Wikileaks : les outils de hacking de la CIA seront « désarmés » avant publication

C'est à une nouvelle crise de confiance que doit faire face l'industrie IT, touchée encore une fois par la divulgation de techniques de hacking montrant que nombre de technologies ne résistent pas – loin s'en faut – aux assauts d'un service de renseignement bien financé. Preuve de la prise de conscience de l'impact que devraient avoir les révélations de Wikileaks sur la CIA, les industriels, Apple en tête, ont réagi très vite, parfois en quelques heures. Alors qu'ils n'ont pour l'instant à se mettre sous la dent que de la documentation, parfois assez imprécise, sur les modus operandi, et non les codes d'attaque proprement dit. Difficile de proposer des correctifs ou des outils de détection dans ces conditions, même si Intel vient de livrer un utilitaire permettant de détecter une compromission de ses firmwares. « *Sans méthode d'attaque précise, cela revient à chercher une aiguille microscopique dans une botte de foin* », résume Gérôme Billois, senior manager en gestion des risques et sécurité chez Wavestone.

Soulagement pour l'industrie, Wikileaks – qui explique que ses premières divulgations (8 761 documents précisément) représentent 1 % seulement de l'ensemble des données en sa possession – s'est engagé à dévoiler les exploits, autrement dit les codes d'attaque, aux éditeurs ou constructeurs concernés avant de les publier en ligne. « *Nous avons un grand nombre d'exploits… que nous voulons désarmer avant de penser à leur publication*, a expliqué hier Julian Assange, le fondateur de Wikileaks. *Nous allons travailler avec certains de ces fabricants pour essayer de mettre au point des antidotes avant de publier des indices qui pourraient aider les cybermafias ou des gouvernements à comprendre les modes de fonctionnement de ces exploits.* »

Les antivirus contournés

Il faut donc s'attendre, dans les jours et semaines qui viennent, à une vague de patchs. D'autant que les missions de la CIA induisent l'utilisation de nombreuses failles zero day afin de compromettre des systèmes. « *Le mode d'action de la CIA est davantage tourné vers l'intrusion informatique, là où la NSA s'intéresse davantage au chiffrement en particulier* », explique Loïc Guézo, le directeur de la stratégie cyber de Trend Micro pour l'Europe du Sud. Et de citer l'exemple des TV Samsung d'une chambre d'hôtel détournées en micros d'ambiance après branchement par un agent de la CIA d'une clef USB.

La déferlante de correctifs touchera en particulier les principaux systèmes d'exploitation (Windows, Linux, iOS, Android) mais aussi les vendeurs d'antivirus, un des documents dévoilés révélant que la plupart des technologies du marché – dont Kasperky, AVG, F-Secure, BitDefender, Trend Micro, Symantec, McAfee, Avast, Microsoft Security Essentials… – peuvent être bypassées. Même si les modes opératoires de ces méthodes de contournement demeurent inconnus. « *Pour les spécialistes, ce n'est pas une surprise. On savait déjà que des assaillants financés par des Etats pouvaient contourner les antivirus* », relativise Gérôme Billois.

Industriels US : le retour des soupçons

Il n'empêche : la publication de Vault 7 constitue un nouveau coup de canif dans la confiance que le grand public accorde aux solutions de sécurité. Un constat qui vaut aussi pour les messageries chiffrées comme WhatsApp ou Telegram, même si la CIA ne semble pas avoir compromis leur chiffrement à proprement parler ! Rappelons que, pour accéder à ces communications, les techniques de l'agence passent par la compromission des supports, ici des OS mobiles iOS et Android.

Les conséquences de ces révélations sur le marché des entreprises sont plus incertaines. Rappelons que les fuites sur les pratiques de la NSA continuent à modifier en profondeur le marché. « *La publication de Wikileaks fait tomber presque deux années d'efforts de l'industrie, qui s'est posée en victime des pratiques de la NSA et a déployé des actions alternatives pour montrer sa bonne foi, comme l'installation de datacenters en Europe* », dit Loïc Guézo. Car, comme le souligne ce dernier, les documents disponibles sur Wikileaks font renaître les soupçons de complicité entre des industriels américains et les services de renseignement des Etats-Unis.

Sur les réseaux sociaux, des spécialistes n'ont ainsi pas tardé à pointer l'existence d'un implant made in CIA ciblant une dizaine de machines Cisco. Ce bout de code permet d'exploiter une nouvelle commande, MITM (soit l'acronyme de Man-in-the-middle), afin d'intercepter des communications. « *Difficile de savoir s'il n'y avait pas un certain niveau de complicité de l'industriel* », dit Loïc Guézo. Notons que le billet de blog qui analysait cet exploit de la CIA, un billet signé par l'architecte sécurité en chef de Juniper – un des concurrents de Cisco –, a depuis été vidé de sa substance : « *En raison de circonstances imprévues, les détails techniques de cet article ont été supprimés* », indique l'auteur.

[Mise à jour le 10/03 à 15h40 : une version archivée du billet de l'architecte sécurité en chef de Juniper figure ici]

« Le facteur temps est crucial »

Au sein des entreprises, les révélations de Wikileaks sur la CIA – comme celles d'Edward Snowden – permettent « *de donner une réalité à la menace, de mieux justifier des investissements et l'utilisation de solutions, y compris celles amenant des contraintes opérationnelles* », dit Gérôme Billois. Pour cet expert, la seule manière de lutter contre des menaces aussi évoluées consiste à multiplier, diversifier les solutions de sécurité, à exploiter des architectures et des administrations séparées de celles employées sur le réseau classique. « *L'objectif est de rendre les attaques plus complexes, plus longues à mettre en œuvre*, précise Gérôme Billois. *Dans des phases de négociation commerciale ou de discussions autour d'un rachat par exemple, le facteur temps est crucial. Si arrêter toutes les attaques est illusoire, les solutions mises en place doivent permettre de détecter les intrusions et isoler les données qui ont fuitées. Ce sont déjà des informations très importantes.* »

Une démarche que rejoint Loïc Guézo, pour qui les approches traditionnelles, consistant à définir un niveau de sécurité pour l'ensemble de l'entreprise en fonction d'un niveau de menace perçu, sont vouées à l'échec : « *Le niveau de la menace est si élevé aujourd'hui que ce n'est plus possible*, argument-t-il. *La sécurité la plus robuste est désormais réservée aux joyaux de la couronne, aux*

informations réellement vitales au bon fonctionnement des organisations. »

A lire aussi :

La CIA n’a pas cassé le chiffrement de WhatsApp, Signal ou Telegram

La CIA collectionne les outils de hacking d’autres Etats… pour masquer ses traces

Juniper retire enfin son algorithme made in NSA… sans s’expliquer

Crédit photo : CIA