Les offres d’essai Cloud pour avoir un superordinateur gratuit ! Une idée qui va faire des eMules…

Les offres d’essai Cloud pour avoir un superordinateur gratuit ! Une idée qui va faire des eMules…

Un botnet gratuit ? C’est l’expérimentation menée par deux chercheurs américains, Rob Ragan et Oscar Salazar. Plutôt que de se fatiguer à infecter des centaines d’ordinateurs appartenant à des utilisateurs peu soucieux de leur sécurité, ils ont décidé de se tourner vers les services Cloud qui proposent généralement tous un service gratuit à l’essai.

À l’aide d’un script, ils ont donc généré des comptes d’essai sur plus de 150 services Cloud tels que Amazon Web Service, puis en utilisant Python Fabric, une librairie permettant de gérer de multiples scripts pythons, ils se sont amusés à utiliser la puissance de calcul ainsi accumulée pour plusieurs expériences.

Un déficit de sécurité

Ils ont ainsi commencé par miner du Litecoin, une cryptomonnaie reposant sur un principe similaire à celui du Bitcoin. Après un test de plusieurs heures, les chercheurs sont parvenus à dégager une rapide estimation de ce que leur

botnet Cloud pourrait leur rapporter : environ 1750 dollars par semaine. « On a construit un superordinateur sans lâcher un centime » explique Rob Ragan dans les colonnes de Wired « Et en s'épargnant même la facture d'électricité ! » précise-t-il.

Pour tester les capacités de ces fournisseurs de service, les deux chercheurs expliquent avoir laissé une partie de leurs scripts dédiés au minage de Litecoin tourner pendant deux semaines, sans qu'ils ne soient inquiétés. Autre utilisation également envisagée : le DDos, qui selon leurs estimations équivaudrait à une attaque provenant lancée depuis un botnet de 20.000 ordinateurs

Une dérive inquiétante

Un botnet basé sur le Cloud, cela n'est pas réellement nouveau : des cas similaires avaient émergés, notamment autour de l'utilisation du malware Zeus. Mais le but de l'expérience est ailleurs : d'une part, les deux chercheurs veulent avant tout alerter les entreprises qui proposent ce type de service sur les risques auxquels ils s'exposent en proposant ainsi des offres gratuites et ne nécessitant pas d'authentification forte.

Mais surtout, cela pose la question de la légalité de ce type de botnet : certes, les chercheurs sont passés outre quelques termes des CGV de ces différents services, mais le risque encouru est nettement moindre qu'un botnet reposant sur des ordinateurs infectés.

Lors d'une conférence à l'événement Black Hat qui aura lieu début aout, les chercheurs détailleront avec plus de précisions les outils et méthodes utilisées pour construire ce superordinateur à peu de frais.

Cet article vous à plu ? Laissez-nous un commentaire (Source

de progrès)

Références :
http://www.zdnet.fr/actualites/un-superordinateur-base-sur-des-offres-d-essai-cloud-39804301.htm

---

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Par le biais d'un email anonyme, un pirate a tenté d'extorquer de l'argent à la BCE en échange de données dérobées dans une base de données liée au site Web de la Banque centrale. Les données de marché sensibles n'ont pas été compromises.

Dans un communiqué, la BCE, la Banque centrale européenne, responsable de la monnaie unique au sein de l'UE, alerte sur le vol d'une base de données de contacts. Selon La Tribune, ce sont potentiellement 20.000 personnes dont les données pourraient être ainsi exposées.

La BCE précise que seules des informations de contacts, dont des adresses email, des noms et coordonnées, ont été dérobées dans cette base de données isolée de son système interne. « Aucune donnée sensible de marché n'a été compromise » assure ainsi la Banque centrale.

Des données partiellement chiffrées

Cette base de données est attachée au site Web de la BCE et contient l'identité des personnes inscrites à des évènements organisés par la Banque, dont ses conférences. Celle-ci précise que seule une partie des données volées sont chiffrées – la nature de ce chiffrement n'est pas mentionnée.

