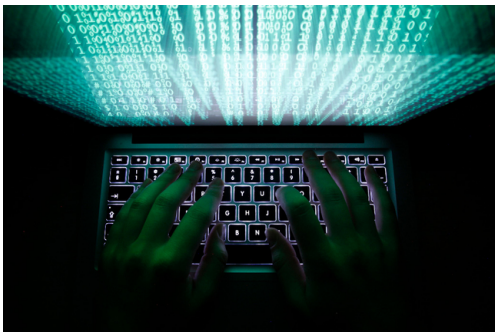
Les sites Internet trompeurs visent de plus en plus les PME| Le Net Expert Informatique

 Image: Photo d’illustration/Reuters	**Les sites Internet trompeurs visent de plus en plus les PME**

Les petites et moyennes entreprises sont aussi concernées par les attaques sur le web. Les pirates se servent des données des sites pour tromper les clients. La manœuvre la plus courante est d'envoyer des mails aux clients en se faisant passer pour l'entreprise.

Les escrocs opérant via Internet ne s'en prennent plus uniquement à des grandes marques connues: de plus en plus, ils imitent les sites web de petites et moyennes entreprises pour tromper leurs clients. Ils accèdent ainsi à leurs mots de passe ou données de cartes de crédit.
La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) intervient quotidiennement pour retirer ce type de contenus frauduleux du web, a-t-elle annoncé le mardi 31 mars. Les derniers cas rapportés témoignent même d'une sophistication accrue.
Les attaques de phishing, par lesquelles des escrocs cherchent à accéder à des données sensibles, concernent différents types de PME ayant un site WEB et qui enregistrent des adresses mail de clients, par exemple pour l'envoi d'une newsletter.
Dans un premier temps, les criminels attaquent le site web de l'entreprise. La plupart du temps, ils exploitent une faille sur le site. Cela leur permet d'accéder à une base de données contenant des mails de clients.
Ensuite, ils envoient des mails à ces clients en se faisant passer pour l'entreprise. Les messages font par exemple état d'un remboursement pouvant être demandé par le biais d'un lien indiqué. Derrière ce lien se cache un site web imitant à l'identique celui de l'entreprise et utilisant un nom de domaine très similaire.

Victime en confiance
Le client y est prié de fournir les détails de sa carte de crédit (numéro, validité, cryptogramme), à l'image d'une page de phishing «classique». En usurpant le mail et en imitant le site web d'une entreprise avec laquelle la victime potentielle est en relation, les escrocs augmentent leurs chances de succès, puisque la cible aura plus de chances de se sentir en confiance.
MELANI conseille aux entreprises d'informer rapidement leurs clients lorsqu'elles remarquent le vol d'e-mails. Quant aux utilisateurs, ils sont priés d'effacer les courriels leur enjoignant de fournir des données de cartes de crédit: aucune entreprise sérieuse ne demande de telles informations par mail, rappelle MELANI.
De plus, il faut se méfier des mails évoquant des conséquences (perte financière, plainte pénale, blocage d'un compte ou d'une carte etc) si le destinataire n'agit pas. Enfin, il faut toujours contrôler l'«adresse Internet» (URL) sur laquelle on est redirigé. Pour ce faire, il suffit de positionner la souris sur le lien sans cliquer. (ats/Newsnet)

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

Source : http://www.tdg.ch/high-tech/sites-internet-trompeurs-visent-plus-pme/story/15578282

L’armée mène une bataille numérique au cœur des entreprises sensibles | Le Net Expert Informatique

L’armée mène une bataille numérique au cœur des entreprises sensibles

3 mars 2015, les responsables d'une entreprise « sensible » sont inquiets. Il semble clair que la PME est l'une des nombreuses cibles d'une cyberattaque massive lancée contre les industriels français depuis plusieurs semaines maintenant. Face à cette attaque d'ampleur nationale et touchant des entreprises sensibles, le gouvernement fait appel à l'armée.

