Thales aurait été la cible d’une cyberattaque | Le Net Expert Informatique

Thales aurait été la cible d’une cyberattaque

Le groupe aurait été victime d’une intrusion dans son système d’informations. Ce mercredi, Thales confirme l’attaque mais indique avoir renforcé sa sécurité depuis.

Selon des informations du Canard Enchainé, le groupe français Thales a été victime d’une attaque informatique. L’offensive a duré plusieurs jours avant de s’interrompre vers la mi-février. Plusieurs pirates seraient parvenus à s’introduire dans des systèmes d’informations du groupe basés aux Etats-Unis, au Canada, en Australie, en Grande-Bretagne puis en France.
Pour l’hebdomadaire, Thales a bien confirmé l’attaque dont le but était de prendre le contrôle de l’ensemble du système d’informations du groupe. L’idée était également de se maintenir dans ce dernier pour récupérer des informations de la société ou d’infecter des postes.
Depuis cette attaque, que Thalès ne commente pas davantage quant à ses motifs ou ses moyens, le groupe précise avoir renforcé ses mesures de sécurité. Une note aurait également circulé auprès de certains collaborateurs du groupe en vue de revoir les process internes de sécurité.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d’entreprise.
Contactez-nous

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

S o u r c e ;
http://www.clubic.com/reseau-informatique/securite-reseaux/actualite-763182-thales.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_16/04/2015&partner=-&svc_position=939819221&svc_misc=-&crmID=639453874_939819221&estat_url=http%3A%2F%2Fwww.clubic.com%2Freseau-informatique%2Fsecurite-reseaux%2Factualite-763182-thales.html

---

Arte victime d’une attaque informatique jeudi | Le Net Expert Informatique

Arte victime d’une attaque informatique jeudi

Le lendemain de l'attaque informatique qui a frappé TV5 Monde mercredi, Arte à Strasbourg a également subi une intrusion dans son réseau. Fort heureusement, il ne s'agissait pas d'une attaque menée par des cyber-djihadistes autoproclamés, mais d'un cas classique de « ransom ware », autrement dit de racket par l'intermédiaire d'un virus.

Rançon contre les fichiers

Téléchargé jeudi en milieu d'après-midi via la messagerie, un virus du type « crypto-wall » ou « cryptolocker » s'est installé sur trois ordinateurs d'Arte Culture avant de rapidement se propager. Un salarié témoigne :

« On a vu nos fichiers et nos dossiers devenir inaccessibles, ils avaient tous une taille de 0 octet. On a appelé le service informatique qui a identifié la menace et a mis en quarantaine tout le service culture et éteint nos ordinateurs. Quelques heures après, on a pu reprendre le travail à partir de sauvegardes. »

Une trentaine de postes ont été isolés pendant le reste de la journée. Les fichiers infectés sont rendus illisibles par le virus, qui les crypte les uns après les autres. Il n'y a aucun moyen de les récupérer, sauf à accepter de payer une rançon, généralement via la monnaie Bitcoin qui a l'avantage d'être difficile à tracer. Arte disposait de sauvegardes pour ses fichiers, mais tout de même 500 Go de données ont été corrompues.

Le service informatique d'Arte n'a pas pu déterminer d'origine à cette attaque, relativement fréquente. Il a renouvelé ses consignes de sécurité auprès des employés, qui consistent essentiellement à se méfier des fichiers envoyés par des inconnus.

