Un exploit des Shadow Brokers modifié cible les firewalls récents de Cisco

C'était une des craintes des chercheurs en sécurité après la mise en ligne de la première archive des Shadow Brokers, et elle n'a pas tardé à se matérialiser. Des spécialistes de Silent Signal, une entreprise hongroise, ont porté un des exploits que les Shadow Brokers prétendent avoir dérobé à Equation (un groupe de hackers qui semble être une émanation directe de la NSA) vers des générations de machines plus récentes que celles qu'il était capable de compromettre à l'origine.

En l'occurrence, ExtraBacon – le nom de cet exploit diffusé par les Shadow Brokers – a ici été adapté pour la version 9.2(4) des firewalls ASA (Adaptive Security Appliance) de Cisco. Une version qui date d'un an seulement. Rappelons que les outils de piratage (implants, exploits…) mis en ligne par les Shadow Brokers semblent être assez anciens et ciblent de ce fait plutôt d'anciennes générations de machines. C'est le cas chez Cisco, mais également chez Fortinet, WatchGuard ou Juniper, qui ont tous analysé et validé la réalité de ces menaces.

« Etendre ExtraBacon ? Facile »,

Les analyses d'ExtraBacon considérait jusqu'à présent que seules les versions 8.x, jusqu'à la 8.4(4), étaient concernées. Sauf que, depuis, Silent Signal est passé par là… « *L'exploit fonctionne parfaitement (sur la version 9.4, NDLR) et comprendre comment l'étendre s'est avéré réellement facile* », explique Balint Varga-Perke, le co-fondateur de Silent Signal dans les colonnes de *ThreatPost*. La société hongroise explique qu'elle ne dévoilera le code de son ExtraBacon revu et visité qu'après la diffusion d'un correctif par Cisco. Mais elle livre tout de même quelques détails dans un billet de blog. Cet épisode montre bien le potentiel de l'archive des Shadow Brokers pour les cybercriminels, qui pourront s'inspirer des techniques made in NSA pour renforcer leur arsenal de menaces.

[A lire aussi : 10 questions pour comprendre l'affaire Shadow Brokers]

Signalons que Cisco a démarré la mise à jour de ses firewall ASA (vendus à plus d'un million d'unités dans le monde selon le constructeur), les utilisateurs sous les versions 7.2 à 8.7 étant appelés à migrer vers la mouture 9.1.7(9). Les entreprises qui font tourner des versions plus récentes (de 9.1 à 9.6) devraient bénéficier d'une mise à jour dans les jours qui viennent, assure le Californien dans un bulletin de sécurité.

Un exploit appelé à durer

La faille ciblée par ExtraBacon se loge dans le protocole SNMP (Simple Network Management Protocol) des Cisco ASA, Cisco PIX (une génération plus ancienne dont le support s'est arrêté en 2009) et du Cisco Firewall Services Module. Via un débordement de mémoire (buffer overflow), elle permet à un assaillant, armé de paquets SNMP spécialement conçus, de prendre le contrôle à distance des machines concernées. Pour exploiter la faille (CVE-2016-6366), et contrôler l'ensemble du trafic passant par le firewall, l'assaillant doit au préalable prendre la main sur un poste

possédant un accès à cet équipement ou dénicher un firewall mal configuré, sur lequel les accès sont mal gérés.

« *Beaucoup disent que les risques associés à cette attaque sont faibles parce que l'interface vulnérable n'est accessible que depuis la zone de management du réseau. Mais, dans de nombreux circonstances, ce n'est pas le cas et il faut aussi penser aux assaillants déjà présents sur le réseau* », explique Balint Varga-Perke. « *Comme nous parlons de logiciels embarqués (sur des firewalls et passerelles VPN, NDLR), les mises à jour ne sont pas toujours triviales et il n'existe pas de bon outil disponible pour détecter la compromission d'un pare-feu*, ajoute le chercheur en sécurité. *Compte tenu de tous ces éléments, nous prévoyons que cet exploit sera un outil de choix dans les années qui viennent pour les assaillants et pour les professionnels des tests de sécurité (pentesters) comme nous.* »

A lire aussi :

Juniper reconnaît (enfin) une faille mise au jour par les Shadow Brokers

Cisco et Fortinet valident le sérieux des Shadow Brokers, hackers de la NSA

Encore une autre faille 'made in NSA' pour Cisco