# OM | L'OM victime d'une fraude à grande échelle | MediafootMarseille

## L'OM victime d'une fraude à grande échelle

Après plusieurs grosses entreprises multinationales comme Michelin ou KPMG, c'est au tour des clubs de football d'être visés par une faste escroquerie.
De faux virement bancaires ont été réalisés vers la Chine durant les mois d'octobre et novembre derniers. Et, selon nos informations, plusieurs clubs de Ligue 1 ont été touchés. L'OM aurait subi un préjudice de **700 000 euros**, somme que n'a pas confirmé le club olympien, désireux de ne pas perturber l'enquête en cours. « Une partie des fonds a pu être recouvrée dans les heures qui ont suivi le préjudice », a pu nous confier un membre de la direction de l'OM.
La LFP essaye de prévenir ces actions frauduleuses en alertant l'ensemble des clubs sur ces problèmes de sécurité financière. Les plaintes répertoriées vont permettre à l'Office central pour la répression de la grande délinquance financière de poursuivre ses investigations.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.mediafootmarseille.fr/actualites/breves/12701-lom-victime-dune-fraude-grande-echelle

---

# Attention à vos comptes Gmail, cibles de pirates…

## Attention à vos comptes Gmail, cibles de pirates…

**Un nombre croissant de comptes piratés est actuellement signalé au Luxembourg. Cela commence toujours par un vol des données de connexion. Dans certains cas, cela passe par un faux message d'erreur qui nous informe que certains e-mails n'ont pas pu être transmis. L'utilisateur est alors prié de cliquer sur un lien qui mène à une prétendue adresse web de Google. C'est ici qu'il devra saisir ses données de connexion.**

Une fois qu'ils ont mis la main sur les données de connexion, les criminels convertissent le compte en arabe. Ensuite, une nouvelle adresse e-mail est créée sur Yahoo, très semblable à l'adresse originale (par exemple: pit.luxi@yahoo.com à la place de pit.luxi@gmail.com).
Tout le courrier entrant sur l'adresse gmail est ensuite redirigé vers la nouvelle adresse e-mail contrôlée par les criminels. L'adresse de réponse des e-mails sortants est également sur le compte Yahoo, de sorte que la victime ne se rend pas compte de ce qui se passe. En outre, les criminels copient la liste entière des contacts de la victime et les suppriment du compte Gmail, pour empêcher la victime de communiquer. Ils vident aussi toute la boîte de réception, ainsi que tous les contenus des différents dossiers.

**Une fraude perfide**
Pendant que la victime se débat avec le rétablissement de la langue d'origine, les escrocs peuvent tranquillement commencer à envoyer des e-mails de phishing ou des demandes d'argent à la liste de contacts des victimes. Si la victime insouciante réinitialise son compte dans les 7 jours, dans sa langue, il verra une notification lui indiquant que tous ses messages sont transférés à l'adresse xxx@yahoo.com. Passé ce délai de 7 jours, la notification disparaît.
Si votre compte Gmail se retrouve subitement dans une autre langue, c'est le signe indubitable qu'il a été piraté et que votre identité à été usurpée.

**Les bons réflexes**
La police, Bee Secure et CASES vous conseillent de réagir de la manière suivante:
• faites repasser votre compte dans la langue d'origine ;
• désactivez la redirection automatique de vos e-mails ;
• ensuite, modifiez votre mot de passe sans attendre. Un mot de passe solide doit comporter 10 caractères au minimum, avec des caractères spéciaux, des majuscules, des minuscules et des chiffres, de manière à ce qu'il ne figure dans aucun dictionnaire ;
• restaurez vos listes de contacts;
• récupérez vos e-mails disparus (suivez le tutoriel vidéo de la police);
• prévenez vos contacts que votre compte à été piraté et qu'ils ne doivent en aucun cas répondre aux e-mails provenant d'une autre adresse (Yahoo en l'occurrence). Dans la mesure du possible, cette adresse doit être signalée et bloquée par le fournisseur.

☞ La police a réalisé un tutoriel video qui vous guide pour les étapes 1 à 5:

**D'un point de vue préventif, les mesures suivantes sont toujours valables:**
activez la double authentification sur vos comptes e-mail;
ne saisissez jamais de données personnelles (login, mot de passe, numéro de carte de crédit..) sur une page web que vous avez ouverte en cliquant sur un lien dans un e-mail ;
suivez les bonnes pratiques e-mail (https://www.cases.lu/fr/e-mail-bonnes-pratiques.html).
suivez les conseils donnés dans l'article clever clicks for safer business (https://www.cases.lu/arnaques.html)
Si un ami ou une connaissance vous demande de lui envoyer de l'argent pour l'aider à se sortir d'une situation difficile, il s'agit très probablement d'une arnaque. En cas de doute, appelez votre ami pour prendre de ses nouvelles.
Si vous pensez que le compte e-mail d'un de vos contacts a été piraté, prévenez-le.
Cette vague de phishing vise pour l'instant les comptes Gmail, mais elle pourrait se produire avec tout autre fournisseur de messagerie. Ouvrez l'oeil!
Pour plus d'information, consultez la chaîne TV de la Police. Bee Secure y a participé à l'émission du 15 janvier sur la Cybercriminalité:

