Un malware résistant à un formatage de disque dur : l'œuvre de la NSA ?

Mais qui se cache derrière le groupe de hackers baptisé Equation ? Dans un rapport, les laboratoires de l'éditeur Kasperky expliquent avoir identifié un groupe de pirates utilisant – au moins depuis 2001 (et peut-être dès 1996) – des techniques d'une grande sophistication, « *dont certaines surpassent la menace Regin en terme de complexité et de sophistication* », assure l'éditeur qui explique avoir là affaire à un groupe ayant un **niveau de compétences qu'il n'avait jamais rencontré auparavant**. L'appellation Equation a d'ailleurs été choisie en raison de la propension de ce groupe à utiliser des techniques pointues de chiffrement, notamment afin de masquer ses agissements.

Une telle description fait évidemment penser à un acteur gouvernemental, ou disposant de l'appui financier d'un Etat. Et s'il ne les désigne pas nommément, Kaspersky soupçonne clairement les Etats-Unis. Un des malwares isolés par l'éditeur (Fanny), assez ancien (il a été créé en 2008), exploite deux failles zero day, qui furent découvertes plus tard lors de la mise au jour de Stuxnet. Rappelons que ce dernier, qui visait les centrifugeuses du programme d'enrichissement d'uranium iranien, a, selon la presse américaine, été mis au point par les Etats-Unis et Israël. « *Les deux exploits ont été utilisés dans Fanny avant d'être intégrés dans Stuxnet* », remarque Kaspersky, qui ajoute que les **usages similaires des deux codes d'exploitation** lui font penser que les auteurs des deux malwares… n'en font qu'un ou travaillent très étroitement ensemble. Un détail troublant qui semble indiquer que le groupe Equation pourrait bien n'être qu'un autre nom pour la NSA.

Grayfish : contrôle total, activité indécelable

D'autant qu'un certain nombre d'artefacts recensés par l'éditeur russe rappellent furieusement les acronymes figurant dans les documents Snowden (citons StealthFighter ou StraitAcid). L'appellation Grok, isolée dans l'activité d'Equation suivie par Kaspersky, apparaît d'ailleurs dans des documents révélés par le lanceur d'alerte. Enfin, l'éditeur russe note que « *certains des patients zéro (les premiers infectés, NDLR) de Stuxnet semblent aussi avoir été la cible du groupe Equation. Il est possible que le malware de ce dernier ait été utilisé pour implanter Stuxnet.* »

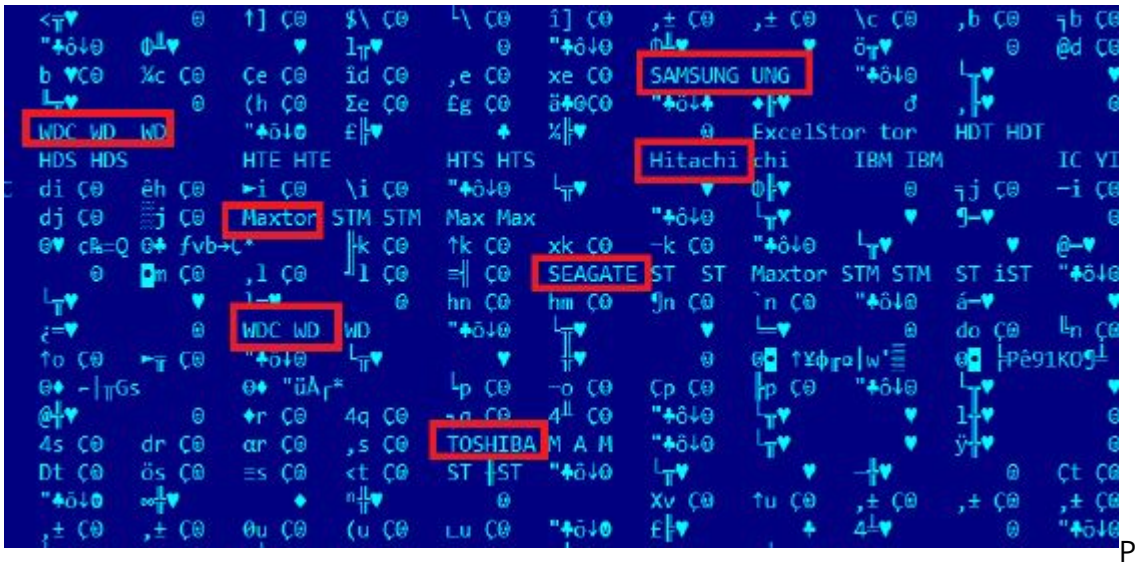
S'appuyant sur le témoignage d'un ancien de la NSA, Reuters confirme les soupçons de Kaspersky, en établissant **un lien entre le groupe Equation et les pratiques de la NSA**. La source de nos confrères assure que le programme mis au jour par l'éditeur russe a autant de valeur aux yeux de l'agence que celui relatif à Stuxnet.

