de KPMG, les acteurs de menaces ont modifié leurs tactiques en matière de rançongiciel. En effet, ils semblent stratégiquement baisser le montant des rançons demandées pour accroître la probabilité qu'elles soient versées. Les entreprises canadiennes ont montré une propension plus grande à payer les rançons exigées quand ces dernières étaient perçues comme « gérables », ce qui a fait grimper le nombre de versements de rançons. Les attaquants commencent souvent par demander un montant exorbitant pour ensuite le réduire de manière substantielle afin d'optimiser leurs profits en touchant des versements plus petits, mais plus nombreux, au lieu de paiements uniques élevés. Cette tendance est particulièrement évidente chez les groupes d'attaquants moins sophistiqués qui dépendent de l'ingénierie sociale et de l'exploitation des données de connexion et non de logiciels malveillants poussés ou de vulnérabilités de jour zéro.

Même s'ils continuent de cibler divers secteurs, les acteurs de menaces ont emprunté des approches différentes, pour les attaques de type rançongiciel, pour le secteur gouvernemental et celui de l'éducation. Dans ces cas, ils ont mis l'accent sur l'exposition médiatique plutôt que sur l'obtention de rançons, afin d'établir leur réputation. En médiatisant les incidents, ces groupes ont exacerbé les craintes, ont établi leur crédibilité et ont exercé une pression sur les futures victimes, pour les inciter à plier plus rapidement.

Avec l'évolution des tactiques impliquant des rançongiciels, il est important que les organisations comprennent que les stratégies de négociation et l'influence médiatique sont devenues des composantes intégrales des stratégies de négociation des attaquants. En 2024, l'équipe de réponse aux incidents de KPMG a consigné des versements de rançons allant de 45 000 $ US à 1,75 M$ US.



Conséquences

Rançongiciel en tant que service : agent amplificateur de l'épidémie de rançongiciel

Les rançongiciels en tant que services continuent de remodeler le paysage des cybermenaces, et rendent les rançongiciels plus accessibles, plus efficaces et plus implacables que jamais. Les rançongiciels ne sont plus l'apanage des pirates informatiques d'élite, puisque les attaquants moins compétents peuvent « s'abonner » à des services de rançongiciel et ainsi obtenir accès à des logiciels malveillants modélisés, à des outils de déploiement automatisé et à des référentiels de négociation.

Étant donné la prolifération de tels abonnements, les organisations ont été inondées d'attaques, ce qui a forcé les équipes de réponse aux incidents à lutter contre plusieurs variants de rançongiciel, de schémas d'attaque imprévisibles et de charges de chiffrement infatigables – et souvent dans les heures suivant la compromission. Puisque l'efficacité de la chaîne de fabrication du rançongiciel en tant que service raccourcit le délai de réponse, les équipes de sécurité se démènent pour contenir les dommages avant l'exfiltration des données ou le cryptage des systèmes.

Techniques d'extorsion

La double extorsion est devenue la norme, et la triple extorsion monte la pression d'un cran. Les attaquants ne se contentent plus de chiffrer les systèmes. Ils commencent par voler des données sensibles, puis les utilisent pour faire du chantage afin d'être payés. Même les entreprises pourvues de sauvegardes sont prises au piège : soit elles paient la rançon, soit elles acceptent de faire potentiellement face à des amendes pour infraction à la réglementation, à des poursuites en justice et à une exposition médiatique.

Nombre de groupes d'utilisateurs de rançongiciels exploitent maintenant des sites de fuites. Ils mettent les données volées aux enchères et humilient publiquement les victimes qui refusent de payer. Mais certains ont poussé la note en passant à la triple extorsion, et font directement chanter les clients, les employés et les partenaires au moyen des renseignements volés.

Innovation stratégique

L'équipe de Réponse aux incidents de KPMG a mis au point plusieurs approches novatrices pour aider les victimes à répondre sans tarder aux incidents, à rétablir leurs activités après ceux-ci, et à profiter d'un environnement plus stable et plus sécuritaire par la suite. L'une de ces innovations clés est la bibliothèque de chasse aux cybermenaces.

Bibliothèque exhaustive de chasses aux menaces

KPMG a créé une bibliothèque exhaustive de chasses aux menaces en se fondant sur les cadres de référence de MITRE ATT&CK, le cyberespace actuel, les cas d'usage observés en présence d'indicateurs de compromission et les TTP utilisées lors d'incidents antérieurs. Les résultats de chaque chasse aux menaces ont permis à nos clients de parfaire leurs alertes, de personnaliser leurs politiques de blocage et de renforcer de manière proactive leurs systèmes de détection afin de se protéger contre les menaces réelles.

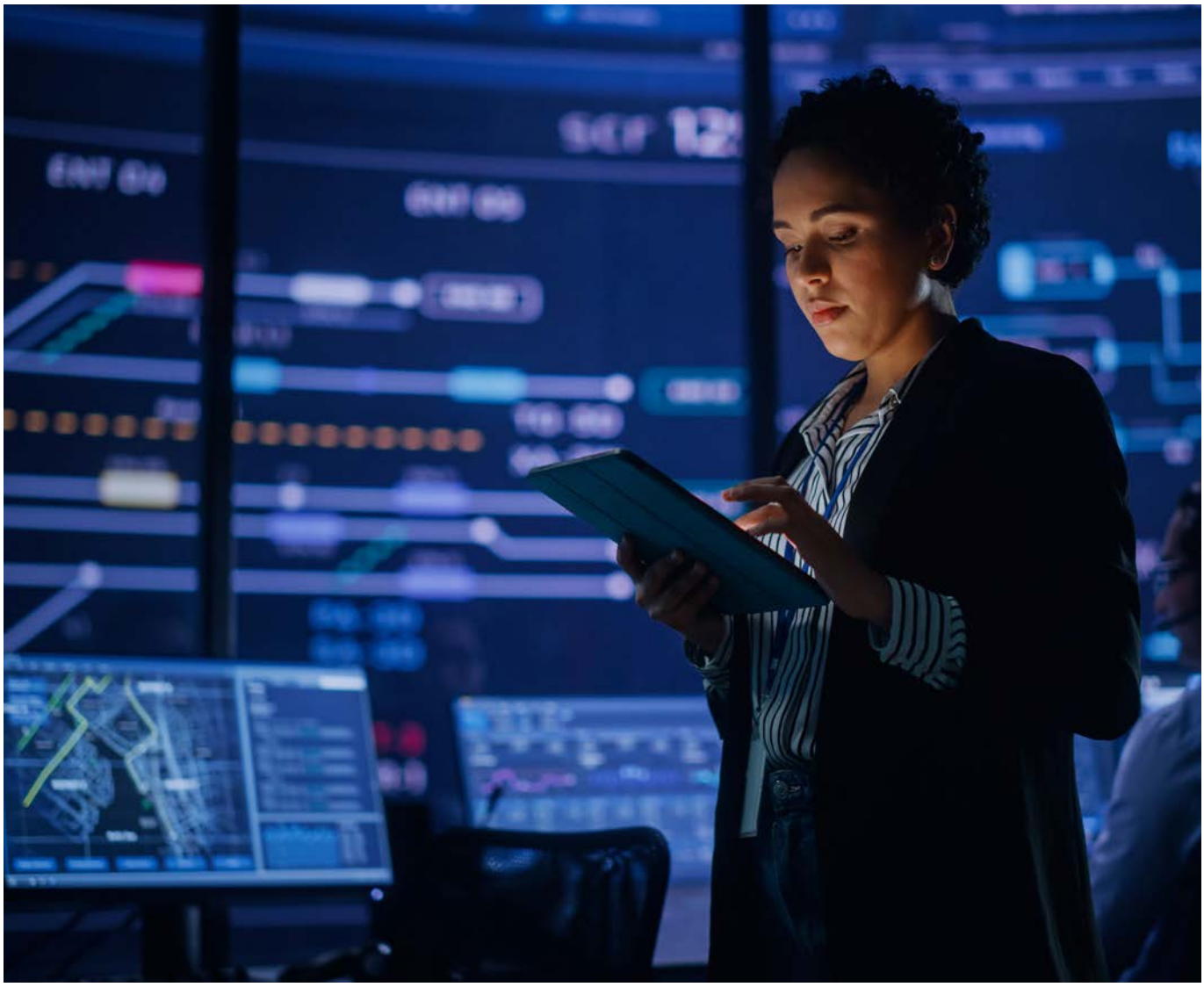
Défi simulation de cybermenaces de KPMG

À l'été 2024, KPMG au Canada a lancé son premier Défi simulation de cybermenaces pour aider les organisations à valider leurs capacités en matière de cybersécurité. L'inscription au défi était gratuite et demandait la participation à un petit exercice de type « Purple Team ».

Le projet a donné à chaque entreprise participante l'occasion d'évaluer sa posture en matière de sécurité dans un environnement contrôlé et d'obtenir de l'information sur son efficacité à détecter les cybermenaces et à y réagir.

Plus de 150 entreprises de partout au Canada s'y sont inscrites. Chaque participant a eu droit à une simulation d'une heure, laquelle intégrait plusieurs scénarios d'attaque, comme les attaques par commande et contrôle, les attaques de type évasion défensives, les attaques à l'aide du protocole Kerberos ou par outil de ligne de commande Rubeus (compromission des données de connexion).

Veuillez noter que les résultats du défi reposent sur les tests effectués auprès d'entités qui s'étaient inscrites au défi. Ils sont limités à ce groupe précis de participants.



Principales observations

- Environ 74 % des entreprises n'ont pas réussi à détecter les attaques.
- Le temps écoulé entre la journalisation des incidents et l'activation des alertes était important.
- L'attaque par exécution a été le type d'attaque le plus fréquemment détecté.
  - À l'inverse, les attaques de type évasion défensives et les MPA ont été celles qui ont été repérées par le moins de participants.
  - Le taux de non-détection était plus élevé chez les plus petites entreprises, ce qui suggère que ces dernières risquent davantage de ne pas déceler les attaques quand elles se produisent.
- Certaines entreprises de secteurs d'activité précis ont eu plus de difficulté à repérer les menaces. Les secteurs les plus touchés sont ceux des services financiers (essentiellement les petites et moyennes institutions financières), des soins de santé et du bien-être, et des aliments et des boissons.
- Les personnes inscrites au défi occupaient des rôles divers. Il y avait une forte représentation de personnes du soutien informatique, de cadres dirigeants et de dirigeants des finances, ce qui démontre que les entreprises souhaitent fortement améliorer leurs mesures de sécurité, qu'elles considèrent de plus en plus la cybersécurité comme une priorité commerciale et qu'elles reconnaissent le besoin émergent pour les équipes de direction de lutter contre les cybermenaces.

