La menace du phishing plane sur les PME : trois étapes pour éviter le pire

La menace du phishing plane sur les PME : trois étapes pour éviter le pire

Les attaques informatiques ciblant de grands groupes, comme TV5monde, font régulièrement la une des journaux. Selon le rapport 2014 PwC sur la sécurité de l'information, 117 339 attaques se produisent chaque jour au niveau mondial.

Depuis 2009, les incidents détectés ont progressé de 66%.
Cependant, ce type d'attaques, très répandue, cible en grande partie les PME. Selon un rapport de l'ANSSI, 77% des cyber-attaques ciblent des petites entreprises.
Les conséquences peuvent être désastreuses pour ces structures à taille humaine, n'ayant pas forcément la trésorerie suffisante pour assurer leur activité en attendant le remboursement de leur assurance. Le coût d'une attaque peut s'avérer très élevé et la crédibilité de l'entreprise visée peut également en pâtir.
Suite à une attaque informatique du type « fraude au président », la PME française BRM Mobilier a ainsi perdu cet été 1,6 M€ et se trouve aujourd'hui en redressement judiciaire.
En mai dernier, le PMU a effectué un test grandeur nature en envoyant un faux email, proposant de gagner un cadeau, avec une pièce jointe piégée. Résultat : 22% des salariés ont téléchargé la pièce jointe et 6% ont cliqué sur le lien contenu dans l'email et renseigné leurs données personnelles.

Comment éviter que ce type de scénario ne vire à la catastrophe ?
1 – Connaitre le déroulé d'une attaque Le phishing, également appelé hameçonnage, est une technique employée par les hackers pour obtenir des données personnelles, comme des identifiants ou des données bancaires.
Le déroulement est simple : le hacker envoie un email en usurpant l'identité d'un tiers de confiance, comme un partenaire, un organisme bancaire, un réseau social ou encore un site reconnu.
L'email contient une pièce jointe piégée ou un lien vers une fausse interface web, voire les deux.
Si le subterfuge fonctionne, la victime se connecte via le lien, et toutes les informations renseignées via la fausse interface web sont transmises directement au cybercriminel.
Autre possibilité : la pièce jointe est téléchargée et permet ainsi à un malware d'infester le réseau de l'entreprise.

2 – Comprendre la dangerosité d'une attaque pour l'entreprise
Pour les entreprises, le phishing peut s'avérer très coûteux. Il est bien évidemment possible que le hacker récupère les données bancaires pour effectuer des virements frauduleux.
Puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites, les informations recueillies sont parfois réutilisées pour pirater d'autres comptes, comme une messagerie, un site bancaire, ou autre.Mais – puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites – il est aussi possible que le hacker réutilise les informations recueillies pour pirater une boite mail, ou un compte cloud.
Le cybercriminel peut ainsi consulter l'ensemble de la boîte mail, ou des comptes de sauvegarde cloud, et mettre la main sur des documents confidentiels, comme des plans ou des brevets, pouvant nuire à l'entreprise.
Enfin, les hackers profitent du piratage des boîtes mails pour envoyer à tous les contacts un nouvel email de phishing. La crédibilité de l'entreprise peut ainsi être touchée et ses clients pourraient subir à leur tour des pertes.

3 – Se préparer et éduquer avant qu'il ne soit trop tard
Les emails de phishing ont bien souvent une notion « d'urgence », qu'il s'agisse d'une demande pressante de la part d'un organisme ou d'un partenaire, ou d'une participation à un jeu concours « express ». Le but étant bien évidemment de ne pas laisser le temps à la victime de prendre du recul.
Comprendre le procédé d'une attaque est la première étape pour organiser sa défense. Il faut donc éduquer les salariés et leur donner quelques astuces pour ne pas tomber dans le piège :
• faire attention aux fautes d'orthographe : bien que les emails de phishing soient de mieux en mieux conçus, on y retrouve régulièrement des erreurs de syntaxe ou d'orthographe.
• regarder l'adresse mail ou le lien URL : même lorsqu'un email ou une interface web est une parfaite copie de l'original, l'adresse de l'expéditeur ou l'URL n'est pas la bonne puisqu'elle ne provient pas du même nom de domaine.
Des salariés éduqués et conscients du danger sont le meilleur atout contre les cyber-attaques, en particulier contre le phishing.
Mais, cela n'est pas suffisant, notamment sur les terminaux mobiles où nous avons tous tendance à être plus spontanés et donc, à adopter des comportement à risques.
Il est donc important de mettre en place un filtre anti-phishing aussi bien sur les postes fixes que sur les terminaux mobiles. Ces filtres scannent automatiquement les expéditeurs et les contenus afin de bloquer les emails suspects.
Pour les PME, il est donc important d'éduquer l'ensemble du personnel, mais aussi de mettre en place des solutions de filtrage email et de sécurité complètes. Par ailleurs, garder une proximité avec son équipe informatique, ou ses fournisseurs de services, peut également jouer un rôle primordial pour limiter les dommages si un employé est tombé dans le piège.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-menace-du-phishing-plane-sur,20151123,57740.htm

