LES DESSOUS DU PIRATAGE DE BERCY

LE 26 MARS 2011 ***JEAN MARC MANACH***

Les pirates informatiques du ministère de l'Economie avaient commencé à préparer leur infiltration au moins six mois avant que les autorités ne mettent un terme à leur opération d'espionnage. Une enquête OWNI.

Nombreux sont ceux qui se sont demandés comment des pirates informatiques avaient réussi à s'infiltrer dans les 150 ordinateurs de la direction du Trésor de Bercy, mais également pourquoi l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**) avait attendu trois mois pour mettre un terme à cette opération d'espionnage.

Près de quinze jours après la révélation des faits, les témoignages recueillis par OWNI montrent que l'opération de transparence effectuée par les autorités autour de cette affaire d'espionnage signe un tournant politique dans l'approche de la sécurité informatique. La France n'est plus victime du syndrome de Tchernobyl[1]: les problèmes de sécurité informatique ne s'arrêtent plus à nos frontières, et l'ANSSI, chargée d'y faire face, a décidé de le faire savoir.

Reste à savoir si, comme semblent le penser certains enquêteurs de la Direction centrale du renseignement intérieur (DCRI), les espions ont bénéficié de la complicité d'une "*taupe*", ou si, comme le soulignent d'autres sources, la complexité et l'ampleur de l'infiltration s'expliquent par le savoir-faire professionnel de ceux qui ont mené l'opération.

Un virus créé tout spécialement pour les cerveaux de Bercy

Comme l'**explique** Jérome Saiz, rédacteur en chef de SecurityVibes France, citant une source proche du dossier, le premier ordinateur à avoir été infecté ne l'a pas été parce qu'un fonctionnaire de Bercy a inconsidérément ouvert une pièce jointe annexée à un spam, mais parce que le ou les pirates avaient envoyé "*à un destinataire particulièrement bien choisi*" un e-mail accompagné d'un fichier .pdf qui avait été piégé au moyen d'un code malicieux développé tout spécialement pour l'occasion. Explication :

> ***Rien de nouveau ici, c'est une technique courante : un mail légitime est intercepté, sa pièce jointe piégée et le tout est renvoyé au destinataire, en se faisant passer pour l'expéditeur original***

Cette technique est d'autant plus sophistiquée qu'il faut d'abord :

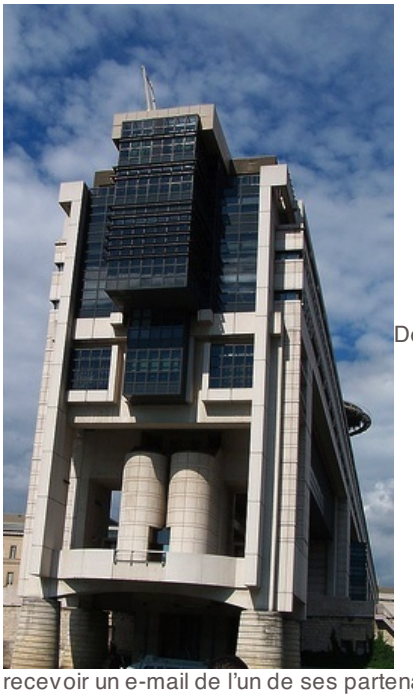
- soit parvenir à intercepter des e-mails échangés par des fonctionnaires hauts placés
- soit effectuer un criblage très précis des cibles visées afin de pouvoir usurper une identité, et créer de toute pièce un "*vrai-faux*" mail ayant toutes les apparences d'un vrai

Elle n'en serait pas moins "*courante*" dans les hautes sphères internationales, comme l'**expliquait l'an passé** à Jérôme Saiz le responsable de la sécurité informatique du Conseil de l'Europe:

> ***Des documents pertinents, émis par le Conseil, sont régulièrement interceptés, piégés dans la journée et renvoyés dans le bon bureau, à la bonne personne qui suit le dossier en question.***

Si le code malveillant a pu s'installer dans l'ordinateur, c'est qu'il avait été créé tout spécialement pour échapper aux radars des antivirus, mais également parce que le ministère de l'Economie n'avait pas installé les systèmes de **défense en profondeur** préconisés par l'ANSSI afin de détecter les signaux faibles révélateurs de telles tentatives d'attaque, **sondes dédiées**, ou **taps**, permettant de surveiller un réseau en toute discrétion et sans le perturber.