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://www.cases.lu/fr/comptes-gmail-pirates-copies-et-convertis-en-arabe.html

# Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

## Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

**L'éditeur Qualys a mis la main sur une vulnérabilité importante qui permettrait de prendre le contrôle à distance de la plupart des distributions Linux. Les appareils de type routeurs-modems ou NAS sont également concernés.**

Les chercheurs en sécurité de la société Qualys ont mis la main sur une faille critique (CVE-2015-0235) qui touche tous les systèmes Linux. Baptisée « Ghost », elle permettrait aux pirates de prendre le contrôle à distance « de tout un système, en se passant totalement des identifiants système », explique l'entreprise dans un communiqué. Un patch a été développé en concertation avec les éditeurs Linux. Il est en cours de diffusion et d'ores et déjà disponible sur certaines distributions, telles de Debian, Red Hat ou Ubuntu.
Cette terrible faille est logée dans une librairie GNU/Linux baptisée« glibc », qui est intégrée dans toutes les distributions Linux et qui permet de gérer les appels système de bas niveau, comme l'allocation d'espace mémoire, l'ouverture de fichiers, etc. Seules les versions antérieures à glibc 2.18 sont vulnérables. « Malheureusement, très de peu distributions Linux ont intégrés les versions récentes de glibc, pour des raisons de compatibilité. C'est pourquoi la plupart sont vulnérables », explique Wolfgang Kandek, directeur technique de Qualys.

**Quid des routeurs ou des NAS ?**
Comment fonctionne Ghost ? Cette vulnérabilité se caractérise par un dépassement de mémoire tampon (buffer overflow) dans les fonctions gesthostbyname et gethostbyaddr. Ces fonctions sont appelées par les applications Linux quand elles doivent gérer des connexions Internet, comme par exemple les serveurs de messagerie. C'est d'ailleurs la cible sur laquelle se sont penchés les chercheurs de Qualys pour développer un exemple de code d'exploitation : ils ont conçu une attaque dans laquelle il suffit d'envoyer un email vers le serveur pour accéder à l'interface ligne de commande (shell). C'est aussi simple que ça !
Qualys recommande aux administrateurs de mettre à jour leurs systèmes Linux aussi rapidement que possible. Mais une question reste en suspens : quid des nombreux objets connectés que nous possédons tous à la maison, tels que les routeurs-modems ou les disques durs en réseau (NAS) ? « Ils intègrent tous la librairie glibc. Mais pour créer une attaque, il faut également que ces appareils utilisent les fonctions vulnérables. Il faut ensuite trouver le bon vecteur d'attaque. Ce n'est pas évident à priori », souligne Wolfgang Kandek. En somme : pas la peine de paniquer tout de suite. Les pirates vont certainement se pencher sur la question, mais ils vont mettre du temps à développer leurs attaques. Pour réduire le risque, il est conseillé de mettre à jour les firmwares des appareils dès qu'ils seront disponibles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/643126/ghost-la-faille-critique-qui-permet-de-prendre-le-controle-des-systemes-linux/
Par Gilbert Kallenborn

# Le site de l’Afnic visé par une attaque informatique DDoS

## Le site de l’Afnic visé par une attaque informatique DDoS

**Le site de l’Afnic était indisponible plusieurs heures dans la journée d’hier. Une maintenance préventive, alors que l’association chargée de la gestion du .fr subissait une attaque Ddos un peu plus sérieuse que d’habitude.**