Les hôtels Hilton victimes d’une cyber-attaque

	Les hôtels Hilton victimes d’une cyber-attaque

La chaîne hôtelière américaine Hilton a annoncé mardi avoir fait l'objet d'une attaque informatique destinée à voler les données bancaires de ses clients.

Cette cyber-attaque s'est déroulée en deux temps, précise le groupe dans un communiqué. Les hackers ont installé un logiciel malveillant du 18 novembre au 5 décembre 2014. Une nouvelle attaque a eu lieu du 21 avril au 27 juillet 2015, ajoute Hilton sans dire si les deux attaques ont été commises par les mêmes pirates informatiques.

« En collaboration avec des experts, des représentants de la loi et des émetteurs de cartes bancaires, Hilton Worldwide est parvenu à déterminer que le logiciel malveillant ciblait des informations spécifiques des cartes de paiement » dont les noms, les numéros, les codes de sécurité et les dates d'expiration.

Aucune adresse personnelle, ni de codes Pin n'ont été volés, assure le groupe hôtelier, qui préconise néanmoins par précaution aux personnes ayant séjourné dans ses établissements lors des périodes des attaques de vérifier leurs déclarations bancaires mensuelles. En cas d'irrégularité, Hilton demande aux clients victimes de contacter immédiatement leur banque.

Cette révélation tombe quatre jours seulement après que la chaîne hôtelière Starwood (Sheraton, St.Regis, W, Le Méridien…) a fait état d'une attaque informatique similaire.

Réagissez à cet article

Source : http://information.tv5monde.com/en-continu/les-hotels-hilton-victimes-d-une-cyber-attaque-69830

Droit à l'oubli : Google dévoile les domaines les plus

affectés

Droit à l'oubli : Google dévoile les domaines les plus affectés

Google a publié un nouveau rapport concernant ses travaux dans le cadre du droit à l'oubli. Celui-ci met en évidence les noms de domaine principalement concernés.

En mai 2014, la Cour de justice de l'Union européenne avait ordonné aux moteurs de recherche en Europe de publier un formulaire de droit à l'oubli.
Ce dernier permet à un individu, ou une entreprise, de gérer sa réputation sur Internet en demandant au moteur de retirer des liens pointant vers certaines pages désuètes, ou qui affectent son image ou sa vie privée.
Au total, Google explique avoir reçu 348 085 requêtes de la part des internautes, lesquelles portent au total sur 1 234 092 liens. Le géant de la recherche affirme avoir accepté 42% de ces demandes.

En France, 73 399 formulaires ont été remplis portant sur 246 158 URL.

Google en a profité pour partager les noms de domaine qui reviennent le plus souvent au travers du formulaire de droit à l'oubli :
www.facebook.com (10220 liens supprimés)
profilengine.com (7986 liens supprimés)
groups.google.com (6764 liens supprimés)
www.youtube.com (5364 liens supprimés)
www.badoo.com (4428 liens supprimés)
plus.google.com (4134 liens supprimés)
annuaire.118712.fr (3930 liens supprimés)
www.twitter.com (3879 liens supprimés)
www.wherevent.com (3465 liens supprimés)
www.192.com (3083 liens supprimés)

Ces noms de domaine compteraient pour 9% de l'ensemble des requêtes reçues par Google.

