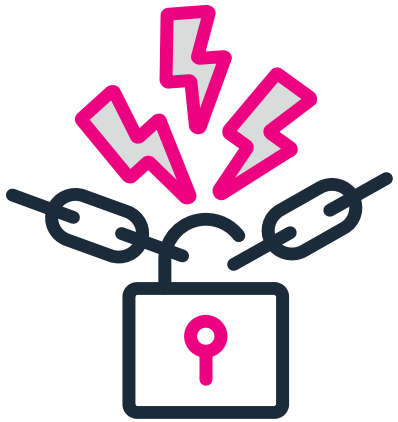
Guide de

protection contre les attaques sur la chaîne logistique

Comment une plateforme de données peut contribuer à protéger les entreprises contre des menaces telles que les attaques SolarWinds

splunk>
turn data into doing™

Une attaque sur la chaîne logistique est une puissante cyberattaque qui peut traverser les défenses de sécurité les plus sophistiquées par l'intermédiaire de fournisseurs tiers légitimes. Comme les fournisseurs ont besoin d'accéder à des données sensibles pour s'intégrer aux systèmes internes de leurs clients, les cyberattaques qui les visent exposent aussi souvent les données de leurs clients. Et comme les fournisseurs stockent les données sensibles de nombreux clients, une seule attaque sur la chaîne logistique permet à des pirates d'accéder aux données sensibles de nombreuses entreprises, dans de nombreux secteurs.



La gravité des attaques sur la chaîne logistique ne saurait être surestimée. Et la récente vague d'attaques de ce genre laisse penser que cette méthode est aujourd'hui à la mode parmi les acteurs étatiques.

Les attaques sur la chaîne logistique SolarWinds sont probablement les plus spectaculaires à ce jour en raison de leur ampleur sans précédent. Plus de 18 000 entreprises et plusieurs agences gouvernementales américaines ont été touchées, et il faudra des mois avant que l'on ne connaisse le véritable bilan de ces attaques.

Les attaques SolarWinds ne sont qu'un exemple parmi d'autres de la raison pour laquelle les entreprises doivent hiérarchiser leurs initiatives de sécurité de manière à détecter et à se défendre contre ces menaces, car il est clair que la probabilité d'autres attaques à grande échelle ne fera qu'augmenter.

Comment fonctionne une attaque sur la chaîne logistique

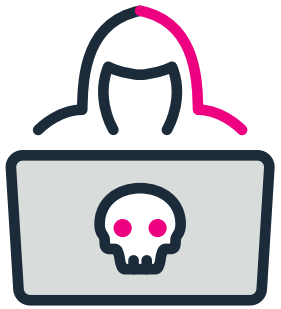
Une attaque sur la chaîne logistique utilise des processus légitimes et fiables pour obtenir un accès complet aux données des entreprises en ciblant le code source du logiciel, les mises à jour ou les processus de compilation d'un fournisseur. Les attaques sur la chaîne logistique sont difficiles à détecter car elles se produisent en décalage par rapport à la surface d'attaque.

Les fournisseurs compromis transmettent alors involontairement des programmes malveillants au réseau de leurs clients. Les victimes peuvent être atteintes par le biais de mises à jour de logiciels tiers, d'installeurs d'applications ou de programmes malveillants présents sur des appareils connectés. Une mise à jour logicielle peut infecter des milliers d'entreprises avec un minimum d'efforts de la part des pirates, qui disposent désormais d'un accès « légitime » pour se déplacer latéralement dans leurs réseaux.

Voyons en détail le fonctionnement de ces attaques : après s'être faufilé à travers les défenses de sécurité du fournisseur, souvent à l'aide de plusieurs vecteurs d'attaque, le code malveillant s'incorpore à un processus signé numériquement de son hôte.

La signature numérique confirme l'authenticité du logiciel et permet sa transmission. Ainsi dissimulé, le code malveillant est alors libre de parcourir le trafic qui circule entre le fournisseur et son réseau client. Le malware contient une backdoor qui communique avec tous les serveurs tiers, et c'est de cette manière qu'il est distribué. Une seule mise à jour logicielle d'un fournisseur compromis peut pénétrer des milliers d'entreprises : dans le cas de l'attaque SolarWinds, elles étaient de plus de 18 000 à être concernées.

Une seule mise à jour logicielle d'un fournisseur compromis peut pénétrer des milliers d'entreprises : dans le cas de l'attaque SolarWinds, elles étaient de plus de **18 000** à être concernées.



Déroulement des attaques SolarWinds

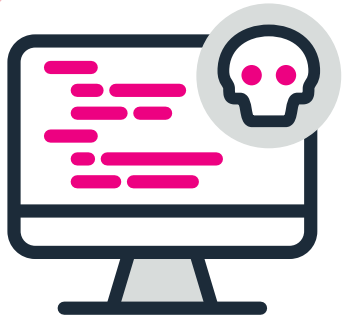
Les attaques SolarWinds incarnent un excellent exemple de l'ampleur des dommages qu'une attaque sur la chaîne logistique peut infliger. Des acteurs étatiques sophistiqués ont compromis le logiciel de SolarWinds et lui ont incorporé un programme malveillant.

Le logiciel malveillant a échappé à toute détection en masquant son trafic réseau sous un protocole autorisé et en stockant les résultats de ses opérations de reconnaissance dans des fichiers légitimes. Une fois intégré, le code malveillant a été déployé via une mise à jour du produit SolarWinds Orion, donnant aux malfaiteurs un accès direct au réseau de tous les clients de la solution.

