Les entreprises françaises touchées par une explosion de la cybercriminalité

	Les entreprises françaises touchées par une explosion de la cybercriminalité

Plus des deux tiers (68%) des entreprises françaises ont été victimes de fraude au cours des deux dernières années, un phénomène dû en particulier à l'explosion de la cybercriminalité, selon une étude de PwC publiée début mars 2016.

Ce chiffre est en progression de 13 points par rapport à la dernière étude de PwC publiée en 2014 sur le sujet, et est nettement supérieur au taux constaté au niveau mondial, qui s'établit à 36%, selon cette enquête réalisée auprès de 6.337 entreprises dans le monde dont 120 françaises.
Les entreprises de moins de 100 salariés sont de plus en plus touchées, 43% d'entre elles déclarant être victimes de fraudes (+14 points par rapport à 2014).
Au premier rang des fraudes figure toujours le détournement d'actifs au sens large, même si ce risque diminue, avec 56% d'entreprises s'étant déclarées victimes de ce phénomène en 2016 contre 61% en 2014.
La cybercriminalité explose pour sa part: 53% des entreprises ont déclaré avoir été victimes de ce type de fraudes contre 28% en 2014. Et 73% des dirigeants français redoutent de subir une cyber-attaque au cours des deux prochaines années, contre 34% au niveau mondial.
Pour autant, « plus de la moitié (des entreprises françaises) n'ont pas encore de plan d'action opérationnel pour répondre à une cyber-attaque », souligne Jean-Louis Di Giovanni, associé de PwC, cité dans le communiqué.
Parmi les autres risques figurent la fraude aux achats (25%), qui se traduit par des surfacturations de biens ou de prestations, et la « délinquance astucieuse », protéiforme, qui recouvre la fraude au président (une personne se fait passer pour le dirigeant de la société et ordonne de procéder en urgence à un virement) ou encore celle aux changements de RIB de fournisseurs.
Celle-ci a presque doublé en deux ans, passant de 10% en 2014 à 18% en 2016, selon PwC… [Lire la suite]

Réagissez à cet article

Source : *Fraude: les entreprises françaises touchées par une*

explosion de la cybercriminalité

Canal+ victime d’un piratage informatique lundi 14 mars 2016

Canal+ victime d’un piratage informatique lundi 14 mars 2016

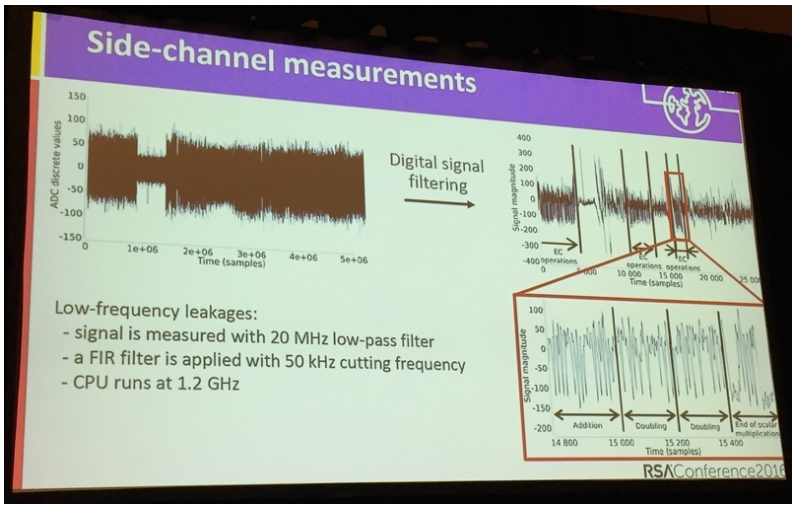
Le site Internet de la chaîne cryptée a été brièvement inaccessible lundi soir à cause d’un piratage.