Autres constats importants : peu d'entreprises sont bien préparées

Lors de chaque séance de simulation d'une heure, de quatre à sept tactiques réelles fréquemment utilisées par les acteurs de menaces (p. ex., les attaques par commande et contrôle, les interrogations exploratoires, les attaques de type évasion défensives les attaques à l'aide du protocole Kerberos ou par outil de ligne de commande Rubeus [compromission des données de connexion], les MPA et les attaques par exécution) ont été testées. S'il s'était agi de véritables attaques, la plupart des participants ne les auraient probablement pas détectées.

Ceux qui ont bien réussi pendant les simulations jouissaient d'outils technologiques robustes pour les aider à déceler et à journaliser les incidents de cybersécurité. En outre, ces outils envoyaient également des alertes pour leur permettre d'intervenir le plus efficacement possible.

Pratiquement tous les participants ont indiqué qu'ils n'avaient jamais testé leurs capacités de détection auparavant. Les recherches de KPMG révèlent que les fournisseurs de services de sécurité gérés (FSSG) n'effectuent pas fréquemment d'exercices de type « Purple Team » pour tester leurs environnements. Par conséquent, nombre d'entreprises pourraient exploiter leurs activités en vertu de cas d'usage de détection inefficaces – et ainsi avoir un faux sentiment de sécurité.

Les tests de simulation sont avantageux pour les entreprises de toutes les tailles

Nombre de personnes croient à tort que les exercices de type « Purple Team » ne sont destinés qu'aux grandes sociétés. Ce type d'exercice profite aux entreprises de toutes les tailles, surtout quand leur portée et leur approche cadrent avec le profil de risque, les ressources et le degré de maturité d'une entreprise. Les interruptions de service et les brèches

Comme **les petites et moyennes entreprises** (PME) n'ont souvent pas de moyens de défense en place, elles sont de plus en plus ciblées par les cybercriminels. Les exercices de type « Purple Team » les aident à déterminer les vulnérabilités de leurs systèmes, à tester leurs moyens de défense et à améliorer leurs processus de sécurité de manière rentable. Ils les sensibilisent et contribuent à renforcer la culture de sécurité des organisations aux ressources limitées.

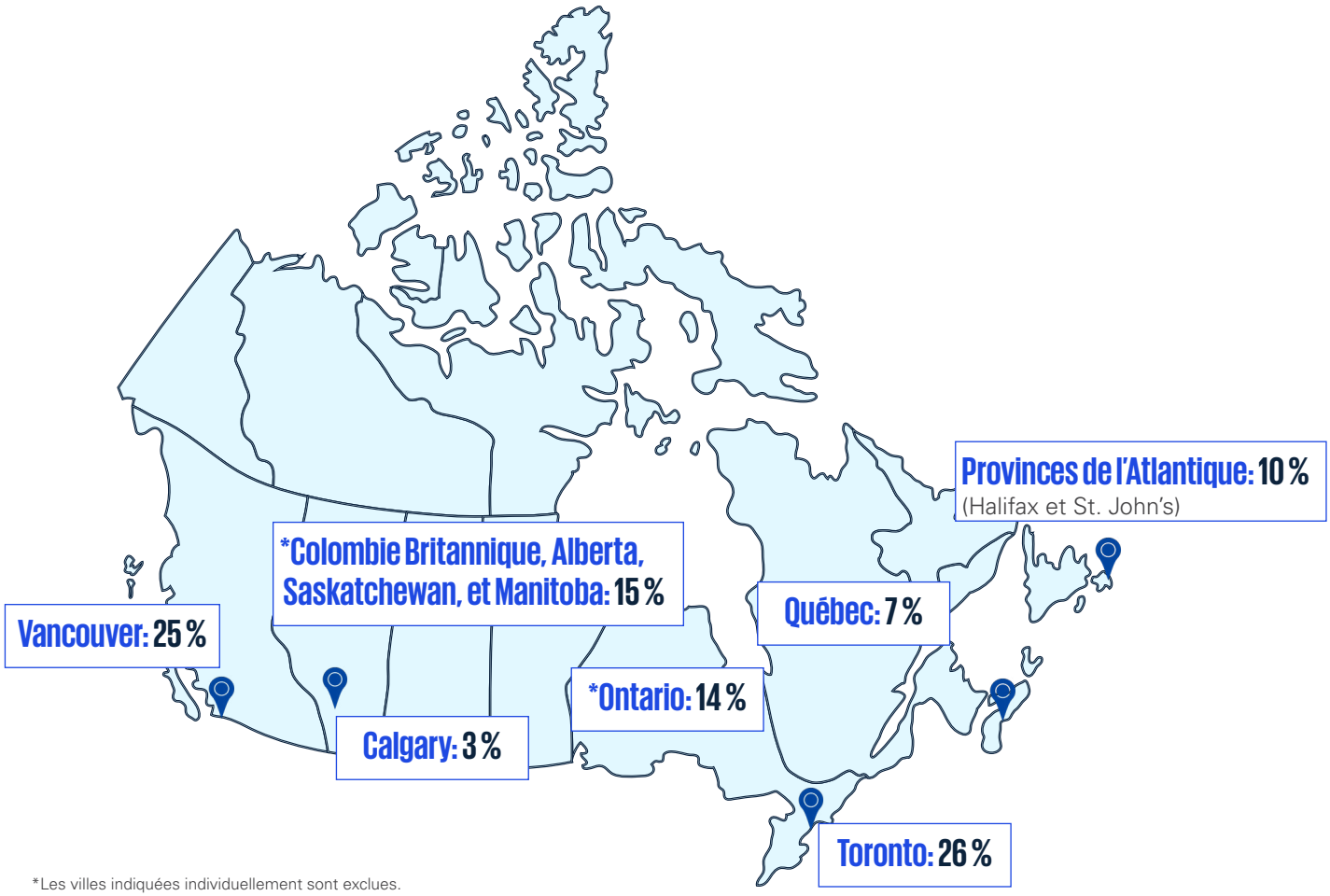
Les **entreprises du marché intermédiaire** doivent jongler avec les complexités grandissantes des environnements informatiques (comme l'infonuagique et l'Internet des objets), tout en continuant de composer avec des contraintes en matière de ressources. Elles font souvent partie de chaînes d'approvisionnement plus vastes, ce qui en fait des cibles plus attrayantes pour les attaquants qui visent les infrastructures essentielles ou les partenaires des entreprises.

Les **grandes sociétés** constituent des cibles de grande valeur pour les MPA, les rançongiciels et les attaques d'États-nations. En présence d'écosystèmes informatiques complexes et d'équipes virtuelles, les exercices de type « Purple Team » permettent d'assurer la collaboration et la coordination entre les équipes « Red Team » et « Blue Team ». Ils servent à valider l'efficacité des outils et des stratégies de sécurité, à peaufiner les processus d'intervention en cas d'incident et à respecter les exigences en matière de conformité.

Les interruptions de service et les brèches peuvent avoir des conséquences catastrophiques, notamment entraîner des risques liés à la sécurité, des pertes financières, des atteintes à la réputation et même des pertes de vies humaines. Du coup, les simulations de type « Purple Team » peuvent jouer un grand rôle dans les activités de cybersécurité d'une entreprise, quels que soient sa taille et son secteur.

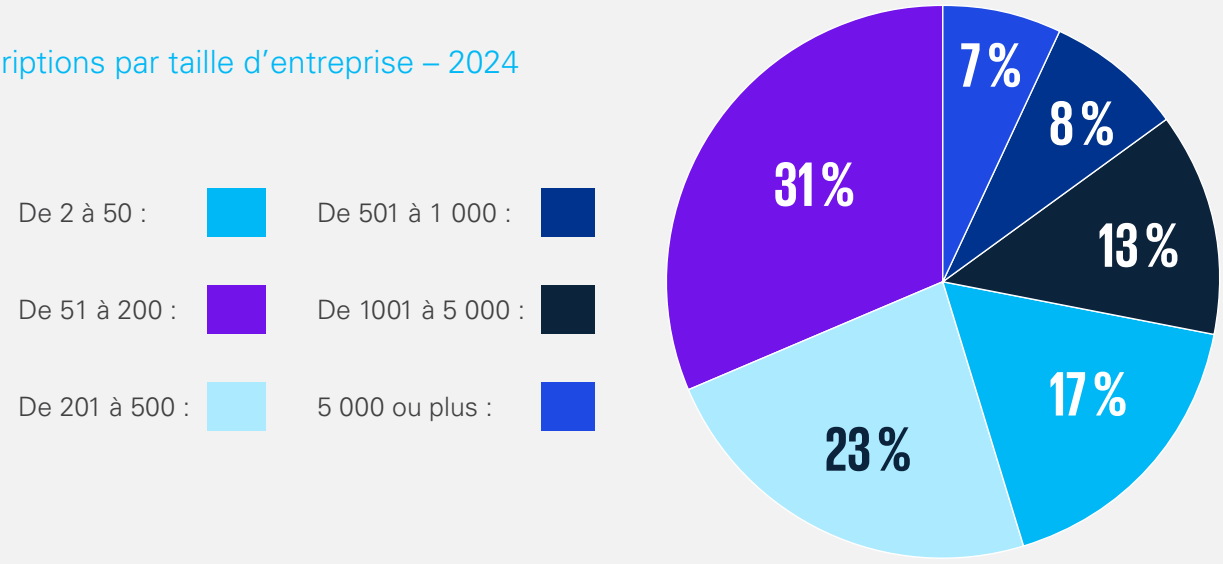
Données démographiques sur les participants

Inscriptions par province – 2024

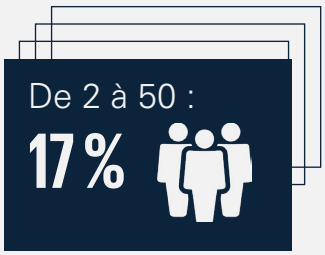


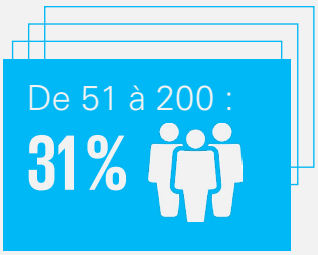
*Les villes indiquées individuellement sont exclues.