L'investigation sur cet assaut se poursuit, mais deux malwares menaçants distincts ont déjà été identifiés : Sunburst et Supernova, qui peuvent provenir de deux acteurs différents.

SolarWinds est utilisé par plus de 30 000 entreprises comme outil de supervision du réseau, et jusqu'à 18 000 de ces clients ont installé des mises à jour qui les ont rendus vulnérables face aux pirates Parmi les victimes confirmées, on compte des membres du Fortune 500 et plusieurs agences du gouvernement américain, dont le Pentagone, le département de la Sécurité intérieure, le département d'État, le département de l'Énergie, l'Administration nationale de sûreté nucléaire (NNSA) et le département du Trésor. L'étendue réelle des dommages n'est pas encore connue, mais certains experts considèrent déjà l'événement comme l'une des pires séries d'attaques de cybersécurité de l'histoire.

Splunk entre en jeu



Pour garder une longueur d'avance sur les attaques sur la chaîne logistique, les entreprises doivent moderniser leurs programmes de sécurité dans les environnements hybrides et multicloud. Plus précisément, les équipes de sécurité doivent normaliser, gérer et acquérir une visibilité sur des sources de données et des applicatifs stratégiques et disparates afin d'identifier les menaces potentielles et mener des investigations et des analyses en quasi-temps réel.

La plateforme Data-to-Everything™ de Splunk permet aux entreprises d'obtenir des informations sur leurs données, où qu'elles se trouvent, afin de mieux se protéger contre les menaces et les vulnérabilités de sécurité.

La plateforme protège les entreprises contre les attaques sur la chaîne logistique en détectant les menaces, en recouvrant une visibilité sur toute l'infrastructure IT et en protégeant les clients, les applications et les ressources de développement.

Sécuriser les affaires

La plateforme Splunk permet aux entreprises de détecter les attaques sur la chaîne logistique comparables aux attaques SolarWinds, de s'en protéger et d'y répondre, en important facilement des indicateurs de menace pour les rechercher dans leur environnement.

La plateforme aide également les professionnels de la sécurité à examiner et à mettre à jour les types de logs importés dans Splunk, ce qui permet de réaliser une analyse des systèmes de noms de domaine (DNS) et des logs de trafic réseau et hôte pour détecter toute trace d'activité de programmes malveillants. Les équipes de sécurité peuvent également examiner les résultats des analyses de vulnérabilité, les hashes et les logs de proxy pour rechercher des preuves d'attaques par webshell (comme dans le cas de Supernova, l'une des attaques SolarWinds).

Il est aussi utile de détecter les activités inhabituelles auprès des fournisseurs d'annuaire et d'authentification pour obtenir des indications d'un deuxième assaut après une attaque sur la chaîne logistique. Les mêmes données peuvent également être utilisées pour rechercher d'autres signes de mouvement latéral à partir d'hôtes compromis.

Regagnez une visibilité sur l'IT

L'une des nombreuses raisons expliquant les effets dévastateurs des attaques SolarWinds a été la perte de visibilité des clients sur leur infrastructure IT suite à la violation. Heureusement, la plateforme Splunk aide les entreprises à recouvrer cette visibilité et à superviser l'état et les opérations de leur pile IT. Cela leur permet d'améliorer leurs services, d'éviter les interruptions de service et d'accélérer la résolution des problèmes.

Protégez vos clients, vos applications et vos ressources de développement

La vélocité des applications augmente constamment, et les entreprises doivent réévaluer leur structure organisationnelle et la façon dont elles créent de la visibilité sur l'ensemble de leur chaîne de livraison de logiciels. Pourquoi ? Parce qu'elle réduit le délai moyen de rentabilité pour les clients, l'augmentation de la vitesse de livraison a également pour effet d'augmenter les vecteurs d'attaque et d'étendre les surfaces exploitables par les pirates.

C'est là qu'intervient le modèle DevSecOps : l'intégration des pratiques de sécurité tout au long du cycle de vie du développement logiciel (SDLC) pour garantir la commercialisation de services sécurisés. Avec la mise en œuvre des pratiques DevSecOps, il est possible de sécuriser à la fois la chaîne de livraison de services et le logiciel qui y est fourni. Pour atteindre son but, la pratique DevSecOps doit être observable, être éclairée par des informations exploitables et complétées par des capacités de réponse aux incidents.

En apportant de la visibilité aux analyses de vulnérabilité, la plateforme Splunk aide les entreprises à mesurer la couverture, l'efficacité et l'activité de leurs processus d'analyse, pour mieux sécuriser les applications. Les visualisations aident aussi les organisations à établir des KPI et des mesures inter-équipes pour mesurer le succès et les performances des pratiques DevSecOps.

Splunk contribue en outre à protéger les chaînes logistiques en sécurisant l'accès aux chaînes d'outils et en supervisant, en identifiant et en signalant les activités et accès suspects dans les environnements de développement et de test d'une entreprise. La plateforme appuie aussi la résilience de l'infrastructure SDLC stratégique d'une entreprise, notamment l'approche CI/CD, la gestion des secrets, les dépôts de code et la gestion des artefacts. Elle peut être utilisée pour sécuriser les applications de production en activant des vérifications continues, en signalant par des alertes les nouvelles vulnérabilités en production et en déclenchant leur correction avant qu'elles ne puissent être exploitées.

En savoir plus.

Vous voulez en savoir plus sur la plateforme Data-to-Everything de Splunk qui peut vous aider à garder une longueur d'avance sur les attaques sur la chaîne logistique ?

En savoir plus

21-17322-SPLK-AGuidetoProtectingAgainstSupplyChainAttacks-EB-108

splunk> turn data into doing™