Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

La cybermenace provenant des chaînes d'approvisionnement

Canada

À propos du présent document

Auditoire

Le présent bulletin sur les cybermenaces s'adresse aux dirigeants ayant un bien de technologies opérationnelles à protéger ainsi qu'aux lecteurs qui s'intéressent à la cybersécurité des technologies opérationnelles.

Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:CLEAR peut être distribuée sans aucune restriction. Pour obtenir de plus amples renseignements sur le protocole TLP (*Traffic Light Protocol*), prière de consulter la page Web https://www.first.org/tlp/.

Coordonnées

Prière de transmettre toute question ou tout enjeu relatif au présent document au Centre canadien pour la cybersécurité à contact@cyber.gc.ca.

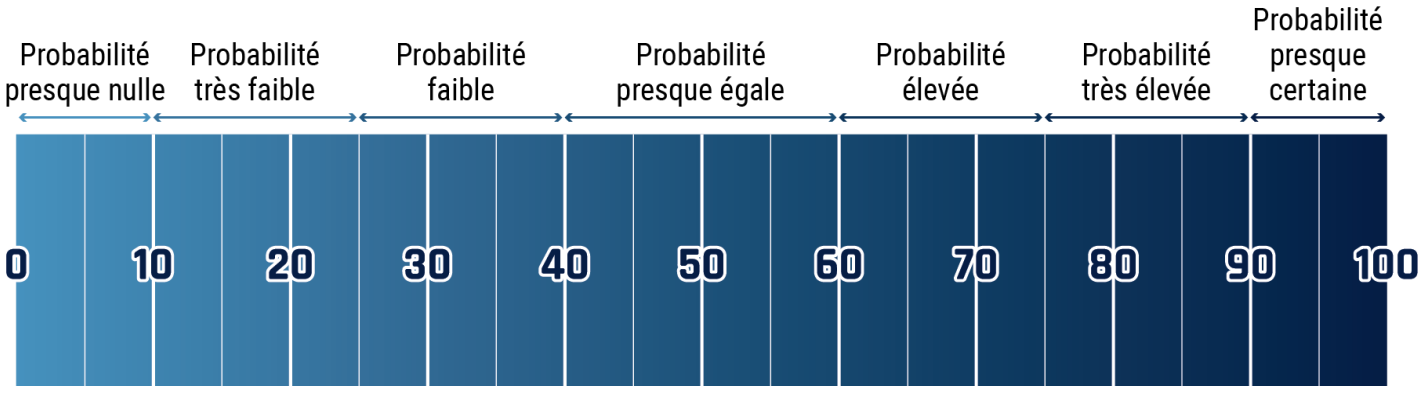
Méthodologie et fondement de l'évaluation

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) en matière de cybersécurité. En défendant les systèmes d'information du gouvernement du Canada (GC), le Centre pour la cybersécurité bénéficie d'une perspective unique lui permettant d'observer les tendances dans l'environnement de cybermenaces et d'appuyer ses évaluations. Dans le cadre du volet du mandat du Centre de la sécurité des télécommunications (CST) touchant le renseignement étranger, le Centre pour la cybersécurité tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes tels que « nous estimons que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probable » et « très probable » pour exprimer les probabilités.

Les évaluations et les analyses sont basées sur des renseignements disponibles en date du 31 août 2022.

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



Principaux avis

- Nous estimons qu'il est fort probable que les auteurs de menace continueront de développer leur capacité à compromettre les organisations en se servant des chaînes d'approvisionnement pour diriger des attaques contre les défenses réseau d'une victime.

- Nous estimons qu'il est fort probable que des auteurs de menace parrainés par un État continueront d'utiliser les chaînes d'approvisionnement pour compromettre des cibles d'intérêt stratégique, et qu'il est fort probable qu'ils continuent d'élaborer des stratégies de persistance au sein des chaînes d'approvisionnement pour faciliter le vol de renseignements utiles.

- Nous estimons qu'il est très probable que des adversaires étatiques puissent influencer leurs fournisseurs domestiques afin qu'ils compromettent eux-mêmes leurs produits dans la poursuite des intérêts nationaux de ces États. Ceci va à l'encontre des intérêts des clients canadiens et des intérêts du Canada.

- Nous estimons qu'il est fort probable que des cybercriminels, plus particulièrement les exploitants de rançongiciels, continuent de cibler des chaînes d'approvisionnement afin de maximiser le nombre de victimes potentielles et les profits qu'ils en tirent à chaque compromission.

- Nous estimons qu'il est fort probable que les logiciels continuent d'être les principaux vecteurs des manœuvres de cybermenace dans les chaînes d'approvisionnement, et nous estimons également qu'il est fort improbable que les chevaux de Troie matériels ou que les compromissions de la chaîne d'approvisionnement matérielle deviennent, à court terme, des vecteurs de menace importants au sein des chaînes d'approvisionnement.

- Nous estimons qu'il y a de fortes chances que des attaques du jour zéro continuent d'être utilisées par des auteurs de menace détenant des moyens sophistiqués dans la compromission de chaînes d'approvisionnement. Les attaques permettent à ces auteurs de contourner les contrôles de sécurité, d'éviter d'être détectés et d'optimiser le précieux exploit.

Table des matières

La cybermenace provenant des chaînes d'approvisionnement

Introduction

Les compromissions de la chaîne d'approvisionnement représentent une menace grandissante pour les entreprises, les infrastructures essentielles et les gouvernements canadiens. Les chaînes d'approvisionnement sont des écosystèmes de confiance composés de prestataires et de fournisseurs de services qui permettent aux organisations de développer et d'offrir des produits et des services. Elles sont devenues une composante de plus en plus importante du mouvement bidirectionnel de l'information numérique en plus du mouvement des produits, des services et de la monnaie. Les cybermenaces se propagent par le transfert d'information numérique, ce qui signifie que les chaînes d'approvisionnement fournissent une surface d'attaque étendue contre les organisations canadiennes et offrent une option pour les auteurs de cybermenace qui leur permet de mener une attaque directe contre les réseaux d'une organisation. Les compromissions de la chaîne d'approvisionnement ne sont pas une nouvelle technique pour les auteurs de menace. Il faut d'ailleurs noter qu'en 2021, plusieurs compromissions importantes ont été au cœur des préoccupations d'organisations au Canada et partout à travers le monde en ce qui a trait à la sécurité de la chaîne d'approvisionnement. Nous estimons qu'il est fort probable que les chaînes d'approvisionnement continuent d'être ciblées par des auteurs de menace à court terme.

Une telle surface d'attaque provenant des chaînes d'approvisionnement peut s'avérer difficile à protéger. Les chaînes d'approvisionnement, plus particulièrement lorsqu'il est question des technologies de l'information et des communications, peuvent être complexes, réparties à l'échelle mondiale, et elles consistent en plusieurs niveaux d'externalisation.[1] La compromission d'un seul fournisseur en amont peut entraîner l'introduction de vulnérabilités dans de nombreux systèmes d'organisations et d'utilisateurs en aval. Au cours des dernières années, les auteurs de menace ont démontré une capacité accrue à naviguer à travers les chaînes d'approvisionnement dans le but de compromettre leurs cibles ultimes. Nous estimons qu'il est fort probable que les auteurs de menace continueront de développer leur capacité à compromettre les organisations en se servant des chaînes d'approvisionnement pour diriger des attaques contre les défenses réseau d'une victime. Nous estimons qu'il est fort probable que les organisations canadiennes continuent, à court terme, d'être confrontées à du cyberespionnage et à de la cybercriminalité émanant des chaînes d'approvisionnement.

