FireEye
SECURITY REIMAGINED

Le ministère de l'Énergie saoudien détecte le malware Shamoon grâce à la technologie FireEye de sécurité du réseau

Étude de cas

LA SÉCURITÉ RÉINVENTÉE

PROFIL DU CLIENT

Le ministère du Pétrole et des Ressources minérales du Royaume d'Arabie saoudite est l'organisme gouvernemental chargé de la mise en œuvre de politiques et de la supervision des activités d'exploration, de développement, de raffinage et de distribution des ressources pétrolières, minérales et gazières. Il surveille et contrôle les sociétés pétrolières et gazières détenues en tout ou partie par le gouvernement saoudien, telles que Saudi Aramco, la filiale saoudienne de Chevron, Aramco Gulf Operation Ltd et bien d'autres. Il préside le conseil d'administration de Saudi Aramco.

LES ENJEUX

L'industrie des hydrocarbures est une cible particulièrement prisée des attaquants de tous types. Pirates à la solde d'un État, terroristes, cybercriminels, hacktivistes : ces individus sont poussés par des motivations diverses, notamment le sabotage, l'espionnage, l'appât du gain ou des causes politiques. En conséquence, le secteur de l'énergie est en proie à des attaques de plus en plus nombreuses et sévères. Pour preuve, le ministère saoudien du Pétrole et des Ressources minérales essuie un déluge permanent de tentatives de compromissions. C'est pourquoi il adopte une position à la fois ferme et proactive en matière de sécurité informatique. Ainsi, dès 2011, ses dirigeants ont pris conscience des limites des antivirus et pare-feux face aux attaques avancées, et se sont aussitôt mis en quête d'une solution plus efficace.

LA SOLUTION

La même année, au terme d'une preuve de concept (POC) concluante, le ministère fait l'acquisition de FireEye® Network Threat Prevention Platform (série NX). En 2012, sur les conseils du ministère, ce fut au tour de Saudi Aramco d'organiser une preuve de concept. Ainsi, lorsque la compagnie nationale d'hydrocarbures fut la cible du malware Shamoon en août 2012, la série FireEye NX fonctionnait en mode surveillance, ce qui lui a permis de détecter le virus sans toutefois pouvoir le bloquer. Le ministère reste convaincu que si la série FireEye NX avait été déployée en production et en mode blocage instantané, Saudi Aramco aurait évité les perturbations et dommages coûteux infligés par Shamoon.

« Lorsque j'ai découvert FireEye en 2011, j'ai tout de suite su que c'était la solution qu'il nous fallait », explique Wahid Hammami, Directeur informatique et DSI du ministère. « En matière de détection et de prévention des attaques avancées, la technologie du moteur FireEye Multi-Vector Virtual Execution™ (MVX) est incomparable. Elle est la seule offre du marché capable de nous protéger contre les attaques zero-day. »

Confronté à de nombreuses attaques sur plusieurs fronts, le ministère a aussitôt décidé d'étendre la série FireEye NX à FireEye® Email Threat Prevention Platform (série EX), puis à FireEye® Central Management (série CM). L'objectif : consolider les fonctions d'administration, de reporting et de partage de données à l'échelle de la solution FireEye. Il s'est également abonné au service FireEye® Dynamic Threat Intelligence (DTI) pour bénéficier des données constamment à jour du système mondial de cyberveille. Il s'appuie en outre sur la plate-forme d'analyse forensique FireEye® (série AX) pour inspecter les fichiers malveillants.

