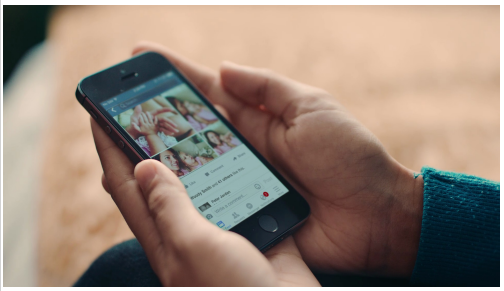
Facebook vous traque sur le Web même si vous n’êtes pas membre

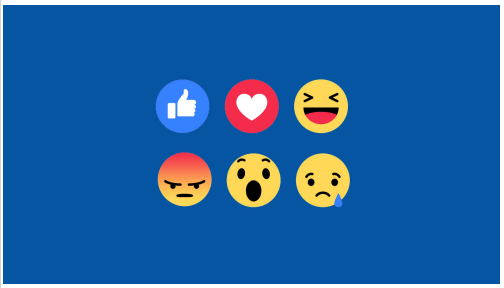
Facebook vous traque sur le Web même si vous n’êtes pas membre

Facebook devient une régie publicitaire ouverte aux sites tiers, et affichera des publicités ciblées y compris pour les internautes qui ne sont pas inscrits sur le réseau social. Il utilisera ses scripts présents sur de nombreux sites pour suivre l'internaute dans ses déplacements sur le Web, et comprendre ce qui l'intéresse.

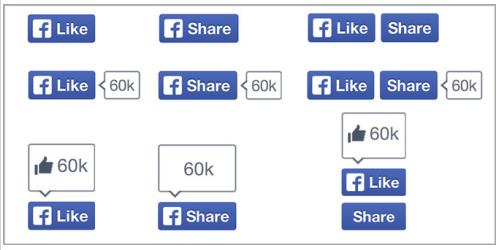


On connaît tous une ou deux personnes qui se refusent à utiliser Facebook et échappent encore et toujours aux griffes du réseau social. Mais l'empire de Mark Zuckerberg ne cesse de s'étendre et touchera bientôt même ces irréductibles qui n'ont jamais ouvert de compte sur la plateforme.

L'entreprise a annoncé qu'elle allait diffuser des annonces à tous les visiteurs de sites utilisant sa régie publicitaire Facebook Audience Network, concurrente de Google Adsense. Autrement dit, même les personnes qui ne sont pas inscrites sur Facebook et celles qui n'y sont pas connectées seront ciblées par des publicités qui, jusqu'ici, n'étaient visibles que par les personnes connectées au réseau social.
Ce n'est un secret pour personne, la force de Facebook réside dans sa capacité à récolter des données sur ses utilisateurs. Grâce à cela, il peut facilement montrer des publicités ciblées et adaptées sur mesure en fonction des préférences identifiées. Une aubaine pour les annonceurs qui ne perdent ainsi pas de temps et d'effort à diffuser tous azimuthes leurs contenus.



TRAQUER LES HABITUDES DE TOUS LES INTERNAUTES
Mais comment Facebook peut-il en faire de même avec les personnes qui ne se trouvent pas dans son réseau ? Il va utiliser plusieurs outils à sa disposition pour traquer efficacement un maximum d'internautes, comme le fait Google. Facebook va ainsi se servir de cookies, de ses propres boutons et plugins de partage affichés sur les sites, ainsi que d'autres informations collectées sur les sites tiers.
« Nos boutons et nos plugins envoient des informations de base sur les sessions de navigation des utilisateurs. Pour les non-membres de Facebook, auparavant nous ne les utilisions pas. Maintenant nous allons les utiliser pour mieux comprendre comment cibler ces personnes », assume très clairement Andrew Bosworth, vice-président de Facebook en charge des publicités et de la plateforme commerciale.



Ce dispositif permettra à Facebook de repérer les habitudes des internautes en insérant des bouts de codes dans les cookies et dans les boutons ou autres contenus « embeddés », qui permettront d'identifier l'internaute, soit directement en tant que membre de Facebook, soit par un numéro unique qui lui sera attribué. Si vous visitez régulièrement un site de cuisine, Facebook affichera des publicités pour une cocotte-minute ou une friteuse sur les autres sites que vous fréquentez, en rémunérant le site qui les affiche.

