FireEye s'offre nPulse, spécialiste de l'investigation réseau

Si les spécialistes de la sécurité se focalisent sur la prévention des attaques à travers la recherche de signaux faibles, les variantes des signatures ou les comportements anormaux, l'analyse des attaques a posteriori est aussi très importante. Ce travail d'enquête permet de découvrir le modus operandi de la cyberattaque, les chemins réseaux, les failles utilisées, etc.

FireEye vient de s'offrir un des spécialistes dans le domaine de l'investigation réseau post attaque : nPulse. La société est basée à Charlottesville en Virginie et édite plusieurs outils comme la plateforme Cyclone Network Forensics qui combine des solutions de récupération de paquets perdus (via une appliance baptisée CPX -Capture Probe Extreme) avec de l'analyse de trafic réseau (adresse IP, enregistrement DSN, en-tête http). **L'objectif est de récolter le maximum d'information pour reconstituer le scénario de l'attaque** et apporter des réponses adéquates. La société indique sur son site qu'elle utilise un framework Big Data pour lancer des analyses en quasi temps réel.

Un portefeuille d'investigation complet

Sur le plan de l'intégration, les différents services de nPulse vont être progressivement intégrés dans le portefeuille Management Defense de FireEye. **David DeWalt**, CEO de FireEye, explique : « *La nouvelle réalité de la sécurité est que chaque entreprise a des bouts de code malveillant dans son réseau. La question importante est : ce bout de code est-il en mesure de compromettre les activités critiques de l'entreprise.* » Il ajoute que « *avec nPulse, **FireEye disposera d'un « enregistreur à la volée »** des évènements de sécurité* ».

Pour acquérir nPulse, FireEye va proposer **60 millions de dollars en cash et 10 millions de dollars en action**, souligne le site Re/code. Il s'agit de la deuxième acquisition dans le domaine de la surveillance des réseaux et l'analyse des incidents. En janvier dernier, le spécialiste de la sécurité fraichement côté en bourse s'était offert Mandiant pour 1 milliard de dollars. Le rachat de nPulse vient compléter ce portefeuille qui scrute les incidents de sécurité du terminal jusqu'au réseau.

A lire aussi :

Dave Merkel, FireEye : « Contre les menaces persistantes, il faut des technologies mais aussi des hommes »

Sécurité : FireEye va se lancer dans la détection d'intrusion