Cyberincidents et Renseignements : 2023

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

Mars 2024

kpmg.ca/fr

Table des matières

01

Introduction

En règle générale, le secteur de la cybersécurité est en constante évolution. La technologie évolue rapidement et les auteurs de la menace sont tout aussi rapides et créatifs, ce qui entraîne que le secteur est en constante mutation; des réflexions approfondies et des décisions éclairées sont donc nécessaires pour assurer la sécurité des organisations. L'année 2023 n'a pas fait exception à cette règle.

Le rapport de KPMG Canada 2023 sur la situation de la cybersécurité met en lumière les avancées significatives dans le domaine des logiciels malveillants, les actions des cybercriminels et les mesures de cybersécurité requises pour les contrer. Nos équipes de Réponse aux Incidents, Renseignements sur les cybermenaces et Gestion des vulnérabilités se sont réunies pour nous donner un aperçu des cas uniques qui ont été résolus au cours de l'année, ainsi que des réflexions éclairées sur les projections pour 2024 et les années suivantes.

Il est à noter que les opinions exprimées dans le présent rapport reflètent de véritables expériences et incidents survenus en 2023. Bien que les événements aient été décrits avec précision, les renseignements sur les victimes ont été modifiés.

02

Intervention en cas d'incident

Les équipes de Réponse aux Incidents et Renseignements sur les cybermenaces ont uni leurs forces pour une deuxième année afin de rédiger le rapport 2023 sur l'état du contexte de la cybersécurité et présentant leurs projections pour l'exercice 2024. Le présent document comprend des rapports et des réflexions provenant des premiers intervenants en cas d'incident, des analystes en cybermenaces et des leaders d'opinion dans le domaine.

Il est à noter que les opinions exprimées dans le présent rapport reflètent de véritables expériences et incidents survenus en 2023. Bien que les événements aient été décrits avec précision, les renseignements sur les victimes ont été modifiés.

Sommaire des interventions

2.1 Aperçu des principales préoccupations de cybersécurité en 2023

Au cours de l'exercice, la cybersécurité est restée une préoccupation majeure pour les organisations canadiennes. La manière dont les dirigeants gèrent les incidents de cybersécurité est de plus en plus scrutée par les organismes de réglementation, le public, ainsi que par leurs propres conseils d'administration et actionnaires

Le rapport de KPMG met en évidence certaines des principales menaces, données et tendances informatiques majeures observées au Canada en 2023. Les rançongiciels continuent de dominer de nombreux secteurs, notamment ceux qui offrent des services essentiels à la population, comme les écoles, les organismes gouvernementaux et les fournisseurs de services publics. Nous remarquons que les groupes d'acteur de menace continuent de privilégier le vol de données plutôt que la forme traditionnelle unique d'extorsion. En 2023, nous avons observé une augmentation des attaques sur les organisations **des secteurs des services financiers et manufacturiers.**

2.2 Observations importantes de l'exercice 2023

Hausse des cas de compromission de tiers : En 2023, la compromission de tiers est devenue une préoccupation de cybersécurité majeure. Elle diffère des attaques directes sur l'environnement informatique d'une organisation puisqu'il s'agit d'une compromission dans les systèmes informatiques ou les produits appartenant aux partenaires externes de nos clients. Ce changement met en évidence l'engagement croissant des fournisseurs et des sous-traitants tiers dans le contexte des fuites de données, ce qui accroît considérablement la complexité des défis liés à la gestion des incidents auxquels les organisations sont confrontées.

Augmentation des tentatives d'exploitation à grand volume : En 2023, KPMG a observé une hausse des tactiques automatisées de type « tirs à l'aveuglette » que les auteurs de la menace utilisent pour exploiter les serveurs vulnérables connectés à Internet. Ces attaquants se servent de cette tactique pour déployer automatiquement des activités malveillantes à grande échelle, souvent sans avoir de cible précise. Au lieu de choisir soigneusement et de viser une organisation spécifique, ils déploient leurs actions malveillantes sur un large éventail de victimes potentielles. L'augmentation de ces exploitations de vulnérabilités, qui peuvent être facilement automatisées, souligne la nécessité pour les organisations de revoir leurs

calendriers de mise à jour et leur posture de sécurité concernant les actifs connectés à Internet.

Prévention de la perte de données et hausse des incidents de sécurité internes : En raison de la réduction des effectifs, de fortes inquiétudes sont apparues dans les organisations en ce qui concerne le vol possible de propriété intellectuelle lors du départ des membres du personnel. Ces inquiétudes ont été exacerbées par l'environnement économique actuel où la réduction et la rotation du personnel sont fréquentes. Pour faire face à ces défis, les organisations ont intensifié leurs efforts en matière de stratégies de prévention des pertes de données, en adoptant une approche multidimensionnelle pour protéger contre le vol d'actifs intellectuels précieux. Plus spécifiquement, elles renforcent la surveillance des comportements des employés, mettent en place des mesures d'accès strictement contrôlées et utilisent des technologies de prévention des pertes de données pour se prémunir contre les fuites.

Changements aux tactiques de la Fraude au Président (Business Email Compromise) : En 2023, les Fraudes au Président (BEC) ont augmenté même si les organisations ont renforcé les mesures de sécurité de leurs courriels, notamment en ajoutant l'authentification multifacteur. Nous avons également constaté une tendance inquiétante dans la capacité des acteurs de la menace à s'adapter aux défenses en place. Ceux-ci créent des domaines frauduleux qui imitent de près l'identité visuelle des entreprises et se servent de renseignements de sources ouvertes pour mieux comprendre les organisations. Ils raffinent ainsi leurs tentatives de fraude pour augmenter leur taux de réussite. De plus, nous avons observé des cas où les attaquants qui ont réussi leurs attaques BEC ont poussé l'audace jusqu'à lancer des attaques frauduleuses à répétition contre une même organisation.

En réponse à ces menaces changeantes, nous encourageons les organisations à aller au-delà de l'authentification multifacteur. Elles devraient plutôt adopter une approche globale comprenant l'amélioration de la formation des membres du personnel sur la sécurité afin qu'ils reconnaissent bien les tentatives d'hameçonnage et les signalent. En outre, les organisations devraient penser à mettre en œuvre des mesures comptables supplémentaires comme l'exigence d'une approbation écrite et verbale lors d'une demande de modification des renseignements bancaires.

2.3 Principales leçons et recommandations

Les principales leçons que certains de nos clients ont tirées d'une brèche de sécurité informatique se trouvent ci-dessous.

Importance de la journalisation : Nous encourageons les organisations à tenir des journaux, notamment de terminaux (p. ex., événements Windows), de réseaux (p. ex., pare-feu) et d'applications (p. ex., liés à des applications propres à l'entreprise), pendant au moins un an. En 2023, environ la moitié des clients de KPMG en réponse aux incidents ont constaté un manque de journaux à analyser lors de l'enquête associée à un incident de cybersécurité. De plus, KPMG recommande que les organisations transfèrent leurs journaux et les événements dans un répertoire centralisé, comme par exemple une solution de gestion de l'information et des événements de sécurité (SIEM).

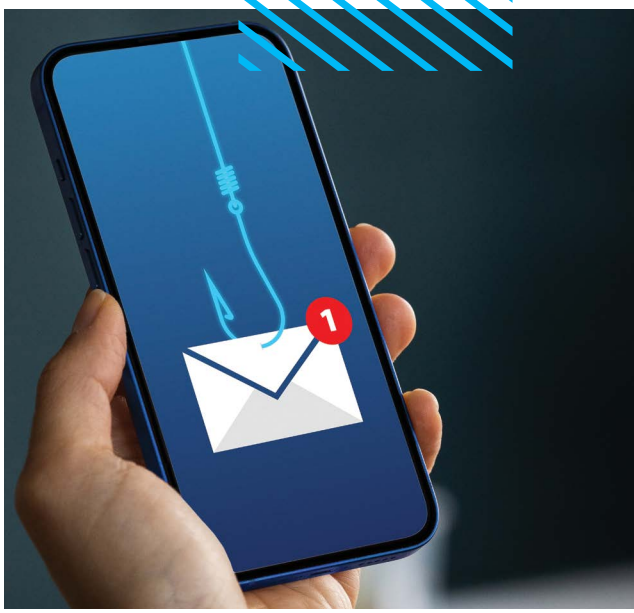
Examen et maintenance d'Active Directory (AD) : Étant l'épine dorsale de l'authentification et de l'autorisation, la plateforme AD demeure une composante essentielle de l'infrastructure des TI de nombreuses organisations. C'est également une cible courante des attaquants. Les organisations doivent être particulièrement attentives aux comptes de service, qui profitent souvent de nombreux privilèges afin de remplir des rôles précis dans un environnement informatique. Malheureusement, ces comptes peuvent devenir des cibles payantes pour les attaquants en raison de leur accès vaste et du manque typique de surveillance régulière lorsqu'ils ne sont pas gérés adéquatement. Les organisations doivent régulièrement passer en revue et vérifier ces comptes pour s'assurer de retirer les privilèges non essentiels, de modifier les identifiants à intervalles réguliers et de désactiver les comptes inactifs.

Les organisations doivent passer en revue les stratégies de groupe (GPO) en plus des comptes de service. Mal

configurées, ces stratégies peuvent accidentellement introduire des vulnérabilités, accorder des permissions inappropriées et même être exploitées par attaquants pour propager des maliciels ou imposer des configurations malveillantes dans l'ensemble du domaine. Des audits et des examens réguliers de ces stratégies permettent de détecter et de corriger ces mauvaises configurations pour veiller à ce que les politiques soient sécuritaires et répondent aux besoins opérationnels de l'organisation.

Indexation et configuration optimales des SIEM : Les solutions de gestion de l'information et des événements de sécurité (SIEM) sont indispensables pour renforcer et examiner les incidents de sécurité, ainsi que pour intervenir lors de tels incidents à travers toute l'organisation. Toutefois, une indexation performante peut améliorer l'efficacité d'une solution SIEM. Les organisations doivent s'assurer que tous les journaux sont correctement configurés et indexés dans leur solution SIEM avant qu'un incident de sécurité ne se produise, au lieu d'attendre pour résoudre les problèmes d'indexation et de performance après un incident, lorsque les recherches sont cruciales. Pour y arriver, elles peuvent notamment standardiser les données des journaux (ex., en convertissant les données du pare-feu dans un format que la solution de SIEM peut analyser facilement), supprimer les données redondantes ou inutiles et se concentrer sur l'indexation par type d'événement de priorité élevée (avec les codes des journaux d'événements de Windows, par exemple). Il est essentiel de revoir régulièrement les stratégies d'indexation et les entrées de journal pour optimiser continuellement la solution SIEM, car les données et l'infrastructure de l'organisation sont en constante évolution.

