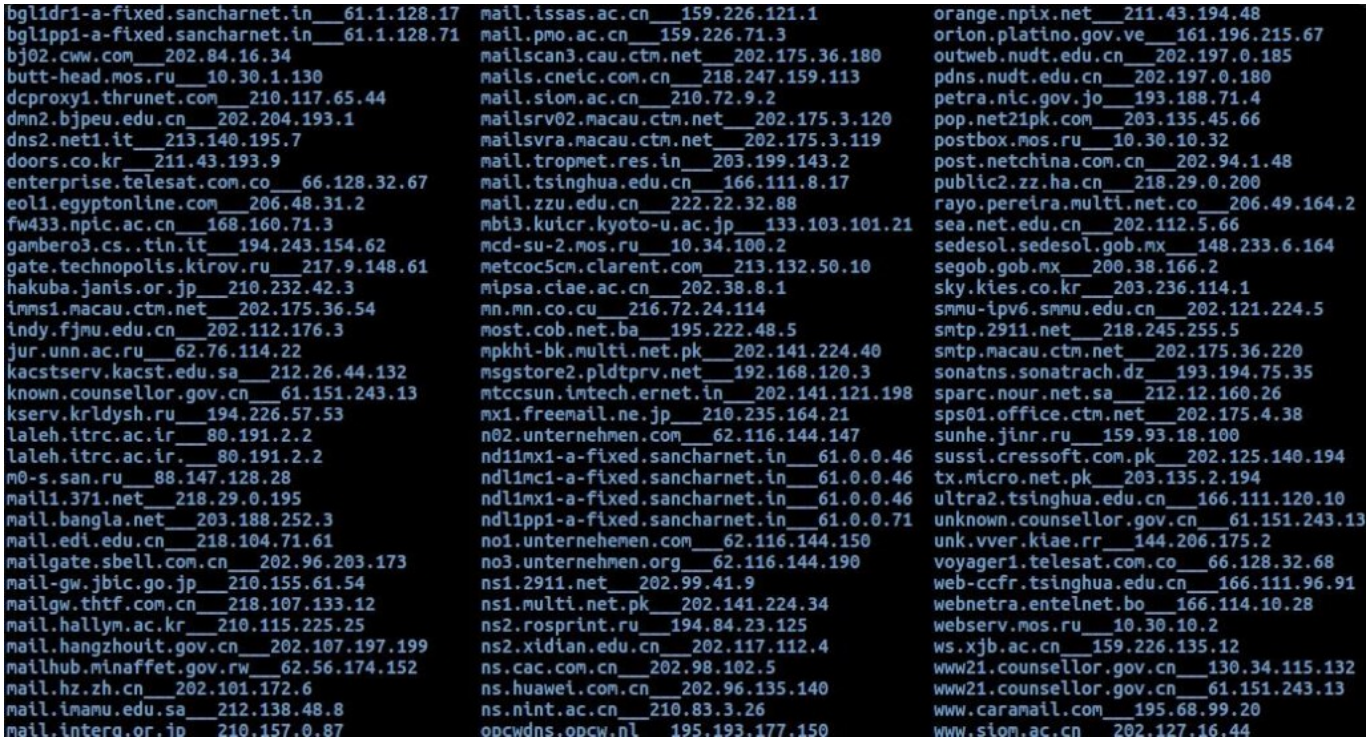
Spécial Halloween : la liste des adresses IP utilisées par la NSA pour ses piratages

Pour Halloween, les Shadow Brokers réservent une nouvelle surprise au gouvernement américain. Le groupe de pirates, inconnu jusqu'en août dernier et qui affirme avoir hacké la NSA, vient en effet de mettre en ligne une archive ainsi qu'un message sur le site de blogging Medium. Ce message est signé avec la même clef PGP que celle employée pour les précédentes communications des Shadow Brokers.

La série de données publiées renferme 300 fichiers ou dossiers, correspondant tous à différents domaines et adresses IP localisées un peu partout dans le monde, avec une concentration importante en Chine, en Corée du Sud, au Japon mais aussi en Espagne ou en Allemagne. Selon une analyse d'un chercheur indépendant, ce sont au total 306 noms de domaines et 352 adresses IP, disséminées dans 49 pays, qui y figurent. En France, signalons la présence de plusieurs domaines appartenant à l'opérateur Colt.

Serveurs Solaris

Selon les Shadow Brokers, il s'agit là d'une liste de serveurs compromis par Equation Group, un faux nez de la NSA servant à hacker des intérêts à l'étranger. Ce sont ces serveurs qui serviraient à lancer des attaques vers les cibles réelles de l'agence de Fort Meade. Les Shadow Brokers livrent donc cette nouvelle archive comme une liste d'indicateurs de compromission : « *beaucoup de missions (de la NSA, NDLR) sur vos réseaux sont venues et viennent encore de ces adresses IP* », assurent les pirates dans leur anglais hésitant.



Selon les premières analyses de chercheurs, nombre de ces serveurs compromis fonctionneraient

sous Solaris, l'OS de Sun désormais dans le giron d'Oracle. Les informations d'horodatage indiquent que les données remontent toutefois à une période allant de 2000 à 2010. Ce qui signifie que la plupart des IP concernées ont vu leur OS évoluer depuis. « *Un scan sur Shodan (outil de recherche portant sur les objets connectés au Net, NDLR) sur ces hôtes montre que certains sont toujours actifs et font tourner le logiciel identifié (par l'archive des Shadow Brokers*) », écrit toutefois la société de conseil Hacker House dans un billet de blog. L'affaire est également révélatrice de la façon dont la NSA procède pour masquer ses traces.

Publication surprise des Shadow Brokers

« Ainsi la NSA pirate des machines depuis des serveurs compromis en Chine ou en Russie. C'est pourquoi l'attribution (des attaques, NDLR) est si difficile », commente le chercheur Mustafa Al-Bassam sur Twitter. Au passage d'ailleurs, rien ne permet d'affirmer que les serveurs que les Shadow Brokers disent être compromis ont tous servi aux opérations offensives de la NSA et que le groupe de pirates n'en profite pas, par exemple, pour trouver une couverture à des activités de hacking menées par un pays ami…

Les Shadow Brokers se sont fait connaître à la mi-août en annonçant avoir piraté des systèmes informatiques utilisés par Equation, réputé proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu avait posté deux archives sur des sites de partage. La première, en libre accès, renfermait 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes. Plusieurs éléments concordants ont permis d'établir un lien direct entre ces fichiers, qui contenaient bien des failles zero days, et la NSA. Une seconde archive, chiffrée et placée cette fois aux enchères, renfermerait du code inédit, *« meilleur que Stuxnet »* selon les Shadow Brokers. Le contenu de cette seconde archive reste toutefois mystérieux pour l'instant.

La mise en ligne surprise des quelque 350 adresses IP de serveurs supposément détournés par la NSA intervient au moment où la source présumée des Shadow Brokers est en détention aux Etats-Unis. Fin août, un ex sous-traitant de la NSA, Harold Martin, a été arrêté par le FBI lors d'une perquisition à son domicile, où il stockait quelque 50 To de données classifiées qui n'auraient jamais dû quitter les systèmes de ses employeurs. Les services américains soupçonnent Martin d'être l'informateur des Shadow Brokers, même s'ils n'ont produit aucun élément réellement probant à ce jour.

A lire aussi :

10 questions pour comprendre l'affaire Shadow Brokers

La NSA aurait dû détecter sa seconde taupe plus tôt

Crédit Photo : produktionsbuero TINUS-Shutterstock