Réagissez à cet article
Source : http://pro.clubic.com/entreprises/google/actualite-787400-droit-oublie-google-domaines-affectes.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1262345739##pid=22889469

Les nouveaux moyens de communication des terroristes

Les nouveaux moyens de communication des terroristes

La cybercriminalité traque en permanence les terroristes et tente par tous les moyens de trouver comment ils communiquent entre eux. Playstation, réseaux sociaux et même, sites de rencontre, tout est envisageable.

« Tout système de communication par messagerie peut potentiellement être utilisé par les terroriste… » s'exprimait Eric Freyssinet, chef de la division de lutte contre la cybercriminalité.
L'appli Telegram utilisée par les djihadistes Cette appli permet aux messages d'être cryptés. C'est par ce biais que Daech communiquerait, une appli qui, contrairement à Viber ou Whatsapp qui gardent tous les messages, permettrait plus de discrétion.
De plus, la plupart du temps ils s'expriment en arabe et en langage codé ce qui complique la tâche des enquêteurs.

La PS4 au centre des attentions
La raison ? Elle aurait été utilisée pour planifier les attentats du vendredi 13 novembre selon le site américain Forbes. Et si vous vous demandez comment, vous pouvez par exemple, avec le jeu Call Of Duty, écrire des mots sur un mur via l'impact des balles, traces qui finiront par définitivement s'effacer, sans laisser de preuves.
« J'ai entendu que le mode de communication entre terroristes le plus difficile à surveiller, c'est la PS4. C'est très, très difficile pour nos services » s'exprimait il y a quelques jours le ministre des Affaires étrangères belge. Sa déclaration n'a pas mis longtemps a agité les internautes…

Réagissez à cet article
Source : http://nextplz.fr/actualite/content/2151616-les-nouveaux-moyens-de-communication-des-terroristes

---

Le Bitcoin financerait le

terrorisme

Le Bitcoin financerait le terrorisme

Les pays européens prévoient d'attaquer le Bitcoin et d'autres modes de paiement anonymes telles que les cartes de crédit prépayées parce qu'ils permettent aux terroristes de financer leurs attaques.

Reuters prétend que les pays européens préparent un projet pour contrer le Bitcoin et d'autres modes de paiement anonymes.

On a le Bitcoin, mais également les cartes de crédit prépayées.

Les ministres de la justice et de l'intérieur de nombreux pays européens vont se réunir la semaine prochaine à Bruxelles afin de voter de nouvelles mesures pour contrer le terrorisme en Europe.

Il y a de nombreuses mesures pénales, mais il y a également un projet pour attaquer les paiements anonymes. Selon les informations obtenues par Reuters, une réunion préliminaire a déjà eu lieu et elle a proposé de meilleurs contrôles sur le Bitcoin, les cartes de crédit prépayées, l'or et les métaux précieux. Notons que l'or ne sera pas directement attaqué (ce serait trop évident), mais il sera interdit d'utiliser des paiements anonymes pour transférer de l'or ou d'autres métaux précieux (Les investisseurs sur les métaux précieux comprendront rapidement ce qui se trame).

Les ministres européens estiment également que le contrôle du Bitcoin et des paiements anonymes permettra de réduire le commerce des biens illicites.

Les attaques sur Paris ont eu le vendredi dernier. Samedi, on a déjà une déclaration de guerre de la part de la France, lundi, on a un projet de loi en France sur l'Etat d'urgence qui transforme ce pays en l'une des pires dictatures avec des pouvoirs de surveillance illimités. Mardi, les républicains aux Etats-Unis profitent de l'attaque sur Paris pour rejeter les réfugiés syriens à la mer, mercredi, les partis d'extrême-droite redoublent d'effort pour alimenter l'islamophobie et jeudi, on attaque le Bitcoin, les paiements anonymes, l'or et les métaux précieux, soit les principales épines dans le pied du système financier.

Est-ce qu'on sait que les terroristes ont utilisé le Bitcoin ? Est-ce que Daesh paie ses armes avec de l'or ? Est-ce que le Bitcoin est principalement utilisé par des criminels ? On a un triple non. En 5 jours, les politiciens américains et européens votent tout ce qu'ils peuvent pour faire chier leurs populations respectives pour les prochaines décennies. Il reste encore 2 jours… On craint le pire.

