Augmentation de la cybercriminalité encore prévu pour 2016

Augmentation de la cybercriminalité encore prévu pour 2016

Le nombre de piratages informatiques a substantiellement augmenté en 2015, une tendance qui devrait encore s'affirmer en 2016. Chefs d'Etat, groupes industriels, médias, banques, petites entreprises ou particuliers, personne n'est à l'abri de la menace.

Si les cyber-attaques (attaques informatiques, ndlr) ont augmenté durant l'année 2015 en France et dans le monde, la tendance ne semble pas près de s'atténuer en 2016. C'est la mise en garde prononcée par de nombreux organismes, dont le Cercle européen de la sécurité et des systèmes d'information. Cet organe, qui fédère les professionnels du secteur de la sécurité informatique, redoute un cyber-sabotage de grande ampleur en 2016.
Difficile cependant de cerner le danger car il vient de partout, emploie des formes diverses et peut toucher tout le monde, directement ou pas. A grande échelle, une attaque déclenchée à distance peut viser des objectifs affectant des bassins entiers de population : réseau électrique, distribution de l'eau, contrôle de la circulation, trafic aérien. Ou encore s'en prendre à des organismes gouvernementaux avec les conséquences que cela implique.

Des attaques en forte hausse

L'Allemagne a eu affaire à ces deux types d'attaques ces douze derniers mois: la mise hors service par deux fois d'un haut-fourneau dans la Sarre et le piratage de l'ordinateur personnel d'Angela Merkel. En France, l'exemple le plus spectaculaire remonte au printemps dernier quand la chaîne francophone TV5Monde (257 millions de foyers à travers le monde) a carrément cessé d'émettre durant plusieurs heures après une attaque perpétrée par Daech.

TV5 Monde avait été ouvertement ciblée par Daech. REUTERS/Benoit Tessier

A moyenne échelle, les malfaiteurs peuvent s'en prendre à une entreprise pour lui voler des données ou gripper son système informatique. Le cabinet PricewaterhouseCoopers révélait en octobre dernier que les cyber-attaques contre les entreprises avaient progressé de 38 % en un an dans le monde et de 51 % en France alors que les pertes financières s'élevaient à 3,7 millions d'euros par entreprise victime d'attaque en moyenne. Il faut noter que plus d'un tiers des sources d'incident provient d'employés de la compagnie attaquée.
A plus petite échelle, les particuliers sont touchés par des escroqueries en tout genre, à la carte de crédit par exemple. Ainsi, un rapport récent de Norton/Symantec révélait qu'un Français sur cinq s'était fait dérober ses données bancaires après un achat en ligne. Le phénomène est tellement répandu que les banques ont peut-être trouvé la parade, du moins provisoirement : le cryptogramme dynamique qui change toutes les 20 minutes, un identifiant qui va commencer à figurer au dos des cartes de crédit en 2016.

De plus en plus sophistiqués

Les hackers, remarquent les professionnels, utilisent des méthodes de plus en plus sophistiquées pour fracturer les systèmes informatiques de leurs cibles. Dans un rapport récent, l'entreprise de sécurité informatique roumaine Bitdefender identifiait des évolutions notables pour 2016. La première touchait aux systèmes de monétisation publicitaires et en particulier les systèmes de blocage de publicité qui pourraient être utilisés par les pirates informatiques pour développer de nouvelles souches de logiciels malveillants.
D'après Bitdefender, le monde de l'entreprise va être encore plus touché en 2016 à travers des attaques ciblées visant essentiellement le vol d'informations. Mais les individus aussi seront plus vulnérables, en partie du fait de la multiplication des objets connectés qui recèlent de nombreuses failles de sécurité exploitables par les cybercriminels. Même des systèmes d'exploitation réputés plus sûrs, comme le Mac OS X d'Apple, ne seraient plus à l'abri d'être percés par les malfaiteurs en ligne, selon Bitdefender.

Réagissez à cet article

Source : *La cybercriminalité devrait encore augmenter en 2016 – France – RFI*

Au bout du compte, combien de secondes fait gagner la high-tech ?

Au bout du compte, combien de secondes fait gagner la high-tech ?

Capteurs électroniques, fibre de carbone, combinaisons en polyuréthane, eyetracking… Jusqu'à quel point la technologie permet-elle aux sportifs de dépasser leurs limites… tout en restant humains ?

Quoi ? Vous vous êtes équipé des applications Nike + Running, STT Sport Tracker ou Micoach d'Adidas, et vous n'avez pas encore battu le record du 100 mètres ? C'est normal. Ces applications n'ont pas pour but de vous transformer en Usain Bolt, mais de vous permettre de mieux gérer vos efforts, et de mesurer vos progrès.

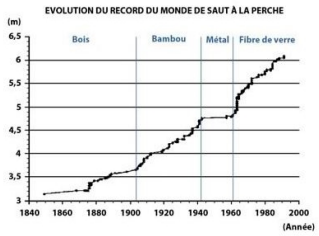
Reste que la technologie a toujours joué un rôle pour améliorer les performances sportives, et faire gagner des centimètres ou des secondes. C'est que la technologie peut améliorer les records grâce à trois facteurs : la mesure de la physiologie, les vêtements de sport et la tenue portée, et les matériaux utilisés.