QUELLE LÉGALITÉ EN EUROPE ?
Ce changement de politique de Facebook va certainement mécontenter une partie de la communauté des internautes, y compris chez les membres qui pourront continuer à être suivis même lorsqu'ils sont déconnectés du réseau social. Elle pourrait surtout déclencher les foudres des autorités si le système est déployé en Europe.
Lorsque la justice belge avait condamné Facebook à ne plus tracer les Belges non-membres de Facebook, le réseau social s'était fait fort de crier à l'injustice, en prétendant que son cookie (le DATR) avait pour seul intérêt de lutter contre le spam. « Nous utilisons le cookie datr depuis plus de 5 ans pour sécuriser Facebook pour 1,5 milliard de personnes à travers le monde », s'était agacé le réseau social. Or six mois plus tard, Facebook prouve que les autorités avaient raison de s'inquiéter.
En France aussi, la Cnil a demandé à Facebook de ne plus tracer les internautes qui ne sont pas inscrits et connectés sur le réseau social. Avec d'autres homologues, elle avait estimé que Facebook devait « se conformer à ce jugement (belge) sur tout le territoire de l'Union européenne ».
Selon la législation européenne, il est illégal de réaliser un traitement de données personnelles à des fins commerciales, sans le consentement explicite de la personne. Or si ce consentement peut être donné à l'inscription par Facebook, il ne peut certainement pas l'être par les non-membres… [Lire la suite]

Article de Omar Belkaab

Réagissez à cet article

Source : *Facebook vous traquera sur le Web même si vous n'êtes pas membre – Business – Numerama*

Sensibilisation aux arnaques aux petites annonces

Sensibilisation aux arnaques aux petites annonces

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Les six choses à faire pour éviter 95% des attaques informatiques

Les six choses à faire pour éviter 95% des attaques informatiques

La cybersécurité est essentielle, d'accord, mais par où commencer ? Pour vous aider à faire le premier pas, nous avons identifier 6 principes clés qui, lorsqu'ils sont suivis, peuvent éviter la grande majorité des attaques.

1/ FAIRE DE LA SÉCURITÉ UN PROCESS (CE N'EST PAS UN PRODUIT)

« Je dois protéger mon entreprise ? Certes. Quel produit faut-il que j'achète ? » La réflexion peut sembler naturelle. Après tout, autant faire appel à des professionnels. Le problème, c'est qu'on ne sécurise pas son entreprise en signant un chèque. La cybersécurité est avant tout une façon de penser, et passe par une organisation, par la mise en place de règles et méthodes. Elle implique de connaître son système d'information sur le bout des doigts pour en cartographier la surface d'attaque, de savoir tout ce qui est connecté (et ce qui ne doit pas l'être). Elle implique aussi de déterminer quels sont les services et les données qui sont réellement cruciaux au fonctionnement de la structure pour s'assurer que l'on concentre ses forces là où elles doivent l'être, sans s'évertuer à défendre plus que nécessaire des ressources non critiques. *« La sécurité est une composante au service du coeur de métier,* explique Eric Filiol, directeur du laboratoire de virologie et de #cryptologie opérationnelles de l'école d'ingénieurs ESIEA. *Il faut comprendre son métier et ce qui est critique. »* La stratégie doit être sensée pour que les ressources engagées (financières, humaines, temporelles) soient utilisées au mieux.

2/ PATCHER, PATCHER, PATCHER

Les révélations sur les méthodes de la NSA ou les gros titres sur les attaques contre des opérateurs d'importance vitale qui s'étalent sur des mois voire des années peuvent laisser penser que les hackers exploitent systématiquement des failles complexes et jamais référencées (appelées « zero days ») pour s'infiltrer dans un SI. Rien n'est moins vrai. Ces zero days ne sont utilisés qu'extrêmement rarement et seulement pour les cibles les plus importantes. La très grande majorité des attaques ciblent au contraire des failles bien connues et pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années. C'est pourquoi il est capital de faire systématiquement ces mises à jour (aussi bien pour le système d'exploitation que les frameworks ou les applications), et de concevoir son SI autour de cette nécessité. *« Il faut savoir que les criminels font du reserve engineering sur les patchs dès leur sortie pour exploiter les failles qu'ils corrigent. Auparavant cela leur prenait des mois, aujourd'hui ce ne sont plus que des heures,* détaille Thomas Tschersich, director of IT security chez Deutsche Telekom.*Et ils automatisent ensuite le processus pour toucher de très nombreuses cibles. »* Et ce besoin reste le même dans le cas d'un environnement de production industriel qui se doit d'être opérationnel 365 jours par an. La perception selon laquelle les environnements industriels sont fondamentalement différents des environnements de bureau est fausse et contribue à renforcer leur vulnérabilité.