L'ordre est donc donné par le Premier Ministre d'agir rapidement et efficacement. La cellule de crise du commandement opérationnel de Cyberdéfense du ministère de la Défense va mobiliser dans les meilleurs délais ses équipes pour intervenir directement dans les entreprises touchées. Tous les relais militaires et civils spécialisés dans la cyberdefense sont en alerte.
Leur mission, atténuer la portée de l'attaque et reconstruire le réseau. Dépêchés le plus rapidement possible au cœur de l'entreprise, des équipes d'une quinzaine de spécialistes encadrés par un officier chargé de la logistique prennent place sur les postes informatiques de l'entreprise. Leurs outils ? Aucun, ils viennent dérouler le fil de l'attaque pour pouvoir mieux l'endiguer, colmater les brèches.
Leur difficulté c'est que pour limiter les dégâts, la PME est totalement coupée d'Internet. Les spécialistes s'acharnent à chercher les preuves, nettoyer en profondeur, détecter toutes les failles et verrouiller les portes. Des observateurs de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) sont présents pour faire remonter les informations auprès de l'organisme et coordonner les actions éventuelles à mener avec les différents ministères du gouvernement.
Une équipe de spécialistes constituée d'étudiants en quatrième année de l'EPITA est déployée par le commandement opérationnel de Cyberdéfense de l'armée pour reconstruire un réseau d'entreprise ayant subi une cyberattaque d'envergure. Dans l'avenir, ces étudiants pourraient faire partie des milliers de réservistes spécialisés que compte recruter le Ministère de la Défense.

« C'est du vécu »
Rapidement, les experts comprennent que le cybermissile s'est introduit tout simplement via une vulnérabilité WordPress du blog de l'entreprise. L'attaquant a installé un relai de scripts sur le serveur du blog qui lui permet d'aller plus avant dans ses funestes objectifs. Il pouvait même prendre la main sur l'ERP de l'entreprise. L'organisation pirate en a profité pour absorber la base de données de la société.
Mais voilà, ce scénario catastrophe est ce que l'armée appelle un « jeu », avec des « joueurs ». En réalité, ce jeu fait partie d'un exercice en grandeur nature réalisé par 600 personnes et encadré par le Ministère de la Défense et l'ANSSI. Baptisé DEFNET, l'expérimentation consiste à mettre en place des équipes constituées de dix à 15 élèves provenant de grandes écoles spécialisées dans le domaine de l'informatique et des télécommunications (Epita, Insa, Télécom Paris Tech, Ensta Bretagne, CentraleSupélec,…).
Encadré par un enseignant et un militaire, l'idée consiste à former à partir de ces ressources, les réservistes dédiés à la cyberdéfense de demain. L'armée compte disposer de plusieurs milliers de réservistes dans les prochaines années.
Lors de l'exercice, auquel ZDNet.fr a pu assister, le contre-Amiral Riban, Directeur Général adjoint de l'ANSSI a tenu à préciser que cette expérimentation repose sur « du vécu », sans en dire beaucoup plus, secret défense oblige. Dans ce genre de situation de crise, l'ANSSI est le chef d'orchestre. En élaguant les vagues de cyberattaques et les défacements de sites web en janvier, qui, pour lui étaient d'un niveau faible, il souligne qu'une véritable cyberattaque ne se résumerait pas forcément uniquement à des conséquences tragiques en termes de vol de données.
Ainsi, si les réseaux informatiques des banques, des aéroports, des réseaux de transport (SNCF, Ratp,…), ou les opérateurs de téléphonie étaient victimes d'une cyberattaque, la France pourrait être paralysée en quelques heures, avec tous les dangers que cela peut représenter. Enfin, interrogé sur une riposte éventuelle suite à une cyberattaque, le contre-amiral a précisé que l'article 21 de la loi de programmation militaire oblige à faire cesser l'attaque, mais pas d'aller au-delà. Le sujet est donc bien la défense…

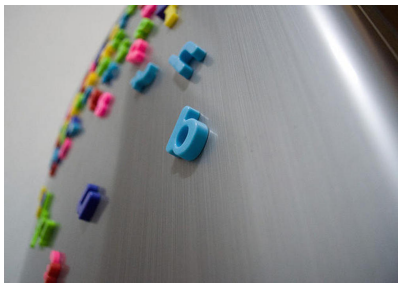
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/cyberdefense-quand-l-armee-mene-une-bataille-numerique-au-coeur-des-entreprises-sensibles-39817126.htm

---

L'attaque des réfrigérateurs

connectés a commencé ! | Le Net Expert Informatique



L’attaque des réfrigérateurs connectés a commencé !

