Sécurité : 14 routeurs Cisco victimes d'un firmware IOS corrompu

En août dernier, Cisco alertait sur de potentiels risques d'attaques de ses routeurs sous environnement IOS par remplacement du firmware de base. Aujourd'hui, il semble bien que l'alerte n'ait pas été appréhendée par tous les administrateurs réseaux et autres responsables sécurité.

Le spécialiste des réponses aux incidents Mandiant vient d'annoncer avoir décelé 14 routeurs infectés dans quatre pays : Ukraine, Philippines, Mexique et Inde. Si le nombre de machines Cisco corrompues semble anecdotique, rien ne dit que le périmètre des attaques est circonscrit à ces 14 routeurs.

Une porte d'entrée dans le réseau de l'entreprise

Selon la filiale de FireEye, les attaquants ont réussi à implémenter SYNful Knock, une version modifiée de l'image du firmware *« qui peut être utilisée pour maintenir la persistance dans le réseau de la victime »*, indique la firme de sécurité. Elle ajoute que le logiciel *« est personnalisable et modulaire par nature et peut donc être mis à jour une fois implanté. Même la présence de la porte dérobée peut être difficile à détecter car il utilise des paquets non-standard comme forme de pseudo-authentification »*. Une corruption d'autant plus sévère qu'elle est difficilement détectable, donc.

Mandiant ne pense pas que les attaquants s'appuient sur une vulnérabilité zero-day pour installer la *backdoor* mais passent plutôt par l'obtention des informations d'identification. Un vecteur d'attaque à l'époque souligné par le constructeur américain. *« Les attaquants doivent disposer des droits d'administration valides ou d'un accès physique au système pour parvenir à leurs fins »*, indiquait Cisco. Toujours est-il que *« la position du routeur dans le réseau en fait une cible idéale pour y pénétrer ou mener d'autres infections »*, souligne Mandiant. Selon la firme de sécurité, les modèles de routeur 1841, 2811 et 3825 de Cisco sont concernés. Des appareils de gestion du trafic souvent exploités par les succursales des entreprises ou les fournisseurs de services réseau managés.

Image persistante après redémarrage du routeur

Il est donc indispensable de se débarrasser de SYNful Knock le plus vite possible. Mandiant insiste sur le fait qu'il s'agit d'une modification de l'image du système IOS et que, à ce titre, elle se maintient de manière persistante dans l'environnement d'exécution, même après un redémarrage de la machine. *« Cependant*, soulignent les experts en sécurité, *les modules supplémentaires chargés par l'attaquant ne peuvent exister que dans la mémoire volatile du routeur et ne seront pas exploitables après redémarrage. »* Un moindre mal. Sur la page de son alerte, Mandiant décrit le fonctionnement du malware. Dans une prochaine contribution, la société de service indiquera comment détecter SYNful Knock. Dans tous les cas, *« il est évident maintenant que ce vecteur d'attaque est bien une réalité et devrait très probablement croître en popularité et en prévalence »*. Les administrateurs réseau sont doublement prévenus.

Lire également

Incidents télécoms en Europe : défaillances et attaques en hausse

Recrudescence d'attaques DDoS depuis de «vieux» routeurs

Failles de sécurité : le double jeu des gouvernements

crédit photo © Inara Prusakova – shutterstock