Le site Internet de Canal+ a été inaccessible pendant un court moment vers 23 heures, lundi soir. Il a en effet été piraté par un groupe nommé AMAR^SHG, rapporte le site NextInpact.
Contre les guerres. Les auteurs de l’attaque ont piraté le site de la chaîne cryptée afin d’y diffuser des messages dénonçant les guerres actuellement en cours dans le monde : « la guerre en Israël, au Kosovo et en Serbie, au Maroc et au Sahara occidental, en Somalie, en Russie et aux Etats-Unis, des gens y meurent chaque jour ». « Et certains trouvent le moyen d’être content (sic) et de penser à eux-mêmes », contient aussi le message envoyé par ce groupe de hackers qui se dit à la fois albanais et marocain. Un autre texte envoyé plus tard dénonce, lui, « le silence » qui entoure des années « de massacre en Syrie ».
Sur son compte Twitter, Canal+ a brièvement évoqué le problème, via une réponse à un internaute : « bonsoir, c’est en cours de résolution, nous sommes dessus »… [Lire la suite]

Réagissez à cet article

Source : *Le site Internet de Canal+ piraté lundi soir*

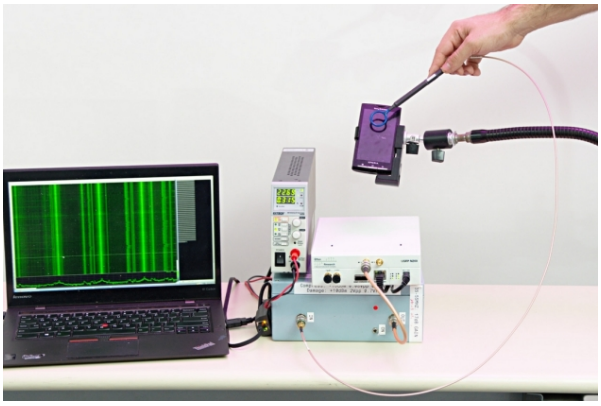
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques



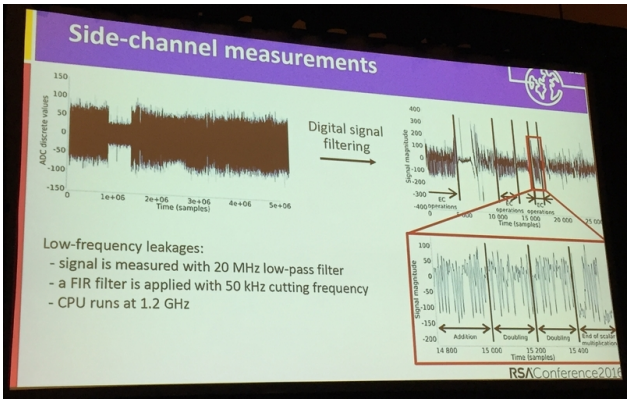
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques

---

Des chercheurs arrivent à extraire des clés de chiffrement privées en captant les signaux involontaires des circuits imprimés. Parmi les applications vulnérables figurent OpenSSL et les porte-monnaie Bitcoin.



Les smartphones d'aujourd'hui embarquent de plus en plus procédés cryptographiques pour sécuriser tout un tas d'échanges et de transactions. L'équipement matériel, toutefois, n'est pas forcément à la hauteur des enjeux. Deux équipes de chercheurs viennent de présenter concomitamment des attaques non invasives qui s'appuient sur les émanations électromagnétiques des terminaux mobiles pour récupérer des clés privées de signatures électroniques. Elles permettraient, par exemple, de pirater des porte-monnaie Bitcoin, des transactions Apple Pay ou des connexions sécurisées par OpenSSL.
La première équipe est française et regroupe quatre chercheurs issus d'Orange Labs, HP Labs, NTT et l'université de Rennes. Le 3 mars, à l'occasion de la conférence RSA 2016, ils ont montré comment extraire d'un téléphone Android des clés privées basées sur les algorithmes de courbes elliptiques (Elliptic Curve Digital Signature Algorithm, ECDSA). Leur étude se limite à une librairie cryptographique spécifique, à savoir Bouncy Castle 1.5. Quand celle-ci réalise les calculs mathématiques liés à la signature d'un message, les circuits intégrés du téléphone émettent des ondes électromagnétiques à basse fréquence (50 kHz).



