Les Shadow Brokers publient les outils de hacking de serveurs de la NSA

Dans leur anglais assez inimitable, les Shadow Brokers font un comeback un peu inattendu. Alors qu'à la mi-janvier, ce groupe de hackers, apparu mystérieusement en août 2016 pour dévoiler une série d'outils de hacking probablement dérobés à la NSA américaine, postait un message pour tirer sa révérence, il a publié un nouveau billet ce week-end. Se déclarant déçus des premières décisions de Donald Trump, dont ils se disent des supporters, les Shadow Brokers dévoilent le mot de passe donnant accès à d'autres outils de hacking de la NSA, des codes qu'ils disent avoir dérobés à Equation Group, un nom de code qui d'après de nombreux experts cacherait l'unité spécialisée en cyber-attaques de l'agence de Fort Meade. Soit, en langage officiel, le département TAO (Tailored Access Operations).

Rappelons qu'à l'appui de leurs affirmations, en août 2016, les hackers avaient dévoilé une série d'exploits, dont certains affectant des firewalls de Cisco, Huawei ou Juniper. Une première livraison qui avait permis de confirmer le sérieux des Shadow Brokers. Ils avaient alors tenté de vendre une seconde archive pour une somme colossale (un million de Bitcoins), avant de faire preuve de davantage de modération et de mettre en vente leurs trouvailles à l'unité. Sans grand succès toutefois. C'est tout ou partie de cette seconde cache d'outils de hacking que dévoile aujourd'hui le groupe de mystérieux hackers.

Caramail détourné dès 2001 ?

S'il est encore trop tôt pour préciser la nature exacte de tous les fichiers que renferme cette nouvelle archive, les premiers éléments semblent indiquer qu'il s'agit là encore de fichiers de la même origine. On trouve ainsi une liste de plus de 900 serveurs appartenant à des universités ou entreprises, serveurs qui auraient été employés par la NSA afin de déployer des malwares, lancer des attaques, voire exfiltrer des données depuis les cibles véritables. On note par exemple que le serveur de messagerie Caramail aurait été détourné par l'agence de renseignement dès 2001. Notons qu'un très grand nombre de ces machines tournaient sous Solaris, l'OS de Sun.

32	PITCHIMPAIR	oiz.sarenet.es	192.148.167.17	2001	9	7	ORANGUTAN	1.3	sparc-sun-solaris2.7
33	PITCHIMPAIR	oiz.sarenet.es	192.148.167.17	2001	9	7	RETICULUM	6.6	sparc-sun-solaris2.7
34	PITCHIMPAIR	dns1.unam.mx	132.248.204.1	2001	9	14	JACKLADDER	2.0	sparc-sun-solaris2.7
35	PITCHIMPAIR_MX	ns.unam.mx.unam.mx	132.248.253.1	2001	9	14	JACKLADDER	2.0	sparc-sun-solaris2.6
36	INT	www.caramail.com	195.68.99.20	2001	9	15	JACKLADDER	2.0	sparc-sun-solaris2.7
37	PITCHIMPAIR	orhi.sarenet.es	192.148.167.5	2001	9	18	JACKLADDER	2.0	sparc-sun-solaris2.7
38	PITCHIMPAIR	orhi.sarenet.es	192.148.167.5	2001	9	18	RETICULUM	6.6	sparc-sun-solaris2.7
39	PITCHIMPAIR	anie.sarenet.es	192.148.167.2	2001	9	19	INCISION	4.6	sparc-sun-solaris2.6
40	PITCHIMPAIR	anie.sarenet.es	192.148.167.2	2001	9	19	JACKLADDER	2.0	sparc-sun-solaris2.6

On y a trouve aussi de nombreux outils permettant précisément de hacker des serveurs, sous Solaris donc, mais aussi sous Linux, HP-UX ou AIX. Citons en particulier PitchImpair qui, associé à divers implants, semble responsable d'un grand nombre d'infections parmi le réseau de serveurs

que la NSA est supposée avoir placé sous contrôle. La nouvelle archive des Shadow Brokers renferme encore une liste de login et mots de passe pour exploiter les outils et les accès sur les systèmes mis en coupe réglée, ainsi qu'un framework qui apparaît tout entier voué à effacer les traces laissées par une attaque sur un serveur (notamment en nettoyant les logs).

Un calendrier très politique

Si les Shadow Brokers nient tout lien avec Moscou, leur calendrier semble intimement lié à l'actualité politique. En janvier, ils avaient tiré leur (fausse) révérence à quelques jours de la prise de fonction de Donald Trump. Là, ils révèlent des secrets encore en leur possession juste après une frappe américaine contre la Syrie de Bachar El-Hassad, fermement réprouvée par la Russie de Poutine.

Certains aux Etats-Unis soupçonnent les Shadow Brokers de n'être qu'un faux nez des services de renseignement russes. Une création de Moscou dont l'objectif aurait été, à l'été 2016, d'envoyer un message à Washington, afin d'éviter toute escalade trop rapide dans l'affaire des piratages des instances démocrates qui a pollué la campagne présidentielle américaine. Des faits que l'administration Obama a rapidement attribués à la volonté de Moscou d'influencer l'élection présidentielle américaine. Remarquons d'ailleurs que, dans cette affaire, les Etats-Unis n'ont officiellement pris des mesures de rétorsion et publié des rapports accusateurs qu'en décembre, le président Obama s'étant contenté dans un premier temps, selon ses dires, de mettre en garde en aparté son homologue, Vladimir Poutine.

A lire aussi :

Fuite Shadow Brokers : la preuve d'une nouvelle taupe à la NSA ?

Une faille Shadow Brokers exploitée par des hackers : Cisco a-t-il bâclé le boulot ?

10 questions pour comprendre l'affaire Shadow Brokers

Crédit Photo : produktionsbuero TINUS-Shutterstock