D’apparence si inoffensive avec leurs façades remplies d’aimants, de cartes postales, de photos et de dessins d’enfants, les réfrigérateurs se sont pourtant dotés récemment d’une potentielle arme : un accès à Internet. Et c’est exactement ce qui est arrivé. Un réfrigérateur a été embrigadé dans un vaste botnet.

Un botnet est un réseau de programmes connectés à Internet servant différents desseins. Souvent, ils sont mis en place et utilisés par des hackers pour mener de vastes opérations d’attaque et/ou de piratage. Selon le spécialiste de la sécurité informatique Proofpoint, pareille attaque a eu lieu entre le 23 Décembre et le 6 Janvier. Plus de 100 000 appareils ont été « réquisitionnés », dont des routeurs, des stations multimédias, des téléviseurs et au moins un réfrigérateur.
Cette attaque aura permis d’envoyer plus de 750 000 emails de spam, par vagues de 100 000, trois fois par jour. Une même adresse IP n’envoyait alors pas plus de 10 emails, rendant la chose très délicate à bloquer. C’est la première fois qu’une cyberattaque de ce genre – faisant participer des appareils si communs – est recensée.
Et comme il fallait s’en douter, si les pirates ont pu utiliser ces machines, ce n’est pas parce qu’ils ont utilisé des moyens sophistiqués mais davantage parce que les mots de passe n’avaient pas été changé ou parce qu’ils étaient branchés sur des réseaux publics.
Comme le rappelle David Knight de Proofpoint : « la plupart de ces appareils sont très peu protégés, au mieux, et les consommateurs n’ont virtuellement aucun moyen de détecter ni de réparer la moindre infection le cas échéant. » Et dire que ces objets connectés seront au nombre de 200 millions d’ici 2020… Le terrain de jeu des hackers s’agrandit sensiblement !

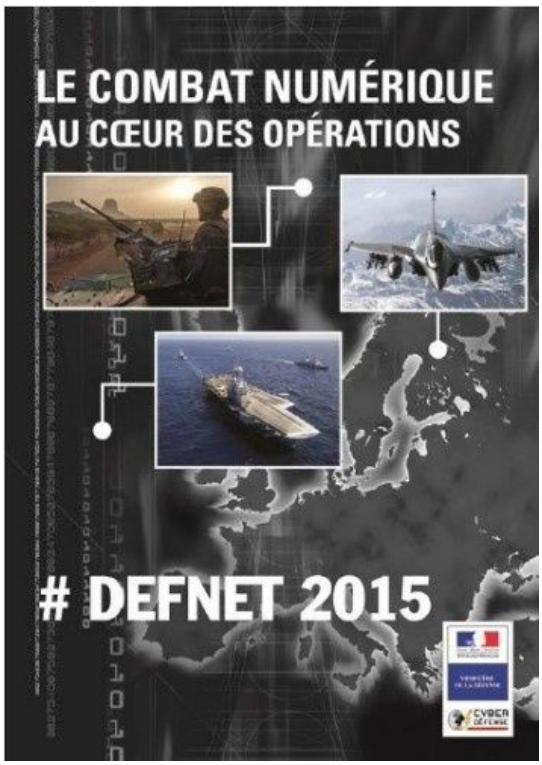
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.gizmodo.fr/2015/03/24/attaque-refrigerateurs-botnet.html

---

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

Projet de loi relatif au renseignement | Le Net Expert Informatique

Projet de loi relatif au renseignement

Le Conseil d'État a été saisi le 20 février 2015 et le 5 mars 2015 du projet de loi relatif au renseignement.