Pourquoi cibler les chaînes d'approvisionnement

Les compromissions de la chaîne d'approvisionnement offrent aux auteurs de menace un autre moyen indirect de compromettre leurs cibles ultimes. Une vulnérabilité peut être implantée à tout moment dans la chaîne d'approvisionnement ou au cours du cycle de vie d'un bien ou d'un service. Les auteurs de menace se retrouvent alors devant une surface d'attaque à exploiter beaucoup plus vaste. Ainsi, ils ne se limitent pas simplement à cibler le périmètre externe du réseau d'une victime. Une fois la vulnérabilité déployée à l'intérieur du réseau de la victime, les objectifs d'un auteur de menace sont les mêmes que pour les cybercompromissions habituelles. Ces objectifs comprennent le cyberespionnage ou une cyberattaque. Dans le cadre des compromissions de la chaîne d'approvisionnement, ces cyberactivités impliquent souvent le vol d'information ou de renseignement important, ou le déploiement de maliciels tels que des rançongiciels.

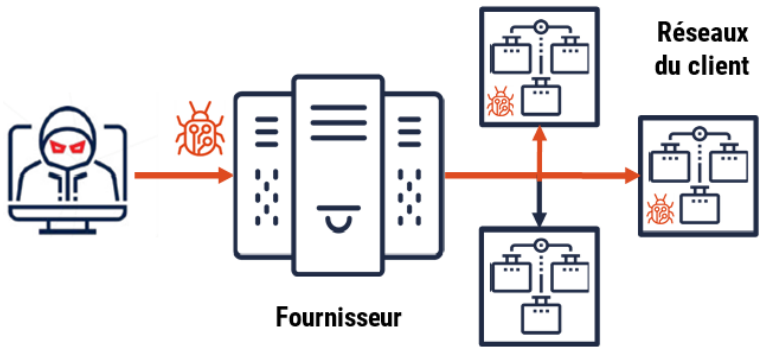


Figure 1 : Le mouvement des menaces dans la chaîne d'approvisionnement

En compromettant un fournisseur, les auteurs de menace peuvent se servir de leurs relations de confiance pour faciliter les compromissions contre des organisations en aval. Ces compromissions peuvent être ciblées ou systématiques.

Les compromissions de la chaîne d'approvisionnement comportent plusieurs caractéristiques qui les différencient des cybercompromissions habituelles. L'une de ces caractéristiques est que les **compromissions de la chaîne d'approvisionnement sont indirectes.** En compromettant d'abord un fournisseur et par la suite en exploitant ses relations de confiance avec des organisations en aval, les auteurs de menace peuvent contourner entièrement le périmètre des cyberréseaux de ces organisations, évitant ainsi de recourir à une intervention directe face aux moyens de protection du réseau ciblé. Ces compromissions peuvent être difficiles à détecter et à imputer, car elles proviennent souvent d'un produit ou d'un service légitime offert par un fournisseur de confiance. C'est pour cette raison que la cybersécurité d'une chaîne d'approvisionnement vaut ce que vaut son maillon le plus faible.

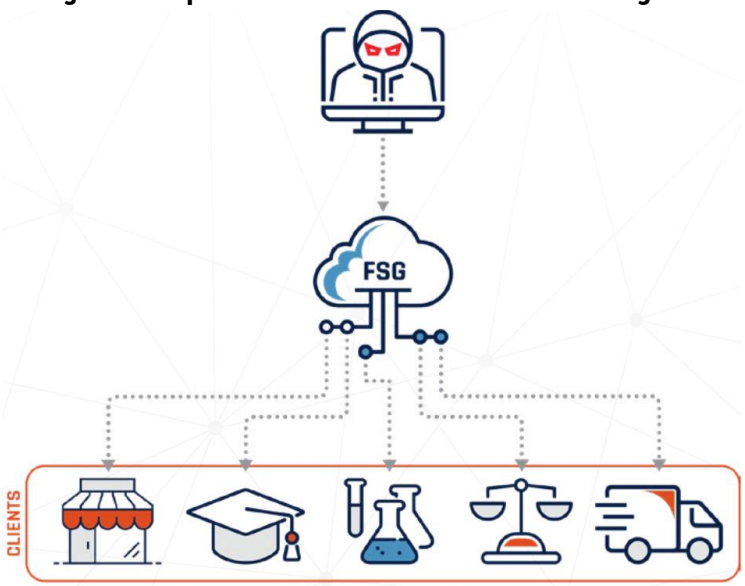
Information importante dans les chaînes d'approvisionnement des infrastructures essentielles

Des organisations industrielles, comme celles œuvrant dans le secteur d'infrastructures essentielles des services publics, sont fortement tributaires d'organismes auxiliaires de l'industrie pour assurer leur fonctionnement au quotidien. Les organismes auxiliaires de l'industrie comprennent les services professionnels d'ingénierie et de consultation du secteur privé qui sont obtenus à forfait par des fournisseurs de services essentiels pour le développement et la gestion des infrastructures, ainsi que les fournisseurs de technologies, de services et de fournitures.[2] Une compromission qui touche des chaînes d'approvisionnement d'infrastructures essentielles peut entraîner une perturbation ou une dégradation de services, ou l'exfiltration de documents ou de schémas de conception susceptibles de procurer un avantage lors de nouvelles tentatives visant à compromettre les réseaux et les systèmes du fournisseur d'infrastructures essentielles.

Par ailleurs, les auteurs de menace peuvent être en mesure d'atteindre leurs objectifs sans jamais avoir à se tourner vers un réseau en aval. Selon l'industrie, les fournisseurs peuvent détenir de l'information d'intérêt pour les auteurs de menace, particulièrement les organisations industrielles dans le secteur d'infrastructures essentielles des services publics, comme il est expliqué dans la zone texte ci-dessous. Au début de 2021, Quanta Computer, un fabricant de produits technologiques taïwanais et partenaire d'Apple, a fait l'objet d'une compromission causée par le groupe de pirates à l'origine du rançongiciel REvil. Les systèmes de Quanta ont été chiffrés et des données sensibles, notamment « ... de grandes quantités de dessins confidentiels et des gigaoctets de données personnelles associées à plusieurs grandes marques », ont été exfiltrées. En plus d'exiger une rançon pour déchiffrer les systèmes touchés, REvil a aussi tenté d'extorquer de l'argent à Apple en demandant une rançon pour empêcher la fuite des données et des schémas volés.[3]

Une autre caractéristique des compromissions de la chaîne d'approvisionnement pour les auteurs de menace est l'extensibilité. Les fournisseurs approvisionnent souvent beaucoup d'organisations en produits et services. Certaines organisations, comme les **fournisseurs de services gérés (FSG), ont un accès accru aux réseaux de nombreux clients**, ce qui permet aux auteurs de menace de toucher plusieurs cibles en même temps au moyen d'une seule compromission grâce aux privilèges réseau qui leur sont accordés, tel qu'il est illustré à la figure 2.

