Scan de ports TCP : comment la NSA et le GCHQ préparent leurs attaques

Selon le journal allemand Heise, le service de renseignement britannique, le GCHQ, a bâti **une base de données des ports TCP ouverts** sur les serveurs connectés à Internet. Des ports ouverts pour des services usuels comme HTTP ou FTP mais également pour des protocoles plus spécialisés SSH (accès à distance) et SNMP (administration de réseaux). La construction de cette base, qui fait partie d'**un programme secret baptisé Hacienda**, passe par le scan d'adresses IP réparties dans le monde entier, des opérations réalisées fréquemment à l'échelle d'un pays. Cette liste, qui peut servir de point de départ pour mener des cyberattaques, est partagée, via un protocole d'échange de données sécurisé, avec les autres services secrets membres de l'alliance dite Five Eyes : la NSA américaine bien sûr, mais aussi ses homologues en Australie, au Canada et en Nouvelle-Zélande.

Les documents secrets que s'est procurés Heise, émanant du GCHQ, de la NSA et du CSEC (Communications Security Establishment of Canada), montrent que le scan de ports avait, en 2009, été pratiqué **contre 27 pays entiers** (pays dont les noms ne sont pas précisés). S'y ajoutent 5 autres nations qui n'ont subi qu'un scan partiel. L'existence de ce programme ne constitue pas réellement une surprise pour les spécialistes. Depuis 2013, un outil de scan automatique de ports, Zmap, est largement disponible. Il parvient à **parcourir l'espace mondial des adresses IPv4 en moins d'une heure** depuis un simple ordinateur personnel, signalent nos confrères.

Scanner les ports : une reconnaissance avant l'attaque

En plus des informations sur les ports ouverts, le GCHQ récolte également d'autres données pour nourrir sa base, comme les informations dites de bannière qu'une application envoie par défaut à un client qui se connecte au port auquel elle est associée. On y trouve notamment des indications détaillées sur le système et l'application, comme **des numéros de versions**. Ces données se révèlent évidemment très utiles en vue d'opérations offensives, la connaissance des versions installées permettant d'exploiter des vulnérabilités. Notamment des failles zero day dont la NSA, partenaire du GCHQ, s'est révélée friande.

Notons d'ailleurs que les slides publiés par Heise ne se limitent pas à décrire un processus de construction d'une base de données de ports ouverts sur les serveurs TCP dans le monde. C'est plutôt un processus complet de piratage qui est mis au jour, processus commençant par une phase de reconnaissance dans laquelle Hacienda jour un rôle clef. Mais qui passe ensuite par **l'infection des cibles, leur pilotage à distance** via des serveurs de contrôle / commande **et l'exfiltration d'informations**. Rappelons que le GCHQ est accusé d'avoir piraté le réseau de l'opérateur belge Belgacom, victime d'une intrusion découverte en septembre 2013. Selon un document d'Edward Snowden, pas moins de 50 000 réseaux étaient compromis en 2012 par l'agence de Fort Meade et ses partenaires des Five Eyes.

La base de données Hacienda joue également un rôle clef dans l'installation de relais, des serveurs

infectés permettant de **dissimuler l'origine d'une attaque ou la destination de documents volés**. Objectif des Five Eyes : disposer d'une « infrastructure cachée » permettant de perpétrer des attaques sans se dévoiler, celles-ci semblant alors émaner d'autres pays. Un programme baptisé Landmark consiste, plusieurs fois dans l'année, à gagner le contrôle d'autant de machines que possible, pour peu que celles-ci ne se situent pas dans les pays membres de l'alliance Five Eyes (à noter que les pays alliés ne semblent pas bénéficier d'un traitement de faveur). Par exemple, en février 2010, une équipe de 24 spécialistes a été capable, en une seule journée de travail de rassembler plus de 3 000 serveurs susceptibles de masquer les activités illégales des Five Eyes. Comme dans d'autres programmes de la NSA dévoilés par les documents dérobés par Edward Snowden, le programme Hacienda et ses ramifications ont visiblement bénéficié de fonctions favorisant une automatisation croissante des processus.

Authentifier le client avant de lui donner de l'information

Heise ne précise pas si les documents analysés proviennent du lanceur d'alerte réfugié en Russie et toujours activement recherché par les autorités américaines. Rappelons que les Etats-Unis soupçonnent l'existence d'une seconde taupe au sein de ses services secrets. Laura Poitras, une des deux journalistes qui ont été les premiers à être en contact avec Edward Snowden et auxquels l'ex-informaticien de la NSA a remis ses documents, a participé à l'enquête de Heise.

Le scan automatique de ports est grandement facilité par **le laxisme du protocole TCP**, au sein duquel un serveur fournit de l'information à un client avant même de vérifier si ce dernier est habilité à exploiter ledit service. Les auteurs de l'article donnent d'ailleurs une méthode pour échapper à Hacienda et au scan automatique de ports orchestré par les Five Eyes. Baptisée « port knocking », celle-ci minimise l'empreinte visible d'un serveur TCP. Avec cette technique, un client doit en effet envoyer un paquet préalable, avant que le port ne se déclare comme ouvert. Même s'il est susceptible de ralentir les espions, le « port knocking » ne saurait les arrêter, jugent toutefois nos confrères. Qui suggèrent une amélioration de cette technique.

Celle-ci, baptisée TCP Stealth, repose sur **l'utilisation d'un token d'authentification par les clients TCP**. Ce qui permettrait aux serveurs de masquer leur présence aux clients non autorisés (comme les scanners de ports). Cette méthode, développée pour Linux et mise au point par Jacob Appelbaum (projet Tor) et par deux chercheurs de l'université de Munich (avec la participation d'un membre de Microsoft Allemagne), est aujourd'hui proposée comme futur standard à l'IETF (Internet Engineering Task Force).

A lire aussi

Espionnage de la NSA : les 8 leçons d'Edward Snowden