La sophistication du groupe Equation apparait clairement dans les malwares que Kaspersky a baptisés **EquationDrug et GrayFish** (le successeur du premier). Après avoir validé l'intérêt d'une victime via un premier malware jouant un rôle de sonde, Equation installe sa plate-forme de malware (sur laquelle se connectent des plug-in et des pilotes), qui lui fournit un contrôle total du système d'exploitation de la machine cible. Pour les OS plus modernes, Equation exploite ainsi GrayFish, développé entre 2008 et 2013. Cette plate-forme offre un accès permanent aux OS Windows (NT 4.0, 2000, XP, Vista, 7 et 8) et un système de stockage caché. Son activité est quasi-

indétectable, assure Kaspersky. Au démarrage, GrayFish détourne les mécanismes de chargement du système et **injecte son code infectieux dans le secteur de boot**. « *Après l'infection, l'ordinateur ne fonctionne plus par lui-même. C'est GrayFish qui le fait tourner, effectuant les changements nécessaires à la volée* », écrit l'éditeur d'antivirus, qui assure qu'il s'agit là des travaux de développeurs de top niveau.

Firmware des disques durs : un accès aux codes source

Au démarrage de Windows, l'installation de GrayFish se déroule en 4 à 5 étapes successives. Si une erreur se produit avant l'installation complète du malware, celui-ci s'auto-détruit pour effacer toute trace. Notons que GrayFish contourne la sécurité des OS modernes, empêchant l'exécution de code non sécurisé au niveau du noyau, via notamment l'exploitation d'une signature non révoquée d'un pilote renfermant une vulnérabilité. Comme tous ses modules ainsi que les données volées sont chiffrés dans la base de registres de Windows, GrayFish est totalement indétectable des antivirus. Signalons aussi que l'analyse de l'activité des serveurs de commande et contrôle par Kaspersky semble indiquer qu'Equation dispose aussi de malwares pour OS X d'Apple.



Plus impressionnant encore, la capacité à **infecter les firmwares des disques durs** présente tant sur EquationDrug que GrayFish, via un module dédié venant se greffer aux plates-formes d'infection. Ce plug-in a deux fonctions principales : reprogrammer les firmware avec un code customisé en fonction des besoins des assaillants et fournir une API offrant un accès à des secteurs masqués sur le disque dur. De quoi tant assurer la survie du malware même en cas formatage du disque et offrir un **stockage caché sur le disque même de la victime**. La dernière version du plug-in cible 12 catégories de disques, dont ceux des principales marques (Western Digital, Seagate, Maxtor, Samsung, Toshiba, IBM, Micron…). « *Le plug-in utilise un grand nombre de commandes ATA spécifiques à ces marques et non documentées* », remarque Kaspersky. Un détail évidemment troublant. Interrogé par Reuters, Costin Raiu, un des chercheurs de Kaspersky, ne s'embarrasse pas de circonvolutions : « *Il y a zéro chance que quelqu'un puisse réécrire le système d'exploitation des disques durs en se basant sur l'information publique disponible* ». Bref, de son point de vue, la NSA a eu accès aux codes source des firmware, soit en les dérobant, soit en les obtenant de leurs concepteurs. Kaspersky signale que

l'usage de ce module d'infection des firmware reste très rare, indiquant probablement qu'Equation le réserve à ses victimes les plus prometteuses.

CD-Rom piégé

Si cette sophistication rappelle l'arsenal d'une division de la NSA spécialisée dans les opérations spéciales électroniques (Tailored Access Operations), s'appuyant elle-même sur une véritable SSII du hack (ANT) dont le catalogue est une des pièces centrales des révélations d'Edward Snowden, d'autres détails évoquent également les pratiques de l'agence de Fort Meade. Comme l'installation de malwares sur des CD-Rom probablement à l'insu de leurs éditeurs légitimes. **Une mésaventure qu'a notamment connue Oracle**, selon Kaspersky. Rappelons que, selon les documents Snowden, la NSA pratique le détournement de colis (par exemple lors de l'envoi de routeurs) pour y implanter des malwares, à l'insu tant de l'émetteur que, évidemment, du destinataire.

Kaspersky a dénombré **au moins 500 victimes du groupe Equation dans 30 pays**, les infections ciblant très souvent des serveurs. « *Comme les infections renferment un mécanisme d'auto-destruction, on peut penser qu'il y a probablement eu des milliers d'attaques dans le monde au cours de l'histoire du groupe Equation* », écrit Kaspersky, qui explique avoir découvert les agissements de ce groupe lors de son enquête sur le malware Regin. Les hackers ciblent de nombreux secteurs : gouvernements, télécoms, aéronautique, énergie, secteur nucléaire, défense, nanotechnologies, média, transports, institutions financières, spécialistes de la cryptographie… Ainsi que des activistes islamistes.

A lire aussi :

NSA : les 5 enseignements des dernières révélations de Snowden
Tout sur l'arsenal secret des espions de la NSA
NSA : les matériels Cisco, Juniper et Huawei transformés en passoire
FIC 2015 : les hackers ont gagné une bataille, pas la guerre