“Operation Socialist” : la cyberguerre entre Européens

16/12/2014 à 18h46

Londres a piraté pour Washington les données de Belgacom, opérateur des institutions européennes, au risque de saborder le réseau. Un véritable acte de guerre.

Par Guerric Poncet

Si vous pensez que l’Europe est une union, vous vous trompez.

> ***Londres l’a prouvé en piratant et en mettant en péril le principal opérateur télécom de Belgique, Belgacom, qui gère les télécommunications de l’Union européenne.***

Selon l’enquête publiée samedi conjointement par *De Standaard* (Belgique), *NRC Handelsblad* (Pays-Bas) et *The Intercept* (média américain proche du lanceur d’alerte Edward Snowden), les services secrets britanniques ont non seulement mis sur écoute les télécommunications de l’Union européenne, mais

> ***ils ont aussi agi de façon très agressive, menaçant la stabilité des infrastructures réseau du continent européen.***

“Il s’agit de la première cyberattaque documentée d’un État européen contre un autre État européen”, confie Edward Snowden à *The Intercept*.

> ***Et ce n'est pas une petite guéguerre entre amis : l'ampleur de cette opération clandestine, semble-t-il soutenue par Washington, en fait un véritable acte de guerre.***

Si la Grande-Bretagne était déjà perçue comme le cheval de Troie américain dans l'UE, elle pourrait désormais être perçue comme son bras armé dans une guerre de l'information… contre l'Europe.

Nommé *Operation Socialist*, le piratage a été lancé dès 2008 par le Government Communications Headquarters (GCHQ) britannique et demeure le plus massif à ce jour contre les institutions de l'UE et les gouvernements de ses États membres. En comparaison, le piratage par les États-Unis et Israël des centrifugeuses du programme nucléaire iranien avec le ver Stuxnet fait pâle figure, tant par le nombre de machines infectées que par la complexité du code, jusqu'alors référence du genre.

Des employés ciblés

Face au chiffrement des communications, les espions britanniques ont déployé Regin, un logiciel malveillant extraordinairement perfectionné.

> ***Cette arme de cyberguerre, la plus évoluée jamais découverte, semble avoir été développée avec l'aide de la toute-puissante agence nationale de sécurité américaine (NSA), le plus gros employeur mondial d'experts informatiques.***

Grâce aux données de navigation issues de Google, Facebook, LinkedIn ou encore Yahoo, les espions ont identifié des ingénieurs et des administrateurs système de Belgacom, et ont infecté leurs machines. Début 2011, selon les documents dévoilés par les trois médias, les services secrets canadiens sont venus en renfort pour affiner le système de détection de ces cibles primaires.

On retrouve là encore un fidèle allié de Washington, l'un des "Cinq Yeux" de la NSA. Grâce à ces "patients zéro", le GCHQ a pu diffuser son code malveillant depuis l'intérieur-même des cyberdéfenses de Belgacom.

Puisqu'il se comporte comme un logiciel authentique de Microsoft, le code est resté invisible pendant des années, avant d'être mis au jour en 2013 et identifié en 2014 comme

> ***une "oeuvre" américano-britannique, aussi détectée en Russie, au Mexique, en Arabie saoudite, en Irlande, ou encore en Iran.***

Pendant des années, Regin a volé et transmis à ses maîtres toutes les télécommunications sensibles des institutions européennes (Commission et Parlement) et des délégations gouvernementales des États-membres, alors même que des négociations commerciales stratégiques avaient lieu entre l'UE et les États-Unis pour – entre autres – la signature d'un traité transatlantique de libre-échange.

Appels téléphoniques, messages, documents : tout ce qui se disait à Bruxelles ou avec Bruxelles a été espionné. Regin se servait à la source, directement sur les ordinateurs ciblés, avant même que les informations ne soient chiffrées pour transiter sur Internet.

Regin "aurait pu rester actif encore plusieurs années"

Même les routeurs, la partie la plus protégée du réseau de Belgacom, ont été infectés. "Les documents secrets du GCHQ (publiés eux aussi samedi, ndlr) montrent que l'agence a pu accéder aux données privées des clients de l'opérateur, qu'elles aient été chiffrées ou non", assure *The Intercept*. Ultime humiliation pour les ingénieurs réseau de l'opérateur : ce sont les services secrets britanniques qui, se sachant

découverts, ont effacé une grande partie de leur code malveillant. Il faut dire que l'opérateur belge a pris son temps, et a même fait preuve de mauvaise volonté : il a par exemple refusé l'accès aux routeurs infectés à ses consultants en sécurité, préférant les confier… au fabricant américain Cisco ! Pire, "certaines parties du code n'ont jamais été totalement nettoyées" malgré les "millions de dollars" investis par Belgacom pour résoudre le problème, précise le site américain qui cite des sources internes chez les "nettoyeurs". Ces mêmes sources estiment que si le serveur de messagerie de Belgacom n'avait pas eu un dysfonctionnement imprévu qui a éveillé les soupçons, Regin "aurait pu rester actif encore plusieurs années".

> ***En plus de l'outrage sur le fond, il est clair que l'infection d'un opérateur d'importance vitale (OIV) est un acte particulièrement irresponsable de la part d'un allié.***

Il met en péril le principal opérateur de Belgique et menace la stabilité des télécommunications non seulement dans le pays, mais aussi sur tout le continent européen. Selon *The Intercept*, Regin désactivait par exemple les mises à jour automatiques des serveurs de Belgacom afin d'éviter d'être évincé par un correctif de sécurité.

Résultat : les serveurs de Belgacom étaient d'autant plus vulnérables, en Belgique et ailleurs.

> ***Pourtant, il y a très peu de chances que la Grande-Bretagne soit sanctionnée,***

malgré les demandes de la députée européenne Sophia in 't Veld, qui a dirigé l'enquête parlementaire sur les révélations d'Edward Snowden.

La Grande-Bretagne doit selon elle être poursuivie "pour avoir violé la loi, bafoué les droits fondamentaux et érodé nos

systèmes démocratiques”.

> ***Mais l’UE refuse d’ouvrir les yeux sur ces pratiques guerrières entre États membres.***

lepoint.fr