print

Oubliez la Corée du nord – la menace mondiale pour le cyber-espace vient des Etats-unis (et du Royaume-Uni)

De John Naughton

Global Research, janvier 02, 2015

Url de l'article:
http://www.mondialisation.ca/oubliez-la-coree-du-nord-la-menace-mondiale-pour-le-cyber-espace-vient-des-etats-unis-et-de-grande-bretagne/5422588

Si vous deviez mesurer l'importance d'un phénomène en termes de colonnes déversées dans la presse écrite, la cyber-attaque dont a été victime Sony aurait été l'affaire du mois.

Les cadres de l'entreprise ont dû poster des notes d'information à l'entrée des bureaux pour demander au personnel de ne pas se connecter sur le réseau une fois assis à leur poste de travail. L'ensemble du réseau de l'entreprise a dû être débranché alors qu'il devait faire face à une demande de rançon qui menaçait de rendre publics des documents confidentiels et des films pas encore sortis en salle, en échange de fortes sommes d'argent.

La grande question est : *qui est responsable de l'attaque ?* **Les spéculations se sont déchaînées, conduisant certains à pointer du doigt la Corée du nord**, sur la base que l'un de ses prochains films « The Interview » se moque du leader du pays, Kim Jong-un.

Cela semble fort improbable à ce chroniqueur que je suis : la Corée du nord peut manquer sérieusement d'humour au sujet de son leader chéri, mais en faire un sujet d'extraction de rançon serait bien maladroit, même pour cet étrange régime.

En fait, il ne semble pas y avoir eu de transfert d'argents : certains documents confidentiels, comme des tableaux Excel révélant les salaires des cadres de Sony les mieux payés, ont commencé à fleurir sur le net et les films secrets à se diffuser sur des sites pirates.

Excitant, non ? Mais la vraie grosse cyber histoire de ces dernières semaines est moins glamour mais bien plus inquiétante sur le long-terme. Elle concerne Regin, un *malware* qui vient tout juste de faire son apparition sur la scène publique, bien qu'il traînerait déjà depuis plusieurs années.

L'entreprise de sécurité *Symantec* le décrit comme *« un malware complexe dont la structure montre un degré de compétence technique rarement vu. Personnalisable avec un degré extensible de potentialités qui dépend de la cible, il fournit à ceux qui le maîtrisent un outil puissant pour une surveillance de masse et il a été utilisé pour des opérations d'espionnage contre les organisations gouvernementales, les opérateurs d'infrastructure, les entreprises, les chercheurs et les particuliers ».*

L'entreprise en va jusqu'à spéculer sur le fait que le développement de Regin a pris *« des mois, si ce n'est des années »* et il en conclut que ***« les moyens et le niveau de compétence mis en oeuvre derrière Regin indique que ce doit être un des principaux outils de cyber-espionnage utilisés par les Etats-nations ».***

Ah, mais quels Etats-nations ? Faisons un pas en avant, et **nous voyons la Grande-Bretagne, les Etats-unis et leurs agences de renseignement respectives, GCHQ (le Government communications Headquarters) et NSA.**

Il y a quelques temps, Edward Snowden a révélé que les agences ont monté des attaques cyberpirates contre Belgacom, un fournisseur belge de services téléphoniques et internet, et contre des systèmes informatiques européens, mais il ne savait pas quels types de logiciels avaient été utilisés dans les attaques.

Maintenant nous savons : c'était Regin, un malware qui se présente sous la forme d'un logiciel Microsoft légitime et vole des données dans les systèmes infectés, ce qui en fait un outil inestimable pour les agences de renseignement qui désirent pénétrer les réseaux informatiques étrangers.

C'est vrai aussi, diriez-vous. Après tout, la raison pour laquelle nous avons GCHQ, c'est bien pour espionner ces vilains étrangers. L'agence était, ne l'oublions pas, à l'origine une branche de *Bletchley Park*, dont la mission était d'espionner les Allemands pendant la Seconde guerre mondiale.

Donc, peut-être que la nouvelle selon laquelle les Belges, en dépit des plus grands efforts déployés par les Monty Python, sont nos amis – ou que la Grande-Bretagne fait partie de l'UE – n'a pas encore été décodée par GCHQ ?

Espionner ses amis comme ses ennemis est un vieux principe de l'art de gouverner. On en usait habituellement pour des raisons de « sécurité nationale » ; maintenant c'est pour des raisons de « cybersécurité » et cela pose un nouveau problème. *Qu'est-ce que la cybersécurité en fait ? Qu'est-ce que GCHQ et NSA essaient de garantir ? Est-ce la sécurité du cyberespace – c'est-à-dire Internet ? Ou une partie du réseau ? Et si oui, laquelle ?*

Ici, certaines lignes apparemment sans conséquences d'un des documents Snowden prennent tout leur sens. *« Les faits qui sont contenus dans ce programme »*, peut-on lire, *« constituent une combinaison d'un grand nombre de faits, hautement sensibles, liés à la mission cryptologique générale de NSA. Leur révélation non-autorisée (…) causerait des dégâts exceptionnellement graves à la sécurité nationale américaine. La perte de ces informations pourrait gravement compromettre certaines relations cryptologiques hautement sensibles, américaines comme étrangères, des investissements de plusieurs années comme ceux futurs de la NSA, et sa capacité à exploiter le cyberespace étranger tout en protégeant le cyberespace américain ».*

Notez bien cette dernière clause. « La cybersécurité » signifie deux choses en fait : premièrement, sécurité nationale, et deuxièmement, que le seul coin de cyberespace dont nous nous préoccupons est le nôtre. **Nous pouvons exploiter le moindre centimètre dans le reste du monde virtuel à nos propres fins (nationales).**

Cela donne carte blanche, par exemple, à la sape de la sécurité en-ligne de quiconque, en affaiblissant les cryptages utilisés pour des transactions commerciales ; le recours à des « exploits zéro-jour » acquis auprès de hackers qui puissent ensuite être utilisés contre les organisations ciblées ; et la diffusion de malware tels que Regin là où est notre bon plaisir.

Bienvenue dans notre monde connecté.

John Naughton

The Guardian

Article original : Forget North Korea – the real rogue cyber operator lies much closer to home, The Guardian, le 7 décembre 2014.

Traduction MA pour http://www.solidarite-internationale-pcf.fr/