Plus de 2 millions d’internautes victimes de phishing en 2015 | Le Net Expert Informatique

Plus de 2 millions d’internautes victimes de phishing en 2015

Pour renforcer la lutte contre le phishing, le Ministère de l'Intérieur a signé le 5 novembre, une convention de partenariat avec l'association Phishing Initiative, soutenue par Lexsi et Microsoft France. Cet accord vise à mutualiser les informations entre sa propre plateforme, PHAROS, et celle de Phishing Initiative qui a identifié de son côté plus de 150 000 adresses uniques de sites frauduleux visant la France depuis sa création en 2011.

Une convention commune pour renforcer la lutte contre le Phishing

En signant la convention de lutte anti-phishing, Catherine Chambon, sous-directeur de la lutte contre la cybercriminalité et Jérôme Robert, président de Phishing Initiative souhaitent renforcer la sensibilisation des internautes aux risques liés à cette malveillance majeure. « La complémentarité de nos actions rend évidente la nécessité d'un rapprochement et d'une coordination entre nos deux organisations », explique Jérôme Robert. « PHAROS et Phishing Initiative opèrent en effet tous deux des plateformes de signalement à destination du grand public. Il est par conséquent possible d'instaurer des conditions de partage de l'information de manière à optimiser d'une part, la recherche de données et d'autre part, la protection de l'internaute. »

Suite à la signature de cette convention et à l'engagement des parties prenantes, le Ministère de l'Intérieur et Phishing Initiative travailleront également à la rédaction d'un rapport commun et à l'élaboration d'un suivi des tendances au service de la protection des internautes.

Phishing Initiative et PHAROS : l'union des expertises

Elaborée et construite sous l'impulsion de Madame Catherine Chambon, Madame Valérie Maldonado, chef de l'OCLCTIC, Messieurs Jérôme Robert, Directeur Marketing, Vincent Hinderer, Expert Cybersécurité chez Lexsi, et Bernard Ourghanlian, directeur technique et sécurité de Microsoft, la convention a pour objectif d'augmenter le nombre d'URLs traitées et analysées. Avec respectivement 60 000 et 30 000 URLs traitées depuis début 2015, Phishing Initiative et PHAROS unissent leurs forces pour protéger les internautes et rendre le web plus sûr. « L'association de nos dispositifs de lutte contre la fraude sur Internet représente une avancée majeure dans la protection des particuliers comme des entreprises » précise Bernard Ourghanlian de Microsoft France. « Face à la malveillance et à la fraude organisée, chaque citoyen et chaque entreprise est acteur d'un Internet plus sûr au bénéfice de tous. » La Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) a développé deux dispositifs destinés aux particuliers : la Plateforme d'Harmonisation d'Analyse et de Recoupement et d'Orientation des Signalements (PHAROS), lancée en janvier 2009, et Info-Escroqueries, une hotline téléphonique dédiée aux arnaques. PHAROS a notamment pour mission de recueillir et traiter les signalements de contenus et de comportements illicites détectés sur Internet.

Phishing Initiative, un programme de lutte européen

Cofinancé par le Programme de Prévention et de Lutte contre le Crime de l'Union Européenne, Phishing Initiative offre à tout internaute la possibilité de lutter contre les attaques d'hameçonnage en signalant de manière simple les liens lui paraissant suspects en un clic sur www.phishing-initiative.fr .

Chaque signalement fait l'objet d'une analyse par les experts Lexsi qui, s'il se révèle frauduleux, est transmis aux partenaires de Phishing Initiative, notamment Microsoft. Ces derniers enrichissent alors leurs listes noires, de sorte que le lien frauduleux est bloqué par les principaux navigateurs Web (Edge, Internet Explorer, Chrome, Firefox et Safari).

Phishing Initiative en chiffres

A ce jour, plus de 400 000 adresses suspectes ont été signalées dans le cadre de la Phishing Initiative, dont plus de 300 000 uniques. Depuis le début de l'année 2015, 110 000 signalements ont déjà été transmis, représentant plus de 60 000 nouvelles adresses uniques. Parmi elles, plus de 35 000 URLs uniques ont été confirmées comme faisant partie d'une campagne de phishing, soit près de 120 adresses distinctes par jour. A noter que le temps médian nécessaire aux analystes pour catégoriser un nouveau cas signalé est de moins de 20 minutes. Microsoft rafraîchit sa liste noire toutes les 20 minutes au sein d'Internet Explorer et Edge, ce qui protège en moyenne les internautes en moins de 40 minutes suite à un signalement sur www.phishing-initiative.fr.