Figure 2 : Exploitation de fournisseurs de services gérés



Les auteurs de menace ciblent les FSG en vue d'accéder à leurs clients (notamment les entreprises, les établissements d'enseignement et les autres institutions) sans avoir à compromettre chaque client directement.

Les chaînes d'approvisionnement donnent l'occasion aux auteurs de menace de maximiser la valeur de l'exploitation des vulnérabilités du jour zéro. Une vulnérabilité du jour zéro désigne une vulnérabilité dont l'existence n'était pas connue du développeur avant d'être détectée comme moyen de compromission.

Étant donné qu'aucun correctif n'existe pour résoudre la vulnérabilité, les attaques du jour zéro ont une probabilité élevée de réussite. Par conséquent, les développeurs sont au cycle de vie « jour zéro » pour appliquer un correctif. Lorsque le jour zéro a été détecté et qu'un correctif a été mis en œuvre, il ne peut plus être utilisé contre des systèmes corrigés.

Au lieu de potentiellement « brûler » ce bien pour compromettre un seul réseau, il peut être utilisé contre un fournisseur qui se trouve à un échelon plus élevé de la chaîne d'approvisionnement pour faciliter l'accès à de nombreux réseaux en aval. Plusieurs vulnérabilités du jour zéro ont été utilisées dans la compromission, en 2021, de Kaseya VSA par le rançongiciel REvil, dont les vulnérabilités CVE-2021-30116[4] et CVE-2021-30120.[5] Il a ainsi été possible de contourner les exigences d'authentification pour accéder aux serveurs de VSA et déployer le rançongiciel dans près de 1 500 réseaux de clients en aval.[6]

Nous estimons qu'il y a de fortes chances que des vulnérabilités du jour zéro continuent d'être utilisées par des auteurs de menace détenant des moyens sophistiqués afin de compromettre les chaînes d'approvisionnement. Les attaques permettent à ces auteurs de contourner les contrôles de sécurité, d'éviter d'être détectés et d'optimiser les précieux exploits. Toutefois, l'utilisation d'exploits du jour zéro dans les compromissions de la chaîne d'approvisionnement sera limitée compte tenu de leur rareté et du coût élevé pour en faire le développement et l'acquisition.

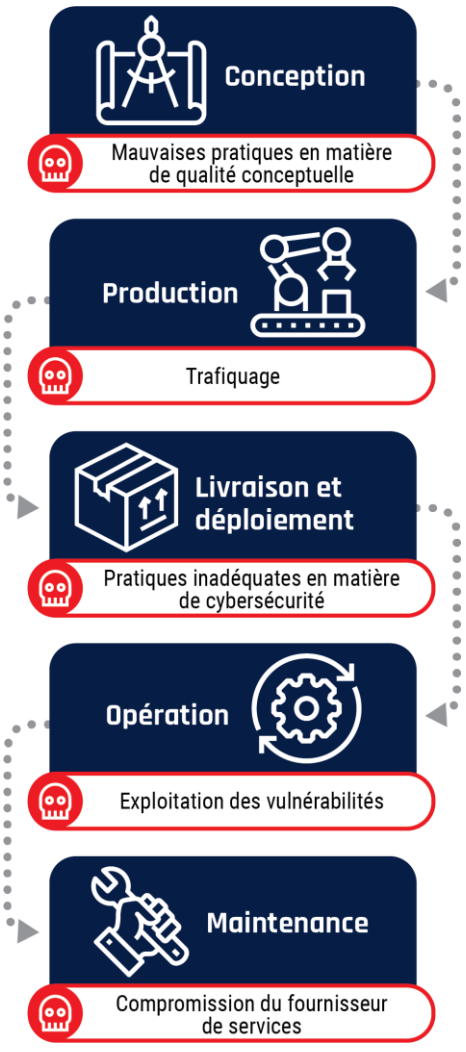
Types de compromissions de la chaîne d'approvisionnement

Nous estimons qu'il est fort probable que les logiciels continuent d'être les principaux vecteurs des manœuvres de cybermenace dans les chaînes d'approvisionnement, et nous estimons également qu'il est fort improbable que les chevaux de Troie matériels ou que les compromissions de la chaîne d'approvisionnement matérielle deviennent, à court terme, des vecteurs de menace importants au sein des chaînes d'approvisionnement. Les compromissions de la chaîne d'approvisionnement de logiciel modifient le logiciel du fournisseur ou elles profitent des relations de confiance d'un fournisseur pour implanter une vulnérabilité ou déployer un maliciel afin d'atteindre la cible ultime : l'acheteur ou l'utilisateur du logiciel.[7]

Tel qu'il est illustré dans la figure 3, les auteurs de menace peuvent avoir une incidence sur la chaîne d'approvisionnement en tout temps au cours du cycle de vie d'un produit ou d'un service. Parmi les méthodes de compromission de la chaîne d'approvisionnement de logiciel les plus souvent observées, notons les composantes libres, la signature de code détournée et les mises à jour compromises. Cette liste de vulnérabilités et de méthodes n'est pas exhaustive – les techniques pour permettre aux auteurs de menace de se propager dans les chaînes d'approvisionnement ne sont limitées que par leur capacité d'exploiter la relation de confiance qui existe entre des organisations et leurs fournisseurs.

Il est à noter que l'exploitation de vulnérabilités logicielles courantes découvertes de manière organique durant le cycle de vie du logiciel, comme les vulnérabilités liées à Microsoft Exchange[8] ou à Log4Shell[9], ne constitue pas des compromissions de la chaîne d'approvisionnement puisqu'elles ne résultent pas de l'activité d'un auteur de menace se trouvant à un niveau supérieur de la chaîne d'approvisionnement.

Figure 3 : Vulnérabilités liées à la chaîne d'approvisionnement



Composantes de logiciels ouverts

Le développement logiciel implique de plus en plus l'utilisation de composantes de logiciels ouverts afin de diminuer le temps de conception et soutenir l'innovation.[10] Les composantes de logiciels ouverts sont des progiciels de code ou de logiciel accessibles à tous gérés par des communautés de collaboration formées de développeurs qui appuient un vaste marché des idées.[11] Les méthodes courantes de compromission comprennent le typosquattage, l'injection de code malveillant et la confusion de dépendance. Une description plus détaillée est donnée au tableau 1 ci-dessous.