Un espion au ministère de l'Economie?



De fait, c'est un fonctionnaire de Bercy qui, intrigué de recevoir un e-mail de l'un de ses partenaires alors que ce dernier n'était pas présent à ce moment-là, a alerté les responsables sécurité du ministère. Ceux-là même ont alerté l'ANSSI qui, découvrant l'infection de l'ordinateur, a d'abord mandaté trois, puis, au vu de l'ampleur du problème, 40 personnes au total, dont 20 à 30 mobilisées en permanence, afin de parer l'attaque.

Il a fallu identifier l'ensemble des ordinateurs compromis, mais également étudier le *modus operandi* et les vecteurs de l'attaque, les heures à laquelle les espions se connectaient, comment, les documents qui avaient fuité… et en référer à l'Élysée puis, comme l'avait déclaré **François Baroin sur Europe 1**, leur envoyer des "*leurres*".

Toutes ces opérations expliquent pourquoi il a fallu attendre trois mois entre la première alerte et la révélation de l'affaire. D'autant qu'il fallait également préparer le nettoyage du réseau et des ordinateurs de Bercy et, comme le souligne Jérome Saiz, l'application des correctifs manquants, "*et bien entendu l'installation des sondes et l'audit du trafic* ", le week-end du 5 mars.

D'après nos informations, le criblage des personnes dont les ordinateurs ont été infectés aurait commencé six mois au moins avant la détection de l'opération, et sa précision serait telle que certains enquêteurs de la DCRI pencheraient pour la thèse d'une taupe, d'un "*tonton*" qui, de l'intérieur même de Bercy, aurait aidé les espions à préparer leur infiltration.

Il est en effet courant, en la matière, de procéder à une enquête fouillée concernant les cibles à espionner afin de mieux préparer le lancement, et le déroulé, du piratage de leurs ordinateurs.

Tout en reconnaissant une "*opération de renseignement très bien menée* ", d'autres sources mettent en doute l'hypothèse d'une taupe infiltrée, avançant que l'organigramme du Trésor est disponible publiquement, tant **sur le site** du ministère que **sur l'annuaire** de service-public.fr, numéros de téléphones et adresses e-mail à l'appui.

La fin du "syndrome de Tchernobyl"

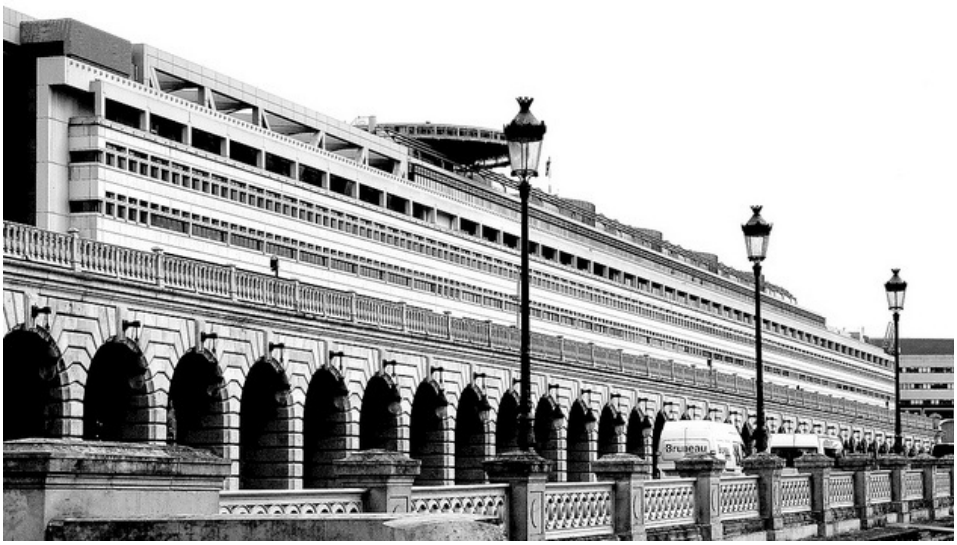
On ne saura peut-être jamais, ou pas avant un certain temps, qui est derrière cette affaire d'espionnage, ni ce qui les intéressait dans les préparatifs du G20 ou les autres documents qu'ils ont réussi à exfiltrer… Mais d'après nos sources, la complexité du mode opératoire indique qu'il ne peut s'agir que d'une équipe de professionnels. Nous serions donc en présence d'une affaire d'espionnage, et pas d'un **acte perpétré par des *Anonymous*** politiques ou des pirates opportunistes.