Des milliers d'internautes contribuent anonymement à ce projet chaque année et plusieurs centaines d'individus ont créé depuis la rentrée un compte personnel sur le site Phishing Initiative. Il leur permet désormais de signaler des URLs suspectes plus simplement et d'accéder à des informations, statistiques et services additionnels, relatifs notamment aux signalements effectués par leurs soins. Ces internautes peuvent, par exemple, suivre l'état du site en temps réel et demander à être prévenus du caractère frauduleux ou non d'une adresse ainsi soumise, mais surtout participer à la lutte anti-phishing et empêcher que d'autres internautes soient victimes de ce fléau.

A propos de Phishing Initiative

Créé sous l'impulsion conjointe du cabinet Lexsi, de Microsoft et de PayPal Europe en 2011, Phishing Initiative, association à but non lucratif, offre à tout internaute la possibilité de vérifier un site suspect et lutter contre les attaques de phishing. En signalant l'adresse d'un site suspecté d'héberger un cas de phishing francophone, vous contribuez à diminuer l'impact de cette cybercriminalité en évitant que d'autres internautes soient piégées par ces attaques. Chaque adresse différente fera en effet l'objet d'une vérification humaine et si confirmée comme frauduleuse d'un envoi pour blocage dans les listes noires des principaux navigateurs Plus d'informations sur : https://phishing-initiative.fr

---

Source : http://www.globalsecuritymag.fr/Plus-de-2-millions-d-internautes,20151105,57293.html

Nouvelle réglementation Européenne sur la protection des données personnelles | Le Net Expert Informatique

Comment être prêt à répondre aux exigences de la nouvelle réglementation européenne sur la protection des données personnelles ?

Les apports du projet de règlement UE sur la protection des données personnelles en matière de gestion de crise sont nombreux et les entreprises peuvent d'ores et déjà se préparer à plusieurs niveaux.
Vous êtes le dirigeant d'une entreprise de la grande distribution, vôtre RSSI vous informe que malgré les mesures de sécurité mises en œuvre, l'entreprise est victime d'un vol massif de données clients. Vous avez conscience que c'est impactant pour votre entreprise mais heureusement les législations européennes et françaises, en matière de violation des données à caractère personnel, ne visent que les fournisseurs de communication électronique. Vous êtes épargnés d'un point de vue réglementaire… Certes, mais plus pour longtemps.
Le projet de règlement sur la protection des données destiné à remplacer la Directive 95/46/CE doit actuellement repasser devant la Commission et son adoption ne saurait tarder. Le règlement vise désormais toutes les organisations traitant des données à caractère personnel et en lien avec l'UE (territorial, résidents UE…).
Celui-ci impose notamment, que si les conséquences de la compromission de données, constituent un risque élevé pour les droits et libertés des personnes physiques concernées, l'organisation doit les informer au plus vite. Elle doit aussi en informer les autorités compétentes en matière de protection des données à caractère personnel. Pour ce faire plusieurs actions doivent être réalisées en étroite collaboration avec le soutien du Data Privacy Officer (DPO) de l'organisation.

La qualification de l'incident
L'objectif est de déterminer si le risque est élevé pour les personnes concernées. Pour ce faire il convient en premier lieu de répondre à deux questions :
• Les données volées rendent-elles les personnes concernées identifiables ?
• Les personnes concernées peuvent-elles connaître des conséquences significatives voire irrémédiables (discrimination, vol/usurpation d'identité, perte financière, atteinte à la réputation) ?
A l'issue de cette première phase, si le risque est élevé pour les personnes concernées (données identifiables et conséquences majeures), il faudra procéder à la notification de l'autorité compétente et des personnes concernées.
L'organisation ne sera toutefois pas tenue de notifier les personnes concernées par la violation si :
• Le responsable du traitement a mis en œuvre des mesures de protection technologiques appropriées rendant les données incompréhensibles à toutes personnes non autorisées à y avoir accès (ex : chiffrement) ;
• Ou si la notification risque d'entrainer des mesures disproportionnées eu égard notamment au nombre de cas concernés ;
• Ou si la notification risque de porter atteinte à un intérêt public important.

La notification de l'incident
Pour la notification à l'autorité en charge de la protection des données, la CNIL en France, l'organisation victime de l'attaque dispose d'un délai de 72 heures. Cette notification devra notamment comporter les éléments suivants :
- La nature de la violation
- Le nombre approximatif de personnes et des enregistrements concernés
- La description des conséquences probables de la violation
- La description des mesures prises

Pour la notification aux personnes concernées, celles-ci doivent aussi être averties sans retard injustifié. Trois éléments principaux doivent être communiqués :
- La nature de la violation des données à caractère personnel
- Les mesures prises ou proposées pour remédier à la violation
- Les recommandations afin d'atténuer les effets négatifs de la violation

Durant toute la gestion de la crise ainsi que durant la sortie de crise, le responsable du traitement doit alimenter puis conserver une trace documentaire de la violation des données à caractère personnel en indiquant son contexte, ses effets et les mesures prises pour y remédier. Ce document aura valeur juridique et pourra être opposable.

En parallèle à ces actions, la gestion de la crise comporte également une gestion technique de l'attaque, une campagne de communication de crise afin de sauvegarder la réputation, ainsi qu'une démarche judiciaire et assurantielle notamment si l'organisation a adopté une cyber-assurance.

Le rôle du DPO
En temps de crise, le Data Privacy Officer (DPO) pourra veiller à ce que les mesures adaptées et la notification à l'autorité de contrôle et aux personnes concernées soient réalisées. Il pourra par ailleurs effectuer toutes les procédures requises auprès de la CNIL ainsi que suivre le dossier. En outre, les relations entre le CIL et la CNIL déjà établies en amont de la crise permettent d'alléger les procédures.

L'existence du CIL dans les entreprises peut être ainsi un élément favorisant l'adoption de réponses adaptées en temps de crise et pouvant réduire le montant de la sanction administrative dans le cas où la responsabilité du responsable de traitement ou du sous-traitant est démontrée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.itpro.fr/a/nouvelle-reglementation-ue-sur-protection-donnees-personnelles/
Par Francesca Serio – Consultante spécialisée en Gestion de crise et Continuité d'Activité – Provadys

Une attaque DDos a duré quasiment deux semaines | Le Net Expert Informatique

Une attaque DDos a.duré quasiment deux semaines

Même si la plupart des attaques DDos ne durent guère plus longtemps que 24 heures, le nombre de ce genre d'attaques de longue durée croît nettement. La plus longue au troisième trimestre a ainsi duré pas moins de 320 heures.

Voilà ce que communique l'entreprise de sécurité Kaspersky Lab dans son rapport trimestriel DDos à propos des trois derniers mois écoulés.
Les attaques DDos se manifestent surtout dans un nombre limité de pays: 91 pour cent des systèmes agressés se trouvent dans 10 pays. Les pays les plus souvent touchés par des attaques DDos sont la Chine, les Etats-Unis et la Corée du Sud. Ces attaques proviennent principalement du même pays où se trouve la cible. La Chine, les Etats-Unis et la Corée du Sud forment donc le trio de tête au classement des attaques lancées. Il s'agit là d'une pratique complètement différente de celle d'autres cyber-attaques, comme les vols de données. Dans ce dernier cas, les attaques émanent de très nombreux pays et certainement pas aussi souvent du pays où se trouve la victime.

La plupart des attaques visent à perturber les activités de la cible, mais le nombre d'attaques de longue durée pouvant entraîner la faillite de la victime, est en augmentation. Elles vont aussi parfois de pair avec des demandes de rançon.

Source :
http://datanews.levif.be/ict/actualite/une-attaque-ddos-a-dure-quasiment-deux-semaines/article-normal-432941.html

---

Les cybercriminels ciblent le paiement mobile | Le Net Expert Informatique

Les cybercriminels ciblent le paiement mobile

Il y a quelques semaines, nous avons traité, du e-Commerce. C'est un registre si vaste et varié que nous choisissons, cette semaine aussi, d'y consacrer quelques réflexions, histoire de susciter chez nos lecteurs quelque intérêt pour une problématique appelée à devenir incontournable. Malgré l'essor du e-Commerce, les modes de paiement mobile peinent à décoller dans de nombreux pays développés. En cause, le conservatisme et la peur de l'inconnu.

L'inconnu, selon de nombreux spécialistes, c'est la cybercriminalité qui donne des sueurs froides aux fournisseurs de solutions. Dans un excellent article au titre très évocateur publié récemment, « Le paiement mobile, nouvel eldorado des escrocs », Benoît Huet de la rédaction de lemondeinformatique.fr nous amène faire une immersion dans les méandres d'un secteur pourtant promu à un bel essor. Les résultats du paiement mobile, il faut bien le concéder, sont assez modestes.

Dans son article, Benoît Huet écrit : « Selon l'institut d'études GFK, qui a mené une enquête dans 17 pays auprès de 17 000 consommateurs, seulement 5% des transactions mondiales sont réellement effectuées avec un appareil mobile ». Presqu'un désert ! Dans un pays comme la France, notre référence à tous, « les transactions via le paiement mobile sont souvent estimées à moins de 1% par les différents cabinets d'études ».