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

Source : http://www.rue89strasbourg.com/index.php/2015/04/10/breve/arte-victime-dune-attaque-informatique-jeudi/

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se

réclamant du groupe Etat Islamique | Le Net Expert Informatique

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique

Stupeur à TV5 Monde. La chaîne publique francophone internationale est victime, mercredi 8 avril au soir, d'une importante attaque informatique menée par des militants islamistes se revendiquant de l'organisation Etat islamique (EI), a confirmé son directeur général Yves Bigot. « Nous ne sommes plus en état d'émettre aucune de nos chaînes. Nos sites et nos réseaux sociaux ne sont plus sous notre contrôle et ils affichent tous des revendications de l'Etat islamique », a-t-il indiqué

Propagande et documents postés sur Facebook

Les pirates ont posté des contenus de propagande sur la page Facebook de la chaîne, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI. Après près de deux heures, les équipes de la chaîne ont pu reprendre la main sur la page de le TV5 Monde sur le réseau social. Les programmes ont par ailleurs été interrompus, tandis que le site internet de TV5 Monde est toujours indisponible.

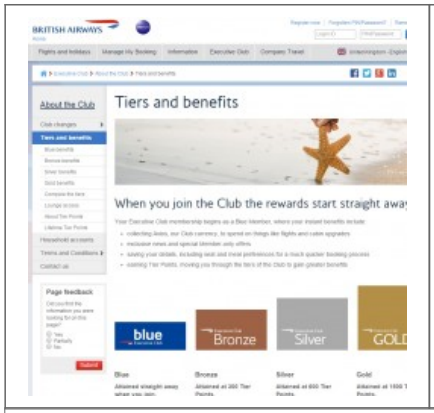
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source :
http://www.francetvinfo.fr/monde/proche-orient/offensive-jihadiste-en-irak/la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789.html#xtor=EPR-51-la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789-20150408-bouton

---

Alerte : Comptes clients piratés chez British Airways | Le Net Expert Informatique



Alerte : Comptes clients piratés chez British Airways

Une action de piratage a visé de nombreux comptes de clients de la compagnie aérienne British Airways. Les points fidélité amassés tout au long des différents trajets ont été effacés.

Depuis quelques jours, un grand nombre de clients de la compagnie aérienne British Airways ont eu la désagréable surprise de trouver que le solde de points fidélités accumulés grâce à leurs précédents trajets en avion avaient disparu. D'autres n'ont tout simplement plus accès à leur compte fidélité, appelé Executive Club. Une situation qui serait loin d'être le fruit du hasard ou d'un bug informatique, mais qui a plutôt à voir avec une opération de piratage sur un grand nombre de comptes.

Interrogée sur un forum dédié par un utilisateur, British Airways a admis avoir été mis au courant d'une activité non autorisée sur son compte. « Il semble que cela soit le résultat d'un tiers utilisant de l'information obtenue quelque part sur Internet, via un processus automatisé, pour tenter d'accéder aux comptes Executive Club », a indiqué British Airways dans un mail. Bien que les pirates sont parvenus à accéder à des comptes, British Airways n'est pour l'instant pas au courant d'accès à des pages d'information de comptes, historiques de vols ou détails de cartes de paiement.

Selon un message posté par la compagnie, les mots de passe des comptes affectés par ce piratage ont été changés et l'utilisation des points fidélité « Avios » suspendue pour quelques jours. La société a par ailleurs également répondu aux utilisateurs affectés par le problème sur Twitter.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-alerte-aux-comptes-clients-pirates-chez-british-airways-60700.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Laboratoire d'analyses médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

Laboratoire d'analyses médicales piraté : demande de rançon et publication de résultats médicaux

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de Synalocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle ne refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés
Aujourd'hui, rebelote avec le même groupe Rex Mundi et, la encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.
Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »
Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates
Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

