Virus Regin : Conséquences informatiques ou clash diplomatique ?

Virus Regin : Conséquences informatiques ou clash diplomatique ?

REGIN – Il est déjà considéré comme l'un des malwares les plus sophistiqués de l'histoire de l'informatique. « Regin », le mystérieux logiciel malveillant dont le spécialiste de sécurité Symantec (éditeur de l'antivirus Norton) a révélé l'existence dimanche soir, pourrait bien continuer à faire parler de lui.

Selon le site américain The Intercept, les services de renseignement américains et britanniques se cacheraient derrière. Pour mémoire, The Intercept a été créé par Glenn Greenwald, l'enquêteur ayant publié les révélations d'Edward Snowden sur les programmes de surveillance la NSA.
Citant des sources du secteur et une analyse technique du logiciel, The Intercept affirme que « Regin » est référencé dans des documents fournis par Edward Snowden lui-même, alors qu'il était encore consultant de l'agence américaine de renseignement. Interrogée sur ces informations, une porte-parole de la NSA a répondu par un lapidaire: « Nous n'allons pas commenter des rumeurs ».

L'affaire est néanmoins prise très au sérieux car « Regin » avait des objectifs très ambitieux
le malware aurait été utilisé contre des réseaux informatiques de gouvernements européens et Belgacom, le réseau public de télécommunications belge.
Dans le détail, « Regin » serait capable d'apporter une grande flexibilité aux attaquants. En effet, ces derniers seraient en mesure de charger des fonctions personnalisées adaptées à des objectifs individuels en cas de besoin. Le virus serait notamment capable de réaliser des captures d'écran, de prendre le contrôle d'une souris et de son curseur, de voler des mots de passe, de surveiller le trafic d'un réseau, et de récupérer des fichiers effacés.

Après l'abandon du dossier des « écoutes Merkel »
Si la nature des assaillants parvient à être authentifiée, les vieux démons pourraient se réveiller des deux côtés de l'Atlantique. L'affaire des écoutes de la NSA venait pourtant de refroidir avec l'abandon samedi de l'enquête concernant la mise sur écoute présumée d'un téléphone d'Angela Merkel. Selon le magazine allemand Focus, aucune preuve n'aurait été trouvée sur la responsabilité de la NSA. « Regin » pourrait donc raviver les tensions.
Interrogé par The Intercept, l'expert en sécurité qui a aidé à supprimer le logiciel espion des réseaux de Belgacom est formel. « Après avoir analysé ce malware et regardé les documents Snowden, je suis convaincu que Regin est utilisé par les services de renseignement américain et britannique », a affirmé Ronald Prins. C'est lui qui permet à l'équipe de Glenn Greenwald d'être si confiante dans ses affirmations.
D'autres sources abondent dans ce sens. « Nous sommes convaincus que ce produit est l'oeuvre des Etats-Unis ou de la Grande-Bretagne », a assuré à SC Magazine Erik de Jong, un expert en cyber-sécurité de la firme Fox-IT. « Nous avons examiné les documents de Snowden, les pièces s'imbriquent ». La société finlandaise F-Secure assure sur son blog que le virus, « pour une fois », ne vient pas de Russie ou Chine.

« Considéré comme révolutionnaire »
Symantec se dispense de donner des noms, mais plutôt des indices sur le niveau de sophistication. « Dans le monde des virus informatiques, rares sont les exemples qui peuvent être réellement considérés comme révolutionnaires. Ce que nous avons là en fait partie ». C'est par cette phrase que débute le rapport de la société publié dimanche.
La complexité de « Regin » implique une phase de conception ayant duré plusieurs mois, voire plusieurs années, et qui a nécessité un investissement financier important. « Le temps et les ressources employés indiquent qu'une nation est responsable », assure Candid Wueest, un chercheur travaillant pour le spécialiste américain de la sécurité informatique.

Encore difficile d'identifier formellement le(s) responsable(s)
Pas question néanmoins d'accuser formellement un Etat. « On ne fait pas d'attribution tant que l'on n'a pas de faits concrets, de preuves irréfutables », se justifie-t-il, « mais il est certain qu'on peut tirer des conclusions ». Chez Kaspersky Lab, le principal concurrent de Symantec en matière de sécurité informatique, on se refuse également à pointer du doigt un pays en particulier. La compagnie russe explique néanmoins que ce virus ne peut avoir été développé qu'avec le financement et les moyens techniques d'une agence nationale de renseignement.
Les experts détaillent ensuite le processus. « Les équipes de Symantec ont détecté des brèches de sécurité avérées dans 10 pays, en premier lieu la Russie puis l'Arabie saoudite, qui concentrent chacune environ un quart des infections », a indiqué Candid Wueest. Les autres pays touchés par ordre d'importance sont le Mexique et l'Irlande suivis par l'Inde, l'Afghanistan, l'Iran, la Belgique, l'Autriche et le Pakistan. Un travail d'orfèvre pour les spécialistes du genre.
Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.huffingtonpost.fr/2014/11/25/regin-virus-snowden-nsa-gchq-belgique-greenwald_n_6217356.html
Par Grégory Raymond