Internet : Razorback de Sourcefire, dÃ©tection et protection des menaces
Internet
PostÃ© par : JPilo
PubliÃ©e le : 30/7/2010 0:00:00

SOURCEFIRE prÃ©sente RAZORBACK, une structure logicielle open source qui offre une **dÃ©tection et une protection multiconstructeur contre les menaces**.

La derniÃ¨re innovation Open Source de Sourcefire permet aux utilisateurs de combiner plusieurs technologies de dÃ©tection des intrusions et de collecte de menaces pour une protection plus rapide et coordonnÃ©e.

Sourcefire, acteur incontournable sur le marchÃ© de la gestion des menaces en temps rÃ©el (Cybersecurity) et crÃ©ateur de SnortÂ® annonce aujourdâ□□hui la sortie de Razorbackâ□¢, une structure logicielle open source conÃ§ue pour permettre une inspection du systÃ¨me en profondeur afin de combattre les menaces dâ□□aujourdâ□□hui les plus complexes.

Razorback est capable de relier les outils de dÃ©tection dâ□□intrusion dâ□□une entreprise pour en optimiser lâ□□efficacitÃ©, offrant ainsi une meilleure visibilitÃ© des diffÃ©rentes menaces dÃ©tectÃ©es par un Ã©ventail de solutions de sÃ©curitÃ©.

DÃ©veloppÃ© pour apporter une rÃ©ponse efficace face aux menaces complexes persistantes, Razorback permet facilement aux administrateurs de collecter, dâ□□analyser et de stocker les donnÃ©es sur les menaces, provenant de diffÃ©rentes technologies, pour mettre en oeuvre une dÃ©tection et une prÃ©vention adaptÃ©es Ã lâ□□entreprise et ses menaces.

Lâ□□objectif de Razorback est dâ□□agir en tant que solution globale pour permettre

dâ□□Ã©tablir une corrÃ©lation, fournir des analyses et proposer des actions Ã mettre Ã oeuvre, le tout basÃ© sur les outils de sÃ©curitÃ© existants (antivirus, IDS, passerelles, e-mailsâ□¦).

Aussi appelÃ©e, lâ□□Intelligence Driven Response (IDR) par Sourcefire, cette mÃ©thode permet dâ□□aller au-delÃ de la rÃ©ponse classique Ã un incident. Elle permet ainsi aux entreprises dâ□□utiliser les informations acquises grÃ¢ce Ã lâ□□analyse des attaques, pour arriver Ã apporter une vÃ©ritable rÃ©ponse personnalisÃ©e. Razorback propose une analyse complexe et un reporting complet, en stockant chaque donnÃ©e identifiÃ©e comme une vulnÃ©rabilitÃ© ou une attaque, et en mettant en Ã©vidence les composants de cette donnÃ©e ayant dÃ©clenchÃ©s une alarme dans le systÃ¨me.

Razorback affiche par ailleurs les informations ciblÃ©es Ã postÃ©riori sur les vecteurs dâ□□attaque les plus frÃ©quemment rencontrÃ©s.

Â« *Lâ□□open source est au coeur de chaque produit chez Sourcefire, et Razorback est la derniÃ¨re innovation qui offre aux entreprises la possibilitÃ© de se protÃ©ger contre les menaces complexes dâ□□aujourdâ□□hui,* Â» confie **Martin Roesch**, fondateur et directeur technique de Sourcefire et crÃ©ateur de Snort. Â« *Sourcefire est connu pour repousser les limites de la dÃ©tection dâ□□intrusions et le moteur dâ□□analyse et de dÃ©tection en quasi-temps rÃ©el de Razorback offre une solution pour contrer les attaques et les logiciels malveillants cÃ´tÃ© client. Nous nous sommes appuyÃ©s sur nos connaissances pour fournir une structure logicielle capable de relier des technologies de sÃ©curitÃ© diffÃ©rentes et pouvant transformer une analyse approfondie des attaques en une vÃ©ritable capacitÃ© de dÃ©tection des menaces ciblÃ©es et des vulnÃ©rabilitÃ©s Zero-day.* Â»

En effet, la structure logicielle innovante de Razorback rÃ©alise une dÃ©tection en quasi-temps rÃ©el (en termes de secondes) et bloque les services tels que la messagerie ou le proxy web, et remonte des alertes en cas dâ□□attaque.

Â« *Razorback a Ã©tÃ© conÃ§u pour affronter les menaces dâ□□aujourdâ□□hui, celles spÃ©cialement Ã©laborÃ©es par des hackers pour dÃ©jouer les outils et les technologies standards,* Â» explique **Matt Watchinski,** Directeur de la Vulnerability Research Team VRT (VRT) de Sourcefire. Â« *Tout en proposant des fonctionnalitÃ©s de dÃ©tection avancÃ©es pour prÃ©venir les menaces difficiles Ã dÃ©tecter, Razorback apporte une vraie rÃ©ponse en matiÃ¨re dâ□□analyse des attaques.* Â»

Une interface conviviale permet aux entreprises lâ□□intÃ©gration rapide et facile des fonctionnalitÃ©s. Sourcefire va continuer de dÃ©velopper les fonctionnalitÃ©s de Razorback, son moteur de dÃ©tection, ses logiciels dâ□□analyse, notamment pour encourager lâ□□innovation au sein de la communautÃ© Open Source.

Comme lâ□□ensemble des autres technologies Open Source, **Razorback est disponible gratuitement**.