Les attaques DRDOS peuvent se propager via les clients BitTorrent | Le Net Expert Informatique

Les attaques DRDOS peuvent se propager via les clients BitTorrent

L'attaque DRDOS (Distributed Reflective Denial of Service) est une variante du DDoS, mais elle est plus puissante et elle peut se propager sur de nombreux protocoles incluant ceux du BitTorrent. Florian Adamsky de la City University London propose un article sur le potentiel nuisible du DRDOS concernant les protocoles BitTorrent.

La plupart connaissent les attaques DDoS, mais le DRDOS est un peu différent. Dans une attaque DDoS, le pirate contrôle un ensemble de machines zombies pour attaquer la cible. Dans une DRDOS, le pirate envoie le trafic à un réseau légitime (appelé le réflecteur) qui transmet ensuite le trafic à la victime. Le trafic qui est envoyé au réflecteur est modifié pour que pour l'adresse IP de la victime soit utilisé plutôt que le paquet d'origine. Et quand le réflecteur respecte les normes habituelles des protocoles internet pour établir la connexion, alors tout le trafic est balancé vers la victime. Et étant donné que cela implique d'envoyer une énorme quantité de trafic vers un réflecteur, les pirates ont trouvé le moyen de l'utiliser pour amplifier le trafic. Les attaques DRDOS peuvent être utilisées vers les protocoles TCP, DNS et NTP. Mais l'article d'Adamsky démontre aussi que le DRDOS peut être exploité avec de nombreux protocoles du BitTorrent.

Les protocoles uTP, MSE, DHT et BTSync sont vulnérables aux attaques DRDOS

Selon Adamsky, les protocoles BitTorrent affectés sont l'uTP (Micro Transport Protocol), le DHT (Distributed Hash Table) et le MSE (Message Stream Encryption). Ces protocoles sont intégrés en natif sur les clients de Torrent BitTorrent, uTorrent et Vuze. De plus, le protocole de synchronisation BTSync, qui est utilisé avec BitTorrent Sync, est également vulnérable. Florian Adamsky a démontré que les tests permettaient d'amplifier le trafic de 50 à 120 fois sur la norme BTSync.

Les attaques DRDOS sur les protocoles BitTorrent sont indétectables par les pare-feu

Mais la mauvaise nouvelle ne s'arrête pas là. En plus d'amplifier considérablement l'attaque, le DRDOS sur BitTorrent ne peut pas être détecté avec des pare-feu standard à cause de l'utilisation de ports dynamiques et du chiffrement pendant les échanges de données sur ces protocoles. Pour contrer ce type d'attaque, il faudrait utiliser une solution telle que DPI (Deep Packet Inspection) qui est trop coûteuse pour la majorité des infrastructures. BitTorrent a corrigé certains de ces problèmes avec sa version en bêta, mais Vuze et BitTorrent travaillent encore pour colmater les brèches qui permettent d'exploiter le DRDOS.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://actualite.housseniawriting.com/technologie/2015/08/16/les-attaques-drdos-peuvent-se-propager-via-les-clients-bittorrent/7227/
Par Houssen Moshinaly