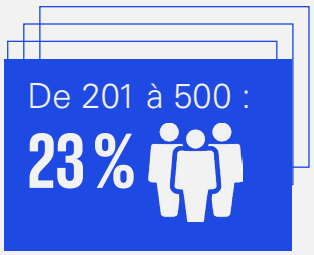
Inscriptions par taille d'entreprise – 2024



Trois plus importantes inscriptions par taille d'entreprise – 2024



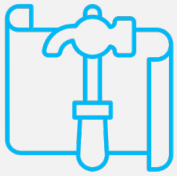




Trois plus importantes inscriptions par secteur d'activité – 2024

Services financiers :
20 %

Technologie :
20 %



Construction :
15 %

Inscriptions par rôle – 2024

Soutien des technologies de l'information	19 %	Services administratifs et juridiques	10 %
Administrateurs et cadres supérieurs	14 %	Gestion opérationnelle	7 %
Hauts dirigeants	14 %	Responsables de la cybersécurité	5 %
Gestion financière	14 %	Innovation et développement technologique	5 %
Poste de direction en technologies de l'information	10 %	Poste de direction en ventes et marketing	2 %

À quoi s'attendre en 2025

Étant donné que les cybermenaces continuent d'évoluer, 2025 devrait être marqué par de nouveaux défis et des attaques plus sophistiquées. Les entreprises subiront une pression accrue pour s'adapter. Selon les enquêtes de KPMG et les tendances sectorielles, les facteurs clés suivants devraient modeler le paysage de la cybersécurité pour l'année à venir :

Tactiques de rançonnage et d'extorsions plus ciblées
Les groupes d'attaquants par rançongiciel vont fort probablement cibler leurs victimes de manière plus stratégique, de façon à augmenter les probabilités d'être payés tout en poursuivant leurs tactiques de double et de triple extorsions pour optimiser leurs répercussions. Attendez-vous à des temps d'attente plus courts et à des tactiques de négociation plus vigoureuses.

Tensions géopolitiques influant sur les cyberactivités
Les conflits mondiaux et les mutations économiques alimenteront la hausse de la cyberactivité des États qui cibleront des infrastructures essentielles, des entités gouvernementales et des secteurs à valeur élevée. L'espionnage, la manipulation des données et les attaques destructives pourraient devenir plus fréquents, et toucher des entreprises coincées dans les conflits géopolitiques. Ainsi, KPMG croit que les outils technologiques (matériels et logiciels) conçus par des États adversaires du Canada feront l'objet d'une surveillance accrue et, potentiellement, de sanctions.

Risques croissants dans le nuage
Avec l'augmentation de l'empreinte infonuagique des entreprises, les attaquants exploiteront de plus en plus les environnements infonuagiques mal configurés, les protocoles d'application à faible sécurité et les comptes à hauts privilèges pour pénétrer l'infrastructure des entreprises.

Utilisation continue des attaques propulsées par l'IA
L'évolution rapide de l'intelligence artificielle (IA) permet aux acteurs de menaces d'accroître leur utilisation des modèles de langage pour concevoir des attaques par hameçonnage personnalisées et contourner les mesures de sécurité et accélérer les intrusions.

Accès plus facile aux menaces du jour zéro
Le marché clandestin des vulnérabilités de jour zéro continue de grandir, et donc fournit un meilleur accès à des vulnérabilités utilisées comme armes.

03 Renseignements sur les cybermenaces

Sommaire

Les difficultés géopolitiques et économiques de 2024 ont été stimulées par les importants développements observés dans les services de renseignements sur les cybermenaces, soit les États tentant de s'attaquer au problème des rançongiciels, la prolifération des cyberguerres et de leurs répercussions, l'exploitation de l'IA par les attaquants, l'hacktivisme, l'espionnage et les acteurs de menaces étatiques. Ces changements s'observent dans tout le paysage de la cybercriminalité et devraient être pris en compte lors de la planification stratégique du programme de cybersécurité des entreprises en 2025 et au-delà.

Situation du côté des rançongiciels

Au cours des dernières années, le modèle de rançongiciel en tant que service a gagné en popularité auprès des acteurs de menaces, puisqu'il leur permet d'attaquer des organisations dans le monde entier. Cette onde de cyberattaques a attiré l'attention des autorités, et mis en évidence l'urgence de contre-attaquer les activités malveillantes des groupes de rançongiciels.

Depuis la fin de 2022, le FBI (Federal Bureau of Investigation), en collaboration avec d'autres organismes d'application de la loi, a infiltré le réseau de plusieurs groupes d'attaquants par rançongiciels. Bien que ces actions les aient secoués, les groupes ciblés se sont pour la plupart repositionnés, reconstruits ou réorganisés, se sont joints à d'autres groupes ou ont formé de nouvelles entités, et ont posé des défis importants aux organismes d'application de la loi. Même si les mesures prises par ces derniers en 2024 ont été bien accueillies, elles n'ont pas nécessairement eu un effet majeur sur la scène de la criminalité.

Pour contextualiser la situation, notre équipe a résumé les efforts accomplis pour démanteler deux acteurs de l'espace des rançongiciels : ALPHV/BLACKCAT et LOCKBIT 3.0.

Groupe de rançongiciels ALPHV/BLACKCAT

En décembre 2023, des organismes d'application de la loi ont démantelé le groupe de rançongiciels ALPHV/BLACKCAT, né du repositionnement de DARKSIDE et de BLACKMATTER. La vaste opération visait à perturber les activités illicites du groupe bien connu, lesquelles ont potentiellement été propulsées par l'association du groupe à la très médiatisée cyberattaque contre MGM au début de 2023. Malgré la réussite initiale de l'opération, le groupe a rapidement relancé ses activités, et visé nombre d'institutions, y compris des hôpitaux – un secteur qu'il avait jusqu'alors épargné.

À son retour, le groupe ALPHV a réussi à pénétrer les systèmes d'un hôpital et lui a demandé une rançon de 22 M$. Après cet incident, les membres affiliés au groupe ALPHV ont allégué que ce dernier avait filé avec la rançon, ce qui indique un conflit interne potentiel et une perte de confiance au sein du groupe.

L'opération de démantèlement du FBI a peut-être eu des retombées négatives pour les membres affiliés au groupe ALPHV, au point de laisser croire que ce dernier planifiait une escroquerie de sortie. Alors que le groupe ALPHV/BLACKCAT semble avoir quitté la scène des rançongiciels, nombre de ses membres affiliés ont possiblement joint d'autres familles de rançongiciels pour maintenir le cycle de cybercriminalité en place. Par ailleurs, on soupçonne les membres restants du groupe ALPHV d'avoir changé d'image et de nom, et de continuer de propager les menaces des groupes de rançongiciels.

Sources : *Security Week: Cybersecurity News, Insights, and Analysis*, 6 mars 2024; Reuters, 23 février 2024; *Infosecurity Magazine*, 19 décembre 2023; CSO Online, 6 octobre 2023;

Tentative de démantèlement du groupe LOCKBIT 3.0

En février 2024, le FBI a lancé une vaste opération contre le fameux groupe de rançongiciels LOCKBIT 3.0 et pris le contrôle de ses serveurs. Dans le cadre de cette opération, il a notamment utilisé le site Web clandestin du groupe pour diffuser des messages concernant sa prise de contrôle – une démarche stratégique visant à perturber les activités du groupe.

Toutefois, deux jours plus tard, le groupe LOCKBIT 3.0 a démontré sa résilience en lançant un nouveau site. Ce groupe est reconnu comme l'un des plus actifs dans le monde de la cybercriminalité. Il fonctionne par le truchement d'un réseau de membres affiliés, ce qui lui permet de cibler une grande variété d'entreprises dans le monde.

Avant l'intervention du FBI, LOCKBIT a lancé une attaque qui a fait les manchettes contre le comté de Fulton aux États-Unis, qui lui a permis, selon lui, d'avoir accès à des fichiers de données sensibles. Il a alors demandé une rançon de 1,2 G$. L'attaque a perturbé les services, et la démarche de reprise des activités s'est étalée sur plus de deux mois.

Malgré les efforts déployés par les organismes d'application de la loi pour démanteler le groupe LOCKBIT 3.0, ce dernier a conservé son statut de joueur majeur du domaine des rançongiciels tout au long de 2024. Selon les observations de KPMG, LOCKBIT aurait infiltré environ 14 entreprises canadiennes pendant cette période, ce qui montre la menace persistante que présente le groupe et révèle les défis que doivent relever les organismes d'application de la loi pour freiner ses activités.

Sources : *Infosecurity Magazine*, 26 février 2024; *Resecurity*, 4 mars 2024.

Menaces de rançongiciels à l'horizon

Les exploitants de rançongiciels ont appris qu'ils devaient, pour maximiser leurs répercussions, raffiner leurs outils, leurs tactiques et leurs techniques. Les probabilités de réussite d'une attaque perpétrée au moyen d'outils non éprouvés contre une société mature dotée d'un environnement hautement surveillé et protégé sont faibles. Pour cette raison, nombre des acteurs de menaces vont parfaire leur art dans des pays en développement.

Les cyberattaques contre le Costa Rica et la République dominicaine, en 2022, constituent des exemples de ce procédé. Lors de ces attaques, les acteurs de menaces CONTI et QUANTUM RANSOMWARE ont lancé d'importantes opérations contre des entités gouvernementales. Dans le cas de l'attaque de CONTI, leur intention annoncée était de renverser le gouvernement au moyen d'une cyberguerre.

L'Instituto Agrario Dominicano (l'équivalent du ministère de l'Agriculture) de la République dominicaine a été spécifiquement ciblé, ce qui a suscité une enquête proactive. Celle-ci a révélé que CONTI avait semé un logiciel malveillant dans la région dix mois avant les attaques. Cette découverte signale l'utilisation d'une stratégie à long terme pour infiltrer l'environnement de la victime et exploiter ses vulnérabilités, et démontre la patience et la persistance dont les attaquants ont fait preuve tout au long de 2024. Le choix des victimes, qui n'avaient probablement pas les moyens de payer une rançon, suggère que ces attaques ont aidé les pirates à perfectionner leurs techniques et à évaluer l'efficacité de leur programme malveillant dans des environnements moins bien protégés.

Les cyberincidents observés par la suite dans d'autres pays en développement, tels que le Sénégal, le Chili, la Colombie et l'Argentine, confirment que ces attaques font partie d'une stratégie plus vaste employée par les acteurs de menaces pour tester leurs méthodes. La transformation numérique rapide de nombreux pays africains, combinée à la difficulté constante de maintenir un mur de défense robuste contre les cyberattaques, fait de ces régions des cibles particulièrement tentantes. Les organisations de ces pays, dont les banques et les institutions gouvernementales, peinent à rester à jour en matière de cyberdéfense. Elles constituent donc sans le vouloir un terrain fertile pour l'expérimentation.

