La supply chain en ligne de mire : cinq mesures pour déjouer la prochaine grande cyberattaque

Si vous pensez que les attaques comme SolarWinds sont derrière nous, vous pourriez en faire les frais

En moins d'un an, les entreprises du monde entier ont été victimes de multiples attaques de grande ampleur, notamment des exploits de Microsoft Exchange Server, des attaques par ransomware sur Kaseya VSA et une myriade d'autres rançongiciels. À l'heure où les cours des cryptomonnaies battent des records, des groupes d'attaque comme REvil (impliqué dans l'attaque sur Kaseya VSA) n'hésitent pas à lancer des campagnes de ransomware pour attaquer et infecter un champ toujours plus large de cibles secondaires. Alors que les cyberattaques se succèdent sans discontinuer, c'est maintenant que les entreprises doivent tout mettre en œuvre pour protéger leur réseau.

Dans ce livre blanc, vous trouverez des conseils et des recommandations pour réduire les vulnérabilités et l'exposition de vos environnements d'entreprise aux menaces, mais aussi protéger votre supply chain.

Introduction

La transformation numérique a incité les entreprises à faire appel à d'innombrables fournisseurs logiciels et technologiques, développant ainsi une vaste supply chain destinée à libérer le potentiel des nouvelles technologies pour accroître leur productivité et améliorer leur efficacité à grande échelle. Les failles de cet écosystème n'ont pas échappé aux attaquants, toujours plus nombreux à cibler la supply chain logicielle afin d'exploiter la confiance intrinsèque des entreprises dans leurs fournisseurs et leurs éditeurs, confiance qui se reflète dans les accès réseau qu'elles octroient à ces derniers. Une fois munis de ce sésame, les attaquants peuvent même compromettre le processus de signature par certificats numériques d'un fournisseur pour contourner les systèmes de défense de leur victime.

Au risque d'attaque sur la supply chain logicielle viennent s'ajouter les problématiques actuelles des équipes de sécurité, y compris un flux interminable d'alertes décousues, dépourvues de tout contexte nécessaire pour déterminer les mesures à prendre. Pour pouvoir traquer efficacement les comportements malveillants, même lorsqu'ils émanent d'un fournisseur authentifié ou de confiance, les entreprises doivent impérativement adopter des outils de détection et de réponse qui intègrent des fonctionnalités de machine learning.

Par ailleurs, la redéfinition de l'architecture réseau autour du principe de Zero Trust peut permettre de migrer d'un modèle de sécurité périmétrique traditionnel vers une démarche de vérification permanente des identités et droits d'accès.

Le temps des remises en question face à des attaquants plus habiles que jamais

En mars 2020, SolarWinds a envoyé une mise à jour logicielle standard contenant du code piraté à ses 33 000 clients Orion®. Au final, 18 000 l'ont installée, avec pour conséquence la compromission d'un large éventail d'entités publiques et privées. Parmi elles figurent une partie du Pentagone, les ministères de l'Intérieur, des Finances, de l'Énergie et des Affaires étrangères, et l'agence chargée de la sécurité nucléaire aux États-Unis, ainsi que plusieurs fournisseurs de solutions de cybersécurité. Il va sans dire que l'onde de choc continue de se faire sentir, à mesure que les entreprises et les acteurs publics poursuivent leur minutieux travail d'analyse forensique.

Ces attaques récentes sur SolarWinds ont montré l'ampleur que peut prendre une attaque avancée sur la supply chain. Compte tenu de l'omniprésence des logiciels et serveurs SolarWinds dans ces organisations pour gérer les réseaux, les systèmes et les infrastructures IT, les attaquants ont bénéficié d'un niveau d'accès sans précédent. Tout le monde s'accorde à dire que l'attaque est passée inaperçue pendant environ 10 mois.

SolarWinds a fini par admettre qu'un attaquant était parvenu à intégrer du code malveillant à une mise à jour logicielle dûment signée. Une fois cette mise à jour installée, le code malveillant s'est montré extrêmement discret. Ce malware nommé SUNBURST restait en effet inactif pendant environ deux semaines avant d'entrer en contact avec un sous-domaine de avsvmcloud[.]com, le serveur de commande et contrôle (CnC) pour le backdoor, dont il obtenait d'autres instructions et d'autres payloads à exécuter. Aux États-Unis, de grandes entreprises et agences gouvernementales ont identifié SUNBURST sur leurs serveurs en production, avec pour conséquence la compromission et l'exposition de données hautement confidentielles.

Il est étonnant que les attaquants aient pu maintenir leur présence sur une période aussi longue, compromettant au passage des organisations connexes alors même que la plupart de leur trafic n'éveillait aucun soupçon. Pour preuve, la totalité des 72 outils de détection des malwares utilisés ont considéré le domaine avsvmcloud[.]com comme inoffensif.