La BCE contacte actuellement l'ensemble des personnes dont les données pourraient ainsi avoir été compromises et a, par précaution, réinitialisé l'ensemble des mots de passe. Une vulnérabilité, non spécifiée mais corrigée selon la BCE, serait à l'origine du vol.

Et comment la Banque centrale a-t-il pris connaissance de cette intrusion informatique ? Grâce à un email anonyme, n'émanant toutefois pas d'un bienfaiteur. Au contraire, l'auteur du message a exigé de l'argent en échange des données subtilisées. La justice allemande – le siège de la BCE est à Francfort – a été saisie et une enquête de police a été ouverte.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.zdnet.fr/actualites/vol-de-donnees-et-racket-aupres

-de-la-banque-centrale-europeenne-39804225.htm

Les clients de 12 banques suisses attaqués par des cybercriminels

Les clients de 12 banques suisses attaqués par des cybercriminels

Des pirates informatiques se sont lancés, depuis peu, dans une attaque d'envergure contre les comptes e-banking de douze banques suisses. Leurs méthodes sont perfides et laissent peu de traces, avertit Switch.

Le virus, de type cheval de Troie, a été nommé Retefe, a indiqué mardi Serge Droz, expert en sécurité auprès de l'organisme qui administre les noms de domaines en Suisse. Il confirmait une information parue sur le site Internet de la Handelszeitung. C'est l'entreprise de sécurité informatique Trend Mikro qui a rendu publique l'information sur l'attaque.

Le client de banque ouvre un spam – un courrier électronique indésirable – qui libère le virus. Le programme malicieux

s’efface, une fois que l’infection a réussi. Aussitôt que le client ouvre une session e-banking, il est redirigé sur un mauvais serveur, sur lequel apparaît une copie de page Internet de sa banque. Le client entre alors ses informations de sécurité, qui sont désormais en main des malfaiteurs.

Lire la suite…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lematin.ch/economie/hackers-s-attaquent-clients-12-banques-suisses/story/16520131

Une manière de nous espionner sur Internet sans laisser de traces !

Une manière de nous espionner sur Internet sans laisser de traces !

Depuis plusieurs années, le mécanisme de suivi des internautes qui récupère votre « empreinte numérique » est utilisé par la société AddThis. Il serait installé sur plus de 5000 sites Web parmi les plus consultés, et surtout difficilement contournable.

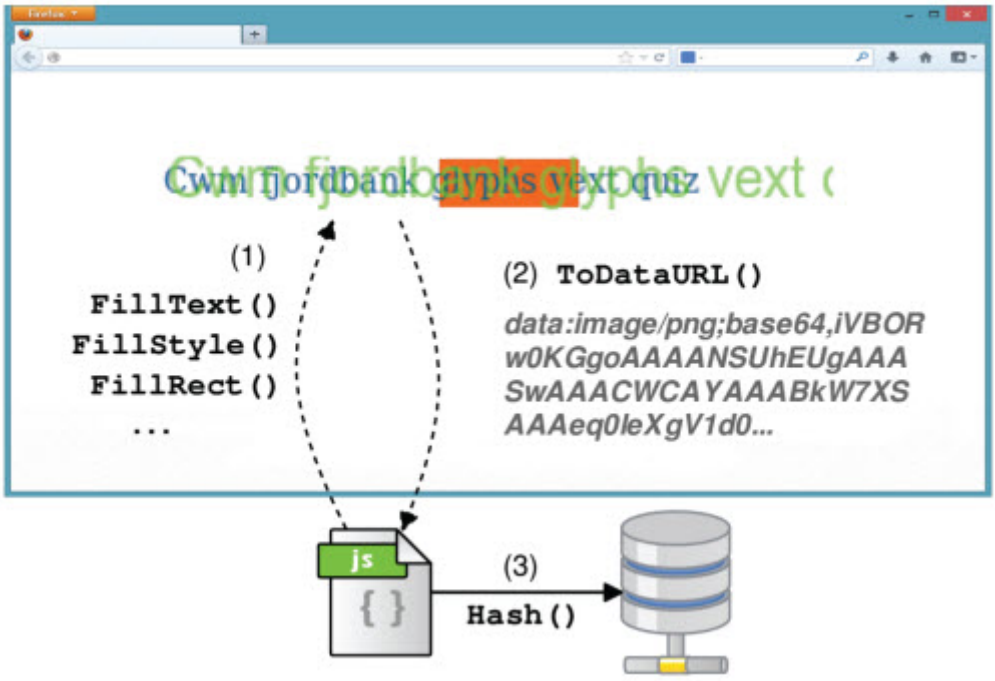
Atlantico, MetroNews, Letudiant, PAP, Telerama, Sports, Elle, LeGorafi… Ce sont autant de sites qui utilisent le fameux mécanisme d'empreinte numérique (la liste entière est consultable ici). Ce ne sont que quelques exemples français. Aux Etats-Unis, le site de la Maison-Blanche l'utilise également. S'il n'est pas tout à fait nouveau, il a été découvert assez récemment par des chercheurs des universités de Ku Leuven en Belgique, et de Princeton outre-Atlantique.

