SALINS DÉJOUE DEUX ATTAQUES CIBLÉES GRÂCE AU SOC DE F-SECURE

Pour assurer sa conformité vis-à-vis de la CNIL et se protéger d'attaques Zero-Day, le Groupe Salins (sel La Baleine) a déployé les sondes RDS sur ses sites européens.

Entreprise : Groupe Salins

Secteur : Production de sel

Pays : France

Solution F-Secure : Rapid Detection and Response Service (RDS)

En 2018, dans un contexte de mise en conformité réglementaire avec le RGPD, Eugène Botella, Responsable de la sécurité des système d'information (RSSI), Délégué à la protection des données (DPO) et responsable du contrôle interne, expose ses doutes sur la capacité du groupe Salins à détecter des attaques de type Zero-Day. Il se met donc en recherche d'une solution de détection et de réponse.

HUMAINS + MACHINES

Le groupe Salins est en relation avec F-Secure depuis plus de 20 ans. Après avoir installé le scanner de vulnérabilités F-Secure Radar en 2017, Eugène Botella accepte la proposition de F-Secure d'effectuer un POC pour tester le service managé F-Secure RDS sur quelques postes de travail.

« Bien sûr, nous avions envisagé d'autres solutions, mais ce qui nous a séduit, c'est qu'en complément des outils standards, F-Secure possède ses propres sondes et son SOC ; les évènements de sécurité, d'abord triés et enrichis par les algorithmes, passent entre les mains d'experts, ce qui assure une analyse très fine. La concurrence utilise surtout des algorithmes sans analyse humaine », précise Eugène Botella.

UN DÉPLOIEMENT RAPIDE, DISCRET ET LÉGER

L'équipe F-Secure assiste le groupe sur le terrain pour définir la méthode de déploiement la plus adaptée à l'environnement industriel et au contexte multi sites du groupe.

« Le déploiement a été très rapide via l'Active Directory : dès que l'utilisateur s'authentifiait, l'agent s'installait immédiatement. C'est rapide, discret et léger à déployer », explique Eugène Botella.

La licence est par la suite ouverte à l'ensemble des sites administratifs et industriels en France, en Italie et en Espagne, soit environ 550 postes de travail et une centaine de serveurs. En cas de croissance, le groupe Salins compte étendre le déploiement du service aux nouvelles filiales.

UN TAUX DE FAUX-POSITIFS TRÈS FAIBLE

Lorsqu'une alerte est remontée par le SOC, l'équipe sécurité informatique réalise un diagnostic et confirme si oui ou non, il s'agit bien d'une attaque réelle en changeant le statut de la détection sur la plateforme.

En cas d'attaque avérée, les équipes de forensique et de réponse collaborent avec la DSI pour les aider à contenir la menace. Les informations peuvent être utilisées comme preuve dans le cadre d'enquêtes criminelles ou à destination de la CNIL.

« Pour la partie support, le service de la plateforme est en anglais mais notre contact chez F-Secure France se charge de faire l'intermédiaire si nécessaire », ajoute Eugène Botella.

Opérationnel depuis octobre 2018, le service a déjà remonté 30 alertes dont 27 menaces réelles, ce qui représente un taux de faux-positifs de seulement 10 %.

F-Secure

DEUX ATTAQUES CIBLÉES CONTENUES

« Il y a peu de temps, notre structure italienne a fait l'objet d'une attaque ciblée. Nous avons pu renforcer nos dispositifs et prévenir les salariés pour qu'ils soient vigilants. Les messages contenaient des fichiers malveillants et étaient très personnalisés avec des noms de clients, un imprimé de commandes correspondant à notre progiciel de gestion, avec des noms de vrais produits. C'est le genre de cas qui n'est pas du tout facile à appréhender : sans RDS, nous n'aurions pas pu le voir aussi rapidement », raconte Eugène Botella.

« Il y a peu de temps, notre structure italienne a fait l'objet d'une attaque ciblée. Nous avons pu renforcer nos dispositifs et prévenir les salariés pour qu'ils soient vigilants. »

Eugène Botella

Au total, deux attaques ciblées ont été déjouées : leurs techniques d'obfuscation très évoluées leur ont permis de contourner les solutions de sécurité en place. La première attaque visait à paralyser certains systèmes, alors que la seconde était destinée à exfiltrer des données critiques de l'entreprise.

« Les premiers résultats sont donc très satisfaisants mais c'est aussi très préoccupant. On avait le sentiment que certaines attaques pouvaient passer entre les mailles de notre solution antivirale : ça nous a permis de voir que nos intuitions étaient fondées. Maintenant, on sait et on peut réagir rapidement », conclut Eugène Botella.

A PROPOS DU GROUPE SALINS

Le groupe Salins est l'un des principaux saliniers européens et le seul à se consacrer exclusivement à la production et à la commercialisation de sel. Avec 4 millions de tonnes de sel produit chaque année, il couvre toutes les applications possibles : alimentation humaine, agriculture, chimie, déneigement, traitement de l'eau et autres activités industrielles. Depuis 150 ans, l'activité historique à Aigues Morte s'est étendue à l'international avec une présence industrielle en Espagne et en Italie. Parmi les marques du groupe Salins, on peut citer : Le saunier de Camargue, La Baleine, Salins Agriculture, Rock, Marine Salt etc.

Pour plus d'informations : www.salins.com

F-Secure