Maintien des connaissances sur les vulnérabilités : Les organisations doivent maintenir une liste complète des serveurs connectés à Internet, y compris les applications hébergées, tout en surveillant de près les vulnérabilités publiées. Il est également essentiel que les organisations établissent une politique qui tient compte de la sévérité d'une vulnérabilité et des conséquences sur l'entreprise si elle devait être exploitée. Cette politique doit aussi comprendre des échéanciers de mesures correctives. Il est essentiel de surveiller constamment les avancées liées à la gestion des mises à jour de sécurité. Lorsqu'il n'est pas possible de déployer rapidement ces mises à jour, les organisations doivent renforcer leurs systèmes de surveillance afin de maintenir une position de vigilance en matière de cybersécurité.



Conservation de trois copies de sauvegarde (en ligne, hors ligne et hors ligne hors site) : Les organisations doivent conserver trois types de sauvegardes pour prévenir les pertes de données associées à un incident de cybersécurité. Les sauvegardes en ligne permettent de récupérer rapidement et efficacement les données en cas de perte accidentelle ou de compromission. Comme elles ne sont pas connectées à Internet ou au réseau, les sauvegardes hors ligne offrent une couche de protection supplémentaire en réduisant le risque de cyberattaques qui compromettraient les données de sauvegarde. De plus, les sauvegardes hors ligne et hors site constituent une stratégie complète de protection contre les cybermenaces et d'atténuation des conséquences de catastrophes physiques, car elles assurent la résilience des données et la continuité des affaires. Cette approche à trois niveaux améliore considérablement la fiabilité et l'efficacité globales de la stratégie de sauvegarde en matière de cybersécurité d'une organisation.

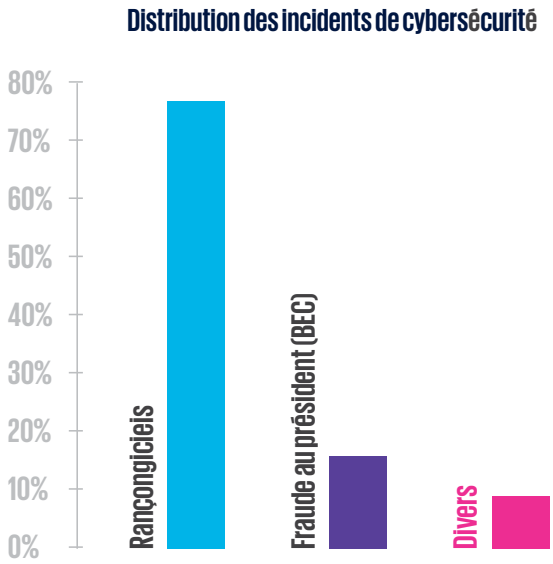
De plus, les organisations doivent vérifier régulièrement l'intégrité et la fiabilité des données de leurs copies de sauvegarde. Sans cette vérification, les organisations pourraient ne pas savoir que leurs sauvegardes sont corrompues ou irrécupérables. En vérifiant régulièrement leurs sauvegardes, elles peuvent cerner hâtivement les problèmes possibles et veiller à ce que les données et systèmes essentiels puissent bien être récupérés en cas de grave incident de sécurité.

Exercices réguliers de simulation de cyberattaque ou de brèches (Tabletop) : Recommandés par l'Institut National des Normes et de la Technologie (NIST), les exercices de tabletop simulent des scénarios possibles dans le but d'évaluer les stratégies d'intervention d'une organisation. Ces exercices offrent un environnement contrôlé pour déterminer les lacunes d'une organisation et peaufiner ses plans d'intervention en cas d'incident. La pratique régulière des processus d'intervention assure une réaction rapide, coordonnée et efficace en cas d'incident réel.

Incidents

3.1 Menaces importantes et statistiques

Les rançongiciels et les BEC continuent d'être les deux principales menaces touchant les organisations canadiennes et les clients de réponse aux incidents de KPMG. En 2023, KPMG est intervenu dans 77 % des incidents liés aux rançongiciels et 15 % des incidents liés aux compromissions d'e-mails d'entreprise (BEC). Les autres incidents étaient associés à divers événements de sécurité. Comparativement à l'exercice précédent, les incidents associés aux rançongiciels ont augmenté de 20 %, tandis que les BEC ont diminué de 11 %.



Étude de cas no 1
À l'exercice 2023, KPMG est intervenu dans un important incident touchant un client du secteur de l'assurance. L'attaque s'est traduite par le vol d'environ 15 000 fichiers. Les enquêtes ont révélé que les acteurs de la menace ont exploité une vulnérabilité dans ManageEngine (une suite logicielle de gestion des TI d'entreprise), CVE-2022-47966, ce qui leur a permis d'exécuter du code malveillant dans l'environnement de TI du client. KPMG a déterminé que les auteurs de la menace ont profité de la vulnérabilité que quelques jours seulement après que le CVE ait été rendu public. Même si le client a corrigé rapidement la vulnérabilité, ses actions ont été dépassées par les attaquants, qui s'étaient déjà introduis dans leur environnement TI. **Cet incident met en évidence la fenêtre restreinte dont les organisations disposent pour déployer des correctifs ou des mises-à-jour, et souligne la lutte de plus en plus intense à laquelle les organisations se livrent contre les cybercriminels.**

Étude de cas no 2
En 2023, KPMG a offert son soutien dans un important incident impliquant une entreprise de services financiers qui desservait des banques canadiennes. L'entreprise a été victime d'un rançongiciel, l'attaquant a volé approximativement 220 Go de données de son environnement TI. Heureusement, l'enquête de KPMG a démontré qu'aucune donnée volée ne contenait des renseignements personnels associés aux clients des banques. Cet incident met l'accent sur les vulnérabilités qui peuvent exister dans les chaînes d'approvisionnement. L'enquête de KPMG a révélé que les attaquants ont d'abord accédé aux données à l'aide d'un compte client sur le réseau virtuel privé (VPN) qui n'avait la fonctionnalité de MFA. **Cette fuite met en évidence l'importance des contrôles de sécurité continus pour les comptes dotés de privilèges supplémentaires, des audits réguliers pour désactiver les comptes inactifs, ainsi que le rôle crucial de l'authentification multifacteur pour renforcer les mesures de sécurité.**

3.2 Analyse propre au secteur

Tout comme en 2022, KPMG a remarqué que les attaques par rançongiciel ont visé majoritairement des organisations canadiennes œuvrant dans différents secteurs d'activités plutôt que dans un secteur en particulier. Il y a toutefois eu une augmentation dans les secteurs manufacturiers et des services financiers.

3.3 Tendances

Dans l'ensemble, KPMG a constaté une hausse des clients acquiesçants aux demandes de rançons, non pas par souci pour les données chiffrées, car de nombreux clients avaient des systèmes robustes de sauvegarde, mais en raison de la publication possible des données volées contenant des renseignements critiques ou personnels. La publication de tels renseignements présente d'importants risques aux organisations, notamment de possibles répercussions juridiques et une atteinte à la réputation. Le paiement de la rançon devient souvent une stratégie pour atténuer ces conséquences graves. Ce changement à la dynamique des rançongiciels souligne l'importance croissante de la gestion des données et de la prévention de leur vol. Au fur et à mesure de l'évolution de l'environnement des cybermenaces, la protection des données contre l'extraction non autorisée deviendra sans aucun doute une stratégie de cyberdéfense indispensable.

Conséquences

L'Intelligence artificielle (IA) : un bien et un mal

De par l'automatisation qu'elle offre, ainsi que ses solutions avancées, telles que l'IA générative (Gen AI), cette dernière continue de transformer différents secteurs. Son influence sur le domaine de la cybersécurité est toutefois double. D'un côté, les outils propulsés par la Gen AI habilitent les organisations à détecter les menaces et à y réagir à une vitesse et avec une précision sans précédent. Inversement, les acteurs de la menace tirent parti de ces avancées pour concevoir des attaques raffinées, automatiser leur fonctionnement et surpasser les mécanismes traditionnels de défense. Avec l'accessibilité croissante des technologies d'IA, le pouvoir en cybersécurité reviendra au groupe qui se servira le mieux de ce type d'intelligence : l'attaquant ou les victimes potentielles.

Le défi que pose l'utilisation illicite des outils de pénétration

Les récents efforts collaboratifs des forces de l'ordre, des géants de la technologie et des fournisseurs d'outils d'intrusion commerciaux (conçus pour simuler les tactiques et techniques sophistiquées des attaquants, la capacité à acheminer les charges utiles et les fonctionnalités de commande et de contrôle (C2)) ont commencé à sévir contre l'utilisation illégale de ces outils, ce qui redéfinit le paysage des menaces. Les mécanismes améliorés de détection pour l'utilisation commerciale des outils de test d'intrusion font pression sur les acteurs de menace. Cette pression les pousse vers la recherche d'outils et de méthodes de remplacement. Alors que la prédominance des outils commerciaux est mis au défi, les organisations se doivent de diversifier leurs stratégies de détection et d'intervention, anticipant ainsi une large gamme d'outils d'attaque.

Innovation stratégique

L'équipe Intervention en cas d'incident de KPMG a adopté plusieurs approches innovantes pour contribuer à l'intervention et à la récupération immédiates advenant un tel cas, en plus de fournir aux victimes un environnement plus stable et sécurisé après l'événement. Voici quelques-unes des principales innovations ayant eu des retombées positives pour les victimes :

01

Collecte Automatisée des évidence forensique : L'équipe de réponse aux incidents de KPMG a développé un mécanisme automatisé pour une collecte rapide d'évidences et de triage forensique, réduisant considérablement la phase de collecte d'images, traditionnellement longue.

02

Techniques avancées de récupération des données – Dans un cas précis impliquant un rançongiciel, l'équipe Intervention en cas d'incident de KPMG a récupéré de façon novatrice des dossiers d'un environnement Slack et a entamé des procédures de récupération. De plus, elle a conçu une méthode unique qui a permis de récupérer des dossiers partiellement chiffrés. Cette découverte offre une solution de rechange au paiement de rançons pour la récupération des données, particulièrement pour les organisations qui n'ont pas perpétué l'habitude des sauvegardes complètes.