Et pourtant, précise l'article de notre confrère, ce n'est pas faute d'avoir essayé. De nombreuses applications permettant de payer avec un smartphone existent : le service PayByPhone pour payer le stationnement et le parking à Boulogne, Nice et dans d'autres villes, ainsi que des commerces qui ont mis en place un terminal NFC (Paiement Sans Contact) pour régler diverses courses.

La première raison, et nous l'évoquions plus haut, le conservatisme culturel : « Si le paiement mobile a encore du mal à percer en France, c'est déjà parce que les moyens de paiement sont très liés à la culture des pays. La France est par exemple un pays fortement tourné vers l'usage de la carte bleue Visa alors qu'en Belgique, c'est la Mastercard qui règne, quant à l'Allemagne, le paiement en liquide est encore très courant ».

Sans vouloir défier la technologie, « Les français ne sont pas encore prêts à payer avec leur mobile, c'est à la fois un problème culturel et un manque de confiance dans les technologies, ils préfèrent donc payer en caisse avec une carte, de l'espèce ou en chèque ».

La seconde raison qui plombe l'essor du paiement mobile vient d'être lâchée : le manque de confiance dans les technologies. Par instinct de survie, la majorité des français boudent le paiement mobile, moins sécurisé à leurs yeux, de peur d'être victime des cyberescrocs qui ont plus d'un tour dans leur sac.

Sans l'affirmer, les conclusions de l'étude donnent raison aux cyber-sceptiques qui semblent se perdre dans la jungle des technologies de communication sans contact comme les balises (Beacons utilisant le Bluetooth) ; le RFID ; le NFC (qu'utilise Apple, entre autres, avec Apple Pay et Google avec Google Wallet) ; le QR code (comme le Flash'NPay créé par Auchan) ; la transmission magnétique (Samsung Pay exploite la technologie transmission magnétique suite au rachat de LoopPay mais aussi le NFC) ; les systèmes de portefeuilles électroniques mobiles comme Orange Cash (Orange et Visa) ; PayPal Mobile et Paylib (initié par les banques françaises). Jungle, il faut bien l'admettre, est vraiment un doux euphémisme pour évoquer cet univers ! Face à un tel environnement, banques et entreprises n'ont d'autres choix que de perfectionner la sécurité des systèmes de paiement mobiles afin de donner davantage d'assurance aux consommateurs. Cette assurance semble passer par des systèmes de cryptage des données très évolués et les dispositifs de détection prédictive de malwares. Notre confrère cite PayPal qui vient de racheter la start-up israélienne CyActive qui a mis au point une technologie capable d'anticiper les futures attaques grâce à des algorithmes permettant d'analyser et de comprendre les processus de piratage.

En parallèle, les fournisseurs ne ménagent pas leurs efforts en apportant, au niveau du terminal, des mécanismes à double authentification comme Apple qui exploite l'empreinte digitale en plus d'un code de sécurité unique et des quatre derniers numéros de la carte de sécurité sociale de l'utilisateur. On le voit bien, il y a de gros efforts en cours pour tendre vers le risque zéro, même s'il n'existe pas.

Les entreprises du secteur et les banques gagneraient à collaborer plus étroitement pour améliorer la sécurité des transactions au plan national et international, tout comme elles sont condamnées à imaginer des standards qui détectent à mille lieues les criminel et les neutralisent sans coup férir.

Enfin, chaque entreprise qui propose des solutions de paiement mobile devrait assortir son plan d'expansion d'une campagne de communication qui permettrait aux utilisateurs d'éviter de tomber dans les pièges, de plus en plus perfectionnés, des cybercriminels.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Source : http://malijet.com/la_societe_malienne_aujourdhui/139922-chronique-du-web-les-cybercriminels-ciblent-le-paiement-mobile.html
Par Serge de MERIDIO

Trois Anonymous jugés pour des cyber-attaques sur des sites lorrains | Le Net Expert Informatique

Ils seront trois à s'aligner à la barre du tribunal correctionnel de Nancy ce lundi matin. Trois Anonymous, mais sans le fameux masque de la BD « V for Vendetta » qui est devenu le signe de ralliement de cette nébuleuse contestataire très active sur le Net.

Le trio a été démasqué et sera jugé à visage découvert pour avoir piraté en décembre dernier les sites du Conseil général de la Meuse, du Conseil régional de Lorraine et de l'Agence nationale de gestion des déchets radioactifs (Andra). Ces cyber-attaques visaient à protester contre le projet de stockage souterrain de déchets nucléaires à Bure dans la Meuse.