Compte tenu du rôle pivot de SolarWinds dans l'automatisation IT, les attaquants ont pu exploiter la connectivité et le positionnement stratégique de cette solution pour accéder au reste de l'environnement des clients. Pour cela, ils compromettaient l'infrastructure SAML dont les certificats leur permettaient ensuite de se déplacer latéralement et d'accéder à des données sensibles dans la messagerie électronique. Si la menace a finalement pu être détectée, c'est notamment grâce à une méthode de détection des techniques et comportements anormaux couramment associés à des malwares et kits d'exploit connus – celle-là même employée par Cortex XDR.

« Récemment, nous avons été confrontés à une tentative de téléchargement de Cobalt Strike sur l'un de nos serveurs SolarWinds. Cortex XDR a bloqué instantanément cette action grâce à notre système de protection contre les comportements suspects. Ensuite, notre SOC a isolé le serveur, enquêté sur l'incident et renforcé la sécurité de notre infrastructure. Suite à cela, nous avons également déployé une série d'IoC pour les produits Palo Alto Networks chez nos clients. »

– Nikesh Arora, PDG, Palo Alto Networks

Le 17 décembre 2020, par le biais de son PDG Nikesh Arora, Palo Alto Networks a révélé qu'en interne, une requête DNS de son serveur SolarWinds Orion avait été bloquée par Cortex XDR et son système de protection contre les comportements suspects, permettant ainsi au SOC de Palo Alto Networks d'isoler le serveur concerné et de lancer une investigation. Sa conclusion : l'attaque a échoué grâce à Cortex XDR. Ni son infrastructure ni aucune donnée n'ont été compromises.

Ce succès, Cortex XDR le doit à ses fonctions de prévention, de détection et de réponse, mais aussi à l'IA et au machine learning qui ont permis d'intégrer automatiquement les données des terminaux, des réseaux et du cloud.

À l'heure où les attaques contre la supply chain gagnent en ampleur et en fréquence, il est clair que les équipes de cybersécurité devront désormais composer avec des groupes d'attaque ciblés, disciplinés et généreusement financés par des États pour atteindre un objectif clair : s'infiltrer dans leurs cibles et s'y maintenir pour accomplir diverses missions, notamment subtiliser des données. La neutralisation de ces types de campagnes sophistiquées passera par de nouvelles approches et technologies capables de vous donner un coup d'avance sur des attaquants toujours plus déterminés, dont les assauts dopés au cloud et à l'automatisation ne feront qu'une bouchée des technologies et pratiques de gestion du risque traditionnelles.

Le temps presse : préparez-vous au prochain SolarWinds

Même avant cette attaque, il était clair qu'un grand nombre de centres opérationnels de sécurité (SOC) étaient encore trop dépendants des interventions humaines et d'une série de produits de sécurité fonctionnant en vase clos. Déjà sous pression, les analystes peinaient à traiter toutes les alertes générées par la multitude de produits déployés par leurs équipes. Au moindre soupçon d'attaque, la plupart doivent encore examiner manuellement les alertes, sachant qu'ils en reçoivent des dizaines de milliers chaque semaine, en provenance de dizaines de produits de sécurité qui réclament leur attention. La réponse et les investigations manuelles prennent souvent beaucoup trop de temps. Il faut collecter des données contextuelles (sur le terminal, l'utilisateur et l'heure des activités suspectes) et conduire une analyse d'incident (évènements associés sur le nom d'hôte, l'adresse IP, le trafic, le domaine, l'application utilisée, etc.), ce qui n'engendre finalement que des évaluations incomplètes et un manque d'efficacité.

D'après une enquête menée en 2019 auprès de RSSI, « plus de 41 % des sondés reçoivent plus de 10 000 alertes par jour et certains en reçoivent même plus de 500 000 ».

Ce même rapport révèle que seuls 24 % des alertes faisant l'objet d'une investigation se révèlent légitimes, contre 34 % en 2018. Il fait également état d'une chute du nombre d'alertes légitimes ayant fait l'objet d'une remédiation – de 51 % en 2018 à 43 % en 2019[1].

Quant aux antivirus, systèmes de détection et de réponse sur les terminaux (EDR) et autres solutions de sécurité d'ancienne génération encore en activité dans de nombreuses organisations, ils ne font qu'amplifier le risque. Face à l'avalanche de données de mauvaise qualité, de nombreux analystes dérèglent les capteurs ou se contentent d'ignorer certaines alertes, ce qui augmente incontestablement leur degré d'exposition. Faute de contexte, beaucoup d'alertes sont classées comme faux positifs, car elles n'apportent pas suffisamment d'éclairages pour justifier une investigation. Pourtant, en les recoupant avec d'autres sources de données, elles pourront permettre de comprendre l'intention malveillante derrière une activité bénigne en apparence.