En déclarant, sur Europe 1, que "*tout a été mis en oeuvre (…) pour envoyer des leurres* " et que "*la communication de ce matin devrait apporter l'information aux hackers : ils ont été repérés"*, François Baroin leur a d'ailleurs tendu une perche. Si d'aventure des documents issus de ce piratage venaient à être exploités, la DCRI aurait beau jeu d'identifier les espions pirates de Bercy. En revanche, leur publication sur un site de type WikiLeaks, ne permettrait probablement pas de remonter à la source.

En **expliquant à Paris-Match** qu'il s'agissait de "*la première attaque contre l'Etat français de cette ampleur et à cette échelle*", Patrick Pailloux, le directeur de l'ANSSI, a contribué à relativiser les failles de Bercy en matière de sécurité informatique. Mais il a également mis en avant le travail ainsi que la montée en puissance et en capacité de ses équipes, dont les compétences, à en croire les **profils de poste recherchés**, sont particulièrement pointues.

En tout état de cause, cette affaire montre que si Bercy, contrairement à d'autres ministères, n'était visiblement pas préparé pour empêcher une telle attaque, "*c'est la preuve que cela n'arrive pas qu'aux autres*", comme nous l'avait **expliqué** un porte-parole de l'ANSSI:

> ***C'est moins un coup de projecteur sur l'agence qu'un formidable moyen de faire de la prévention dans les institutions. Il n'y a pas de nuage de Tchernobyl qui s'arrête aux frontières dans le domaine de la sécurité informatique.***



Quand le contre-espionnage diabolisait les hackers

Cette approche des questions de sécurité informatique est un véritable tournant dans la façon dont l'État aborde ses sujets. Et nombreux sont les **journalistes et blogueurs** férus de sécurité informatique qui, de fait, avaient d'abord **exprimé des doutes**, portant notamment sur le timing de cette annonce, le mode opératoire (**vieux comme une antiquit é**), la "*piste chinoise*" ou encore le côté "*plan com'"* de cette révélation.

Pour mieux comprendre ce tournant, il faut revenir sur l'histoire des hackers, et plus particulièrement sur la façon dont ils ont été perçus et gérés par les autorités françaises.

En 1989, le **Chaos Computer Club** allemand, le plus important des groupes de hackers dans le monde[2], est impliqué dans la première affaire de cyberespionnage internationale. Plusieurs de ses membres avaient piraté des ordinateurs américains pour le compte du KGB. Le cadavre de l'un d'entre-eux, **Karl Koch**, a été retrouvé carbonisé dans une forêt, la police concluant au suicide.

Découvrant que des jeunes bidouilleurs pouvaient ainsi mettre en péril la sécurité nationale, la Direction de la surveillance du territoire (DST), en charge du contre-espionnage, décide

alors de **recruter** de jeunes hackers, profitant du service militaire alors obligatoire, pour attirer en son sein un certain nombre de petits génies de l'informatique.

Parallèlement, la DST **demande** à un musicologue et informaticien, **Jean-Bernard Condat**, de créer le **Chaos Computer Club de France**, afin de mieux pouvoir cerner et de surveiller le milieu des hackers français.