« Nous n'avons rien fait de mal »

Si ces actions ont passablement énervé les autorités qui ont mis le paquet pour identifier et arrêter les trois Anonymous, ces derniers peuvent toutefois compter sur un courant de sympathie dans l'opinion. Des appels à se mobiliser en leur faveur circulent en effet depuis plusieurs jours sur les réseaux sociaux. Un tract a également été distribué sur Nancy pour appeler à une manifestation devant le tribunal ce lundi matin.

S'ils font cause commune, les trois prévenus sont toutefois aussi dissemblables que possible. Ils ne se connaissent d'ailleurs pas. Ils ne se sont jamais rencontrés et n'ont eu des contacts que sur le Web pour préparer leur opération de piratage. L'un est un chômeur de Reims. Un autre est un trentenaire de Nantes très actif dans les mouvements altermondialistes. Le dernier, enfin, Loïc Schneider, est un jeune étudiant nancéien idéaliste, sans compétence informatique particulière.

Son but lors du procès ? Obtenir une relaxe et « faire comprendre que notre objectif n'était pas de nuire ou de causer des dégâts mais de faire passer un message » , explique le jeune homme qui se voit plus comme un « lanceur d'alerte » que comme un redoutable activiste. Loïc Schneider entend d'ailleurs bien continuer à jouer ce rôle devant le tribunal. Il a prévu de lire un texte expliquant ses motivations. « On voulait juste un référendum sur le projet d'enfouissement des déchets de Bure. C'est tout ! Et nous n'avons rien fait de mal. Nous n'avons ni volé, ni abîmé des données informatiques. Ce que nous avons fait s'apparente à un sit-in ou un blocus. Rien de plus » , développe le jeune Anonymous qui joue gros lors de son procès.

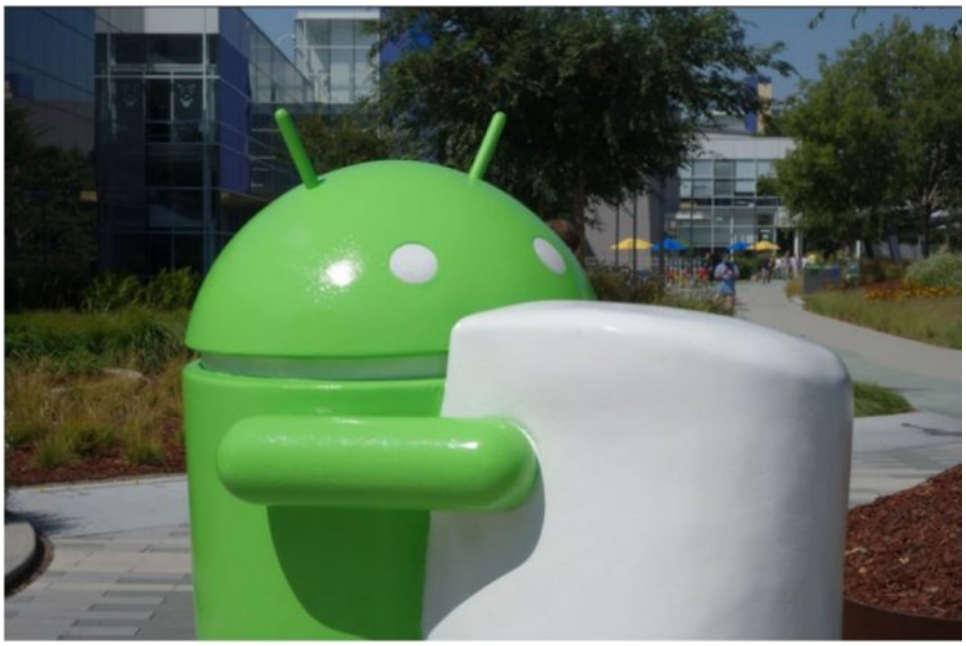
Lui et ses camarades risquent en effet 10 ans de prison et 150 000 € d'amende. C'est un maximum. En cas de condamnation, ils n'auront jamais des peines aussi élevées. Ce que Loïc Schneider redoute le plus, c'est une inscription sur son casier judiciaire. Ce qui l'empêcherait de réaliser le projet professionnel qu'il a en tête : devenir avocat en droit de l'environnement. Pour y parvenir, la première cause qu'il va devoir plaider et gagner sera donc la sienne.