En somme, l'avenir des opérations de sécurité dépend du remplacement des outils de sécurité traditionnels en silos par des solutions intégrées, dotées de fonctions d'analyse, de machine learning et de détection automatisées pour une réponse plus rapide et plus précise. Lorsque les bons outils sont intégrés à des données pertinentes et consolidées, les entreprises peuvent accélérer leur réponse et mener leurs investigations sur la base d'une vue complète et détaillée sur les incidents.

Reste donc à identifier la marche à suivre. Comment les acteurs des secteurs public et privé peuvent-ils se préparer à la prochaine attaque sur la supply chain et aux nouvelles menaces qui ne manqueront pas de planer sur elles dans un avenir proche ?

Nous vous invitons à envisager les cinq mesures qui suivent et leurs effets bénéfiques sur vos activités, de l'évaluation de votre profil de risque à l'élargissement de votre stratégie de sécurité opérationnelle.

1. *Anticipating the Unknowns*, Cisco, mars 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

1. Maîtrise de votre surface d'attaque

À l'heure où les salariés, les partenaires et les fournisseurs travaillent hors du périmètre réseau des entreprises, les données et systèmes internes sont plus susceptibles d'être exposés et attaqués. Pour réduire ce risque, les organisations peuvent recourir à des tests d'intrusion, des analyses de vulnérabilité, ou encore à une nouvelle pratique appelée gestion de la surface d'attaque (ASM, Attack Surface Management).

Tour d'horizon de la gestion de la surface d'attaque

Le SANS Technology Institute définit l'ASM comme suit :

> « Une catégorie émergente de solutions destinées à aider les organisations à résoudre cette problématique en offrant un point de vue externe sur leur surface d'attaque... La surface d'attaque d'une entreprise se compose de tous les matériels, logiciels, ressources cloud et SaaS accessibles par Internet qu'un attaquant peut détecter. Pour résumer, votre surface d'attaque correspond à toute ressource externe qu'un attaquant pourrait repérer, attaquer et exploiter pour s'infiltrer dans votre environnement[2]. »

Il liste également quelques cas d'usage courants des solutions ASM :

- Identification des angles morts externes
- Détection des ressources inconnues et du Shadow IT
- Gestion des risques sur la surface d'attaque
- Priorisation des vulnérabilités basée sur les risques
- Évaluation des risques liés aux filiales et fusions-acquisitions

Que vous choisissiez de déployer des solutions ASM ou de réaliser des tests d'intrusion ou des analyses de vulnérabilité, une chose est sûre : vous devrez identifier les exigences produits et opérationnelles (fonctionnalités, capacités, critères d'évaluation, etc.) pour trouver la meilleure option.

2. Prévention d'un maximum de menaces

Malgré l'offre pléthorique sur le marché des solutions de sécurité, les cyberattaques continuent à créer le chaos et à gagner en complexité (avec des groupe cyber semble-t-il de mieux en mieux financés).

Pourtant, force est de constater que de nombreuses attaques à fort retentissement reposaient sur des vecteurs relativement courants comme des pièces jointes infectées, des e-mails de phishing et des escalades de privilèges. D'où l'importance de mettre en place des technologies et bonnes pratiques capables de bloquer toutes ces menaces et de vous permettre de vous concentrer sur l'essentiel.

Mesures de prévention de base

- Investissez dans la sécurisation de vos terminaux. Les plateformes de protection des terminaux (EPP) reposent sur de multiples techniques de prévention, notamment les analyses statiques pour inspecter les fichiers pouvant contenir un malware, les règles heuristiques pour bloquer les exploits et les analyses comportementales pour déterminer la dangerosité d'un fichier sur la base des fonctions qu'il exécute.
- Développement, assurance qualité, production... quel que soit l'environnement, une solution de sécurité intégrée s'avère essentielle pour transmettre les données de vulnérabilité à vos outils existants, comme les traqueurs de bugs, pour une remédiation rapide.
- Utilisez des mots de passe complexes. Le simple fait de choisir un mot de passe d'au moins 10 caractères renforcera votre sécurité. Même si le système ne vous le demande pas, changez votre mot de passe deux ou trois fois par an.
- Maintenez vos logiciels de sécurité à jour. Installez les correctifs régulièrement.
- Limitez l'accès réseau aux seuls hôtes et réseaux de confiance. Autorisez l'accès Internet uniquement pour les services réseau qui en ont besoin. Et sauf en cas de nécessité absolue, ne déployez jamais de systèmes accessibles directement par Internet. Pour les accès à distance, envisagez les VPN, le SSH ou d'autres méthodes d'accès sécurisé.
- Pour prévenir le phishing et les autres infections transmises par e-mail, formez vos salariés à vos politiques et aux bonnes pratiques, comme la suppression des pièces jointes suspectes.
- Si possible, utilisez l'authentification multifacteur (MFA).
- Configurez vos filtres antispam pour une couverture maximale.