La nouveauté : il permet de traquer les internautes sans qu'ils s'en rendent compte et sans pouvoir y échapper. Car aucun mécanisme, une application tierce par exemple, ne permet de la contourner : le Graal pour les annonceurs, un fléau pour la vie privée ! Il existe toutefois des moyens d'y échapper, en bloquant le chargement des JavaScript sur votre navigateur, en utilisant NoScript par exemple, en choisissant Tor ou l'extension (expérimentale) Chameleon.

Le mécanisme de fonctionnement de l'empreinte numérique.
Cette technique d'empreinte numérique, décrite par des chercheurs californiens en 2012 (consultez le PDF du détail de la technique), est notamment proposée dans les outils de la société AddThis, qui fournit entre autres des boutons de partage vers les réseaux sociaux.

Le système est très simple en théorie. Lorsqu'un internaute se connecte sur un site Web, une requête est envoyée demandant au

navigateur de « dessiner » une image invisible qui est ensuite transmise à AddThis par exemple. Il utilise la fonction Canvas de HTML5 (« canvas fingerprinting »). Et c'est grâce à cette image unique qu'il est possible de pister discrètement et individuellement chaque internaute.



Dans cet article, on peut y voir AddThis reconnaître avoir commencé à tester ce système depuis le début de l'année cherchant « une alternative aux cookies traditionnels ». Depuis la publication de l'article, certains sites ont fait marche arrière, à l'instar de YouPorn notamment.

Le PDG de l'entreprise estime que le mécanisme est tout à fait légal, même si les premiers résultats ne seraient pas satisfaisants, selon lui. AddThis se défend sur son blog, expliquant que le mécanisme est utilisé uniquement dans un but de R&D. Il nous tarde de connaître la réaction de la CNIL : un mécanisme divulgué à tous et incontournable semble difficile à imposer en toute légalité…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.linformaticien.com/actualites/id/33713/tous-traques-addthis-nous-suit-a-la-trace-sans-laisser-de-traces.aspx

---

Les entreprises sous-estiment le risque juridique du Big Data

Pour le Boston Consulting Group (BCG) et le cabinet d'avocats DLA Piper dans leur étude sur « Le Big Data face au défi de la confiance » publiée le 18 juillet 2014, l'exploitation de très nombreuses données peut exposer l'entreprise à des risques juridiques et économiques méconnus.

De fait, ils constatent que la surveillance exercée à grande échelle par la NSA sur les communications électroniques et téléphoniques, la navigation sur Internet et les réseaux privés ou encore les services de Cloud américains et étrangers, a heurté un public déjà très sensibilisé aux problématiques de protection des données. Ils rappellent que « certains acteurs clés d'Internet comme Google et Facebook ont été violemment critiqués après avoir modifié leurs règles de confidentialité ».

