DES MILLIERS D'EMAILS PIRATABLES SUR LES SITES .GOUV.FR

LE 14 MAI 2010 ***JEAN MARC MANACH***

On imagine mal la NSA, ou la CIA, proposer aux internautes de les contacter grâce à une adresse email de type @laposte.net ou @wanadoo.com. C'est pourtant ce que proposent la Direction du Renseignement Militaire (DRM)...

On imagine mal la NSA, ou la CIA, proposer aux internautes de les contacter grâce à une adresse email de type laposte.net ou wanadoo.com. C'est pourtant ce que proposent la Direction du renseignement militaire (**DRM**), qui utilise **deux adresses @yahoo.fr**, et la Direction de la Protection et de la Sécurité de la Défense (DPSD), qui utilise une adresse **@laposte.net** et une autre **@wanadoo.fr**. Je m'en étais étonné en 2005, dans un article consacré à **guerre de l'information** que se livrent les grandes puissances mondiales en terme d'intelligence économique, d'espionnage industriel, et de guerre électronique.

La DPSD et la DRM sont loin d'êtres les seules entités de l'armée dans ce cas. Citons, ainsi, l'**Ecole militaire**, le **Commandement Air des Systèmes de Surveillance, d'Information et de Communication**, le **service de santé des armées**, le **responsable de la communication de l'armée de terre** sur le quart sud-est de la France, la **direction des ressources humaines de l'armée de l'air** et la **direction du personnel militaire de l'armée de l'air**, un **administrateur civil** de la **Délégation aux affaires stratégiques**, placée sous l'autorité directe du ministre de la Défense et chargée du conseil géopolitique, stratégique et prospectif…

Les mails de Sarah Palin et de députés piratées

Non content de déléguer la gestion de leurs boîtes aux lettres électroniques à des sociétés privées dont certaines sont contrôlées par des entreprises américaines, ces militaires prennent aussi le risque, tout bête, de se voir pirater leurs adresses e-mails.

Car le problème, avec ces webmails, c'est qu'il suffit de cliquer sur le lien "*J'ai oublié mon mot de passe*" pour se voir proposer de répondre à une ou deux questions du type "*Où avez-vous rencontré votre conjoint ?*" pour réinitialiser le mot de passe, et donc prendre le contrôle de la boîte aux lettres. Ce qui est arrivé, l'an passé, à **Sarah Palin**, leader du parti républicain aux Etats-Unis. Sa question supposée secrète était "*où avez-vous rencontré votre mari?*" **La réponse était sur le web**. **Deux députés français** se sont également récemment fait ouvrir leurs boîte aux lettres virtuelles de cette manière.

L'**attaque contre Twitter**, menée par le désormais célèbre **Hacker Croll**, se fondait également sur une faille de sécurité des webmails. En l'espèce, un employé de Twitter utilisait Gmail, qui proposait d'envoyer le mot de passe oublié à une adresse e-mail secondaire. Cette dernière, hébergée chez Hotmail, était désactivée. Croll n'a eu qu'à la réactiver pour récupérer le mot de passe…

Une étude a montré que 20% des internautes pouvaient deviner les réponses aux questions de sécurité de leurs amis. Au Texas, **des chercheurs se sont aperçus** que 30% des noms de jeune fille des internautes pouvaient être obtenus en consultant des archives publiques.

Une équipe britannique **a établi** qu'un cracker avait à peu près 1 chance sur 80 de trouver la réponse aux questions de sécurité de type "*Quel est le nom de jeune fille de votre mère ?* " en se basant uniquement sur les noms les plus courants. En Corée par exemple, où la concentration des noms est la plus forte, vous avez **40% de chances** que le nom en question soit Kim, Park ou Lee.