Le traitement du signal révèle les opérations mathématiques (« addition », « doubling »)

Les chercheurs captent ce signal au moyen d'une antenne appliquée sur le téléphone et arrivent, par traitement de signal, à reconnaitre les différentes opérations de ce calcul. Cette information est suffisante pour récupérer in fine la clé secrète. La librairie vulnérable a, depuis, été modifiée de telle manière que l'on ne puisse plus reconnaitre les opérations (version 1.51). Néanmoins, une attaque concrète aurait pu être, selon les chercheurs, de cibler les porte-monnaie Bitcoin car ils s'appuient sur Bouncing Castel.
Ainsi, un attaquant aurait pu piéger le lecteur NFC d'un commerce qui accepte les Bitcoins et, ainsi, récupérer les adresses Bitcoin des clients. Ce qui lui permettait alors d'en disposer comme bon lui semble. « On pourrait également imaginer des attaques à plus longue distance, à condition de disposer d'un équipement de captation suffisamment puissant, comme peuvent en avoir les agences gouvernementales », nous explique Mehdi Tibouchi, l'un des quatre chercheurs français, à l'issue de leur présentation.

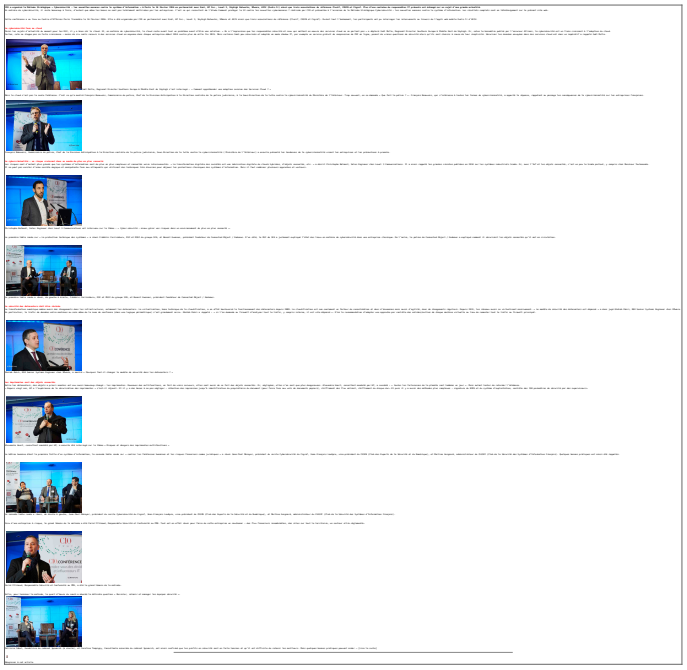
Des attaques low-cost
La seconde équipe qui a planché sur ce type d'attaques est israélienne et regroupe cinq chercheurs issus de l'université de Tel Aviv et de l'université d'Adelaide (Australie). Leur attaque cible également les signatures basées sur les courbes elliptiques ECDSA, mais son domaine d'application est nettement plus large.
Ainsi, ces chercheurs ont réussi à extraire des clés privées sur les librairies OpenSSL et CoreBitcoin sur iOS, qui sont toujours vulnérables à l'heure actuelle. Ils ont également réussi des extractions partielles de clés privées avec la librairie CommonCrypto d'iOS et la version Android d'OpenSSL. Toutefois, CommonCrypto – qui est notamment utilisé par Apple Pay – n'est pas vulnérable au-delà de la version iOS 9 car Apple a intégré des « mécanismes de défense » contre ce type d'attaques.
Selon les chercheurs israéliens, les fuites de signaux peuvent être captées de façon électromagnétique par une petite antenne, ou de manière électrique par une petite résistance intégrée au niveau du câble de chargement USB (prix : quelques dollars). Dans les deux cas, le signal est envoyé dans l'entrée d'une carte son Creative Track Pre Sound, ce qui permet de le numériser et de l'amplifier (prix : 50 dollars). Au final, la mise en œuvre de l'attaque est donc de faible coût. Les chercheurs ont réalisé leurs tests avec un iPhone 3GS et un Sony-Ericsson Xperia x10 … [Lire la suite]

Réagissez à cet article

Source : *On peut pirater les smartphones iOS ou Android à cause de leurs fuites électromagnétiques*

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d'information ?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

Est-ce légal d'utiliser un VPN pour contourner le filtrage géographique ?

