ÉTUDE DE CAS

Endiguement et remédiation rapides face à une cyberattaque de grande envergure

Kudelski Security fournit des services efficaces de réponse aux incidents à une entreprise agroalimentaire mondiale.

« Nous avons toujours eu conscience de l'importance d'une réponse efficace aux incidents. Mais c'est seulement après avoir souscrit au service d'astreinte de réponse aux incidents de Kudelski Security que nous en avons mesuré tous les avantages, notamment celui d'avoir à nos côtés une équipe d'experts qui nous guide en cas d'incident ou de compromission. »

- Responsable des opérations réseau et sécurité, entreprise internationale de boissons

EN BREF

- **Secteur** : alimentation et boissons
- **Taille** : 19 000 salariés répartis dans 80 pays
- **Offre** : services managés de détection et de neutralisation des menaces (MDR), services managés de protection des terminaux, services de surveillance et de traque des menaces 24 h/24 et 7 j/7, service d'astreinte assuré par l'équipe de réponse aux incidents de sécurité informatique (CSIRT), responsable de compte technique
- **Mission** : réponse aux incidents 24 h/24 et 7 j/7 pendant 20 jours à la suite d'une cyberattaque de grande envergure

JOUR 1 : DÉTECTION

Kudelski Security a détecté des comportements malveillants sur certains postes de travail le 24 décembre 2019. Les investigations ont révélé un incident de grande envergure ayant touché plus de 200 serveurs et postes de travail de l'entreprise sur trois continents.

JOUR 1 : ANALYSE

L'équipe Kudelski Security a élaboré une stratégie de gestion de crise qui a permis une communication fluide entre les membres de la direction du client, ses équipes techniques et le groupe de travail de Kudelski Security.

- Les investigations à distance ont débuté immédiatement, avec l'intervention de 15 experts en cyberintrusion de notre Cyber Fusion Center (CFC).
- Ces derniers ont travaillé sans relâche en Europe et aux États-Unis pour dresser un premier profil de l'attaque : chronologie, points d'accès, persistance et mécanismes de déplacement.
- Une analyse numérique a été effectuée pour étudier le profil de l'attaque et répertorier les indicateurs de compromission (IoC).
- Nous avons ajouté de nouvelles sources de journalisation (SIEM) pour éliminer les angles morts au niveau de la surveillance et faciliter la mise en corrélation des données sur les menaces.

JOUR 1 : ENDIGUEMENT

- Les équipes du CFC ont isolé les systèmes compromis à l'aide de la technologie CrowdStrike.

RÉSULTATS

- Détection rapide du déplacement latéral dans l'environnement
- Visibilité en temps réel sur les activités et les empreintes des cybercriminels
- Endiguement immédiat
- Remédiation complète à l'échelle de l'entreprise
- Cyberrésilience grâce à la remédiation et aux recommandations
- Détection de nouveaux indicateurs de compromission et de nouvelles tactiques, techniques et procédures
- Génération de rapports à l'intention du directeur mondial de la technologie
- Élaboration d'une présentation à l'intention des cadres dirigeants

- Elles ont aidé le client à mettre en place un objet de stratégie de groupe (GPO) pour son domaine, afin de bloquer l'accès à distance aux comptes locaux (technique utilisée par les cyberpirates pour se déplacer latéralement) et ainsi limiter la propagation de l'infection.
- Le CFC a ensuite validé l'efficacité de cette méthode.

JOURS 2 à 18 : ÉRADICATION ET REPRISE

- Un centre de crise a rapidement été mis sur pied pour permettre des analyses plus approfondies et assurer la remédiation.
- Les investigations ont révélé que certaines parties non surveillées de l'environnement avaient été infiltrées par l'assaillant depuis longtemps, à des fins de cryptominage.
- Les opérations de traque des menaces et de surveillance menées ont permis de découvrir de nouveaux indicateurs de compromission et de valider la méthode d'éradication.
- Grâce aux agents EDR de CrowdStrike déployés sur plusieurs systèmes et à différents emplacements, quelques minutes nous ont suffi pour repérer d'autres techniques, outils d'attaque et indicateurs de compromission. Cette rapidité de détection nous a permis de dégager du temps pour d'autres opérations de surveillance en temps réel, ce qui a *in fine* contribué à améliorer la détection des menaces et la remédiation globales.
- Grâce à la remédiation, le client a rapidement pu reprendre le cours normal de ses activités. Il a restauré ses systèmes compromis, défini des règles de surveillance pour valider la méthode d'éradication et reconnecté ses systèmes au réseau.

ACTIVITÉS POST-INCIDENT

Les équipes du CFC ont continué à fournir leur assistance après l'incident :

- Identification de plusieurs lacunes en termes de cyberrésilience et recommandations pour y remédier
- Génération de rapports à l'intention du directeur mondial de la technologie
- Élaboration de rapports à l'intention du conseil d'administration et des cadres dirigeants.

RÉSULTATS

En 20 jours de travail sans relâche, nous avons réussi à endiguer l'attaque, à effectuer une remédiation complète, à réduire le risque et à renforcer la cyberrésilience de l'entreprise.

L'impact sur les activités du client a été limité au strict minimum.