Regin : 5 éléments pour comprendre le logiciel espion

Après les révélations sur la découverte d'un logiciel espion sophistiqué d'origine étatique, nous avons en voulu en savoir un peu plus sur la fiche signalétique de Regin. Nous avons demandé l'avis de consultants en cybersécurité.

Une particularité : l'espionnage du réseau GSM

Hier, le monde découvrait un nouveau nom dans le panorama de la cybersécurité, Regin. Son nom évoque à la fois **l'inversion de In Reg** pour In Registry « à l'intérieur du registre », mais aussi une **référence à un maître forgeron** dans la religion nordique. Après Stuxnet, Duqu ou Flame, ce malware a été découvert par une équipe de chercheurs de Symantec et son niveau de technicité laisse à penser que des Etats sont derrière son élaboration. « *Son élaboration fonctionnelle et opérationnelle est parmi les plus avancées. Il est suffisamment complexe pour laisser le moins de traces possibles. Les moyens ont été mis pour placer du code dans un framework* », constate **Vincent Hinderer**, expert en sécurité pour le cabinet Lexsi. Kaspersky est monté au créneau en expliquant que le terme malware était inapproprié, car Regin s'apparentait à une plateforme de cyberattaque. Un avis partagé par Gérôme Billois, senior manager gestion des risques et sécurité de l'information chez Solucom, « *le degré de sophistication tourne autour de deux axes, un mode discret avec du chiffrement à pratiquement chaque niveau d'exécution et l'existence de modules spécialisés* ».

La catalogue d'attaques est « *relativement connu* », analyse l'expert de Lexsi avec plusieurs modules capables d'exécuter un système de fichiers virtuels chiffrés unique. Les portes d'entrée sont multiples, comme l'exploitation d'une faille zéro day dans Yahoo Messenger. Un autre vecteur est l'utilisation d'un faux site imitant les réseaux sociaux pour piéger l'utilisateur, marque de fabrique des agences de renseignements diront certains spécialistes. Cependant, les experts en sécurité distinguent un module parmi les autres, celui capable de **pirater les outils d'administration du trafic GSM**. Kaspersky a livré un rapport technique où la présence de Regin dans les logs d'activité des stations de base a été retrouvée.

Les cibles : opérateurs, entreprises, chercheurs, etc.

La présence de Regin sur les stations de base pourrait être à l'origine du piratage de l'opérateur Belgacom. Plusieurs journaux dont Intercept ont fait le rapprochement avec une attaque qui a eu lieu en 2013. L'opérateur, par la voix de son porte-parole a précisé : « *pour nous, il a toujours été clair qu'il s'agissait d'un programme sophistiqué, mais aujourd'hui tout a été nettoyé et c'est de l'histoire ancienne* ». Pour Vincent Hinderer, viser un opérateur permet souvent d'atteindre d'autres cibles : *« il s'agit souvent d'un point névralgique pour ensuite remonter à la cible visée* ».

Kaspersky dévoile le nom d'une des cibles de Regin, Jean-Jacques Quisquater, spécialiste reconnu de la cryptographie. En février 2014, il avait été victime d'une intrusion sophistiquée et avait fourni aux éditeurs les éléments de cette attaque. Pour Kaspersky, il s'agit bien d'une victime de la

plateforme Regin. Le problème aujourd'hui est que le nombre de victimes recensé est relativement faible : « *une vingtaine pour Symantec et une trentaine pour Kaspersky* », observe Vincent Hinderer. Il s'attend à ce que ce chiffre augmente, « *le domaine privé n'est pas le seul concerné par Regin, des organisations publiques ont été touchées en raison du contexte diplomatique* ». Pour autant, le **faible nombre de victimes** laisse supposer des **campagnes très ciblées** pour obtenir des informations très précises.