3/ NE PAS SE CROIRE NON CONCERNÉ

Si les réseaux industriels sont de plus en plus visés par des attaques informatiques, c'est parce qu'ils y sont particulièrement vulnérables. La faute à l'évolution dramatique de la connectivité à Internet au cours des 20 dernières années. Lors de leur conception, il était assumé que ces systèmes ne couraient pas de risques car ils n'étaient pas visibles. Quand bien même ce fut jamais vrai, ce n'est définitivement plus le cas. Des services gratuits comme shodan.io permettent depuis des années de chercher parmi des centaines de milliers de systèmes ouverts, connectés à Internet sans aucune protection. Cela va de simples caméras de surveillance (résidentielles ou industrielles) jusqu'aux ICS qui supervisent le parc machine, que les opérateurs laissent sans protection car ils veulent pouvoir en prendre facilement le contrôle à distance. *« Il y a beaucoup de négligence et de mauvaises pratiques,* assène Frédéric Planchon, PDG de FPC Ingénierie. *Cela laisse des portes ouvertes à des malwares qui ne sont normalement pas si nocifs. »* Peu importe la taille de votre installation ou la nature de votre activité, si vous êtes vulnérables, vous serez tôt ou tard attaqué. Et ce même lorsqu'il n'y a rien à en obtenir, car de nombreux hackers agissent simplement « pour le sport ».

4/ PROTÉGER SES DONNÉES

La meilleure façon de garantir la sécurité de ses données, que ce soit contre le vol ou contre des attaques de type ransomwares, c'est de prendre les mesures adéquates en amont. Cela passe par deux axes clés : le chiffrement et la sauvegarde. Le chiffrement garantit que seuls les individus autorisés peuvent accéder aux données, même si le canal de communication ou le support de stockage est compromis. Ainsi, même en cas de vol, les dégâts restent minimaux. De son côté, la sauvegarde évite la perte de données, qu'elle soit dûe à un accident ou à un acte de malveillance. Une politique de sauvegarde rigoureuse et régulière peut faire la différence entre « plus de peur que de mal » et « la clé sous la porte ».

5/ FORMER SES TROUPES

Une vaste majorité d'attaques ont un point commun : l'erreur humaine. Un collaborateur qui ouvre le mauvais email ou clique sur le mauvais lien. Un autre qui perd son appareil ou sa clé USB. Un troisième qui laisse traîner ses identifiants de connexion (ex. post-it sur l'écran) ou les communique par erreur/inattention… La sécurité n'est pas innée, elle s'enseigne. Il est impératif de former les équipes aux bonnes pratiques à adopter et de les sensibiliser aux conséquences que la négligence peut avoir. Les rendre personnellement responsables de la protection de leurs données et appareils au travers de mesures simples peut suffire à largement diminuer les accidents.

6/ SÉCURISER AUSSI LES ACCÈS PHYSIQUES

Une #attaque informatique n'est pas forcément menée depuis l'autre bout du monde. Il faut donc s'assurer en premier lieu que le périmètre de l'entreprise est sécurisé pour limiter les accès non autorisés en interne. Car le « social engineering », qui consiste à obtenir accès à un système en trompant son interlocuteur, est au coeur de nombreuses attaques. Il suffit parfois de mettre un uniforme de réparateur, de prendre une boîte à outils et de demander poliment l'accès à un local technique pour qu'on vous ouvre. Ou de mettre un costume et de se tenir devant une porte les bras chargés de documents. *« Nous appelons ça les attaques 'femme de ménage', et cela permet de prendre le contrôle d'un serveur en 5 secondes, »* explique Eric Filiol. Autre exemple, lorsque le réseau Wi-Fi interne d'une usine, non protégé car l'accès au bâtiment est restreint, peut aussi être capté depuis le parking… Les cas de figure sont nombreux et leur exploitation bien documentée. Ces éléments doivent donc systématiquement être pris en compte.

Article de Julien BERGOUNHOUX

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : Les six choses à faire pour éviter 95% des attaques*

La France adopte son arsenal anti-hackers

La France adopte son arsenal anti-hackers

La loi de programmation militaire a placé le secteur financier en première ligne des 12 opérateurs d'importance vitale, soumis à de nouvelles règles de sécurité.