« L'eyetracking » pour garder l'oeil sur les performances

Pour la mesure des performances corporelles, l'institut des sciences du sport de Berne utilise par exemple l'eyetracking pour étudier « le comportement du regard, ainsi que ses répercussions sur le comportement décisionnel en situations sportives ». Mais la mesure n'a pas de limite : développé par la NASA pour ses astronautes, la « pilule thermomètre » peut être ingérée pour prendre en permanence la température du sportif en plein effort – puis être ensuite restituée par les voies naturelles.

Des « vêtements dopants » ?

Même les vêtements et accessoires peuvent « doper » la performance : ainsi, les combinaisons de nageurs en polyuréthane ont-elles été interdites en 2009, du fait de leur trop grande efficacité. Les scientifiques ont évalué en 2008 que ces tenues permettaient de gagner 1 à 2% sur le chronomètre, et les chercheurs de l'Institut de recherche biomédicale et d'épidémiologie du sport (Irmes) ont estimé que deux tiers des records du monde de natation battus depuis 2000 l'ont été grâce aux combinaisons.



Fibre de carbone, aluminium, graphite…

Quant aux matériaux, ils jouent bien sûr un rôle essentiel dans les gains de performance. La preuve chiffrée en a été apportée de manière éclatante dans la discipline du saut à la perche. Comme le montre le graphique ci-dessous, les perches en bois permettaient à peine de dépasser 3,5 mètres. Avec le bambou, on atteint 4,5 mètres. Le métal permet de tutoyer les 5 mètres et, avec la fibre de carbone, les records explosent, jusqu'à dépasser les 6 mètres.

En 2010, le cycliste Fabian Cancellara a défrayé la chronique parce qu'il utilisait un pédalier optimisé (qui réduit les forces de frottement par un roulement à billes de graphite et huile) qui lui faisait gagner 2 secondes au kilomètre. Toujours dans le cyclisme, l'utilisation d'un cycloergomètre (vélo immobile servant à des mesures scientifiques) a montré que le plateau de type Harmonic permet une augmentation significative de la puissance maximale développée (+ 3%) lors d'un sprint ou d'une montée.

Bien entendu, les prothèses du coureur amputé Oscar Pistorius présentent un cas extrême. Non seulement elles lui permettaient de courir, mais elles furent accusées de lui offrir un avantage face à ses rivaux : une expertise a révélé que l'énergie restituée par les prothèses lors de la poussée était quasiment trois fois plus élevée que celle des chevilles humaines – au point qu'en janvier 2008, l'Association internationale des fédérations d'athlétisme lui a interdit de participer avec les valides aux jeux de Pékin.

La prochaine étape ? Sans doute des capteurs électroniques ou des régulateurs d'hormones greffés en permanence, qui brouilleront les frontières entre les sportifs et les cyborgs…

Réagissez à cet article

Source : *Big Data : La high-tech fait-elle gagner des secondes ?*

Plus fort que les cookies, découvrez les super-cookies

Plus fort que les cookies, découvrez les super-cookies

Dans un précédent bulletin d'actualité [1], était présenté comment les cookies HTTP (ou témoins de connexion), pouvaient être utilisés à des fins de profilage de l'utilisateur, dans le but notamment de pouvoir lui proposer du contenu ciblé. Après un bref rappel, cet article se propose de parcourir plus largement les mécanismes complémentaires existants à l'heure actuelle, à des fins de sensibilisation aux problématiques de vie privée sur l'Internet, et dans l'optique de permettre la prise des précautions d'usage adaptées à son utilisation au quotidien, dans un contexte professionnel comme personnel.

Techniques de pistage – Cookies – et évolutions

La technique la plus utilisée en matière de pistage d'utilisateurs sur l'Internet repose sur l'exploitation des cookies. Nous rappelons que le terme cookie désigne une variable utilisée par un serveur HTTP pour sauvegarder des informations sur la session HTTP courante. Il est composé d'une paire obligatoire nom/valeur, et d'attributs optionnels, comme la date d'expiration, le domaine et le chemin. Ces informations sont créées et mises à jour lors des échanges entre un serveur et un client Web grâce à des en-têtes dédiés du protocole HTTP (« Set-Cookie », « Cookie ») [2].
Le premier cas d'usage des cookies est tout à fait nécessaire à la navigation sur de nombreux sites Web, par exemple pour le maintien d'une session applicative ou la mémorisation d'un panier d'achats, on parle alors de « cookies de premier niveau ». Il existe cependant d'autres cas d'utilisations controversés sur le plan du respect de la vie privée. En particulier, l'usage de « cookies tiers » (ou « tierce partie ») [1], notamment dans l'optique d'établir des statistiques de consultation, peut permettre par exemple d'offrir des services de publicité ciblée. Ces cookies sont reconnaissables en particulier à leur domaine d'appartenance différent de celui de la page consultée, et peuvent parfois permettre d'identifier finement un utilisateur donné (par exemple cookies Google).