Source :
http://www.vosgesmatin.fr/actualite/2015/11/09/nancy-trois-anonymous-juges-pour-des-cyber-attaques-sur-des-sites-lorrains

---

20 000 apps Android

détournées dans les boutiques parallèles | Le Net Expert Informatique

	20 000 apps Android détournées dans les boutiques parallèles

Sous l’apparence d’applications Android très utilisées comme WhatsApp ou Google Now, des copies malveillantes, proposées sur des boutiques aux critères de sélection moins stricts que Google Play, installent au coeur des terminaux mobiles des adwares extrêmement difficiles à déloger.

Des experts en sécurité de Lookout ont trouvé plus de 20 000 exemples d’apps Android compromises, dont certaines sont des copies d’applications figurant parmi les plus populaires comme Facebook, Google Now, SnapChat, Twitter ou WhatsApp. Elles contiennent du code malveillant et affichent agressivement des publicités sur les terminaux.

Par ailleurs, contrairement aux habituels adwares, ces apps sont installées de telle façon que les utilisateurs ne peuvent pas les supprimer. Elles noyautent les terminaux en accédant aux accès racines permettant de sortir des sandbox restreignant les manipulations et peuvent ainsi prendre le contrôle complet du terminal, de ses applications et de ses données.

Les apps compromises résident sur des boutiques parallèles à Play

Les utilisateurs qui téléchargent leurs apps de façon classique sur la boutique Google Play, ne sont normalement pas concernés car ces applications comportant un cheval de Troie sont principalement distribuées à travers d’autres boutiques d’apps en ligne. Cependant, certains utilisateurs passent par ce type de boutiques car elles proposent souvent des apps que Google Play n’autorise pas, relatives aux jeux en ligne ou pornographiques.

Les pays dans lesquels Lookout a détecté le plus grand nombre d’applications compromises sont les Etats-Unis, l’Allemagne, l’Iran, la Russie, l’Inde, la Jamaïque, le Soudan, le Brésil, le Mexique et l’Indonésie. Les chercheurs de la société spécialisée en sécurité mobile ont distingué trois familles d’apps qui noyautent automatiquement les terminaux à la racine, respectivement dénommées Shedun, Shuanet et ShiftyBug. Les pirates qui les exploitent repackagent les apps les plus populaires de Google Play et les installent sur des boutiques en ligne moins regardantes sur la sécurité. « Nous pensons que ce type d’adware intégrant des chevaux de Troie vont devenir de plus en plus sophistiqués avec le temps et qu’ils pourront mieux dissimuler leur présence sur le terminal », expliquent les chercheurs de Lookout dans un billet.

Source :
http://www.lemondeinformatique.fr/actualites/lire-20-000-apps-android-detournees-dans-les-boutiques-paralleles-62898.html
Article de Lucian Constantin / IDG News Service (adapté par Maryse Gros)

---

12 % des entreprises belges victimes d’attaques

informatique…| Le Net Expert Informatique

12 % des entreprises belges victimes d'attaques informatique…

Quelque 12% des PME belges ont déjà été confrontées au moins une fois à une attaque par déni de service, également appelée DDoS, suivies de près (11%) par les PME plus petites ou unipersonnelles.

Les entreprises de plus grande taille obtiennent, quant à elles, un résultat légèrement meilleur, avec 9%, ressort-il mercredi d'une étude de Kaspersky Lab, société spécialisée dans la sécurité des systèmes d'information. Au niveau mondial, un quart des attaques a entraîné la perte de données sensibles.

De telles attaques visent à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur ou en accaparant ses ressources jusqu'à épuisement.

Le coût pour tout rétablir peut aller jusqu'à 367.000 euros. «En moyenne, une attaque DDoS coûte aux organisations plus de 40.000 euros en factures de restauration. Les grandes entreprises dépensent des montants encore supérieurs à la récupération après une perturbation externe ou attaque de cyber-espionnage. L'investissement moyen après une attaque DDoS s'élève ainsi à environ 367.000 euros contre les 546.000 euros dépensés en moyenne par ces entreprises pour se remettre d'autres formes d'attaques», détaille l'étude 'Corporate IT Security Risks Survey', réalisée par Kaspersky Lab et B2B International auprès de 5.500 entreprises à travers le monde.

Au niveau mondial, 9% des attaques qui paralysent un service durent de deux jours à une semaine et, dans 7% des cas, ce type d'attaque dure plusieurs semaines ou davantage. Mais les dommages ne se limitent pas au temps d'arrêt: ils peuvent également perturber totalement les activités des entreprises et provoquer, pour environ 7% des PME sondées, la perte de données confidentielles.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lavenir.net/cnt/dmf20151028_00726712

Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement | Le Net Expert Informatique

Une vulnérabilité dans les Cartes bancaires connue et exploitée discrètement

Des chercheurs viennent de publier un rapport d'étude sur l'exploitation concrète mais discrète d'une vulnérabilité affectant les cartes EMV et connue depuis plus de 5 ans.