Le Ddos est la nouvelle tendance de ce début d’année 2015. Enfin, le défacage de sites fait également un retour en force mais depuis le début de l’année, les attaques de déni de service se succèdent et se ressemblent un peu. L’Afnic n’y a pas échappé : hier à la mi-journée, le site web de l’association Française pour le nommage Internet en coopération était inaccessible.
Une maintenance provoquée par une attaque Ddos comme l’explique l’Afnic sur son site : plusieurs services ont été interrompus brièvement, il était par exemple devenu impossible d’enregistrer des noms de domaines en .fr sur le site de l’Afnic dans le courant de l’après midi et les services tels que le whois étaient inaccessibles. La résolution DNS en revanche n’a pas été affectée, ce qui limite fortement la visibilité de l’attaque au grand public. Les perturbations sur les autres services du site se sont poursuivies tout au long de la journée avant un retour à la normale dans la soirée.
Interrogé par nos confrères de Next Inpact, Pierre Bonis directeur adjoint de l’Afnic est revenu sur l’attaque « Nous avons régulièrement des attaques DdoS, mais celle-ci nous est parue plus importante. Elle a fait tomber un de nos pares-feu » explique-t-il dans leurs colonnes. Face à l’ampleur de l’attaque, le directeur adjoint explique que l’Afnic a préféré mettre son site web en maintenance afin de protéger le reste des services.
L’attaque n’a pour l’instant pas été revendiquée et les investigations et analyses sont encore en cours, l’Afnic ayant fait part de son souhait de porter plainte suite à cette attaque. Dans le contexte actuel, on serait tenté de faire le lien entre cette attaque et la récente vague d’attaques subie par les sites web français à la suite des attaques terroristes de début janvier mais pour l’instant aucun élément concret ne vient étayer cette hypothèse.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/ddos-le-site-de-l-afnic-vise-par-une-attaque-39813445.htm
Par Louis Adam

# Faut-il craindre une cyberguerre ?


Faut-il craindre une cyberguerre ?

**Leurs PC sont leurs armes et leur guerre se mène en ligne. Après les attentats à Paris, des cyberattaques ont été menées contre des sites internet français, par des hackers affirmant agir au nom du groupe Etat islamique (EI). Dans le même temps, des « hacktivistes » se revendiquant d'Anonymous ont piraté des sites et comptes sur les réseaux sociaux des organisations islamistes et de leurs membres.**

Mais c'est loin d'être terminé. Des comptes YouTube et Twitter appartenant au commandement militaire américain au Moyen-Orient (Centcom) ont également été visés, et une attaque d'envergure est annoncée pour jeudi 15 janvier. Sommes-nous à l'aube d'une cyberguerre ? Non, toujours pas, répond Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).

**Francetv info :** Peut-on parler de cyberguerre lorsque l'on évoque les attaques informatiques menées par des hackers qui se revendiquent du jihad ?
**Gérôme Billois :** Non, on n'y est pas du tout. Ce serait exagéré de parler de « guerre ». Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruption de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel.

**Alors comment pourrait-on appeler cela ?**
Il n'existe pas vraiment de mot pour déterminer ces actes. Après l'attaque contre la société Sony Pictures, qui a subi une destruction massive de son système d'information et le vol d'une importante quantité de données, Barack Obama parlé de cybervandalisme. Le terme semble assez juste. Ce qui se passe aujourd'hui, c'est comme si des activistes entraient dans des centaines de boutiques pour y coller leurs affiches et repartir. Les propriétaires de ces magasins n'avaient pas bien fermé la porte en partant et en revenant le lendemain matin, ils trouvent des affiches qui font la publicité de l'Etat islamique.

**Pour vous, ces actions restent plutôt d'ordre symbolique ?**
Extrêmement symbolique, puisqu'il s'agit d'une lutte entre deux idéologies. Avec d'un côté l'#opFrance (pour « Opération France », lancée par des cyberjihadistes), annoncée pour le 15 janvier, qui vise à tenir l'image de la France en attaquant un grand nombre de structures dans l'Hexagone, et de l'autre l'#opCharlieHebdo, qui vise à dénoncer et rendre indisponibles des sites jihadistes.

**Qui se trouve derrière cette contre-attaque ? Certains revendiquent leur appartenance aux Anonymous…**
On ne peut pas dire qu'il s'agit « des » Anonymous. Ce sont, en fait, des groupes très divers. Il faut d'ailleurs savoir que certains des groupes qui attaquent la France aujourd'hui ont pu participer à des opérations des Anonymous, ou s'en revendiquer. Il y a des acteurs en commun, qui œuvraient auparavant dans une même direction et se divisent aujourd'hui sur ce cas particulier. La logique de « l'hacktivisme » au sens large c'est : « Il se passe un événement, je me positionne par rapport à celui-ci et à chaque nouvel événement je redéfinis ma doctrine ».

**Quelle est la force de frappe des cyberjihadistes aujourd'hui ?**
Aujourd'hui, ils mènent des attaques de faible intensité. Sur une échelle de 1 à 10, ils atteignent 5, au maximum. Ces piratas utilisent des vulnérabilités connues depuis longtemps ainsi que des outils disponibles facilement sur internet. De plus, ils s'attaquent à des sites peu sécurisés et pas mis à jour. Il existe tout de même un risque à moyen terme. Ces groupes de pirates, petit à petit, vont apprendre, se développer, et augmenter ainsi leurs capacités d'attaque pour viser des services plus importants. On sait que l'EI dispose d'importants moyens financiers. Il n'aura, de toutes façons, pas de problème de matériel : avec un simple PC, vous pouvez lancer des attaques.