D'autres mécanismes permettent la conservation de données utilisateur, qui exploitent d'autres modes de création et de stockage que les cookies HTTP. On regroupe généralement ceux-ci sous le terme « supercookie ». Ils s'appuient notamment sur l'utilisation :
• mécanismes de stockage local dédiés à des applications Web au-dessus du protocole HTTP, comme Adobe Flash (« Local Shared Objects », également appelés « cookies Flash »), Microsoft Silverlight (« Silverlight Isolated Storage ») ou encore HTML5 (« HTML5 storage ») ;
• d'objets dans le contenu des pages Web, comme la propriété « window.name » en JavaScript, qui peut être détournée pour stocker temporairement des informations ;
• du cache du navigateur et de l'historique de navigation, pour stocker sous forme encodée des informations ;
• de HSTS (« HTTP Strict Transport Security ») [3], mécanisme de politique de sécurité pour HTTP, permettant à un serveur de demander le passage vers HTTPS via un champ d'en-tête HTTP (« Strict-Transport-Security »), mais dont une utilisation détournée permet à tiers contrôlant plusieurs domaines d'identifier de façon unique un utilisateur [4].

Cette liste, non exhaustive, montre bien qu'il existe de nombreuses façons de stocker des données issues de la navigation Web, et qu'un simple nettoyage des cookies HTTP via le navigateur ne peut pas suffire à effacer proprement l'ensemble de celles-ci. D'ailleurs, on parle de « cookie zombie » pour désigner des cookies HTTP qui sont régénérés après leur suppression grâce à l'utilisation des supercookies. L'application Evercookie [5], par exemple, illustre cela, permettant la propagation des cookies HTTP dans autant que mécanisme de stockage que possible afin d'assurer la résilience de l'information.

Autres techniques
Si les cookies (et assimilés) permettent d'obtenir une masse d'informations très intéressante, ils ne sont pas pour autant la seule source considérée par les entités cherchant à pister l'utilisateur. Il existe en particulier de nombreuses autres méthodes permettant d'identifier de façon unique un utilisateur, parfois à la granularité du terminal utilisé (téléphone, ordinateur, téléviseur connecté, tablette, etc.).
Ces méthodes peuvent être classées en cinq catégories [6] :
• entification générée par le client : certains terminaux ou applications clientes génèrent un identifiant unique pouvant être accessible par les services tiers à des fins publicitaires (advertising identifiers).
• Identification via des éléments réseau : certains équipements réseau situés entre le client et le serveur insèrent des éléments permettant, volontairement ou non, d'identifier l'utilisateur. Par exemple, l'utilisation du champ « X-Forwarded-For » dans l'en-tête HTTP précise l'adresse IP d'origine d'un client se connectant à travers un serveur mandataire.
• Identification par le serveur : certains serveurs ajoutent des pixels-espions [7], images de très petite taille généralement non repérables par l'utilisateur, qui permettent la génération de cookies tiers.
• Identification unique : certains services permettent à l'utilisateur de s'authentifier pour accéder à un ensemble de ressources (sites, applications), induisant ainsi la création d'un identifiant unique, censé faciliter la navigation (unique portail d'authentification, gestion des préférences utilisateur, etc.). On peut citer par exemple Facebook Connect, Windows Live ID, Google Account, etc.
• Identification statistique : certaines données issues du navigateur, de l'application ou encore du système d'exploitation permettent le calcul d'une empreinte entraînant la capacité à singulariser l'utilisateur. Ce calcul peut par exemple s'appuyer sur le User-Agent, la valeur du champ HTTP Accept, la politique de gestion des cookies, la résolution de l'écran, ou encore les extensions installées [8].

La directive 2002/58 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [9][10] précise que l'utilisation de cookies est autorisée à condition que l'utilisateur se voie donner des informations claires et précises sur la finalité de ces cookies ainsi que les informations placées sur l'équipement terminal qu'il utilise. L'utilisateur pourra refuser l'utilisation de ces dispositifs, cependant cette disposition ne fait pas obstacle au stockage de données utilisées à des fins exclusivement techniques.
Techniquement, des solutions amont ont été proposées, comme l'en-tête HTTP « Do Not Track » (DNT, 2009), pour permettre d'indiquer à un site web qu'un utilisateur ne souhaite pas être tracé. Cependant, bien qu'intégré dans tous les navigateurs modernes, il est purement déclaratif et peut être ignoré par le site visité.
D'un point de vue pratique, une des solutions les plus simples afin de limiter ces traces est de bloquer les cookies tiers. Ces cookies ne sont généralement pas utiles pour la navigation et il est recommandé de les refuser par défaut [11].
Enfin, de nombreuses extensions pour navigateur permettent de limiter le suivi d'un utilisateur existant. Elles ont principalement pour effet :
• blocage des traceurs (DoNotTrackME, Disconnect, uBlock Origin, AdBlock),
• le blocage des scripts (NoScript, ScriptNo),
• la génération de fausses informations afin de brouiller le calcul des empreintes numériques (Random Agent Spoofer),
• le basculement automatique vers HTTPS si disponible (HTTPS Everywhere).