Le 9 mars 2020, GitHub, un site Web qui héberge et facilite le partage de code, a été informé qu'un maliciel s'était manifesté dans plusieurs dépôts hébergés sur sa plateforme. Lorsqu'un utilisateur téléchargeait un projet dans l'un de ces dépôts, il téléchargeait également un maliciel qui faisait un balayage de son système pour détecter l'environnement de développement NetBeans fonctionnant avec Java et, si cet environnement était trouvé, un injecteur de maliciel ayant téléchargé un cheval de Troie avec accès à distance était installé.[12] Les propriétaires des dépôts n'étaient pas au courant de cette activité, et il semblerait que les dépôts aient été infectés dès 2018. Au total, GitHub a trouvé 26 dépôts ayant été infectés par ce maliciel, appelé Octopus Scanner.[13]

Tableau 1 : Compromissions courantes des logiciels ouverts

Typosquattage :	Hébergement (par exemple, sur GitHub) d'une composante malveillante dont le nom est semblable à celui d'un projet légitime, mais ce nom est fondé sur les fautes de frappe et d'orthographe pouvant être facilement commises par un développeur en tentant de charger la composante dans son projet de développement.
Injection de code malveillant :	Intégration d'un code malveillant dans une composante de source libre légitime par quelque procédé que ce soit lorsque la composante est appelée.
Confusion de dépendance :	Attaque ciblée en vertu de laquelle les auteurs de menace identifient les dépendances logicielles propriétaires et téléversent des composantes malveillantes du même nom dans un dépôt public. Lorsque l'on s'attend à ce qu'une dépendance propriétaire soit utilisée, il est possible que le logiciel charge involontairement la composante malveillante accessible à tous.

Altération d'une signature de code

La signature de code est une méthode de validation de l'authenticité et de l'intégrité des exécutables et des scripts (c.-à-d. un code). Si un auteur de menace modifie un code tout en conservant l'intégrité de la signature, le destinataire va, sans le savoir, incorporer les ajouts malveillants à son code. Cela peut se faire en compromettant une autorité de certification (c.-à-d. la source du certificat de confiance) ou en faisant l'acquisition des clés privées d'un développeur légitime. Les clés privées peuvent être volées ou divulguées par inadvertance par l'auteur. Par ailleurs, si le code est signé au moyen d'une cryptographie faible, un auteur de menace pourrait être en mesure de pénétrer le chiffrement et de contrefaire la signature.

En janvier 2019, une entreprise spécialisée en cybersécurité a découvert que l'utilitaire ASUS Live Update avait été utilisé pour installer un maliciel sur environ 500 000 ordinateurs.[14] La compromission, appelée Operation ShadowHammer, était en cours depuis au moins le milieu de 2018. La raison pour laquelle ces compromissions duraient depuis si longtemps est en partie due au fait que les fichiers malveillants comportaient toujours une signature numérique valide. Généralement, toute modification apportée aux fichiers risque « d'endommager » la signature, ce qui indique que des modifications ont été faites. Toutefois, les auteurs de menace ont été en mesure de compromettre la signature numérique elle-même et de la réappliquer aux fichiers après avoir apporté les modifications malveillantes. Bien que les fichiers compromis aient été téléchargés à grande échelle, le maliciel a été conçu de façon à identifier et à mener des activités exigeant un suivi seulement auprès de cibles précises.[15]

Mises à jour détournées

Un élément distinctif de la chaîne d'approvisionnement logicielle est que le logiciel est pris en charge après sa sortie par des mises à jour publiées par le développeur pour résoudre des bogues et des problèmes liés à la sécurité ou pour ajouter des fonctionnalités. Les mises à jour provenant des fournisseurs de logiciels sont fiables et souvent installées par les utilisateurs sans en connaître le code sous-jacent ou son intégrité relative. Lorsqu'il est question de mises à jour détournées, on parle ici d'un code malveillant inséré par des auteurs de menace. Ce code est acheminé par des canaux de mises à jour officiels et fiables. Les mises à jour font l'objet du même niveau de privilège que le logiciel auquel elles sont appliquées, ce qui peut s'avérer considérable, particulièrement s'il s'agit d'une application en lien avec la sécurité qui permet à un code malveillant d'éviter certaines mesures de sécurité et de possiblement obtenir l'autorisation de modifier des fichiers système essentiels.

Operation ShadowHammer est aussi un exemple de compromission impliquant des mises à jour détournées, puisque la mise à jour compromise a été distribuée aux utilisateurs directement par l'entremise du vrai utilitaire ASUS Live Update. Un autre exemple de compromission par mises à jour détournées est lié au populaire logiciel utilitaire, CCleaner. CCleaner est un logiciel qui permet aux utilisateurs de supprimer de leurs systèmes des fichiers et des programmes indésirables. Les auteurs de menace ont tiré parti de l'accès au compte développeur Piriform pour mettre à jour le programme d'installation du logiciel CCleaner de façon à intégrer le maliciel. Les utilisateurs qui ont mis à jour ou téléchargé le logiciel CCleaner en passant par le site Web officiel de l'entreprise en août et en septembre 2017 ont reçu des versions du logiciel ayant été modifiées dans l'intention de nuire. Des chercheurs en matière de sécurité ont informé Avast de la situation le 13 septembre 2017 et, avec l'aide du FBI, les systèmes de commande et de contrôle de l'auteur de menace ont été désactivés. Mais déjà, la version malveillante de CCleaner avait été téléchargée par 2,27 millions d'utilisateurs.[16] Malgré le nombre élevé de téléchargements injectés, seule une quarantaine de machines ont été ciblées par le maliciel de second niveau, et seules onze de ces machines ont fait l'objet d'autres exploitations ciblées menées par l'auteur de menace.[17]

Menace provenant de produits matériels et physiques

Nous estimons qu'il est fort improbable que des chevaux de Troie matériels ou que des compromissions de la chaîne d'approvisionnement matérielle deviennent, à court terme, des vecteurs de menace importants au sein des chaînes d'approvisionnement. Les compromissions de la chaîne d'approvisionnement matérielle désignent un ajout malveillant ou une modification de composantes avec l'intention de créer une porte dérobée ou une vulnérabilité émergente à exploiter lorsque l'acheteur a déployé le matériel. Cette vulnérabilité peut ensuite être utilisée pour installer un dissimulateur d'activité ou un accès au système à distance, exfiltrer des données, ou dégrader ou détruire l'équipement au moyen d'une commande à distance.

Alors que des produits physiques sont devenus un vecteur d'infection dans des chaînes d'approvisionnement, ils sont généralement utilisés comme véhicules pour les menaces basées sur un logiciel. En 2018, par exemple, Schneider Electric a émis un avis de sécurité concernant des clés USB qui avaient été expédiées avec d'autres produits. Schneider a appris que ces dispositifs amovibles avaient été contaminés par un maliciel pendant la fabrication. Cette infection provenait de l'un de ses fournisseurs, et bien que le maliciel aurait pu être détecté et neutralisé par la plupart des programmes antimaliciels, l'entreprise a recommandé de se débarrasser de ces produits.[18] Même si la vulnérabilité a été transportée par le matériel, elle est de nature logicielle. Un cheval de Troie matériel pourrait hypothétiquement fournir à des auteurs de menace un moyen d'introduire systématiquement des vulnérabilités difficiles à détecter dans des produits ou des composantes, mais cette menace n'a pas encore été observée.