Envisager l'avenir

Des postures de sécurité renforcées : Un grand nombre d'organisations ont réalisé des avancées significatives dans le renforcement de leur cyberdéfense. On observe une augmentation notable de l'adoption de mesures de sécurité solides ; les organisations investissent massivement dans des outils sophistiqués de détection et de réponse, affinent leurs stratégies de sauvegarde et suivent des formations rigoureuses en matière de cybersécurité. Ces actions proactives ont considérablement diminué les vulnérabilités de nombreuses entités.

Le couteau à double tranchant de l'interconnectivité : La toile complexe du monde des affaires d'aujourd'hui compte son lot de défis. Bien qu'elle favorise la collaboration et la croissance, l'interconnectivité des entreprises présente aussi de possibles défauts dans l'armure. Même si une organisation a consolidé ses défenses, son exposition à des tiers, que ce soit via des produits, des partenariats ou des chaînes d'approvisionnement, peut se transformer en son point faible. Il ne serait pas étonnant de constater une augmentation des malversations provenant de canaux tiers. Par conséquent, au lieu de se focaliser exclusivement sur leur propre sécurité, les organisations devraient également porter une attention particulière à la sécurisation de l'ensemble de leur écosystème.

La puissance subtile des attaques non chiffrées : Certaines cybermenaces ont évolué d'une façon qui remet en question les croyances conventionnelles. Le groupe d'attaquants Cl0p par exemple, a notamment démontré que le chiffrage n'est pas le seul moyen de causer des ravages dans une organisation. Les attaques ciblent souvent des produits ou des services utilisés par de nombreuses organisations plutôt que des entités individuelles, illustrant ainsi la puissance de cette stratégie. En se focalisant sur une unique vulnérabilité présente dans un produit ou un service largement répandu, les auteurs de menaces peuvent décupler l'impact de leurs actions.

La menace des *Zero-Days* : Les vulnérabilités de type *Zero-Day* continuent d'être une menace persistante et imminente. Les organisations doivent être particulièrement prudentes avec les produits et services qui, s'ils sont compromis, pourraient servir de portail vers de nombreux clients. L'exploitation réussie de ces failles par le rançongiciel Cl0p met en évidence le caractère urgent de ce problème. Le secteur pourrait voir une augmentation dans l'exploitation des *Zero-Days* ciblant des services populaires et largement utilisés, étant donné que ceux-ci présentent un potentiel de dommage accru.

L'adaptation à la nouvelle normalité : À la lumière de ces tendances émergentes, les organisations doivent réévaluer leurs stratégies de défense. Bien que le renforcement des défenses individuelles soit essentiel, il est de plus en plus important d'examiner et de sécuriser les interactions avec les tiers. De même, alors que les attaques basées sur le chiffrement sont monnaie courante, l'industrie doit également se préparer à des menaces plus subtiles, mais tout aussi dévastatrices, qui ne sont pas basées sur le chiffrement.

Une année électorale aux États-Unis : Comme 2024 est une année électorale aux États-Unis, on s'attend à une hausse de l'intensité des menaces. Les acteurs de la menace s'engageront pleinement à tenter d'influencer et de façonner le paysage politique du pays. De plus, avec les activités géopolitiques en cours en Europe de l'Est et au Moyen-Orient, il est probable que des acteurs de menaces de divers horizons, y compris des États-nations, cibleront différentes organisations américaines et canadiennes qui font des affaires avec les États-Unis.

Des cyberattaques propulsées par l'IA : En se servant de la Gen AI, les acteurs de menace pourraient développer des méthodes d'attaque plus efficaces et plus raffinées. L'IA pourrait servir à automatiser la sélection des cibles, à adapter les messages d'hameçonnage et même à découvrir et à exploiter de nouvelles vulnérabilités.

Le chemin à venir promet d'être difficile, mais avec adaptabilité et prévoyance, les organisations peuvent naviguer dans ce labyrinthe cybernétique complexe.

03

Renseignements sur les cybermenaces

Renseignements sur les cybermenaces

Constatations de l'exercice 2023

Le paysage de la cybermenace s'est considérablement élargi en 2023. Bien que dans les années précédentes, de nombreuses organisations aient trouvé leurs adversaires dans des organisations criminelles aux objectifs financiers, 2023 a vu de plus en plus d'activités cybernétiques liées à des objectifs politiques.

Dans cette hausse des activités, une multiplication des acteurs de menace plus discrets a été observée. Ceux-ci ne sont pas directement ou clairement connectés aux groupes de rançongiciel ou aux groupes infâmes tels que Lockbit 3.0, Cl0p ou BlackCat.

En parallèle à l'augmentation de l'activité des acteurs de menaces discrets, il y avait des appels à l'action de la part des acteurs de menaces aux initiés d'entreprise. Alors que les marchés d'accès initiaux continuent de croître, l'accès acheté n'est jamais aussi fiable ou pratique qu'un initié interne, aidant activement un acteur de menace.

Lorsque les initiés et les marchés d'accès initiaux échouent, les méthodes éprouvées des logiciels malveillants entrent en jeu. En 2023, nous avons observé un changement dans les attaques pour cibler les systèmes d'exploitation qui avaient précédemment été considérés comme des cibles secondaires, comme Linux. Bien qu'il ne devrait pas être surprenant que les acteurs de menaces ciblent de tels systèmes, l'augmentation du volume est notable et devrait être prise en compte lors de la conception de votre environnement de sécurité.

L'une des grandes évolutions de 2023 a été l'émergence des Grands Modèles d'Apprentissage (GML). Bien que ces GML présentent une opportunité énorme pour améliorer la sécurité et l'efficacité, ces améliorations sont également exploitées par les acteurs de menaces. L'essor des maliciels et des acteurs de menaces améliorés par les GML ou l'IA est très réel et sera une considération majeure en 2024.

Cela nous ramène à l'éléphant dans la pièce de 2023, soit les activités des États-nations et le cyberactivisme. Bien que cette activité en ligne ne soit pas nouvelle pour les gouvernements comme pour les activistes, nous avons constaté beaucoup de mouvement dans cet environnement qu'à l'exercice précédent. Des organisations qui ne croyaient pas être des infrastructures essentielles ou des cibles d'acteurs étatiques se sont soudainement retrouvées dans leur mire, les conflits de notre monde débordant dans le cyberespace.

Ces tendances continueront probablement en 2024 et doivent être surveillées de près.

Bon nombre de groupes de menace discrets observés en 2023

L'impact collectif des acteurs de menaces discrets, bien que moins médiatisé, peut représenter une menace significative pour les entreprises. Leurs cibles couvrent différents secteurs, y compris ceux des industries critiques. Ces groupes émergents ont profité de l'incertitude entourant les récents événements mondiaux pour compromettre avec succès des organisations. L'absence de données historiques substantielles sur ces acteurs de menaces par rapport à ceux plus en vue, rend plus difficile l'anticipation de leurs tactiques, techniques et procédures (TTP), intensifiant ainsi le risque qu'ils représentent. L'attribution à des acteurs de menaces existants ou à des États-nations est particulièrement difficile en l'absence d'un grand échantillon de TTP.

- **UnSafe/Nsafe :** Le groupe de menace UnSafe/Nsafe s'est discrètement imposé en novembre 2022 en publiant sur sa chaîne Telegram des renseignements volés de différentes bases de données et de fuites de données. Cette technique initiale a possiblement servi à rassembler des partisans. Le groupe a attaqué des entités de secteurs et de tailles variés, ce qui suggère que ses motifs étaient plutôt opportunistes et non liés à un secteur en particulier. Son modus operandi est d'annoncer ses opérations sur des plateformes de sources ouvertes, puis de fermer immédiatement son site à la suite d'une brèche pour ensuite le rouvrir quelques jours plus tard pour annoncer une autre victime, ce qui souligne ses efforts pour rester dans l'ombre.

- **Phobos :** Actif depuis 2018 et nouveau nom du rançongiciel CrySiS, Le ransomware Phobos change continuellement d'extensions et de variantes pour rester discret. Phobos utilise plusieurs adresses e-mail pour les relier aux victimes pour les paiements de rançon, une autre technique pour les aider à échapper à la détection. Le groupe demande des rançons à bas prix aux petites organisations qu'il cible, possiblement parce qu'elles sont plus susceptibles de les payer. Bien qu'il ne soit pas très présent sur les médias sociaux et le Web caché, Il représente néanmoins une menace considérable pour les organisations, étant donné qu'il génère constamment de nouvelles variantes et collabore avec de nombreux partenaires, dont beaucoup utilisent sa version de rançongiciel.

KPMG a observé quelques groupes de menace qui ont affiché une empreinte négligeable avant et après leurs attaques. Ils exploitent des vulnérabilités, réussissent à déployer des rançongiciels et perturbent les activités d'exploitation tout en laissant très peu de traces sur le web caché, voire aucune. On ignore s'il s'agit de membres rebelles d'une équipe établie ou de cybercriminels de niveau inférieur cherchant à percer dans le domaine des menaces.

La croissance des activités des nouveaux acteurs de menace discrets et leur capacité à passer inaperçus signifie qu'aucun secteur n'est à l'abri des cyberattaques. Cela met en évidence le besoin des organisations, petites et grandes, d'accorder la priorité à la cybersécurité.

Menaces internes

Les menaces internes réfèrent à des situations où un individu, de manière intentionnelle ou non, fait un usage inapproprié de ses droits d'accès ou de ses privilèges au sein de l'organisation, compromettant ainsi des informations sensibles. Bien que les incidents provoqués par ces menaces internes représentent une minorité parmi l'ensemble des cyberincidents, ils peuvent néanmoins s'avérer parmi les plus onéreux en termes de rétablissement suite à une attaque.

Les fuites attribuées aux menaces internes ont augmenté de 47 % de 2018 à 2020. La montée de l'infonuagique, qui rend la détection des incidents internes plus difficile pour les employeurs, a joué un rôle dans cette hausse. En 2022, 31 % des fuites étaient associées à des menaces internes et leur coût total était de 8,76 M$. L'essor des plateformes de réseaux sociaux, l'utilisation des appareils mobiles et la confiance accordée à l'effectif ont tous joué leur rôle dans cette montée en flèche.