C'est un test d'envergure pour les banques françaises. L'Etat a placé le secteur financier en première ligne des douze secteurs d'importance vitale qui devront adopter les nouvelles règles en matière de cybersécurité, arrêtées par la loi de programmation militaire de 2013.
Ce choix n'est pas dû à une recrudescence des cyber-risque dans le secteur, assure la puissance publique – en l'occurrence, c'est Bercy qui a fait l'objet de l'attaque la plus grave ayant jamais visé une administration en France en 2011. *« Le niveau de sécurité du secteur financier est jugé satisfaisant,* indique Yves Jussot, coordinateur sectoriel à l'Agence nationale de la sécurité des systèmes d'information (Anssi). *Cependant la menace évolue vite et de façon continue, en particulier avec le développement du numérique. »*
Considérées comme *« pionnières »* dans l'identification des menaces informatiques et de lutte contre les cyberfraudes, les banques fixeront la barre des nouvelles exigences en matière de protection, qui s'appliqueront aux autres secteurs vitaux comme l'énergie, aux transports, en passant par la santé. Définies par un arrêté d'ici au 1er juillet, celles-ci promettent d'être élevées. Des règles renforcées en matière d'administration des systèmes sont par exemple définies pour cantonner davantage les flux de données.
Surtout, l'Etat voit son pouvoir renforcé en matière de contrôle. L'Anssi, rattachée au secrétaire général de la Défense et de la sécurité nationale, pourra mener des audits réguliers, et des amendes pourront être délivrées pour infraction à la sécurité informatique ou non-application de la réglementation. Les incidents qui pouvaient jusqu'à présent ne pas être déclarés devront être notifiés et, en cas d'attaque majeure, l'Anssi pourra prendre la main sur les systèmes. L'Etat a pris soin de travailler de concert avec les banques, au travers du Forum des compétences, qui regroupe les experts informatiques des banques et des assurances. Restera la question des moyens. *« La course à la transformation digitale entre banques impose d'aller vite et d'y allouer des moyens. La mise à niveau des systèmes informatiques peut ne pas suivre et ne pas être prioritaire »*, note un expert en cybersécurité…[Suite de l'article original de Anne RIF et Véronique CHOCRON]

Réagissez à cet article

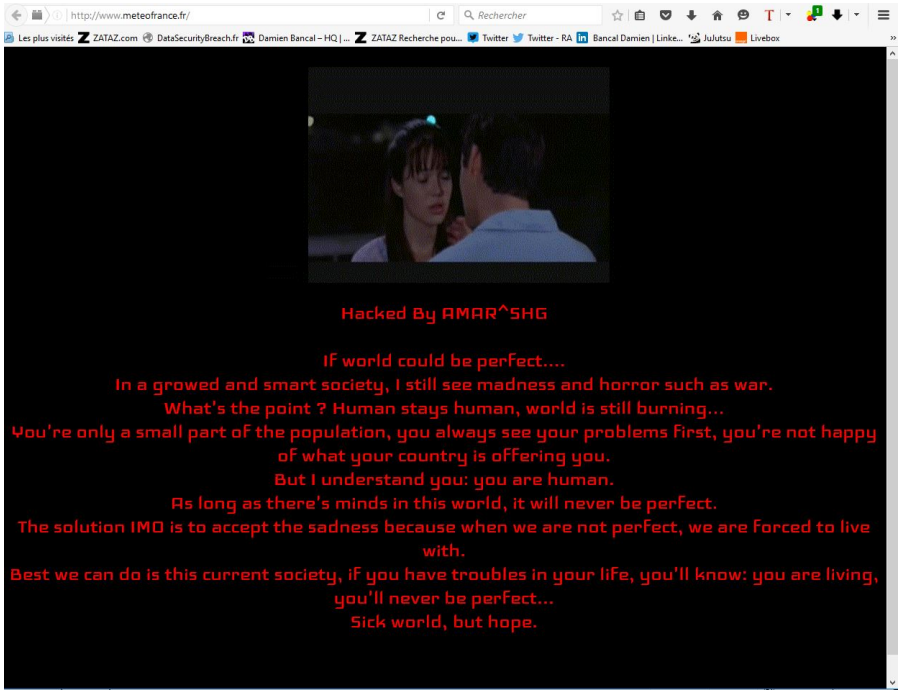
Source : *La France adopte son arsenal anti-hackers, Banque – Assurances*

Le site Internet de Météo

France piraté

	**Le site Internet de Météo France piraté**

Après les sites de Canal +, un nouveau message d'espoir mis en ligne par un pirate informatique sur l'ensemble des sites Internet de Météo France. Un détournement de DNS radical.



