Les réseaux SDN ouverts à tous les vents (mauvais)

Les réseaux SDN ouverts à tous les vents (mauvais)

Des scientifiques italiens démontrent une vulnérabilité de sécurité propre au fonctionnement intrinsèque des réseaux SDN. Inquiétant alors que les déploiements ont déjà démarré…

Et si l'un des principes de base du fonctionnement des SDN masquait une inquiétante faille de sécurité ? Les contrôleurs des Software Defined Networks, pilotés de manière logicielle, configurent le réseau en attribuant de nouvelles règles de traitement des flux aux switches. Et c'est ce fonctionnement même qui poserait problème.

C'est du moins le résultat des travaux de trois chercheurs italiens, Mauro Conti (de l'université de Padoue), Fabio De Gaspari et Luigi V. Mancini (tous deux de l'université de Sapienza). *« Nous pensons que des aspects importants de la sécurité des SDN restent encore inexplorés »*, notent-ils dans leur rapport. Pour en convaincre la communauté, ils ont mis au point une nouvelle forme d'attaque, baptisée Know Your Enemy (KYE), au moyen de laquelle un attaquant peut recueillir des informations vitales sur la configuration du réseau.

Moisson d'informations de configuration

A travers leurs travaux, ils entendent démontrer comment un attaquant peut recueillir des informations sur la configuration des outils de sécurité du réseau (dont les seuils de détection d'attaque par scan), sa politique de qualité de service ou encore sa virtualisation. Et d'ajouter qu'une seule table de routage d'un commutateur peut fournir ces informations tout en servant de canal d'attaque. Cerise sur le gâteau : *« nous montrons qu'un attaquant peut effectuer une attaque KYE dans un mode furtif, à savoir sans risquer d'être détecté »*, expliquent-*ils*.

Selon les universitaires, un attaquant pourrait se connecter aux ports d'écoute passive qu'intègrent la plupart des commutateurs pour le débogage à distance afin de récupérer le plan de routage (notamment avec la commande 'dpctl' sur les HP Procurve qu'ils ont utilisés au cours de leurs travaux), en déduire des informations sur la table de routage, espionner le contrôle du trafic en cas d'absence de protection de ce dernier (par chiffrement TLS ou usage de certificats d'authentification), exploiter les vulnérabilités connues dans les systèmes d'exploitation des switches pour introduire une backdoor, ou encore extraire la table de routage ou le contenu de la mémoire du commutateur pour la copier vers un support externe au réseau.

Obscurcir pour limiter les risques

Autant d'informations qui permettent une attaque ou un espionnage plus massif ou plus ciblé du SI dans l'absolu. Les conclusions des chercheurs italiens sont d'autant plus inquiétantes que, en apportant une flexibilité optimale de gestion des réseaux, les technologies SDN sont de plus en plus adoptées par les opérateurs et grandes entreprises. Le rapport insiste bien sur le fait que ces possibilités d'espionnage ne sont pas liées aux systèmes matériels présents sur le réseau, mais bien à son fonctionnement intrinsèque.

Pour limiter les risques d'attaque, les scientifiques détaillent une contremesure basée sur un « *obscurcissement* » des flux entrants. *« S'il était possible d'empêcher l'attachant de comprendre quel flux est responsable de l'application des règles de routage, l'attaque KYE serait irréalisable »*, indiquent-ils. Ce qu'ils ont réussi à faire en exploitant la possibilité de modification du transit des flux dont dispose un switch OpenFlow. Et les chercheurs de rappeler que les risques décrit dans leur travail ne touchent que les réseaux SDN, les structures « traditionnelles » étant par défaut épargnées. Ce qui ne les empêche pas d'avoir leurs propres soucis de sécurité.

Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Sécurité : les réseaux SDN ouverts à tous les vents (mauvais) | Silicon