- **Actions intentionnelles :** Les acteurs malveillants ciblent activement les employés mécontents, les incitant à cliquer sur des liens dans des courriels ou à participer à des fuites d'informations, souvent en échange d'une récompense financière. Les employés malveillants peuvent représenter une menace interne significative pour une organisation. Ils peuvent voler des informations sensibles et les vendre sur le dark web ou les divulguer intentionnellement pour nuire à l'organisation. Ces actions peuvent causer des dommages financiers et de réputation considérables à l'organisation. Les données exfiltrées par une menace interne peuvent inclure des informations sensibles et précieuses. Les acteurs de la menace fréquentent des plateformes open-source comme le web caché, les blogs, les forums souterrains et les plateformes de médias sociaux où les employés mécontents expriment parfois leurs frustrations ou discutent de leur insatisfaction professionnelle. Armés de ces informations, les acteurs de la menace peuvent attirer et exploiter ces individus avec des motifs malveillants.

- **Actions involontaires :** Les acteurs de menace s'en prennent aux individus ayant un accès privilégié en utilisant l'ingénierie sociale ou l'exploitation de vulnérabilités pour prendre le contrôle de leurs comptes. Les adversaires utilisent des campagnes d'ingénierie sociale pour manipuler les individus à faire des actions qu'ils n'avaient pas l'intention de faire, comme les diriger vers une fausse page web ou cliquer sur un lien d'email, chargeant involontairement un logiciel malveillant et ouvrant la porte à une attaque. La négligence d'un individu peut être l'utilisation d'un mot de passe faible ou la négligence face à une demande, ce qui pourrait conduire à un événement potentiellement néfaste.

Bien que les contrôles généraux des entreprises et les contrôles d'accès basés sur les rôles puissent atténuer les dommages potentiels causés par une menace interne non intentionnel, le risque posé par un initié malveillant est plus grand. KPMG a observé que les acteurs de la menace recrutaient ou apprenaient à recruter des initiés d'entreprise jusqu'en 2024. Dans de nombreuses communautés d'acteurs de la menace, la pratique est devenue assez courante pour mériter un raccourci - le « *inny* » en anglais.

Les acteurs de la menace ont profilé des cibles potentielles pour le recrutement d'initiés (inny) et utilisent l'ingénierie sociale et d'autres méthodes d'exploitation pour tirer parti des employés mécontents. Les acteurs de la menace offrent souvent soit un paiement en espèces forfaitaire pour l'accès, soit un pourcentage des gains après une attaque réussie. Ils vont aussi loin pour essayer d'assurer l'anonymat de l'initié travaillant avec eux.

Menaces de logiciels malveillants sur Linux

Pendant un certain temps, Linux a bénéficié de moins d'attention de la part des acteurs de la menace que d'autres systèmes d'exploitation, malgré le fait que Linux soit crucial pour de nombreuses entreprises d'infrastructure critique, représentant environ 80% des serveurs Web et étant le système le plus utilisé pour les appareils IoT. La dépendance à Linux dans ces domaines, ainsi que son utilisation pour la virtualisation dans l'environnement d'entreprise, a conduit à une récente augmentation de nouveaux maliçiels (y compris les rançongiciels) ciblant le système d'exploitation.

Au cours de l'année passée, nous avons assisté à une montée en flèche de nouveaux maliçiels, avec une attention particulière portée sur Linux. Le rançongiciel, parmi d'autres menaces, a commencé à introduire des variantes Linux, contribuant à l'augmentation des menaces pour ce système d'exploitation.

- **Rootkits :** À partir de mi-2022, nous avons commencé à détecter une vague de maliçiels basés sur Linux avec des capacités de rootkit, et au fur et à mesure que l'année avançait, leur nombre augmentait. Cela a marqué le début d'une nouvelle tendance qui a continué sa trajectoire jusqu'en 2023.

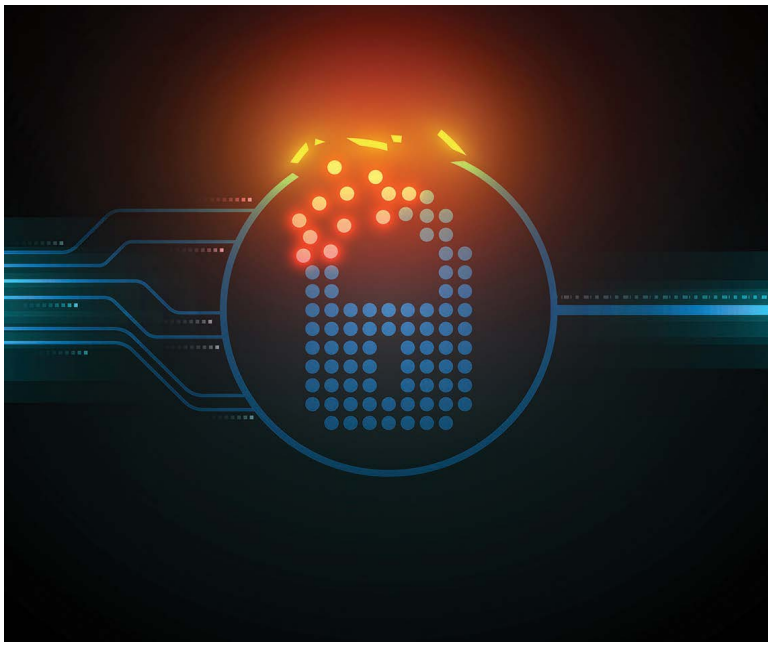
- **Rançongiciels :** Un important changement a eu lieu dans le paysage de la cybersécurité vers la fin de l'exercice 2022. Les groupes de rançongiciels, y compris de nombreux acteurs de menaces de haut profil tels que LockBit et Black Basta ransomware, ont commencé à étendre leur maliçiels incluant des variantes pour attaquer les systèmes Linux. Alors que nous atteignions le milieu de 2023, les variantes spécifiques à Linux associées à plusieurs groupes de rançongiciels de haut profil et plus discrets ont commencé à dominer l'écosystème cyber. Ces variantes étaient adaptées pour infecter les plateformes Linux, y compris les serveurs VMware ESXi. Des groupes de rançongiciel prédominants comme Akira, Royal et ALPHV/BlackCat, des groupes de menaces connus pour cibler les infrastructures critiques, ont présenté leur maliçiel Linux, démontrant la gravité de l'évolution du paysage des menaces.

Menaces provenant de nouveaux outils générés par l'IA

Alors que l'IA continue de transformer le marché mondial et la cybersécurité, les organisations doivent prendre des mesures proactives pour atténuer les menaces liées à l'IA. L'adoption généralisée d'outils, tels que les chatbots basés sur l'IA, les a rendus une cible pour les acteurs de menaces cherchant à exploiter leur popularité pour déployer des maliciels, posant des risques significatifs pour les entreprises mondiales et les chaînes d'approvisionnement.
Les outils d'IA générative peuvent être utilisés pour lutter contre la cybercriminalité. Les entreprises ont commencé à adopter ces outils pour mieux comprendre comment et pour sécuriser les environnements. Cependant, les adversaires les ont vus comme un moyen de les aider dans les attaques ciblées

Voici quelques-uns des outils malveillants qui se sont tracé un chemin dans le cyberespace l'an dernier :

FraudGPT – Cet outil fonctionne comme ChatGPT, mais est adapté pour faciliter les cyberattaques. Il est apparemment capable de créer des maliçiels indétectables, de composer du code malveillant, d'identifier des vulnérabilités, de concevoir des pages d'hameçonnage et de favoriser l'apprentissage des techniques de piratage.



WormGPT – Ce module d'IA basé sur le cadre de ChatGPT, a été mis de l'avant sur les plateformes du drak web en 2023. Les acteurs de menace ont entraîné WormGPT avec un éventail de sources de données afin d'automatiser la création de courriels d'hameçonnage très élaborés et personnalisés en fonction de leur destinataire.

WolfGPT – Basé sur Python, WolfGPT utilise l'IA générative pour créer des outils de piratage malhonnêtes. Il conçoit des logiciels malveillants chiffrés et compose des messages d'hameçonnage raffinés. WolfGPT assure la confidentialité des sessions et du contenu généré par IA.

DarkBART et DarkBERT – DarkBERT a été créé avec l'intention de combattre le cybercrime. On croit qu'à l'étape de recherche, des pirates informatiques ont accédé au code et créé la version malveillante, DarkBART. Son auteur indique que l'outil communique dans 27 langues différentes. DarkBERT est formé avec une grande quantité de texte provenant du dark web, ce qui en fait un outil puissant pour les cybercriminels. Ce logiciel est conçu pour favoriser différentes activités malveillantes, notamment les attaques avancées de manipulation d'ingénierie sociale, l'exploitation de systèmes, la distribution de rançongiciels et les campagnes d'hameçonnage. Il peut également aider les cybercriminels à trouver des vulnérabilités de type *Zero-day* ainsi que des faiblesses dans les infrastructures essentielles.

Actuellement, il y a quelques doutes sur ces outils malveillants ; cependant, l'entrée des outils d'IA générative et l'augmentation des malwares d'IA et des chatbots malveillants similaires, peuvent encourager de nouveaux acteurs de menaces à se tourner vers des activités cybernétiques néfastes. Ces outils peuvent créer des emails d'hameçonnage parfaits, imitant le langage et la culture de l'entreprise ciblée, améliorant l'efficacité d'un email de phishing. Nous pourrions voir l'IA générative utilisée comme une arme dans d'éventuelles cyberattaques, posant des défis significatifs pour le paysage de la cybersécurité.