En exploitant les vulnérabilités dans les pays en développement, les acteurs de menaces peuvent fignoler leurs tactiques et leurs outils pour, ultimement, obtenir un avantage concurrentiel lorsqu'ils visent les systèmes plus résilients des pays développés, comme les États-Unis, le Canada et le Royaume-Uni.

Ce cycle d'exploitation ne met pas uniquement les victimes immédiates en danger. Il pose un danger plus grand à la cybersécurité mondiale, puisque les attaques fructueuses dans les pays en développement peuvent mener à des opérations plus complexes et dommageables dans des pays dotés de solides moyens de défense.

Sources : BleepingComputer.com, 24 août 2022; *Financial Times*, 9 juillet 2022.

Cyberguerre et ses conséquences

L'utilisation étatique de cyberarmes dans les conflits classiques et le transfert de ces outils, de ces tactiques et de ces techniques dans les mains du monde interlope soulèvent des préoccupations depuis longtemps. Ces dernières se sont raffermies en 2024, avec la tenue d'importantes attaques liées au conflit entre la Russie et l'Ukraine, et la probabilité que des logiciels malveillants dévastateurs ciblant les systèmes de contrôle industriel (SCI) se retrouvent dans le monde criminel.

Portée des nouveaux programmes malveillants grâce aux cyberarmes

La cyberattaque du réseau Lvivteploenergo, dans la région de Lviv, en Ukraine, en janvier 2024, fut un incident majeur. Les attaquants ont probablement infiltré le réseau près d'un an plus tôt, soit le 17 avril 2023, en exploitant une vulnérabilité non relevée d'un routeur Mikrotik exposé à l'Internet. L'absence de segmentation adéquate du réseau a permis aux adversaires de manipuler les routes réseau codées en dur, et d'accéder aux contrôleurs du système de chauffage du district. Par la suite, ils ont installé une version allégée du micrologiciel ne comprenant pas de fonctions de surveillance, ce qui leur a évité d'être détectés.

Des mois après l'attaque, le logiciel malveillant FrostyGoop a été repéré et associé à l'incident. Il cible tout particulièrement le protocole Modbus, qui est largement utilisé dans le milieu industriel. Il est reconnu comme le neuvième logiciel malveillant en importance s'attaquant aux SCI, après CosmicEnergy et Industroyer2, qui ont aussi été associées à des tentatives du groupe SANDWORM visant à compromettre les fournisseurs d'énergie ukrainiens.

Même si l'acteur de menaces demeure inconnu, l'attaque semble liée à une adresse IP de Moscou. Ces tactiques et ces programmes malveillants peuvent servir de plan directeur pour d'autres acteurs de menaces qui souhaitent attaquer des infrastructures SCI pour des motifs financiers.

En mars 2024, les menaces du groupe SANDWORM appuyé par la Russie se sont intensifiées, ce qui a entraîné le dévoilement du logiciel malveillant – jusque-là indétecté – utilisé par le groupe pour attaquer 20 installations, dans 10 régions de l'Ukraine, dans des secteurs essentiels, comme ceux de l'énergie, de l'eau et du chauffage. La campagne se voulait fort probablement une réplique aux attaques de l'Ukraine contre la Russie. Elle utilisait quatre variants de logiciel malveillant : BIASBOAT (fondé sur le langage Linux), LOADGRIP (fondé sur le langage Linux), GOSSIPFLOW (fondé sur le langage Go) et la porte dérobée Kapeka, un successeur du logiciel malveillant GreyEnergy de SANDWORM, lui-même un variant de BlackEnergy. Ce dernier a été utilisé pour attaquer le réseau électrique de l'Ukraine en 2015.

Source : *Cybernews – Latest Cybersecurity and Tech News, Research & Analysis*, 23 juillet 2024

Sous-groupes associés à SANDWORM

Quelques jours avant cette vaste attaque contre l'Ukraine, les activités de quatre petits fournisseurs de services Internet ukrainiens ont été perturbées. Le groupe hacktiviste SOLNTSEPEK, associé à la Russie, a revendiqué ces attaques. Il a de plus déclaré avoir obtenu les bases de données des clients et les données internes des entreprises victimes. Ce groupe a proclamé avoir préalablement déclenché l'attaque contre Kyivstar, un des grands opérateurs en télécommunications de l'Ukraine, en décembre 2023, qui s'est avéré une cyberattaque très perturbatrice. Elle a en effet touché des millions de clients qui ont été privés de services pendant plusieurs jours. SOLNTSEPEK serait un pseudonyme ou une identité d'emprunt pour SANDWORM liant potentiellement ce dernier à ces attaques.

Bien que les activités de SANDWORM aient été concentrées en Ukraine, il semblerait que les sous-groupes qui y sont affiliés cibleraient plutôt des installations aux États-Unis, en Pologne et en France. Le sous-groupe associé à SANDWORM appelé Cyber Army of Russia Reborn (CARR) a revendiqué des attaques perpétrées dans ces trois pays. L'attaque de janvier 2024 contre un système d'alimentation en eau au Texas a entraîné le débordement d'un réservoir d'eau. Pour révéler la brèche, CARR a lancé une chaîne YouTube pour montrer comment il avait manipulé les systèmes informatiques de l'installation.

La constante prise en cible des SCI et des technologies opérationnelles (TO) prouve la valeur que les adversaires donnent aux infrastructures critiques. Les acteurs commandités par un État cherchent à obtenir des avantages stratégiques dans des conflits géopolitiques, tandis que les hacktivistes continuent de revendiquer des attaques contre des infrastructures critiques pour transmettre leurs messages et semer la peur, l'incertitude et le doute. Les acteurs par rançongiciels continueront certainement d'exploiter la convergence grandissante des réseaux de TI et de TO, et de miser sur les piètres pratiques de sécurité et la segmentation de réseau pour accéder aux systèmes industriels.

Comme ces menaces se perfectionnent, les entreprises doivent être proactives et renforcer leurs défenses critiques. Elles doivent mettre l'accent sur les contrôles de sécurité multicouches, la surveillance continue et le strict respect des exigences réglementaires pour arrêter cette escalade des menaces contre les SCI et les environnements de TO.

Mise à profit de l'intelligence artificielle par les acteurs de menaces

En février 2024, OpenAI, l'entreprise d'intelligence artificielle derrière ChatGPT, et Microsoft, ont annulé des comptes associés à cinq groupes étatiques. Les acteurs de menaces de différents pays ont été identifiés, dont certains ciblaient des infrastructures critiques. En réponse à ces menaces, Microsoft a publié de façon proactive des directives pour prévenir la mauvaise utilisation de ses systèmes d'IA par les acteurs de menaces étatiques.

Ces directives comportent plusieurs mesures clés :

- Le repérage et l'interruption de l'utilisation malveillante des technologies d'IA
- L'importance de partager les constats avec les autres fournisseurs d'IA pour favoriser l'adoption d'une approche collaborative en matière de sécurité
- La nécessité de gérer les risques associés au déploiement de l'IA
- La consignation des activités liées aux acteurs de menaces pour mieux comprendre le portrait et améliorer les stratégies d'intervention
- La présentation des contre-mesures prises par l'entreprise pour limiter les menaces

Ces mesures démontrent l'engagement de la société à protéger les technologies de l'IA, surtout face à la hausse des menaces provenant des acteurs commandités par un État.

ChatGPT-4 pour exploiter les systèmes en utilisant uniquement les alertes de sécurité publique

En 2024, plusieurs observations ont démontré comment ChatGPT-4 peut être utilisé pour exploiter les vulnérabilités, et ce, uniquement à l'aide des alertes de sécurité publique en guise de source. L'agent d'IA a été utilisé pour tester 15 vulnérabilités connues des logiciels à code source libre – qu'il a d'ailleurs réussi à exploiter dans 78 % des cas. Un acteur de menaces qui met à profit des outils comme GPT-4 pourrait automatiser l'exploitation des vulnérabilités dès leur publication.

À l'avenir, l'impact de l'IA dans le domaine des cybermenaces sera profond et multiple. La capacité des outils d'IA, comme GPT-4, d'exploiter les vulnérabilités ne fait pas qu'accélérer la rapidité à laquelle les cybermenaces peuvent être perpétrées. Elle soulève aussi d'importantes questions concernant la sécurité des infrastructures numériques. L'IA continuera d'évoluer, et la course entre les attaquants et les victimes s'intensifiera. Il deviendra impératif que les parties prenantes adaptent et modifient leurs approches relatives à la cybersécurité.

Sources : *WIRED*, 17 avril 2024; *Cyber Security News*, 24 avril 2024; *The Record Media*, 22 mars 2024; *Restack*, 18 février 2025; Microsoft Tech Community – Educator Developer Blog, 11 décembre 2024; *Cyber Security News*, 22 avril 2024; *The Hacker News*, 14 février 2024.

Hacktivisme et menaces par déni de service distribué (DDoS) en 2024

L'hacktivisme réalisé au moyen d'attaques DDoS constituait toujours une menace en 2024 et ce sera probablement encore le cas en 2025. Les groupes d'hacktivistes sont reconnus pour leurs cyberactivités politiquement motivées qui visent souvent des infrastructures liées aux États ou à des organisations qu'ils perçoivent comme des adversaires, ou encore qui servent à faire des déclarations politiques.

Les répercussions opérationnelles de bon nombre de ces attaques ont été minimes, et certaines attaques n'ont même pas été confirmées. Cependant, nous devrions assister à une poursuite de ce type de menace en 2025 avec l'aggravation des tensions géopolitiques.

Attaques DDoS contre des entités canadiennes

En mai 2024, le groupe d'hacktivistes NONAME057(16) a revendiqué de multiples attaques par déni de service distribué (DDoS) contre diverses organisations européennes. À la mi-juin 2024, il indiquait avoir des entités canadiennes dans sa mire. Il a affirmé avoir lancé une attaque par DDoS contre le fournisseur de télécommunications TELUS et une entreprise financière du Québec.

En mai 2024, l'aéroport international Richardson de Winnipeg a subi une attaque par DDoS considérable, laquelle a perturbé ses services en ligne et affecté l'accès aux passagers. Deux groupes d'hacktivistes ont indiqué en être les auteurs : HACKNET et PEOPLE'S CYBER ARMY. Ces groupes sont reconnus pour leurs cyberactivités politiquement motivées qui visent souvent des infrastructures liées aux États qu'ils perçoivent comme des adversaires, ou encore qui servent à faire des déclarations politiques. Même si les motifs précis de l'attaque contre l'aéroport n'ont pas été explicités, des attaques similaires de ces groupes se sont souvent avérées être liées à de plus vastes tensions géopolitiques, dont des réactions contre les politiques du gouvernement ou les mesures prises par des États participant à des conflits internationaux.