Est-ce légal d'utiliser un VPN pour contourner le filtrage géographique ?

Vous songez à utiliser un VPN pour accéder aux catalogues de Netflix diffusés dans d'autres pays, mais ne savez pas si c'est légal ? La réponse.

Alors que NordVPN part en guerre contre le blocage de ses serveurs par Netflix, vous vous posez peut-être la question : est-ce légal pour un internaute de passer par les services d'un VPN pour contourner le filtrage géographique et accéder à des œuvres qui, normalement, ne sont pas diffusées en France ou le sont par d'autres services ?
La réponse est loin d'être aussi évidente qu'on pourrait le penser. Elle n'est en tout cas, comme souvent en droit, pas binaire. Il est impossible de répondre « oui » ou « non ». Mais tentons une réponse argumentée.
Il fait peu de doute que les blocages géographiques imposés par les ayants droit peuvent être considérés comme des mesures techniques de protection, qui sont celles destinées à « empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ». Quand un studio accorde des droits à Netflix US, il le fait pour autoriser l'accès depuis les États-Unis, pas depuis les autres pays, et le blocage géographique vise à s'en assurer.
Or l'article L335-3-1 du code de la propriété intellectuelle punit bien de 3 750 euros d'amende « le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace (…) afin d'altérer la protection d'une oeuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle ».
Fin de l'histoire ? Non. Car il y a deux obstacles.

LE FILTRAGE GÉOGRAPHIQUE, UNE MESURE TECHNIQUE DE PROTECTION « EFFICACE » ?

Le contournement du filtrage géographique par contrôle d'adresse IP n'est interdit que s'il s'agit d'une mesure technique « efficace », ce qu'il ne faut pas prendre au sens commun. Il suffit pas de pouvoir contourner pour dire que ça n'est pas efficace.
La loi précise que les « mesures techniques sont réputées efficaces lorsqu'une utilisation […] est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection ».
Il paraît clair que le contrôle de l'adresse IP n'est pas un contrôle de code d'accès, ni un procédé de transformation de l'œuvre tel que le brouillage ou le cryptage. Mais s'agit-il d'un « mécanisme de contrôle de la copie » ? Il y aurait débat, puisque techniquement, l'utilisateur de Netflix ne réalise pas de copie. Mais admettons.

L'UTILISATEUR D'UN VPN EST-IL RESPONSABLE ?

Un deuxième problème se pose. L'amende de 3 750 euros prévue par l'article L335-3-1 ne peut s'appliquer que si le contournement est réalisé par « d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant » qui existe déjà, fourni par un tiers.
Dans ce dernier cas, c'est le fait de « procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace » qui devient punissable, de six mois de prison et 30 000 euros d'amende. L'idée est que c'est d'abord celui qui fournit l'outil en toute connaissance de cause qui doit être tenu responsable pénalement, et pas celui qui s'en sert.

Dès lors, il faut distinguer deux cas, assez paradoxaux :
Si l'internaute utilise un service de VPN qui est clairement promu comme un outil de contournement du filtrage (typiquement NordVPN), il n'est pas responsable ;
Si l'internaute utilise un service de VPN totalement neutre, qui ne fait que fournir une adresse IP géolocalisée dans d'autres pays, sans dire à quoi ça peut servir, c'est lui qui le transforme en outil de contournement de la mesure technique de protection, et il devient donc responsable.
Dans tous les cas, l'internaute est potentiellement coupable de recel de contrefaçon, mais c'est une réflexion qui nous amènerait trop loin. Et songez surtout qu'en pratique, il reste extrêmement peu probable qu'existe un jour une plainte pour utilisation d'un VPN, qui demanderait d'obtenir l'adresse IP des internautes en cause. Mais si vous vous posiez la question, vous avez une réponse.

