BERCY, LE PIRATAGE QUI TOMBE À PIC

LE 7 MARS 2011 ***OLIVIER TESQUET***

Faut-il avoir peur du piratage de 150 ordinateurs au ministère de l'Economie et des Finances? C'est surtout l'occasion pour l'Etat de communiquer autour de la sécurité informatique.

"Gigantesque affaire d'espionnage à Bercy" . Le titre de **l'article de Paris-Match** publié lundi 7 mars ne laisse que peu de place à la nuance. Depuis le mois de décembre, 150 ordinateurs du ministère de l'Economie et des Finances auraient été *"infiltrés par des hackers"* . Que cherchaient-ils? *"Pour l'essentiel, des documents liés à la présidence française du G20 et aux affaires économiques internationales"*. Malgré la prudence langagière qui accompagne ce genre d'événements, le propos se précise d'emblée.

Déjà, les spéculations vont bon train sur l'attribution de cette attaque sans précédent. Comme lors de **l'épisode Stuxnet** il y a quelques mois, des légions d'experts planchent sur les commanditaires de cette intrusion, et des objectifs qu'ils poursuivent. Pourtant, la chronologie est plus saillante que toutes les hypothèses. *"Depuis deux mois, entre 20 et 30 personnes de l'ANSSI travaillent jour et nuit sur cette affaire"*, estime Patrick Pailloux, directeur de l'Agence nationale de sécurite des systèmes d'information (**ANSSI**), en première ligne dans ce dossier. Alors pourquoi avoir attendu aujourd'hui pour évoquer publiquement le sujet?

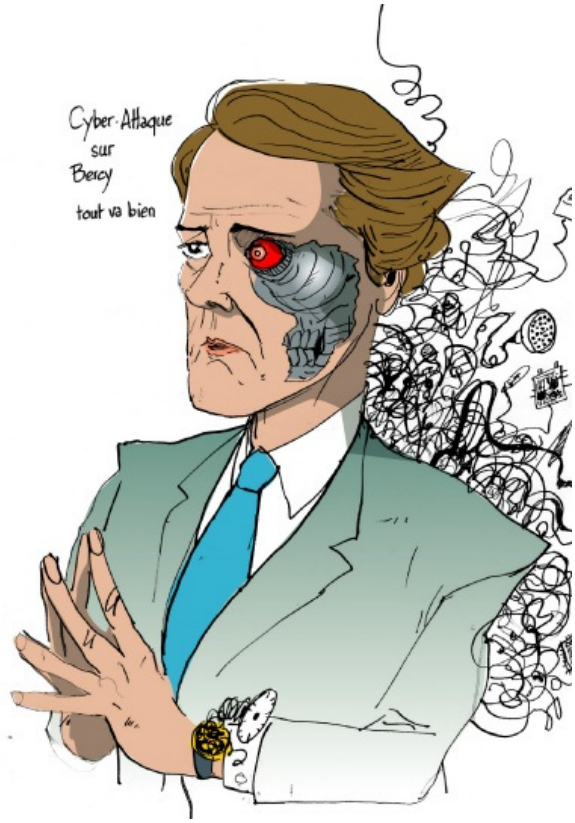
Nouvelles prérogatives

Le **10 janvier** dernier, dans une **longue interview** au site lTespresso, le Directeur Général adjoint de l'ANSSI, Michel Benedittini, revient sur le cahier des charges de l'agence, créée en juillet 2009. De 120 employés, elle devrait en compter 250 à l'horizon 2012, et être dotée d'une enveloppe de 90 millions d'euros, sept fois supérieur à **celui de l'Hadopi:**

> ***L'ANSSI n'est pas touchée par les restrictions budgétaires globales au sommet de l'État. Cela illustre une volonté des décideurs politiques qui sont convaincus du travail à accomplir pour changer complètement de braquet en matière de cyber-défense.***

Auditionné à l'Assemblée, le **26 janvier**, Bernard Bajolet, coordonnateur national du renseignement, explique qu'"*après avoir renforcé l'agence nationale de sécurité des systèmes d'information, le gouvernement va créer un poste de directeur des systèmes d'information de l'État, chargé de sécuriser les réseaux des ministères*", et précisé qu'"*il s'agit d'un dossier que le Président de la République suit de très près*".

