Wikileaks dévoile les dernières méthodes d'espionnage de la CIA

Snowden avait déjà alerté le monde sur un programme de surveillance massif, automatique et systématique d'Internet. Des révélations qui semblaient faire des renseignements américains un système quasi-omniscient. Wikileaks ouvre aujourd'hui, sous le nom de fil « Vault 7 », les vannes d'une nouvelle révélation sur les moyens d'espionnages du renseignement américain. En quoi ces révélations diffèrent-elles des précédentes de Snowden ?

Il ne s'agit pas d'un programme de masse…

Ces documents, au nombre de 8761, sont techniques mais ne décrivent pas une nouvelle technologie. Il s'agit en premier lieu des informations sur des produits existants, tant du matériel (objets connectés, smartphones, routeurs, PC) que du logiciel (systèmes d'exploitation, Windows, macos, GNU/Linux…) décrivant les failles de sécurités de ces systèmes et la manière de les exploiter pour en capter des informations, voir pour en prendre le contrôle. Ce type d'information ne peut avoir son utilité que dans des usages ciblés et identifiés, loin donc d'un usage systématique et automatisé, de masse. Il s'agit en outre de vraiment faire les choses de façon invisible pour tous les acteurs.

Les dernières TV Smart Samsung sont ainsi particulièrement étudiées car elles réagissent aux commandes vocales. Quasi-toutes les technologies réagissant à la voix nécessite actuellement une connexion réseau Internet car ce sont des serveurs qui analyse la commande (un smartphone ou une télé n'a pas le nécessaire embarqué pour être en capacité de le faire). Le but de la CIA étant de pouvoir espionner la pièce y compris lorsque la télé est éteinte. Tout est donc fait pour mimer un mode veille sans pour autant désactiver le capteur vocale ni le flux réseau. Le malware déployé va même jusqu'à bloqué les mise à jour système du téléviseur car cela se fait sans le consentement du constructeur qui ne se cache pas, lui-même, dans son contrat d'utilisation de faire une grosse captation de données qui n'ont rien à voir avec les commandes vocales émises par les utilisateurs et utilisatrices.

D'autres types d'attaques sont élaborées : par un film vérolé lu par le lecteur libre VLC, ou l'usage d'un CD contenant un malware parfaitement invisible, etc.

Les fichiers contiennent aussi des descriptions de faille dites « zero day »

particulièrement critique, donnant des droits d'accès totale à distance sur un système.

Ce sont quelques exemple mis en exergue, mais en pratique tous les systèmes d'exploitation pour n'importe quel types de produits pourvus sont touchés d'une manière ou d'une autre : du simple PC au derniers modèles de voitures connectées, en passant les smartphones et les montres…

Le chiffrement est toujours un obstacle à l'État policier

Les programmes de surveillances de masses sur les réseaux sont très bons pour capter toutes informations qui transitent en claires… mais sont purement inefficace pour toutes informations chiffrées ! Aucune agence de renseignement au monde ne peut actuellement s'attaquer systématiquement aux échanges chiffrés. Ils ne le peuvent qu'au cas par cas sachant que craquer un chiffrement requiert des ressources importantes de temps et puissances bien supérieurs aux machines de pointe que nous pouvons avoir dans nos bureaux.

C'est la raison de cette base de donnée de failles et de techniques d'exploit : le but est de capter les données à partir du système hôte lui-même au moment où elles sont manipulées ou lues en clair par les interlocuteurs.

Il n'y a pas a priori pas d'attaque réelle sur les services d'échanges chiffrés comme WhatsApp, Telegram ou Signal. Les éditeurs de ces programmes ne se sentent pas dans l'immédiat concerné par ces révélations et n'ont, a priori, pas de faille à colmater. Plus difficile par contre pour d'autres sociétés. Si Apple a déjà annoncé avoir colmaté beaucoup des brèches révélés dans les versions récentes d'iOS, Samsung et Google sont moins loquaces. Et pour cause : ils se servent de leur produit pour investir les données des utilisateurs et utilisatrices. Ayant intérêt dans leur modèle économique à sauvegarder cette captation pour leur compte, les moyens de résoudre certaines contradictions ne leurs sont pas aussi aisé que pour Apple qui ne fait pas ce type de captation. Google est d'autant plus embêté que son système d'exploitation Android a la particularité de se développer dans un environnement dit « fragmenté » : son système est modifié par chaque constructeur et adapté différemment à chaque modèle de téléphone. De fait, et les documents de la CIA sont assez parlant, les failles d'Android, à version égale du système, ne sont pas les mêmes d'un smartphone à l'autre. Sans compter pour les versions différentes. Ce système est par conséquent compliqué à maintenir dans ses multiples ramifications et sur un modèle neuf ces mises à jours n'ont lieu que pendant quelques mois.

On s'y attendait

Ces « révélations » ne sont pas une surprise. En vrai de plus de plus d'État adaptent leur législation et reconnaissent le piratage d'appareils d'informatiques pour faire

avancer les enquêtes. Les États-Unis et le Royaume Uni sont déjà dans ce cas depuis un moment, et il est logique que les documents dérobés fassent état d'une collaboration entre la CIA américaine et le MI5 britannique. Quand on parle de reconnaissance, nous disons que les informations captées par ces méthodes obtiennent une valeur juridique, ce sont des éléments à charge.

Depuis plusieurs mois aux États Unis, des éditeurs de logiciels et des associations dénoncent la rétention de ces informations sur les failles de sécurité des systèmes qui mettent en danger particulier et organisations (parfois des entreprises) d'attaque malveillante par des pirates isolés, des concurrents, des États peut-être. Il est de notoriété publique que les services de renseignement ou même simplement le FBI, se servent de telles failles non communiquées, parfois achetées sur un marché noir à des prix variant entre dizaines de milliers de dollars et pouvant atteindre plus du millions pour une seule faille. Le conflit ayant opposé Apple et le FBI autour du déchiffrement des données de l'iPhone d'un terroriste de San Bernardino s'est finalement résolu par l'achat d'une telle information par le FBI. Ces communications concernant les failles de sécurités existent mais sont sélectionnées à partir de critères obscurs et très spéculatifs sur la possibilité d'un tiers de se saisir d'une telle brèche pour l'exploiter.

Finalement c'est une bonne nouvelle…

Le panel hétéroclite d'entreprise, de particulier, de journaliste, de partis ou d'association a finalement gagné, pas par la voie légale mais par une action subversive de vol par effraction numérique. La CIA voit ses moyens se retourner contre elle, d'autant qu'il n'y a pas de que des informations sur la manière de pirater le maximum de système qui ont fuité, mais également les programmes, les exécutables, qui servent à ces piratages.

Nous devrions alors pouvoir bénéficier prochainement de mises à jours qui diminue la surface d'attaque contre nos systèmes et le sécurise d'avantage, que nous utilisions des logiciels libres (par exemple Linux ou Firefox) ou des logiciels propriétaires/privatifs (Windows, macos, iOS, Android…).

Frédérick Lorie, le 10 mars 2017