**Qu'est-ce qui pourrait rendre ces groupes plus dangereux ?**
Pour eux, il s'agit d'abord de gagner en expérience. Mais ils peuvent aussi acheter ce qu'on appelle des « vulnérabilités zero day », c'est-à-dire des connaissances sur une vulnérabilité qui n'est pas encore connue des éditeurs de sécurité. Quand vous possédez cet atout, vous pouvez attaquer un système, même s'il est mis à jour. Pour poursuivre l'analogie des boutiques vandalisées : imaginons que quelqu'un, comme un chercheur, découvre que pour la marque de serrure XYZ il existe un pass universel. Avec cette information, il peut faire deux choses : soit prévenir le fabricant de la serrure pour qu'il corrige son produit, soit vendre cette vulnérabilité à des criminels sur le marché noir.

**Les pirates ont donc toujours un temps d'avance sur les systèmes de sécurité…**
Oui et non. Une partie des pirates, les plus pointus, certains groupes de cybercriminels, peuvent aller jusqu'à dédier une partie de leurs moyens à faire de la recherche en attaques et trouver ces « vulnérabilités zero day ». Ces groupes-là, oui, peuvent avoir cette capacité. Il peut s'agir soit d'Etats un peu belliqueux, soit de cybercriminels pointus. Mais il n'y en a pas des milliers. Dans le cas qui nous intéresse, les pirates n'ont pas cette avance. Ils utilisent simplement des failles connues, dont certaines ont été rendues publiques depuis 2012. Or, nous sommes en 2015 et les systèmes qu'ils attaquent n'ont pas été corrigés. On parle de petites mairies, d'universités, de PME… Ces structures-là n'ont pas forcément l'expertise ni les moyens pour maintenir leurs systèmes à jour.

**D'autres structures, susceptibles de devenir des cibles plus importantes comme les grandes banques françaises par exemple, sont-elles mieux protégées ?**
Oui, les systèmes sensibles sont mieux protégés. Les grandes sociétés ont les capacités nécessaires pour investir dans la sécurité. Les banques en ligne, par exemple, réalisent quotidiennement, voire plus encore, des tests de vulnérabilité automatisés, qui mènent les mêmes actions que les pirates. Les résultats de ces tests remontent aux services de sécurité informatique qui peuvent très rapidement effectuer les mises à jour nécessaires. Ce qui n'empêche qu'un site d'une grande banque est tombé, pendant une des attaques. Mais il s'agissait d'un site satellite sur lequel il n'y avait aucune transaction financière.

**Là, nous parlons de sites internet. Qu'en est-il des systèmes informatiques internes ?**
Ces systèmes-là disposent d'un niveau de sécurité, a priori, plus fort. Ne peuvent y rentrer que des employés ou des collaborateurs connus. Soit parce qu'il existe une protection physique : il faut entrer dans le bâtiment de la société. Soit parce qu'il y a des mots de passe ou des cartes à puce pour accéder à distance aux données. On n'est pas pour autant à l'abri d'une attaque visant le système d'information interne. C'est ce qui est arrivé chez Sony. Le FBI l'a dit : 90% des sociétés américaines seraient tombées si elles avaient été confrontées à la même méthode de piratage. C'est énorme.

**Donc la menace existe…**
Oui. La vraie question est de savoir si les jihadistes passeraient à ce type d'actions. Leur logique, pour l'instant, est plutôt de faire du bruit, de multiplier les cibles, de casser des milliers de sites, pour pouvoir dire mille fois qu'ils l'ont fait. Une attaque plus poussée, qui ferait plus de mal, aurait peut-être moins de résonance médiatique.

**C'est tout de même une menace prise au sérieux, sur laquelle l'Otan se penche sérieusement. Est-ce à cause des menaces de ces jihadistes ?**
Pas seulement. On distingue trois grandes « familles d'attaquants » : les « hacktivistes », qui attaquent par idéologie comme les cyberjihadistes, les cybercriminels, qui volent des données pour les monnayer, et enfin les Etats, qui développent des capacités défensives et offensives. Mais on peut craindre des regroupements entre ces groupes. Dans l'exemple de Sony, l'attaque est attribuée à la Corée du Nord, mais on sait qu'elle aurait été appuyée par des groupes d' »hacktivistes ».