Le 22 novembre 2024, le groupe d'hacktivistes pro-russe NONAME057(16) a revendiqué une série d'attaques par DDoS exécutées contre plusieurs sites Web (entreprises de télécommunications et entités gouvernementales canadiennes). Parmi les organisations touchées figurent des ministères du gouvernement et des fournisseurs de services de transport (portail de service à la clientèle). Les revendications de NONAME057(16) n'ont pu être vérifiées, et le groupe affiche un historique de fausses menaces, utilisées pour intimider.

Sources : : X, 13 juin 2024; Daily Dark Web, 24 mai 2024.

Menaces d'États et menaces contre la sécurité nationale émergentes

Les activités attribuées aux acteurs commandités par un État sous-entendent habituellement la collecte des données stratégiques de gouvernements et d'entreprises privées. Pouvant baigner dans l'espionnage, les acteurs de menaces commandités par un État sont souvent intéressés par la technologie ayant des applications économiques ou militaires potentielles, comme l'informatique quantique, les réseaux 6G et l'équipement aéronautique.

Le Centre de la sécurité des télécommunications Canada (CST) a attiré l'attention sur des MPA provenant de la Chine, de la Russie et de l'Iran. Cela dit, il a aussi ajouté l'Inde à la liste des menaces émergentes, précisant que son intérêt potentiel pour l'espionnage des systèmes gouvernementaux canadiens contribuait aux récentes tensions diplomatiques.

Une administration provinciale canadienne parmi les victimes d'acteurs de menaces commandités par un État

Une cyberattaque présumément commanditée par un État a été portée contre 22 boîtes de courriels du gouvernement de la Colombie-Britannique; elle aurait potentiellement compromis les renseignements sensibles de 19 personnes. Le 3 juin 2024, le ministre de la Sécurité publique a confirmé que seuls les fichiers d'employés avaient été touchés et que les personnes concernées en avaient été informées. L'administration a détecté la brèche le 10 avril 2024. En réaction, les représentants ont demandé aux fonctionnaires en question de changer leurs mots de passe. L'acteur de menaces ou l'État derrière cet incident est inconnu. Cela dit, un rapport subséquent alertait les Canadiens sur l'ingérence étrangère persistante dans les affaires politiques canadiennes.

Microsoft visée par Midnight Attack

En janvier, Microsoft a confirmé avoir subi une brèche après une attaque par rafale de mots de passe d'un groupe commandité par un État lié au Service de renseignements extérieurs (SVR) de la Russie appelé BLUEBRAVO. Ce dernier a ainsi pu accéder à un ancien compte pour environnement de test dont la fonction d'authentification à deux facteurs n'avait pas été activée, bénéficiant ainsi d'un accès aux systèmes compromis de la société.

Infiltration de plusieurs fournisseurs de large bande américains par SALT TYPHOON

En 2024, le groupe appuyé par un État SALT TYPHOON a infiltré une dizaine de grandes entreprises américaines du secteur des télécommunications. Selon ce qui a été rapporté, les adversaires auraient recueilli des renseignements sensibles sur des citoyens américains, y compris sur leurs habitudes de communication – tout particulièrement leurs interlocuteurs, les dates des communications et leur emplacement géographique.

Sources : *The Record Media*, 4 juin 2024; BleepingComputer.com, 8 mars 2024; Microsoft Threat Intelligence, 25 janvier 2024; CNET, 8 octobre 2024; Dark Reading, 25 septembre 2024; *Malicious Life* by *Cybereason*, aucune date.

SALT TYPHOON aurait notamment indiqué avoir écouté des communications non chiffrées sur des appareils mobiles de nombreux hauts politiciens américains. Les évaluations initiales suggèrent que les attaquants ont la capacité d'accéder aux données de tous les citoyens américains, ce qui montre l'intérêt du groupe étatique pour la surveillance des activités d'Américains moins connus. En réaction, le Consumer Financial Protection Bureau (CFPB) du gouvernement américain a transmis des directives à ses employés les enjoignant d'éviter d'utiliser leur téléphone cellulaire personnel pour leurs communications de nature professionnelle. Il les a plutôt invités à utiliser les plateformes sécurisées à leur disposition pour tenir leurs réunions et leurs échanges comportant des données non publiques. Cet incident souligne l'importance d'utiliser des canaux de communication chiffrés pour protéger les données sensibles contre les adversaires potentiels.

L'augmentation de l'empreinte numérique du Canada et les mesures de cybersécurité vieillissantes offrent des occasions aux acteurs de menaces. Le paysage changeant des menaces nécessite une plus grande collaboration entre les agences fédérales et provinciales, et les partenaires du secteur privé. Les plateformes de partage d'information fondées sur l'initiative i100 du Royaume-Uni, les protocoles exhaustifs de réponse aux incidents et les investissements massifs dans les infrastructures de cybersécurité pourront aider à atténuer les risques que posent les cybermenaces avancées.

Menaces émergentes pour la sécurité nationale

Menaces internes

Adversaires nord-coréens se faisant passer pour des travailleurs des TI pour décrocher des emplois à l'international

Le 23 juillet 2024, une entreprise de cybersécurité américaine a signalé qu'elle avait embauché par inadvertance un travailleur des TI affilié à la Corée du Nord pour un poste à distance en ingénierie. Cet événement est survenu près de trois mois après qu'un organisme d'application de la loi américain ait inculpé plusieurs personnes impliquées dans une vaste manœuvre frauduleuse d'embauche, et signalé que des travailleurs des TI associés à la Corée du Nord avaient fraudé 300 entreprises et touché des « millions » pour le régime.

L'entité touchée a avoué n'avoir détecté aucune anomalie lors de la vérification des antécédents du nouvel employé et de ses autres procédures de traitement des demandes d'emploi qui comprenaient plusieurs entrevues vidéo. Pour poser sa candidature, le fraudeur aurait utilisé une photo modifiée par IA ainsi que des renseignements obtenus grâce au vol d'une identité aux États-Unis.

L'entreprise qui l'a embauché a repéré l'activité frauduleuse quand le nouvel employé a tenté de téléverser un logiciel malveillant et d'autres programmes non autorisés dans son portable fourni par l'entreprise. Depuis au moins 2020, on voit des groupes de cyberespionnage commandités par la Corée du Nord tenter de placer des personnes à des postes au sein d'entreprises de l'Occident des secteurs des TI, de la cryptomonnaie et du développement de logiciels.

Technologie mise à profit dans les attaques des adversaires

Routeurs TP-Link : une menace potentielle pour la sécurité nationale

TP-Link, un fournisseur mondial d'équipements de réseautage Wi-Fi et d'appareils pour maison intelligente, a fait l'objet d'une surveillance accrue en raison d'un niveau inhabituellement élevé de vulnérabilités dans les routeurs. Les attaquants ont exploité ces vulnérabilités pour réaliser divers actes malveillants, dont la création de puissants réseaux de bots informatiques. Les groupes commandités par un État, comme VOLT TYPHOON et CAMARO DRAGON, ont été tout particulièrement actifs, le premier étant notoire pour sa campagne de piratage contre des infrastructures importantes des États-Unis, et le dernier, pour l'implantation d'un micrologiciel dans les routeurs TP-Link d'entités d'affaires étrangères européennes.

L'exigence pour les chercheurs chinois en sécurité de signaler les vulnérabilités au gouvernement chinois avant de les annoncer au grand public – ce qui pourrait permettre aux attaquants commandités par un État de les exploiter – préoccupe les organismes d'application de la loi. Cette information est particulièrement pertinente, car de nombreux groupes de MPA sont connus pour cibler les routeurs afin d'obtenir un accès initial.

Sources : Arstechnica, 24 juillet 2024; The Global Authority on PC Games, 20 août 2024; Cybernews, 15 août 2024.

Sécurité nationale menacée par la technologie d'identification, de détection et de télémétrie par laser (LIDAR) chinoise

Un rapport de 2024 de la Foundation for Defense of Democracies a soulevé des questions relativement aux répercussions de la technologie de télédétection avancée de la Chine, spécialement la technologie de détection et de télémétrie par laser, sur les infrastructures essentielles et la sécurité nationale. La technologie LIDAR, qui se sert des impulsions laser pour générer des cartes tridimensionnelles détaillées, est de plus en plus intégrée aux systèmes essentiels, y compris ceux liés à la sécurité publique, au transport et aux services publics.

Le rapport révèle que les entreprises chinoises se taillent une place de choix dans le marché mondial de la technologie LIDAR, ce qui pourrait représenter une menace pour les intérêts américains et occidentaux. L'intégration de capteurs LIDAR fabriqués en Chine aux infrastructures essentielles inquiète en raison du potentiel d'espionnage et de sabotage, puisque ces technologies pourraient fournir au gouvernement chinois un accès à des données sensibles ou encore lui donner la capacité de perturber des activités vitales. Cela fait écho à des préoccupations antérieures formulées à propos de la technologie de communication de Huawei, qui fait l'objet d'allégations semblables. À la lumière de ces constatations, les législateurs américains proposent des lois conçues pour restreindre la technologie LIDAR chinoise et encourager les pays à concevoir et à fabriquer de telles technologies.

Sources : Foundation for Defense of Democracies, 2 décembre 2024; Reuters, 2 décembre 2024.

Importantes vulnérabilités en 2024

Bien que l'essentiel de ce rapport porte sur les menaces stratégiques provenant d'acteurs étatiques, de groupes de rançongiciels, de l'IA, d'hacktivistes et d'autres malfaiteurs, la vulnérabilité la plus commune continue de se présenter sous la forme d'un fort vecteur d'accès initial aux systèmes menant à d'importantes attaques et perturbations.

Dans cette optique, l'équipe présente ici un sommaire des plus importantes vulnérabilités rapportées en 2024 dont il faudrait tenir compte, tant pour y remédier que se souvenir que la gestion des vulnérabilités constitue la base d'un programme de sécurité efficace

CVE-2024-45387 : Une vulnérabilité par injection SQL du contrôle d'opérations des versions 8.0.0 à 8.0.1 de la fonctionnalité de contrôle d'accès d'Apache permet à un utilisateur doté de privilèges et d'un rôle d'administrateur (« Admin »), de fédération (« Federation »), d'exploitation (« Operations »), de portail (« Portal ») ou de direction (« Steering ») d'exécuter des commandes SQL arbitraires dans la base de données en envoyant une requête PUT spécialement conçue. Un pirate pourrait exploiter cette vulnérabilité à distance et faire une attaque par injection SQL pour contourner le processus d'authentification du système ciblé.