Menaces d'États-nations : activité en temps de guerre

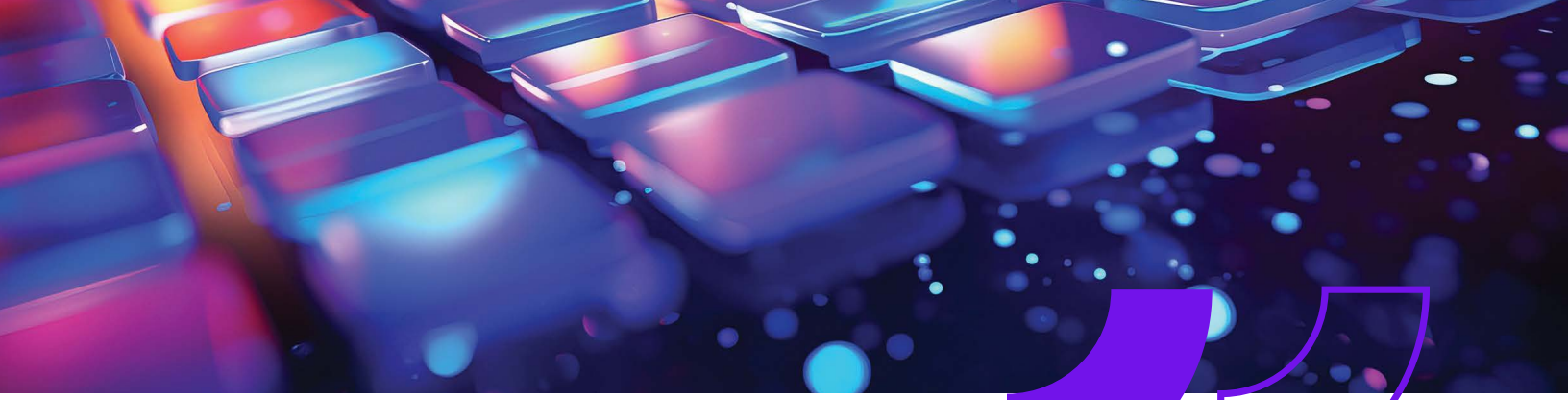
Les groupes de menaces d'État-nation sont motivés par des objectifs gouvernementaux/géopolitiques plutôt que par l'enrichissement personnel, ce qui conduit à une plus grande concentration sur le vol de propriété intellectuelle, l'espionnage et les attaques contre les infrastructures critiques. En période de troubles géopolitiques significatifs, les acteurs d'État-nation travaillent souvent en conjonction avec d'autres acteurs de menaces, tels que les groupes de crime organisé, les hacktivistes ou les cyber-extorqueurs, pour intercepter, influencer ou perturber les relations entre les nations. Leur objectif ultime peut être de subvertir, influencer ou distraire les gouvernements concurrents ou, plus directement, de permettre des actions cinétiques ou la capacité de se défendre contre elles.

- **Sandworm –** Reconnu pour leurs attaques sur le réseau électrique ukrainien en décembre 2015 et décembre 2016, il est considéré comme l'un des groupes d'État-nation les plus destructeurs actuellement actifs.

  – Sandworm a interrompu un réseau d'électricité ukrainien vers la fin de 2022, causant une panne d'électricité. Coordonnée avec des tirs de missiles sur des infrastructures essentielles partout en Ukraine, cette cyberattaque est passée inaperçue jusqu'en novembre 2023.

  – En mai et en septembre 2023, Sandworm a ciblé 11 fournisseurs de services de télécommunications en Ukraine, ce qui a entraîné des perturbations de service et de possibles fuites de données.

  – En mai 2023, Sandworm a ciblé 22 entreprises d'infrastructures essentielles au Danemark. C'était le plus important événement informatique à menacer les infrastructures essentielles dans ce pays. L'attaque a notamment visé 16 fournisseurs d'énergie danois, corrompant du même coup 11 entités associées à l'énergie.



Activités des cyberactivistes en 2023

Bien que le cyberactivisme ait déjà évoqué des images du masque de Guy Fawkes et des demandes d'Anonymous exigeant la publication de documents ou d'autres actions soutenant un objectif politique décentralisé, il a évolué et grandi depuis. De nombreuses activités de cyberactivisme soutiennent maintenant des objectifs d'États-nations et peuvent être associées à une plus grande campagne de désinformation, ou dans certains cas, d'actions physiques.

Cet élargissement est un important développement, car les cyberactivistes sont souvent motivés par la passion plutôt que par l'argent. Les fervents partisans peuvent fournir plus d'efforts, de temps et d'attention à leurs attaques ou à leurs tentatives d'accès que les criminels cherchant à faire des profits rapidement et facilement. Les risques émanant de ces groupes ont augmenté en 2023. Voici quelques exemples de groupes de cyberactivistes appuyant des États-nations.

Zarya

Zarya est apparu au début de 2022 en s'associant au groupe de menace Killnet. Son leader a sous-entendu qu'avant ce partenariat, son groupe était actif sous différents noms, dont « 0x000000 » et « Quarantine ». En 2022, ce groupe a divulgué des dossiers sur des entités ukrainiennes corrompues. Vers la fin de 2022, il s'est détaché de Killnet en formant une marque de piratage distincte.

- Des documents divulgués en avril 2023 faisaient référence à Zarya. Ces documents contenaient des affirmations voulant que le groupe a réussi à accéder en février 2023 au réseau des systèmes de contrôle industriel d'une compagnie de gaz canadienne anonyme, lui permettant d'augmenter la pression des valves, de désactiver des alarmes et de forcer l'arrêt d'un centre de distribution de gaz. Il n'est toujours pas clair si ces dossiers étaient légitimes ou s'ils faisaient partie d'une campagne de désinformation, une tactique que les cyberactivistes emploient couramment.

NoName057(16)

NoName057(16) est un groupe de cyberactivistes actif depuis mars 2022. Il mène principalement des attaques par déni de service distribué contre des entités gouvernementales et d'infrastructures essentielles, en Ukraine et ailleurs où on appuie ce pays.

- Le 10 avril 2023, NoName057(16) a dirigé ses menaces vers des entités canadiennes lors d'attaques par déni de service distribué qui ont duré une semaine. Le groupe a encouragé d'autres groupes de menace à sévir contre les sites web associés au gouvernement du Canada en leur promettant une récompense pécuniaire.

Anonymous Sudan

Anonymous Sudan attaque des entreprises américaines en guise de protestation contre l'implication des États-Unis dans les affaires du Soudan. Le groupe est cependant associé à des groupes qui appuient la Russie, ce qui suggère que le nom n'est qu'un leurre.

- En juin 2023, Anonymous Sudan a revendiqué une attaque par déni de service distribué qui a ralenti le service du portail Azure de Microsoft.
- En novembre 2023, OpenAI a été victime d'une attaque par déni de service distribué ce qui a perturbé ses services API et ChatGPT, qui étaient ciblés.

Indian Cyber Force

Les cyberactivistes d'Indian Cyber Force (ICF) visent plusieurs pays. On a toutefois remarqué qu'ils ciblent particulièrement les pays qu'ils croient être contre l'Inde ou son programme politique.

- En octobre 2023, plusieurs sites web du gouvernement du Canada ont été inaccessibles pendant une ou deux heures à la suite d'une série d'attaques par déni de service distribué. Ces attaques ont fait suite aux allégations du premier ministre du Canada insinuant que le gouvernement de l'Inde avait joué un rôle dans l'assassinat d'un important leader du Khalistan en sol canadien. ICF a revendiqué ces attaques en soutenant que le gouvernement canadien avait « dépassé les bornes ».

SiegedSec

SiegedSec est un groupe de cyberactivistes qui corrompt des bases de données de grandes organisations, dont beaucoup œuvrent dans les secteurs des infrastructures essentielles, pour y voler des renseignements permettant d'identifier des personnes. Après que le conflit entre Israël et la Palestine ait éclaté, SiegedSec et Anonymous Sudan ont déclaré qu'ils cibleraient les infrastructures essentielles et les systèmes industriels de l'Israël, de même que le système mondial de navigation par satellites. En juin 2023, Anonymous Sudan a revendiqué une attaque par déni de service distribué contre le portail Azure de Microsoft, ralentissant ainsi le service.

- En octobre 2023, le groupe a allégué avoir volé près de 3 000 documents d'une entreprise intergouvernementale.
- En novembre de la même année, SiegedSec a revendiqué une fuite avec vol de données personnelles des membres de l'effectif d'un laboratoire américain. Ce laboratoire et un cabinet de cybersécurité ont récemment annoncé leur partenariat pour combattre les cybermenaces aux infrastructures essentielles à l'aide de renseignements propulsés par l'informatique.

Attaques contre les chaînes d'approvisionnement en 2023 et étude de cas sur SCATTERED SPIDER

Dans le cadre de l'évolution rapide de la cybersécurité, la méthode « attaque par chaîne d'approvisionnement » est devenue un imposant vecteur de menace. Elle s'éloigne des cyberattaques conventionnelles, qui se concentrent généralement sur l'exploitation des vulnérabilités dans le réseau d'une seule organisation. Contrairement aux menaces traditionnelles, une attaque par chaîne d'approvisionnement traverse habilement la toile complexe de fournisseurs et de prestataires de services, lesquels forment collectivement l'ossature de la livraison de biens et de services.

L'une des caractéristiques distinctives d'une attaque par chaîne d'approvisionnement est son exploitation stratégique de la confiance. Lors d'une cyberattaque traditionnelle, les auteurs de menace se fient souvent aux vulnérabilités et faiblesses techniques. En revanche, une attaque par chaîne d'approvisionnement profite de la confiance implicite que les organisations accordent à leurs collaborateurs. Un niveau de confiance est atteint à mesure que les organisations solidifient leurs partenariats avec les fournisseurs et les prestataires de service, ce qui donne lieu à un flux continu de biens et d'information. Les cybercriminels exploitent cette confiance pour introduire des éléments malveillants dans la chaîne d'approvisionnement, manipulant ainsi les mêmes relations sur lesquelles les organisations comptent pour leurs activités.

Lorsqu'on l'observe dans le contexte d'une attaque par chaîne d'approvisionnement, le réseau d'une organisation va bien au-delà de ses systèmes internes. Il englobe un écosystème complexe et entrecroisé qui comprend les fournisseurs, les prestataires de services et diverses autres entités essentielles à la production et à la livraison de biens et de services. Il est primordial de comprendre les subtilités de ce réseau interconnecté pour maîtriser les vulnérabilités et les risques possibles associés aux attaques par chaîne d'approvisionnement.

Selon le média Bleeping Computer, l'un des plus importants incidents associés à la compromission par chaîne d'approvisionnement a été la cyberattaque contre l'administrateur de système virtuel (ASV) de Kaseya, en 2021. Le groupe de rançongiciel REvil a profité d'une vulnérabilité du jour zéro dans le très populaire logiciel d'ASV de Kaseya, une des solutions préférées des fournisseurs de services de gestion (FSG). Essentiel pour la surveillance et la gestion à distance des systèmes de TI, ce logiciel est devenu le vecteur involontaire des cybercriminels, qui s'en sont servi pour déployer le rançongiciel notoire. Les conséquences de cet acte dommageable se sont répercutées bien au-delà des FSG, en atteignant la structure même de leur clientèle. REvil a créé une vague de chaos en demandant une rançon exorbitante de 70 M$ en échange de la clé qui allait déchiffrer les données de toutes les organisations ciblées par l'attaque.