L'opération d'infiltration ne fut révélée qu'en 1995, par Jean Guisnel, dans un livre intitulé **Guerres dans le cyberespace, services secrets et Internet**, mais le mal était fait : en France, depuis, plus personne ne se revendique officiellement de l'étiquette "*hacker*", de peur de passer pour une taupe de la DST, ou de se retrouver placé sous sa surveillance rapprochée.

La cécité informatique des autorités

Eric Filiol, lieutenant-colonel de l'armée de Terre, qui se définit lui-même comme un "*corsaire*", pour se démarquer des "*pirates*", et qui avait créé un laboratoire de cryptologie et de virologie du temps où il était militaire, **estimait** ainsi l'an dernier que "*le problème c'est que la France a pendant longtemps diabolisé les hackers*", contribuant à placer un écran de fumée au-dessus des questions de sécurité informatique.

Lorsque je l'avais **interviewé** en 2010, il déplorait la "*défiance totale vis-à-vis de l'informatique (et la) totale méconnaissance*" ayant amené les responsables politiques à voter les lois **Hadopi** puis **Loppsi** alors que, pour lui, l'État devrait s'appuyer sur les hackers, plutôt que de les diaboliser. Signe de cette déconnexion des autorités avec la réalité de la sécurité informatique :

> ***En France, la sécurité informatique ressemble aux nuages nucléaires: les problèmes s'arrêtent aux frontières. Pourtant, on a dénombré pas moins de 600 attaques critiques envers l'administration française en 2008 !***

Au vu de ce passif, on comprend un peu mieux les doutes exprimés par ce même Eric Filiol qui, **réagissant** à l'annonce du piratage de Bercy, avait d'emblée mis en doute l'hypothèse chinoise, un ***péril jaune*** régulièrement avancé par les responsables politiques en matière d'espionnage informatique. Daniel Ventre, ingénieur chercheur au CNRS et auteur de deux livres sur la guerre de l'information, exprimait les mêmes réserves en notant qu'"*il ne sortira probablement pas grand chose de cette affaire*" :

> ***La Corée du Sud a elle aussi connu des déboires similaires il y a quelques temps, à l'occasion du G20. Elle a accusé la Corée du Nord, la Chine, et en a profité pour valider son projet de création d'unités de cyberdéfense.***

En l'espèce, et comme OWNI s'en était d'ailleurs étonné en évoquant un **piratage qui tombe à pic**, l'ANSSI venait tout juste d'être dotée, un mois plus tôt, de capacités de "***cyberdéfense***" la faisant clairement monter en puissance, et alors même que le coordonnateur national du renseignement avait de son côté déclaré, fin janvier, qu'"*il s'agit d'un dossier que le Président de la République suit de très près*".

Si tu ne viens pas à Lagardère, Lagardère ira à toi

De fait, le timing de cette révélation, à 7h du matin, **sur ParisMatch.com**, puis par le ministre du Budget François Baroin, interrogé par Jean-Pierre Elkabbach à 8h **sur Europe 1**, avait de quoi susciter quelques interrogations. Ces médias sont en effet les deux vaisseaux amiraux du groupe Lagardère Publishing, propriété du ***"frère"*** de Nicolas Sarkozy.

A ceci prêt qu'il ne s'agissait nullement d'une collusion mais bel et bien d'un hasard complet. Contacté par OWNI, David Le Bailly, le journaliste de Paris Match à l'origine du scoop, nous explique qu'il avait eu vent, le lundi précédent et de la part d'une personne qui ne connaît pas grand chose aux questions de sécurité informatique, d'une "*attaque informatique sur Bercy*".

Après avoir recoupé l'information, il contacte l'ANSSI. Son directeur, Patrick Pailloux, le rappelle le lendemain et lui fait comprendre qu'il ne répondra à aucune question, mais que si le journaliste peut attendre jusqu'au week-end suivant, il lui raconterait tout, "*en exclusivité* ".