CVE-2024-52046 : Le décodeur de sérialisation d'objets d'Apache MINA utilise le protocole de désérialisation natif de Java pour traiter les données sérialisées entrantes, mais il n'est pas doté des défenses et des contrôles de sécurité nécessaires. Cette grave vulnérabilité permet aux attaquants d'exploiter le processus de désérialisation pour envoyer des données sérialisées malveillantes spécialement conçues pouvant potentiellement permettre des attaques par exécution de code à distance. Cette faille touche plusieurs versions de la populaire bibliothèque réseau et soulève d'importantes préoccupations liées à la sécurité.

Code	Gravité	Note CVSS
CVE-2024-52046	Critique	10

Produits et versions touchés

- Versions 2.0.0 à 2.0.26 d'Apache MINA
- Versions 2.1.0 à 2.1.9 d'Apache MINA
- Versions 2.2.0 à 2.2.3 d'Apache MINA

CVE-2024-26633 : Plusieurs produits NetApp intègrent un noyau Linux. Certaines versions du noyau Linux sont sensibles à une vulnérabilité qui, quand elle est exploitée, pourrait entraîner la divulgation de renseignements sensibles ou une attaque par déni de service. Les produits touchés sont : FAS/AFF Baseboard Management Controller (BMC) – A900/9500 et FAS/AFF Baseboard Management Controller (BMC) – FAS2820.

Code	Gravité	Note CVSS
CVE-2024-26633	Critique	9.1

CVE-2024-3393 : Palo Alto Networks a signalé une très grande vulnérabilité (CVE-2024-3393) de son logiciel PAN-OS pour les pare-feu de nouvelle génération. Cette brèche permet aux attaquants non authentifiés d'utiliser la fonction de sécurité de DNS en envoyant des paquets DNS spéciaux pour engendrer un déni de service, la relance des pare-feu et le passage au mode de maintenance. Le problème découle d'un mauvais traitement des conditions exceptionnelles de la fonction de sécurité de DNS, ce qui permet aux attaquants d'envoyer des paquets nuisibles causant des pannes.

Code	Gravité	Note CVSS
CVE-2024-3393	Élevée	8.7

Produits et versions touchés

- PAN-OS 11.2 : versions inférieures à 11.2.3
- PAN-OS 11.1 : versions inférieures à 11.1.5
- PAN-OS 10.2 : versions inférieures à 10.2.8, et correctifs supplémentaires dans les mises à jour de maintenance
- PAN-OS 10.1 : versions inférieures à 10.1.14

CVE-2024-56145 : Une vulnérabilité de jour zéro critique a été découverte dans Craft CMS, un système de gestion de contenu largement utilisé et reposant sur le langage PHP. Elle permet aux attaquants non authentifiés d'exécuter du code arbitraire à distance, ce qui pose un important risque pour la sécurité de plus de 150 000 sites Web dans le monde. Elle se produit dans le réglage register_argc_argv du langage PHP, qui est activé par défaut. Ce réglage peut être exploité pour modifier le chemin des fichiers et exécuter du code malveillant pendant le processus d'amorce de Craft CMS. L'équipe responsable de Craft CMS a promptement réglé le problème en déployant les versions corrigées 5.5.2+ et 4.13.2+. and 4.13.2+.

Code	Gravité	Note CVSS
CVE-2024-56145	S. O.	S. O.

Produits et versions touchés

- Version 3.9.14 ou antérieure de Craft CMS
- Version 4.13.2 ou antérieure de Craft CMS
- Version 5.5.2 ou antérieure de Craft CMS

CVE-2024-38094 (vulnérabilité d'exécution de code à distance de SharePoint activement exploitée) : Des chercheurs ont découvert que des attaquants avaient infiltré un serveur, s'étaient déplacés dans le réseau et avaient compromis l'intégralité du domaine, et ce, pendant deux semaines sans se faire détecter. Les attaquants ont obtenu accès au système en exploitant la vulnérabilité CVE-2024-38094 (une vulnérabilité d'exécution de code à distance) d'un serveur SharePoint privé. Ils ont utilisé une série de requêtes GET et POST pour installer une porte dérobée (aussi appelée un webshell) intitulée ghostfile93.aspx dans le système ciblé. Après avoir exploité une brèche initiale découlant d'une vulnérabilité de Microsoft SharePoint, les acteurs de menaces sont allés plus loin dans le système en compromettant le compte de service Microsoft Exchange assorti de privilèges administratifs. Ils ont utilisé différents outils et différentes techniques pour accroître leur portée :

- **Impacket :** Ils ont essayé d'installer et d'exécuter cet ensemble de scripts Python pour les interactions du protocole réseau.
- **Antivirus Horoung :** Ils ont installé cet antivirus chinois pour désactiver les solutions de sécurité en place.
- **Fast Reverse Proxy (FRP) :** Ce serveur mandataire a été déployé pour garder un accès externe en passant par les pare-feu.

Les attaquants ont démontré une connaissance fine des techniques d'évasion et de pénétration de réseau :

- **Exploitation d'Active Directory :** Ils ont utilisé des outils comme ADExplorer64.exe, NTDSUtil.exe et nxc.exe pour cartographier l'environnement Active Directory et obtenir des données de connexion.
- **Collecte de données de connexion :** Ils ont utilisé Mimikatz (caché sous le nom 66.exe) pour extraire des renseignements de connexion.
- **Altération de journaux :** Ils ont désactivé la fonction de journalisation et vidé les journaux des tâches pour effacer leurs traces.
- **MPA :** Ils ont mis en place des tâches programmées dans le contrôleur de domaine pour l'outil FRP.

Les acteurs de menaces ont essayé de cacher leurs activités en changeant les journaux du système et en désactivant le processus de journalisation sur le serveur compromis. Ils ont aussi utilisé l'antivirus Huorong pour désactiver les produits de sécurité et opérer plus librement.

Code	Gravité	Note CVSS
CVE-2024-38094	Élevée	7.2

CVE-2024-47575 : L'absence d'authentification pour une fonction essentielle de FortiManager FGFM Daemon pourrait permettre à un attaquant non authentifié d'exécuter des commandes ou du code arbitraire au moyen de requêtes spécialement créées. Il a été noté qu'un nouvel acteur de menaces, UNC5820, exploitait activement cette vulnérabilité de FortiManager depuis au moins le 27 juin 2024. Il aurait activé et exfiltré des données de configuration des appareils FortiGate gérés par le programme FortiManager. Ces données contiennent des renseignements de configuration détaillés sur l'équipement géré ainsi que sur les utilisateurs et leurs mots de passe cryptés au moyen de FortiOS256. UNC5820 et d'autres cybercriminels pourraient les utiliser pour compromettre davantage FortiManager, se rendre jusqu'aux appareils Fortinet gérés et, ultimement, compromettre les environnements de l'entreprise.

En plus de mettre à jour les plus récentes versions, Fortinet a aussi offert plusieurs solutions de rechange à ceux qui ne pouvaient faire la mise à niveau sur-le-champ. Par exemple, les utilisateurs peuvent activer le réglage fgfm-deny-unknown pour empêcher les appareils inconnus d'essayer de s'inscrire à FortiManager.

Code	Gravité	Note CVSS
CVE-2024-47575	Critique	9.8

Produits et versions touchés

Produit	Version	Solution
FortiManager 7.6	7.6.0	Mise à niveau à la version 7.6.1 ou supérieure
FortiManager 7.4	Versions 7.4.0 à 7.4.4	Mise à niveau à la version 7.4.5 ou supérieure
FortiManager 7.2	Versions 7.2.0 à 7.2.7	Mise à niveau à la version 7.2.8 ou supérieure
FortiManager 7.0	Versions 7.0.0 à 7.0.12	Mise à niveau à la version 7.0.13 ou supérieure
FortiManager 6.4	Versions 6.4.0 à 6.4.14	Mise à niveau à la version 6.4.15 ou supérieure
FortiManager 6.2	Versions 6.2.0 à 6.2.12	Mise à niveau à la version 6.2.13 ou supérieure
FortiManager Cloud 7.4	Versions 7.4.1 à 7.4.4	Mise à niveau à la version 7.4.5 ou supérieure
FortiManager Cloud 7.2	Versions 7.2.1 à 7.2.7	Mise à niveau à la version 7.2.8 ou supérieure
FortiManager Cloud 7.0	Versions 7.0.1 à 7.0.12	Mise à niveau à la version 7.0.13 ou supérieure
FortiManager Cloud 6.4	Toutes les versions 6.4*	Passage à une version corrigée

CVE-2024-28987: The vulnerability impacts SolarWinds Web Help Desk (WHD) software. This flaw involves hardcoded credentials within the Web Help Desk application. Attackers can remotely access the system without authentication, allowing them to modify help desk tickets and access sensitive data. This vulnerability is extremely severe, as it can expose sensitive data, such as passwords from reset requests and shared service account credentials. SolarWinds users are urged to update to version 12.8.3 Hotfix 2 to patch this vulnerability. The fix requires prior installation of Web Help Desk 12.8.3.1813 or 12.8.3 HF1.

Analyse

Code	Gravité	Note CVSS
CVE-2024-28987	Critique	9.1

Code	Produits touchés
CVE-2024-9680	Versions Firefox antérieures à 131.0.3
	Versions Firefox ESR antérieures à 115.16.1
	Versions Firefox ESR antérieures à 128.3.1
	Versions Thunderbird antérieures à 115.16
	Versions Thunderbird antérieures à 128.3.1
	Versions Thunderbird antérieures à 131.0.1

Vulnérabilités de jour zéro dans Palo Alto PAN-OS – CVE-2024-0012 et CVE-2024-9474

Palo Alto Networks a publié des rustines de sécurité pour corriger deux vulnérabilités de jour zéro activement exploitées dans leurs pare-feu de nouvelle génération (NGFW). La CVE-2024-0012 est une vulnérabilité de contournement du processus d'authentification critique de l'interface Web de gestion PAN-OS. Cette brèche permet à un attaquant non authentifié d'obtenir un accès réseau à l'interface Web de gestion et ainsi obtenir des privilèges d'administrateur PAN-OS pour réaliser des tâches administratives, modifier la configuration ou exploiter d'autres vulnérabilités, comme la CVE-2024-9474. Cette dernière est une vulnérabilité d'élévation des privilèges qui permet à un administrateur PAN-OS d'effectuer des tâches sur le pare-feu au moyen de privilèges d'administrateur.