Le **11 février**, un **décret du Premier ministre** vient modifier la compétence de l'ANSSI, qui devient l'Agence nationale de défense des systèmes d'information. Cette validation des propos tenus quelques semaines auparavant par Benedittini crée une nouvelle prérogative. Désormais, c'est l'agence qui conseillera l'État en cas de menace contre l'intégrité de ses infrastructures. Contactée par OWNI à cette époque, l'ANSSI avait nié tout agenda et rappelé que cette légère mutation s'inscrivait *"dans le cadre du livre blanc de la Défense, et des leçons tirées de l'exercice* ***Piranet***", du nom donné au plan Vigipirate de l'internet.



Au même moment, la jeune autorité publie un opuscule (**PDF**) intitulé *"Défense et sécurité des systèmes d'information: Stratégie de la France"*. Le secrétaire général de la défense et de la sécurité nationale (SGDSN), Francis Delon y détaille quatre grands *"objectifs stratégiques, en comparant le cyberespace à de "nouvelles **Thermophyles**"*:

Être une puissance mondiale de cyberdéfense
Garantir la liberté de décision de la France par la protection de l'information de souveraineté
Renforcer la cybersécurité des infrastructures vitales nationales
Assurer la sécurité dans le cyberespace

Eteindre Internet

Suivent *"sept axes d'effort"* , parmi lesquels *"communiquer pour informer et convaincre"* . C'est exactement ce qui est en train de se passer. Quelques jours après la publication du décret au journal officiel, Patrick Pailloux **pose les jalons** de cette nouvelle doctrine. *"Nos observations montrent que la menace croit, menace que nous classons en espionnage, perturbation et destruction"*, explique-t-il alors. Il rappelle également que l'ANSSI aura le pouvoir de déconnecter une partie du réseau si le besoin s'en fait sentir:

> ***C'est la nécessité de déterminer qui édicte les règles en cas d'attaque pour que, lorsqu'on demande à quelqu'un de prendre une mesure de déconnexion, de filtrage, etc. on ne se pose pas juridiquement la question pendant trois heures pour savoir qui doit édicter cette règle.***

En d'autres termes, sa structure aura le pouvoir d'éteindre un pan du web si *"les opérateurs d'importance vitale"* sont touchés. "*Ce qui est certain* , **précise** Pailloux à 01Net, *c'est que nous devrons être en mesure de donner des instructions aux acteurs concernés, dont les opérateurs de communications électroniques. Il pourra s'agir effectivement de leur demander de bloquer du trafic en provenance de machines utilisées pour mener des attaques*". Tout dépend alors de l'endroit où on positionne le curseur.

Dernière étape enfin, le **22 février**, avec la nomination, **par décret là encore**, de **Jerôme Filippini** au poste de directeur des systèmes d'information (DSI) de l'Etat. Rattaché à Matignon, il *"oriente, anime et coordonne les actions des administrations de l'État visant à*

améliorer la qualité, l'efficacité, l'efficience et la fiabilité du service rendu par les systèmes d'information et de communication." Cette désignation marque une nouvelle étape: désormais, la cyberdéfense est une priorité nationale.

D'après certains connaisseurs du milieu, Nicolas Sarkozy en personne se serait emparé du dossier.

Syndrome de Tchernobyl et aubaine

Au micro d'Europe1 lundi matin, François Baroin, le ministre du Budget, évoque une *"immense opération de maintenance ce week-end à Bercy"* , visant à nettoyer les postes de travail infectés. L'ANSSI reconnaît de son côté avoir "*coupé les connexions du ministère pour effectuer un assainissement entre samedi et dimanche après-midi*", mais réfute toute corrélation entre son nouveau rôle et l'incident si médiatisé. Pourtant, c'est le décret du 11 février qui lui a permis d'intervenir directement dans les bureaux de Bercy…

"On n'est pas le pays des Bisounours, il y a des attaques d'intelligence économique contre les entreprises et l'Etat", poursuit Baroin. C'est pourtant ce syndrome du nuage de Tchernobyl que déplore l'ANSSI par le biais d'un de ses porte-paroles:

> ***C'est la preuve que cela n'arrive pas qu'aux autres. 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.***

Avant de céder à la panique, il faut se rappeler qu'une attaque identifiée n'est déjà plus si dangereuse. Nettoyée, la menace qui pesait sur Bercy se transforme alors en astucieuse opération de communication.

