La dernière innovation Open Source de Sourcefire permet aux utilisateurs de combiner plusieurs technologies de détection des intrusions et de collecte de menaces pour une protection plus rapide et coordonnée.

Paris, le 28 juillet 2010, Sourcefire, acteur incontournable sur le marché de la gestion des menaces en temps réel (Cybersecurity) et créateur de Snort® annonce aujourd'hui la sortie de Razorback™, une structure logicielle open source conçue pour permettre une inspection du système en profondeur afin de combattre les menaces d'aujourd'hui les plus complexes.

Razorback est capable de relier les outils de détection d'intrusion d'une entreprise pour en optimiser l'efficacité, offrant ainsi une meilleure visibilité des différentes menaces détectées par un éventail de solutions de sécurité.
Développé pour apporter une réponse efficace face aux menaces complexes persistantes, Razorback permet facilement aux administrateurs de collecter, d'analyser et de stocker les données sur les menaces, provenant de différentes technologies, pour mettre en œuvre une détection et une prévention adaptées à l'entreprise et ses menaces.

L'objectif de Razorback est d'agir en tant que solution globale pour permettre d'établir une corrélation, fournir des analyses et proposer des actions à mettre à œuvre, le tout basé sur les outils de sécurité existants (antivirus, IDS, passerelles, e-mails…).

Aussi appelée, l'*Intelligence Driven Response* (IDR) par Sourcefire, cette méthodepermet d'aller au-delà de la réponse classique à un incident. Elle permet ainsi aux entreprises d'utiliser les informations acquises grâce à l'analyse des attaques, pour arriver à apporter une véritable réponse personnalisée. Razorback propose une analyse complexe et un reporting complet, en stockant chaque donnée identifiée comme une vulnérabilité ou une attaque, et en mettant en évidence les composants de cette donnée ayant déclenchés une alarme dans le système. Razorback affiche par ailleurs les informations ciblées à postériori sur les vecteurs d'attaque les plus fréquemment rencontrés.

« *L'open source est au cœur de chaque produit chez Sourcefire, et Razorback est la dernière innovation qui offre aux entreprises la possibilité de se protéger contre les menaces complexes d'aujourd'hui,* » confie **Martin Roesch, fondateur et directeur technique de Sourcefire et créateur de Snort**. « *Sourcefire est connu pour repousser les limites de la détection d'intrusions et le moteur d'analyse et de détection en quasi-temps réel de Razorback offre une solution pour contrer les attaques et les logiciels malveillants côté client. Nous nous sommes appuyés sur nos connaissances pour fournir une structure logicielle capable de relier des technologies de sécurité différentes et pouvant transformer une analyse approfondie des attaques en une véritable capacité de détection des menaces ciblées et des vulnérabilités Zero-day.* »

En effet, la structure logicielle innovante de Razorback réalise une détection en quasi-temps réel (en termes de secondes) et bloque les services tels que la messagerie ou le proxy web, et remonte des alertes en cas d'attaque.

« *Razorback a été conçu pour affronter les menaces d'aujourd'hui, celles spécialement élaborées par des hackers pour déjouer les outils et les technologies standards,* » explique **Matt Watchinski, Directeur de la Vulnerability Research Team VRT (VRT) de Sourcefire.** « *Tout en proposant des fonctionnalités de détection avancées pour prévenir les*

menaces difficiles à détecter, Razorback apporte une vraie réponse en matière d'analyse des attaques. »

Une interface conviviale permet aux entreprises l'intégration rapide et facile des fonctionnalités. Sourcefire va continuer de développer les fonctionnalités de Razorback, son moteur de détection, ses logiciels d'analyse, notamment pour encourager l'innovation au sein de la communauté Open Source.

Comme l'ensemble des autres technologies Open Source, Razorback est disponible gratuitement.
Pour plus d'informations ou pour télécharger Razorback, rendez-vous sur le site : http://labs.snort.org/razorback.

A propos de l'équipe VRT de Sourcefire (Vulnerability Research Team™)
L'équipe de recherche de vulnérabilités de Sourcefire rassemble des experts de la prévention d'intrusions qui travaillent pour découvrir, évaluer et répondre aux tendances les plus récentes en matière d'attaques, de tentatives d'intrusion et de vulnérabilités.
Au sein de l'équipe VRT se trouvent plusieurs professionnels de la sécurité informatique, de la plus grande renommée dans l'industrie, comprenant notamment les auteurs de plusieurs ouvrages de référence sur la sécurité. Cette équipe est aussi soutenue par les communautés Open Source Snort et ClamAV, faisant d'elle le plus grand groupe dédié à l'essor de la sécurité réseau. Pour rester informé des recherches et découvertes de la sécurité réseau, rendez-vous sur : http://vrt-sourcefire.blogspot.com/.

A propos de Sourcefire
Sourcefire, Inc. (Nasdaq: FIRE), créateur de Snort® et éditeur open source innovant est l'un des leaders sur le marché des solutions de sécurité des réseaux d'entreprise. Sourcefire révolutionne la façon de gérer le réseau des entreprises (grands comptes et PME) et des organismes gouvernementaux en contrôlant et minimisant les risques de sécurité. L'IPS de Sourcefire et sa technologie « Real-time Adaptative » offre un système de défense efficace et performant en temps réel en protégeant les réseaux avant, pendant et après une attaque. Depuis plusieurs années, Sourcefire est régulièrement reconnue par ses clients, les médias et les analystes pour son leadership industriel innovant – avec plus de 40 récompenses et consécrations à son palmarès. Aujourd'hui, le nom de Sourcefire et celui de son fondateur Martin Roesch sont devenus tous deux synonymes d'innovation et d'intelligence sur le marché de la sécurité informatique. Pour plus d'informations à propos de Sourcefire, rendez-vous sur www.sourcefire.com.