Source : Guillaume CHAMPEAU

Réagissez à cet article

Source : *Est-ce légal d'utiliser un VPN pour contourner le filtrage géographique ? – Politique – Numerama*

Alerte vigilance – Ransomware Lockyx

Alerte vigilance – #Ransomware Lockyx

Bonjour, Une vague d’attaques du ransomware Locky touche actuellement de nombreuses entreprises dans le monde et depuis peu en France.Voici nos conseils pour se protéger contre cette nouvelle menace :

CONSEIL N°1 : VIGILANCE UTILISATEUR

Informez vos collaborateurs de l’importance de ne pas ouvrir la pièce jointe d’un email envoyé par un expéditeur inconnu. Soyez très vigilant notamment avec les pièces jointes .zip, .doc, .xls : sources de propagation de Locky.

Les sensibiliser à l’utilisation des macros et/ou les désactiver, source de propagation de Locky.

CONSEIL N°2 : SOLUTION DE PRA

Assurez-vous que vos machines sont correctement sauvegardées, et les images externalisées pour une restauration rapide en cas d’attaque.

Les équipes ESET sont mobilisées à l’heure actuelle pour vous apporter une solution rapide et continue contre ce ransomware et ses multiples variantes quotidiennes.

Note : si vos machines sont déjà infectées, isolez-les des autres, initiez leur restauration et lancez une analyse complète de vos systèmes.

Cordialement,

L’équipe ESET

… [Lire la suite]

Réagissez à cet article

Source : *Alerte vigilance – Ransomware Lockyx*

Apple condamné à créer un firmware spécial pour le FBI

Apple condamné à créer un firmware spécial pour le FBI

Le tribunal de Californie a ordonné à Apple de fournir au FBI les moyens technologiques pour accéder au contenu en clair d'un téléphone utilisé par l'auteur de la tuerie de San Bernardino. Apple ne devra pas déchiffrer lui-même, mais supprimer une protection d'iOS 8 qui permet d'éviter les tentatives d'accès par force brute.

À la demande du FBI, un tribunal de Californie a ordonné mardi à Apple de fournir une « assistance technique raisonnable » aux enquêteurs de la police fédérale, qui cherchent à accéder au contenu en clair du téléphone de l'auteur de la tuerie de San Bernardino, Syed Rizwan Farook. Cette attaque terroriste avait fait 14 morts le 2 décembre 2015.

Estimant que ses principes de protection de la confidentialité des données de ses clients étaient indérogeables, Apple avait refusé d'apporter son concours actif au déchiffrement de l'iPhone 5C du suspect, dont le contenu est illisible tant qu'il n'est pas débloqué. La firme de Cupertino se dit de toute façon incapable de déchiffrer le contenu, puisque la clé est générée et stockée sur le téléphone lui-même, et qu'il n'a donc pas davantage la main que les experts en cryptologie des services de renseignement américains.

FAIRE SAUTER LA PROTECTION APRÈS 10 TENTATIVES INFRUCTUEUSES

Mais le FBI a obtenu de la justice qu'Apple l'aide autrement. L'entreprise dirigée par Tim Cook devra fournir une mise à jour du firmware, qui fasse sauter la protection du téléphone contre les tentatives abusives d'accès (il n'est pas précisé comment une telle mise à jour pourrait être installée). En effet le suspect avait activé sur son smartphone la fonctionnalité de sécurité d'iOS qui fait qu'après 10 saisies erronées de codes PIN, le contenu du téléphone est automatiquement effacé.

Apple devra fournir au FBI le moyen de modifier le système iOS sur l'iPhone 5c de Farook, pour que la fonction d'effacement du contenu du téléphone ne soit pas activée. Le FBI espère ainsi opérer par force brute pour deviner le mot de passe à force de tentatives répétées, et ainsi gagner l'accès au contenu en clair du téléphone.

APPLE DEVRAIT FAIRE APPEL

Par ailleurs, toujours dans le même objectif, Apple devra fournir au FBI le moyen de tester rapidement plusieurs combinaisons, pour éviter d'avoir à construire un robot qui tape lui-même lentement les codes les uns après les autres. Avec quatre chiffres pour le code PIN, 10 000 combinaisons sont possibles.

Selon la BBC, Apple devrait toutefois faire appel de la décision. L'entreprise craint certainement que sa coopération soit interprétée comme la fourniture d'un backdoor à l'administration américaine, qui minerait la confiance qu'ont les clients dans la protection apportée par Apple.