« En matière de détection et de prévention des attaques avancées, la technologie FireEye MVX est incomparable. »

La sécurité multiniveau du ministère est exemplaire à plus d'un titre. La suite de produits FireEye lui offre de nombreux avantages :

- **Détection et blocage des attaques avancées sur plusieurs fronts.** La série FireEye NX détecte et analyse de façon dynamique le trafic en provenance ou à destination d'URL suspectes, tandis que la série FireEye EX se charge de l'analyse du contenu des e-mails et de leurs pièces jointes. Dès qu'une menace est avérée, la communication est interrompue et les fichiers malveillants sont placés en quarantaine.
- **Prévention du vol de données et des attaques multiphases.** La série FireEye NX bloque la communication avec les hôtes Web malveillants sur plusieurs protocoles (notamment HTTP, FTP et IRC) pour empêcher les attaquants de voler des données ou télécharger des outils supplémentaires.
- **Consolidation des fonctions de cyberveille et de reporting.** Grâce au service forfaitaire Dynamic Threat Intelligence, le ministère est certain de recevoir les informations les plus récentes sur les tactiques des attaquants, collectées partout dans le monde par la communauté FireEye. De plus, ses hauts fonctionnaires sont continuellement informés de la situation grâce aux rapports générés par FireEye Central Management.
- **Enquête sur les malwares à travers de multiples environnements Windows.** La série FireEye AX permet au ministère de tester et d'analyser le comportement des malwares sur un large éventail de navigateurs, plug-ins, applications et systèmes d'exploitation.

LES AVANTAGES

Grâce au déploiement parallèle de plusieurs produits FireEye, le ministère saoudien du Pétrole et des Ressources minérales bénéficie de fonctionnalités complètes de détection, de prévention et de cyberveille au sein d'une solution intégrée. Le partage des informations est automatisé et le reporting entre les produits s'effectue avec une grande simplicité.

« Avec Central Management pour l'intégration de tous les produits de la suite et Dynamic Threat Intelligence pour ses informations de cyberveille, FireEye se démarque clairement des autres fournisseurs », constate Wahid Hammami, Directeur des systèmes d'information. « En juin 2013, c'est l'ensemble du secteur énergétique public qui a été pris pour cible, et nous sommes parvenus à écarter le danger. »

Suite à l'acquisition de Mandiant par FireEye en 2013, le ministère a par ailleurs accès aux compétences des experts en sécurité les plus talentueux.

« En Arabie saoudite, on ne trouve pas un niveau d'expertise comparable à celui de Mandiant », déclare M. Hammami. « Mandiant a récemment réalisé un bilan de nos procédures et de notre environnement de sécurité, au terme duquel il nous a délivré un rapport consultatif exhaustif. » L'investissement engagé dans les produits FireEye et les services Mandiant offre au ministère de nombreux avantages :

- **Détection et prévention d'une multitude d'attaques.** Le ministère et ses sociétés affiliées du secteur de l'énergie sont régulièrement la cible d'attaques. La solution FireEye a détecté et bloqué de multiples tentatives de compromission via le Web et les e-mails.
- **Réduction des perturbations des opérations et des coûts de neutralisation.** Les attaques visant le secteur de l'énergie sont notoirement destructrices, mais grâce à la détection précoce des menaces, au blocage de la communication avec les hôtes malveillants et à la mise en quarantaine des malwares, le ministère est parvenu à rester opérationnel et à éviter toute intervention de remédiation.
- **Accompagnement par les meilleurs experts en sécurité au monde.** Le ministère a su pallier à la pénurie de compétences en sécurité en Arabie saoudite en faisant appel à la très réputée équipe de services professionnels de Mandiant pour bénéficier en permanence de ses précieux conseils.

LA VISION

Le ministère prévoit d'acquérir FireEye® Content Threat Prevention Platform (série FX) dans le courant de l'année pour la détection d'éventuel contenu malveillant sur ses serveurs de fichiers. Il envisage également d'améliorer la sécurité des terminaux mobiles pour protéger les tablettes, ordinateurs portables et terminaux personnels des fonctionnaires lorsque ceux-ci accèdent à distance à ses services informatiques.

FireEye, France | 4, place de la Défense, Paris La Défense Cedex 92974 | +33 1 58 58 01 76 | france@FireEye.com | **www.FireEye.fr**

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | **www.FireEye.com**