Il se nomme Amar^SHG. Ce jeune pirate informatique (Il serait un Albanais) est dans la mouvance des hacktivistes politiques qui, par le biais de la modification de site Internet (defacement, barbouillage), trouvent un moyen de faire passer des messages. Amar^SHG a fait la pluie et le beau temps sur les sites de Météo France via un détournement de DNS radical.
Lundi soir, le pirate a mis la main sur un moyen informatique qui lui a donné l'occasion de détourner l'ensemble des noms de domaines de Météo France. Comme il a pu me l'indiquer sur Twitter, les domaines .fr, .mobi, . Paris, … ont été impactés.

Détournement de DNS

*Les visiteurs accédaient, ce lundi soir (vers 22h30), à une page noire et rouge, portée par la musique « Wonderful life » de Katie Melua. Côté message, le cyber manifestant souhaitait viser ceux qui « **se plaignent pour leurs propres problèmes** ». AMAR ^ SHG parle d'espoir, d'un monde qui n'est pas parfait « **Il faut vivre avec, avec espoir** »… [Lire la suite]*

Article de Damien BANCAL

Réagissez à cet article

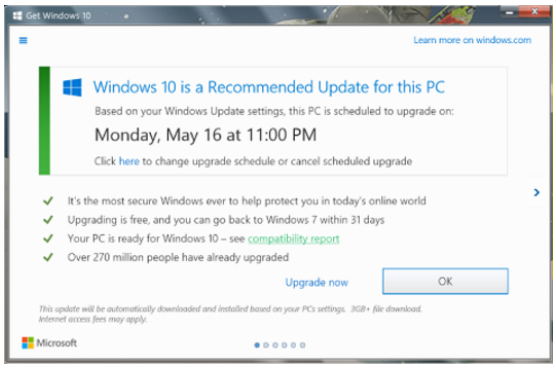
Source : *ZATAZ Détournement de DNS – Un pirate passe par Météo France – ZATAZ*

Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?

	**Vous ne voulez pas installer Windows 10, comment Microsoft vous-y oblige ?**

« Mon ordinateur m'a demandé si je voulais passer à Windows 10. J'ai cliqué sur le bouton X pour fermer la fenêtre car je ne voulais pas, et une heure après, Windows 10 est en train de s'installer. » Ce type de commentaire s'est multiplié sur les réseaux sociaux ces derniers jours. De nombreux internautes se sont plaints de voir leurs ordinateurs installer automatiquement la mise à jour vers Windows 10, alors qu'ils pensaient l'avoir refusée. Tous avaient cliqué sur la croix rouge permettant de fermer la fenêtre proposant ce téléchargement.

En général, ce bouton sert à fermer une pop-up sans avoir à donner de réponse à sa proposition. Mais depuis quelques jours, le fait de cliquer dessus a l'effet inverse : cela installe Windows 10. Une « *tromperie* », selon de nombreux utilisateurs du célèbre système d'exploitation de Microsoft.



Si l'utilisateur ferme cette fenêtre, alors Windows 10 s'installera automatiquement sur son ordinateur. Microsoft

L'entreprise, de son côté, assume et explique sur son site le fonctionnement de cette fenêtre. En fait, celle-ci fait plus que proposer une mise à jour : elle indique que la mise à jour est déjà programmée et précise la date. L'utilisateur est alors invité à cliquer sur le gros bouton « OK ». Il a aussi la possibilité, inscrite en petits caractères, de modifier la date ou d'annuler la programmation de mise à jour. Mais s'il décide simplement de fermer la fenêtre, alors Microsoft part du principe que l'utilisateur accepte la mise à jour, comme s'il avait cliqué sur « OK ».

Les utilisateurs forcés. Normal ?