« Apple n'a jamais collaboré avec une quelconque autorité publique, de quelque pays que ce soit, afin de créer une « porte dérobée » dans ses produits ou services », peut-on lire sur le site officiel d'Apple. « Sur les appareils sous iOS 8 ou ultérieur, vos données personnelles sont protégées par votre code. En effet, pour ces appareils, Apple ne peut répondre aux demandes d'extraction de données iOS émanant des autorités : les fichiers à extraire sont protégés par une clé de chiffrement liée au code de l'utilisateur, auquel Apple n'a pas accès ».

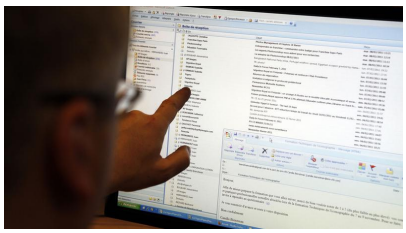
… [Lire la suite]

Réagissez à cet article

Source : *Apple condamné à créer un firmware spécial pour le FBI – Politique – Numerama*

---

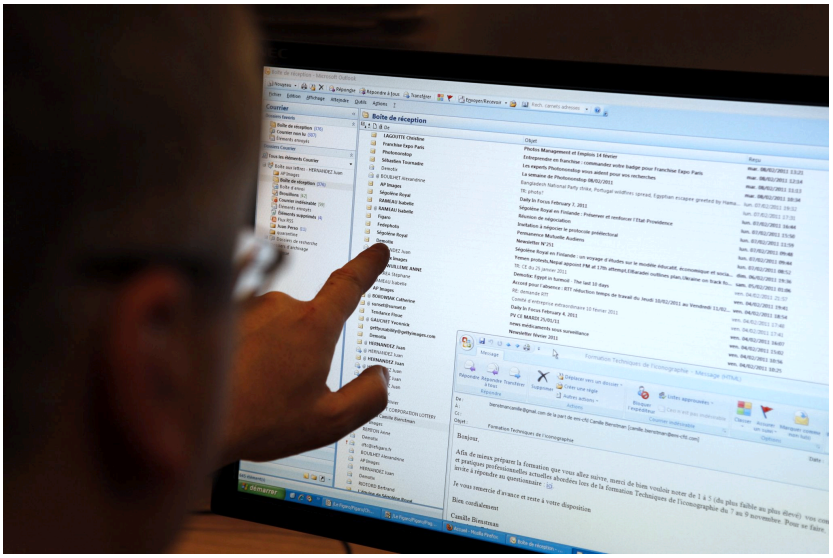
100 fois plus de victimes vol de données personnelles en deux ans en France



100 fois plus de victimes vol de données personnelles en deux ans en France

---

En 2015, cette pratique visant à dérober des informations personnelles par Internet ou par téléphone a fait plus de 2 millions de victimes en France. C'est cent fois plus qu'il y a deux ans.



Véritable piège pour les internautes, la pratique du phishing ne cesse de se répandre en France. Contraction de «fishing» (pêche) et «phreaking» (piratage de lignes téléphoniques), ce procédé malveillant vise à soutirer des données personnelles (mot de passe, identifiant de connexion, numéros de cartes bancaires). On parle également de «hameçonnage».

Sur la seule année 2015, plus de 2 millions de personnes auraient été victimes du phishing en France. C'est 100 fois plus qu'il y a deux ans, selon Europe 1 qui reprend un rapport de Phishing Initiative, site reconnu par les services de lutte contre la cybercriminalité. Le plus souvent, cette arnaque se manifeste par la réception d'un mail personnalisé provenant d'un organisme financier (banques), d'une entreprise (fournisseur d'Internet, EDF…) ou même d'une administration publique (CAF)… Du moins en apparence.

Car le message en question, aussi crédible et réaliste qu'il puisse paraître, vous invite en réalité à cliquer sur un lien, lequel vous redirige vers un site vous demandant de mettre à jour vos données personnelles. Dès lors, en se faisant passer pour des tiers, les cybercriminels à l'origine de ces mails frauduleux sont en mesure de récupérer vos informations personnelles. «L'augmentation des pratiques de phishing s'explique notamment par le nombre croissant de cybercriminels organisés en réseaux très structurés. D'autant que leurs méthodes sont de plus en plus sophistiquées. Auparavant, des fautes d'orthographe présentes dans les mails permettaient d'éveiller les soupçons. Désormais, c'est plus dur à déceler car ils paraissent davantage crédibles», explique Raphaël Renaud, spécialiste des questions liées au phishing.

