Vault 7 : Wikileaks dévoile les rapports cachés entre la société de sécurité Raytheon et la CIA

Wikileaks poursuit la publication, lancée en mars dernier, des documents «Vault 7» sur les outils de cybersurveillance utilisés par la CIA. La nouvelle série de cinq documents diffusés hier par le site de Julian Assange ne révèle cette fois pas un outil de piratage particulier, mais témoigne de l'aide soutenue que l'agence américaine du renseignement a reçu d'un fournisseur de sécurité, Raytheon Blackbird Technologies en l'occurrence. Raytheon a participé au projet Umbrage Component Library (UCL) qui réunit des outils d'exploitation de failles ainsi que d'autres techniques d'attaques utilisées par la CIA.

Les documents ont été fournis à l'agence de Langley entre le 21 nombre 2014 (*« deux semaines à peine après que Raytheon ait racheté Blackbird Technologies »*, fait remarquer le lanceur d'alerte) et le 11 septembre 2015. Ils contiennent des idées de prototypes et des évaluations de vecteurs d'attaques. En soit, ils n'ont rien de très secret dans la mesure où il s'agit essentiellement de compilations de documents publics émanant de chercheurs en sécurité et d'entreprises évoluant également dans la sphère de la sécurité informatique. Notamment ceux de Symantec (sur Regin) et de FireEye (sur HammerToss).

Un scout technologique

Les travaux de Raytheon ont servi à alimenter la Remote Development Branch (RDB) de la CIA, qui prend en charge les projets de développement d'applications malveillantes. *« Raytheon Blackbird Technologies a agi comme une sorte de « scout technologique » pour la RDB de la CIA en analysant les attaques en cours de logiciels malveillants et en conseillant les équipes de développement de la CIA pour des compléments d'enquête et des prototypes s'inscrivant dans leurs propres projets de développement de malware »*, résume Wikileaks. Sans indiquer si la collaboration entre les deux organisations s'est poursuivie au-delà du 11 septembre 2015. Rappelons que le lanceur d'alerte s'est engagé à désarmer ses publications avant de les rendre publiques. Autrement dit, à s'assurer qu'il existe bien des correctifs aux vulnérabilités ainsi dévoilées.

Le premier document mis en ligne s'intéresse à une variante de HTTPBrowser Remote Access Tool (RAT), conçu pour capturer des frappes au clavier dans les systèmes cibles et qui a été utilisé par un groupe de hackers chinois baptisé Emissary Panda. Une variante de NfLog RAT (également connu comme IrSpace) fait l'objet du deuxième document. Nflog a également été utilisé par des pirates chinois, baptisés Samurai Panda. Combiné à un faille Adobe Flash (CVE-2015-5122) et à des techniques de contournement du contrôle des comptes utilisateur (UAC), le malware pouvait également détecter les identifiants de proxy pour contourner les firewalls Windows.

Le troisième document rappelle que Regin, qui a probablement été développé par les Etats-Unis, s'avère plus sophistiqué de Stuxnet et Duqu pour l'espionnage et le vol de données. HammerToss,

abordé dans le quatrième document, s'appuie sur des comptes Twitter, GitHub et d'autres sites compromis pour orchestrer des fonctions de commande et contrôle à distance. On attribue son usage par la Russie. Enfin, le cinquième document s'attache à Gamker, un cheval de Troie doué pour s'auto-répliquer et exploiter des API afin de voler des informations. Entre autres.

Lire également

OutlawCountry : la CIA détourne le trafic des PC et serveurs Linux

Vault 7 : Wikileaks lève le voile sur les méthodes d'écoute de la CIA

Comment la CIA suit les PC à la trace à l'aide du Wifi