2. Pierre Lidome, "The SANS Guide to Evaluating Attack Surface Management", SANS Institute, 26 octobre 2020, https://www.sans.org/reading-room/whitepapers/analyst/guide-evaluating-attack-surface-management-39905.

De nombreuses compromissions sont souvent le fruit d'un concours de circonstances mêlant erreurs humaines, systèmes non corrigés et attaquants plus déterminés que jamais, qui ont eux aussi su profiter de la transformation numérique.

En cas de compromission potentielle :

- Si seulement quelques systèmes sont infectés, déconnectez-les immédiatement (physiquement) de votre réseau interne pour contenir l'infection. Si vous ne pouvez pas les déconnecter rapidement ou si un plus grand nombre de systèmes est touché, et si vous n'avez pas implémenté des serveurs proxys et un filtrage renforcé des données de sortie sur vos pare-feu, alors bloquez immédiatement TOUT le trafic sortant vers des réseaux externes.
- Implémentez des filtres sur les pare-feu, les routeurs internes et autres équipements réseau pour isoler les segments infectés et pour surveiller le trafic réseau afin de garantir l'herméticité de votre environnement ou de suivre l'infection à la trace et d'identifier les hôtes touchés.
- Surveillez tout le trafic réseau pour contrer les éventuelles attaques multidimensionnelles.
- Examinez les fichiers journaux concernés pour tenter d'identifier le premier système infecté et le vecteur d'attaque utilisé.
- Il est primordial de déterminer si l'un des systèmes infectés a pu se connecter à un quelconque site Internet et, le cas échéant, quelles informations ont été exposées.

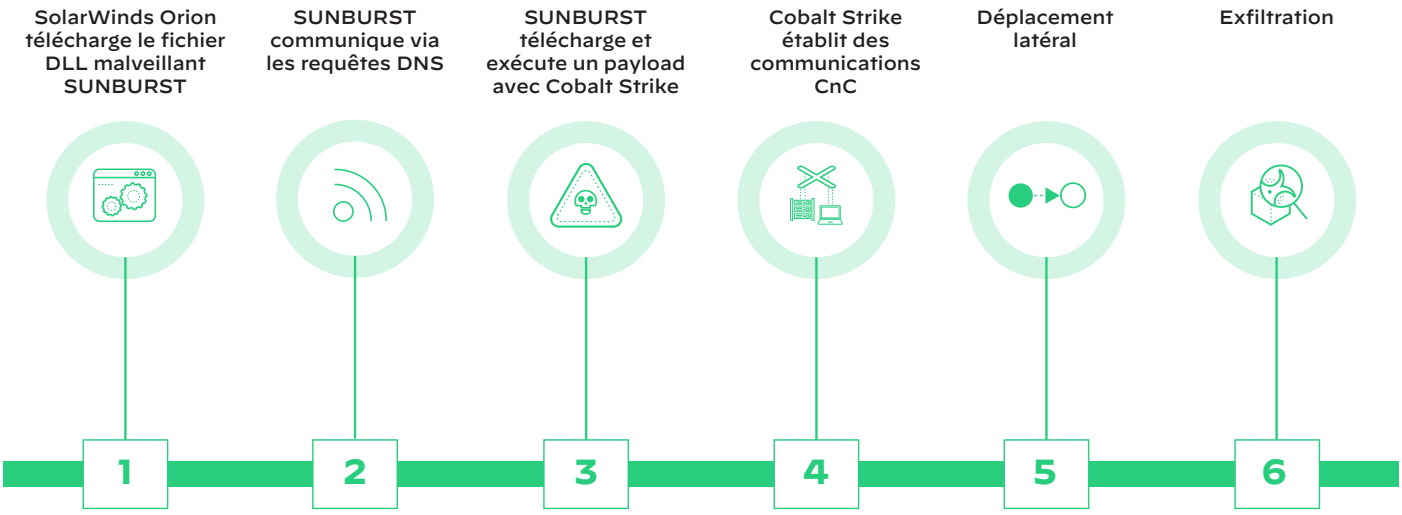

Figure 1 : L'attaque SolarStorm bloquée au stade 3 par Cortex XDR

À cet égard, Cortex XDR vous épargne le temps et les coûts associés à la création de votre propre infrastructure mondiale de sécurité des terminaux. Ce déploiement simplifié – sans licence serveur, base de données et autre infrastructure supplémentaires – permet aux organisations de protéger rapidement leurs terminaux.