Réagissez à cet article

Source : http://actualite.houss
eniawriting.com/tech
nologie/2015/11/19/leurope-va-attaquer-le-bitcoin-
parce-quil-finance-le-terrorisme/10675/

Beijing (Pékin) renforce son niveau de sécurité

	**Beijing (Pékin) renforce son niveau de sécurité**

L’Agence de presse Xinhua a annoncé que la police de Beijing a déclaré samedi avoir renforcé la sécurité de la capitale dans le cadre d’un effort de lutte contre le terrorisme qui a vu une augmentation des forces de police et des contrôles plus stricts des colis.

Le Bureau municipal de la Sécurité Publique de Beijing (PSB) a relevé le niveau de sécurité pour la capitale le 15 novembre, deux jours après les attentats de Paris.
Davantage de policiers ont été mobilisés, et des contrôles plus stricts sur les services de messagerie, les grands événements et les transports publics ont été imposés.
Le PSB a mobilisé à la fois la police armée et les policiers réguliers, demandant « à la police de la circulation d’arrêter les voitures, aux hommes et femmes affectés aux patrouilles d’inspecter et d’enregistrer toutes les activités, à la police armée de faire une démonstration de force, et à la police auxiliaire de coopérer », a rapporté dimanche le Beijing Youth Daily.
Les forces de police collaborent pour effectuer des contrôles 24 heures sur 24 sur les gens, les voitures et les objets à chaque entrée de la municipalité de Beijing.
Selon le Beijing Youth Daily, depuis novembre, Beijing a inspecté plus d’1 million de voitures et plus d’1,6 million de personnes, et a arrêté plus de 100 suspects sur diverses charges.
De son côté, le Beijing Times a rapporté les propos de Wang Xiaohong, chef du PSB, qui avait dit en avril que la sécurité du transport par métro était la plus grande priorité pour les efforts de lutte contre le terrorisme. Ni Lexiong, un expert anti-terrorisme, a pour sa part dit dimanche que la prévention du terrorisme est non seulement une responsabilité de la police, mais aussi de la société dans son ensemble.
« Les entreprises et les organisations manquent actuellement de sensibilisation à la lutte contre le terrorisme. Si elles étaient attaquées par des terroristes, les résultats seraient inimaginables », a-t-il expliqué.
M. Ni a noté que dans Beijing, les endroits faisant face aux plus grands risques d’être attaqués par des terroristes comprennent les pôles de transport majeurs, les écoles, les hôtels et les lieux de réunion. Il a conseillé qu’une attention particulière soit également être accordée aux festivals chinois, en particulier le Nouvel An chinois. Xinhua a de son côté rapporté que la police de Beijing a également lancé des exercices anti-terroristes en mai et en octobre 2014.
« Malgré les efforts de la police, les écoles, les hôtels, les entreprises et les organisations devraient consacrer plus de personnel et d’argent à l’organisation d’exercices anti-terroristes et devraient proposer leurs propres plans pour faire face aux situations d’urgence », a souligné M. Ni.
Selon lui, la capitale a la capacité de surveiller les nouveaux canaux de communication, y compris la console de jeux vidéo PlayStation 4, si les terroristes l’utilisaient pour communiquer.
Li Wei, expert anti-terrorisme à l’Instituts des relations internationales contemporaines de Chine, estime pour sa part que la Chine est confrontée à des menaces plus terroristes et que le gouvernement devrait prendre davantage de mesures, y compris des actions contre le cyber-terrorisme, pour empêcher les attaques et protéger la vie et la propriété des gens.
Xinhua a également rapporté qu’au cours de la conférence sur la sécurité en cas d’urgence tenue le 15 novembre, Guo Shengkun, le patron de la police chinoise, a souligné la nécessité de renforcer la sensibilisation et le renforcement des mesures préventives anti-terrorisme.
Enfin, le Beijing Youth Daily a rappelé qu’en mars 2014, Beijing a aussi adopté de nouveaux règlements qui stipulent que les citoyens qui rapportent des informations liés à la violence et au terrorisme seront récompensés.

Réagissez à cet article
Source : http://french.china.org.cn/china/txt/2015-11/23/content_37138481.htm

Faut-il avoir peur des cyberdjihadistes ?

Faut-il avoir peur des cyberdjihadistes ?