Ce projet de loi définit la **mission des services spécialisés de renseignement** et les **conditions dans lesquelles ces services peuvent être autorisés, pour le recueil de renseignements** relatifs à des intérêts publics limitativement énumérés, à recourir à des techniques portant sur l'accès administratif aux données de connexion, les interceptions de sécurité, la localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques, enfin à des mesures de surveillance internationale.
Il instaure pour l'ensemble de ces techniques, à l'exception des mesures de surveillance internationale, un régime d'autorisation préalable du Premier ministre après avis et sous le contrôle d'une autorité administrative indépendante dénommée « Commission nationale de contrôle des techniques de renseignement », qui pourra recevoir des réclamations de toute personne y ayant un intérêt direct et personnel. Il fixe les durées de conservation des données collectées.
Il prévoit un régime spécifique d'autorisation et de contrôle pour les mesures de surveillance et de contrôle des transmissions émises ou reçues à l'étranger.
Il institue un recours juridictionnel devant le Conseil d'État ouvert à toute personne y ayant un intérêt direct et personnel, ainsi qu'à la Commission nationale de contrôle des techniques de renseignement, tout en prévoyant des règles procédurales dérogatoires destinées à préserver le secret de la défense nationale.
Le Conseil d'État a veillé à ce que soient conciliées les nécessités propres aux objectifs poursuivis, notamment celui de la protection de la sécurité nationale, et le respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'est attaché à préciser et renforcer les garanties nécessaires à la mise en œuvre des techniques de renseignement, tenant en particulier à l'existence, d'une part, d'un contrôle administratif s'exerçant au moment de l'autorisation et en cours d'exécution, d'autre part, s'agissant d'une procédure administrative spéciale, d'un contrôle juridictionnel approfondi du Conseil d'État statuant au contentieux.

Lire la suite….

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

Source : http://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/Projet-de-loi-relatif-au-renseignement-PRMX1504410L-19-03-2015

Apologie du terrorisme : un premier site bloqué en France | Le Net Expert Informatique

Crédit capture d'écran ministère de l'Intérieur

Apologie du terrorisme : un premier site bloqué en France

En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet pourraient être concernés par ces mesures de blocage.

Le blocage du site www.islamic-news.info a été demandé par l'Office central de lutte contre la cybercriminalité.
Pour la première fois en France, un site internet a été bloqué administrativement pour apologie du terrorisme, a révélé le site spécialisé Next INpact. Consécutivement à l'adoption au mois de décembre de la loi de « lutte contre le terrorisme », le site www.islamic-news.info n'est plus accessible depuis le lundi 16 mars.
Sa page d'accueille redirige les internautes vers le site su ministère de l'intérieur et affiche le message suivant : « Vous avez été redirigé vers ce site officiel car votre ordinateur allait se connecter à une page dont le contenu provoque à des actes de terrorisme [sic] ou fait publiquement l'apologie d'actes de terrorisme ».
Un décret de la loi de « lutte contre le terrorisme » permet à l'Office central de lutte contre la cybercriminalité (OCLCTIC) d'exiger aux fournisseurs d'accès à internet le blocage sous 24 heures des sites désignés comme faisant « l'apologie du terrorisme ». Et ce sans consultation d'un juge.
En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet jihadistes pourraient être concernés par ces mesures de blocage.
D'après David Thomson, le journaliste de RFI qui a découvert ce blocage, le site » islamic-news.info » est « un site pro-jihad assez peu influent ». Celui-ci se définit comme « un site d'information musulman qui se concentre en particulier sur les territoires dits islamiques » et dit vouloir « fournir une information détaillée de l'actualité du monde musulman ainsi que des explications d'ordre politique et historique ».
Les auteurs du site précisent : « Ce site d'information n'est en aucun cas partisan d'un quelconque groupe, organisation ou mouvement politique, religieux, civil ou armé. Ceci étant, nous considérons qu'il est de notre droit de dénoncer la manipulation, même lorsqu'elle concerne des organisations classées comme 'terroristes' à l'image d'Al-Qaïda, de l'Etat islamique ou des Frères musulmans. Le fait de réfuter des affirmations s'attaquant à ces organisations ne peut en aucune manière signifier une adhésion de notre part à celles-ci ni même faire la promotion de leurs idées et actes. »