Auteurs de menace

Les auteurs de menace parrainés par un État

Nous estimons qu'il est fort probable que des auteurs de menace parrainés par un État continueront d'utiliser les chaînes d'approvisionnement pour compromettre des cibles d'intérêt stratégique, et qu'il est fort probable qu'ils continuent d'élaborer des stratégies de persistance au sein des chaînes d'approvisionnement pour faciliter le vol de renseignements utiles.

Les auteurs de menace parrainés par un État ont à leur disposition des outils supplémentaires pour atteindre leurs objectifs par l'entremise des chaînes d'approvisionnement. Au lieu de compromettre un fournisseur de façon clandestine, ils peuvent être en mesure de légalement obliger la coopération de fournisseurs qui relèvent de leur compétence sur le plan des activités militaires et de renseignement. À titre d'exemple, ils pourraient ordonner la production de données sur les clients ou d'un code source d'application pouvant leur permettre d'exploiter des applications plus efficacement dans des environnements ciblés lors d'opérations ultérieures. L'un de ces programmes est le programme d'accès légal de la Russie appelé système pour activité d'enquête opératoire (SORM pour *Operative Investigative Activities*). Le SORM est directement administré par le Service fédéral de sécurité (FSB) et ce système se veut peu efficace contre l'arbitraire et les abus.[19] Le SORM et les lois russes en matière de localisation de données donnent au FSB et à d'autres organismes de renseignement et d'application de la loi de nombreuses occasions de contraindre des organisations œuvrant en Russie à divulguer de l'information sensible.[20] Nous estimons qu'il est très probable que des adversaires étatiques puissent influencer leurs fournisseurs domestiques afin qu'ils compromettent eux-mêmes leurs produits dans la poursuite des intérêts nationaux de ces États. Ceci va à l'encontre des intérêts des clients canadiens et des intérêts du Canada.

En plus d'avoir tirer profit des techniques de compromissions des chaînes d'approvisionnement telles que la compromission des mises à jour, les auteurs de menace parrainés par un État ont démontré leur habileté à compromettre des fournisseurs de services comme des FSG en infiltrant la chaîne d'approvisionnement d'organisations d'intérêt stratégique, en établissant une persistance et en assurant l'accès à des cibles en aval.[21] Établir une persistance au sein de réseaux de fournisseurs de services assure un développement opportuniste, mais aussi sélectif de cibles stratégiques. La compromission SolarWinds Orion est un exemple qui décrit bien ce genre de campagne. Il a été démontré que les phases initiales de cette compromission ont commencé près d'un an avant sa découverte en décembre 2020, et que le maliciel avait été déployé des mois avant sa détection.[22]

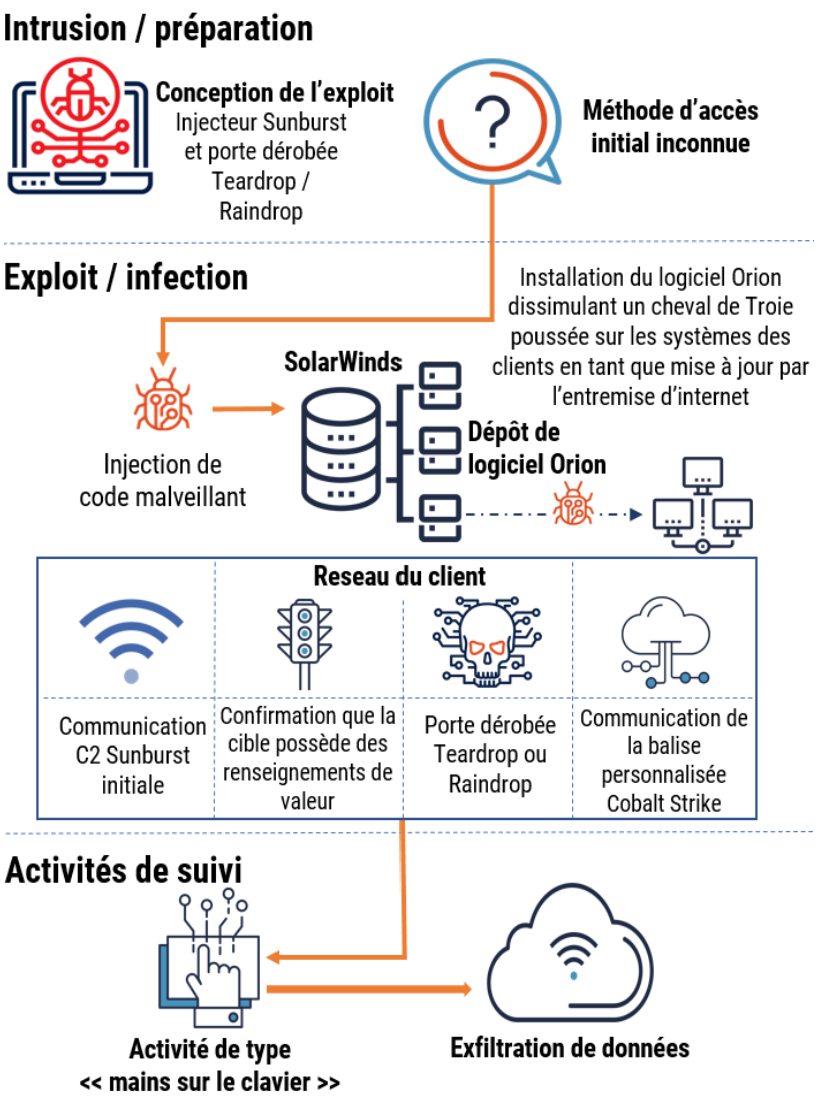
Étude de cas : Plateforme Orion de SolarWinds

SolarWinds est un fabricant de logiciels et un FSG qui a retenu l'attention du public à la fin de 2020 lorsque la firme de cybersécurité FireEye a découvert qu'un auteur de menace avait obtenu l'accès à ses systèmes par une mise à jour compromise provenant de SolarWinds Orion – un environnement de logiciel-service (SaaS) qu'utilisent les entreprises pour centraliser la surveillance et le contrôle de leurs réseaux, et qui a été largement utilisé par des organisations industrielles et gouvernementales en Amérique du Nord, en Europe, en Asie et au Moyen-Orient.[23] Le Canada et ses partenaires ont plus tard formellement désigné les services de renseignement étranger (SVR) russes, alias APT 29 ou Cozy Bear, comme étant l'auteur de cette compromission.[24]

Orion est une plateforme qui fonctionne sur les réseaux du client au lieu d'être hébergée sur des serveurs SolarWinds. Ainsi, les clients doivent régulièrement télécharger les mises à jour logicielles de SolarWinds pour appliquer les plus récents correctifs de sécurité. De telles mises à jour sont signées par l'éditeur afin de certifier que leur contenu est authentique, et le destinataire a la possibilité de s'assurer que le contenu n'a pas été modifié.[25]

La figure 4 illustre la chaîne de destruction,[26] c'est-à-dire la séquence des activités réalisées par l'auteur de menace au cours de la compromission. L'auteur de menace a implanté un logiciel malveillant dans l'environnement de développement de Solarwinds. Le code source d'Orion a ainsi été affecté par le maliciel SUNBURST. L'installation de la version compromise a

Figure 4 : Analyse de la chaîne de destruction de SolarWinds Orion



été poussée sur les systèmes des clients en tant que mise à jour de leurs installations Orion existantes, ce qui a déployé SUNBURST dans l'environnement des clients. SUNBURST a ensuite communiqué avec les auteurs de menace, qui devaient alors vérifier que l'environnement auquel ils ont eu accès renfermait des renseignements utiles méritant d'être exfiltrés. Si d'autres mesures étaient prises, la porte dérobée TEARDROP ou RAINDROP allait être déployée, et la balise personnalisée Cobalt Strike installée dans l'environnement. S'ensuivrait l'énumération du domaine pour permettre ensuite la collecte et l'exfiltration de renseignements utiles au moyen de techniques de type « mains sur le clavier ».

