# Après DNS et NTP, les DDoS jouent sur TFTP

Des chercheurs de l'université Napier à Edimbourg ont découvert un nouveau vecteur pour l'amplification des attaques en déni de service : le protocole TFTP. Le Trivial File Transfer Protocol pourrait être exploité pour lancer des attaques DDoS. Cette version simplifiée du FTP est généralement utilisée dans les réseaux internes pour déployer fréquemment des images d'OS vers les terminaux. Cisco l'utilise par exemple pour mettre à jour ses téléphones VoIP. Près de 600 000 serveurs TFTP publics sont aujourd'hui en service. Et les chercheurs ont découvert que le TFTP offre un facteur d'amplification plus élevé que les autres protocoles Internet.

« *La vulnérabilité découverte pourrait permettre à des pirates d'utiliser ces serveurs ouverts au public pour amplifier leur trafic, de manière similaire à d'autres attaques DDoS par réflexion comme l'amplification de DNS,* déclare Boris Sieklik, l'un des chercheurs de Napier, à nos confrères de *The Register*. *Si toutes les conditions sont remplies ce trafic peut être appliqué jusqu'à 60 fois le volume initial.* » On peut d'ailleurs s'étonner qu'une telle capacité d'attaque n'ait, apparemment selon les universitaires, par encore été exploitée par les cybercriminel. Jusqu'à quand ?

S'il est exploité, le TFTP ne sera pas le premier protocole réseau permettant de lancer des attaques DDoS par amplification. Il rejoindra des cas similaires précédemment constatés avec les protocoles DNS (Domain Name System) et NTP (Network Time Protocol). Une mauvaise intégration et/ou un paramétrage inadéquat de ces protocoles sur des services de sites ont permis de lancer des attaques DDoS ces dernières années. Ces attaques s'appuient particulièrement sur des méthodes de réflexion des paquets. Elles consistent à envoyer une requête volontairement mal formulée avec la référence du site visé pour générer une réponse souvent plus lourde que la demande initiale. L'envoi massivement répété de ce type de réponse peut ainsi faire tomber le site web de la cible référencé dans la requête. Les entreprises ont donc tout intérêt à soigner l'intégration de ces protocoles pour éviter les catastrophes.

---

**Lire également**

Une faille BIND ouvre la voie aux attaques DDoS des serveurs DNS
Failles NTP : la machine à détraquer le temps menace aussi le chiffrement
Une vulnérabilité enrôle massivement pour amplifier les attaques DDoS

**Crédit Photo : Lightspring-Shutterstock**