Références

Bulletin d'actualité CERTA-2010-ACT-005 (05 février 2010)
http://www.cert.ssi.gouv.fr/site/CERTA-2010-ACT-005/CERTA-2010-ACT-005.html
RFC 6265 (HTTP State Management Mechanism) (avril 2011)
https://www.rfc-editor.org/rfc/rfc6265.txt
RFC 6797 (HSTS) (novembre 2012)
https://tools.ietf.org/html/rfc6797##section-14.9
How HSTS supercookies make you choose between privacy or security (02 février 2015)
https://nakedsecurity.sophos.com/2015/02/02/anatomy-of-a-browser-dilemma-how-hsts-supercookies-make-you-choose-between-privacy-or-security/
Evercookie (github)
https://github.com/samyk/evercookie
IAB Cookie White Paper (janvier 2014)
http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf
Web beacon (9 janvier 2014)
https://www.iab.net/wiki/index.php/Web_beacon
Browser uniqueness
https://panopticlick.eff.org/browser-uniqueness.pdf
Directive 2002/58/CE (12 juillet 2002)
http://eur-lex.europa.eu/legal-content/fr/TXT/?uri=CELEX:32002L0058
Sites web, cookies et autres traceurs (CNIL)
http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/que-dit-la-loi/
Conseils aux internautes (CNIL)
http://www.cnil.fr/vos-droits/vos-traces/les-cookies/conseils-aux-internautes/

Vulnérabilités critiques au sein de Juniper ScreenOS

Contexte

Le 18/12/2015, le CERT-FR a émis l'alerte CERTFR-2015-ALE-014 [1] concernant plusieurs vulnérabilités critiques impactant le système ScreenOS des équipements Juniper. D'après le bulletin de sécurité publié par Juniper [2], ces vulnérabilités ont été découvertes suite à un audit de code interne et auraient été introduites volontairement pour affaiblir la sécurité de ScreenOS. Il s'agit en l'occurrence de deux portes dérobées qui permettent de :
– contourner le mécanisme d'authentification en place au niveau des services SSH et Telnet,
– déchiffrer les communications entre un client et le service VPN d'un équipement Juniper vulnérable.

Marqueurs de détection

La société Fox-It propose des signatures au format Snort afin d'identifier toute tentative de connexion à un équipement Juniper vulnérable via la porte dérobée. Ces signatures sont cependant limitées au service Telnet. De plus, la vulnérabilité liée au service VPN étant exploitable après une interception passive du trafic chiffré, il n'est pas possible de détecter son exploitation.
Versions affectées
La porte dérobée permettant d'accéder à l'interface d'administration de l'équipement via le protocole Telnet ou SSH impacte le logiciel Juniper ScreenOS de la version 6.3.0r17 à 6.3.0r20.
La vulnérabilité permettant de déchiffrer les communications réseau liées au service VPN impacte le logiciel Juniper ScreenOS versions 6.2.0r15 à 6.2.0r18 et les versions 6.3.0r12 à 6.3.0r20.
Ces vulnérabilités permettant un accès illégitime sont respectivement référencées par les identifiants CVE-2015-7755 et CVE-2015-7756.

Description des portes dérobées

CVE-2015-7755
La porte dérobée permettant d'accéder à l'interface d'administration d'un équipement Juniper vulnérable est localisée au sein du code de vérification des identifiants de connexion. Ce code compare le mot de passe saisie par l'utilisateur avec une chaîne de caractère codée en dur dans le système ScreenOS. Si elles sont identiques, l'accès est autorisé.
CVE-2015-7756
La seconde porte dérobée reposait sur une faiblesse du générateur de nombres aléatoires utilisé par l'algorithme de chiffrement et permettait à un attaquant d'accéder au contenu des communications VPN, obtenues à partir d'une écoute passive du trafic réseau.

Corrections

Le CERT-FR recommande d'appliquer les mesures préconisées dans le bulletin d'alerte CERTFR-2015-ALE-014.

Documentation

1
Bulletin d'alerte du CERT-FR :
http://cert.ssi.gouv.fr/site/CERTFR-2015-ALE-014/index.html
2
Bulletin de sécurité de l'éditeur :
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST
3
Versions de ScreenOS vulnérable :
https://isc.sans.edu/diary/Infocon+Yellow%3A+Juniper+Backdoor+(CVE-2015-7755+and+CVE-2015-7756)/20521
1 – Rappel des avis émis
Dans la période du 21 au 27 décembre 2015, le CERT-FR a émis les publications suivantes :
CERTFR-2015-ALE-015 : Campagne de messages électroniques non sollicités de type TeslaCrypt
CERTFR-2015-AVI-554 : Multiples vulnérabilités dans le noyau Linux de Debian
CERTFR-2015-AVI-555 : Vulnérabilité dans VMWare
CERTFR-2015-AVI-556 : Multiples vulnérabilités dans Citrix XenServer
CERTFR-2015-AVI-557 : Multiples vulnérabilités dans Cisco IOS et IOS XE
CERTFR-2015-AVI-558 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
CERTFR-2015-AVI-559 : Vulnérabilité dans Xen
CERTFR-2015-AVI-560 : Vulnérabilité dans Cisco IOS XE
CERTFR-2015-AVI-561 : Multiples vulnérabilités dans le noyau Linux de Fedora
CERTFR-2015-AVI-562 : Multiples vulnérabilités dans ISC Bind
CERTFR-2015-AVI-563 : Multiples vulnérabilités dans le noyau Linux de SUSE
Durant la même période, les publications suivantes ont été mises à jour :
CERTFR-2015-ALE-014-1 : Vulnérabilité dans Juniper ScreenOS (ajout de règles Snort dans les contournements provisoires.)
Gestion détaillée du document
28 décembre 2015 version initiale.
Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-052
CERT-FR
2015-12-28

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-052*

Lourds investissements par les banques pour ne pas se faire pirater

	**Lourds investissements par les banques pour ne pas se faire pirater**

Pour ne pas se faire pirater, les banques investissent massivement dans la cybersécurité, souligne le Wall Street Journal dans une enquête datée du 20 décembre. Elles essayent également d'instaurer de bonnes pratiques chez leurs employés, responsables de 30% des fuites de données.