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

Source : http://www.atlantico.fr/pepites/apologie-terrorisme-premier-site-bloque-en-france-2042029.html

Attention, insérer cette clé USB dans votre PC peut le détruire ! | Le Net Expert Informatique

Attention, insérer cette clé USB dans votre PC peut le détruire !

Un facétieux hacker a mis au point une fausse clé USB capable de griller une machine lorsqu'elle est insérée dans une prise d'un ordinateur.

On ne le répètera jamais assez : n'insérez jamais dans votre ordinateur une clé USB si vous ne savez pas d'ou elle provient. Car elle pourrait non seulement inoculer un malware dans votre machine, mais aussi carrément… le détruire !
Bon, inutile de trop s'inquiéter, ce danger n'est encore que très théorique. Mais un facétieux hacker russe a bel et bien mis au point une fausse clé USB en mesure de griller les circuits d'un ordinateur en lui infligeant une décharge électrique. L'idée de ce projet est partie d'une légende urbaine amusante : « j'ai lu un article sur un gars qui a volé une clé USB dans le métro. Elle traînait dans la poche extérieure du sac d'un autre type. Il y avait marqué 128 dessus. Le gars est rentré chez lui, l'a inséré dans son ordinateur et la clé a grillé la machine. Alors il a écrit 129 sur la clé et l'a mis dans la poche extérieure de son sac. »

Pour fabriquer sa petite bombe, notre homme, qui travaille dans une entreprise d'électronique, a conçu un petit circuit imprimé et acheté quelques composants. Sa fausse clé contient plusieurs condensateurs et un convertisseur DC/DC. Lorsque la clé est branchée, les condensateurs se chargent grâce au port USB. Lorsqu'ils sont chargés, le convertisseur s'arrête et un transistor décharge l'énergie via les fils de données du port. Lorsqu'ils sont déchargés, le processus de charge reprend… et ainsi de suite jusqu'à ce que la clé grille la machine. Il estime être capable de détruire jusqu'au processeur avec son « invention ».
Ouf, notre hacker ne donne aucun détail qui pourrait permettre de créer son propre « USB Killer ». Il a évidemment plutôt conçu son appareil pour éveiller les consciences aux dangers que représente une clé USB inconnue. Et termine par une boutade : « quant aux applications de cet appareil, je ne les évoquerai pas. Mais un ancien collègue me dit que c'est comme la bombe atomique : c'est cool de l'avoir, mais il ne faut pas l'utiliser. »

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

Source : http://www.01net.com/editorial/648920/attention-inserer-cette-cle-usb-dans-votre-pc-peut-le-detruire/
Par Eric LB

Piratage de plans de

réacteurs nucléaires : le hacker fait du chantage | Le Net Expert Informatique

	Piratage de plans de réacteurs nucléaires : le hacker fait du chantage

SEOUL, 12 mars (Yonhap) – Le pirate informatique qui a rendu publics des plans de réacteurs nucléaires du pays à la fin de l'année dernière a fait ce jeudi du chantage, demandant de l'argent en contrepartie de sa promesse de ne pas dévoiler d'informations sensibles à des pays tiers.

