LA FIN DU MONDE, “MADE IN CHINA”

LE 4 AOÛT 2011 ***OLIVIER TESQUET***

Dans un rapport, l'entreprise américaine McAfee affirme avoir découvert la plus grande attaque informatique répertoriée à ce jour, visant plus de dix pays. Déjà, les regards se tournent vers la Chine, et c'est tout sauf un hasard.

Cette fois-ci, c’est sûr, certain, gravé dans le marbre, écrit dans un épais rapport. Cette fois-ci, ce sont les Chinois. De quoi les accuse-t-on? D’être derrière la plus vaste attaque informatique jamais enregistrée, inédite par son ampleur et sa durée. Tant et si bien que *Vanity Fair*, qui s’est fait le premier écho de l’affaire dans la presse, **parle** d’une *“campagne de cyber-espionnage sans précédent”* et va jusqu’à consacrer un dossier à la **menace sino-technologique**.

Mise au jour par l’éditeur de logiciels de sécurité américain McAfee, l’opération *“Shady RAT”* (*“outil louche de contrôle à distance”* en bon français, ou *“Mouchard Ténébreux”* , **dixit RFI**) aurait pillé les informations de plus de 70 gouvernements, entreprises ou organisations pendant cinq ans. Pourtant, Dmitri Alperovitch, le directeur de recherche qui a identifié la cellule souche et **la décrypte sur son blog** et dans un rapport de 15 pages (**PDF**, en), se garde bien d’accuser ouvertement Pékin. En revanche, il dédouane *“les mouvements activistes vaguement organisés”* (des **Anonymous** à **LulzSec**), pour évoquer un commanditaire autrement plus coordonné:

> ***Même si l’ampleur et la durée de Shady RAT peuvent choquer ceux qui n’ont pas été intimement impliqués dans les investigations sur ces opérations précises d’espionnage, j’aimerais vous prévenir que ce que je décris ici a été une opération spécifique conduite par un seul acteur.***

La muleta chinoise

Parmi les victimes de ce grand détroussage dont les conséquences immédiates restent assez floues, les États-Unis sont les plus touchés: sur 72 cibles, 49 sont américaines. Et pas n’importe lesquelles, puisque 13 entreprises d’armement et plusieurs agences gouvernementales figurent dans la liste. Concomitance ou signe avant-coureur, plusieurs mastodontes du complexe militaro-industriel **avaient été dépouillés** il y a quelques semaines. Parmi eux, Lockheed Martin, L-3 Communications et Northrop Grumman, tous pesant des dizaines de milliards de dollars.

Aux côtés des États-Unis, on retrouve une douzaine d'autres pays, dont le Canada, le Japon, la Corée du Sud, l'Allemagne, le Royaume-Uni ou l'Inde. La présence de Taïwan serait quant à elle la preuve formelle de l'implication chinoise. C'est en tout cas l'avis de James Lewis, un analyste du Center for Strategic and International Studies (CSIS), un think tank bipartisan de Washington D.C. :

> ***Tous les signes pointent vers la Chine… Qui d'autre espionne Taïwan?***

La conclusion peut sembler hâtive, toujours est-il qu'elle a été relayée par bon nombre d'experts, y compris **chez Microsoft**. Toujours prompts à pointer du doigt un Empire du milieu décidément bien encombrant, ceux-ci s'en donnent à cœur joie. Très à la mode dans les milieux de l'intelligence économique – le **précédent Renault** suffit pour s'en convaincre – le chiffon rouge chinois n'est pas non plus une muleta créée *ex nihilo* et agitée par des pays occidentaux empêtrés dans une révolution numérique qui les submerge. En 2010 aux Etats-Unis, 11 citoyens chinois **ont été poursuivis pour espionnage**. Dix d'entre eux s'intéressaient à des objectifs de haute technologie.

Course aux cyber-armements

Même si les autorités chinoises passent leur temps à **disqualifier les accusations américaines** en réclamant des preuves que le camp d'en face est incapable de fournir, les bataillons de ***honkers*** (ces hackers patriotes formés aux frais du Parti) et l'attaque surmédiatisée **contre Google** début 2010 ont définitivement changé la donne géopolitique.

Désormais, selon une rhétorique post-Guerre froide largement alimentée par les deux discours d'Hillary Clinton **sur la liberté d'Internet**, les éditorialistes évoquent une ***"course aux cyber-armements"*** où les capacités de réactions aux virus remplacent la bombe H et les fusées. S'adressant à un parterre de spécialistes de la sécurité informatique lors de la conférence Black Hat à Las Vegas, un vétéran de la CIA, Cofer Black, a affirmé que ***"la guerre des codes"*** était sur le point d'éclater (une terminologie que nous utilisions déjà **début juin**, avec une lecture sensiblement différente).