Les banques dépensent sans compter pour se défendre contre une armée invisible de hackers, qui essayent par tous les moyens de récupérer des données sur leurs clients et les énormes quantités de fonds qu'elles stockent sur leurs comptes.
Le patron de Bank of America, Brian Moynihan, a déclaré lors d'une conférence au mois de novembre que le budget cybersécurité de son entreprise était illimité, comme le rapporte le Wall Street Journal.
JP MORGAN INVESTIT 500 MILLIONS DE DOLLARS EN 2016 DANS LA CYBERSÉCURITÉ
Même topo pour l'américaine Wells Fargo, première banque mondiale en terme de valorisation boursière : « Nous dépensons un océan d'argent » dans la cybersécurité, a expliqué son PDG John Stumpf dans une interview récente, reprise par le média américain. Un porte-parole de la société a refusé de donner plus de détails sur les montants investis.
J.P. Morgan Chase a été victime en 2014 d'un piratage massif de données : 76 millions de clients étaient concernés par cette fuite d'informations sensibles. La banque américaine a considérablement renforcé son dispositif de cybersécurité. Elle va investir 500 millions de dollars pour se protéger contre les hackers en 2016, soit environ deux fois plus qu'en 2014, détaille le Wall Street Journal.

LA VULNÉRABILITÉ NUMÉRO UN DES BANQUES : LEURS SALARIÉS
Souvent, les hackers jouent sur la vulnérabilité numéro un des banques pour récupérer des informations sensibles : les salariés. Ils envoient notamment des messages de phishing (hameçonnage), demandant à leurs destinataires de cliquer sur un lien. Cela leur permet d'installer dans les ordinateurs ciblés des logiciels espions. J.P. Morgan a envoyé un faux mail de phishing à ses salariés, pour les tester. Résultat ? 20% d'entre eux ont mordu à l'hameçon…
En moyenne, 30% des fuites de données dans les entreprises sont liées à une erreur d'un salarié, selon une enquête diffusée en décembre par l'Association of Corporate Counsel, une association professionnelle d'avocats américains. Pour limiter les dégâts, les banques interdisent donc à leur salariés d'utiliser des clefs USB venues de l'extérieur, d'utiliser leur adresse mail personnelle pour s'inscrire à des services sur Internet (site de e-commerce par exemple).

NE PAS ALLER JUSQU'AU « FLICAGE »
Elles leur demandent aussi d'être vigilants par rapport aux informations qu'ils postent sur les réseaux sociaux. « Mais jusqu'où les banques peuvent-elles aller dans le 'flicage' de leurs salariés sur ces sites ? », s'interrogent les experts du secteur.
Impossible de poursuivre un collaborateur qui poste des photos de ses vacances sur son profil Facebook, même si cela pourrait permettre à un pirate de s'introduire à son domicile et de voler son ordinateur professionnel. Alors que faire ? Cette réflexion délicate doit être conduite par les institutions financières si elles veulent protéger au mieux les données sensibles de leurs clients.

Réagissez à cet article

Source : *Cybersécurité : Les banques investissent « un océan d'argent » pour ne pas se faire pirater*

Lelia de MATHAREL

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*

Scientists create world’s first biologically powered computer chip

Scientists create world’s first biologically powered computer chip

The dream of melding biological and man-made machinery is now a little more real with the announcement that Columbia Engineering researchers have successfully harnessed a chemical energy-producing biological process to power a solid state CMOS integrated circuit.

The dream of melding biological and man-made machinery is now a little more real with the announcement that Columbia Engineering researchers have successfully harnessed a chemical energy-producing biological process to power a solid state CMOS integrated circuit.
According to study lead professor Ken Shepard, this is the world's first successful effort to isolate a biological process and use it to power an integrated circuit, much like the ones we use in phones and computers.
The researchers developed the system by using an artificially created lipid bilayer membrane containing naturally occurring ion pumps, which are powered by the biological world's « energy currency molecule, » ATP (adenosine triphosphate). ATP is the coenzyme that transfers chemical energy between living cells. It is an end product of processes such as photosynthesis and cellular respiration, and it powers the mechanical work of living systems such as cell division and muscle contraction.
The scientists connected the lipid membrane to a conventional solid-state complementary metal-oxide-semiconductor (CMOS) integrated circuit, and the ion pumps powered the circuit.
« Ion pumps basically act very similarly to transistors, » Shepard tells Gizmag. « The one we used is the same kind of pump that is used to maintain the resting potential in neurons. The pump produces an actual potential across an artificial lipid membrane. We packaged that with the IC and we used the energy across that membrane due to those pumped ions to power the integrated circuit. »
Using an isolated and artificially created biological component is a different approach to interfacing whole living systems with chips, which was done in the past with varying success.
« We don't need the whole cell [now], » Shepard says. « We just grab the component of the cell that's doing what we want. For this project, we isolated the ATPases because they were the proteins that allowed us to extract energy from ATP. »
Shepard says the team is excited about the prospect of extending the range of possibilities in electronics.