Usurpées, les banques comme les grandes entreprises sont, elles aussi, directement concernées par le phishing. En modernisant leurs systèmes de sécurité, elles parviennent parfois à contrer les menaces. C'est le cas de Google qui a bloqué 7000 sites utilisés pour des attaques de phishing en 2015. De leur côté, les établissements bancaires assurent «un service de veille et donc une certaine publicité pour prévenir leurs clients, mais celle-ci est souvent insuffisante», remarque Serge Maître, secrétaire général de l'Association Française des Usagers des Banques (AFUB), avant de souligner que «le cryptogramme et le 3D Secure ont montré leurs limites face aux attaques de phishing.»

Comment réagir face au phishing?

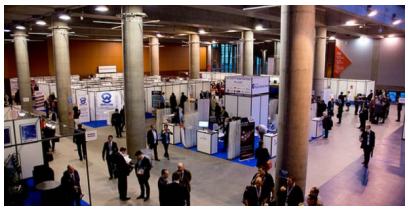
S'il n'est pas encore trop tard, plusieurs méthodes permettent de contrer le phishing. Dans un premier temps, il est préférable de disposer d'un antivirus performant. Ensuite, «l'ultime chose à faire est de ne jamais cliquer dans un lien provenant d'un e-mail. Les services sérieux (banque, opérateurs téléphoniques, etc…) ne vous demandent jamais de changer un mot de passe de cette manière», explique Raphaël Richard avant d'ajouter «qu'il faut directement se connecter sur le site officiel pour ne pas avoir de doute». Enfin, certains sites tels que ou Phishing Initiative permettent de faire vérifier un mail en cas de soupçon mais également de signaler des adresses qui semblent suspectes.

En revanche, si un internaute vient d'être victime de phishing, il doit «déposer plainte si possible devant une brigade spécialisée dans les 48 heures car au-delà, cela devient plus compliqué. Il faut également contacter … [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : le nombre de victimes de vol multiplié par 100 en deux ans en France*

Fic 2016 : La sécurisation des objets connectés préoccupe enfin…

	**Fic 2016 : La sécurisation des objets connectés préoccupe enfin…**

Le 8e Forum international de la cybersécurité, qui s'est tenu à Lille les 25 et 26 janvier, a permis de découvrir des solutions qui émergent en France en termes de sécurisation des objets de communication et des systèmes d'information auxquels ils sont connectés. Certaines sont encore à construire comme la plateforme Scop, d'autres sont déjà opérationnelles comme le CERT-Ubik et le boitier Hardsploit.

La multiplication des objets communicants, les IoT en anglais pour Internet Of Things, est une excellente opportunité pour la cybercriminalité. Sachant qu'à chacun de ces objets correspond une adresse IP, leur diffusion rend les réseaux très perméables.

« On estime à plus 50 milliards leur nombre d'ici 2020, soit 7 objets connectés par personne sachant qu'il y aura 7,5 milliards d'habitants sur terre. Les hackers vont pouvoir profiter d'une perméabilité des systèmes d'informations jamais atteintes jusqu'à présent. Et si la sécurité était en réalité le principal enjeu de l'Internet des objets ? »

A cette question posée en introduction de son exposé lors du 8e Forum International de la Cybersécurité, Christophe Joly, le directeur sécurité de Cisco France, a bien sûr répondu par l'affirmatif en chiffrant à plus de 375 milliards de dollars le marché annuel du cybercrime qui se profile. Mais comme avec les voitures au début du vingtième siècle et avec Internet plus récemment, le législateur attendra sans doute qu'une catastrophe ait lieu avant de mettre en place des règles. En attendant, rien n'empêche de se protéger.

Sécuriser l'électronique embarquée

Pour Cisco, le leader mondial des technologies informatiques de connectivité, les moyens de le faire passent par une bonne connaissance de son infrastructure informatique et des objets qui s'y connectent. Mais cette approche ne suffit pas toujours, entre autres quand l'objet communique par radiofréquence. De plus, la sécurité des objets connectés ne porte pas uniquement sur les réseaux et les… *Lire la suite…*

Réagissez à cet article

Source : *Cybercriminalité: la sécurisation des objets connectés est en marche au FIC*

Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes

---

Deux entrepreneurs se retrouvent en garde en vue après avoir trouvé une vulnérabilité dans le site de Forum international de la cybercriminalité (FIC). Ce dernier, en effet, a porté plainte pour accès frauduleux dans un système informatique.

Attention, le métier de chercheur en sécurité n'est pas totalement sans risque, comme viennent de le constater deux jeunes entrepreneurs qui viennent tout juste de créer Cesar Security, une société spécialisée dans les audits de sécurité et la prévention contre la fraude bancaire.

La semaine dernière, ils trouvent une faille sur le site web du Forum International de Cybersécurité (FIC) qui se déroule ce jour à Lille.

Selon eux, la vulnérabilité – désormais corrigée – était assez banale, mais permettait quand même d'accéder à la base de données des participants. Pas terrible pour l'image de marque d'un tel évènement qui accueille chaque année le gratin français en matière de cybersécurité. Les deux hommes veulent faire les choses bien et contactent l'éditeur du site, à savoir la Compagnie Européenne d'Intelligence Stratégique (CEIS), co-organisateur de l'évènement. Parallèlement, ils envoient une alerte sur Twitter.

Ils sont aimablement reçus au téléphone par un consultant en sécurité du CEIS auprès de qui ils détaillent leur trouvaille. Ils lui envoient un rapport technique de la faille avec une proposition de correctif, un accord de confidentialité ainsi qu'un devis pour un audit de sécurité. « Au départ, nous lui avons proposé un audit gratuit, mais il a dit que ce n'était pas un problème, que l'on pouvait lui envoyer un devis chiffré », nous explique S. Oukas, l'un des deux entrepreneurs. Puis, c'est le silence radio, plus aucune nouvelle. Le 20 janvier, ils envoient donc un nouveau tweet, pour « prendre des nouvelles ».

© DR

Le jour suivant, c'est la surprise. A 9h du matin, les gendarmes sur Centre de lutte contre les cybercriminalités numériques (C3N) toquent à leur porte. Ils apprennent que l'éditeur du site a porté plainte pour « accès frauduleux à un système de traitement automatisé de données » (STAD), un délit passible de deux ans d'emprisonnement et d'une amende de 60 000 euros.

Tout le matériel informatique est saisi. « Nous avons tout perdu : les trois ordinateurs dans notre bureau, un téléphone, un ordinateur personnel et même une PlayStation. Nous sommes tombés de très haut. Nous qui pensions que le FIC aurait encouragé une jeune startup, ils nous mettent à genou. Nous avons perdu nos outils de travail, nous ne pouvons plus rien faire », souligne M. Oukas.

Vente forcée ou chevalier blanc ?

De son côté, le CEIS n'a pas la même interprétation des choses. « Cette société nous a bien contactés, mais ce n'était pas désintéressé car elle nous a proposé ses services. Nous ne l'avons jamais autorisé à effectuer cette recherche. C'est de l'audit sauvage », estime Guillaume Tissier, directeur général du CEIS, qui n'a pas apprécié non plus que Cesar Security publie son alerte de sécurité de manière publique sur Twitter, aux yeux de tous. « Au tribunal, le débat tournera certainement autour de cette question, car on peut le voir comme une forme de vente forcée », estime pour sa part Bernard Lamon, avocat.

L'ironie du sort, c'est que cette affaire tombe pile au moment où les députés votent un amendement visant à protéger les lanceurs d'alerte qui trouvent des failles informatiques. Selon le texte, une telle personne sera exempte de peine « si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système ». Ce texte, s'il est adopté au final, pourrait néanmoins jouer en faveur de Cesar Security. « Même si les faits sont antérieurs, le texte sera applicable car il est plus clément », souligne Bernard Lamon.

Réagissez à cet article

Source : *Ils notifient une faille sur un site web puis reçoivent la visite des gendarmes*