MàJ [16h40]: **Dans la Tribune**, le député UMP du Tarn Bernard Carayon (qui milite pour la **création d'un confidentiel défense des affaires**) explique qu'il n'est aucunement surpris par le hacking de Bercy, affirmant qu'il avait déjà identifié les *"vulnérabilités"* du système français.

—

Crédits photo: ***tOad***, ***Alexandre Vialle***

MOUTBINAM
le 7 mars 2011 - 16:17 • SIGNALER UN ABUS - PERMALINK

Who is talking false flag operation here ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PIPOTRON
le 7 mars 2011 - 16:37 • SIGNALER UN ABUS - PERMALINK

Qu'il y ait de la récupération pour faire de la comm, pourquoi pas…

Cela étant, l'astucieuse opé de comm n'est pas là où on l'attend. S'il n'y avait eu l'opération de 'maintenance', cette affaire ne serait jamais sortie : Se faire hacker à cette échelle, c'est tout simplement la honte intégrale.

En revanche, ce qui sort de la comm gouvernementale, c'est que l'attaque a duré longtemps , qu'on ne sait pas si elle est finie, que au moins les hackers ont été 'avertis', et que 'vraisemblablement' ils visaient des infos relatives au G20 : en gros le brouillard total depuis des mois.

Et, étrangement, au milieu de toutes ces incertitudes, une -et une seule- certitude clamée haut et fort : "les dossiers personnels des français n'ont pas été touchés"

Mais si, on y croit très fort :-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

VINCENT
le 7 mars 2011 - 17:00 • SIGNALER UN ABUS - PERMALINK

J'ai adoré l'interview de votre journaliste Jean-Marc Manach (en espérant ne pas écorcher son nom) sur LCI. Clairement, certains savent de quoi ils parlent, et d'autres pas du tout. Merci pour l'éclairage différent.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PIPOTRON
le 7 mars 2011 - 17:50 • SIGNALER UN ABUS - PERMALINK

@Vincent

à propos de l'intervention de JMM, il semble opportun de rappeler la petite phrase récemment sortie par un fonctionnaire de Bercy à propos de l'affaire Renault :

"Entre le complot et la connerie, il faut toujours choisir la connerie"

bref, on a affaire à des incompétents qui essaient de sauver la face. Aucun spécialiste digne de ce nom ne se mouillera à affirmer que les données perso n'ont pas été compromises, sauf à vouloir ruiner sa réputation.

Il a été pris soin de laisser les énarques sortir les pipos…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GROSHA
le 7 mars 2011 - 19:26 • SIGNALER UN ABUS - PERMALINK

c'est rigolo de voir à quel point les bons élèves des grandes écoles du précédent millénaire sont méconnaissant de l'informatique…
Comme dans une quelconque dictature d'Afrique du nord…
gazdarem lou moral !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

FABRICE EPELBOIN
le 7 mars 2011 - 21:41 • SIGNALER UN ABUS - PERMALINK

@grosha

Détrompez vous, il existait des dictatures en Afrique du Nord avec à leur tête, des gens très au fait de l'internet et de son potentiel. Ben Ali est un geek, passionné d'électronique, d'informatique et d'internet.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

STANISLAS
le 7 mars 2011 - 21:59 • SIGNALER UN ABUS - PERMALINK

Votre article me fait sourire. Croire que les technocrates et les geeks de l'ANSSI aient un savoir-faire à ce point machiavélique dans le domaine de la communication, c'est très amusant.