Combien de cas réellement constatés ? Combien de cas non constatés ? C'est la question que soulève l'étude que viennent de publier Houda Ferrradi, Rémi Géraud, David Naccache et Assia tria, de l'Ecole normale supérieure et du CEA-TEC Paca.

Dans celle-ci, les quatre chercheurs se penchent des cartes bancaires EMV modifiées pour permettre leur utilisation sans en connaître le code PIN, en toute discrétion, grâce à deux puces câbles l'une sur l'autre, sur la puce d'origine : « la première puce est clipsée sur une carte authentique volée. La seconde puce joue le rôle d'intermédiaire et communique directement avec le terminal de point de vente. L'ensemble est intégré au corps en plastique d'une autre carte également volée ».

Le concept est connu depuis début 2010. C'est le chercheur Steven J. Murdoch, de l'université de Cambridge qui avait levé le voile sur une vulnérabilité potentiellement grave des cartes bancaires à puces dites EMV. Une faille qui « permet à un fraudeur d'utiliser une carte de paiement à puce volée pour régler un achat, via un terminal de paiement électronique non modifié, sans connaître le code PIN du porteur légitime de la carte bancaire ». Ainsi, un dispositif électronique intercepte et modifie les communications entre la carte à puce et le terminal de paiement électronique. Lorsque celui-ci demande à la carte de vérifier le code PIN saisi par l'utilisateur, le dispositif du pirate intercepte la requête et se charge, à la place de la carte, de répondre au TPE que le code a été vérifié et confirmé. Voilà ce que décrivait alors, par le menu, le chercheur britannique dans un rapport d'étude préliminaire.

Lors d'un entretien téléphonique avec LeMagIT, Steven J. Murdoch évoquait alors l'ampleur de la menace : « le reçu indique que la transaction a été autorisée par code PIN », du moins était-ce le cas lors de ses tests au Royaume-Uni, pour des transactions de type offline comme online – à savoir, avec ou sans connexion aux serveurs de contrôle des transactions. Un détail lourd de conséquences : même armé d'une déclaration de perte ou de vol, comment le porteur légitime de la carte pourra-t-il dégager sa responsabilité face à un banquier qui ne manquera pas de lui rappeler qu'il est responsable de la confidentialité de son code PIN ? Pour Steven J. Murdoch, le risque était notamment que « d'autres aient découvert la faille avant nous ».

La lecture du rapport des quatre chercheurs français nous apprend qu'environ 40 modifications frauduleuses de cartes, exploitant la vulnérabilité dévoilée par Murdoch, ont été découvertes en 2011 : « en mai 2011, le GIE Cartes Bancaires a relevé qu'une dizaine de cartes EMC, volées en France quelques mois plus tôt, étaient utilisées en Belgique. Une enquête de police a été ouverte ». Le montant de la fraude liée à cette opération : un peu moins de 600 000 € sur plus de 7 000 transactions.

Début 2010, sans surprise, le GIE Cartes Bancaires minimisait toutefois la menace, estimant qu'elle « nécessitait des équipements qui ne sont pas très discrets ». Certes, la carte frauduleuse présente une puce d'apparence plus épaisse que la normale. Mais au moins dans le cas de cette fraude ayant fait l'objet d'une enquête, cela n'a pas éveillé de soupçons.

Source :
http://www.lemagit.fr/actualites/4500256061/Cartes-bancaires-une-vulnerabilite-connue-exploitee-discretement
par Valéry Marchive

40 % des lycéens de l'agglomération de Mont-de-Marsan victimes de cyber-attaques | Le Net Expert Informatique

40 % des lycéens de l'agglomération de Mont-de-Marsan victimes de cyber-attaques

Le résultat est issu d'une étude menée l'an passé par l'Education nationale dans les établissements secondaires de l'agglomération montoise.

Depuis lundi 12 octobre et jusqu'au jeudi 22, le Bureau information jeunesse (BIJ) de Mont-de-Marsan, en lien avec l'Education nationale, pilote une série d'animations collectives inédites autour d'Internet, de ses atouts, mais surtout de ses risques, notamment pour les plus jeunes. Cette opération baptisée @Sans Danger a été imaginée suite aux résultats préoccupants d'un sondage mené l'an passé dans les établissements secondaires de l'agglomération montoise.