Des centaines de milliers d'e-mails vulnérables

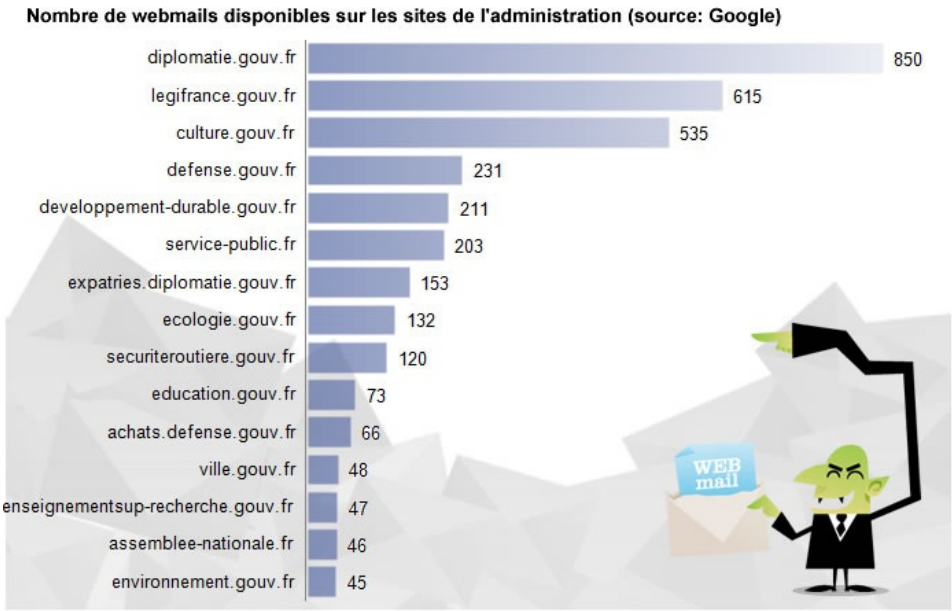
Pour mieux mesurer l'ampleur du problème, j'ai proposé à **Nicolas Kayser-Bril**,

“***datajournaliste***” à Owni.fr, de développer une petite application, que nous avons intitulé **mail.icio.us**, afin de voir combien d’adresses e-mails vulnérables sont disponibles sur les sites des principales administrations. Et force est de constater qu’elles sont légions.

On dénombre ainsi près de 55 000 mentions d’adresses utilisant des webmails piratables sur l’ensemble des sites en .gouv.fr, plus d’une dizaines de milliers d’associations et de contacts sur celui du Journal Officiel, des centaines de mairies sur service-public.fr, mais également, et c’est plus gênant, des centaines de contacts dans les ambassades et d’adresses d’expatriés sur le site du ministère des Affaires étrangères, de militaires ou prestataires sur celui de la défense nationale, des dizaines d’experts automobiles sur celui de la sécurité routière, de professionnels de l’éducation nationale, une trentaine de députés …

Aux États-Unis, on trouve ainsi plus de 750 000 mentions d’adresses utilisant des webmails sur l’ensemble des sites en .gov, dont plus de 25 000 sur les serveurs de l’armée américaine, un millier sur ceux de la NASA, la National Science Foundation ou la Chambre des représentants, et près de 100 sur le site du FBI…

La situation est encore plus critique dans les pays où les fonctionnaires n’ont pas d’autre choix que d’utiliser des webmails, par manque d’infrastructure locale. En Afrique, la plupart des ministres utilisent des boîtes mail hébergées par Yahoo. Et sur les 40 contacts de l’Agence Internationale à l’Energie Atomique en Afrique, par exemple, pas moins de **21 utilisent Yahoo**.



Ces données ont été récupérées à partir de listes des administrations aux **Etats-Unis**, en **France** et en **Allemagne**.

Nous avons ensuite utilisé l’**API de Google Search** pour obtenir une estimation du nombre de pages contenant une adresse webmail @hotmail.fr (et .com), @yahoo.fr (et .com), @laposte.net ou @voila.fr, les plus “*simples*” à pirater. Cette estimation n’est pas extrêmement fiable, ce qui explique les différences de résultats entre nos données et celles que vous pourrez trouver en faisant une recherche vous-même. Par ailleurs, le chiffre compte des pages, qui peuvent contenir plusieurs adresses e-mail (voir l’appli **mail.icio.us**).