3. Visibilité maximale

Grâce à une approche unifiée des données à travers toute la supply chain, il est possible de créer une vue globale sur les applications et l'infrastructure, auxquelles peuvent venir s'ajouter les données télémétriques des terminaux, des réseaux et des environnements cloud. La visibilité, c'est aussi pouvoir corréler ces sources de données afin d'établir un lien entre les différents évènements et de déterminer si un comportement donné est suspect ou non, en fonction du contexte.

Associées au machine learning, les données télémétriques et les analyses forensiques permettent de faire toute la lumière sur une chaîne d'attaque, avec à la clé une analyse détaillée au cours du tri et de la vérification d'une alerte et, in fine, une simplification et une accélération des investigations et de la réponse.

Dans le cas de l'attaque sur SolarWinds, malgré l'intégration du code malveillant au logiciel du fournisseur, la solution Cortex XDR interne de Palo Alto Networks a su bloquer une tentative de téléchargement de Cobalt Strike sur l'un de ses serveurs SolarWinds grâce au système de protection contre les comportements suspects (cf. Figure 1).

Face à des attaques avancées comme celle-ci, les organisations ont donc besoin d'une visibilité complète pour pouvoir les détecter et les bloquer à tous les stades (même en cas de compromission de l'hôte). Si une attaque est si sophistiquée qu'elle parvient à contourner vos systèmes de prévention, vous devez pouvoir détecter les activités que l'attaquant mène post-intrusion pour atteindre ses objectifs.

4. Réponse rapide

Si les hackers ont infiltré le système de SolarWinds vers janvier 2019, il semble que l'accès à son infrastructure était déjà en vente sur le forum Exploit Cybercrime du dark web le 13 octobre 2017, ce qui souligne l'attrait financier des campagnes APT.

En mars 2021, Microsoft et FireEye ont signalé de nouveaux indicateurs de compromission (IoC), y compris un backdoor et d'autres malwares destinés à établir un accès durable aux réseaux touchés. D'après Microsoft :

> « [Nous avons] découvert ces nouveaux outils et fonctionnalités malveillants sur des réseaux clients compromis, sur lesquels ils ont été utilisés entre août et septembre 2020. Une analyse plus poussée a révélé qu'ils étaient sans doute déjà sur les systèmes compromis en juin 2020. Ces outils constituent de nouveaux malwares propres à cet attaquant. Conçus pour des réseaux bien spécifiques, ils semblent avoir été installés après que l'attaquant se soit infiltré à l'aide d'identifiants compromis ou via le fichier binaire SolarWinds, et après une latéralisation via TEARDROP et d'autres actions manuelles[3]. »

Une fois un attaquant infiltré, il lui reste encore à contourner les systèmes de détection et à s'implanter durablement pour pouvoir mener à bien sa mission. Baptisé SolarStorm, le groupe à l'origine de la compromission de SolarWinds avait exploité des identifiants volés pour accéder aux services cloud, ainsi que des identités compromises pour infiltrer les réseaux et s'y maintenir via des VPN et des outils d'accès à distance.

C'est pourquoi il est indispensable, et même urgent, de réduire la durée de présence (ou les délais de détection d'une compromission) et les déplacements latéraux associés, afin de contenir et d'éliminer la menace et de se remettre rapidement d'une attaque. Outre l'éventuelle atteinte à l'image de l'entreprise, les amendes pour non-conformité et les pertes de données critiques, plus la détection et l'endiguement d'une compromission prennent du temps, plus l'impact financier est important.

Dans son rapport intitulé "Quantifying the Value of Time in Cyber-Threat Detection and Response", Aberdeen Group remarque que, lorsque la durée de présence est limitée à sept jours, l'impact en est réduit de 77 %. Et lorsque la compromission ne subsiste qu'une journée, on constate une baisse de 96 % de son impact sur l'entreprise (cf. Figure 2[4]).

