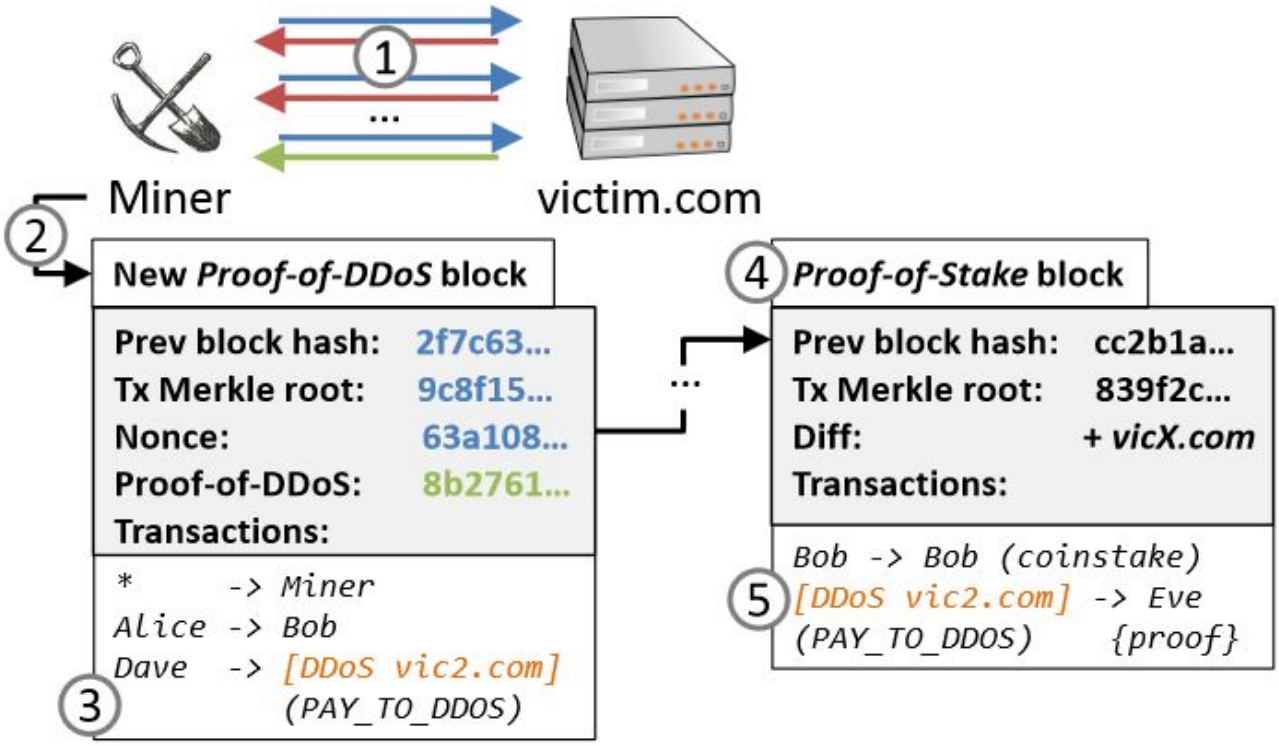
Bientôt un Bitcoin pour rémunérer les attaques DDoS ?

Dans une monnaie comme le Bitcoin, les mineurs mettent à disposition du système de la puissance de calcul, employée pour gérer et sécuriser la monnaie électronique, contre une récompense financière, elle-même en Bitcoin. Lors de la conférence Usenix, qui se tenait la semaine dernière aux Etats-Unis, deux chercheurs, Eric Wustrow, de l'université du Colorado, et Benjamin Vandersloot, de l'université du Michigan, imaginent une nouvelle forme de monnaie électronique, où les mineurs sont récompensés pour leur participation… à des attaques par déni de service distribué (DDoS, consistant à inonder un serveur de requêtes empêchant les utilisateurs légitimes d'y accéder).

« *Nous proposons un concept permettant à des mineurs de prouver qu'ils ont participé à une attaque par déni de service – ou DDoS – contre une cible déterminée*, écrivent les deux chercheurs. *Les mineurs sont incités à envoyer et recevoir des grands volumes de trafic réseau vers et en provenance des cibles afin de prouver leur activité. Comme avec d'autres monnaies basées sur le chiffrement, ces preuves peuvent être vérifiées à bas coût par des tiers et les mineurs reçoivent une récompense pour leur travail.* » Les deux chercheurs imaginent par exemple des rémunérations en Bitcoin ou dans d'autres monnaies (virtuelles ou non). « *Ce qui permettrait aux possesseurs de botnet et à d'autres de collecter directement des revenus pour leur participation à des attaques DDoS* », ajoutent-ils.

TLS 1.2 crée la preuve de la connexion

Leur recherche, qui se limite à une démonstration de faisabilité, pointe surtout une fonctionnalité de TLS 1.2, autorisant précisément la création d'une monnaie du DDoS. Le concept de ce 'DDoSCoin' exploite en effet les réponses qu'envoient les serveurs après la connexion d'un client. « *Dans les versions modernes de TLS, le serveur signe un paramètre fourni par les clients pendant l'initialisation de la connexion (handshake), ainsi que des valeurs fournies par le serveur utilisées lors de l'échange de clefs* », notent Eric Wustrow et Benjamin Vandersloot. Bref, avec cette version du protocole de chiffrement, un client peut prouver à d'autres qu'il s'est bien connecté à tel serveur. « *Et la valeur signée retournée par le serveur n'est pas prédictible par le client et se voit distribuée de manière aléatoire* », ajoutent les chercheurs. Donc le système paraît sécurisé contre les risques de fraude… Publiée en 2008, TLS 1.2 est employé par 56 % du premier million de sites Web recensés par Alexa.



Ce détournement de TLS (Transport Layer Security, le successeur de SSL pour le chiffrement des échanges sur Internet) pourrait ouvrir la voie à une nouvelle étape dans la professionnalisation des DDoS. Si ce type d'attaques est déjà vendu clef en main par des organisations criminelles, celles-ci utilisent la plupart du temps la duperie pour enrôler des machines sur leurs botnets. Les attaques sont en pratique menées par les PC et serveurs d'internautes enrôlés à leur insu via un malware. La naissance d'une crypto-monnaie dédiée pourrait décupler le nombre de participants aux botnets d'attaques DDoS.

A lire aussi :

Les attaques DDoS en hausse de 40% au 4e trimestre 2015

Attaques DDoS : bluffer suffit pour bien gagner

Après DNS et NTP, les DDoS jouent sur TFTP

Crédit Photo : Andrey Armyagov-Shutterstock