Communiquer est un axe essentiel de la SSI, régulièrement évoqué par tous les documents stratégiques depuis 10 ans et régulièrement très marginalement mis en oeuvre. Or, dans les pays anglo-saxon, il est frappant de voir que de nombreuses affaires dans ce domaines ont été connues. Très peu en France.

Ce qui est à noter, et à saluer ici, c'est que l'ANSSI semble avoir reçu le droit de prendre en main une communication de crise. Il semble que l'on veuille en finir avec la loi du silence ou de la dénégation. C'est bien, parce que c'est nécessaire, pour aller plus loin que les questions de moyens et d'organisation de la SSI. Il faut toucher les utiliser pour changer les mentalités.

Le "i" du sigle "ANSSI" n'est pas "informatique" mais "information". Un système d'information a grosso modo 3 "piliers" : le support matériel (souvent informatique, bien sûr), le personnel (l'humain) et les procédures (organisation). Un SI exprime un métier ou une fonction d'un organisme. C'est cela qu'il faut faire passer. La protection de l'information, ce n'est pas que le problème du technicien informatique. Or, la SSI c'est comme la sécurité routière : on ne l'intègre vraiment que lorsque, d'une manière ou d'une autre, le problème nous touche personnellement.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 8 mars 2011 - 1:38 • SIGNALER UN ABUS - PERMALINK

@Stanislas: Vous avez raison. Si je pointe à ce point la communication, c'est précisément parce qu'elle est tombée dans l'escarcelle de l'ANSSI (vers qui renvoient le SGDSN comme le SGG). L'angle de mon papier se résume même à cette nouvelle donne: désormais, l'omerta c'est (presque) fini. Reste à détailler le contenu de l'attaque …

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

TOTOPIPO
le 8 mars 2011 - 9:06 • SIGNALER UN ABUS - PERMALINK

Marrant cette allusion à tchernobyl, ça colle à la peau je trouve : http://www.hns-info.net/article.php3?id_article=11053

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CORRECTOR
le 2 novembre 2012 - 22:26 • SIGNALER UN ABUS - PERMALINK

Non trouvé!

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI REPONDRE

DODOT
le 8 mars 2011 - 10:01 • SIGNALER UN ABUS - PERMALINK

Belle opération de com, ils vont pouvoir créer la loi DMCA version française ! Ah non c'est déjà fait.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JEAN JACQUES GANGHOFER
le 9 mars 2011 - 2:40 • SIGNALER UN ABUS - PERMALINK

Ils finiront bien par le faire, ce CSA du Net !!!!!

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PINTE JEAN-PAUL
le 9 mars 2011 - 7:57 • SIGNALER UN ABUS - PERMALINK

Bonjour

je m'apprêtais à évoquer ce syndrome de Tchernobyl.
Comme si en effet les attaques pouvaient s'arrêter au limites d'un territoire informationnel.

Ceci dénote bien le manque de culture informationnelle de notre état autour de la cybercriminalité en France.

Nous n'en sommes qu'au début et il y a du travail, croyez moi pour faire face aux nouveaux modes d'attaques qui attendent les états.

Pour vous en convaincre, regardez ce qui se passe déjà depuis un bon moment outre Atlantique

Voir ma réaction lors d'interview sur la Nouvelle République
http://www.lanouvellerepublique.fr/ACTUALITE/24-Heures/L-information-une-valeur-monnayable

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CORRECTOR
le 2 novembre 2012 - 22:34 • SIGNALER UN ABUS - PERMALINK

> Depuis le mois de décembre, 150 ordinateurs du ministère de l'Economie et des Finances auraient été "infiltrés par des hackers". Que cherchaient-ils? "Pour l'essentiel, des documents liés à la présidence française du G20 et aux affaires économiques internationales".

Ravi de voir que le G20 intéresse quelqu'un. Ou alors ces mecs sont maso. Ou alors, c'est Sarko qui a commandité cette attaque pour faire croire que la présidence du G20 est un enjeu stratégique.

> sa structure aura le pouvoir d'éteindre un pan du web

du Web ou de l'Internet?

Si vous ne faites pas bien la différence, vous devriez éviter de discuter de ces sujets un peu techniques : l'amateurisme n'a pas sa place. Demandez conseil à des spécialistes!