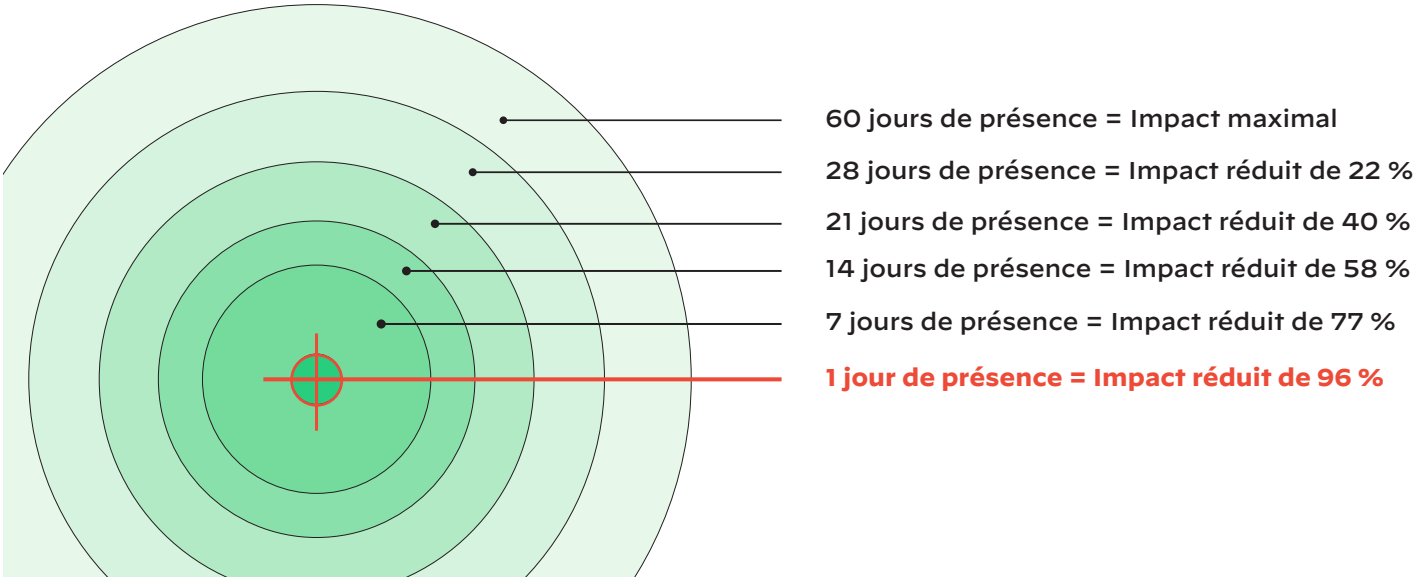

Figure 2 : Conclusions du rapport "Quantifying the Value of Time in Cyber-Threat Detection and Response" d'Aberdeen Group, février 2016

3. Ramin Nafisi et coll., "GoldMax, GoldFinger, and Sibot: Analyzing NOBELIUM's Layered Persistence", 4 mars 2021, https://www.microsoft.com/security/blog/2021/03/04/goldmax-goldfinder-sibot-analyzing-nobelium-malware/4.
4. Aberdeen Group, "Quantifying the Value of Time in Cyber-Threat Detection and Response", février 2016.

Au-delà de l'importance d'une réponse immédiate aux attaques, il est crucial de tenir compte de la vitesse et de la fréquence à laquelle les attaquants cherchent et trouvent d'éventuels vecteurs d'attaque. Les progrès des technologies d'analyse leur permettent en effet de repérer de tels vecteurs rapidement et facilement, en leur révélant des ressources non autorisées, mal configurées ou laissées en déshérence, et susceptibles de servir de backdoor dans le cadre d'une compromission.

Dans son rapport Cortex Xpanse 2021 intitulé « Surface d'attaque : les leçons des grands groupes », Palo Alto Networks a présenté les principales conclusions de son analyse de la surface d'attaque publique de certaines des plus grandes entreprises de la planète. De janvier à mars, son équipe a en effet surveillé les scans de plus de 50 millions d'adresses IP rattachées à 50 entreprises mondiales. L'objectif : mesurer à quelle vitesse les hackers repèrent les systèmes vulnérables et rapidement exploitables.

Parmi les points à retenir de cette étude :

- **Des attaquants toujours à l'œuvre** – Engagés dans un interminable jeu du chat et de la souris, les attaquants effectuent un nouveau scan toutes les heures, tandis que la même opération peut parfois prendre des semaines aux entreprises mondiales.
- **De nouvelles vulnérabilités rapidement exploitées** – Entre janvier et mars, les attaquants ont démarré un scan dans les 15 minutes suivant la publication d'une nouvelle CVE (Common Vulnerabilities and Exposures). Ils ont également réagi dans les cinq minutes qui ont suivi la publication du correctif de la vulnérabilité zero-day découverte dans Microsoft Exchange Server.
- **Le cloud en première ligne** – Les environnements cloud représentent 79 % des problématiques de sécurité les plus critiques observées dans les entreprises mondiales (contre 21 % pour les environnements sur site), ce qui souligne encore une fois le risque inhérent aux services basés/hébergés dans le cloud.

Le délai moyen de détection (MTTD) correspond au temps qu'il faut pour identifier un incident de sécurité potentiel dans une entreprise.

Le délai moyen avant défaillance (MTTF) correspond au temps qu'il faut à un système défectueux pour s'arrêter.