Alors que le Pentagone **se prépare** sérieusement à la "*cyber-guerre*", **tout comme la gendarmerie française**, il est frappant de constater des failles béantes dans la sécurité des administrations nationales. Le gouvernement dépense des dizaines de millier d'euros pour assurer la sécurité de ses communications privées (**voir chez Thales**, par exemple). L'utilité de ces défenses est sérieusement diminuée si un assaillant peut avoir accès à de nombreuses boîtes e-mails au sein de l'administration.

Une fois à l'intérieur d'une boîte mail, un cracker peut facilement gagner la confiance des collègues ou des supérieurs en se faisant passer pour sa victime. Il est alors plus facile de leur envoyer des logiciels malveillants en pièces jointes. Une bonne partie de l'**opération Aurora**, lors de laquelle Google a été attaqué en Chine, s'appuyait sur ce type de stratégie (**voir cette présentation**).

Les solutions sont très faciles à implémenter. Il suffit d'utiliser des webmails plus sécurisée ou d'utiliser les solutions mises à disposition par l'administration (les adresses de type prenom.nom@ministere.gouv.fr). Rajoutez à ça un bon mot de passe et vos communications en ligne deviennent beaucoup, beaucoup plus sûres. Ca n'empêchera pas un assaillant déterminé d'avoir accès à vos données. Mais ça lui compliquera la tâche.

Contactées, la DRM et la DPSD n'ont pas voulu répondre à nos questions. A suivre, une interview d'Eric Filiol, directeur d'un laboratoire de virologie et de cryptologie qu'il avait créé du temps où il était lieutenant-colonel de l'armée française, et un manuel de contre-espionnage informatique, pour apprendre à se protéger.

—

Retrouvez les autres articles de **ce premier volet** de notre série sur le Contre-espionnage informatique : **Blinde ton mot de passe** et **Enquête : 70 centimes les 1000 captchas**.

Retrouvez également les **deuxième** et **troisième** volets de cette série sur le Contre-espionnage informatique.

NIAL
le 17 mai 2011 - 1:15 • SIGNALER UN ABUS - PERMALINK

Intéressant l'article… google

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

BARMINA
le 28 mai 2012 - 19:57 • SIGNALER UN ABUS - PERMALINK

Bonjour,
je m'appelle barmina julienne j'ai 28 ans je suis a londrès et j'aimerais correspondre avec toi. Voici mon courriel :
barminajulienne@hotmail.fr //barminajulienne@gmail.com//barmina_julienne@yahoo.fr
Merci pour la compréhension

Julienne Barmina

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

4 pings

Les tweets qui mentionnent 55 000 webmails piratables sur les sites .gouv.fr » Article » owni.fr, digital journalism -- Topsy.com le 14 mai 2010 - 16:15

[...] Ce billet était mentionné sur Twitter par jean marc manach, Nicolas Voisin, Aurélien Fache, Olivier Depiesse, Owni et des autres. Owni a dit: RT @nicolasvoisin: http://bit.ly/mail_icio_us 55 000 webmails piratables sur les sites .gouv.fr + l'appli #mailicious /-) [...]

KoopTech » Scoop » Verwaltung nutzt unsichere Webmail-Adressen le 14 mai 2010 - 18:19

[...] Sicherheit. Doch in der Praxis sieht das noch immer anders aus – wie übrigens auch ein Test in Frankreich gezeigt hat. Dort waren übrigens wesentlich mehr Beamte betroffen als in Deutschland! VN:F [...]

Tech #35 – Seesmic IO | Frenchspin.com (fr) le 25 mai 2010 - 16:39

[...] – Le site de Guillaume. Owni.fr – L'article dont s'inspire la Minute [...]

SCiencextrA » Blog Archive » Internet en France sous haute surveillance le 19 octobre 2011 - 0:44

[...] d'offres, une adresse email @wanadoo.com… comme OWNI l'avait déjà souligné lors de notre enquête sur les dizaines de milliers d'adresses e-mails "piratables"utilisées par des militaires et fonctionnaires français. En novembre 2008, Elexo, l'une des [...]