La compromission a rendu vulnérables près de 18 000 des 300 000 clients de SolarWinds, et il a aussi été déterminé qu'au moins 200 organisations ont fait l'objet d'activités de suivi ciblées.[27] Parmi les organisations qui ont été touchées se trouvent de nombreux leaders de l'industrie, dont Microsoft. Dans le cadre de cet incident particulier, des pirates ont été en mesure de voir certains des codes sources de Microsoft.[28] La compromission a aussi touché des ministères du gouvernement américain, dont le département de la Justice, le département d'État et la National Nuclear Security Administration.[29]

Bien que l'on estime que certaines organisations canadiennes aient téléchargé les versions compromises de SolarWinds Orion, il semblerait qu'aucune organisation canadienne n'a fait l'objet d'une activité d'exploitation de suivi menée par l'auteur de menace. Les conséquences de la compromission restent encore à déterminer, mais selon des chiffres estimatifs, le coût pour les organisations à travers le monde s'élève à des centaines de milliards de dollars, sans compter le coût lié au vol de propriété intellectuelle.[30] Microsoft a aussi imputé des compromissions en cours par ce même auteur de menace étatique (fort probablement les services de renseignement étranger [SVR] russes) au groupe qui a visé des fournisseurs de services infonuagiques, des FSG et d'autres secteurs de la chaîne d'approvisionnement technologique. Les compromissions auraient ciblé jusqu'à 609 organisations avec un total de 22 868 attaques.[31]

La menace des cybercriminels

Nous estimons qu'il est probable que des cybercriminels, plus particulièrement les exploitants de rançongiciels, continuent de cibler des chaînes d'approvisionnement afin de maximiser le nombre de victimes potentielles et les profits qu'ils en tirent à chaque compromission.[32] La grande majorité des cybercriminels sont motivés par l'appât du gain. Ils cherchent à exfiltrer des renseignements ayant une valeur commerciale pour la vente, à extorquer de l'argent à des victimes par le déploiement d'un rançongiciel ou à déployer des capacités de minage clandestin. Il s'agit dans ce cas d'un maliciel qui « mine » la cryptomonnaie en se servant des ressources d'un appareil infecté.[33]

Les compromissions criminelles de la chaîne d'approvisionnement sont particulièrement préoccupantes compte tenu de l'absence de discrimination dans leur ciblage. Les compromissions de la chaîne d'approvisionnement peuvent potentiellement exposer un large éventail d'organisations à des perturbations opérationnelles, ce qui comprend des éléments des infrastructures essentielles comme les écoles, les hôpitaux, les services publics et d'autres cibles de type « chasse au gros gibier » comme l'indique la description dans la zone de texte ci-dessous. Alors que certains cybercriminels ont fait savoir qu'ils ne cibleraient pas certains secteurs, d'autres groupes criminels démontrent moins de scrupules en attaquant spécifiquement des cibles comme les hôpitaux, sachant que ceux-ci ne peuvent se permettre des interruptions de services et qu'ils ont les ressources financières nécessaires pour payer des demandes de rançon élevées.[34]

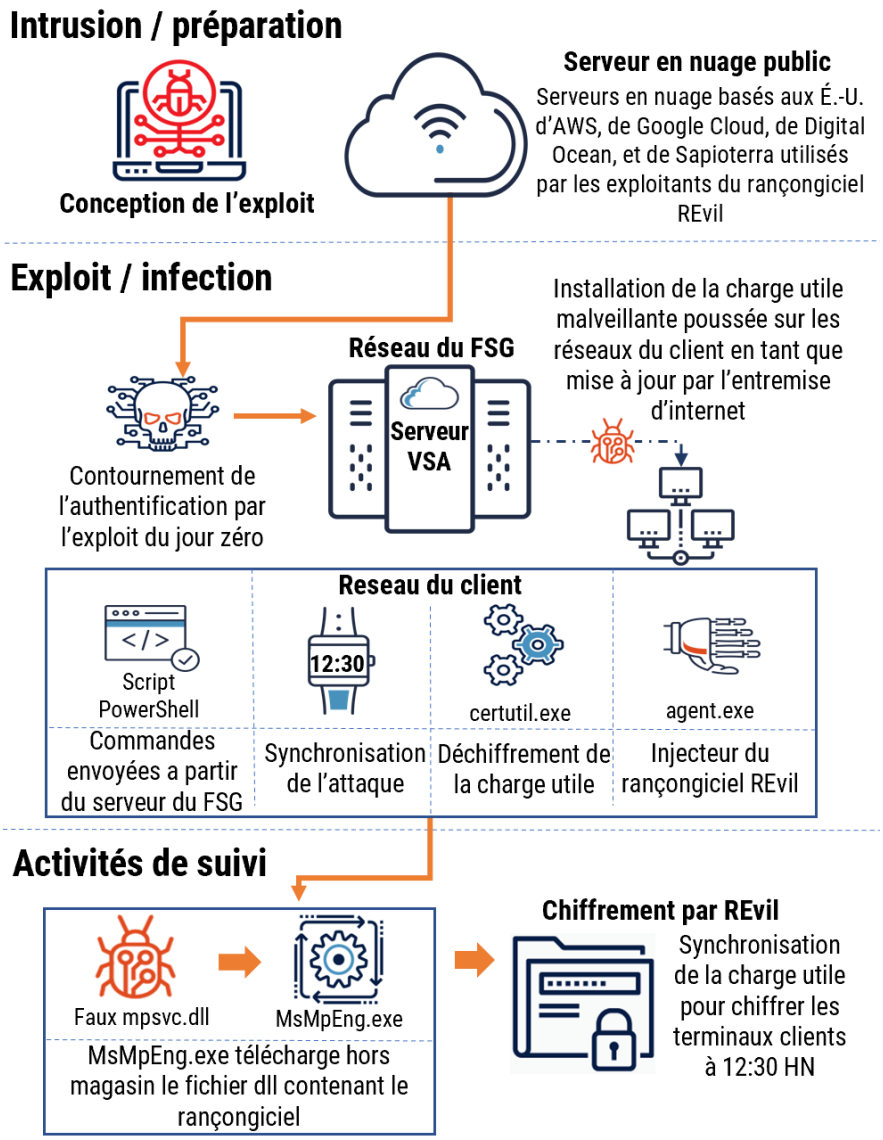
Les compromissions de composantes de logiciels libres sont devenues également un outil courant pour les cybercriminels, qui profitent d'une méthode d'entrée facile en propageant une vulnérabilité ou un ajout malveillant à un logiciel. En mai 2021, Palo Alto, un fournisseur de solutions de cybersécurité, a publié les résultats de son enquête sur des logiciels malveillants hébergés sur le populaire site communautaire du développeur, Docker Hub. Palo Alto a découvert 30 fichiers malveillants ayant recours au typosquattage de téléchargements populaires. Les fichiers malveillants contenaient des capacités de minage clandestin[35] et ils avaient été téléchargés plus de 20 millions de fois, générant ainsi un montant estimé à 200 000 dollars américains de revenus avant d'être retirés.[36]