Le délai moyen de réponse (MTTR) correspond au temps qu'il faut à une équipe pour contrôler, neutraliser ou éliminer une menace après son identification.

Le délai moyen entre défaillances (MTBF) reflète la fiabilité et la disponibilité d'un système. Il sert à évaluer les performances de ce système dans des conditions prédéterminées, pendant une période donnée.

5. Modèle Zero Trust intégré

Si le modèle Zero Trust de la cybersécurité ne date pas d'hier, c'est en 2009 qu'il a réellement commencé à faire parler de lui, une fois formellement énoncé par Forrester Research[5]. En bref, il s'agit à la fois d'un modèle architectural pour les réseaux et d'un framework pour la définition des politiques de sécurité.

Le Zero Trust repose sur une vérification et une validation rigoureuses de chaque individu, appareil ou entité qui tente d'accéder aux ressources réseau. L'objectif principal : prévenir les attaques, les exploits, les compromissions et les corruptions de données, d'applications et de systèmes critiques.

Les principes du Zero Trust visent à réduire les expositions et les accès non autorisés à travers tout le champ des menaces. Ils ont été minutieusement pensés pour garantir la sécurité des applications critiques et des données sensibles dans toute une entreprise. Le mieux dans tout cela, c'est que vous pouvez aisément intégrer ces principes à votre stratégie de sécurité. Parmi eux :

- **Principe du moindre privilège (PoLP)** – L'idée est d'octroyer aux utilisateurs uniquement les droits d'accès dont ils ont absolument besoin pour accomplir leur mission. Ainsi, vous réduisez les points d'entrée et les expositions aux malwares et aux attaquants, ainsi que les risques d'exfiltration de données.
- **Microsegmentation** – Pour isoler les workloads, vous pouvez diviser votre réseau en plusieurs segments séparés, ou « zones sécurisées », dans vos data centers ou environnements cloud, l'accès à ces zones étant soumis à la saisie d'identifiants différents. Cela limite également les déplacements latéraux (est-ouest) sur les réseaux internes en cas de compromission.
- **Authentification multifacteur (MFA)** – Ce protocole de sécurité impose aux utilisateurs de s'authentifier à l'aide de plusieurs procédures de sécurité obligatoires. Il s'agit généralement d'une combinaison d'éléments que l'utilisateur connaît (un mot de passe ou un code PIN, par exemple), qu'il possède (jeton physique, badge, etc.) et qui le constituent (des données biométriques comme la voix et les empreintes digitales).

5. John Kindervag et coll., "No More Chewy Centers: The Zero Trust Model of Information Security", 23 mars 2016, https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682?objectid=RES56682.

Voici quelques recommandations pour affiner vos capacités Zero Trust :

- Surveillez toutes les activités et collectez toutes les données – et non uniquement celles associées à des évènements suspects.
- Détectez les comportements anormaux à l'aide de l'analytique et du machine learning.
- Détectez et bloquez les comportements malveillants sur les terminaux.
- Utilisez des pare-feu sur hôte pour segmenter les accès.
- Surveillez et limitez l'accès des équipements USB non autorisés à l'aide du contrôle des appareils. Les utilisateurs ne peuvent connecter aucun périphérique de stockage à la machine, à l'exception des appareils autorisés dans des cas bien précis et pour une durée limitée.
- Bloquez les hôtes distants malveillants.
- Orchestrez les contrôles de sécurité. L'automatisation et l'orchestration permettent d'identifier d'éventuelles brèches dans les architectures Zero Trust et de soit les combler automatiquement, soit déclencher des workflows pour aider les analystes à les éliminer. D'après le rapport Forrester intitulé "The Zero Trust eXtended (ZTX) Ecosystem", mieux vaut « éviter les solutions qui fonctionnent en vase clos et opter pour celles qui s'intègrent à un écosystème afin de renforcer la visibilité et le contrôle sur ce dernier et de garantir une orchestration robuste des défenses. »

Pour d'autres conseils sur l'élaboration d'une approche Zero Trust, nous vous invitons à consulter les publications suivantes :

- Sur le site du National Institute of Standards and Technology : Zero Trust Architecture: NIST Publishes SP 800-207
- Sur le site du National Cyber Security Centre : Zero trust principles - beta release
- Publication de la National Security Agency : Embracing a Zero Trust Security Model
- Rapport Forrester Research : Les cinq étapes de la mise en place d'un réseau Zero Trust*, à savoir :
  1. Identifier vos données sensibles.
  2. Cartographier les flux de données sensibles.
  3. Concevoir un micropérimètre Zero Trust.
  4. Miser sur l'analytique de sécurité pour passer à la loupe tout l'environnement Zero Trust.
  5. Implémenter l'automatisation et l'orchestration de la sécurité.

