Affaire Kaseya : analyse d'un bis repetita du ransomware

Début juillet, des cybercriminels ont lancé la plus grande attaque par ransomware de l'histoire depuis celles de WannaCry et NotPetya perpétrées en 2017. Selon les estimations, entre 800 et 1 500 organisations — principalement des spécialistes de l'infogérance (MSP) et leurs clients — ont été touchées, et l'identification d'autres victimes se poursuit encore à l'heure actuelle.

Les services répressifs et les agences gouvernementales chargées de la cybersécurité qui participent à l'enquête, notamment le FBI, la Cybersecurity and Infrastructure Security Agency (CISA), et les agences de sécurité dans le monde, exhortent les organisations touchées à prendre des mesures immédiates pour déployer les meilleures pratiques en matière de cybersécurité.

L'infection initiale de Kaseya : une attaque d'envergure et d'impact

L'attaque par ransomware visait initialement Kaseya, un fournisseur de logiciels de gestion IT pour les MSP et les petites et moyennes entreprises. Selon les premiers rapports, les attaquants ont probablement identifié et exploité une vulnérabilité leur permettant de compromettre la solution Virtual System Administrator (VSA) de Kaseya, qui est utilisée pour surveiller et gérer à distance les terminaux et les serveurs.

Après avoir pris le contrôle des serveurs Kaseya VSA sur site et en mode SaaS, ainsi que d'autres serveurs sur site gérés par les MSP, les attaquants ont diffusé une fausse mise à jour logicielle contenant le ransomware sur tous les terminaux gérés.

Comme dans le cas de l'attaque de la chaîne d'approvisionnement de SolarWinds, le malware s'est propagé parmi la clientèle mondiale de Kaseya et ses clients en aval. Face à l'ampleur potentielle de l'attaque de Kaseya, le FBI a déclaré ne pas pouvoir avec certitude être en mesure de « répondre à chaque victime individuellement ».

Les pirates qui ont revendiqué l'attaque ont exigé de Kaseya le paiement d'une rançon faramineuse de 70 millions de dollars afin de restaurer les données des entreprises et des clients concernés. Entre-temps, les organisations de toute la chaîne d'approvisionnement ont rapidement ressenti les effets de l'attaque, de cabinets dentaires à des cabinets comptables en passant par des restaurants.

En Suède, une importante chaîne d'épiceries a été contrainte de fermer des centaines de magasins pendant plusieurs jours en raison de caisses enregistreuses hors service. En Nouvelle-Zélande, ce sont des écoles et plus de 100 jardins d'enfants qui ont été mis hors ligne et ont dû se tourner vers le papier et le crayon. Selon le New York Times, certaines organisations victimes auraient même reçu des demandes de rançon atteignant 5 millions de dollars.

Une réminiscence de l'attaque de supply chain par Cloud Hopper

Bien que les détails de cette campagne internationale de ransomware soient encore en train d'émerger, les schémas d'attaque rappellent la méga attaque Cloud Hopper ; il s'agissait d'une cyber-invasion de plusieurs années révélée pour la première fois en 2016 et qui visait les principaux fournisseurs de services technologiques du monde et leurs clients.

Dans le cas de Cloud Hopper, un seul terminal compromis a suffi pour affecter des centaines d'entreprises qui étaient en contact avec les fournisseurs de services cloud visés. Pour l'une des victimes, le cycle d'attaque s'est poursuivi pendant au moins cinq ans.

Dans le cadre de l'attaque actuelle, comme dans le cas de l'attaque précédente contre SolarWinds, les attaquants ont tiré parti de l'automatisation et de la confiance qui permettent de distribuer et de déployer des logiciels malveillants sous la forme d'un logiciel coopératif légitime.

Dans le cas de l'incident impliquant Kaseya, les attaquants se concentrent sur la compromission des logiciels et des processus de confiance. Le fait de cibler des services de confiance permet aux attaquants de tirer parti des autorisations et des accès accordés par les services de confiance.

Cloud Hopper, SolarWinds, Codecov et de nombreuses attaques par ransomware récentes ont prouvé que les périmètres de sécurité traditionnels ne suffisent plus. En ciblant les fournisseurs de services cloud, les attaquants peuvent se déplacer facilement d'un environnement « isolé » à un autre et parmi plusieurs organisations. Les déplacements latéraux ne sont plus limités au réseau physique d'une organisation, ce qui étend de façon exponentielle la portée des attaques.

Atténuer les risques pour que cela ne se répète pas de nouveau

Afin de limiter l'impact de l'attaque et d'atténuer les risques futurs, la CISA et le FBI ont diffusé des recommandations à l'attention des MSP et de leurs clients affectés par l'attaque par ransomware ayant ciblé la supply chain de Kaseya VSA. Ces dernières portent notamment sur les principes fondamentaux de la cybersécurité, comme l'activation de l'authentification multi-facteurs (MFA) et l'application du principe du moindre privilège.

Il est important que toutes les organisations en prennent connaissance et déploient des moyens de renforcer leurs protections contre les ransomwares.

1. Déployer ou renforcer les contrôles de leurs accès à privilèges

Ces comptes permettent à un utilisateur d'accéder à n'importe quel emplacement des systèmes ou du réseau et d'accéder aux actifs les plus critiques de l'entreprise. Appliquer le principe du moindre privilège – c'est-à-dire n'accorder que les accès nécessaires à l'utilisateur dans le cadre de sa mission pour une durée déterminée – peut ainsi favoriser la mise en place des niveaux d'accès minimaux requis pour les identités humaines et les machines.

En outre, d'autres contrôles efficaces des accès à privilèges, tels que la rotation des informations d'identification à privilèges et la surveillance des sessions, peuvent contribuer à réduire rapidement les risques.

2. Adopter une approche de défense en profondeur à l'égard de la sécurité des terminaux

Les cybercriminels qui utilisent des ransomware exploitent les vulnérabilités des terminaux pour dérober ou chiffrer des informations confidentielles. Le déploiement de mesures de moindre privilège représente un élément important d'une stratégie de défense en profondeur qui permet d'empêcher les adversaires de se déplacer latéralement et les oblige à utiliser des méthodes qui révèlent leur présence.

3. Activer l'authentification multi-facteurs (MFA).

Cette mesure permet de bloquer la majorité des attaques de compromission de comptes.
Si des contrôles d'accès sont déjà en place, les entreprises peuvent les renforcer avec une authentification multi-facteur (MFA) adaptative basée sur l'IA afin d'attribuer un risque à chaque occurrence d'accès, en fonction du contexte et du comportement.

L'attaque de Kaseya VSA témoigne une nouvelle fois du fait que les attaques par ransomware contre les supply chains augmentent tant en fréquence qu'en complexité et en ampleur. C'est pourquoi, des mesures proactives et préventives doivent absolument être prises pour sécuriser les actifs les plus précieux des organisations et garder une longueur d'avance sur les attaquants.