« As technology scaling ends, we have to be a little bit more creative and expansive in the way we define an electronic device and the material systems that we use to create electronic devices, » he says. « How do we expand the palette? That's essentially what this work is about. »
The key challenges now are to try to scale the system down, and to look for ways to manage biological decay.
Challenges aside, the potential for combining biological and electronic processes certainly fires the imagination.
« 100 Intel designers couldn't design a system that could tell if there's a skunk in the room or not, and the best synthetic biologists in the world couldn't build a radio, » quips Shepard. « But if we can just use the piece of the biological process that we want and use its function with solid state electronics, we'll get that enhanced functional palette of capabilities that don't exist with chips alone. »
The research was recently published in Nature Communications.
Source: Columbia University

Réagissez à cet article

Source : *Scientists create world’s first biologically powered computer chip*

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

	**Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso**

Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.

Ainsi, il convient de prendre les précautions suivantes :

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
LA PRESIDENTE

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*

Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

	Utilité et conformité des mesures de blocage de sites Internet faisant l’apologie du terrorisme dans le cadre de l’état d’urgence.

A ce jour, il existe certains exemples de moyens, usités par les terroristes, permettant de contourner une mesure de blocage d'un site, notamment, l'utilisation d'un « Virtual Private Network » (Réseau Privé Virtuel).

Ce dernier établi un réseau fictif, reliant un ordinateur (celui du client VPN) à un serveur (le serveur VPN), afin de permettre une connexion à Internet de manière anonyme.

De cette façon, les échanges de données sont cryptés et sont protégés par des clés de chiffrement. De plus, ce système permet d'utiliser une adresse IP différente de celle réellement utilisée par un ordinateur, ce qui complique considérablement la localisation de cette machine. De même, le logiciel « Tor » permet de se connecter à Internet par le biais de serveurs répartis dans le monde dans l'anonymat. Il convient de noter que ces procédés cryptologiques sont parfaitement légaux, effectivement, l'article 30 de la loi LCEN du 21 juin 2004 érige en principe que « l'utilisation des moyens de cryptologie est libre ». Dès lors, peut-on envisager l'introduction d'un contrôle par l'autorité administrative, sous forme d'autorisation préalable, lorsque l'utilisation de tels procédés est faite à des fins de provocation au terrorisme ?

Enfin, ces mesures de blocage de sites peuvent sembler illusoires étant donné que celles-ci ne s'appliquent qu'à des FAI et hébergeurs situés sur le territoire français. D'autant que de telles mesures drastiques ne sont pas exemptes de risques de « surblocage ». En 2013, l'Australie a pu en faire les frais en bloquant par accident 250 000 sites sur sa toile.

En conséquence, loin d'être la panacée, cette nouvelle disposition, faussement pragmatique, semble foncièrement superfétatoire.

Sur la conformité de la loi par rapport au bloc de constitutionnalité ?

A titre liminaire, il importe de se poser la question de savoir si la loi du 20 novembre 2015 est susceptible d'être déclarée non conforme à la constitution compte tenu de l'absence de consécration constitutionnelle du statut de l'état d'urgence. A cette fin, il conviendra d'appliquer mutatis mutandis le raisonnement adopté par le Conseil Constitutionnel dans deux décisions : celle du 10 juin 2009 concernant la loi HADOPI et celle relative à la loi sur la pédopornographie du 10 mars 2011.

Dans sa décision du 10 juin 2009, le Conseil en raison du caractère disproportionné du blocage et de sa contrariété avec l'article 11 de la DDHC censure la loi HADOPI soumise à son contrôle « considérant que les pouvoirs de sanction institués par les dispositions critiquées habilitent la commission de protection des droits, qui n'est pas une juridiction, à restreindre ou à empêcher l'accès à internet de titulaires d'abonnement ainsi que des personnes qu'ils en font bénéficier ; que la compétence reconnue à cette autorité administrative n'est pas limitée à une catégorie particulière de personnes mais s'étend à la totalité de la population ; que ses pouvoirs peuvent conduire à restreindre l'exercice, par toute personne, de son droit de s'exprimer et de communiquer librement, notamment depuis son domicile ; que, dans ces conditions, eu égard à la nature de la liberté garantie par l'article 11 de la Déclaration de 1789, le législateur ne pouvait, quelles que soient les garanties encadrant le prononcé des sanctions, confier de tels pouvoirs à une autorité administrative dans le but de protéger les droits des titulaires du droit d'auteur et de droits voisins ».

En substance, les Sages expliquent que l'octroie par la loi à une autorité administrative du pouvoir de suspendre l'accès à internet est une entorse à la « la libre communication des pensées et des opinions ». L'autorité administrative n'ayant pas le statut de juridiction, elle ne peut se voir octroyer ce pouvoir exorbitant de bloquer un site illicite.

A rebours, dans sa décision du 10 mars 2011, les Sages valident l'article 4 de la loi Loppsi 2 permettant de procéder au blocage administratif de sites pédopornographiques « considérant, en second lieu, que les dispositions contestées ne confèrent à l'autorité administrative que le pouvoir de restreindre, pour la protection des utilisateurs d'internet, l'accès à des services de communication au public en ligne lorsque et dans la mesure où ils diffusent des images de pornographie infantile ; que la décision de l'autorité administrative est susceptible d'être contestée à tout moment et par toute personne intéressée devant la juridiction compétente, le cas échéant en référé ; que, dans ces conditions, ces dispositions assurent une conciliation qui n'est pas disproportionnée entre l'objectif de valeur constitutionnelle de sauvegarde de l'ordre public et la liberté de communication garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 ».