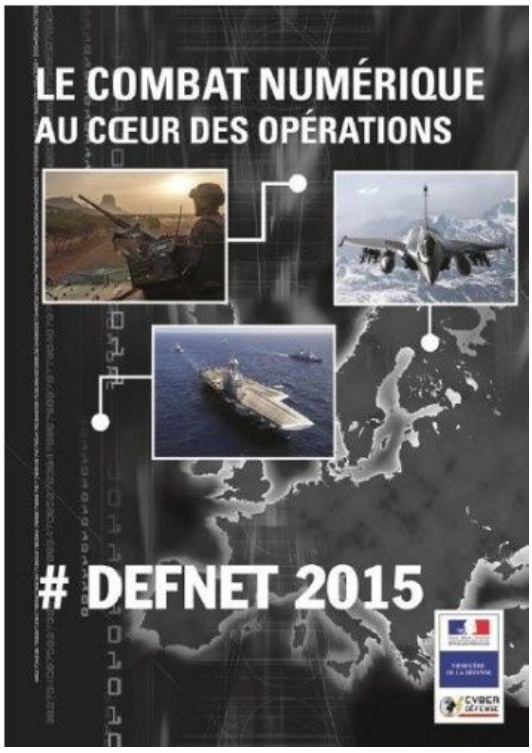
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINE et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Horte – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Puricard
Laboratoire de Saint Rémy de Provence

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

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm

Deux bâtiments de notre marine nationale victime d'une cyberattaque sans précédent | Le Net Expert Informatique



Deux bâtiments de notre marine nationale victime d'une cyberattaque sans précédent

Vengeance de Vladimir Poutine ? Malveillance d'un hacker jihadiste ? On ne sait pas… Toujours est-il que deux bâtiments de notre marine nationale, le « Mistral » et son jumeau le «Tonnerre », actuellement en opérations en Méditerranée, viennent de faire de l'objet de cyberattaques simultanées. Leurs ordinateurs de bord ont été infectés par un virus informatique, générant un dysfonctionnement du SCADA, le système de contrôle automatisé qui permet gérer les principales fonctions de ces bateaux de guerre, à commencer par leurs radars et leurs systèmes d'armes. Un groupe d'intervention rapide composé de six membres de nos forces spéciales de cyberdéfense est en cours de déploiement sur les deux navires afin de résoudre la crise au plus vite.

Jusqu'au 27 mars, ce second exercice interarmées doit valider les choix de la chaîne de cyber-défense des armées françaises. Les administrations et opérateurs vitaux sont également concernés.

La cyberdéfense monte en puissance au sein des armées françaises avec la tenue jusqu'au 27 mars de DEFNET 2015, le second exercice interarmées grandeur nature consacré à ce thème.
« Il s'agit d'entraîner l'ensemble de la chaîne de cyber-défense » explique Le lieutenant-colonel Stéphane Dossé, le directeur de l'exercice, qui précise : « Il ne faut pas voir la cyber-défense comme un grand show hollywoodien. C'est un travail opérationnel du quotidien où il faut maintenir et renforcer une ligne de défense, comme dans l'armée de terre ».
Dans la forme, on risque donc d'être bien loin de la vidéo promotionnelle publiée par le Ministère de la Défense en février dernier sur la cyber-guerre : pas de terroristes encagoulés tapis dans l'ombre, pas de missiles expédiés en salve depuis un bâtiment de marine, pas de sergent chef Néo pour prendre à bras le corps la Matrice.
'La cyberdéfense : le combat numérique au coeur des opérations ', vidéo promotionnelle publiée en février 2015 par le Ministère de la Défense.

Un premier exercice avait eu lieu en octobre dernier, avec « un thème simple, sur un seul lieu ». DEFNET 2015 s'articule lui sur une dimension multi-sites. Sept sites militaires sont concernés, ainsi que deux bâtiments de la Marine nationale.
Le scenario de DEFNET 2015 simule, dans un contexte international fictif, des menaces et des attaques cyber multiples contre plusieurs sites sur des thèmes très différents, mentionne le communiqué de presse du Ministère de la Défense. Il associe les spécialistes de cyberdéfense des unités interarmées et des trois armées.
SI militaire, opérateurs vitaux et administrations
Le Ministère de la défense définit la cyberdéfence comme « l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations ».
Mais dans le cadre de cet exercice, le périmètre de protection couvre en plus des systèmes d'information militaires, les opérateurs d'importance vitale et les administrations, raison pour laquelle l'Anssi est associée au projet.
A noter que cet exercice est l'occasion de tester le nouveau modèle de réserve cyber. Il s'agit d'accueillir des équipes de volontaires sur des sites militaires, simulant des sites d'intervention. Des équipes d'expérimentation sont constituées d'un réserviste des armées, d'un ou deux enseignants et de 10 à 12 étudiants en informatique et télécommunication d'un niveau bac+ à bac+5 (CentraleSupélec, Telecom Paris Tech ou encore l'Epita sont partenaires).
Elles devront effectuer un travail d'éradication de code malveillant et de réinstallation de système.
L'exercice rassemble en tout un effectif de 580 personnes.

