Les failles Juniper exploitées par le GCHQ britannique

Si l'on ignore officiellement qui est à l'origine de la backdoor installée depuis au moins 2008 dans ScreenOS de Juniper Networks, il se pourrait que le GCHQ ne soit pas étranger à son exploitation. Un document classé Top secret et daté de février 2011 indique que l'agence britannique de sécurité exploitait, avec l'accord de son homologue américaine la NSA, la vulnérabilité de l'OS de Juniper dans 13 différents modèles de firewall et VPN NetScreen de l'équipementier américain, révèle *The Intercept*. Les produits en question sont les modèles NS5gt, N25, NS500, NS204, NS208, NS5200, NS500, SSG5, SSG20, SSG140, ISG 1000 et ISG 2000.

Rappelons qu'un *« code non autorisé »* a été découvert dans les lignes de ScreenOS pour les versions 6.2.0r15 à 6.2.0r18 et 6.3.0r12 à 6.3.0r20 de l'OS à l'occasion d'un audit de ce dernier. L'équipementier a pudiquement révélé son existence à travers un récent bulletin de sécurité. La backdoor en question ouvre la possibilité de déchiffrer du trafic VPN en utilisant le générateur de nombres aléatoires Dual_EC_DRBG (pour générer la clé de chiffrement) dont les défaillances étaient notoires. Standardisé par l'Institut américain des standards et technologies (le NIST) en 2007, Dual_EC avait été fortement poussé par… la NSA. Déjà en 2013, RSA signalait la présence de la backdoor de la NSA dans ses produits BSafe. Le problème est que le générateur de clé made in NSA a probablement été récupéré par une autre organisation, gouvernementale ou non, et permettrait à son tour d'espionner les communications VPN des équipements de Juniper. Y compris les communications de la NSA dans un scénario qui n'est pas sans évoquer le classique arroseur arrosé.

La menace Juniper

Le document révélé par *The Intercept* et issu des informations dévoilées en masse par le lanceur d'alerte Edward Snowden, éclaire un peu les motivations des agences de sécurité nationale américaine et britannique à disposer d'un accès aux produits réseau de l'équipementier. *« Alors que Juniper n'est pas nécessairement leader dans une de ses activités [routeurs et sécurité, NDLR], c'est une entreprise importante avec une technologie avancée à travers plusieurs marchés majeurs d'un point de vue SIGNIT [*signals intelligence*, NDLR]*, peut-on y lire. *Juniper est au cœur de l'Internet pour des années dans nombre de pays en vertu de son statut de fournisseur de routeurs. [Et] dans quelques marchés de niche, dont un qui est très important en regard du SIGINT, Juniper est vu comme le concurrent [de Cisco] le plus apte à fournir des technologies SSL VPN. »* Autrement dit, l'équipementier présent sur les marchés occidentaux comme asiatiques s'inscrit comme un acteur incontournable pour les grandes oreilles du GCHQ (et de la NSA).

Car si Juniper est une «*cible*», c'est aussi une *« menace »*, indique l'auteur du document de l'agence britannique. *« La menace vient des investissements et l'accentuation de Juniper à vouloir être un leader de la sécurité. Si la communauté SIGINT échoue [à contrôler l'accès aux équipements réseau], il faudra des années avant de retrouver une capacité d'accès à un pare-feu ou routeur Juniper. »*

Depuis 2007 ?

En apportant son récent correctif, l'équipementier vient-il de mettre indirectement cette menace à exécution ? Pas sûr. La NSA ou le GCHQ ont pu, depuis, trouver d'autres moyens pour conserver un accès aux firewalls et routeurs de l'équipementier américain. Toujours est-il que, dans sa réponse à *The Intercept*, l'entreprise de Sunnyvale se défend de toute collaboration avec la NSA. *« Intégrer intentionnellement des backdoors qui pourraient compromettre nos produits ou mettre la sécurité de nos clients en péril est contre la politique de Juniper. En outre, notre politique s'oppose à travailler avec des tiers pour introduire des vulnérabilités dans nos produits. »* Une déclaration contraire eut pour le moins été étonnante.

Le document mis en exergue par Glenn Greenwald, le journaliste à l'origine des révélations d'Edward Snowden, est par ailleurs à rapprocher d'un article de 2013 du *Spiegel* qui pointait un programme de la NSA baptisé FEEDTHROUGH visant les firewall de Juniper de la gamme Netscreen sur la base d'un document daté, lui, de 2007.

Il n'en reste pas moins que, bientôt peut-être, les agences de sécurité n'auront nullement besoin de se cacher pour avoir accès aux contenus qui circulent dans les réseaux des opérateurs. Des Etats-Unis au Royaume-Uni en passant par la France ou la Chine, l'idée de mettre en place de backdoor dans les équipements réseau est aujourd'hui discutée dans des projets de lois visant à lutter contre le terrorisme. Avec le risque que l'usage de ces backdoor soit détourné à d'autres fins.

Lire également
Faille Juniper : les hackers sont déjà à l'affût
Juniper : une backdoor made in NSA… récupérée par une organisation inconnue
Backdoor ou erreur de code dans les firewall de Juniper

Ken Wolter / Shutterstock.com