Par la suite, Kaseya s'est frayé un chemin dans le contexte complexe de la cybersécurité en collaboration avec des experts et des organismes d'application de la loi. L'entreprise a rapidement déployé des correctifs pour compenser les vulnérabilités dans son logiciel et renforcer ses défenses contre d'autres attaques possibles.

Plus récemment, Okta, une importante entreprise américaine de gestion des accès et des identités, a rapporté que les données de tous ses clients ont été corrompues lors d'une récente brèche de ses systèmes de soutien. Au départ, l'entreprise avait indiqué que seule une petite fraction de ses clients, soit approximativement 1 %, ou 134 organisations, avait été touchée. La brèche, qui a eu lieu en octobre 2023, a été provoquée par un pirate informatique qui s'est servi d'identifiants volés pour accéder au système de soutien de gestion de cas d'Okta et dérober des jetons de session téléversés par les clients afin de rendre possible l'accès non autorisé aux réseaux des clients d'Okta.

Dans un billet de blogue publié plus tard pour résumer les événements, le chef de la sécurité d'Okta a révélé l'ampleur de la brèche, qui englobait plus de clients. Bien qu'il n'ait fourni aucun chiffre exact, le chef de la sécurité d'Okta a expliqué que le 28 septembre, le pirate informatique a accédé à un rapport contenant des données appartenant à « tous les utilisateurs du système de soutien à la clientèle d'Okta ». Pour la majorité des clients (99,6 %), l'information consultée comprenait des noms complets et des adresses courriel.
Dans certains cas, les pirates pourraient également avoir récupéré des numéros de téléphone, des noms d'utilisateur et certains détails sur les postes des membres du personnel.

Selon Bleeping Computer et plusieurs autres médias, la pire attaque par chaîne d'approvisionnement a été possible en raison d'une vulnérabilité dans l'application de transfert de fichiers MOVEit. Vers la fin janvier 2023, le groupe de rançongiciel Cl0p a orchestré un raid tenace en profitant de cette vulnérabilité du jour zéro afin d'exploiter la plateforme de transfert géré de fichiers MFT. D'une durée de dix jours, le raid a permis d'accéder à environ 130 victimes. Le groupe Cl0p a notamment confirmé et revendiqué le vol de données réussi de la plateforme de gestionnaire MFT durant cette période.

Ces cyberattaques soulignent la complexité croissante des groupes de rançongiciel et leur capacité à exploiter les vulnérabilités du jour zéro pour commettre des effractions ciblées. Tandis que les organisations se battent contre des cybermenaces qui évoluent, il devient impératif d'améliorer les mesures de cybersécurité, de mener des évaluations détaillées des vulnérabilités et de renforcer les systèmes pour atténuer les risques de telles incursions. Ces incidents sont un rappel brutal des défis persistants que présentent les cybercriminels et du besoin continu en stratégies de cybersécurité proactives face à des environnements de menace qui progressent rapidement.

Une enquête réalisée récemment par l'équipe Renseignements sur les cybermenaces de KPMG au Canada a mis en évidence une attaque par chaîne d'approvisionnement orchestrée par l'auteur de menace connu sous le nom de SCATTERED SPIDER. L'entreprise victime a une vaste clientèle et offre différents services à diverses entités. La découverte a mis en lumière la nature complexe et évolutive des cybermenaces en soulignant l'acharnement des auteurs de menace à aller jusqu'à attaquer des organisations bien établies.

SCATTERED SPIDER a utilisé une approche multidimensionnelle en se servant de vecteurs d'attaque constants pour corrompre la sécurité de l'entreprise, et par conséquent, celle de ses clients. Trois principaux vecteurs d'attaque ont été décelés :

1. **Pourriel d'authentification à deux facteurs (A2F)**
   L'auteur de menace a ciblé les mécanismes d'A2F mis en œuvre par l'organisation victime. En visant particulièrement l'effectif de l'organisation, le cybercriminel a bombardé sa main-d'œuvre de demandes d'A2F. La pression sur la victime ou sa lassitude l'a éventuellement poussée à accepter la demande d'A2F malveillante, donnant ainsi à l'auteur de menace un accès total à l'infrastructure.

2. **Tactiques d'intimidation du personnel à l'aide de textos**
   En plus des pourriels d'A2F, SCATTERED SPIDER a envoyé des textos non sollicités. Le groupe a menacé le personnel de sévices corporels ou d'autre type de violence pour qu'ils acceptent les demandes d'A2F malveillantes. Cela concorde avec les récentes procédures et tactiques d'intimidation que le groupe de menace avait utilisées contre le centre des opérations de sécurité et les autres défenseurs du réseau.

3. **Utilisation des appareils vulnérables personnels**
   SCATTERED SPIDER a également ciblé les terminaux de la victime à l'aide de lecteurs qui étaient particulièrement malveillants. Le groupe a conçu son propre lecteur pour dérouter les logiciels de détection de terminaux et les antivirus. L'auteur de menace installait le lecteur malveillant et, à l'aide d'une application, supprimait les défenses du terminal.

La réussite des attaques répétées de SCATTERED SPIDER sur l'infrastructure de sa victime a eu de graves conséquences allant au-delà de la cible immédiate. L'entreprise étant un important fournisseur de services, son effectif avait accès à l'infrastructure interne de différentes organisations clientes. La compromission de l'entreprise victime est devenue un point d'accès à partir duquel les auteurs de menace ont pu infiltrer les réseaux de ces clients, entraînant une chaîne de fuites dans de nombreuses entreprises.

Les attaques ciblées soulignent l'effet d'entraînement des cybermenaces dans les écosystèmes d'entreprises interconnectées. En plus de compromettre les données sensibles et les opérations de la victime visée, la fuite a également tracé le chemin de compromissions en chaîne dans d'autres organisations. L'incident met en évidence l'importance vitale des mesures de cybersécurité robustes, de la vigilance soutenue et des efforts collectifs pour atténuer les menaces en constante évolution que posent les auteurs habiles et tenaces comme SCATTERED SPIDER. Tandis que les organisations composent avec l'environnement complexe de la cybersécurité, il est impératif de reconnaître que la compromission d'une entité peut se répercuter dans l'ensemble de la toile interconnectée des entreprises, ce qui réaffirme le besoin de résilience collective et de stratégies de défense proactive.

Évidemment, les attaques contre la chaîne d'approvisionnement émergent en tant qu'important problème de cybersécurité répandu, et différents facteurs contribuent à leur fréquence. La complexité croissante et l'interconnectivité fondamentale des chaînes d'approvisionnement mondiales font partie des principaux contributeurs de cette tendance. Combiné à la dépendance à un éventail diversifié de fournisseurs et de prestataires de services, l'élargissement des réseaux d'organisations crée une énorme surface d'attaque et offre aux auteurs malveillants de nombreux points d'entrée possibles. Les cybercriminels trouvent des occasions d'exploiter les vulnérabilités de certains composants de la toile complexe des dépendances qui caractérisent les chaînes d'approvisionnement, accédant ainsi à l'écosystème élargi.

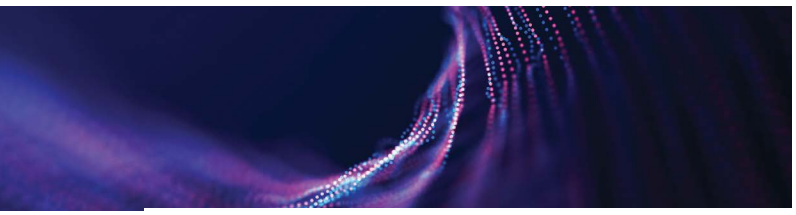
Le concept de l'amplification est un autre des facteurs notoires contribuant aux attaques par chaîne d'approvisionnement. Cibler stratégiquement un fournisseur ou un prestataire de service unique peut se traduire par des conséquences considérables à mesure que la compromission se répand dans les réseaux interconnectés. Les cybercriminels comprennent l'effet de ricochet de l'infiltration d'un lien central dans la chaîne d'approvisionnement, ce qui leur permet de corrompre de nombreuses entités en aval. En plus d'augmenter l'échelle de l'attaque, cette amplification présente un défi pour les organisations qui tentent de trouver l'origine et la portée exactes de la fuite.

Le troisième facteur d'importance est lié à la confiance accordée aux fournisseurs et aux prestataires de services. Les organisations nouent souvent des relations avec leurs fournisseurs en fonction de la confiance, en tenant pour acquis que leurs partenaires adoptent des pratiques solides en matière de cybersécurité. Malheureusement, cette confiance peut être exagérée, car les fournisseurs pourraient avoir de faibles postures de sécurité ou devenir eux-mêmes victimes d'attaques. Les cybercriminels exploitent cette relation en sachant qu'une brèche chez un fournisseur de confiance peut servir de point d'entrée caché dans l'organisation ciblée et permettre d'échapper aux mesures de sécurité habituelles.

En outre, il ne faut pas sous-estimer les mesures incitatives financières stimulant les attaques par chaîne d'approvisionnement. Les cybercriminels cherchent de plus en plus à obtenir un gain financier, et compromettre la chaîne d'approvisionnement offre des possibilités de rentabiliser la propriété intellectuelle et les données volées ou d'en tirer parti à l'aide de rançongiciels. Combiné aux complexités de l'attribution dans les chaînes d'approvisionnement complexes, le potentiel de retombées financières considérables rend ces attaques alléchantes pour les auteurs malveillants qui cherchent des occasions profitables.

Séquences pour les renseignements sur les cybermenaces

L'environnement des renseignements sur les cybermenaces est assujetti aux mêmes conséquences que celui de l'intervention en cas d'incident. Il est probable que les auteurs de menace continuent d'abuser des GML et des technologies d'IA et, par conséquent, que les méthodes et outils d'attaque évoluent. Cette évolution constante minera dramatiquement l'efficacité des indicateurs de compromission que recueillent les équipes de juricomptabilité dans un environnement touché par une fuite et entravera probablement les efforts d'attribution des attaques à un auteur de menace précis. Avec le dynamisme accru de l'environnement, les équipes de renseignements sur les cybermenaces devront adapter et réviser leurs modèles d'attribution ainsi que leur approche de soutien des programmes de sécurité pour mettre davantage l'accent sur les indicateurs de comportement et les techniques de détection et d'attribution des compromissions.