**Comment les Etats se préparent-ils face à cette menace ?**
La cyberdéfense ne se résume pas à créer des murs en attendant que des pirates tentent de les casser. Cela inclut aussi des techniques de contre-attaque, pour pouvoir neutraliser les attaquants. Tous les Etats s'y préparent. Pour ce qui est de mener des attaques, on peut estimer que tous les pays industrialisés ont déjà des moyens et les renforcent au quotidien.

**Concrètement, en quoi consiste la contre-attaque face à des cyberjihadistes ?**
Les moyens de contre-attaque sont quasiment les mêmes que les moyens d'attaque. On peut imaginer attaquer leurs systèmes, les rendre inopérants, capturer les données pour bien comprendre qui ils sont. On peut aussi « boucher leurs tuyaux » pour éviter que les attaques ne passent.
Mais la difficulté, dans ce domaine, est de bien savoir qui se trouve en face de nous. Dans le cas Sony, on lit que l'attaque serait partie d'un hôtel en Thaïlande. A mon avis, elle est passée par là, mais ce n'est pas son point de départ. J'ai déjà vu des attaques menées contre certains de mes clients provenir de serveurs d'écoles maternelles au Vietnam. On se doute bien que ce n'est pas un écolier vietnamien qui l'a lancée, qu'il s'agit simplement de brouiller les pistes. Dans des scénarios plus vicieux, il peut s'agir de faire croire que l'attaque vient d'un endroit en particulier, pour provoquer une contre-attaque sur cette cible. Si l'on n'attribue pas l'attaque au bon responsable, on risque d'infliger des sanctions à un leurre.

**Quand vous parlez de « boucher les tuyaux », s'agit-il d'attaques par déni de service, méthode qu'utilisent justement certains hackers ?**
Cette méthode-là n'est efficace que temporairement, pour freiner une attaque. Mais les Etats ont la possibilité, à distance, de faire tomber les réseaux, de les couper, plutôt que de les boucher. Je parle bien des Etats, car les entreprises privées n'ont pas le droit de contre-attaquer. La légitime défense n'existe pas dans le cyberespace. En France, le seul cadre légal aujourd'hui, c'est la loi de programmation militaire, qui donne cette capacité à l'Agence nationale de sécurité des systèmes d'information (Anssi) ou, en tout cas, aux services rattachés au Premier ministre.

**Manuel Valls va annoncer une série de mesures, dont certaines concernent internet. Où placer le curseur, entre la neutralité de net, la surveillance pour empêcher les cyberjihadistes de nuire et la protection de la vie privée ?**
C'est une question idéologique fondamentale, mais on n'y trouvera pas de réponse parfaite. Ce qui est certain, c'est qu'il y a une menace, qui, il faut le préciser, représente une très faible portion des usages d'internet. L'énorme majorité des usages sont très bénéfiques, pour l'économie, la culture, notre quotidien. Le plus important, selon moi, c'est le contrôle des moyens qu'on se donne. Il faut, certes, pouvoir être très réactif, car les attaques peuvent être menées très vite, mais il faut se contrôler pour éviter de tomber dans la surveillance généralisée. Ce contrôle peut être exercé par la justice ou des autorités indépendantes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyberguerre_796909.html

---

# Après les attentats de Paris – Mesures contre le piratage informatique


Après les attentats de Paris – Mesures contre le piratage informatique

**Un groupe se réclamant de l'Etat islamique (EI) a piraté, lundi, le compte Twitter du commandement de l'armée américaine au Moyen-Orient et en Asie centrale (US Central Command, CentCom).**
**Le #ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre les attaques informatiques.**

Le ministère français de la Défense a annoncé avoir renforcé ses systèmes de protection contre le piratage informatique quelques jours après les attentats jihadistes de Paris et à la suite d'une dizaine d'attaques dont ses sites internet ont été la cible. Deux de ces attaques « concernaient deux régiments de l'armée de Terre, dont une école », a ainsi déclaré à la presse le vice-amiral Arnaud Coustillière, responsable du pôle cyber-défense à l'état-major des Armées.
Au lendemain de la manifestation monstre, dimanche à Paris, en hommage aux 17 personnes tuées dans les attentats de la semaine dernière, « il a été décidé de monter le niveau de vigilance sur internet » et, « depuis mardi, je dispose d'une cellule de crise pour surveiller » les pirates informatiques, a ajouté le vice-amiral Coustillière. « Nous considérons que c'est une crise comme une autre, nous prenons des mesures de précaution et de vigilance (…) mais on ne peut pas parler de cyber-guerre », a-t-il ajouté, rappelant que le ministère de la Défense a environ 350 sites internet.