Cette manœuvre de Microsoft est considérée par beaucoup comme une manière de leur forcer la main, alors que l'entreprise a annoncé sa volonté d'équiper un milliard de machines de Windows 10 en trois ans. D'autant qu'une date clé se rapproche dangereusement : à partir du 30 juillet, la mise à jour, jusqu'ici gratuite pour les utilisateurs de Windows 7 et 8, deviendra payante. Il sera alors bien plus compliqué de convaincre les sceptiques de s'y convertir.

Source : *L'étrange méthode de Microsoft pour imposer le téléchargement de Windows 10*

Réagissez à cet article

Google Chrome v51 corrige 42 failles de sécurité

	Google Chrome v51 corrige 42 failles de sécurité

Google vient de publier une nouvelle mouture stable de son navigateur Chrome, en version 51.

Chrome 51 est disponible au téléchargement pour Windows, OS X et Linux. Cette mouture intègre les interfaces de programmation Credential Management. Avec ces dernières, les sites Internet peuvent directement communiquer avec le gestionnaire de mots de passe mais aussi avec Google Smartlock ou les autorisations liées à un compte Facebook. Le processus de connexion s'en trouve simplifié, notamment sur smartphones.

L'équipe a en outre procédé à des optimisations du chargement des pages, notamment en ne récupérant pas les éléments non visibles à l'écran. Il en résulterait une meilleure gestion de la batterie avec un navigateur 30% moins gourmand.

Coté sécurité, les ingénieurs ont comblé 42 failles de sécurité en reversant au total 65 000 dollars aux experts ayant partagé leurs recherches. Retrouvez davantage d'informations sur cette page.

- Téléchargez Google Chrome 51 pour Windows
- Téléchargez Google Chrome 51 pour OS X
- Téléchargez Google Chrome 51 pour Linux

Article de Guillaume Belfiore

Réagissez à cet article

Source : *Chrome 51 : Google corrige 42 failles de sécurité*

Blogueurs, attention aux promesses des Publicités …

Blogueurs, attention aux promesses des Publicités …

Publicité malveillante – Elles se nomment Elena, Yoana, Elise… elles sont toutes éditrices indépendantes et recherchent des espaces publicitaires sur votre blog. Attention, piège à la Publicité malveillante pour casinos.

Des courriers et autres sollicitations commerciales sont légions dans le monde des blogueurs. Achats d'espaces publicitaires, d'articles ou de liens sponsorisés sont des demandes constantes dès qu'un site fonctionne et attire les internautes. Je vais cependant vous mettre en garde contre des promesses venues du ciel 2.0. « ***Bonjour, je me présente, je m'appelle Yoana et je suis une éditrice indépendante. Je suis intéressée par l'achat d'un espace publicitaire sur votre site http://www.zataz.com . Je souhaite acheter la publication pour un de nos articles, qui contiendra un ou plusieurs liens internes.***«
L'espace entre l'url est important à prendre en compte, je vais vous expliquer pourquoi. Les espaces situés entre le début et la fin de l'adresse Internet sont générés par un logiciel qui automatise les courriels. Bilan, Elena, Yoana, Elise… ne savent pas qui vous êtes. Elles (ou ils), il s'agit aussi très certainement de la même personne officiant d'Italie et d'Israel, espèrent une réponse de votre part. Ne mordez pas à son hameçon. « ***Je peux payer via Paypal sous 24/48h*** » stipulent les interlocutrices.

Publicité malveillante
Mais que proposent donc ces « dames » ? Tout simplement… des articles et des liens renvoyant sur de faux blogs dédiés aux Casinos. L'idée est simple, plus il y aura de liens vers ces faux blogs, plus ils seront référencés. Plus ils seront référencés, plus les internautes auront envie de cliquer sur les autres adresses Internet proposées par ces faux blogs. Des urls qui dirigent tous vers des casinos illicites, interdits en France.
Elena, Yoana, Elise… ne vendent pas les liens directs vers ces casinos, mais pièges les blogueurs qui seraient tentés. Bref, ne sombrez pas aux sons de ses Calliopes car le prochain son que vous pourriez entendre risque d'être celui d'une convocation par le service central des courses et jeux de la Direction Centrale de la Police Judiciaire.