Auditer le matériel

Problème, ce nouveau terrain de jeu, doublé d'un paradigme stratégique aux contours pas très nets, vient se juxtaposer à une réalité quelque peu déconcertante. Faites donc le test: regardez derrière vos unités centrales, sous vos ordinateurs portables, et comptez le nombre de produits estampillés *"Made in China"* (en réalité, le bout de la chaîne, **comme l'expliquait** le *New York Times* dès 2006). Tant et si bien que le Congrès américain commence à auditionner des spécialistes inquiets. L'un d'entre eux, Kevin Coleman, **estime qu'il vaudrait mieux auditer** le matériel du Pentagone ou des agences fédérales avant de jouer les vierges effarouchées:

> ***Si nous ne décidons pas de tout fabriquer chez nous, alors il faut améliorer les outils et les techniques de validation.***

Si demain, Foxconn, le sous-traitant chinois d'Apple, **décide de programmer ses robots** pour qu'ils implémentent des malwares dans des iPhone destinés à la vente mondiale, les États-Unis risquent fort d'être pris au dépourvu. Et ce n'est pas tout. Il y a un peu plus d'un an, 600 responsables de la sécurité informatique de grandes entreprises **répondaient à un sondage** et établissaient le palmarès des pays les plus perméables aux attaques informatiques. Les États-Unis arrivaient en tête, avec 36% des suffrages, devant la Chine. L'étude était commissionnée par… McAfee.

Crédits photo: McAfee, Flickr CC ***kallao***, ***thelustlizardofmelancholycove***

particulier les États-Unis. Pourquoi ne le ferait-elle pas? En fait, tout un chacun espionne tout un chacun. Quant à McAfee, je ne leur fais absolument pas confiance. Lancer un rapport comme celui-là, c'est s'assurer des contrats lucratifs.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CMF
le 5 août 2011 - 3:46 • SIGNALER UN ABUS - PERMALINK

Faut-il vraiment un rapport pour montrer que les Chinois espionnent le monde occidental ?
Je ne serai pas étonnée de savoir qu'il en est de même inversement.
Cette accusation serait pour faire peur aux chinois et les ralentir ? Que de temps perdu …

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PLOCK
le 5 août 2011 - 9:35 • SIGNALER UN ABUS - PERMALINK

les usa, ferait bien de balayer devant leur porte dns un premier temps, avec leur NSA et le syteme de surveillance planétaire "échelon" qui dispose de plus de 200 satellites, des antennes d'interceptions de telecommunication reparties sur toute la planète, etc, etc…

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PGP
le 8 août 2011 - 11:20 • SIGNALER UN ABUS - PERMALINK

Peut-être que tout-un chacun serait moins vulnerable si le logiciel libre devenait la norme? Une bonne question pour un specialiste et fini les gros sous pour McAfee.

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DTH
le 8 août 2011 - 13:07 • SIGNALER UN ABUS - PERMALINK

Ah ? McAfee ? L'entreprise dont le président avait sorti en 2008 de son chapeau un chiffre totalement affabulateur sur les dégâts de la cyber-délinquance mondiale reprit en boucle pour justifier tout un tas de politiques sécuritaires ?

Tiens ? les Etats-Unis, le pays dont on sait qu'il a officiellement demandé à l'ensemble de son corps diplomatique de se transformer en agents de terrains au service du renseignement (récolte d'ADN etc.) ?

Je ne sais pas pourquoi mais autant je ne ferais pas confiance à du matos informatique venue d'une firme chinoise (et non pas seulement fabriqué), autant ce rapport que je ne prendrais même pas la peine de lire m'inspire un large sourire…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

EDOM
le 21 janvier 2012 - 10:28 • SIGNALER UN ABUS - PERMALINK

La future plateforme politique de la réglementation d'internet ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

2 pings

La fin du monde, "made in China" – Owni | What's New France le 4 août 2011 - 18:44

[...] Owni [...]

#FrenchRevolution #WorldRevolution La fin du monde, “made in China” par Owni.fr : #FrenchRevolution le 5 août 2011 - 1:39

[...] http://owni.fr/2011/08/04/espionnage-hacking-chine-etats-unis-cyberguerre/ [...]