**LE MINISTÈRE DE LA DÉFENSE VISÉ LE 6 JANVIER**
« Les attaques contre le site de la Dicod (service de communication du ministère) continuent, il y a régulièrement des gens qui viennent tester le site de la Dicod », a précisé l'officier. « Pour moi, ces attaques sont la réponse à la manifestation de dimanche dernier, par des gens qui n'adhèrent pas à un certain nombre de valeurs », a-t-il dit.
Le site internet du ministère de la Défense avait déjà été cible le 6 janvier d'une attaque informatique revendiquée par le groupe Anonymous qui affirmait vouloir « venger » le militant écologiste Rémi Fraisse tué en octobre pendant la répression d'une manifestation.
Ces données sont à rapporter au fait que, selon les sources ouvertes et disponibles, mais qui n'émanent pas du ministère de la Défense, il y a eu depuis le 10 janvier de l'ordre de 20.000 attaques en France, par des « groupes plus ou moins structurés ou des hackers islamistes bien connus », contre les sites internet les plus variés, d'écoles, d'institutions, de pizzerias, etc., a ajouté le responsable. Ces attaques se font soit par saturation des sites, soit par pénétration ou « défacement », une opération qui consiste à remplacer la page d'accueil par une autre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.parismatch.com/Vivre/High-Tech/Mesures-contre-le-piratage-informatique-691194

# L’hôpital cible d’une attaque informatique

## L’hôpital cible d’une attaque informatique – 16/01/2015

**Châteauroux. Des pirates informatiques s’en sont pris, mercredi soir, au réseau informatique du centre hospitalier. A priori, sans conséquences graves.**

**» Ce Web dont les djihadistes se servent est aussi un allié »**

L’attaque s’est produite mercredi soir. « Nous avons constaté un ralentissement des ordinateurs », raconte Xavier Bailly, directeur adjoint de l’hôpital de Châteauroux. Selon lui, le virus aurait infecté les ordinateurs du centre hospitalier « connectés à Internet ». D’après nos informations, il s’agirait de Trojan Kryptik, cheval de Troie qui aurait la capacité de dérober des données stockées.

« Nos équipes informatiques ont fait le nécessaire auprès des endroits sensibles de l’établissement pour sécuriser certains postes de travail. » Selon lui, le fonctionnement normal des différents services n’aurait pas été impacté. Pourtant, d’après nos informations, le Samu est resté, mercredi, injoignable pendant une quinzaine de minutes.

**Cyberdjihadistes contre Anonymous**

Hier, le site Internet du centre hospitalier, www.ch-chateauroux.fr, était « temporairement indisponible ». « Les autorités nous ont indiqué qu’une action de malveillance d’envergure aurait peut-être lieu aujourd’hui (lire hier), révèle Xavier Bailly. C’est pourquoi nous avons coupé Internet. »

Hier, l’état-major de l’armée française a annoncé que plus de 19.000 sites Internet français avaient été la cible, ces derniers jours, de cyber attaques similaires. D’après une source proche de l’enquête, celle dont a été victime l’hôpital de Châteauroux a été pilotée depuis l’étranger, sans qu’on puisse encore en définir la provenance exacte.

Cette attaque informatique d’ampleur nationale serait une réponse aux Anonymous, groupe d’hackers activistes qui traquent, depuis l’attentat à Charlie Hebdo, les « cyberjihadistes » sur Internet et les réseaux sociaux. D’après le site Internet Zataz.com, spécialisé dans l’actualité informatique, certaines opérations ont été baptisées : Opération anti France, Opération anti Charlie, Opération Je ne suis pas Charlie, etc.

Ce n’est pas la première fois que l’hôpital de Châteauroux est la cible de pirates informatiques. « Nous avons déploré d’autres actes, il y a huit ou neuf mois », reconnaît Xavier Bailly. La vie des services n’en avait pas été bouleversée.

**réactions**

» Pas d’autres sites ciblés « , selon la préfecture de l’Indre

**Préfecture de l’Indre** : « A notre connaissance, il n’y a pas eu d’autres sites ciblés mais il n’est pas exclu qu’il y en ait eu. Il n’y a pas de conséquences importantes pour l’instant. Nous recommandons de mettre régulièrement à jour les systèmes antivirus. »

> Philippe Guibon, directeur de la clinique Saint-François : « Nous avons eu un problème serveur, mercredi, mais c’était en interne, cela n’a rien à voir avec une cyber attaque. En revanche, nous avons appris que, dans d’autres régions, des établissements avaient été alertés, dès lundi, d’un risque potentiel d’une attaque, le 15 janvier, pour les sites Internet français. Nous sommes étonnés et un peu inquiets de ne pas avoir été mis au courant. »