De plus, ils relèvent que la nouvelle réglementation européenne en cours d'élaboration aura « des incidences certaines sur les entreprises utilisant le Big Data (…). Le poids et le coût administratif du traitement de données pourraient augmenter. Cet ensemble de règles nouvelles pourrait aussi constituer une menace pour les stratégies de monétisation de données, diminuer l'innovation et réduire les opportunités futures ».

« Le Big Data face au défi de la confiance », 18 juill. 2014 ; Site de BCG

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124969/Default.aspx

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL autorise la collecte de prévention de la délinquance pour les Collectivités locales

La CNIL a adopté une nouvelle autorisation unique n° AU-038 par une délibération du 26 juin 2014 « portant autorisation unique concernant les traitements de données relatifs aux personnes faisant l'objet d'un suivi par le maire dans le cadre de ses missions de prévention de la délinquance ».

Cette autorisation unique encadre uniquement les traitements mis en œuvre dans le cadre du fonctionnement des groupes relevant directement des pouvoirs du maire en la matière comme les conseils locaux de sécurité et de prévention de la délinquance (CLSPD) et les conseils pour les droits et devoirs des familles (CDDF).

Pour les traitements concernés, la délibération de la CNIL précise les finalités exactes qui peuvent être poursuivies et les utilisations qui doivent être exclues, notamment

l’alimentation d’autres traitements locaux ou de fichiers nationaux.

Elle établit une liste limitative des données qui peuvent être collectées dans le cadre de ces fichiers et prévoit des conditions supplémentaires pour le traitement de certaines données sensibles du point de vue de la protection des données personnelles.

Elle liste également les seules personnes habilitées à connaître des informations collectées dans le cadre de la prévention de la délinquance, en distinguant les personnels pouvant disposer d’un accès direct aux traitements mis en œuvre, des personnes à qui ces informations peuvent être communiquées, pour certaines de manière ponctuelle uniquement.

L’autorisation unique n° AU-38 prévoit enfin une durée de conservation limitée, des modalités particulières d’information des personnes concernées ainsi que des mesures de sécurité adaptées à la sensibilité des traitements mis en œuvre.

Délib. CNIL n° 2014-262, 26 juin 2014, JO 22 juill. ; Site de la CNIL

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/124981/Default.aspx

Les objets connectés à notre e-santé dévoilent nos données personnelles

Les objets connectés à notre e-santé dévoilent nos données personnelles

Alors que la présence du wearable (ensemble des vêtements et accessoires comportant des éléments informatiques et électroniques avancés) croît rapidement et avec elle, la collecte d'informations de santé, la Commission fédérale du commerce américain s'inquiète de ce que peuvent devenir ces données très personnelles.

Samsung a SAMI, Apple a Healthkit Google a Google Fit.

Trois grands noms des smartphones et trois approches de l'e-santé qui ont pour point commun de recueillir, formaliser et stocker vos données de santé sur votre téléphone ou sur des serveurs.

Quoi de plus personnel que votre état de santé et ses indicateurs ? Quoi de plus précieux et éventuellement de plus

valorisés pour fournir des services complémentaires ?

Julie Brill, commissaire au sein de la Commission fédérale du commerce (FTC) s'inquiétait en tout cas de l'accélération de cette tendance qui va prendre encore plus d'importance avec la multiplication des montres et bracelets connectés. Pour elle, la façon dont les données sont « siphonnées » par ces applications est préoccupante. « Nous ne savons pas où ces informations vont en définitive », indiquait-t-elle devant un groupe de discussion organisé par le site politique The Hill. « Cela met les consommateurs dans une situation inconfortable », continuait-elle. La Commissaire a souligné devant le Congrès l'importance de voter une loi pour interdire la collecte d'informations personnelles sous de faux prétextes.

Le besoin de régulation ?