Vendredi, une opération de maintenance informatique est annoncée à Bercy. L'information remonte jusqu'au journal Libération, qui interroge le ministère de l'Economie et des finances, mais ne parvient pas à recouper l'information.

Dimanche soir, Patrick Pailloux répond aux questions de David Le Bailly, lui demandant de garder l'embargo jusqu'au lundi 9h, de sorte que les fonctionnaires de Bercy découvrent le message qui allait s'afficher sur leurs ordinateurs avant d'entendre parler de cette histoire dans la presse :

> ***Comme cela a été annoncé vendredi, d'importantes maintenances informatiques ont été effectuées afin de renforcer la sécurité. Cette opération a été décidée suite à des attaques informatiques visant le réseau informatique de Bercy.***

Mais le journaliste de Paris Match, découvrant le dimanche soir que François Baroin devait être interviewé par Elkabbach sur Europe 1, le lundi à 8h20, craint de se voir griller son scoop, et décide finalement de le publier à 7h.

En tout état de cause, l'information avait commencé à fuiter, les fonctionnaires de Bercy commençaient à en causer, 12 000 postes étaient concernés par l'opération de maintenance, il était impossible de continuer à garder le secret.

Des sources proches du dossier nous ont confirmé que l'ANSSI avait prévu, avant même que David Le Bailly ne les contacte, de nettoyer tous les ordinateurs de Bercy ce week-end là, mais également de communiquer sur le sujet. Par contre, François Baroin n'aurait pas prévu, initialement, d'évoquer l'affaire sur Europe 1.

Contactée, l'ANSSI, qui a été très sollicitée suite à la révélation de l'affaire par Paris Match, et qui avait fait un **point presse** le lendemain, a décidé de ne plus s'exprimer sur la question au motif qu'elle a répondu à toutes les questions et que tout a été dit. Reste, maintenant, à attendre les conclusions de l'enquête de la DCRI.

—

Photos CC **Vicent-t**, **Pierre Numérique**, **regis frasseto**, **jfgornet**, **jfgornet**, **regis frasseto**

1. **selon Jean-Marie Cohen**, le syndrome de Tchernobyl peut se définir ainsi: "*Dans n'importe quel contexte de crise fortement médiatisée, on ne croit plus les autorités en France, réputées mentir. Pour que la communication officielle soit crue, elle doit être cautionnée par des instances extérieures*". [↩]
2. Le "CCC" créé en 1981 est connu notamment pour avoir démontré que, contrairement à ce qu'affirmaient les autorités, on pouvait détourner de l'argent grâce au minitel allemand [↩]

NICOLAS PATTE
le 26 mars 2011 - 15:56 • SIGNALER UN ABUS - PERMALINK

Et l'administration française sous Linux c'est pour quand? /-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ABITBOL
le 26 mars 2011 - 17:34 • SIGNALER UN ABUS - PERMALINK

Linux : le meilleur moyen de mettre une administration hors d'état de nuire ! (cf administration allemande)

désolé pour le troll, mais c'était plus fort que moi …

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

STANISLAS
le 27 mars 2011 - 13:43 • SIGNALER UN ABUS - PERMALINK

Excellent article. J'apprécie de voir un texte expliquer concrètement les choses sans verser dans le jargon techno-technique ou à l'inverse employer des termes et un ton gloubi boulga hollywood avec BREAKNEWS CYBERWAR !!! et jingle de la mort et force trompettes saturant les enceintes…

J'ai lu ailleurs, une hypothèse intéressante également sur le fait que le G20 n'aurait pas été la cause de l'attaque mais le thème. C'est à dire que la préparation de l'événement a

donné aux attaquants la possibilité de rédiger un mail piégé très crédible. Je ne sais pas si vous avez des informations qui peuvent infirmer cette hypothèse. Mais avec mon mauvais esprit j'ai du mal à croire qu'une équipe de pros investit plus de 6 mois de boulot et moyens de haut niveau pour aller racler des notes sur un événement comme celui là…

J'ai également tenté de corroborer cette interprétation, mais… non, je ne sais pas, mes interlocuteurs se contentant de confirmer que furent visés les hauts fonctionnaires en charge du G20, sans pouvoir être en mesure de préciser si d'autres informations, hors G20, ont fuité ou étaient ciblées.

