BlackNurse : un déni de service à bas volume ciblant les firewalls

C'est une attaque au parfum franchement vintage mais à l'efficacité redoutable. Baptisée BlackNurse, cette technique, exploitant l'envoi de paquets ICMP (Internet Control Message Protocol, utilisé par envoyer et recevoir des messages d'erreur), s'avère pertinente contre des firewalls modernes, conçus par Cisco, Palo Alto, SonicWall ou Zyxel, selon le centre opérationnel de sécurité (SOC) de l'opérateur danois TDC.

Entre la mi-2014 et la mi-2016, les chercheurs de TDC disent avoir observé au moins 95 attaques ICMP ciblant les clients protégés par le SOC. Parmi celles-ci, *« l'attaque BlackNurse a attiré notre attention, parce que nous avons observé, dans notre solution anti-DDoS, que même si le trafic et le nombre de paquets par seconde étaient faibles, cette technique pouvait maintenir hors service les opérations de nos clients. Y compris ceux possédant des liens remontant importants et des firewalls de classe entreprise* », écrivent ces spécialistes de la lutte anti-DoS (déni de service). Pour qui l'attaque possède donc un potentiel de nuisance important, l'opérateur expliquant que 1,7 million d'équipements répondent à un ping ICMP sur le seul sol danois.

15 à 18 Mbit/s seulement

L'attaque mise en évidence par l'opérateur danois est toutefois différente de celles ayant cours dans les années 90 et qui consistaient à saturer les équipements avec des pings ICMP (type 8). BlackNurse s'appuie sur une saturation des firewalls avec des paquets indiquant que la destination et le port sont inaccessibles (type 3). Un choix qui rend l'attaque efficace même à des bandes passantes très faibles en comparaison des attaques par déni de service classiques. Selon TDC, 15 à 18 Mbit/s suffisent (à comparer aux attaques par DDoS menées depuis des objets connectés détournés qui, ces dernières semaines, ont dépassé les 1 Tbit/s). Soit seulement 40 000 à 50 000 paquets par seconde. « *Et cela importe peu que vous ayez une connexion Internet à 1 Gbit/s. L'impact que nous avons mesuré sur différents firewalls se traduit souvent par une charge processeur importante sur les machines* », écrivent les chercheurs du SOC.

Un laptop suffit à BlackNurse

Ces derniers livrent également des indications permettant de tester la vulnérabilité des équipements. Ce qui permet, au passage, de prendre conscience de l'ampleur du problème, puisqu'un seul ordinateur portable peut produire un débit de 180 Mbit/s d'attaques BlackNurse avec l'entrée de quelques commandes. Un seul smartphone Nexus 6 génère, lui, l'équivalent de 9,5 Mbit/s de paquets ICMP de type 3. Insuffisant pour bloquer une entreprise, selon les calculs de l'opérateur. Mais deux smartphones ciblant la même IP pourraient bien y parvenir.

La liste des matériels concernés figure en bas d'un billet de blog de la société spécialisée en sécurité Netresec, qui a collaboré avec TDC sur ces travaux. Palo Alto assure toutefois que ses machines ne sont vulnérables que dans des cas « *très spécifiques* », violant les bonnes pratiques.

Cisco, de son côté, considère qu'il ne s'agit pas d'un problème de sécurité, selon un billet du SANS Institute. Même si le constructeur ne s'est pas expliqué sur cette assertion, il est probable qu'il renvoie ses clients à la configuration de leurs firewalls. Contrer les attaques BlackNurse revient en effet à bloquer les paquets ICMP suspects ou, au minimum, à limiter le trafic sur ces paquets.

Mise à jour le 16/11 à 11h45 : suite à notre article, SonicWall nous envoie la précision suivante : « *nos tests ont montré que le pare-feu SonicWall n'était pas vulnérable (à l'attaque BlackNurse, NDLR) lorsque la protection du ping flood (ICMP) était activée* ».

A lire aussi :

Des attaques DDoS de plus de 10 Tbit/s en vue ?

DDoS : Le botnet IoT Mirai a bien participé au raid contre Dyn

FPGA : l'arme secrète d'OVH pour parer les attaques DDoS