Des pirates informatiques se présentant comme des hackers de Daesh multiplient les actions sur le Web. Les spécialistes tirent la sonnette d'alarme.

Depuis l'attaque du site internet de la chaîne de télévision TV5 Monde, en avril dernier, la France a essuyé des dizaines d'attaques informatiques émanant de prétendus cyberbataillons de l'organisation État islamique. Mardi matin, au cours d'une visite au QG d'interception des services de renseignements britannique à Cheltenham, George Osborne, chancelier de l'Échiquier (l'équivalent de notre ministère de l'Économie) du Royaume-Uni, a déclaré redouter des attentats numériques d'ampleur de la part de Daesh. « Ce mouvement terroriste utilise déjà Internet pour ses hideux objectifs de propagande, pour la radicalisation, pour la gestion de ses opérations », a déclaré George Osborne.
« Ils n'ont pas encore pu l'utiliser pour tuer, en s'en prenant à notre infrastructure. Mais nous savons qu'ils souhaitent le faire et font tout leur possible pour y parvenir », a-t-il ajouté.
Après l'intrusion en octobre dernier d'un hacker pro-palestinien dans la boîte mail de plusieurs officiels américains, à commencer par le directeur de la CIA, la menace d'attaques numériques est prise très au sérieux par les spécialistes de cybersécurité. « Cette réalité est considérée avec gravité depuis plusieurs années en Israël.
L'Europe commence à s'en préoccuper », confie Guy-Philippe Goldstein, l'un de ces consultants qui intervient au sein de l'Institute for National Security Studies (INSS), un think tank basé à Tel-Aviv. « Le niveau d'expertise des hackers djihadistes ne leur a permis jusque-là que de perturber temporairement le fonctionnement de sites officiels, mais on sait qu'ils peuvent sous-traiter certaines missions en recourant à des savoir-faire disponibles sur le dark web [la partie du réseau qui n'est accessible que par les pirates informatiques, NDLR] », poursuit Guy-Philippe Goldstein. Combien d'hommes comptent les cyberbataillons djihadistes ? La question reste en suspens, mais agite nombre de conversations dans les travées du Milipol, le salon professionnel dédié à la sécurité intérieure des États, qui s'est ouvert la semaine dernière à Villepinte. Quel que soit leur nombre, les membres de l'équipe qui s'est autoproclamée Cybercalifat réalisent des intrusions de plus en plus profondes dans nos systèmes de défense. La plus sérieuse a eu lieu en décembre dernier aux États-Unis. À cette occasion, des données confidentielles concernant des officiers supérieurs de l'armée américaine ont été subtilisées, qui ont ensuite été postées sur le compte Twitter de plusieurs sympathisants du groupe État islamique. Une menace prise au sérieux « En marge de ces opérations de déstabilisation psychologique que constituent la prise de contrôle et la dégradation de sites d'administration, et en dehors du coût que ces dégâts engendrent, d'autres interventions sont à craindre », indique Solange Ghernaouti, professeur à l'université de Lausanne, sollicitée par l'état-major suisse pour des missions de conseil. Cette enseignante en informatique, diplômée de l'université Paris-VI et ancienne auditrice de l'Institut de hautes études en défense nationale (IHEDN), a elle-même vu le site de l'équipe de recherche qu'elle dirige être attaqué en mars dernier. « Il m'a fallu trois jours pour tout remettre en état », indique-t-elle. En affirmant que les autorités britanniques surveillent attentivement 450 sites internet de « services sensibles » (énergie, distribution et traitement de l'eau, défense) susceptibles d'être visés par des interventions de pirates informatiques de Daesh, George Osborne accrédite l'idée que ces hackers auraient atteint une capacité de nuisance inquiétante. « Probablement liée au rapprochement qu'ont effectué les terroristes avec le monde très fermé de la cybercriminalité », estiment conjointement Guy-Philippe Goldstein et Solange Ghernaouti.

Réagissez à cet article
Source : http://www.lepoint.fr/high-tech-internet/faut-il-avoir-peur-des-cyberdjihadistes-17-11-2015-1982367_47.php

---

Des amendes plus lourdes de

la part de la Cnil ? – Denis JACOPINI Expert informatique

	**Des amendes plus lourdes de la part de la Cnil ?**