Fausse publicité mais vrai piège
*Les sommes varient pour cette publicité malveillante. Selon son emplacement de l'article, sa durée de mise en ligne. J'ai pu constater des propositions pécuniaires, qui m'étaient faites, pouvant aller de 200 à 1.500€. Autant dire que pour un blogueur, la manne financière est loin d'être négligeable. D'autant plus que Elena, Yoana, Elise… fournissent le texte, les photos, les liens. Malines, quelques jours après la diffusion de l'article en question, elles demandent une modification dans les urls, les ancres dédiées à certains mots du texte. Une manipulation permettant un référencement plus « musclé » dans les moteurs de recherche. « **C'était de l'argent facile**, me confiait il y a quelques temps Clément [prénom modifié], un blogueur. **Mon post était en ligne à 16h. J'ai reçu mon paiement à 20h. J'ai modifié l'article et les liens le lendemain. Une semaine plus tard je recevais un avertissement de l'ARJEL... et une convocation devant les policiers.***

L'ARJEL veille
*Ce qu'oublient de dire les mystérieuses sirènes, les sites qu'elles souhaitent mettre en avant dans la publicité malveillante commercialisée ne sont pas reconnues par l'ARJEL, l´Autorité de Régulation des Jeux en Ligne veille. En France, depuis le 12 mai 2010, l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ne permet plus aux blogueurs d'afficher n'importe quel site dédié aux casinos. Une loi qui s'applique à toute personne proposant, en France, une offre de jeux d'argent et de hasard en ligne. Bref, diffuser un article, des liens, vers des casinos et autres portails dédiés aux jeux de hasard non titulaires de l'agrément ARJEL, peut entraîner de sérieux ennuis aux blogueurs ne respectant pas la loi : « **Quiconque fait de la publicité, par quelque moyen que ce soit, en faveur d'un site de paris ou de jeux d'argent et de hasard non autorisé en vertu d'un droit exclusif ou de l'agrément prévu à l'article 21 est puni d'une amende de 100 000 €. Le tribunal peut porter le montant de l'amende au quadruple du montant des dépenses publicitaires consacrées à l'activité illégale. Ces peines sont également encourues par quiconque a, par quelque moyen que ce soit, diffusé au public, aux fins de promouvoir des sites de jeux en ligne ne disposant pas de l'agrément prévu à l'article 21, les cotes et rapports proposés par ces sites non autorisés.**«
Elena, Yoana, Elise… ne risquent rien, elles sont à l'étranger (Italie, Israël…). En France, 3 ans de prison et 90.000€ d'amende pour « **Quiconque aura offert ou proposé au public une offre en ligne de paris ou de jeux d'argent et de hasard sans être titulaire de l'agrément mentionné à l'article 21 ou d'un droit exclusif**« . Des peines portées à sept ans d'emprisonnement et à 200 000 € d'amende lorsque l'infraction est commise en bande organisée… [Lire la suite]*

Merci à Damien BANCAL l'auteur de cet article pour toutes ces précieuses informations.

Réagissez à cet article

Source : *ZATAZ Publicité malveillante : Piége à blogueur – ZATAZ*

Augmentation de 30% des demande de rançon informatique en 3 mois

	**Augmentation de 30% des demande de rançon informatique en 3 mois**

Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

Un nombre qui va sans cesse croissant.
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

Une autre raison explique la croissance des attaques de ransomware : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybersécurité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*

Un gros botnet détourne des requêtes de recherche

Un gros botnet détourne des requêtes de recherche

Depuis septembre 2014, un botnet a pu compter près d'un million de zombies pour faire gonfler des revenus publicitaires de cybercriminels.

Actif depuis mi-septembre 2014, un botnet est parvenu à prendre le contrôle de près d'un million d'ordinateurs dans le monde. L'agent infectieux est un malware intégré dans un fichier d'installation modifié de type MSI pour Windows.
Botnet-Redirector.Paco-carte-BitdefenderCes fichiers corrompus sont associés à des programmes tels que WinRAR, YouTube Downloader, Connectify, Start8 et KMSPico. Après installation sur la machine prise pour cible, le nuisible dénommé Redirector.Paco s'appuie sur un fichier PAC (Proxy auto-config) pour rediriger des requêtes de recherches sur Google, Bing ou Yahoo.
Au gré de quelques modifications dans la base de registre, le trafic sera redirigé vers des publicités contextuelles permettant de générer des revenus ici frauduleux grâce au programme AdSense pour les recherches de Google.
Les opérateurs du botnet détournent les recherches vers un autre moteur de recherche personnalisé spécifiquement conçu qui affiche ses propres résultats, et détournent par la même occasion des revenus publicitaires… [Lire la suite]
Article de Jérôme GARAY

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Un gros botnet détourne des requêtes de recherche*