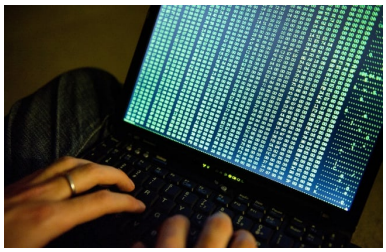
> Alexis Rousseau-Jouhennet, chargé de communication de la ville de Châteauroux : « Nous avons, tous les jours, des tentatives d’intrusion. Lundi, l’adresse mail d’un agent communal a été piratée mais cela n’a rien à voir avec les réseaux islamistes. Nous avons une veille informatique permanente. Nous sommes vigilants. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.lanouvellerepublique.fr/Indre/Actualite/Faits-divers-justice/n/Contenus/Articles/2015/01/16/L-hopital-cible-d-une-attaque-informatique-2187330

# Sites d’info bloqués: La thèse de la cyberattaque

# écartée



## Sites d’info bloqués: La thèse de la cyberattaque écartée

**Ce n’est sans doute pas la grosse attaque promise par les hackers islamistes qui s’en prennent depuis une semaine au Web français, mais le timing interroge. De nombreux sites d’information, dont 20minutes.fr, ont été bloqués une heure et demie ce vendredi matin en raison d’un incident technique chez leur hébergeur Oxalide d’une ampleur a priori inédite.**

**France Inter, Le Parisien, Slate… et Sushi Shop**
Les sites de 20 Minutes, L’Express, Mediapart, France Info, France Inter, Le Parisien, Slate, ZDNet ou encore Marianne, tous hébergés par Oxalide, sont devenus inaccessibles vers 10h. Des sites d’e-commerce, comme Sushi Shop, ont eux aussi été perturbés. Vers 11h30 certains sont redevenus accessibles. «Le niveau actuel d’information ne permet ni d’affirmer que la responsabilité d’Oxalide soit engagée, ni qu’il s’agisse d’un acte malveillant lié à l’actualité», affirmait l’hébergeur un peu avant 13h. Un peu plus tard, il tweetait: «Les premiers éléments en notre possession nous permettent d’écarter l’hypothèse d’une attaque externe de type DDoS.»
Même s’il semble dès lors écarté, le scénario d’une cyberattaque était considéré comme plausible en fin de matinée par les experts en sécurité informatique. «Toutes les caractéristiques techniques d’une attaque par déni de service (DDoS, lorsqu’un site est noyé sous les requêtes de connexion)» étaient réunies, selon Thierry Karsenti, directeur technique Europe de l’entreprise de sécurité informatique Checkpoint. «Il s’agit probablement d’une attaque DDoS», estimait auprès de 20 Minutes Olivier Hassid, directeur général du Club des directeurs de sécurité des entreprises. «Vu les cibles, on peut penser à une attaque virtuelle venant d’islamistes», renchérissait Eric Filiol, expert à l’École supérieure d’informatique, électronique, automatique.

**Mercenaires en ligne**
Pour Gérôme Billois, expert du cabinet Solucom, «si une attaque par déni de service menée dans le but de nuire à la liberté d’expression était confirmée, on ne serait plus sur du menu fretin.» Car jusqu’ici, les très nombreuses cibles touchées par les hackers tendance islamistes souffraient de failles faciles à identifier souvent causées par un simple défaut de mise à jour logicielle. S’en prendre à l’hébergeur de nombreux sites de presse dénoterait une montée en puissance, peut-être rendue possible grâce à l’achat des services de cybercriminels dotés de véritables moyens.
Car comme le rappellent Gérôme Billois et Eric Filiol, la cybercriminalité est un business en pleine expansion et les hackers s’achètent comme des mercenaires. «Il existe une grille tarifaire», explique Gérôme Billois. «Pour 200 dollars, des sites hébergés en Europe centrale proposent de louer à l’heure 1.000 machines infestées permettant de lancer une attaque DDoS», illustre Eric Filiol. Qu’elle ait lieu aujourd’hui ou plus tard, une attaque contre la presse française serait peut-être moins la preuve d’une montée en puissance des «cyberdjihadistes» que de leur volonté de mettre la main au portefeuille.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.20minutes.fr/high-tech/1518695-20150116-sites-info-bloques-incident-technique-attaque-informatique
Par Nicolas Bégasse et Romain Lescurieux

# Attentats : les attaques contre les sites Web français s’intensifient

| | |
|---|---|
|  | Attentats : les attaques contre les sites Web français s’intensifient |

**Si les attaques sont pour le moment limités à du 'défaçage', les experts en sécurité craignent que les hacktivistes islamistes changent de braquet ce jeudi. Mais pour le moment, les attaques sont nombreuses mais limitées.**

L'escalade des attaques a bien eu lieu. Premiers à réagir, les Anonymous qui ont promis de venger les victimes de Charlie Hebdo avec l'opération #OpCharlieHebdo. Cette offensive des hactivistes a évidemment provoqué une réaction de hackers de l'autre bord, soutenant les islamistes radicaux.
Et ces derniers ont massivement attaqué de nombreux sites Web français de tout ordre (églises, municipalités, universités, hôpitaux…). « Plus d'un millier de sites ont été touchés au total, plus ou moins fortement. Ces sites sont majoritairement de petite taille », explique à l'AFP François Paget, expert chez McAfee. D'autres sources avancent un chiffre de 19.000 sites touchés.