Utilisant un compte sous le nom de président du soi-disant groupe antinucléaire, le hacker a posté 25 nouveaux fichiers sur Twitter qui incluraient des documents sur le réacteur 1400 développé par la Corée du Sud.
«Besoin d'argent. Vous n'avez qu'à répondre à quelques demandes. […] De nombreux pays d'Europe du Nord, d'Asie du Sud-Est et d'Amérique du Sud disent qu'ils achèteront des informations sur le réacteur nucléaire. Peur que la vente de la totalité des informations ne détruise les efforts de la présidente Park (Geun-hye) visant à exporter des réacteurs nucléaires», a-t-il dit sur son compte Twitter.
Le pirate informatique n'a pas précisé le montant qu'il voulait mais a dit que la Corée du Sud finira par perdre beaucoup plus si elle tente d'économiser des centaines de millions de dollars.
Des responsables de Korea Hydro & Nuclear Power Co. (KHNP) ont déclaré n'avoir pas encore pu déterminer la nature des documents dévoilés car le protocole de sécurité bloquait les téléchargements et l'ouverture des fichiers. Il s'agit de la sixième menace de ce genre depuis le 15 décembre dernier.
«Depuis que le soi-disant groupe antinucléaire a fait sa cinquième annonce le 23 décembre, aucune attaque informatique ou fuite d'information n'a eu lieu. Les documents publiés aujourd'hui semblent avoir été obtenus bien avant (le 23 décembre)», a déclaré l'entreprise dans un communiqué.
Jusqu'à présent, le pirate avait demandé à la KHNP de fermer quelques réacteurs nucléaires, menaçant de «semer la destruction» dans les usines nucléaires si ces demandes n'étaient pas respectées avant Noel. Rien ne s'était passé après Noel. La KHNP insiste que le pirate n'a pas pu se procurer d'information confidentielle car son serveur interne a été entièrement isolé depuis le début de l'année dernière.
Le pirate a également félicité dans son dernier message la KHNP pour avoir trouvé 7.000 virus, tout en affirmant que 9.000 autres attendent ses ordres. Les informations divulguées aujourd'hui comprendraient également la transcription d'une conversation téléphonique datant du 1er janvier entre la présidente Park Geun-hye et le secrétaire général des Nations unies Ban Ki-moon.

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

Source : http://french.yonhapnews.co.kr/news/2015/03/12/0200000000AFR20150312002400884.HTML
Par mathieu@yna.co.kr

Colloque « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique » | Le Net Expert Informatique

Colloque à Montpellier « Innovation et cybercriminalité : l'Europe face aux défis de la transformation numérique »

Programme du Mercredi 8 avril 2015

13:30-14h Accueil des participants

14h:00 Ouverture du colloque :
Philippe Augé, Président de l'Université de Montpellier
Marie-Elisabeth André, Doyen de la Faculté de Droit et Science politique de Montpellier
Adel Jomni, Enseignant-chercheur, Université de Montpellier
Michal Choras, Représentant du projet européen CAMINO
Akhgar Babak, Représentant du projet européen COURAGE

14h30 Session 1: Innovations numériques, Cybercriminalité et Cyber-terrorisme : Enjeux et défis : quelles stratégies ? :
Lord Carlile of Berriew, Membre du Parlement du Royaume-Uni,
Général Marc Watin-Augouard, Directeur du centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)
Andy Archibald, Directeur adjoint de l'unité nationale cybercriminalité de l'Agence Nationale de la Criminalité du Royaume-Uni
Marco Lozano, Représentant INCIBE (Instituto Nacional de Ciberseguridad de España)

16h:00 Pause

16h:15 Session 2: Les menaces cybernétiques : Analyse des risques et des stratégies? :
Président de session : Cormac Callanan, Expert auprès du Conseil de l'Europe, CEO, Aconite, Irlande
– Etat des lieux des cyber menaces – Jean-Dominique Nollet, Directeur de l'unité d'investigation et recherche (European Cybercrime Centre (EC3-Europol)
– L'investigation et la coopération entre les organisations internationales (Interpol, Europol,..) – Valérie Maldonado, Directrice de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)
– Analyse des réseaux sociaux et sécurité nationale – Thomas Delavallade, THALES
– Comment améliorer la résilience face à la cybercriminalité et au cyber-terrorisme (Projet Européen CAMINO – FP7) – Michal Choras,Professeur, Coordinator du projet FP7-CAMINO, ITTI, Pologne