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

Source :
http://www.zdnet.fr/actualites/defnet-2015-un-exercice-de-cyberdefense-multi-sites-est-en-cours-39816640.htm
Par Guillaume Serries

Toulouse attaqué par le virus «Rançongiciel» | Le Net Expert Informatique

Toulouse attaqué par le virus «Rançongiciel»

Ce mardi 10 mars, le système informatique de la ville de Toulouse a été attaqué par le virus «Rançongiciel», a confirmé hier une source municipale à La Dépêche du Midi3.

Vendredi 6 mars, les services informatiques municipaux avaient été mis en garde sur une éventuelle attaque par une autre collectivité de l'agglomération, qui avait elle-même été la cible de ce virus. «Rançongiciel» se propage par l'ouverture de pièces jointes dans les courriels, le téléchargement de fichiers infectés, la navigation sur internet. Il s'installe silencieusement dans l'ordinateur contaminé dont il crypte certains types de documents qui deviennent alors illisibles. Les pirates adressent alors un message dans lequel ils demandent une rançon en échange de la clé de déchiffrement des données. Généralement, cette clé n'est jamais fournie, même en cas de paiement.

Ce mardi 10 mars, un «Rançongiciel» a été détecté dans le système informatique de la ville de Toulouse qui avait été placé sous surveillance. Des mesures de précaution, comme l'interruption du travail en réseau, ont été prises immédiatement pour éviter sa propagation. De source interne, aucun fichier n'a été endommagé. Le réseau a été rétabli ce jeudi à 15 heures.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.ladepeche.fr/article/2015/03/13/2065766-le-reseau-de-la-ville-attaque-par-le-virus-rancongiciel.html

---

Alerte ! Des escrocs se font passer pour des techniciens en informatique | Le Net Expert Informatique

Alerte ! Des escrocs se font passer pour des techniciens en informatique

Mercredi, une habitante de Saint-Pal-de-Mons a subi une tentative d'escroquerie par des cybercriminels. Elle a reçu un appel téléphonique d'une personne parlant anglais se présentant comme employée d'une célèbre entreprise d'informatique. Selon les dires de son interlocuteur, son ordinateur serait infecté d'un virus. L'appel a été transmis à un second présumé technicien qui, toujours en anglais, a proposé à la San-palouse de prendre la main sur la machine.

La femme a alors eu la puce à l'oreille lorsqu'on a lui a demandé ses coordonnées bancaires. Elle a raccroché et s'est rendue dans une entreprise spécialisée. Des fichiers de son ordinateur ont été endommagés.
Elle a ensuité déposée plainte auprès des gendarmes de la communauté de brigades de Saint-Didier-en-Velay.
Selon nos informations, les premiers éléments tendraient vers une escroquerie depuis l'étranger, l'indicatif « 00221 » au moment de l'appel étant celui du Sénégal.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.leprogres.fr/faits-divers/2015/03/13/cybercriminalite-ils-se-font-passer-pour-des-techniciens-en-informatique

---

Des salariés de Twitter sont la cible de menaces de mort de la part de terroristes de l'état islamique | Le Net Expert Informatique

Des salariés de Twitter sont la cible de menaces de mort de la part de terroristes de l'état islamique