En tout cas, la communication de l'ANSSI sur ce dossier est très encourageante. C'est vrai qu'il y a une vrai rupture avec le passé. L'avenir nous dira si nos dirigeants présents et à venir tiendront le cap : on croise les doigts.

C'est clair que dans encore de très très nombreuses administrations et entreprises il y a un énorme changement de mentalité à réaliser. On ne s'en sortira pas avec des millions et de la technique. Il faut également que les utilisateurs s'y mettent.

Cela me fait penser à la sécurité routière. Après avoir améliorées les voitures et les infrastructures routières, il reste que si l'automobiliste dépasse la limite raisonnable de vitesse, en cas de choc, il y laissera la vie.

C'est banal de dire qu'un bon RSSI doit sensibiliser ses utilisateurs. Mais j'ai moins vu des explications et de bons exemples sur le "comment". La communication est un juste équilibre à trouver dans le contenu du message, sa forme, sa cible, le moment où il est délivré, sa répétition, son adéquation avec les préoccupations métiers, etc. C'est loin d'être trivial. Et c'est un boulot à recommencer encore et encore. A recommencer sans gaver les gens…

En tout cas, encore bravo pour votre article : ça aide.

Merci; je n'ai pas pu le vérifier, et ne l'ai donc pas écrit dans mon papier, mais un certain nombre de hauts fonctionnaires ne comprenaient pas ce pour quoi ils devaient arrêter d'utiliser leurs PC; il a donc fallu, non seulement passer par leurs supérieurs hiérarchiques, mais également faire jouer les "relations" de certains rétifs, et passer par ceux qui, ayant fait les mêmes grandes écoles qu'eux, pouvaient leur faire comprendre que c'était vraiment important.

Reste que, et au final, l'ANSSI semble avoir vraiment été entendue; ce qui constitue une bonne nouvelle, au vu de la perception que semblaient avoir jusque là les plus hautes autorités en matière de sécurité informatique.

manhack

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

WILNOCK
le 5 avril 2011 - 4:30 • SIGNALER UN ABUS - PERMALINK

Merci pour ce retour d'information detaille et complet. Il reste a esperer que cette communication ouverte n'aura pas ete le fait d'un One Shot, mais que d'autres axe de communication moins anxiogene et plus productif se mettent en place quand il sera question de parler de securite informatique, prevention et protection.

NICOLAS troll sur l'utilisation de Linux en administration, j'aurai tendance a croire que dans ce cas precis, avec un virus specialement cible pour Bercy, Linux ou pas, le groupe cible qui veut s'attaquer a Bercy ne se serai pas degonfler pour autant.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

2 pings

Texto casi Diario » Blog Archive » Italo Calvino: "El verdadero oficio de la literatura consiste en escribir de tal manera que los demás se pongan nerviosos; en provocar reacciones. Si no, uno se duerme". le 27 mars 2011 - 10:45

[...] Les dessous du piratage de Bercy: Les pirates informatiques du ministère de l'Economie avaient commencé à préparer leur infiltration au moins six mois avant que les autorités ne mettent un terme à leur opération d'espionnage. Une enquête OWNI. _____ Enrique Vila-Matas: Surfear. _____ Pulso de España (avance libro encuesta a 5.000 personas) El País. [Comments (0)] [link] [...]

Les yeux carrés « Hacker Area …….. ……..Territoire Hacker le 6 juillet 2012 - 16:13

[...] Le faux club de pirates des services de renseignement (passage “Quand le contre-espionnage diabolisait les hackers”) Share this:TwitterFacebookJ'aime ceci:J'aimeBe the first to like this. Tags:full disclosure, Hackito Ergo Sum 2010, hacktivisme, histoire Comments RSS feed [...]