Les commanditaires : NSA et GHCQ pointés du doigt

Une question revient en boucle : qui est derrière Regin ? Si les éditeurs de sécurité et les experts sont formels sur le fait qu'une telle plateforme ne peut provenir que d'un Etat, ils se gardent bien d'accuser spécifiquement une ou des nations en particulier. Par contre, la presse ne s'en prive pas, à commencer par Intercept qui voit derrière Regin les petites mains de la NSA et du GCHQ (le service britannique). Le framework aurait servi, comme nous l'avons vu précédemment, pour pirater le réseau de l'opérateur Belgacom, mais aussi **le système d'information de l'Union européenne**. Ces attaques étaient mentionnées dans les documents transmis par Edward Snowden ; on y parle d'un malware sans mettre un nom dessus. Sur Intercept, Ronald Prins, expert en sécurité chez Fox IT qui est intervenu dans l'affaire Belgacom, affirme : « *je suis convaincu que Regin a été utilisé par les services de renseignements anglais et américain* ». Dans son analyse posté sur son blog, F-Secure écarte l'idée « *que ce malware soit issu de la Chine ou de la Russie* ».

Quand on regarde la **cartographie des cibles** recensées, **la Russie et l'Arabie Saoudite** arrivent en tête avec un quart chacun du total. Vient ensuite l'Irlande et le Mexique, puis une succession d'attaques visant l'Inde, l'Afghanistan, l'Iran, la Belgique, l'Autriche et le Pakistan. On constatera que ni l'Angleterre, ni les Etats-Unis ne sont dans la liste des territoires touchés. De même, la traçabilité des serveurs de commandes et contrôle se révèle très difficile car ils utilisent des protocoles de communication P2P et une topologie relativement complexe.

La détection : des marqueurs sur Regin publiés

Face à ce type d'attaques, les entreprises et les équipes de sécurité peuvent logiquement « *exprimer une certaine lassitude sur leurs efforts visant à construire des politiques de sécurité* », admet Gérôme Billois. Avec les moyens d'un Etat, c'est une **bataille du pot de fer contre le pot de terre**. Pour autant, les consultants en sécurité estiment qu'il y a des moyens de bien réagir devant ce type de menaces.

« *Les éditeurs de sécurité publient dans ce genre de situation des rapports techniques en donnant à la communauté des marqueurs (IOC, Indicator of compromise) qui permettent de détecter la présence ou non du malware* », explique Gérôme Billois. Des tests sont en cours auprès des clients de Solucom pour vérifier leur exposition, mais sans résultat pour l'instant.

« *Il n'y a pas de silver bullet sur ce genre d'attaques* », rétorque Vincent Hinderer et d'ajouter : « *l'idée est de prendre un ensemble de mesures de sécurité pour rendre la vie plus difficile aux velléités des Etats* ». Les deux consultants restent néanmoins philosophes, ce type d'évènement amène petit à petit une prise de conscience sur les enjeux liés à la cybersécurité, mais les dirigeants d'entreprise sont **plus sensibles à des piratages du type Sony Pictures**, qu'à l'existence d'un logiciel espion piloté par un

Etat.

Les évolutions : des variantes déjà actives

Dans son rapport, Symantec a expliqué avoir trouvé deux versions de Regin. La première aurait été active en 2008 avec un arrêt brutal et non expliqué en 2011. La **V2** (en version 64 bits) a, elle, été utilisée **à partir de 2013**, mais a pu être active avant. Kaspersky précise que cette version 64 bits était encore active au printemps dernier. Gérôme Billois constate que le cycle d'apparition des techniques d'espionnage gouvernemental est assez régulier : « *quasiment tous les 9 mois, on découvre des malwares étatiques* ».

Il ajoute : « *les marqueurs ou IOC vont changer pour viser d'autres cibles et ainsi nous verrons apparaître des Regin 2 ou 3 dans les prochains mois* ». Les investigations sont en cours et d'autres éléments devraient prochainement être fournis par les éditeurs de sécurité. D'ici là, un autre malware étatique quittera l'ombre pour la lumière des médias…

A lire aussi :
L'espionnage de la NSA pourrait « casser Internet » selon les géants du Web
La cartographie du Net de la NSA pirate les réseaux d'opérateurs allemands
Scan de ports TCP : comment la NSA et le GCHQ préparent leurs attaques

Crédit Photo: SergeyNivens-Shutterstock