En mai dernier, la FTC rendait un rapport dans lequel elle indiquait qu'une bonne part des développeurs d'applications d'e-santé donnait accès aux données de santé collectées à des sociétés extérieures. Ainsi, l'étude menée sur douze applications de fitness et e-santé démontrait que ces informations électriques étaient partagées avec 76 entreprises différentes, y compris pour du marketing.

Face à un paysage si inquiétant et totalement dépourvu de cadre légal, la commissaire de la FTC s'inquiète que « personne ne parle de nouvelle réglementation ».

L'ACT, Association for Competitive Technology, lobby qui défend les intérêts des développeurs d'applications, craint

évidemment qu'une quelconque réglementation nuise à l'innovation. Morgan Reed, directeur exécutif de l'ACT, déclarait ainsi à l'occasion de ce groupe de discussion : « L'industrie de la santé mobile a besoin d'éduquer la FTC sur les apports positifs que peut avoir la collecte d'informations sur la santé. […] Si nous échouons dans ce rôle, la commission pourrait prendre des décisions qui pourraient dévaster les développeurs d'applications ».

Ci-dessous à la 34ème minute, Julie Brill, commissaire au sein de la Commission fédérale du commerce.

http://www.ustream.tv/recorded/50427445

Si les bénéfices de la surveillance régulière de notre santé sont indéniables, il va une fois encore faire attention à ne pas devenir un produit dans la stratégie marketing d'acteurs peu soucieux de nos vies privées. Pour éviter ces pièges, Julie Brill préconise qu'un gros effort pédagogique soit fourni, d'une part et d'autre part que les utilisateurs soient toujours informés des informations recueillies et partagées. Un effort de transparence pour les plus personnelles de nos données…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.01net.com/editorial/624302/e-sante-debut-de-la-bataille-pour-nos-donnees-entre-la-ftc-et-les-lobbies/#?xtor=EPR-1-NL-01net-Actus-20140724

Cybercriminalité : La Tunisie dispose de compétences hautement qualifiées pour lutter contre le terrorisme

La Tunisie dispose de compétences hautement qualifiées dans le domaine des technologies de l'information et de la communication (TIC) capables de protéger l'espace cybernétique de la Tunisie et de lutter contre la cybercriminalité et contre le terrorisme et la violence ». C'est en tout cas ce que vient de déclarer à l'agence TAP, le ministre de l'Enseignement supérieur, de la Recherche scientifique et des TIC, Taoufik Jelassi, en marge de la conférence participative sur la réforme de l'enseignement supérieur et l'employabilité, organisée dans la soirée du dimanche 20 juillet à Monastir.

M. Jelassi a soutenu que la sécurité informatique et cybernétique est une priorité nationale, notamment au cours de cette étape, ajoutant qu'il a été convenu, au terme d'une réunion, la semaine dernière avec des responsables de la sécurité de l'espace cybernétique, de soutenir davantage l'Agence technique des télécommunications (ATT). « L'agence assurera l'appui technique des investigations judiciaires dans le domaine de la cybercriminalité et appuiera les efforts des autorités judiciaires et sécuritaires dans la protection du pays », a-t-il dit.

Le ministre des TIC a par ailleurs indiqué que l'Agence technique des télécommunications veille sur la protection des citoyens et des intérêts supérieurs du pays 24h/24 et 7jours/7, conformément à la loi et sous contrôle judiciaire.