Dans cette décision, la mesure de blocage est déclarée conforme à l'article 11 de la DDHC de 1789 au motif qu'il existe un recours au fond ou en référé des décisions de blocage et qu'il est consacré un objectif à valeur constitutionnelle de sauvegarde de l'ordre public (ici l'exploitation sexuelle des mineurs).
En ce qui concerne la conformité du nouveau dispositif, il est à noter que ce nouvel article 11 de la loi de 1955 énonce que « le ministre de l'Intérieur peut prendre toute mesure » de blocage de sites faisant l'apologie du terrorisme. La large marge d'appréciation laissée à l'exécutif amène à s'interroger sur le caractère proportionné de cette disposition. Ainsi, un parallèle peut être opéré avec l'article L. 336-2 du CPI prévoyant des mesure de blocage en cas de violation d'un droit d'auteur ou d'un droit voisin. Celui-ci met en évidence l'éventuel caractère excessif du nouveau dispositif. Si ce dernier rend possible « toutes mesures », l'article L. 336-2 du CPI autorise seulement « toutes mesures propres » en vue de bloquer un site.

La référence au principe de proportionnalité, tangible dans cet article du CPI, ne l'est pas en ce qui concerne cette nouvelle mesure. Dans le cadre d'un raisonnement analogue à celui employé dans la décision du 10 juin 2009, on peut appréhender une potentielle censure par les Sages. En effet, la loi du 20 novembre 2015, compte tenu de sa rédaction large et générale, peut habiliter le ministre de l'Intérieur à « restreindre ou à empêcher l'accès à Internet ». De ce fait, un accroc à l'article 11 de la DDHC peut être redouté. D'ailleurs, le rapporteur au Sénat énonçait que « la disposition proposée [la loi lopssi 2] présente une portée beaucoup plus restreinte [que la loi HADOPI] puisqu'elle tend non à interdire l'accès à internet mais à empêcher l'accès à un site déterminé en raison de son caractère illicite ». Ainsi, le nouveau texte de 2015 risque de connaître le même sort que celui donné à la loi HADOPI, en ce que rien n'interdit au ministre de l'Intérieur de prendre des mesures bloquant l'accès à un site sans pour autant bloquer un site en particulier.
Par ailleurs, une autre incertitude juridique semble planer sur cette loi du 20 novembre 2015 au regard de la décision du 10 mars 2011. S'il est vrai que la suppression du délai de 24 heures ne semble pas impacter la conformité de ce texte, il en va autrement de l'éviction du rôle de contrôle de la CNIL. En effet, l'article 66 de la Constitution dispose que l'autorité judiciaire est « gardienne de la liberté individuelle ». Auparavant, la loi de 2014, chargeait la CNIL d'assurer ce rôle de gardien a posteriori, c'est-à-dire, en actionnant en aval les recours nécessaires devant la juridiction compétente. De même, la CNIL détenait la faculté de contrôler le bien fondé des demandes de retrait de l'autorité administrative. La nouvelle loi éludant cet encadrement exercé par la CNIL, peut laisser sceptique sur sa conformité au texte constitutionnel. D'autant que la loi ancienne (de 2014) n'a jamais fait l'objet d'un contrôle, que ce soit de manière a priori ou a posteriori, devant le Conseil Constitutionnel !

Sur le risque de contrariété de la loi avec la Convention Européenne des Droits de l'Homme ?

Dans un récent arrêt CEDH du 1er décembre 2015, la Cour censure des mesures de blocage de sites pratiquées par le gouvernement turc. En l'espèce, les autorités turques avaient ordonné le blocage de Youtube en raison de dix vidéos accusées de faire outrage à la mémoire d'Atatürk, fondateur de la République laïque turque. Des mesures de blocage ont été ordonnées entre 2008 et 2010.
La Cour reconnait une ingérence de l'autorité publique dans l'exercice des droits garantis par l'article 10 de la convention portant sur la liberté d'expression. De la même façon, la loi de novembre 2015 n'excluant pas la possible coupure d'un site Internet, elle encourt le risque d'être déclarée disproportionnée au regard de l'intérêt légitime poursuivi, à savoir, la lutte contre l'apologie du terrorisme.
Toutefois, l'article 15 de la CEDH autorise dérogation aux obligations de cette convention dans une situation d'état d'urgence, excepté pour les principes non dérogeables, dont ne fait pas partie l'article 10 de la CEDH. Mais un prolongement durable de l'état d'urgence posera nécessairement une difficulté relative à sa compatibilité avec l'article 15 de la CEDH. A moins, (ce que le gouvernement envisage) d'établir un socle juridique solide de l'état d'urgence, au sein de la constitution. En conséquence, de lege lata, la conformité de ce nouveau dispositif semble loin d'être évidente au regard d'un certain nombre de droits fondamentaux garantis.
Somme toute, est-ce qu'« à force de sacrifier l'essentiel pour l'urgence, on finit par oublier l'urgence de l'essentiel » ? (Edgar Morin)

Réagissez à cet article

Source : *Utilité et conformité des mesures de blocage de sites Internet faisant l'apologie du terrorisme dans le cadre de l'état d'urgence. Par Dan Scemama.*

Mobile strategies increase need for data loss prevention technology in Europe

Mobile strategies increase need for data loss prevention technology in Europe

Data loss prevention technology that covers all popular mobile platforms and is easy to use and implement is called for as mobile strategies evolve

Mobile has entered business strategy from two directions. The business wants to grab the opportunity to better serve the mobile masses, while employees want to mobile devices as part of their work
This has created an environment that security teams have had to come to terms with quickly.