Étude de cas : Kaseya VSA

Le 2 juillet 2021, soit le vendredi précédant la longue fin de semaine du Jour de l'Indépendance des États-Unis, Kaseya a lancé un avertissement selon lequel son équipe d'intervention en cas d'urgence enquêtait sur une possible compromission impliquant son service d'administrateur de système virtuel (VSA pour *Virtual System Administrator*).[37] Le service VSA de Kaseya a été compromis par REvil, aussi appelé Sodinokibi, qui est un groupe de cybercriminels russes à l'origine du rançongiciel comme service portant le même nom. Un VSA est un système par lequel les FSG administrent les réseaux de leurs clients. En tant qu'outil administratif, le VSA doit, pour fonctionner, détenir des privilèges administratifs à l'intérieur des réseaux d'un client. Le groupe REvil a compromis les serveurs VSA vulnérables qui étaient hébergés par des FSG en tirant parti de plusieurs exploits du jour zéro.

La figure 5 illustre la chaîne de destruction de la compromission Kaseya VSA. L'auteur de menace a développé ou acheté des exploits spécialisés pour tirer profit des vulnérabilités du jour zéro découvertes dans le logiciel Kaseya VSA. Le premier accès de l'auteur de

Figure 5 : Analyse de la chaîne de destruction de Kaseya



menace aux environnements des FSG s'est fait par un exploit du jour zéro d'authentification, suivi par l'exploitation d'un ajout de type jour zéro pour téléverser le maliciel et exécuter le code malveillant. La charge utile a été distribuée aux clients des FSG par une mise à jour compromise imitant un correctif d'urgence. Après avoir attendu jusqu'à une heure précise, la charge utile du rançongiciel a été déployée simultanément dans l'ensemble des environnements des clients, ce qui a permis le chiffrement des données et le verrouillage des systèmes.

La compromission du service Kaseya VSA a non seulement touché les FSG qui utilisent le logiciel Kaseya, mais aussi tous les clients de chacun des FSG. La compromission a infecté près de 60 FSG et touché environ 1 500 clients en aval de partout en Amérique du Nord, en Europe, en Australie et en Nouvelle-Zélande. Les organisations en aval touchées par la compromission comprenaient notamment des écoles publiques en Nouvelle-Zélande et des pharmacies en Suède.[38]

Le groupe REvil a demandé 70 millions de dollars américains pour un déchiffreur universel. Cette demande a été publiée sur le site Web clandestin du groupe, nommé « Happy Blog », où il diffuse des demandes de rançon, ou publie ou vend aux enchères les données des victimes.[39] Ce qui différencie la compromission de Kaseya des précédentes attaques par rançongiciel menées par des cybercriminels est l'utilisation de vulnérabilités du jour zéro, la sophistication de l'attaque et le nombre élevé d'organisations touchées.

Conclusion

Les chaînes d'approvisionnement étant de plus en plus numériques et réparties à l'échelle mondiale, les auteurs de menace ont des occasions accrues de cerner les faiblesses et d'exploiter la confiance établie entre les organisations. Le risque d'activité de cybermenace provenant des chaînes d'approvisionnement doit être géré tout au long du cycle de vie des produits ou des services, et ce, dès la conception et la production et jusqu'au déploiement et à la mise hors service. Les organisations doivent maintenir un solide programme d'intégrité de la chaîne d'approvisionnement et veiller à ce que leurs fournisseurs respectent l'intégrité de la chaîne d'approvisionnement et les pratiques exemplaires en matière de sécurité. Dans le cadre de cette évaluation, nous avons mis en lumière les raisons qui font que les chaînes d'approvisionnement sont des cibles intéressantes pour les auteurs de menace et décrit les techniques les plus courantes visant à compromettre les chaînes d'approvisionnements. Nous avons également établi les motivations des cybercriminels et des auteurs de menace parrainés par un État, de même que leur capacité relative à compromettre des chaînes d'approvisionnement.

Un grand nombre de cybermenaces peuvent être atténuées grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de cybersécurité et de continuité des activités. Les cybermenaces continuent d'être fructueuses à ce jour puisqu'elles n'exploitent pas uniquement les vulnérabilités technologiques, mais également les habitudes sociales et comportements humains profondément ancrés. Pour défendre le Canada contre les cybermenaces et les opérations d'influence connexes, il faut se pencher sur les aspects techniques et sociaux des activités de cybermenace. Des investissements en cybersécurité permettront aux Canadiens de bénéficier de nouvelles technologies tout en s'assurant de ne pas exposer indûment à des risques la sécurité, la vie privée, la prospérité économique et la sécurité nationale.

Le Centre pour la cybersécurité s'est engagé à faire avancer la cybersécurité et à accroître la confiance des Canadiens dans les systèmes qu'ils utilisent au quotidien, en soutenant les infrastructures essentielles ainsi que d'autres systèmes qui sont importants pour le Canada. Notre approche collaborative en matière de sécurité permet de combiner l'expertise du gouvernement, du secteur privé et du milieu universitaire. En travaillant ensemble, nous rendrons le Canada plus fort et plus résilient face aux cybermenaces. Les investissements en cybersécurité permettront aux exploitants de biens de technologies opérationnelles de profiter des possibilités qu'offrent les nouvelles technologies tout en évitant des risques inutiles pour que les Canadiens puissent compter sur des services essentiels sûrs et fiables.

Consultez les ressources en ligne ci-dessous pour obtenir de l'information supplémentaire ainsi que des avis et conseils utiles :

Détection et atténuation des menaces :

- La cybersécurité et la chaîne d'approvisionnement : évaluation des risques - ITSAP.10.070
- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)
- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Protéger votre organisation contre les menaces de la chaîne d'approvisionnement des logiciels – ITSM.10.071
- Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. National Institute for Standards and Technology. 2022
- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev, 2). National Institute for Standards and Technology. 2018
- Best Practices in Cyber Supply Chain Risk Management. National Institute for Standards and Technology. 2021
- Security and resilience – Security management systems (ISO 28000:2022). International Standards Organization. 2022
- Cybersecurity – Supplier relationships (ISO 27036:2021). International Standards Organization. 2021

Évaluation des menaces :

- Évaluation des cybermenaces nationales 2023-24
- Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles
- Bulletin sur les cybermenaces : La menace des rançongiciels en 2021

Planification :

- Principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada
- Guide sur les rançongiciels (ITSM.00.099)

NOTES DE FIN DE TEXTE

[1] Joe Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, et Matthew Fallon. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1) (en anglais seulement), National Institute of Standards and Technology, mai 2022.