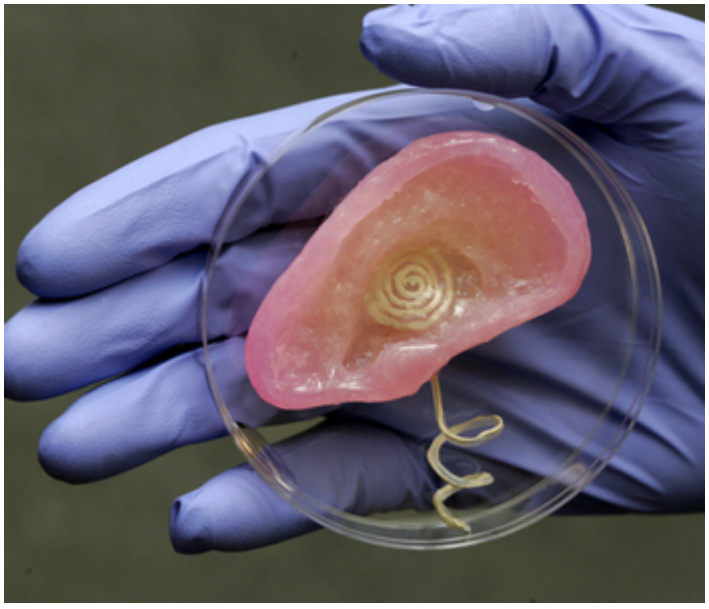
A noter que l'agence technique des télécommunications a été créée en vertu du décret 4506 en date du 6 novembre 2013..

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.webmanagercenter.com/actualite/technologie/2014/07/21/152736/terrorisme-la-tunisie-dispose-de-competences-hautement-qualifiees-pour-lutter-contre-le-terrorisme

Une oreille bionique fabriquée avec une imprimante 3D



Une oreille bionique fabriquée avec une imprimante 3D

Une équipe de chercheurs de l'université de Princeton a imprimé une oreille bionique mi-électronique mi-cartilage. © Frank Wojciechowski

En combinant l'impression 3D de matériaux électroniques, de plastique et de cartilage, des chercheurs de l'université de Princeton ont réussi à créer une « oreille » bionique. Cette oreille est capable de percevoir des fréquences inaudibles par un humain normal et ouvre donc la voie à des organes « augmentés », se réjouissent les chercheurs auteurs de cet exploit.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.journaldunet.com/economie/magazine/creations-en-3d/oreille-bionique.shtml

---

Le «Wall Street Journal» victime d’une cyberattaque – News High-Tech: Web – 24heures.ch

Le «Wall Street Journal» victime d’une cyberattaque

Le «Wall Street Journal» a annoncé dans la nuit de mardi avoir été victime d'une cyberattaque par un hacker qui proposait de vendre des codes d'accès au serveur du journal économique américain.

Dans son édition en ligne, le quotidien des affaires Wall Street Journal, indique que son service infographie a été «piraté par des tierces parties» tout en affirmant qu'aucun «dommage» n'a pour l'heure été constaté.

«A ce stade, nous ne voyons aucune preuve d'un quelconque impact sur les clients de Dow Jones ou sur les informations personnelles des clients», a assuré une porte-parole du journal, citée dans l'article.

Aucune altération sur des infographies (chartes, tableaux…) n'a par ailleurs été relevée mais le système est encore «en cours d'examen», assure le journal, précisant que plusieurs ordinateurs ont été mis hors ligne afin d'«isoler» les attaques.

Le Wall Street Journal (WSJ) dit avoir révélé cette intrusion informatique après sa «revendication» sur Twitter par un hacker qui offrait, moyennant finances, des informations de clients mais également des données permettant d'accéder au serveur du journal.

Selon Andrew Komarov, l'expert en cybersécurité qui a alerté le quotidien, un tel accès permettrait de «modifier des articles, d »ajouter des nouveaux contenus (…) et de supprimer des comptes d'utilisateurs».

Selon le WSJ, Andrew Komarov, patron de la firme californienne IntelCrawler, est sur les traces de ce pirate informatique qui s'est successivement fait connaître sous le pseudonyme de Rev0lver et de Worm et qui a fondé un marché noir des «failles informatiques» baptisé Worm.in.

Les Etats-Unis ont à plusieurs reprises alerté sur les dangers de la cybercriminalité et de son impact économique. Mi-juillet, le secrétaire au Trésor américain Jacob Lew avait ainsi affirmé qu'une cyberattaque «réussie» pourrait menacer la stabilité financière du pays.

Lire