Renseignements et innovation stratégique

KPMG au Canada est fier d'offrir des services de renseignements d'affaires. En prenant en considération les répercussions de deuxième et de troisième ordre découlant d'une détection dans les activités commerciales de clients, le cabinet a accentué en 2023 son approche du renseignement axée sur les affaires, une approche qu'il a toujours mise de l'avant.

Intégrer pleinement les équipes de renseignements sur les cybermenaces et de gestion des vulnérabilités permet à celles-ci de bien comprendre l'environnement de menace et offrir de meilleures observations quant aux tactiques, techniques et procédures des auteurs de menace ainsi qu'une évaluation plus complète des vulnérabilités. Ensemble, elles sont en mesure d'enrichir leurs découvertes mutuelles et de procurer ainsi une valeur ajoutée grâce aux renseignements opportuns, exploitables et pertinents qu'elles produisent.

Les renseignements sur les cybermenaces sont le tissu conjonctif qui permet aux équipes de sécurité de s'entrecroiser et de collaborer afin d'offrir un maximum de valeur et d'efficacité.

Vulnérabilités constatées à l'exercice 2023

Introduction de nouveaux systèmes de notation des vulnérabilités : CVSS 4.0, la nouvelle norme du système commun de notation des vulnérabilités, et la dernière version du système de notation des prévisions d'exploitations (EPSS).

CVSS 4.0 est la nouvelle norme du système commun de notation des vulnérabilités. Simplification et clarification sont parmi les principales mises à jour et améliorations apportées à sa version actuelle. Elles ont été possibles grâce à la mise au point des idées liées aux exigences et à la complexité des attaques, ce qui rend la note plus facile à comprendre.

La nouvelle note CVSS 4.0 introduit également de nouvelles mesures et une structure améliorée permettant aux organisations d'adapter les systèmes de notation en fonction de leurs besoins et de leurs circonstances. La note est enrichie de renseignements sur les menaces et les risques associés en tenant compte de facteurs additionnels, notamment la probabilité d'une attaque et les conséquences de l'exploitation menant réellement à des atteintes à la sécurité.

Le système de notation des prévisions d'exploitations (EPSS) utilise une approche basée sur les données qui vise à aider les organisations à se concentrer sur la réparation d'une vulnérabilité en fonction de la probabilité de son exploitation dans son état actuel. C'est une excellente façon d'introduire un système de gestion des vulnérabilités en fonction des risques. La note de probabilité EPSS varie de 0 % à 100 %; plus le pourcentage est élevé, plus le risque d'exploitation est grand. Une note EPSS est indiquée pour tous les codes CVE publiés.

	CVSS	EPSS
Échelle de notation	De 0 à 10	De 0 % à 100 %
Définition de la note	Gravité d'une vulnérabilité	Possibilité qu'une vulnérabilité soit exploitée dans les 30 prochains jours
Sources de données	Paramètres temporels, environnementaux, de base et d'attaques calculés dans la note	Sources propulsées par l'apprentissage machine, y compris les données actuelles et historiques
Dernière mise à jour	CVSS 4.0 (8 juin 2023)	Notes mises à jour quotidiennement

1. CVE-2023-27524 (exécution de code à distance Apache Superset) : Cette vulnérabilité de contournement d'authentification provient d'une configuration par défaut non sécurisée dans l'outil Apache Superset, une plateforme de source ouverte de visualisation et d'exploration de données. L'exploitation réussie de cette faille entraîne une exécution de code à distance qui permet aux auteurs de menace d'obtenir un accès administratif aux serveurs ciblés afin de corrompre ou de voler les identifiants des utilisateurs.

Cette vulnérabilité est le résultat de la clé SECRET_KEY utilisée par Flask et ayant une valeur par défaut prévisible au moment de l'installation, ce qui exacerbe les attaques de validation de session. Plusieurs groupes malveillants ont exploité cette faille.

Versions touchées : toutes les instances de serveur qui appliquent la valeur SECRET_KEY par défaut, des versions 1.4.1 à 2.0.1.

Bien qu'il n'y ait pas de preuves concrètes d'exploitation répandue, des milliers de serveurs Apache Superset sont vulnérables à cette attaque.

2. CVE-2023-2868 (passerelle de sécurité de courriel Barracuda) : Cette vulnérabilité d'injection de commande de système d'exploitation dans l'appareil de passerelle de sécurité de courriel Barracuda existe en raison d'une mauvaise validation d'entrée lors du traitement des archives .tar. La passerelle de sécurité de courriel Barracuda est un appareil matériel conçu pour protéger les entreprises contre différents types d'attaques, notamment les pourriels, les virus, l'hameçonnage, les menaces par courriel et les maliciels.

L'exploitation réussie de cette vulnérabilité permettrait aux auteurs de menace d'envoyer une archive malveillante à l'appareil et d'exécuter des commandes arbitraires Perl sur le système ciblé, ce qui pourrait le corrompre en totalité. Cette vulnérabilité permet de lancer et d'exécuter un tunnel inversé sur l'appareil Barracuda afin d'établir la communication avec le serveur de commande et de contrôle de l'attaquant.

Elle est activement exploitée par différents groupes malveillants comme SocGholish et DogeRAT, ainsi que des groupes de rançongiciel tels BlackByte et LockBit, Cl0p.

3. CVE-2023-27350 (PaperCut NG/MF) : Cette vulnérabilité de contrôle d'accès inapproprié dans le logiciel PaperCut NG/MF existe en raison de mauvaises restrictions d'accès dans la catégorie SetupCompleted. PaperCut NG/MF est un logiciel de gestion d'imprimante qui aide les organisations à effectuer les tâches d'impression et de photocopie. Cette vulnérabilité permet aux auteurs de menace de contourner l'authentification afin d'exécuter un code arbitraire avec les privilèges du système.

Versions touchées : PaperCut NG/MF antérieures à 22.0.9

Cette vulnérabilité a été exploitée telle quelle, et différents groupes malveillants comme les rançongiciels Buhti et Bl00Dy, ainsi que Havoc C2 binary, Cobalt Strike et Lockbit 3.0 en ont profité.

4. CVE-2023-27351 (PaperCut NG/MF) : Cette faille d'authentification inappropriée dans le logiciel PaperCut NG/MF est causée par une erreur dans la catégorie SecurityRequestFilter. Elle permet aux auteurs de menace de contourner le processus d'authentification afin d'obtenir un accès non autorisé à l'application.

Permettant à l'utilisateur de réaliser des attaques simples nécessitant peu d'interactions, elle a été exploitée telle quelle par divers groupes d'auteurs, notamment les rançongiciels Ransom X, BlackByte, LockBit, Cl0p et Bl00Dy.

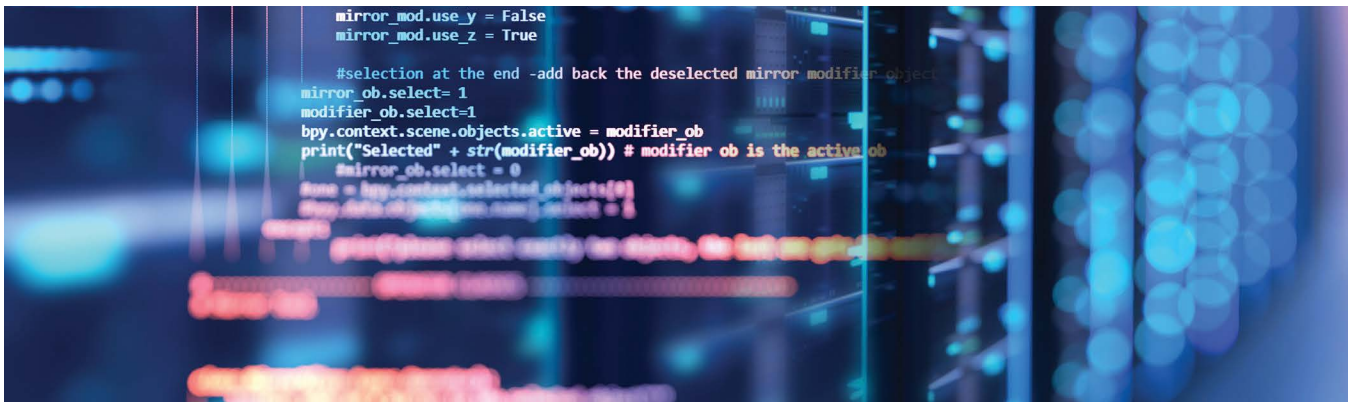
Versions touchées : PaperCut NG/MF antérieures à 22.0.9

5. CVE-2023-34362 (MOVEit Transfer et MOVEit Cloud) : Cette vulnérabilité d'injection SQL est causée par le nettoyage insuffisant des données fournies par les utilisateurs. Les auteurs de menace peuvent envoyer une demande spécialement conçue à l'application touchée et exécuter des commandes SQL dans la base de données de l'application.

Cette vulnérabilité a été exploitée par différents groupes malveillants, le plus important étant le groupe de rançongiciel Cl0p, qui s'en est servi pour déployer une coquille web sans précédent, LemurLoot, afin de voler les données des utilisateurs et d'extorquer de l'argent à ces derniers. Le groupe a publié une déclaration sur son site de fuite de données Tor. Des activités d'exploitation associées à cette vulnérabilité ont été observées dans des pièges à pirates depuis juin 2023.

6. CVE-2023-38035 (Ivanti) : Cette vulnérabilité existe en raison d'un manque d'authentification sur certaines interfaces API. Les auteurs de menace peuvent envoyer des demandes HTTP malveillantes au port TCP 8443 afin de contourner l'authentification et exécuter un code arbitraire sur le système.

Cette vulnérabilité a été catégorisée comme étant critique, et divers groupes malveillants et auteurs de menace l'ont exploitée en même temps que la vulnérabilité d'authentification inappropriée CVE-2023-35078 (Ivanti).



7. Vulnérabilités Codesys : Quinze vulnérabilités ont été observées dans le logiciel de contrôle de systèmes industriels de Codesys; elles pourraient potentiellement causer l'arrêt de centrales électriques et la collecte de données sensibles d'infrastructures essentielles. La trousse de développement logiciel sert à configurer et à tester des automates programmables (API) pour les systèmes industriels.