[2] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles, 29 juin 2021, p. 9.

[3] GATLAN, Sergio. REvil gang tries to extort Apple, threatens to sell stolen blueprints (en anglais seulement), Bleeping Computer, 20 avril 2021.

[4] NIST. CVE-2021-30116 Detail (en anglais seulement), 25 mars 2022.

[5] NIST. CVE-2021-30120 Detail (en anglais seulement), 1 mars 2022.

[6] ANDERSSON, Alexander. How the Kaseya VSA Zero-Day Exploit Worked (en anglais seulement), TrueSec, 6 juillet 2021; OLENICK, Doug. List of Victims of Kaseya Ransomware Attack Grows (en anglais seulement), Bank Info Security, 8 juillet 2021.

[7] CLANCY, Charles, Joe FERRARO, Robert A. MARTIN, Adam G. PENNINGTON, Cristopher L. SLEDJESKI, et Craig J WIENER. Deliver Uncompromised, Securing Critical Software Supply Chains (en anglais seulement), Mitre, janvier 2021, p. 1; ODNI. Software Supply Chain Attack Graphic (en anglais seulement), 2017.

[8] Centre canadien pour la cybersécurité. Voir Alerte – Exploitation active de vulnérabilités liées à Microsoft Exchange, 2 mars 2021.

[9] Centre canadien pour la cybersécurité. Voir Alerte – Exploitation active de la vulnérabilité Apache Log4j, 10 décembre 2021.

[10] HERR, Trey, William LOOMIS, Stewart SCOTT, et June LEE. Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain (en anglais seulement), Atlantic Council, juillet 2020, p. 20.

[11] AYUKAWA, Michael, Mohammed AL-SANABANI et Adefemi DEBO-OMIDOKUN. How Firms Relate to Open Source Communities (en anglais seulement), Technology Innovation Management Review, janvier 2011; JOSHUA, J.V., D.O. ALAO, S.O. OKOLIE et O. AWODELE. Software Ecosystem: Features, Benefits and Challenges (en anglais seulement), International Journal of Advanced Computer Science and Applications 4, 8 (2013): 242-247.

[12] SEALS, Tara. Octopus Scanner Sinks Tentacles into GitHub Repositories (en anglais seulement), ThreatPost, 2 juin 2020.

[13] MUNOZ, Alvaro. The Octopus Scanner Malware: Attacking the open source supply chain (en anglais seulement), GitHub Security Lab, 28 mai 2020.

[14] ZETTER, Kim. Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers (en anglais seulement), Vice, 25 mars 2019.

[15] SecureList. Operation ShadowHammer: a high-profile supply chain attack (en anglais seulement), 23 avril 2019.

[16] KHANDELWAL, Swati. CCleaner Attack Timeline – Here's How Hackers Infected 2.3 Million PCs (en anglais seulement), The Hacker News, 18 avril 2018.

[17] HAY NEWMAN, Lily. Inside the Unnerving Supply Chain Attack that Corrupted CCleaner (en anglais seulement), Wired, 17 avril 2018.

[18] Schneider Electric. Security Notification – USB Removable Media Provided with Conext Combox and Context Battery Monitor (en anglais seulement), 24 août 2018.

[19] Roman Zakharov v Russia [GC] (en anglais seulement), European Court of Human Rights Judgement 4.12.2015 [GC], 25 décembre.

[20] SHERMAN, Justin. Reassessing RuNet: Russian internet isolation and implications for Russian cyber behaviour (en anglais seulement), Atlantic Council, 12 juillet 2021.

[21] MEYERS, John. A Recent Chinese Hack Is a Wake-up Call for the Security of the World's Software Supply Chain (en anglais seulement), The Diplomat, 7 septembre, 2022.

[22] CHESNEY, Robert. Cybersecurity Law, Policy, and Institutions (Public Law Research Paper No. 716, 2021) (en anglais seulement), University of Texas, 23 août 2021, p. 6.

[23] MANDIA, Kevin. Global Intrusion Campaign Leverages Software Supply Chain Compromise (en anglais seulement), FireEye Stories Blog, 13 décembre 2020.

[24] White House Briefing Room. FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government (en anglais seulement), 15 avril 2021; GAC. Déclaration sur la cybercompromission de SolarWinds, 15 avril 2021.

[25] CHESNEY, Robert. Cybersecurity Law, Policy, and Institutions (Public Law Research Paper No. 716, 2021) (en anglais seulement), University of Texas, 23 août 2021, p. 4-6.

[26] Lockheed Martin. Gaining the Advantage: Apply Cyber Kill Chain Methodology to Network Defences (en anglais seulement), 2015.

[27] TURTON, William. List of Hacked Organizations Tops 200 in SolarWinds Case (en anglais seulement), Government Technology, 21 décembre 2020.

[28] PERLROTH, Nicole. Microsoft Says Russian Hackers Viewed Some of its Source Code (en anglais seulement), The New York Times, 31 décembre 2020.

[29] JIBILIAN, Isabella et Katie CANALES. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal (en anglais seulement), Business Insider, 15 avril 2021.

[30] GALLAGHER, Ryan. SolarWinds Adviser Warned of Lax Security Years Before Hack (en anglais seulement), Bloomberg, 21 décembre 2020; RATNAM, Gopal. Cleaning up SolarWinds hack may cost as much as $100 billion (en anglais seulement), Roll Call, 11 janvier 2021.

[31] LAKSHMANAN, Ravie. Microsoft Warns of Continued Supply-Chain Attacks by the Nobelium Hacker Group (en anglais seulement), The Hacker News, 25 octobre 2021.

[32] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : La menace des rançongiciels en 2021, 9 décembre 2021.

[33] CHEN, Jay. Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub (en anglais seulement), PaloAlto, 16 octobre 2019.

[34] NAKASHIMA, Ellen et Jay GREENE. Hospitals being hit in coordinated, targeted ransomware attack from Russian-speaking criminals (en anglais seulement), The Washington Post, 29 octobre 2020.

[35] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2020, 2020, p. 17; Cryptojacking (en anglais seulement), Interpol, septembre 2020.

[36] SASSON, Aviv. 20 million miners: finding malicious cryptojacking images in docker hub (en anglais seulement), PaloAlto, 26 mars 2021.

[37] Kaseya. Important Notice (en anglais seulement), 4 août 2021.

[38] Malwarebytes Labs. Kaseya hijacked, thousands attacked by REvil, fix delayed again (en anglais seulement), 7 juillet 2021.

[39] ILASCU, Ionut. REvil ransomware asks $70 million to decrypt all Kaseya attack victims (en anglais seulement), Bleeping Computer, 5 juillet 2021; IKEDA, Scott. Revil Ransomware Group Missing from Dark Web; Temporary Vacation, or Permanently Out of Business? (en anglais seulement), CPO Magazine, 16 juillet 2021.

CAT. D96-93/2022F-PDF
ISBN 978-0-660-46247-9