Sécurité : l'IoT reste un risque majeur pour les attaques DDoS

L'IoT demeure un facteur de risque majeur pour les attaques DDoS. Cisco confirme la tendance dans l'édition 2018 de son « Cybersecurity Report ».

Historiquement concentrées sur la couche réseau, les attaques contre l'IoT se déplacent progressivement vers la couche applicative et exploitent des mécanismes d'amplification.

Cette croissance des attaques DDoS par réflexion inquiètent d'autant plus les experts qu'un tiers des organisations interrogées se déclarent incapables d'y faire face. A l'automne 2016, un botnet nommé Mirai avait été conçu pour prendre le contrôle d'objets connectés faiblement sécurisés, typiquement, ceux dont on n'a pas changé le mot de passe par défaut. Il avait notamment été exploité dans le cadre d'une attaque par déni de service distribué (DDoS) contre OVH, dont les serveurs avaient été mis à mal par les requêtes simultanées de plus de 100 000 caméras IP.

DNS, NTP et SSDP

Dans son rapport, Cisco détaille les trois cas d'attaque DDoS par réflexion les plus utilisés.

>Réflexion DNS : les appareils connectés, dont les attaquants ont pris le contrôle, sont utilisés pour envoyer des requêtes simples à des serveurs qui renvoient des réponses beaucoup jusqu'à 80 fois plus lourdes… vers l'adresse IP des machines ciblées. Cette technique d'attaque
permet à un petit Botnet (qui comprend peu de machines) d'inonder sa cible d'un énorme volume de requêtes.

> Réflexion NTP : ce type d'attaque concerne les serveurs NTP qui synchronisent les horloges locales. Via la commande « get monlist », qui renvoie la liste des 600 derniers hôtes connectés, l'attaquant envoie la requête pour saturer les serveurs.

> Réflexion SSDP : Cette attaque exploite le protocole Simple Service Discovery
(SSDP) qui permet à des appareils – caméras, imprimantes – à la norme UPnP (Universal Plug and Play) de se référencer sur le réseau auquel ils sont connectés. Lorsqu'une machine reçoit le message envoyé à ces fins, elle demande une description complète des services que propose l'appareil UPnP. Les attaquants utilisent cette réponse, multipliée par le nombre d'appareils, pour cibler les serveurs cible.