D'après cette enquête, plus de 40 % des jeunes interrogés disent en effet avoir été victimes au moins une fois d'une « cyber attaque », et 12 % confient avoir déjà déploré une usurpation d'identité.

Pour aller plus loin, le service scolaire du lycée montois Frédéric-Estève a travaillé avec le BIJ et l'Agence landaise pour l'informatique (Alpi) sur un échantillon de 30 autres élèves. Si 85 % avouent être très actifs sur les réseaux sociaux, 66 % confessent avoir déjà été gênés par des commentaires ou photos mis en ligne.

Autre réalité intéressante, trois quarts des sondés ont « conscience qu'il faut se protéger », notamment en ce qui concerne les données personnelles. Or, aussi actifs soient-ils sur le Web, bien peu d'entre eux savent réellement comment s'y prendre.

Tout le programme de cette « semaine d'éducation cyber citoyenne » est en ligne sur le site de la mairie.

Source :

http://www.sudouest.fr/2015/10/13/mont-de-marsan-40-des-lyceens-de-l-agglomeration-victimes-de-cyber-attaques-2153291-3452.php

par Vincent Dewitte

En France, les cyber-attaques sur les entreprises explosent | Le Net Expert Informatique

	En France, les cyber-attaques sur les entreprises explosent

Les entreprises françaises ont subi en moyenne 21 incidents de cybersécurité par jour en 2015. C'est 51% de plus qu'il y a un an selon une étude mondiale du cabinet PwC.

La menace représentée par les cyberattaques sur les entreprises se précise alors que le gouvernement va présenter avec l'Anssi (Agence nationale de la sécurité des systèmes d'information), une charte pour la sécurité des emails signée par cinq fournisseurs de services de messagerie, une étude mondiale révèle l'ampleur du problème.
Selon l'étude The Global State of Information Security Survey 2016 réalisée par le cabinet d'audit et de conseil PwC, en France, le nombre de cyber-attaques recensées a progressé à hauteur de 51% au cours des 12 derniers mois.
Cette explosion est supérieure à la hausse constatée au niveau mondial, le nombre de cyber-attaques visant les entreprises ayant progressé de 38% en 2015.
Cette étude, qui recense la façon dont plus de 10.000 dirigeants dans 127 pays gèrent la cybersécurité dans leurs organisations relève également que ces derniers ont augmenté leur budget pour lutter contre la cyber-criminalité
Au niveau mondial, ces budgets ont augmenté de 24%, renversant la tendance baissière de l'année dernière.

PwC – Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit un budget en hausse de 29% par rapport à l'année dernière

Le budget moyen de cybersécurité des entreprises françaises interrogées s'est établi à 4,8 millions d'euros par entreprise en 2015, soit une hausse de 29%, plus élevée que celle constatée au niveau mondial.
Ce chiffre est à comparer avec le niveau estimé des pertes financières liées à des incidents de cybersécurité, soit en moyenne à 3,7 millions d'euros par entreprise en France, soit une augmentation de 28% par rapport à 2014.

Le piratage de la chaîne TV5 Monde aurait ainsi coûté plus d'une dizaine de millions d'euros.
En France comme dans le monde, la source des menaces reste majoritairement interne aux entreprises. Cependant les sources de cyber-attaques qui ont progressé le plus en 2015 sont, elles, externes aux entreprises.
Le fait saillant tient au fait que la responsabilité des fournisseurs et des prestataires de service actuels est de plus en plus invoquée dans la progression de ces incidents informatiques.

« Ce qui ne peut être protégé, peut être assuré »
Cette responsabilité est en hausse d'environ 32% pour les fournisseurs et de 30% pour les prestataires de services. Cela est dû au fait que les entreprises travaillent de plus en plus en collaboration avec des partenaires commerciaux et industriels externes, ce qui accroît les « portes d'entrée » pour le piratage informatique.
Selon Philippe Trouchaud, associé chez PwC, « Les chiffres indiquent qu'une entreprise française sur 5 pense que ses concurrents sont potentiellement à l'origine de certaines attaques subies en 2015. En effet, ces derniers sont particulièrement attirés par les données de type propriété intellectuelle, les business plans, les données de R&D, etc ».
« Ce qui ne peut pas être protégé peut être assuré », note PwC, qui estime que le marché mondial de la cyberassurance (pour atténuer les effets financiers d'une cyberattaque) va tripler d'ici 2015, à 7,5 milliards de dollars.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://bfmbusiness.bfmtv.com/entreprise/en-france-les-cyber-attaques-sur-les-entreprises-explosent-922703.html
Par F.Bergé