> Il pourra s'agir effectivement de leur demander de bloquer du trafic en provenance de machines utilisées pour mener des attaques

Bloquer une adresse IP se fait couramment en cas d'attaquer DOS. Cela n'a rien de nouveau ni de remarquable, c'est le B-A-BA de la réponse à une attaque en cours, et c'est typiquement le genre de situation où la "neutralité du net" ne s'applique pas (quand on protège un réseau).

> Il n'y a pas de nuage de Tchernobyl qui s'arrête aux frontières dans le domaine de la sécurité informatique.

Le “nuage de Tchernobyl qui s’arrête aux frontières” est une invention des journaleux, reprise en boucle par les propagandistes anti-nucléaires!…

8 pings

Internet l A qui profite le piratage de Bercy ? l Le blog le7.net le 7 mars 2011 - 23:09

[...] Auditionné à l’Assemblée, le 26 janvier, Bernard Bajolet, coordonnateur national du renseignement, expliquait de son côté qu’”après avoir renforcé l’agence nationale de sécurité des systèmes d’information, le gouvernement va créer un poste de directeur des systèmes d’information de l’État, chargé de sécuriser les réseaux des ministères“, et précisait qu’”il s’agit d’un dossier que le Président de la République suit de très près“ (voir Bercy, le piratage qui tombe à pic). [...]

La France attaquée par les CyberChinois : mais que fait la CyberPolice ? l ReadWriteWeb French edition le 8 mars 2011 - 16:00

[...] Cette coincidence heureuse de dates qu’évoque Manach est également soulevée par Olivier Tesquier dans Owni. [...]

Combattre le virus du langage : des antidotes de Burroughs à ceux du web 2.0 le 10 mars 2011 - 17:32

[...] qui saura déchiffrer le langage secret de l’autre. Enfin, le cryptage, c’est aussi une bataille de communication politique : annoncer qu’on sait déjouer une attaque informatique – que ce soit vrai ou [...]

La dérive de l’intelligence économique à la française « Les élucubrations d'Hugo le 20 mars 2011 - 14:19

[...] de 150 ordinateurs de la direction du Trésor, à Bercy, est plus le fruit d’une opération de communication de l’Etat que d’une quelconque investigation de Paris [...]

Les dessous du piratage de Bercy » Article » OWNI, Digital Journalism le 26 mars 2011 - 15:24

[...] Bercy, le piratage qui tombe à picLes Sanofi en grèveThe IT Crowd et le piratageCensure de l’Internet: la parodie qui dit toutLady Gaga Chatroulette versionTélécharger tueRien appris, rien comprisBercy: la piste de l’altermondialisme numériqueLivre numérique: on refait en France les mêmes erreurs qu’avec la musiqueEric Besson vs les concepts fondateurs du Net [...]

La France, internet, et la Revolution.. le 27 mars 2011 - 19:19

[...] http://owni.fr/2011/03/07/bercy-le-piratage-qui-tombe-a-pic/ [...]

Sans parler de la nullité crasse des responsables ultrapayés de ses systèmes informatiques qui devraient revenir au balai de maïs…A qui profite le piratage de Bercy ? « Aviseur international le 17 avril 2011 - 22:40

[...] Auditionné à l’Assemblée, le 26 janvier, Bernard Bajolet, coordonnateur national du renseignement, expliquait de son côté qu’”après avoir renforcé l’agence nationale de sécurité des systèmes d’information, le gouvernement va créer un poste de directeur des systèmes d’information de l’État, chargé de sécuriser les réseaux des ministères“, et précisait qu’”il s’agit d’un dossier que le Président de la République suit de très près“ (voir Bercy, le piratage qui tombe à pic). [...]

Bercy, le piratage qui tombe à pic « Cybercriminalité, cyberdéfense, cyberguerre,cybersécurité, cyberterrorisme, … le 3 novembre 2012 - 9:07

[...] En savoir plus ici Évaluez ceci :Share this:ShareLinkedInTwitterJ'aime ceci:J'aimeSoyez le premier à aimer ceci. [...]