La liste des routeurs Cisco infectés par SYNful Knock s'allonge

FireEye a poursuivi son investigation sur l'infection qui touche certains routeurs Cisco. Si, la semaine dernière, le spécialiste des réponses aux incidents dénombrait 14 routeurs victimes de SYNful Knock dans quatre pays, leur nombre se compte en dizaines d'unités et leur présence s'étend à beaucoup plus de régions.

Les Etats-Unis les plus touchés

Rappelons que SYNful Knock est une version modifiée de IOS, le firmware signé Cisco qui pilote le routeur, probablement implémentée suite à l'obtention d'identifiants d'administration plus que par exploitation d'une éventuelle faille zero day. Une fois installé, SYNful Knock est persistant et peut évoluer au grès des stratégies des attaquants comme n'importe quel firmware. Il s'inscrit comme une potentielle porte d'entrée pour accéder au reste du réseau de l'entreprise. Les modèles de routeurs 1841, 2811 et 3825 de Cisco sont concernés. Ce sont généralement des appareils de gestion du trafic exploités par les succursales des entreprises ou les fournisseurs de services réseau managés.

Les experts de la filiale de Mandiant ont poursuivi leur travaux sur cette infection en utilisant l'outil Zmap de l'université du Michigan qui permet de sonder l'ensemble des adresses IPv4 du réseau à la recherche de SYNful Knock (selon une méthodologie décrite ici). Le résultat ne s'est pas fait attendre puisque 79 machines situées dans une vingtaine de pays ont répondu positivement à la requête. Aux précédents Ukraine, Philippines, Mexique et Inde s'ajoutent désormais la Russie (avec 8 routeurs infectés), le Liban (12 routeurs touchés) et, surtout, les Etats-Unis qui s'inscrivent comme le principal territoire concerné avec 25 routeurs affectés (et deux au Canada). Notons également que si, en Europe, l'Allemagne, le Royaume-Uni, la Pologne et la Turquie sont touchés (respectivement avec 2, 1, 1 et 2 routeurs affectés), la France est visiblement épargnée. Pour le moment du moins, la liste pouvant s'allonger au fil des recherches.

Résultats trompeurs

Mais ces résultats peuvent être trompeurs. Il est en effet difficile de savoir si la réponse des machines renvoie bien à la présence de SYNful Knock ou si elles ont été configurées pour répondre à la requête TCP de contrôle des paquets IP envoyés par les attaquants afin de tracer l'origine de leur attaque. Bref, certains routeurs ont peut-être été configurés pour servir de «pots de miel» et, à ce titre, renvoient un faux-positif.

Pour vérifier l'éventuelle présence de SYNful Knock sur les routeurs, FireEye conseille une approche en deux volets. A savoir un accès au routeur depuis le réseau de l'entreprise (Network-based indicators) et, quand c'est possible, un accès direct aux machines (Host-based indicators) pour exécuter les commandes de vérification localement. En cas d'infection, FireEye conseille de réinstaller une image saine de Cisco IOS. Et de vérifier l'état du reste du réseau, il va sans dire.

Lire également

Attaque sophistiquée sur les routeurs Cisco IOS

Une faille SSH béante sur les appliances réseau Cisco

Recrudescence d'attaques DDoS depuis de «vieux» routeurs

crédit photo © Aleksandr Stepanov – shutterstock