Le 14 novembre, Palo Alto Networks a confirmé qu'une campagne de menace exploitait activement la vulnérabilité CVE-2024-0012. Bien qu'elle ne soit pas explicitement liée à cette campagne, la vulnérabilité CVE-2024-9474 peut être exploitée en même temps que cette dernière. Des rapports font état d'environ 11 000 adresses IP exposées à l'Internet et exécutant les interfaces de gestion PAN-OS – les appareils les plus vulnérables se trouvant aux États-Unis, en Inde, au Mexique, en Thaïlande et en Indonésie. Cette vulnérabilité de jour zéro a d'abord été vue le 8 novembre 2024, quand Palo Alto a publié le bulletin PAN-SA-2024-0015 à la suite de rapports indiquant qu'un acteur de menaces inconnu vendait l'accès à cette vulnérabilité sur des forums de discussion clandestins. Aux dernières nouvelles, il n'y a aucune preuve d'exploitation publiquement disponible pour ces vulnérabilités.

Gravité et note CVSS

Code	Gravité	Note CVSS
CVE-2024-0012	Critique	9.3
CVE-2024-9474	Moyenne	6.9

Produits et versions touchés

Versions de produit	CVE-2024-0012	CVE-2024-9474	Version réparée
PAN-OS 10.1	Non touchée	Version 10.1.14-h4 et inférieure	Version 10.1.14-h6 et supérieure
PAN-OS 10.2	Version 10.2.12-h1 et inférieure	Version 10.2.12-h1 et inférieure	Version 10.2.12-h2 et supérieure
PAN-OS 11.0	Version 11.0.5-h2 et inférieure	Version 11.0.5-h2 et inférieure	Version 11.0.6-h1 et supérieure
PAN-OS 11.1	Version 11.1.4-h7 et inférieure	Version 11.1.4-h7 et inférieure	Version 11.1.5-h1 et supérieure
PAN-OS 11.2	Version 11.2.3-h3 et inférieure	Version 11.2.3-h3 et inférieure	Version 11.2.4-h1 et supérieure
Cloud NGFW	Non touchée	Non touchée	S. O.
Prisma Access	Non touchée	Non touchée	S. O.

Vulnérabilité d'un navigateur de 18 ans nuisant aux appareils tournant sous macOS et Linux

Il a été récemment divulgué qu'une vieille vulnérabilité touchait d'importants navigateurs Web et entraînait des risques de cybersécurité importants. Grâce à cette faille, surnommée la vulnérabilité « 0.0.0.0 Day », les pirates informatiques peuvent manipuler les requêtes destinées à une adresse IP précise, les redirigeant vers des serveurs privés. L'exploitation de cette vulnérabilité consiste à tromper les utilisateurs en leur faisant visiter des sites Web malveillants qui peuvent accéder à des données sensibles, et potentiellement infiltrer les réseaux internes. Soulignons que cette faille touche particulièrement les systèmes tournant sous Linux et macOS, et non ceux tournant sous Windows. Tant les particuliers que les entreprises sont à risque, ce qui démontre l'étendue de la menace que pose ce problème.

Les chercheurs ont décelé plusieurs occurrences d'exploitation active de cette vulnérabilité. Il y a notamment eu la campagne ShadowRay que ces mêmes chercheurs ont relevée en mars dernier. Elle cible les charges de travail d'IA lancées localement, sur l'équipement de développeurs, et tout spécialement les grappes de serveurs Ray. L'attaque est lancée quand une victime clique sur un lien qui a été envoyé par courriel ou qui se trouve sur un site malveillant. Cela active une commande JavaScript servant à transmettre une requête HTTP au port http://0[.]0[.]0[.]0:8265, qui est habituellement utilisé par Ray. La requête atteint la grappe de serveurs Ray locale et ouvre la porte à l'exécution de code arbitraire, aux shells inversés et à la modification de la configuration.

Dans un autre cas, la campagne a ciblé Selenium Grid. Dans ce scénario, les attaquants ont utilisé JavaScript dans un domaine public pour envoyer des requêtes au port http://0[.]0[.]0[.]0:4444. Ces dernières sont destinées aux serveurs Selenium Grid et visent à permettre aux attaquants d'exécuter du code ou de faire de la reconnaissance réseau. De plus, la vulnérabilité ShellTorch, qui a été signalée par des chercheurs en octobre 2023, liait par défaut le panneau TorchServe à l'adresse IP 0.0.0.0 plutôt qu'au serveur local, ce qui le rendait vulnérable aux requêtes malveillantes.

Même si les chercheurs ont signalé ces activités malveillantes, les développeurs de navigateurs Web ne font que commencer à réagir :

- Google Chrome, le navigateur Web le plus largement utilisé, a annoncé son intention de bloquer l'accès à l'adresse IP 0.0.0.0 par vague, en commençant par la version 128 (à venir), puis en poursuivant jusqu'à la version 133.
- Mozilla Firefox n'utilise actuellement pas d'accès réseau privé (PNA), mais c'est l'une de ses grandes priorités de développement. Un correctif temporaire a été déployé d'ici à ce qu'un tel PNA soit mis en place, même si aucune date de lancement précise n'a été donnée.
- Apple a déployé des vérifications d'IP supplémentaires dans Safari par le truchement de mises à jour WebKit, ce qui bloquera l'accès à l'adresse 0.0.0.0 dans la version 18 du navigateur qui est déployée en même temps que macOS Sequoia.

Vulnérabilité dans le langage PHP utilisé pour propager un logiciel malveillant et lancer des attaques par DDoS – CVE-2024-4577

Récemment divulguée, une vulnérabilité touchant le langage PHP et affectant des installations fonctionnant en mode CGI a été activement exploitée le lendemain de son annonce. Elle cible principalement les installations Windows dont la langue configurée est le chinois ou le japonais, bien que sa portée puisse être plus grande. Les exploitations associées à cette vulnérabilité incluent des campagnes par injection de commande et le déploiement de logiciels malveillants, comme Gh0st RAT, les mineurs de cryptomonnaie RedTail et XMRig.

Cette vulnérabilité critique a été repérée dans les versions 8.1.* de PHP (antérieures à la version 8.1.29), 8.2* (antérieures à la version 8.2.20) et 8.3* (antérieures à la version 8.3.8). Elle permet aux attaquants d'exécuter du code à distance en raison de la façon dont les modules de traitement PHP et CGI analysent des caractères Unicode précis. Différents acteurs de menaces exploitent activement cette vulnérabilité pour cibler des appareils sensibles.

Gh0st RAT est un outil d'accès à distance à code source libre qui a été transmis en tant que fichier exécutable de Windows comprimé au moyen de UPX. Dans un environnement de bac à sable, l'outil a déposé un autre fichier exécutable nommé lqgqosc.exe qui énumérait des périphériques et des lecteurs connectés tout en interrogeant le registre. Le logiciel malveillant a établi une connexion à un serveur de commande et de contrôle en Allemagne, à l'adresse IP 146[.]19[.]100[.]7 (port 8001). Une autre adresse IP (147[.]50[.]253[.]109) a été associée à plusieurs certificats portant le nom commun BangCloud et liés à un petit hébergeur de serveurs en Thaïlande. La plupart des adresses IP associées à ces certificats se trouvaient dans le même bloc de routage interdomaine sans classes (CIDR), en tant qu'adresse 147[.]50[.]253[.]109, et ont été signalées pour leur lien avec des fichiers malveillants, selon VirusTotal, puisqu'elles partageaient des codes de hachage et des noms de fichier.

La campagne de minage de cryptomonnaie RedTail a exploité la vulnérabilité CVE-2024-4577 dans les jours qui ont suivi sa divulgation. L'attaquant a utilisé une requête qui profitait de la faille pour exécuter une requête WGET et lancer une séquence de commandes en langage naturel. Cette dernière a envoyé une requête réseau à une adresse IP en Russie pour obtenir une version x86 du logiciel malveillant de minage de cryptomonnaie RedTail. Le but est de téléverser le fichier de minage en utilisant une commande WGET ou CURL, ou une connexion TCP en tant que repli, pour trouver les répertoires détenus par la victime qui avait des droits de lecture, d'écriture et d'exécution. La requête excluait les répertoires assortis de l'option Noexec, ainsi que ceux comportant la mention « /tmp » et « /proc ». Elle a réussi à récupérer l'architecture du système, à tester des droits d'écriture, puis à télécharger et à exécuter ses données utiles en fonction de l'architecture du système de la victime, pour enfin renommer le fichier Redtail.

Par ailleurs, la séquence de commandes en langage naturel a récupéré un fichier ELF nommé « pty3 » d'une autre adresse IP, qui est considéré comme un échantillon du logiciel malveillant Muhstik. Ce dernier est reconnu pour cibler les appareils d'Internet des objets et les serveurs Linux pour y faire du minage de cryptomonnaie et lancer des attaques DDoS.

Vulnérabilité critique – Preuve d'exploitation par exécution de code à distance – GeoTools de GeoServer – CVE-2024-36401

CVE-2024-36401 : GeoServer est un serveur à code source libre qui permet aux utilisateurs de partager et de modifier des données géospatiales. Avant les versions 2.23.6, 2.24.4 et 2.25.2, plusieurs réglages des requêtes OGC permettaient à des utilisateurs non authentifiés d'exécuter du code à distance en envoyant une commande spécialement conçue à une installation GeoServer par défaut puisque les noms de propriété en tant qu'expressions XPath n'étaient pas évalués de façon sécuritaire. L'interface API de la bibliothèque GeoTools que GeoServer interpelle évalue les noms de propriété ou d'attribut pour y repérer des types de fonction d'une façon qui permet de transmettre de manière non sécuritaire à la librairie Apache Commons JXPath, laquelle peut exécuter du code arbitraire lors de l'évaluation des expressions XPath. Cette évaluation ne devrait servir que pour des types de fonctions complexes (comme les jeux de données du schéma d'application), mais elle est inadéquatement appliquée aussi à des types de fonctions simples, ce qui fait que cette vulnérabilité s'applique à toutes les instances GeoServer.

Bien que la vulnérabilité n'était pas activement exploitée à l'époque, les chercheurs ont rapidement diffusé des preuves d'exploitation qui démontraient comment il était possible d'exécuter du code à distance sur des serveurs exposés et d'ouvrir des shells inversés, d'établir des connexions sortantes ou de créer un fichier dans le répertoire /tmp. Les mainteneurs du projet ont réparé la faille dans les versions 2.23.6, 2.24.4 et 2.25.2 de GeoServer et recommandé à tous les utilisateurs de passer à ces versions. Les développeurs ont aussi proposé des solutions de rechange tout en précisant qu'elles pouvaient nuire à certaines fonctionnalités de GeoServer. Selon un moteur de recherche OSINT, environ 16 462 serveurs GeoServer sont exposés en ligne, essentiellement aux États-Unis, en Chine, en Roumanie, en Allemagne et en France.