Code CVE	Composante CODESYS	Note CVSS	Incidence
CVE-2022-47379	CmpApp	8.8	Attaque par déni de service distribué, exécution de code à distance
CVE-2022-47380	CmpApp	8.8	
CVE-2022-47381	CmpApp	8.8	
CVE-2022-47382	CmpTraceMgr	8.8	
CVE-2022-47383	CmpTraceMgr	8.8	
CVE-2022-47384	CmpTraceMgr	8.8	
CVE-2022-47385	CmpAppForce	8.8	
CVE-2022-47386	CmpTraceMgr	8.8	
CVE-2022-47387	CmpTraceMgr	8.8	
CVE-2022-47388	CmpTraceMgr	8.8	
CVE-2022-47389	CMPTraceMgr	8.8	
CVE-2022-47390	CMPTraceMgr	8.8	
CVE-2022-47391	CMPDevice	7.5	Attaque par déni de service distribué
CVE-2022-47392	CmpApp/ CmpAppBP/ CmpAppForce	8.8	
CVE-2022-47393	CmpFiletransfer	8.8	

8. CVE-2023-36884 (exécution de code à distance dans Microsoft Office et Windows HTML) : Cette vulnérabilité est causée par la validation insuffisante de l'entrée fournie par les utilisateurs touchant les produits Microsoft Windows et Office. Les auteurs de menace peuvent inciter les utilisateurs à ouvrir un fichier malveillant afin de pouvoir exécuter un code à distance.

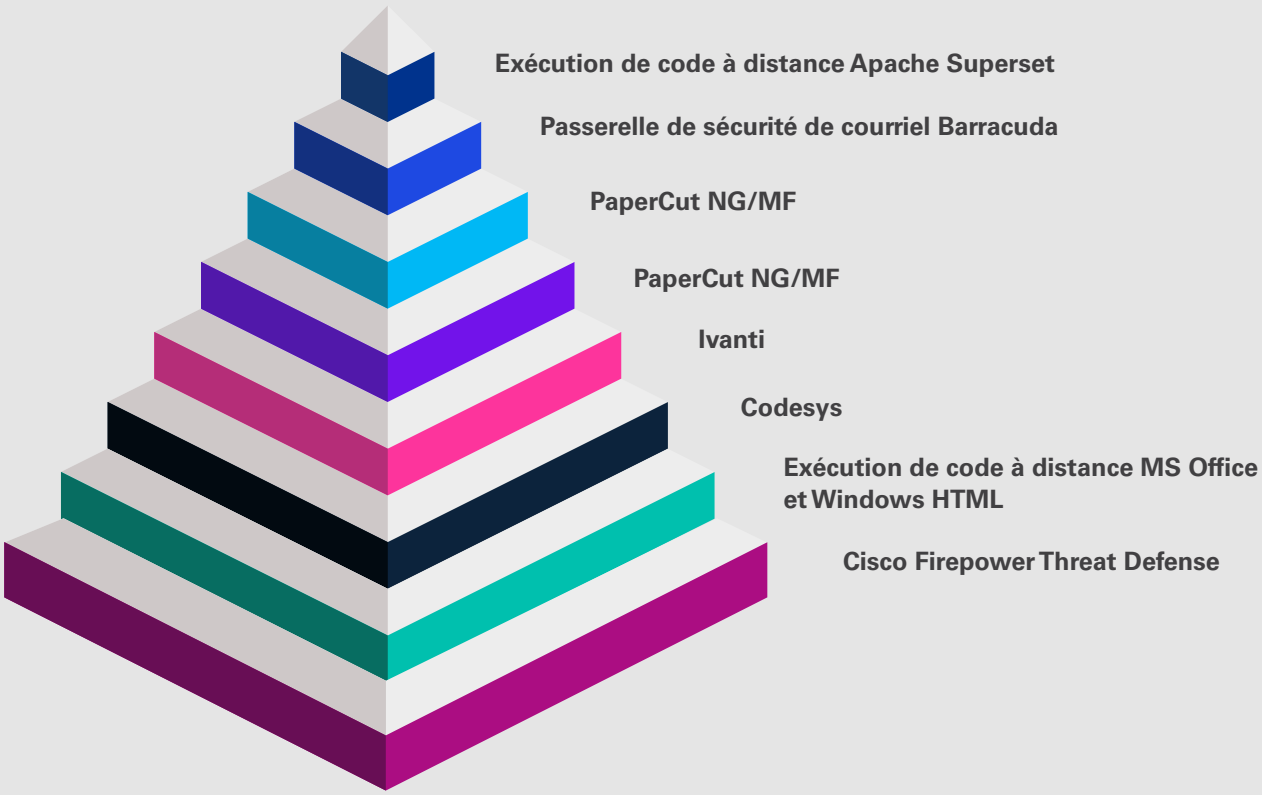
Plusieurs groupes de maliciels ont profité de cette vulnérabilité, le plus important étant Storm-0978, aussi connu sous le nom de RomCom, soit le nom de la porte dérobée qu'il distribue. Ce groupe cybercriminel est réputé pour ses opérations d'extorsion et ses raids ciblés de collecte d'identifiants en soutien aux opérations de renseignements.

Historiquement, les raids ciblés de Storm-0978 ont touché des organisations gouvernementales et militaires en Ukraine ainsi que des organisations en Europe et en Amérique du Nord possiblement impliquées dans les affaires ukrainiennes. Ces raids ont affecté les secteurs des télécommunications et des finances, entre autres.

9. CVE-2023-20269 (Cisco Firepower Threat Defense) : Cette vulnérabilité de contournement de l'authentification existe en raison d'une mauvaise séparation de l'authentification, de l'autorisation et de la comptabilité entre la fonctionnalité d'accès à distance par réseau privé virtuel (RPV) et les fonctionnalités de gestion HTTPS et de RVP intersuccursales. Les auteurs de menace peuvent mener des attaques brutales pour établir sans autorisation une session SSL RPV sans client.

Différents groupes malveillants en ont profité, notamment les groupes de rançongiciel LockBit, Conti et Snatch. Le groupe de rançongiciel Akira a exploité cette vulnérabilité à des fins pécuniaires, et il a vendu à plusieurs reprises cette exploitation d'exécution de code à distance dans un forum russe pour 100 000 $.

10. Principales vulnérabilités exploitées



Dans l'année à venir et par la suite, la collaboration et le partage d'information entre pairs du secteur, organismes gouvernementaux et forces de l'ordre demeureront essentiels à la défense collective contre les cybercriminels. L'expérience et les renseignements collectifs de la communauté de cybersécurité seront précieux au fil de l'évolution des menaces.

Regard vers l'avenir

Ce qui est prévu pour 2024 n'est pas très différent de l'année précédente. La cyberactivité criminelle et celle des États, de même que l'exploitation des vulnérabilités, resteront les principales influences sur la cybersécurité dans un avenir proche. Cela dit, 2024 présente des facteurs contextuels particuliers qui auront une incidence sur ces influences.

Cyberactivité des États

La hausse des opérations de désinformation suit la montée en volatilité de la politique mondiale. La majorité de ces opérations ont réussi, quoiqu'à différents degrés. Ainsi, à l'approche de l'élection présidentielle de 2024 aux États-Unis, nous anticipons une hausse continue des opérations de désinformation de la part d'États partout dans le monde. Il est probable que ces campagnes ciblent la mésinformation et la désinformation à l'intérieur des États-Unis; des raids concernant les actions d'États étrangers pourraient également avoir lieu selon le résultat de l'élection.

Ce dernier pourrait également donner lieu à des campagnes étrangères encourageant les personnes en interne de prendre des mesures informatiques perturbatrices ou destructives contre les employeurs ou les entités du gouvernement.

Cyberactivité criminelle

Une hausse des efforts de recrutement de personnes en interne dans les entreprises de la part des auteurs de menace a été enregistrée en 2022 et en 2023; cette augmentation risque de se poursuivre en 2024. À mesure que les auteurs de menace constatent une réussite accrue dans l'ensemble de l'environnement et ont davantage de ressources disponibles, il est possible qu'ils se tournent vers l'accès par des personnes en interne plutôt que vers le développement d'outils adaptés et le travail de recherche minutieux sur la cible. Bien que les outils de compromission soient efficaces, rien n'égale les actions malveillantes d'une personne faisant partie de l'environnement visé.

Conjointement, la montée des groupes d'auteurs de menace et de rançongiciels inconnus ou peu connus risque de se poursuivre. En évitant de se faire connaître, bon nombre de ces groupes espèrent passer sous le radar des autorités de lutte contre les cybermenaces envers les États. En adoptant une méthode d'attaque plus solitaire, ces groupes deviendront plus difficiles à détecter et à cibler.

Exploitation des vulnérabilités

L'augmentation de l'interconnectivité et des dépendances entre fournisseurs se poursuivra en 2023 et en 2024. Bien que cette connectivité aide les défenseurs grâce à une hausse des sources et des données entrées dans des journaux, pour la majorité des organisations, elle fait aussi croître considérablement le risque d'une fuite provenant d'un tiers. Il est important de comprendre que les programmes de gestion des vulnérabilités sont efficaces, mais qu'ils ne peuvent pas protéger les organisations d'un programme moins efficace chez un fournisseur essentiel.

L'utilisation de renseignements sur les cybermenaces pour surveiller la compromission des tiers essentiels devrait dorénavant être une fonctionnalité de base dans les programmes de gestion des vulnérabilités.

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*

Owen Key

Amir Rokinford

Renseignements sur les cybermenaces

Mike Rosenlund

Aindrea Skelly

Samanvitha Oruganti

Marie Eve Bergeron Tourangeau

Devin McDonald

Karan Ghoshal

Intervention en cas d'incident

Aleksander Wagner

Yiwei Guo

Mohak Kamboj

Kyle Johnston

Chris Walker

Ganesh Ramakrishnan

Xavier Normand

Robin Penrat

Jordan Michallet

Anne Labbé

Nous joindre

Intervention en cas d'incident

Alexander Rau
associé
alexanderrau@kpmg.ca

Ganesh Ramakrish
directeur principal
gramakrishnan@kpmg.ca

Mansoor Haqanee
directeur
mhaqanee@kpmg.ca

Guillaume Clement
associé
guillaumeclement@kpmg.ca

Valentin Bromont
directeur principal
vbromont@kpmg.ca

Xavier Normand
directeur
xnormand@kpmg.ca

Renseignements sur les cybermenaces et vulnérabilités exploitées

Robert Moerman
associé
rmoerman@kpmg.ca

Mike Rosenlund
directeur
mrosenlund@kpmg.ca

Marie-Eve Bergeron-Tourangeau
directrice principale
mbergerontourangeau@kpmg.ca

KPMG