Roman Foeckl, CEO at security supplier CoSoSys, says the increasing number of mobile devices in the enterprise, and new versions of an operating system, is forcing organisations to rethink ways of securing corporate data.
It is not just about mobile the applications, he says, but also how employees interact with other organisations and people. Mobile provides low-cost computing power that is available to everyone and enables staff to collaborate with others, but this is a recipe for security breaches in businesses.
Foeckl says traditional security is irrelevant in many cases. For example, he says the shift from open file systems (Windows 7) to application sandboxes (Android, iOS, Windows Phone/Pro/RT), is making traditional antimalware, especially antivirus, less relevant.
For example, on iOS, there is little need for antimalware or antivirus products because neither they, nor any other app on the device, can access another app's storage or memory.
According to Foeckl, when planning a mobile security strategy there is no one size fits all: "Every company has to choose a cross-platform solution that works on Apple iOS, Android mobile devices, Windows, Mac OS X and Linux computers to cover the entire fleet of workstations."
Sufficient resources for data loss protection
But what are companies doing to incorporate endpoint and mobile security tools in applications to make sure they are secure?
"This can be achieved by implementing data loss prevention (DLP) features into applications and more," says Foeckl. "However, the administrators have to be sure that IT resources under their control are ready to co-operate with advanced features like file tracing and file shadowing."

With DLP, the amount of data being monitored and the number of copies stored could quickly absorb a sizeable chunk of the available IT resources.
"In European countries, sometimes we are faced with the situation that a CIO or administrator evaluates resources as insufficient for DLP use," says Foeckl. "In such cases it is recommended to look at cloud-managed DLP and mobile device management [MDM] that offer easy evaluation, implementation and scalability. It's also a good way to safely reap the benefits of the cloud protecting data."
In central and eastern European countries, one obstacle is the fact that many companies still prefer their own datacentres or computing power over cloud services, says Foecki.

Authorisation and security awareness
The software being used in enterprises is changing, so security teams must understand different security features and their limitations.
Foeckl says CoSoSys increasingly supports Macs and iOS devices. It has experience with preventing data breaches that could happen with the use of Google Drive, One Drive, Dropbox, on Windows and Mac OS X computers, for example.

Réagissez à cet article

Source : *Mobile strategies increase need for data loss prevention technology in Europe*

Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

Le 23 décembre, la DGAC (Direction Générale de l'Aviation Civile) a mis en ligne les évolutions réglementaires en matière de drones, aéromodèles, etc. Elles se veulent plus lisibles et mieux adaptées aux besoins.

Si le Père Noël vous apporte un drone, voici quelque chose qui devrait vous intéresser : ce que vous avez le droit de faire ou non avec, les règles à respecter, etc.

Tout d'abord, sachez que deux textes datant du 17 décembre 2015 définissent désormais la réglementation pour l'usage de drones. Il s'agit d'un arrêté relatif à la conception, aux conditions d'utilisation et aux qualifications des télépilotes et d'un autre arrêté relatif aux conditions d'insertion dans l'espace aérien.
Comme le rappelle la DGAC, les deux textes font la distinction entre les différents pilotes : professionnels ou non. Par exemple, « lorsque cette utilisation est limitée au loisir et à la compétition, on parle d'aéromodèles ». Ce sont les drones achetés dans les grandes surfaces ou des boutiques high-tech. D'autre part, on évoque les drones réservés à une utilisation professionnelle.

Règles basiques

Si l'espace aérien est libre en-dessous de 150 mètres, il faut toutefois respecter certaines consignes basiques :
• Voler en dehors des agglomérations et des rassemblements de personnes ou d'animaux ;
• Voler en dehors des zones proches des aérodromes ;
• Et voler en dehors d'espaces aériens spécifiquement réglementés qui figurent sur les cartes aéronautiques.
• Il est également interdit de survoler des villes ou des rassemblements de personnes sans autorisation préfectorale.
• Dans tous les cas, le « télépilote d'un drone est responsable des dommages causés par l'évolution de l'aéronef ou les objets qui s'en détachent aux personnes et aux biens de la surface (article L.61613-2 du code des transports) ».

Protection de la vie privée

Le texte compte tout un tas d'autres interdits. Notamment, les personnes sourdes ne peuvent pas piloter d'aéromodèles puisqu'un pilote doit toujours être en mesure de détecter visuellement et auditivement les autres drones. Il est aussi interdit de voler la nuit, ou de piloter un drone depuis une voiture.

La DGAC rappelle aussi que la « prise de vue aérienne est réglementée par l'article D133-10 du code de l'aviation civile », afin de veiller à la protection de la vie privée. Une amende de 45 000 euros et d'un an d'emprisonnement est prévue s'il y une volonté manifeste de porter atteinte à l'intimité de la vie privée d'autrui.

Réagissez à cet article

Source : *Un drone à Noël ? Voici vos nouveaux droits et devoirs*