Failles NTP : la machine à détraquer le temps menace aussi le chiffrement

Dérégler l'horloge de l'Internet ? C'est en somme le tour de passe-passe que dévoilent des chercheurs dans un article publié la semaine dernière : ce dernier met en exergue les failles du Network Time Protocol (NTP), le (très ancien) protocole de synchronisation qui permet de caler l'horloge locale d'ordinateurs sur une référence, un serveur présent sur le réseau. Or, ces connexions entre clients et serveurs sont en pratique rarement chiffrées – même si le protocole l'autorise – laissant la porte ouverte à des attaques de type Man-in-the-Middle où un serveur 'pirate' vient s'intercaler dans la communication. Une façon de modifier l'horloge des systèmes clients. Quelle importance pourrait-on penser en première approche, puisqu'il ne s'agit que d'une simple modification de l'heure ?

« *NTP se cache en arrière-plan de bien des systèmes*, écrivent les 4 chercheurs issus de l'université de Boston (Massachussetts). *Quand NTP échoue sur un système, de nombreuses applications de ce système peuvent à leur tour planter, toutes en même temps* ». Tout sauf de la science-fiction, ajoutent les auteurs de l'étude. En 2012, deux serveurs NTP de la marine américaine, la Navy, sont remontés dans le temps de 12 années, provoquant des pannes sur une multitude de systèmes, comme l'authentification Active Directory, des autocommutateurs ou des routeurs. Qui plus est, ce type d'attaques DDoS un peu originales peuvent être menées sans que l'assaillant ait à monitorer le trafic entre les clients et le serveur NTP.

La faille Heartbleed reloaded

C'est par exemple le cas de l'attaque dite du 'baiser-de-la-mort' (**Kiss-o'-Death** ou KoD), qui consiste à envoyer quelques paquets à chaque client NTP pour que ceux-ci cessent de demander la mise à jour de leur horloge. « *Comme l'assaillant ne doit envoyer que quelques paquets à chaque victime, des outils de scan réseau standards (nmap, zmap) peuvent être adaptés pour lancer très rapidement l'attaque, en masse, sur la plupart des clients ntpd (le composant implémentant NTP, NDLR) présents sur Internet* », explique Sharon Goldberg, un des chercheurs.

Au-delà de ces formes d'attaque visant à causer des interruptions de service ou des pannes, les chercheurs imaginent des scénarios d'attaque bien plus sophistiqués. Exemple avec les **certificats TLS** (utilisés pour le HTTPS) : en faisant monter des systèmes dans 'la machine à remonter le temps' du NTP, un assaillant peut les amener à **accepter des certificats révoqués**. Par exemple, en ramenant les horloges avant la mi-2014, époque où plus de 100 000 certificats TLS ont été rayés de la carte en raison de la faille Heartbleed. Même constat avec DNSSEC, le protocole qui fournit l'authentification sur les données DNS (Domain Name System, le système de correspondance entre URL et adresses IP). En se servant de la durée de vie très faible des certificats du DNSSEC, un assaillant peut, en utilisant NTP, faire tomber toutes les connexions aux domaines sécurisés par DNSSEC. Ces scénarios d'attaque, mariant manipulation de l'horloge et durée de vie des certificats, peuvent aussi être employés contre les services Cloud, comme Amazon S3 ou Dropbox. L'idée ? Se baser sur les limites d'horodatage que mettent en place ces services pour empêcher des accès non

autorisés, pour barrer l'accès aux utilisateurs légitimes ou – justement – ménager des accès non autorisés en se projetant quelques minutes en arrière, au moment où une authentification devenue depuis obsolète était encore valide.

Profiter du reboot pour faire un saut dans le temps

Si ces scénarios sophistiqués sont évidemment inquiétants, reste à savoir s'ils sont utilisables en pratique. D'abord, un changement brutal dans l'horloge risque fort de provoquer des erreurs dans les systèmes d'exploitation ou les applications des clients ciblés. Rendant toute extraction de données illusoire. Ensuite, le protocole NTP prévoit normalement que les clients rejettent des modifications temporelles de plus de 1000 secondes (environ 16 minutes). Sauf que les chercheurs de l'université de Boston expliquent que deux méthodes permettent de contourner cette sécurité. D'abord, via une série de modifications de l'horloge, chacune inférieure à la limite prévue. Entre deux modifications, un intervalle de 5 minutes doit toutefois être respecté (sur ntpd v4.2.8). Conséquence : avancer ou reculer l'horloge d'un client d'un an prendrait… 114 jours ! Les chercheurs de l'université de Boston présentent donc une méthode plus efficace, exploitant la capacité des systèmes à accepter n'importe quel saut dans le temps au moment du reboot.

Certaines des attaques évoquées par les chercheurs ne surprendront pas les spécialistes. En août dernier, le chercheur Jose Delvi en présentait déjà certaines. Ce dernier a même réalisé un outil, un serveur NTP permettant de tester ces méthodes, baptisé Delorean en hommage à la voiture des voyages spatio-temporels du film Retour vers le futur. Jose Delvi a publié le 21 octobre 2015, le jour choisi par Marty McFly, le héros du film, pour son second voyage dans le futur, un billet de blog, dans lequel il fait le constat suivant : « *tous les vendeurs d'OS que j'ai testés utilisent les Network Time Protocol (NTP) afin de garder les horloges internes à l'heure juste, ce qui est très important pour certains protocoles d'authentification notamment. La plupart d'entre eux ne déploient pas ce service de façon sécurisée, le rendant vulnérable à des attaques de type Man-in-the-Middle* ».

Amplificateur de DDoS

De leur côté, les chercheurs de l'université de Boston ont publié une page de diagnostic et de recommandations concernant tant les serveurs que les clients NTP. Ils recommandent notamment l'usage de NTP v4.2.8p4 (qui élimine le KoD) ainsi que diverses autres options de configuration censées limiter la portée ou la variété des attaques possibles contre le protocole.

Notons que la vulnérabilité de NTP avait également été mise en évidence début 2014, quand des assaillants avaient utilisé le protocole pour amplifier une attaque DDoS contre des sites de jeu en ligne. Une requête aux serveurs NTP semblant émaner de ces sites renvoyait un message jusqu'à

58 fois plus volumineux, décuplant ainsi les capacités des assaillants et saturant les systèmes ciblés.

A lire aussi :

Apple corrige automatiquement des failles dans NTP pour Mac OS X
Comment la NSA a (probablement) cassé le chiffrement par VPN
SHA-1 : un algorithme clef du chiffrement HTTPS n'est plus sécurisé

Crédit photo : Alex Yeung / Shutterstock