**Plus de 1000 sites français cybervandalisés**
La plupart du temps, il s'agit de campagnes de «defacement», soit une modification de la page d'accueil des sites visés avec la publication de messages à caractère idéologique. «Il n'y a de Dieu qu'Allah», «Death to France» (Mort à la France) ou encore «Death to Charlie»… Il ne s'agit donc pas d'une cyberguerre (comme certains voudraient le faire croire) mais plutôt de cybervadalisme.
Ces attaques ne sont d'ailleurs pas bien compliquées à mener : « des CMS, des applications Drupal, Joomla, WordPress tout simplement non mis à jour. Des mots de passe un peu trop légers… », commente le spécialiste Zataz.
Mais ces attaques pourraient prendre une nouvelle dimension ce jeudi. « Les revendications initiales parlaient d'un point d'orgue le 15 janvier », indique Gérôme Billois, expert du Cercle européen de la sécurité informatique et consultant pour le cabinet Solucom.
« Ce ne sont bien sûr que des suppositions, mais on pourrait par exemple assister jeudi à l'attaque de sites plus visibles, à des attaques plus groupées, ou à un changement de technique », estime le spécialiste.
A titre préventif, l'Agence nationale de la Sécurité des Systèmes d'information (ANSSI) a envoyé un petit manuel pédagogique dans les ministères, afin de faire le point sur les mesures de sécurité à prendre en urgence tandis que le volet numérique du plan vigipirate aborde les questions de sécurité informatique pour les opérateurs d'importance vitale.
AnonGhost a ainsi revendiqué ce jeudi la publication de coordonnées personnelles d'une dizaine d'employés des ministères des Finances et de l'Intérieur et affirment posséder une base de plus de 10.000 noms. Le collectif MECA (Middle-East Cyber Army revendiquait de son côté trois attaques contre le syndicat Sud Michelin, et l'institut de mathématiques de Toulouse….
Bref, on est encore très loin de la cyberguerre mais « C'est la première fois qu'un pays est confronté à une vague aussi importante de cybercontestation », observe ainsi le vice-amiral Arnaud Coustillière, officier-général de la cyberdéfense.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/attentats-les-attaques-contre-les-sites-web-francais-s-intensifient-39812939.htm

---

# Alerte au phishing sur LinkedIn


# Alerte au phishing sur LinkedIn

**L'éditeur de sécurité Symantec a lancé une alerte à propos de mails de phishing ciblant les utilisateurs du réseau social LinkedIn. Ce mail frauduleux contient une pièce jointe à ne surtout pas ouvrir.**

Satnam Narang, manager sécurité chez Symantec, a lancé une alerte sur la multiplication de mails de phishing visant les utilisateurs de LinkedIn. Dans un billet, ce dernier explique avoir observé un accroissement de mails prétendument envoyés par le service support du réseau social professionnel. En fait, il n'en est rien : il s'agit bien de mails frauduleux tentant de tromper les utilisateurs qui pourraient être tentés de suivre les recommandations indiquées dans ce message.


*« En raison d'activités irrégulières, votre compte LinkedIn a fait l'objet d'une mise à jour de sécurité obligatoire. Parfois, LinkedIn rejette les identifiants dans les cas où nous pensons que le compte pourrait avoir été compromis. Pour ce faire, nous avons développé une nouvelle façon de garder votre compte sûr et attaché à ce mail un formulaire pour achever ce processus. Merci de le télécharger et de suivre les instructions sur votre écran »* peut-on lire dans le mail de phishing.

Celui-ci est écrit de façon tout à fait correcte et peut donc piéger d'autant plus facilement l'utilisateur.
En cliquant sur le formulaire, une copie du véritable site, dont la source a été modifiée, s'affiche invitant l'utilisateur à se connecter avec ses identifiants. *« La méthode utilisée permet de contourner les listes noires du navigateur qui souvent détectent les sites web suspicieux pour prévenir les utilisateurs qu'ils sont victimes de phishing […] Les utilisateurs devraient envisager d'activer l'authentification à double facteur qui est la véritable mise à jour de sécurité […] »*, a prévenu Satnam Narang

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-au-phishing-sur-linkedin-59912.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Par Dominique Filippone