NSA : les matériels Cisco, Juniper et Huawei transformés en passoire

Avec quelques heures d'avance, Edward Snowden vient d'envoyer ses meilleurs vœux à l'industrie IT. En confirmant les pires soupçons qui pèsent sur certains des fournisseurs clefs des utilisateurs de technologies, le lanceur d'alertes risque fort de **bousculer les prévisions commerciales de grands noms de l'industrie**.

En appui d'un groupe spécialisé dans les opérations spéciales électroniques (Tailored Access Operations), la NSA disposerait en effet d'une **division chargé de trouver des failles** – ou de les acheter auprès de sociétés spécialisées ? – dans les principaux systèmes des grands fournisseurs du marché.

Cette **division, baptisée ANT**, met à la disposition de ses « clients » internes de la NSA un **catalogue de techniques** leur permettant de monter les opérations d'espionnage de l'agence. C'est ce catalogue de 50 pages (datant de 2008) qu'Edward Snowden a confié à Der Spiegel. Parmi les multiples éléments concernés par les techniques de ANT (des claviers, aux réseaux mobiles en passant les PC, les serveurs ou le protocole USB), la **porosité des principaux équipements réseaux** attire l'attention. Dans les documents que publie le journal allemand, sont notamment cités Juniper, Cisco et Huawei.

Alcatel épargné ?

Retrouver les noms des deux fournisseurs américains ne constitue qu'une demi-surprise, y voir celui de Huawei est un peu plus inattendu. Même s'il est vrai que Cisco a accusé son rival asiatique d'avoir illégalement copié son logiciel – donc potentiellement les défauts qu'il abrite. « *Pour les Etats-Unis, l'Asie est devenue une cible prioritaire économiquement, retrouver le nom de Huawei n'est donc pas si surprenant. En revanche, c'est une excellente nouvelle pour Alcatel, dont le nom n'est pas cité pour l'instant*, observe une source du secteur des télécoms interrogé par la rédaction. *Comme MacOS en son temps, qui n'attirait pas les pirates faute de base installée suffisante, la faible taille de l'équipementier français est, dans ce contexte, un atout.* »

Les routeurs de Juniper, eux, n'échappent pas à la sagacité des hackers de ANT. Via Stuccomontana, une technique ciblant le Bios des **routeurs de la classe T**, utilisés par les grands opérateurs de services mobiles, vidéos ou Cloud selon la description qu'en fait le fournisseur. Cette technique résiste aux mises à jour et elle est **supportée par les principales versions de Junos**, l'OS de Juniper basé sur FreeBSD. Notons que les **séries J** (pour les entreprises) et **M** (entreprises et fournisseurs de services) sont concernées par des techniques similaires, permettant d'assurer la résistance d'un logiciel d'écoute aux mises à jour. Même en cas de remplacement d'une carte Flash.

Pour **Huawei**, la vulnérabilité, baptisée Headwater, touche les routeurs du Chinois en implantant une **backdoor permanente dans la mémoire ROM** de démarrage de ces machines. Cet exploit permet la prise de contrôle à distance de ces routeurs.

Du côté des firewalls, le constat est encore moins brillant. Un des documents mis au jour dévoile ainsi une vulnérabilité, localisée dans le **firmware des firewalls PIX Series 500 et ASA** (Adaptive Security Appliance, modèles 5505, 5510, 5520, 5540 et 5550) **de Cisco**. Cet implant, baptisé Jetplow, « *modifie le système d'exploitation Cisco au démarrage* », écrit la division ANT dans le document publié sur Der Spiegel. Jetplow peut s'installer et être mis à jour à distance.

Juniper : hécatombe dans les firewalls

Chez **Juniper**, ANT utilise un exploit baptisé GourmetTrough , autre implant pour firmware, pour cibler **différents modèles de firewalls** (nsg5t, ns50, ns25, ISG 1000 et le document de promettre le « support » prochain de ssg140, ssg5 et ssg20). Un autre document évoque lui un autre programme malicieux, FeedTrough, ciblant **d'autres pare-feu issues de Netscreen**, société rachetée par Juniper (les modèles ns5xt, ns25, ns50, ns200, ns50), ainsi que le modèle ISG 1000, et permettant à d'autres logiciels d'écoute de la NSA de survivre aux redémarrages et même aux upgrades des systèmes hôtes. FeedTrough « *a été déployé sur de nombreuses plates-formes cibles* », s'enorgueillit la division ANT dans son document. Les **séries SSG 300 et 500**, autres firewalls de Juniper, ne sont pas épargnées, une technique permettant d'y installer un logiciel espion persistant et même une backdoor figure au catalogue de ANT.

Chez Huawei, ce sont les **firewalls Eudemon** qui sont porteurs d'une **backdoor cachée dans la ROM de démarrage** (via une technique appelée Halluxwater). La faille concerne les séries **200 et 500** (plutôt destinées aux entreprises), mais aussi **1000** (ciblant les opérateurs et fournisseurs de services). Bien entendu, Halluxwater survit aux mises à jour de l'OS et également à celles de la ROM.

Cisco réagit

Ce catalogue de « services » est certes daté de 2008 – certains des matériels cités ne sont plus vendus par leurs fabricants – mais on peut raisonnablement imaginer que ANT, **véritable SSII du hack**, a continué à le mettre à jour afin de s'adapter aux nouvelles versions de logiciels et matériels proposés par l'industrie. Certains de ces services de piratage sont associés à des coûts (probablement pour la refacturation interne). Sur les documents consultés par Der Spiegel, ceux-ci vont de zéro à 250 000 dollars.

Selon Der Spiegel, le catalogue ne mentionne aucune complicité active des fournisseurs cités. Cisco n'a pas tardé à réagir par le biais d'un billet posté par son directeur de la sécurité, **John Stewart**. Celui-ci précise que Cisco « *ne travaille avec aucun gouvernement afin d'affaiblir ses produits pour les rendre exploitables (dans le cadre d'écoutes, NDLR), pas plus que n'il n'implémente des portes dérobées dans ses produits* ». Une source chez un équipementier, interrogée par la rédaction, fait toutefois remarquer que Cisco, comme les autres fournisseurs, travaille avec les différents gouvernements afin de faciliter les interceptions de sécurité prévues dans le cadre légal. Autant d'informations précieuses que pourraient exploiter ensuite des services de renseignement avides d'accès rapides à des systèmes cibles ?

Crédit photo : © Sergej Khackimullin – Fotolia.com

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes