Récupération de mot de passe : la question secrète une fausse bonne idée… | Le Net Expert Informatique

	Récupération de mot de passe : la question secrète une fausse bonne idée…

Vous avez oublié votre mot de passe ? Alors souvenez-vous des questions secrètes paramétrées et des réponses associées pour récupérer l'accès au service. Mais selon des experts de Google, mémorisation et sécurité ne font pas bon ménage.

Oublier son mot de passe pour accéder à un service en ligne, cela n'a rien d'improbable. Pour permettre de rétablir l'accès au service, les fournisseurs ont imaginé un système de récupération basé sur des questions secrètes ou challenge.

Le principe est simple : l'utilisateur sélectionne ou définit des questions et y associe une réponse. En cas d'oubli, pour rétablir son compte, l'utilisateur devra répondre correctement à ces questions. Une procédure sécurisée et efficace ?

Sécurité moindre que le mot de passe

Manifestement non selon une étude réalisée par des ingénieurs de Google. Des données analysées, il ressort ainsi que les questions secrètes offrent un niveau de sécurité de loin inférieur à celui du mot de passe défini par le titulaire du compte.

Cette procédure peut donc être exploitée par un individu malveillant pour accéder frauduleusement à un compte, contournant de cette façon la protection du mot de passe – déjà loin d'être elle-même infaillible. Mais il ne s'agit toutefois pas de la seule faiblesse de ce système.

Les chercheurs constatent qu'une part importante d'utilisateurs (37%) fournissent de fausses réponses à ces questions, partant du principe que cela renforcera la sécurité du challenge. L'effet en matière de sécurité s'avère toutefois inverse, les réponses volontairement erronées étant dans les faits plus prévisibles.

Mais l'étude estime en outre que cette fonctionnalité manque son objectif principal, c'est-à-dire la récupération effective du mot de passe. Les réponses aux questions secrètes présentent ainsi un faible niveau de mémorisation ou tendant à s'altérer.

40% des utilisateurs américains de l'échantillon examiné ont ainsi tout simplement oublié leurs réponses. Une procédure de régénération de mot de passe par SMS présente en comparaison un taux de succès de 80%, rappellent les experts de Google.

Le temps passe et on oublie

Est-il si difficile de mémoriser ces questions/réponses secrètes ? D'après l'étude, plus la robustesse de la question est forte et plus faible est la mémorisation. « Nous concluons qu'il semble presque impossible de trouver des questions secrètes qui soient à la fois sécurisées et mémorisables » jugent par conséquent les chercheurs.

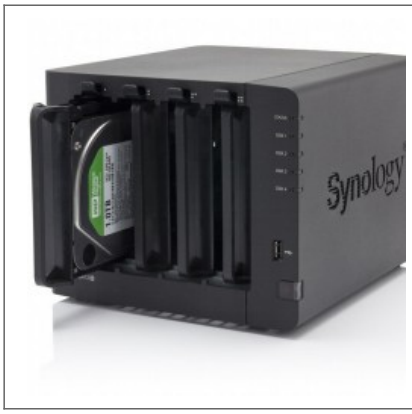
Et le temps est un facteur important dans le processus de mémorisation. Un exemple : si la question porte sur la nourriture préférée de l'utilisateur, celui-ci aura 74% de chances de s'en souvenir après un mois, mais seulement 53% à trois mois et 47% à un an.

La mémorisation s'altère plus encore lorsque l'utilisateur, par souci de sécurité, fournit une réponse à la question secrète volontairement fausse. Avec le temps, le risque s'accroît en effet qu'il ait oublié avoir utilisé une telle pratique et la réponse alors fournie. Enfin la réponse à une question peut également, et tout simplement, changer avec le temps.

Pour Google, si le recours aux questions secrètes dans le cadre d'une procédure de récupération de mot de passe continue d'avoir une certaine utilité, il devrait néanmoins être combiné à d'autres méthodes ou remplacé par une « alternative plus fiable ».

Source : http://www.zdnet.fr/actualites/recuperation-de-mot-de-passe-la-question-secrete-une-fausse-bonne-idee-39819706.htm
Par Christophe Auffray

De graves failles dans les NAS Synology à corriger | Le Net Expert Informatique



De graves failles dans les NAS Synology à corriger

Le fabricant de NAS Synology a corrigé plusieurs vulnérabilités dans son OS maison DSM (DiskStation Manager) – et ses composants associés – qui anime ses appliances de stockage, dont l'une pouvait permettre à des attaquants de compromettre les données stockées.

En effet, la vulnérabilité la plus sérieuse concerne donc Synology Photo Station, une fonction du DSM, le système d'exploitation basé sur Linux. Photo Station permet aux utilisateurs de créer des albums photo en ligne et des blogs accessibles à distance via l'adresse IP publique du périphérique. Mais des chercheurs en sécurité de l'entreprise néerlandaise Securify ont découvert que Photo Station n'effaçait pas correctement les entrées utilisateur, laissant à des attaquants la possibilité d'injecter des commandes système qui pourraient être exécutées avec les privilèges du serveur web.
De plus, Photo Station n'est pas protégé contre le cross-site request forgery (CSRF), une technique qui permet à un site web de forcer le navigateur d'un visiteur à exécuter des actions malveillantes sur un site différent de celui sur lequel il se connecte. Donc, même si Photo Station n'est pas configuré pour être accessible depuis Internet, un attaquant pourrait inciter un utilisateur situé sur le même réseau que le périphérique NAS à visiter une page web malveillante qui utiliserait le CSRF pour exploiter la vulnérabilité par commande d'injection sur le réseau LAN local. « En tirant parti de cette faille, des attaquants pourraient compromettre le périphérique NAS, et toutes les données qui y sont stockées », ont expliqué les chercheurs dans un avis qui comprend également une preuve de concept de l'exploit.

Des ransomwares s'attaquent à Synology
La version 6.3-2945 de Photo Station livrée la semaine dernière par Synology corrige cette vulnérabilité. Mais les notes de version font simplement état « d'améliorations de sécurité » sans donner de détails. La nouvelle version corrige aussi deux vulnérabilités cross-site scripting (XSS) identifiées par les chercheurs de Securify. Celles-ci pourraient être exploitées pour tromper les utilisateurs de Photo Station en les incitant à cliquer sur une URL malveillante qui exécute un code voyou dans leurs navigateurs. En cas de succès de ces attaques, des pirates pourraient voler les jetons de session ou les identifiants de connexion des utilisateurs de Photo Station ou exécuter des actions arbitraires en usurpant leur identité.
La semaine dernière Synology a corrigé une vulnérabilité similaire dans l'interface de gestion de DiskStation Manager. Les utilisateurs sont invités à mettre DSM à jour en version 5.2-5565 Update 1. Dans le passé, les boitiers NAS de Synology ont déjà été la cible de pirates. Ainsi, pas plus tard que l'an dernier, des attaquants ont exploité une vulnérabilité pour infecter plusieurs boitiers avec un ransomware destiné à crypter les fichiers stockés. Auparavant, les pirates avaient réussi à s'introduire dans les boitiers NAS de Synology pour faire tourner des programmes qui généraient de la crypto-monnaie pour leur compte.

Source : http://www.lemondeinformatique.fr/actualites/lire-synology-corrige-de-graves-failles-dans-son-os-dsm-61277.html
Par Jean Elyan

Android : vos données personnelles impossibles à effacer ? | Le Net Expert Informatique

Des chercheurs ont mis en lumière les problèmes de sécurité du système d'exploitation mobile de Google.
Grâce à un seul petit bouton « Restaurer les paramètres d'usine », Google promet à ses utilisateurs de supprimer tous les contenus de leur smartphone Android. La mémoire du smartphone serait ainsi totalement effacée. Mais à en croire une étude menée par deux chercheurs de l'université de Cambridge, il n'en est rien : cette fonction de suppression serait inefficace sur plus de 500 millions de smartphones Android. Explications.

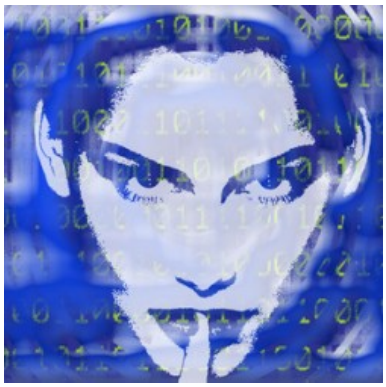
Quelles données ont été récupérées ?
Les chercheurs ont examiné 21 smartphones de 5 grandes marques et sous différentes versions d'Android : Samsung Galaxy S2 et S3, LG Optimus L7, Nexus 7, HTC Desire C, Motorola Razr I, etc. Cet échantillon représenterait près de 500 millions de smartphones actuellement en circulation. Sur la totalité des smartphones étudiés, les données personnelles ont pu être récupérées après avoir été effacées. Les deux chercheurs ont ainsi pu mettre la main sur les identifiants Google des utilisateurs sur tous les modèles. Puis, ils ont pu accéder aux informations des services Google associés à ces comptes : Gmail, Calendrier, Drive, etc. Enfin, les chercheurs ont pu récupérer des données de communications (SMS, e-mails, appels, etc.) et des fichiers multimédias (photos et vidéos).

Comment c'est possible ?
Comme l'explique le résultat des recherches, lorsqu'un utilisateur appuie sur le bouton pour effacer ses données, le smartphone supprime en réalité l'accès à ces données et non les informations elles-mêmes. « C'est comme pour un ordinateur : un formatage du disque dur ne suffit pas à effacer les données », explique à Europe 1 Jean-François Beuze, expert en sécurité informatique.

Comment être sûr que toutes les données sont effacées ?
« Il faut chiffrer ses données », conseille le spécialiste en sécurité. C'est à dire ajouter une étape de protection supplémentaire à ces informations personnelles. Pour cela, il faut se rendre dans les réglages du smartphone, puis dans le menu Sécurité et enfin cocher la case « chiffrer les données sur le smartphone ». Si une carte mémoire est utilisée pour étendre le stockage de l'appareil, l'utilisateur devra également chiffrer celle-ci. Pour les données les plus sensibles, « il existe des appareils émettant un champ électromagnétique pour effacer toute donnée sur le smartphone », ajoute Jean-François Beuze. Mais ces appareils restent réservés aux professionnels en raison de leur coût élevé.

Source : http://www.europe1.fr/technologies/android-les-donnees-personnelles-impossibles-a-effacer-970842

Attaque à grande échelle de routeurs | Le Net Expert Informatique



Une attaque à grande échelle utilise les browsers pour détourner les routeurs

Des chercheurs ont découvert un outil d'attaque web qui permet à des pirates de détourner les serveurs DNS des routeurs et de les remplacer par des serveurs voyous.

Des cybercriminels ont développé un outil d'attaque web à grande échelle qui leur permet d'exploiter les vulnérabilités des routeurs et de détourner leurs paramètres DNS quand les utilisateurs visitent des sites web compromis ou sont dirigés vers des publicités malveillantes depuis leurs navigateurs. L'objectif de ces attaques est de remplacer les serveurs DNS configurés sur les routeurs par des serveurs voyous contrôlés par des attaquants. Ainsi, les pirates peuvent intercepter le trafic, le rediriger vers des sites frauduleux, détourner les requêtes de recherche, injecter des publicités malveillantes sur les pages web et plus encore.

L'adresse DNS, qui est comparable à un annuaire de l'Internet, a un rôle essentiel. Elle traduit les noms de domaine, plus faciles à mémoriser, en adresses IP indispensables pour faire communiquer les ordinateurs entre eux. La gestion des adresses DNS se fait en cascade. Quand un utilisateur tape le nom d'un site Web dans un navigateur, la requête est d'abord transmise au système d'exploitation. Et, pour diriger le navigateur vers l'adresse IP demandée, le système d'exploitation doit passer par le routeur local qui est lui-même chargé d'interroger les serveurs DNS généralement configurés et gérés par le fournisseur d'accès internet. La chaîne de commandes se poursuit jusqu'à ce que la demande parvienne au serveur ayant autorité pour le nom de domaine recherché ou jusqu'à ce qu'un serveur fournisse les informations de son cache. Or, si des attaquants d'immiscent dans une des étapes du processus, ils peuvent répondre à la requête en renvoyant une adresse IP frauduleuse. Ils peuvent ainsi tromper le navigateur et l'orienter vers le site d'un serveur différent. Typiquement, ce site pourrait, par exemple, héberger la réplique d'un site réel qui servirait aux pirates à dérober des informations de connexion d'un utilisateur.

Détecter le routeur pour adapter l'attaque

Un chercheur en sécurité indépendant, connu en ligne sous le nom de Kafeine, a récemment observé des attaques dites « drive-by » lancées à partir de sites web compromis qui redirigeaient les utilisateurs vers un kit d'exploits inhabituel basé sur le web, spécifiquement conçu pour compromettre les routeurs. En général, les kits d'exploits vendus sur les forums illégaux et utilisés par les cybercriminels cherchent à exploiter des vulnérabilités dans les plug-ins pour navigateurs comme Flash Player, Java, Adobe Reader ou Silverlight. Leur but est d'installer des logiciels malveillants sur les ordinateurs qui n'auraient pas téléchargé les dernières versions de ces modules populaires. Le plus souvent la stratégie de ces attaques consiste à injecter un code malveillant dans des sites compromis ou de l'inclure dans des publicités malveillantes, code qui redirige automatiquement les navigateurs vers un serveur d'attaque chargé de déterminer l'OS, l'adresse IP, la localisation géographique, le type de navigateur utilisé, les plug-ins installés et d'autres détails techniques. En fonction de ces informations, le serveur d'attaque sélectionne dans son arsenal d'exploits ceux qui ont le plus de change de réussir.
Mais, les attaques observées par Kafeine fonctionnent différemment : cette fois, les utilisateurs de Google Chrome ont bien été redirigés vers un serveur malveillant, mais celui-ci a chargé un code destiné à déterminer le modèle de routeur utilisé afin de remplacer les serveurs DNS configurés sur l'appareil. « Beaucoup d'utilisateurs pensent que si leurs routeurs ne sont pas configurés pour la gestion à distance, les pirates ne peuvent pas exploiter les vulnérabilités de leurs interfaces d'administration web à partir d'Internet, parce que ces interfaces ne sont accessibles qu'à partir des réseaux locaux. Mais, cela est faux », a déclaré le chercheur. De telles attaques sont possibles grâce à une technique appelée Cross-Site Request Forgery (CSRF), laquelle permet à un site web malveillant de forcer le navigateur à exécuter des actions malveillantes sur un site Internet différent. Et le site cible peut justement être l'interface d'administration d'un routeur uniquement accessible via le réseau local. De nombreux sites web ont mis en place des défenses pour se protéger contre ces attaques CSRF, mais les routeurs ne bénéficient généralement pas de ce type de protection.

Les principaux routeurs vulnérables

Le nouveau kit d'exploits drive-by identifié par Kafeine a utilisé la technique du Cross-Site Request Forgery pour détecter plus de 40 modèles de routeur de divers fournisseurs dont Asustek Computer, Belkin, D-Link, Edimax Technology, Linksys, Medialink, Microsoft, Netgear, Shenzhen Tenda Technology, TP-Link Technologies, Netis Systems, Trendnet, ZyXEL Communications et HooToo. Selon le modèle, l'outil essaie de changer les paramètres DNS du routeur en exploitant des vulnérabilités connues par injection de commande ou en utilisant des identifiants d'administration courants. Dans ce cas aussi, il utilise la technique CSRF. Et en cas de succès de l'attaque, le serveur DNS primaire du routeur passe sous contrôle des attaquants et le serveur secondaire, utilisé comme relais en cas de panne, est paramétré en tant que serveur DNS public de Google. De sorte que, si le serveur malveillant est temporairement hors service, le routeur disposera toujours d'un serveur DNS parfaitement fonctionnel pour résoudre les requêtes, et le propriétaire ne pourra pas soupçonner une défaillance, ni être tenté de reconfigurer l'appareil.

Selon Kafeine, l'une des vulnérabilités exploitées par l'attaque affecte les routeurs de divers fournisseurs, et a été rendue publique en février. « Certains fournisseurs ont effectué des mises à jour de firmware sur leurs routeurs, mais le nombre de matériels mis à jour au cours des derniers mois reste probablement très faible », a déclaré le chercheur. Car la plupart des routeurs doivent être mis à jour manuellement et l'opération exige certaines compétences techniques. Voilà pourquoi un grand nombre de routeurs ne sont pas mis à jour. Et les attaquants le savent. En fait, d'autres vulnérabilités sont ciblées par ce kit d'exploits, dont l'une a été identifiée en 2008 et l'autre en 2013.

1 million de tentatives le 9 mai

Toujours selon le chercheur indépendant, il semble que l'attaque a été menée à grande échelle : au cours de la première semaine du mois de mai, le serveur d'attaque a comptabilisé environ 250 000 visites uniques par jour, avec un pic de près de 1 million de visites le 9 mai. Les pays les plus touchés étaient les États-Unis, la Russie, l'Australie, le Brésil et l'Inde, mais la répartition du trafic a été plus ou moins globale. Pour se protéger, les utilisateurs doivent vérifier régulièrement si de nouvelles mises à jour de firmware pour leurs routeurs sont disponibles sur les sites Web des fabricants et ils doivent les installer, surtout si ces mises à jour concernent des correctifs de sécurité. Si le routeur le permet, les utilisateurs devraient également limiter l'accès à l'interface d'administration à une adresse IP à laquelle aucun terminal n'a normalement accès, mais qu'ils peuvent affecter manuellement à leur ordinateur en cas de besoin de façon à pouvoir modifier les paramètres de leur routeur.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-attaque-a-grande-echelle-utilise-les-browsers-pour-detourner-les-routeurs-61265.html
Par Jean Elyan

Comment s’assurer contre le cyber-risques ? | Le Net Expert Informatique

	Comment s’assurer contre le cyber-risques ?

Diverses études montrent que les entreprises sont mal préparées pour lutter contre le hacking. Les grands assureurs affinent leurs stratégies commerciales.

Sony, Home Depot, JP Morgan, TV5 Monde, Target… Le nombre d'entreprises victimes de cybercriminalité explose. Mais les couvertures d'assurance contre ce type de méfait ne font qu'émerger. Les vols de données, espionnages et autres attaques de systèmes informatiques coûtent pourtant 300 à 1000 milliards de dollars, selon la société de sécurité informatique McAfee.
La Suisse n'est pas épargnée. Dernier exemple en date: Implenia. Selon une étude récente de l'Université de Saint-Gall (https://www.alexandria.unisg.ch/Projekte/238276), plus de 90% des entreprises ont été touchées par des attaques de hackers, l'année passée. «Les PME se sentent, à tort, à l'abri. Leur protection est insuffisante», juge son auteur, Martin Eling.
Elles semblent effectivement ne pas être préparées, comme en témoigne le sondage de KPMG auprès de 64 entreprises, présenté mercredi à la presse. Son auteur, Matthias Bossardt, parle d'un «cycle de complaisance». **Plus de la moitié des sociétés interrogées croient que leur organisation est capable de détecter des attaques. Mais 45% n'ont pas de plan pour y répondre**. Même si celles-ci ne cessent de se transformer, 79% des entreprises interrogées n'ont pas changé leurs plans, ces 12 derniers mois. 7% d'entre elles n'ont même pas pris de mesure, après une attaque.

En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise
Les entreprises ne découvrent que fort tard qu'elles sont piratées. «**En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise**», explique Manuel Meier, directeur général de la division entreprises pour Zurich Insurance. Sur le plan global, le coût du cyber-risque correspond à celui des catastrophes naturelles. Mais sa complexité est supérieure. L'incendie ou l'effraction sont plus aisés à localiser et immédiatement visibles. «La cybercriminalité, dont l'origine est souvent étrangère, change la façon d'appréhender un sinistre», analyse l'assureur.
Le thème s'est imposé aux Etats-Unis, où «un tiers des entreprises ont déjà signé un contrat de cyberassurance», affirme Manuel Meier. Le marché américain est estimé à 1,3 milliard de dollars en 2013 par le rapport «Betterley», contre 150 millions d'euros en Europe continentale.
«Le cyber-risque nous préoccupe surtout depuis cinq ans», précise Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. L'importance du cyber-risque s'est accrue fortement à la suite de l'«obligation de notification», soit le devoir d'annoncer quand une infraction s'est produite, fait valoir Manuel Meier. Le client qui a été frappé par une attaque doit être averti, par exemple si les informations contenues sur sa carte de crédit ont été violées. Aux Etats-Unis, l'entreprise est pénalisée par un risque de publicité et par un coût d'information qui peut atteindre «plusieurs douzaines de millions de francs», explique Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. Son bénéfice est réduit d'autant. Les entreprises suisses actives aux Etats-Unis, ou ayant un client américain, sont directement touchées si la filiale américaine l'est, parce que l'obligation d'annonce la touche immédiatement.
A l'origine, les entreprises parlaient de sécurité «informatique». Parce que c'est le département du même nom qui était en charge du sujet. Mais elles se sont aperçues que tout leur personnel était concerné et qu'il ne suffisait plus d'avoir un pare-feu ni de changer leurs mots de passe régulièrement.
Si le hacking s'est aussi vite répandu, c'est parce que presque tous les objets sont connectés à Internet, de la voiture à la maison, multipliant les opportunités de piratages. Les risques d'intrusion dans les systèmes informatiques dépassent les produits de consommation et frappent aussi les hôpitaux et leur responsabilité civile en cas de vol de documents.
Les assurances peuvent offrir leur service habituel de transfert de risque. Mais ce dernier ne va jamais couvrir l'ensemble des cyber-risques, même s'il contribue à la réduction des coûts économiques. «Les coûts juridiques d'une attaque sont énormes», observe Manuel Meier. Une grande partie de la couverture d'assurance se concentre sur ceux-ci. «Il arrive que la couverture d'assurance soit entièrement utilisée pour les risques juridiques et qu'il ne reste rien pour la responsabilité civile», fait valoir Carine Gantenbein. L'assurance paie les coûts d'annonce et de rétablissement des données ainsi que l'interruption d'activité. Mais elle ne couvre pas les conséquences d'un piratage, comme l'absence de transaction ou la perte de confiance. Les entreprises peuvent décider de couvrir elles-mêmes les cyber-risques dans une filiale dite «captive» ou faire appel à un réassureur. La définition du prix pose toutefois problème. Il manque encore un historique. «Les assureurs sont dans une phase d'essais et d'erreurs», analyse Manuel Meier.
En outre, les risques d'interruption d'activité conduisent à des estimations compliquées, puisque tout est interconnecté. «Les clients utilisent les mêmes nuages (clouds). Si l'un d'entre eux est attaqué, certaines entreprises ne peuvent plus livrer leurs produits», explique Zurich Insurance.

Si ce marché se situe avant tout aux Etats-Unis, en raison des coûts juridiques, il devrait s'étendre à l'Europe. L'Union européenne débat aussi de l'introduction du devoir d'obligation», indique Manuel Meier. Le temps à cet effet est réduit, sous peine de sanctions supplémentaires. L'UE pourrait mettre en œuvre cette obligation en 2016. La sanction atteindrait 5% du chiffre d'affaires ou jusqu'à 100 millions d'euros.

Le marché suisse de la cyberassurance est encore minuscule, selon l'étude de l'Université de Saint-Gall, réalisée sur mandat du courtier Kessler. Il s'élève à 5 millions de francs. Mais Martin Eling est d'avis qu'il devrait décupler en cinq ans. Dans le monde, le marché devrait quintupler pour s'élever à 10 milliards de dollars.

Les assureurs répondent à ces défis en offrant une combinaison de services de prévention (pare-feu, logiciels) et de protection. C'est une chasse gardée des grands groupes internationaux. Les acteurs actifs dans ce domaine sont AIG Europe Limited, Allianz Global Corporate & Specialty AG (AGCS), Chubb Insurance Company of Europe SE, Zurich et Axa Winterthur. Les grands groupes suisses doivent souvent signer des accords de partenariat. Axa Winterthur travaille par exemple avec Nexos AG, tandis que Zurich Insurance collabore avec Kudelski.

Axa Winterthur offre des mesures de préventions et de couverture de sinistres spécifiques. Dans le cas d'une perte de données, Axa assume la réinstallation du système d'exploitation et des programmes ainsi que la récupération des données. En cas de perte de chiffre d'affaires, à l'image d'une boutique en ligne dont le système est bloqué à la suite d'une attaque et indisponible pendant trois jours, l'assureur verse le manque à gagner, déduit de la franchise.

Auprès de Zurich Insurance, l'assurance cyber-risque est définie selon le principe des modules. La composante de base est toujours la responsabilité civile, laquelle peut s'accompagner de la récupération des données et des coûts d'annonce, s'il y a des clients américains et dès 2016 européens. Elle offre aussi la couverture du risque de chantage. Le prix dépend du nombre de données sensibles et de la branche. Une petite banque est bien plus chère qu'une PME industrielle. Le tarif d'une couverture correspond à 0,6% du chiffre d'affaires, mais des changements sont fréquents. Les statistiques sont encore insuffisantes.

Au sein des entreprises, le travail de sensibilisation intègre chaque employé, selon Carin Gantenbein. Les PME n'ont pas les moyens d'établir de tels processus. L'assureur offre à ses clients des conseillers pour les sinistres, la communication et l'analyse des processus.

Pour les personnes privées, il existe une assurance cybermobbing pour les privés. L'assureur se charge d'éliminer certaines histoires répandues sur le Web. Un privé n'obtiendra pas satisfaction s'il téléphone à Google pour changer un site, explique Manuel Meier.

Et dans cinq ans? Si l'obligation de notification est introduite dans l'Union européenne, la Suisse suivra, promet le directeur de Zurich Insurance. Le marché en deviendra plus transparent. On en parlera davantage, la perception sera supérieure. Et l'offre d'assurance sera élargie.

Source : http://www.letemps.ch/Page/Uuid/01ccdc38-f4e7-11e4-bb1f-074820583190/Les_solutions_des_assureurs_face_au_cyber-risques
Par Emmanuel Garessus

87% des actes cybercriminels commis en France sont du fait

de hackers made in France | Le Net Expert Informatique

87% des actes cybercriminels commis en France sont du fait de hackers made in France

Une étude révèle que 87% des actes cybercriminels commis en France sont du fait de hackers made in France. Russes, Africains, Chinois ou Coréens seraient moins offensifs qu'on ne le pense.

La dernière étude de ThreatMetrix va secouer les idées reçues sur la cybercriminalité en France. Selon ce rapport, qui porte sur le 1er trimestre 2015, « la plus grande cyber-menace ayant pesé sur les entreprises françaises durant cette période aurait pour origine l'hexagone ».

L'étude précise que 87% des attaques sont commises depuis la France. Pour les auteurs du rapport, il ne s'agit pas de pointer la performance de la cyberdélinquance made in France, mais de noter que désormais, les attaques menées dans chaque pays sont pilotées dans leur frontière. Ce constat est « en rupture avec les tendances dominantes où la grande majorité des cyberattaques avaient pour origine la Russie, l'Asie ou l'Afrique. »
Ainsi, la France n'est donc pas une exception, mais elle exprime une véritable tendance. En Grande-Bretagne, 75% des actes cybercriminels proviennent d'Irlande ou d'Angleterre, 81% en Allemagne, 54% aux Pays-Bas, 94% en Italie et 85% en Russie.
Sur les attaques, ThreatMetrix a constaté que l'usurpation d'identité (spoofing) est devenue la plus courante. Lors des fêtes de Noël, le cabinet a dénombré 11.4 millions de tentatives de transactions frauduleuses.

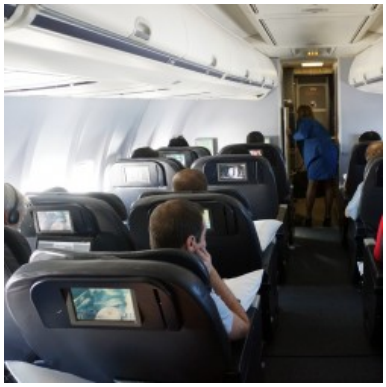
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://bfmbusiness.bfmtv.com/entreprise/les-hackers-francais-sont-les-rois-du-cybercrime-en-france-888210.html
Par Pascal Samama

Affaire United : selon le

FBI, un hacker a modifié en vol la puissance d’un réacteur – Le Monde Informatique | Le Net Expert Informatique

	Un hacker a modifié en vol la puissance d’un réacteur

Selon une note du FBI, en trois ans, le chercheur en sécurité Chris Roberts a réussi à pirater une vingtaine de fois les systèmes informatiques d'avions de ligne. Le dernier en date, sur un vol d'United Airlines entre Denver et Chicago, a entraîné son interpellation à la sortie de l'avion le 15 avril 2015.

Le FBI soupçonne aujourd'hui le chercheur en sécurité Chris Roberts, fondateur et CTO de One World Labs, d'avoir modifié la puissance d'un des réacteurs du vol d'United Airlines du 15 avril dernier entre Denver vers Chicago. M. Roberts avait été interpellé par le FBI à sa descente d'avion suite à un tweet suggérant qu'il avait scanné les systèmes informatiques (EICA) d'un Boeing 737. Cette arrestation et la saisie de tout son matériel informatique semblent faire suite à des dysfonctionnements relevés par United Airlines. Interrogé par le FBI, le chercheur, justement spécialisé dans les failles de sécurité des systèmes embarqués en aéronautique, a indiqué avoir réussi à accéder une vingtaine de fois aux systèmes informatiques d'avions de ligne.

Le 17 avril, l'agence fédérale américaine a obtenu un mandat pour perquisitionner les locaux du chercheur. Dans sa demande de mandat, le FBI révèle des informations provenant des trois interrogatoires de M. Roberts. Il n'a pas encore été accusé d'un crime, même si United Airlines l'a interdit de vol sur ses avions. On ne sait pas encore si l'incident impliquant le moteur de l'avion a eu lieu ou si l'avion aurait pu être en danger à la suite de celui-ci.

Un tweet dévastateur

Dimanche dernier, M. Roberts a écrit sur Twitter que «au cours des cinq dernières années, mon seul but a été d'améliorer la sécurité des avions … compte tenu de la situation actuelle, on m'a conseillé de ne pas en dire plus. » La défense du chercheur en sécurité est assurée par Nate Cardozo, un avocat travaillant avec l'Electronic Frontier Foundation. M. Cardozo a déclaré que son client n'était pas disponible pour commenter autre chose que ce qu'il a écrit sur Twitter.

En ce qui concerne l'incident de moteur, l'agent spécial Mark S. Hurley a écrit dans la demande de mandat que M. Roberts a indiqué qu'il avait connecté son PC portable au système de divertissement en vol (In Flight Entertainment System ou IFE) de l'avion United Airlines en utilisant le Seat Electronic Box (SEB), qui se trouve sous certains sièges passagers. Après le piratage du système IFE, il a accédé aux autres systèmes de l'avion, précise l'agent spécial. M. Roberts « a déclaré qu'il avait modifié le code du Thrust Management Computer (TMC) de l'avion pour modifier la puissance des moteurs », ajoute M. Hurley. « Il a déclaré qu'il a commandé avec succès le système pour consulter et modifier les commandes de vol (CLB ou climb command). Un des moteurs de l'avion a commencé à augmenter sa puissance, « entrainant un mouvement latéral ou sur le côté de l'avion lors d'un de ces vols », précise le mandat de perquisition. L'agent Hurley écrit encore que M. Roberts a précisé qu'il avait compromis 15 à 20 fois des systèmes IFE de 2011 à 2014. Selon l'agent spécial, les systèmes IFE compromis sont fabriqués par Thales et Panasonic (les moniteurs vidéo installés à l'arrière de sièges passagers), .

Un boitier SEB forcé sous le siège passager

Les problèmes judiciaires de Chris Roberts ont vraiment commencé le 15 avril quand il a écrit un tweet suggéré qu'il sondait les systèmes d'un Boeing 737/800 d'United Airlines lors d'un vol Denver/Chicago. Il a ensuite poursuivi son voyage de Chicago vers Syracuse (dans l'état de NY). Entretemps le département Cyber Security Intelligence d'United Airlines qui avait vu ce tweet faisant référence au système EICAS, a envoyé une équipe de sécurité interpeller M. Roberts à sa sortie de l'avion pour le remettre au FBI.

Après son interpellation, un agent spécial a examiné la cabine de première classe où avait voyagé M. Roberts vers Chicago. Les boitier SEB sous les sièges 2A et 3A montraient des signes d'effraction. « Le SEB sous le siège 2A a été endommagé » indique le mandat de perquisition. « L'enveloppe extérieure de la boîte a été ouverte d'environ 1,27 cm, et une des vis de fixation était manquante ». Redevenu très prudent, M. Roberts a affirmé aux agents du FBI qu'il n'avait pas compromis le réseau de l'avion sur le vol à destination de Chicago, selon le mandat. En février et mars dernier, le FBI avait déjà interrogé Chris Roberts qui avait également affirmé avoir réussi à pirater les systèmes IFE à bord d'avions.

Cette affaire devrait en n'en pas douter, impacter le monde de la sécurité aérienne dans les prochains mois, voire années, et aboutir au renforcement des règles dans ce domaine.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-affaire-united%C3%82%C2%A0-selon-le-fbi-un-hacker-a-modifie-en-vol-la-puissance-d-un-reacteur-61170.html
Par Serge Leblal avec IDG NS

Les PME connaissent les risques informatiques mais ne

réagissent pas| Le Net Expert Informatique

Les PME connaissent les risques informatiques mais ne réagissent pas

Bien que les petites et moyennes entreprises soient conscientes des menaces qui pèsent sur leurs systèmes d'information, le baromètre Ipsos-Navista montre qu'elles ne consacrent qu'un budget dérisoire à leur protection.

Une récente étude menée par Ipsos-Navista auprès des PME françaises indique que 99% d'entre elles sont équipées en informatique et que les postes clients et terminaux mobiles qu'elles utilisent sont connectés à Internet. 82 % des entreprises interrogées permettent à leurs salariés de se connecter à n'importe quel site web. Elles sont en outre 80% à voir des terminaux mobiles utilisés dans leurs murs et à leur donner accès à leur réseau dans 2 cas sur 3. Autant dire qu'elles laissent la porte grande ouverte aux menaces de tous types. Pourtant, 9 sociétés sur 10 évaluent bien l'usurpation des mots de passe et l'utilisation frauduleuse ou malveillante de leurs ressources informatiques comme un risque. Par ailleurs, 76% des gérants se savent pénalement responsables de l'utilisation d'internet dans leur entreprise.

Une PME sur deux n'a pas de pare-feu

Malgré ce contexte de fort équipement, d'accès ouvert au web et de conscience des risques, les PME françaises sont loin de faire ce qu'il faut pour se protéger. Elles sont par exemple une grande majorité à utiliser la messagerie native de leur FAI, ou un web mail peu sécurisé. Plus grave encore sur le plan juridique, les trois quarts d'entre elles sont incapables de dire où sont sauvegardées les pièces-jointes échangées avec leurs clients, sans garantie de confidentialité. La liste égrenée par l'étude Ipsos-Navista ne s'arrête pas là. Elle précise aussi que 26% des petites et moyennes entreprises ne possèdent pas d'anti-virus, qu'elles ne sont que 36 % à utiliser un antiphising et 52 % un pare-feu.

50€ par an et par salariés pour la sécurité

Dans ces conditions, on comprend pourquoi le budget annuel que les PME allouent par employé à la sécurité informatique n'excède pas les 50€ par an pour plus de la moitié d'entre elles. L'étude relève que la « légèreté de ce budget est à considérer au regard des sommes que coûteraient en moyenne une violation des données de l'entreprise, pouvant atteindre parfois plusieurs millions d'euros ». 11 % des entreprises interrogées déclarent avoir déjà été victimes d'actes de malveillance. Un chiffre qui ne prend pas en compte les sociétés qui n'ont pas rendu publique les attaques dont elles ont fait l'objet ni celles qui ne s'en sont pas aperçu.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Vous souhaitez participer à une de nos formations ?
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.distributique.com/actualites/lire-securite-les-pme-connaissent-les-risques-mais-ne-reagissent-pas-23077.html

Enjeux et défis du web profond | Le Net Expert Informatique

Enjeux et défis du web profond

Le web profond (Deep Web) désigne le sous-ensemble d'internet qui n'est pas indexé ou mal indexé par les grands moteurs de recherche comme Google, Yahoo ou Bing,…On sait que cet ensemble de données reste difficilement mesurable mais qu'il occupe un espace très supérieur à celui de l'ensemble des sites web bien indexés par les moteurs classiques. Certaines études avancent un ratio de 80% de Deep Web contre 20% de web de surface à l'image de la partie immergée d'un iceberg…

Profond comme le web

Le contenu du deep web demeure hétérogène. On y trouve de grandes bases de données, des bibliothèques volumineuses non indexées par les moteurs en raison de leur tailles, des pages éphémères, mal construites, à très faible trafic ou volontairement rendues inaccessibles par leurs créateurs aux moteurs traditionnels.
D'après une étude récente de la Darpa, l'agence américaine en charge des projets de défense, plus de 60 millions de pages à vocation criminelle ont été publiées depuis deux ans dans les profondeurs du web. Les moteurs de recherche classiques, Google en tête, utilisent des algorithmes d'indexation dérivés du puissant Pagerank qui s'appuient sur une mesure de popularité du site ou de la page.
Cette approche qui a fait le succès de Google va de fait exclure les pages à faible trafic, éphémères ou furtives. Ce sont précisément ces pages qui sont utilisées par les acteurs de la cybercriminalité pour diffuser de l'information tout en restant sous les radars des grands moteurs. Lorsque cette information concerne une activité criminelle, c'est dans le Dark Web qu'elle sera dissimulée et rendue accessible aux seuls clients potentiels via des outils d'anonymisation spécialisés comme Tor. Le web profond réunit donc de la donnée légitime, souvent de haute qualité lorsqu'il s'agit de bases de données scientifiques volumineuses peu ou mal indexées par les moteurs.
Il réunit de la donnée sécurisée accessible seulement par mot de passe mais aussi de la donnée clandestine issue de trafics et d'activités criminelles. Cet ensemble informationnel hétérogène intéresse depuis longtemps les grands acteurs du numérique, chacun avec une motivation spécifique. L'accès au web profond constitue un élément stratégique du dispositif global de lutte contre la cybercriminalité qui reste l'une des grandes priorités de l'administration américaine. Les efforts pour obtenir des capacités de lecture du web profond se sont concrétisés avec le développement en 2014 du moteur de recherche Memex tout droit sorti des laboratoires de la Darpa.

Memex, le moteur Darpa

Dans son communiqué officiel publié le 9 février 2014 [1], l'agence Darpa décrit Memex comme « le moteur qui révolutionne la découverte, l'organisation et la présentation des résultats de recherche en ligne. Le programme Memex imagine un nouveau paradigme, où il est possible d'organiser rapidement et intelligemment un sous-ensemble de l'internet adapté à l'intérêt d'une personne ».

Le moteur est construit autour de trois axes fonctionnels:
1. l'indexation de domaines spécifiques,
2. la recherche de domaines spécifiques
3. la mise en relation de deux premiers axes

Après plus d'un an d'utilisation en phase de test par les forces de l'ordre américaines, Memex a permis de démanteler un réseau de trafiquants d'êtres humains. Durant la finale du Super Bowl, Memex a servi pour détecter les pages associées à des offres de prostitution. Ses outils d'analyse et de visualisation captent les données invisibles issues du web profond puis tracent la graphe des relations liant ces données. De telles fonctionnalités s'avèrent très efficaces pour cartographier des réseaux clandestins de prostitution en ligne.

D'après les récents communiqués de la Darpa, Memex ne traite pour l'instant que les pages publiques du web profond et ne doit donc pas être associé aux divers outils de surveillance intrusifs utilisés par la NSA. A terme, Memex devrait offrir des fonctionnalités de crawling du Dark Web intégrant les spécificités cryptographiques du système Tor. On peut raisonnablement imaginer que ces fonctions stratégiques faisaient bien partie du cahier des charges initial du projet Memex dont le budget est estimé entre 15 et 20 millions de dollars… La Darpa n'est évidemment pas seule dans la course pour l'exploration du web profond. Google a parfaitement mesuré l'intérêt informationnel que représentent les pages non indexées par son moteur et développe de nouveaux algorithmes spécifiquement adaptés aux profondeurs du web.

Google et le défi des profondeurs

Le web profond contient des informations provenant de formulaires et de zones numériques que les administrateurs de sites souhaitent maintenir privés, hors diffusion et hors référencement. Ces données, souvent très structurées, intéressent les ingénieurs de Google qui cherchent aujourd'hui à y avoir accès de manière détournée. Pour autant, l'extraction des données du web profond demeure un problème algorithmiquement difficile et les récentes publications scientifiques des équipes de Google confirment bien cette complexité. L'Université de Cornell a diffusé un article remarquable décrivant une infrastructure de lecture et de copie de contenus extraits du web profond [2],[3].

L'extraction des données s'effectue selon plusieurs niveaux de crawling destinés à écarter les contenus redondants ou trop similaires à des résultats déjà renvoyés. Des mesures de similarités de contenus sont utilisées selon les URL ciblées pour filtrer et hiérarchiser les données extraites. Le système présenté dans l'article est capable de traiter un grand nombre de requêtes sur des bases de données non adressées par le moteur de recherche classique de Google [4].

A moyen terme, les efforts de Google permettront sans aucun doute de référencer l'ensemble du web profond publiquement accessible. Le niveau de résolution d'une requête sera fixé par l'utilisateur qui définira lui même la profondeur de sa recherche. Seuls les contenus privés cryptés ou accessibles à partir d'une identification par mot de passe demeureront (en théorie) inaccessibles à ce type de moteurs profonds.

Vers une guerre des moteurs?

Les grandes nations technologiques ont pris en compte depuis longtemps les enjeux stratégiques de l'indexation des contenus numériques. Peu bruyante, une « guerre » des moteurs de recherche a bien lieu aujourd'hui, épousant scrupuleusement les contours des conflits et les concurrences de souverainetés nationales. La Chine avec son moteur Baidu a su construire très tôt son indépendance informationnelle face au géant américain.

Aujourd'hui, plus de 500 millions d'internautes utilisent quotidiennement Baidu à partir d'une centaine de pays. La Russie utilise massivement le moteur de recherche Yandex qui ne laisse que peu de place à Google sur le secteur du référencement intérieur russe puisqu'il détient plus de 60% des parts du marché national. En 2014, Vladimir Poutine a souhaité que son pays développe un second moteur de recherche exclusivement contrôlé par des capitaux russes et sans aucune influence extérieure. Plus récemment, en février 2015, le groupe Yandex a déposé une plainte contre Google en Russie pour abus de position dominante sur les smartphones Android. Yandex reproche en effet à Google de bloquer l'installation de ses applications de moteur de recherche sur les smartphones fonctionnant sous Android. Les constructeurs sont contraints aujourd'hui à pré-installer sur leurs machines les Google Apps et à utiliser Google comme moteur par défaut sous Android…

Le moteur face aux mégadonnées

La course à l'indexation des contenus du web profond apparaît comme l'une des composantes stratégiques de la guerre des moteurs. Si la géopolitique des données impose désormais aux nations de définir des politiques claires de stockage et de préservation des données numériques, elle commande également une vision à long terme de l'adressage des contenus. La production mondiale de données dépassera en 2020 les 40 Zo (un zettaoctet est égal à dix puissance vingt et un octets). L'évolution de cette production est exponentielle: 90% des données actuelles ont été produites durant les deux dernières années. Les objets connectés, la géolocalisation, l'émergence des villes intelligentes connectées et de l'information ubiquitaire contribuent au déluge de données numériques. La collecte et l'exploitation des mégadonnées (le terme officiel français à utiliser pour big data) induiront le développement de moteurs polyvalents capables d'indexer toutes les bases de données publiques quelle que soient leurs tailles et leurs contenus.

Le moteur de recherche doit être considéré aujourd'hui comme une infrastructure de puissance stratégique au service des nations technologiques. Qu'attend l'Europe pour développer le sien?

_____

[1] La présentation du moteur Memex par l'agence Darpa
http://www.darpa.mil/newsevents/releases/2014/02/09.aspx
[2] « Google's Deep-Web Crawl » – publication de l'Université Cornell
http://www.cs.cornell.edu/~lucja/publications/i03.pdf
[3] « Crawling Deep Web Entity Pages » – publication de recherche, Google
http://pages.cs.wisc.edu/~heyeye/paper/Entity-crawl.pdf
[4] « How Google May index Deep Web Entities »
http://www.seobythesea.com/2015/04/how-google-may-index-deep-web-entities/

Source : http://www.huffingtonpost.fr/thierry-berthier/enjeux-et-defis-deep-web_b_7219384.html
Par Thierry Berthier

Propriétaires de sites WordPress : attention aux »script-kiddies » pro-Etat Islamique | Le Net Expert Informatique

Le FBI alerte sur les attaques continues de défacement visant des sites Internet. Les victimes ont en commun d'utiliser des plugins WordPress vulnérables. Quant aux auteurs, ils utilisent le nom de l'EI par souci de visibilité.

En janvier, suite aux attentats en région parisienne, de très nombreuses attaques de défacement de sites Web avaient été constatées. Ces opérations de cybervandalisme étaient revendiquées par des partisans des islamistes radicaux, et notamment de l'Etat Islamique (Daesh).
« La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service (DDoS) qui exploitent les failles de sécurité de sites vulnérables » précisait alors l'Anssi.

Des cibles choisies pour leur usage de plugins WordPress
De telles attaques se poursuivent et pas seulement en France. Et elles ont souvent une cible de prédilection : les sites WordPress. Les Etats-Unis, par l'intermédiaire du FBI, viennent d'ailleurs de publier un bulletin de sécurité concernant ces attaques.
Certes, note le FBI, ces « défacements traduisent un faible niveau de sophistication » mais ils s'avèrent néanmoins coûteux en raison des pertes d'activité et des dépenses qu'ils génèrent afin de réparer les systèmes infectés.
Quant aux victimes de ces intrusions, elles sont très diverses. Et pour cause puisque les attaquants ciblent moins les propriétaires des sites que la plateforme technique de ceux-ci. Les victimes ont un point commun : l'utilisation de plugins WordPress vulnérables.

Les pirates pas membres de Daesh
« Le FBI estime que les auteurs ne sont pas des membres de l'organisation terroriste Etat Islamique. Ces individus sont des hackers exploitant des méthodes relativement simples afin d'exploiter des vulnérabilités techniques et utilisent le nom ISIS pour gagner plus de notoriété que l'attaque sous-jacente aurait autrement recueilli. »
C'était déjà l'analyse publiée par ZDNet en janvier. « Nous n'avons constaté aucune excentricité ou coordination dans les attaques, ni de déni de service bien outillé » confiait Loïc Guézo, expert en sécurité chez Trend Micro. « Le résultat est surtout visuel, c'est une volonté de communiquer » par des défacements.
Quant au profil des attaquants, il était « plutôt celui de personnes avec des compétences de base, au sens de la gestion du PC et de certains outils » ajoutait-il. Ils s'apparenteraient ainsi à des « script kiddies » plutôt qu'à des hackers chevronnés.

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

Source : http://www.zdnet.fr/actualites/proprietaires-de-sites-wordpress-attention-aux-script-kiddies-pro-etat-islamique-39817644.htm
Par Christophe Auffray