Code	Gravité	Note CVSS
CVE-2024-36401	Critique	9.8

Produits et versions touchés

Paquet	Versions touchées	Versions corrigées
org.geoserver.web:gs-web-app (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>= 2.25.0, < 2.25.2	2.25.2
	< 2.23.6	2.23.6
org.geoserver:gs-wfs (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>= 2.25.0, < 2.25.2	2.25.2
	< 2.23.6	2.23.6
org.geoserver:gs-wms (Maven)	>= 2.24.0, < 2.24.4	2.24.4
	>=2.25.0, <2.25.2	2.25.2
	< 2.23.6	2.23.6

À quoi s'attendre en 2025

Il devrait y avoir un profond virage en 2025. Étant donné les différents changements de gouvernement dans le monde entier, nous devrions aussi observer un mouvement au chapitre des priorités, des investissements et des stratégies, ce qui aura d'importantes répercussions sur la cybersécurité. Ces changements se feront particulièrement sentir au Canada où des élections devraient bientôt être déclenchées, faisant du pays une cible alléchante pour les ennemis géopolitiques et les cybercriminels, et où l'imposition de droits de douane aura potentiellement une incidence sur les budgets de sécurité et la capacité des entreprises canadiennes à attirer les meilleurs talents.

Voici certains des principaux défis en matière de sécurité qu'il pourrait falloir relever :

Délai d'attaque

L'exploitation constante des modèles de langage de grande taille et des autres systèmes d'IA par les acteurs de menaces pourrait grandement réduire le temps qu'il faut à ces derniers pour générer et déployer des logiciels malveillants personnalisés qui ciblent des vulnérabilités précises. Le raccourcissement du délai d'attaque fera grimper le stress des équipes de sécurité qui devront accélérer leur conception de règles de détection et de trousses de chasse aux menaces pour contrer les attaques.

La baisse du délai d'attaque va de pair avec un fléchissement de la barrière à l'entrée pour les logiciels malveillants personnalisés. En utilisant ces outils pour générer des codes d'exploitation ou des logiciels malveillants propres à des vulnérabilités spécifiques, les acteurs de menaces moins aguerris qui faisaient probablement préalablement affaire avec des fournisseurs de logiciels malveillants en tant que service (MaaS) pourraient maintenant avoir la capacité de réaliser des attaques plus importantes. Même si leur taux de succès ne sera pas nécessairement plus élevé, l'affaiblissement de la barrière à l'entrée pourrait contribuer à élever substantiellement la fréquence des incidents auxquels les organisations doivent réagir.

Avec le temps, cette hausse de la fréquence, combinée à la rapidité accrue et à la précision poussée des attaques, augmente le risque auquel sont exposées les victimes potentielles des cyberattaques.

Ingénierie sociale

Les attaquants qui mettent l'IA à profit n'utiliseront pas cette dernière uniquement pour exploiter les vulnérabilités et abaisser la barrière technique à l'entrée. Ils s'en serviront aussi pour complexifier leurs attaques par hameçonnage ou par hameçonnage vocal, et leurs autres attaques d'ingénierie sociale. Au fur et à mesure que les modèles de langage de grande taille qui génèrent du contenu se sophistiqueront, nous devrions voir une hausse de la fraude misant sur cette technologie.

Les réseaux sociaux regorgent d'exemples rudimentaires de ce type d'exploitation où des publicités malveillantes montrent des sources de nouvelles de confiance annoncer que telle célébrité, telle entreprise ou tel gouvernement a lancé un nouveau produit, un nouveau programme ou un nouvel avantage pour un groupe cible. En se spécialisant, ces attaques pourraient s'adresser à de nouvelles cibles pour recueillir les données de connexion ou les renseignements sensibles de personnes

Espionnage et pénétration

Comme nous l'avons vu en 2024, les acteurs étatiques ont concerté leurs efforts pour obtenir l'accès aux systèmes essentiels, et ce, dans tous les secteurs d'activité. Cette tendance devrait se poursuivre en 2025, et nous nous attendons à ce que les malfaiteurs jettent davantage leur dévolu sur les infrastructures essentielles, notamment de défense. Les attaques pourraient avoir pour but d'obtenir de l'information, de voler des technologies, de se positionner pour perpétrer de futures attaques ou de compromettre les personnes dans leur mire. À la lumière des incidents de 2024, les entreprises vulnérables devraient songer à renforcer leur cyberdéfense, c'est-à-dire leur matériel et leurs solutions de sécurité, ainsi que leur plan de communication.

Leurs démarches devraient aussi intégrer les partenaires de leurs chaînes d'approvisionnement – pas seulement ceux qui appuient directement leurs activités de production, mais aussi les fournisseurs d'équipement qui sont souvent tenus pour acquis. Cela pourrait être utile pour planifier les interruptions de la chaîne d'approvisionnement tout comme repérer les points de compromission potentiels du matériel critique.

Cyberactivité criminelle

Outre la hausse des menaces liées à l'IA, nous devrions observer une augmentation des incidents de rançongiciels en 2025. Ce type de menace ne risque pas de s'estomper dans un proche avenir, et les sociétés devraient tenir compte des problèmes énumérés par notre équipe Réponse aux incidents quand elles évaluent leur position défensive et établissent leurs plans d'intervention en cas d'incident.

Opérations d'information

En 2024, la majeure partie des activités d'opération d'information (efforts délibérés pour contrôler les messages en ligne, diffuser de la fausse information et modeler la perception publique à l'égard d'une politique bien précise) portait sur les élections présidentielles américaines. L'objet de ces activités pourrait bien changer et devenir le Canada. En raison des élections fédérales et provinciales imminentes, des tensions internationales entre le Canada et ses partenaires commerciaux, et de l'attisement des frictions géopolitiques, les Canadiens seront fort probablement la cible d'importantes opérations d'information.

Bien que celles-ci servent souvent à obtenir un résultat politique précis, elles peuvent aussi être mises à profit pour recruter des initiés dans les entreprises ciblées. Par conséquent, les organisations devraient examiner leurs programmes de prévention des risques liés aux initiés ainsi que la probabilité d'être visées par de tels efforts.

Droits douaniers

Bien qu'ils ne soient pas directement une cybermenace, les droits douaniers peuvent constituer une contrainte financière pour les sociétés et exercer une pression sur les budgets de sécurité. Les entreprises canadiennes qui devront composer avec cette pression pourraient devenir des cibles plus intéressantes, car les compressions du budget de sécurité rehausseront leur vulnérabilité.

04 Comment KPMG peut aider

Le groupe Cybersécurité de KPMG au Canada offre des services d'intervention immédiate pour vous aider à détecter les intrusions dans vos systèmes informatiques, à adopter les mesures nécessaires et à reprendre vos activités. Forts de leur expérience en enquêtes, en juricomptabilité informatique et en reprise d'activités, nos professionnels de la cybersécurité vous assistent dans l'obtention des éléments de preuve. Ils peuvent aussi vous aider à comprendre ce qui s'est produit, à atténuer les risques et à contribuer aux enquêtes internes, judiciaires et policières.

Chez KPMG, nous aidons des entreprises à gérer leurs données les plus précieuses, à se prémunir contre toutes sortes de menaces et à faire face à toute éventualité. Nous voyons la cybersécurité non pas comme un projet ponctuel, mais plutôt comme une stratégie d'ensemble évolutive, adaptée aux objectifs d'exploitation et axée sur la valeur à long terme de l'entreprise. Nous vous aidons ainsi à protéger votre avenir et à élargir les possibilités.

Les solutions de cybersécurité de KPMG comprennent ce qui suit :

Préparation et plan d'intervention en cas d'incident – Nous vous aidons à améliorer votre état de préparation et vos capacités d'intervention afin que votre organisation soit en mesure de répondre rapidement et efficacement si un incident de sécurité survient.

Enquêtes informatiques et mesures correctives – Nous vous aidons à réagir de façon efficace aux cyberincidents. Lorsqu'une fuite se produit, nous procédons à une enquête approfondie et à une analyse juricomptable pour déterminer ce qui s'est passé, comment cela s'est produit et, le cas échéant, qui y a pris part.

Renseignements sur les menaces – Nous vous aidons à hiérarchiser les actifs, à cerner les menaces et les vulnérabilités potentielles et à évaluer les répercussions sur l'organisation. Cela permet de réduire les coûts et la complexité des efforts visant la protection proactive des actifs informatiques essentiels et la réaction aux attaques .

Dépistage des données et mesures correctives – Nous vous aidons à exploiter efficacement la technologie pour gérer de façon sécuritaire les données confidentielles, repérer les données redondantes, obsolètes et inutiles (« ROT » en anglais) aux fins de correction, et les rendre disponibles dans le cadre du processus décisionnel de l'entreprise.

Service de détection et réponse gérées (DRG) – Ce service réduit le délai de détection et de réponse en combinant des technologies avancées de lutte contre les menaces à la surveillance et à l'analyse de l'environnement de sécurité d'une organisation, en tout temps. Cela permet aux analystes de sécurité d'identifier et d'examiner les menaces possibles en temps réel. Notre service est conçu pour aider les organisations à identifier les cybermenaces et à y répondre avant qu'elles causent des dommages ou des pertes de données considérables en sonnant l'alarme pour les renseignements précis et pertinents les plus exploitables. Grâce à l'automatisation et à la réponse guidée par un analyste, le service de DRG favorise la correction et la reprise efficaces des actifs.

05 Contributeurs

Securité OT

Karan Ghoshal

Arvind Prabaharan

Mike Rosenlund

Aindrea Skelly

Intervention en cas d'incident

Mansoor Haqanee

Kyle Johnston

Anne Labbé

Jordan Michallet

Xavier Normand

Robin Penrat

Ganesh Ramakrishnan

Chris Walker

Nous joindre

Intervention en cas d'incident

Alexander Rau
Associé
alexanderrau@kpmg.ca

Guillaume Clement
Associé
guillaumeclement@kpmg.ca

Ganesh Ramakrishnan
Directeur principal
gramakrishnan@kpmg.ca

Chris Walker
Directeur principal
chriswalker2@kpmg.ca

Anne Labbé
Directrice principale
alabbe@kpmg.ca

Xavier Normand
Directeur principal
xnormand@kpmg.ca

Renseignements sur les cybermenaces et vulnérabilités exploitées

Robert Moerman
Associé
rmoerman@kpmg.ca

Mike Rosenlund
Directeur principal
mrosenlund@kpmg.ca