** Gratuit pour les abonnés Forrester, ce rapport est disponible à la vente.*

Cortex XDR : une arme plus si secrète

La bonne nouvelle, c'est qu'il existe un moyen efficace d'intégrer ces principes à votre stratégie de sécurité. Les plateformes de détection et de réponse étendues (XDR) de nouvelle génération collectent et corrèlent automatiquement les données de multiples sources – terminaux, serveurs, workloads cloud et réseau – afin d'accélérer la détection des menaces, ainsi que les délais d'investigation et de réponse des analystes sécurité.

Pour sa part, Palo Alto Networks Cortex® XDR™ est la toute première plateforme de détection et de réponse étendues à intégrer en natif les données des terminaux, des réseaux et du cloud pour permettre aux utilisateurs de bloquer les menaces avancées instantanément, à partir d'une seule et même console.

Cortex XDR est la seule solution à aider les équipes de sécurité à :

- **Détecter automatiquement les attaques furtives**, quel que soit le vecteur d'attaque, grâce aux analyses comportementales des données des terminaux, des réseaux et du cloud. La technologie Cortex XDR assimile le comportement de chaque appareil et utilisateur, puis le compare aux autres présents sur le réseau de l'organisation. Ces profils servent à détecter d'éventuels écarts par rapport aux comportements passés, à ceux des pairs et aux comportements attendus de l'entité sous surveillance.
- **Accélérer les investigations** en recoupant les données télémétriques et les alertes de multiples terminaux, ainsi que d'autres sources de données, puis en les raccordant à un seul et même incident pour en trouver la cause racine. Cette visibilité sur toutes les sources de données élimine les angles morts, permet d'identifier les attaques avancées à travers différentes couches de données et fournit davantage de contexte afin de simplifier les investigations. La consolidation des données permet également de réduire le nombre de produits de détection et de réponse à gérer par les clients.
- **Adapter sans cesse leurs défenses** en tirant les leçons d'investigations passées pour bloquer les menaces futures. Ainsi, vos analystes peuvent stopper rapidement la propagation des malwares, isoler les terminaux infectés et éliminer les malwares en temps réel, et même y accéder directement et enquêter sur les menaces sans déranger les utilisateurs.

Conclusion

Les attaques comme celle sur SolarWinds sonnent comme un rappel à tous les professionnels de la cybersécurité, tous secteurs et tous postes confondus : la protection des réseaux contre les menaces APT exige une vigilance de tous les instants. Au moment où le secteur connaît une sorte d'accalmie toute relative, dissèque ces évènements et essuie les plaies laissées par l'attaque sur SolarWinds, les organisations doivent prendre conscience de l'urgence d'un renforcement de leurs défenses. Après tout, la prochaine attaque majeure pourrait frapper d'un jour à l'autre.

Les attaquants conçoivent déjà des techniques qui repoussent sans cesse les limites du possible, dans leur perpétuelle quête de nouveaux moyens de causer un maximum de dégâts sans se faire prendre.

C'est donc le moment de capitaliser sur la manne de bonnes pratiques et de solutions de sécurité désormais disponibles pour renforcer votre protection. Visibilité sur la surface d'attaque, prévention maximale, principes Zero Trust... vous pouvez procéder par étape afin d'orienter vos équipes de sécurité dans la bonne direction.

Mieux encore, vous pouvez envisager des solutions de nouvelle génération comme les plateformes XDR, qui s'inscrivent dans la droite lignée de technologies éprouvées comme l'EDR. Les plateformes XDR intègrent les données EDR et d'autres types de télémétrie pour fournir la visibilité et le contrôle nécessaires sur les composants métiers adjacents.

Capable d'exploiter les flux de données de sécurité pour améliorer continuellement les modèles de machine learning – et coordonner la détection et la réponse – le XDR s'avère extrêmement prometteur pour tenir à distance les menaces à venir.

Envie d'apprendre de nouvelles compétences en traque des menaces ou d'en savoir plus sur la capacité de Cortex XDR à protéger votre environnement ? Organisez un atelier pratique avec nos experts ou demandez une démo de Cortex XDR.

Ressources complémentaires sur XDR

Téléchargez notre eBook intitulé XDR : le guide indispensable.

Téléchargez notre fiche technique sur Cortex XDR.

Rendez-vous sur notre page Cyberpedia consacrée à la technologie XDR.

Pour de plus amples informations sur la phase 3 de l'évaluation MITRE ATT&CK®, téléchargez notre eBook.

Forrester Research nous classe parmi les leaders dans son rapport The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers du 3e trimestre 2020. Cliquez sur le lien pour télécharger le rapport.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr