Alerte destinée aux clients : Avis de sécurité urgent – Atteinte à la sécurité du logiciel Orion[MD] de Solar Winds[MD]

*À partir du mardi 8 décembre et jusque dans l'après-midi du 14 décembre, les services de nouvelles ont signalé plusieurs incidents de cybersécurité importants, notamment ceux qui ont visé une entreprise de cybersécurité et d'autres organisations et institutions comme les départements de la Sécurité intérieure, du Trésor et du Commerce des États-Unis[1]. **Au fil des développements, il est apparu évident que tous les incidents semblaient partager un vecteur d'attaque commun : la compromission réussie de la chaîne d'approvisionnement d'un outil de sécurité mis au point et distribué par la société d'informatique SolarWinds, basée à Austin, au Texas[2].***

Aperçu. Bien que la situation continue d'évoluer, voici ce que l'on sait jusqu'à présent selon les avis du gouvernement, les communiqués de presse de SolarWinds et les rapports provenant des milieux du renseignement :

- L'attaque ayant visé SolarWinds est apparemment une attaque ciblée de la chaîne d'approvisionnement attribuée à des auteurs de menace parrainés par un État-nation étranger. Les attaquants ont intégré du code malveillant dans le produit Orion de SolarWinds avant qu'il ne soit distribué aux clients. Tout client ayant installé une version d'Orion touchée est ainsi devenu vulnérable au déploiement du code malveillant intégré.
- Les auteurs de la menace ont troyennisé les mises à jour des logiciels d'entreprise Orion de SolarWinds afin de distribuer des logiciels malveillants aux utilisateurs finaux de sociétés et d'autres entreprises.
- Les logiciels touchés sont ceux de la plateforme Orion[MD] de SolarWinds[MD] versions **2019.4 HF 5** et **2020.2 *sans correctif d'urgence installé*** ou **2020.2 HF 1**. (Source : SolarWinds Security Advisory, mis à jour le 15 décembre 2020 à 8 h HC.)
- Les entreprises, les organisations à but non lucratif et d'autres types d'organisations partout dans le monde ayant utilisé le logiciel SolarWinds concerné sont à risque, car le logiciel pourrait éventuellement permettre aux auteurs de la menace d'accéder à leurs réseaux et de compromettre les justificatifs d'identité.
- Selon les rapports, après avoir compromis les justificatifs d'identité, l'auteur de la menace semble tirer parti de plusieurs techniques au sein d'un environnement d'utilisateur final pour éviter d'être détecté et occulter ses activités[3]. Chaque attaque semble également avoir été personnalisée, adaptant les noms des hôtes malveillants pour qu'ils correspondent aux conventions de désignation au sein de l'environnement de la cible.
- D'autres rapports indiquent qu'il s'agit d'une campagne d'envergure, qui touche des organisations publiques et privées partout dans le monde[4].
- Cette campagne, qui est toujours en cours, pourrait avoir commencé dès le printemps 2020.

Êtes-vous touché? Selon l'avis de sécurité de SolarWinds mis à jour le 15 décembre 2020, si les versions **2019.4 HF 5** et **2020.2 *sans correctif d'urgence*** ou **2020.2 HF 1** de la plateforme Orion ont été installées dans votre environnement (voir la liste des produits concernés sous « Known affected products » sur le site Web de SolarWinds), votre réseau est possiblement affecté par la présence du code malveillant et peut ensuite avoir été compromis par les auteurs de la menace.

Selon les observations, les auteurs de la menace par l'État-nation étranger ont utilisé le logiciel compromis pour établir une emprise initiale dans le réseau. Après avoir obtenu l'accès au réseau, l'auteur de la menace peut remonter la hiérarchie jusqu'à ce qu'il obtienne les droits d'accès administratifs généraux. L'auteur de la menace peut utiliser les droits d'accès administratifs généraux pour se faire passer pour n'importe quel utilisateur, y compris les utilisateurs administratifs, sur le réseau. Une fois que l'auteur de la menace a réussi à obtenir ce niveau de contrôle et d'autorité sur un réseau, il peut circuler au sein du réseau de l'entreprise, y compris vers l'infrastructure infonuagique si le réseau s'étend jusqu'à cet espace.

Que devriez-vous faire? Si vous avez actuellement ou avez déjà eu une version troyennisée de la plateforme Orion de SolarWinds dans votre infrastructure, Stroz Friedberg vous conseille d'adopter une approche fondée sur les risques pour gérer la situation. Les mesures suivantes sont à envisager et à prendre :

1. Installer le correctif de mise à jour de SolarWinds. Cependant, même si le correctif de SolarWinds est une composante essentielle du processus, le travail nécessaire n'est pas terminé. En « réparant » le point d'entrée initial sans procéder à une enquête pour comprendre la portée de l'incident, vous laissez votre organisation dans l'ignorance en ce qui a trait à ses répercussions. Étant donné le niveau élevé de sophistication du groupe de cybermenace associé à cette attaque complexe, il est recommandé d'adopter une approche fondée sur les risques pour gérer cette situation.

2. Travailler avec une équipe d'intervention en cas d'incident pour évaluer votre situation particulière. Il n'y a pas de solution unique pouvant convenir aux clients qui proviennent de divers secteurs et ont différentes ressources internes pour appliquer des mesures correctives et enquêter, différents profils de menace par un État-nation, et différents niveaux d'expérience dans la gestion des incidents, des menaces et des risques.

3. Effectuer une chasse aux menaces et une évaluation des compromissions, y compris, sans s'y limiter, une recherche des indicateurs de compromission connus associés à ce code malveillant et à cette attaque.

4. Prendre immédiatement des mesures correctives lorsque des indicateurs de compromission ou des codes malveillants sont découverts.

5. Surveiller la sécurité en tout temps et avec diligence, mais particulièrement jusqu'à ce que tous les correctifs et toutes les mises à jour aient été distribués (certains sont encore à venir), et jusqu'à ce qu'une évaluation des compromissions ait été effectuée.

6. Continuer de surveiller la situation et les nouveaux développements, notamment les nouveaux indicateurs de compromission publiés et les nouveaux correctifs de SolarWinds.

Voici plusieurs ressources à envisager :

Le Centre de réponse aux problèmes de sécurité de Microsoft – cette ressource fournit des détails techniques, incluant les méthodes mises à profit par l'auteur présumé des cyberattaques récentes par un État-nation, afin de permettre à l'ensemble de la communauté de la sécurité de traquer les activités dans ses réseaux et de contribuer à une défense commune contre cet auteur de menace sophistiqué.

- **https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/**

Département de la Sécurité intérieure des États-Unis – le département de la Sécurité intérieure a publié l'injonction 21-01 en réponse à cet incident.

- **https://cyber.dhs.gov/ed/21-01/**
- Prendre note de l'exigence du département qui consiste à « prendre une image judiciaire de la mémoire système et/ou des systèmes d'exploitation qui hébergent toutes les instances de la plateforme Orion de SolarWinds » pour les versions touchées. Il s'agit d'une étape importante pour assurer la préservation des artéfacts utiles à l'enquête ultérieure qui permettra de déterminer les répercussions éventuelles de la compromission.

SolarWinds – SolarWinds conseille à ses clients ayant des produits qui figurent dans la liste des logiciels touchés pour la **plateforme Orion v2020.2** ***sans correctif d'urgence*** ou **2020.2 HF 1** d'effectuer dès que possible la mise à niveau à la version **2020.2.1 HF 1** de la plateforme Orion « pour assurer la sécurité de [leur] environnement ». Cette version est actuellement offerte à l'adresse customerportal.solarwinds.com. SolarWinds demande également à ses clients ayant des produits qui figurent dans la liste des logiciels touchés pour la **plateforme Orion v2019.4 HF 5** d'effectuer la mise à jour à la version **2019.4 HF 6,** qui est également offerte à l'adresse customerportal.solarwinds.com. Vous pouvez consulter l'avis de sécurité de SolarWinds à l'adresse **https://www.solarwinds.com/securityadvisory**.

Selon SolarWinds, les entreprises qui ne peuvent effectuer immédiatement la mise à niveau doivent protéger leur instance de la plateforme Orion en suivant les directives figurant sur le site Web de SolarWinds à l'adresse : **https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm**. Les principales mesures d'atténuation consistent à protéger votre plateforme Orion au moyen de pare-feu, à désactiver l'accès Internet pour la plateforme Orion, et à limiter les ports et les connexions uniquement à ce qui est nécessaire.

Solutions de risques cybernétiques d'Aon continue de suivre de près l'évolution de la situation. Nous communiquerons d'autres détails au fur et à mesure qu'ils se présenteront.

Personnes-ressources :

John Ansbach
Vice-président
214.377.4566
john.ansbach@strozfriedberg.com

Heidi Wachs
Vice-présidente
202.464.5813
heidi.wachs@strozfriedberg.com

Cheri D. Carr
Directrice générale et RSSI, Solutions de risques cybernétiques
469.866.2478
cheri.carr@strozfriedberg.com

Jonathan Rajewski
Vice-président
802.238-8530
jonathan.rajewski@strozfriedberg.com

Sources

1. Sources : ZDNet, « FireEye, one of the world's largest security firms, discloses security breach », 8 décembre 2020; *Washington Post*, « DHS, State and NIH join list of federal agencies – now five – hacked in major Russian cyberespionage campaign », 14 décembre 2020.
2. Source : *Wall Street Journal*, « Suspected Russian Cyberattack Began With Ubiquitous Software Company », 15 décembre 2020.
3. Source : FireEye, « Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor », 13 décembre 2020.
4. Source : *Newsweek*, « SolarWinds Says Hack Afected 18,000 Customers, Including Two Major Government Agencies », 14 décembre 2020.

À propos de Solutions de risques cybernétiques : Solutions de risques cybernétiques d'Aon offre une approche globale de la gestion des cyberrisques, des compétences inégalées en investigation, ainsi que des technologies exclusives qui aident les clients à repérer et à quantifier les cyberrisques, à protéger les actifs essentiels et à se rétablir après des cyberincidents.

À propos d'Aon : Aon plc (NYSE : AON) est le principal fournisseur mondial d'une vaste gamme de solutions pour la gestion du risque, des régimes de retraite et des programmes de santé. Nos 50 000 employés de 120 pays génèrent des résultats pour les clients grâce à des données et à des analyses exclusives produisant des points de vue permettant de réduire la volatilité et d'améliorer le rendement.

Empower Results®