Quand le protocole CLDAP amplifie les DDoS

A l'heure de la rentrée des vacances de Pâques, l'écosystème des attaques DDoS accueille un nouvel élément : le protocole CLDAP. Ce dernier est l'acronyme de Connection-less Lightweight Directory Access Protocol. Il est défini par la RFC 1798 remplacée par la RFC 3352. Il s'agit d'une alternative au protocole LDAP qui, tout comme lui, permet l'interrogation et la modification des services d'annuaire. Les deux protocoles utilisent le port 389. Mais LDAP passe en TCP, alors que CLDAP fonctionne en mode UDP.

En octobre 2016, Akamai a commencé à détecter des attaques DDoS via un protocole inconnu qui s'est révélé être CLDAP. Cette découverte était concomitante avec celle de l'éditeur Corero sur des attaques basées sur LDAP. Pour Akamai, les deux types d'offensives étaient menés de manière similaire avec la volonté d'amplifier les attaques. Concrètement, un attaquant envoie une requête LDAP ou CLDAP à un serveur LDAP avec une adresse IP falsifiée. La victime, en répondant à l'adresse usurpée, envoie du trafic réseau intempestif vers la cible du pirate. On appelle cela la réflexion, car l'attaquant envoie plusieurs milliers de requêtes réfléchies vers la cible de l'attaque.

Un fort facteur d'amplification

Les attaques DDoS par LDAP ou CLDAP sont amplifiées, c'est-à-dire que le paquet géré par le serveur LDAP s'agrandit pendant le traitement. Habituellement sur d'autres protocoles, le facteur d'amplification est de 10, ce qui signifie qu'un paquet de 1 octet est envoyé sur le serveur vulnérable et amplifié à 10 octets. Dans le cas de LDAP, Corero estime que le facteur d'amplification est de 46 en moyenne avec des poussées jusqu'à 55. En ce qui concerne les attaques CLDAP, le facteur est plus puissant avec 56 en moyenne et 70 en crête.

Dans son rapport Akamai indique que depuis le 14 octobre 2016, date de la première attaque DDoS sur CLDAP, il y a eu 50 charges au total, provenant de 7629 réflecteurs CLDAP uniques, c'est-à-dire des serveurs LDAP avec le port 389 exposés sur Internet. Le site Shodan, qui répertorie les connexions de la Toile, considère qu'il y a actuellement 250 000 terminaux dont le port 389 est exposé sur Internet. La plus grande offensive a affiché un pic de 24 Gbit/s, suffisant pour faire tomber un site Web. Les experts d'Akamai considèrent que les attaquants ont voulu tester cette technique de réflexion et d'amplification. Avec dans l'optique de proposer cette procédure dans un portefeuille de DDoS as Service. Il faut donc s'attendre à voir les attaques par saturation via LDAP et CLDAP augmenter et se perfectionner.

A lire aussi :

Les attaques DDoS, l'autre machine à cash des cybercriminels

Augmentation de 140% des attaques DDoS à plus de 100 Gbit/s en 2016