---

Programme du Jeudi 9 avril 2015

9h:00 Session 3: Enjeux et risques liés au développement des monnaies virtuelles
Président de session : Daniel Guinier, Expert en cybercriminalité, Cour Pénale Internationale de La Haye
– Flux illicites et monnaies virtuelles – Myriam Quéméner, Magistrate, Cour d'appel de Versailles
– Monnaie virtuelle et crypto monnaie : quels enjeux et réponses réglementaires? Quelles préconisations pour les utilisateurs et les entreprises? – Cathie-Rosalie Joly, Avocate
– Paiements 2.0: nouveaux défis de sécurité et rôle de l'Autorité Bancaire Européenne – Geoffroy Goffinet, European Banking Authority (EBA)- Bruxelles

---

10h:15 Pause

10h:30 Session 4: Big data, Internet des objets, Cybersécurité et protection de la vie privée
Président de session : Christian Aghroum, Membre CDSE, Expert en Cybersécurité
– Big Data et sécurité : le pouvoir de l'anticipation au service de la cybersécurité – Adel Jomni, Enseignant-chercheur, Université de Montpellier
– Le droit est-il un frein pour le développement du Big Data ? – Francesca Bosco, Chef de projet UNICRI (United Nations Interregional Crime and Justice Research Institute); Giuseppe Vaciago, Cybercrime Institute, Germany
– Objets connectés et santé : l'innovation au service ou au détriment du citoyen? – Corinne Thierache, Avocate
– Le Big Data : un déclencheur de changement des règles juridiques – Fraser Sampson, Responsable de l'office des crimes – West Yorkshire Police

---

13h:00 Pause déjeuner

14h:00 Session 5: Projets européens, coopération internationale, recherche et formation dans le domaine de la lutte contre la Cybercriminalité et le Cyberterrorisme
Président de session : – Nigel Jones,Directeur du Centre for Cybercrime Forensics, Université de Canterbury
– Défis majeurs de la recherche dans le domaine de la cybercriminalité et le cyber terrorisme – Akhgar Babak, Projet Européen COURAGE
– Nouvelles approches de la protection des données et Cryptographie -Projet ENISA (European Union Agency for Network and Information Security) – María Pilar Torres Bruna,Responsable Cybersécurité chez Everis, Espagne
– Nouvelles méthodes d'investigation et de formation forensique dans un environnement virtuel (cloud) (projet D-FET) – Adrian Smalesn Researcher, Université Napier d'Edimbourg
– La coopération internationale pour renforcer les capacités de protection des infrastructures d'information critiques 2015-2020 (CIIP) – Jean-Christophe Letoquin, Expert auprès du Conseil de l'Europe, Président de SOCOGI
– Coopération internationale en matière de formation cyber (enjeux et rôles des partenaires) ? – Yves Vandermeer, Federal Computer Crime Unit, Belgique E.C.T.E.G Chair (Europol)

16h:00 Fin du colloque

Emportez le programme avec vous ! Téléchargez le PDF

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…

Piratage de ses comptes sociaux : prévenir, repérer et réagir ! | Le Net Expert Informatique

Piratage de ses comptes sociaux : prévenir, repérer et réagir !

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

I- Prévenir un piratage

Choisissez des mots de passe complexes, différents et non-signifiants !

Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

Ne communiquez pas votre mot de passe

Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maitre ou dans une application non sécurisée.

Activez un dispositif d'alerte en cas d'intrusion

La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par mail. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

Déconnectez à distance les terminaux encore liés à votre compte

Là encore, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

Désactivez les applications tierces connectées à votre compte

Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisés l'accès par le passé et qui ne vous servent plus.

Réglez vos paramètres de confidentialité

En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

II- Repérer un piratage

• votre mot de passe est invalide
• des tweets/posts imprévus sont envoyés depuis votre compte
• des messages privés sont envoyés de façon non volontaires
• des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
• une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse email associée à votre compte.

III- Réagir en cas de piratage

1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe.

Si un site/réseau social n'apporte pas de réponse satisfaisante, contactez la CNIL

3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

---

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

Source : http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/piratage-de-ses-comptes-sociaux-prevenir-reperer-et-reagir/