92% des salariés français sont incapables de détecter du phishing

92% des salariés français sont incapables de détecter du phishing

Le facteur humain est toujours le point faible en matière de cybersécurité. Il s'avère que 92% des salariés français sont incapables de détecter les tentatives de phishing les plus courantes. Intel Security estime que le coût global de la cybercriminalité dans le monde peut être estimé à quelque 445 milliards de dollars. Il est par ailleurs estimé que deux tiers des courriels envoyés dans le monde sont des spams destinés à extorquer de l'information ou de l'argent.

Une étude conjointe menée par McAfee Labs, filiale d'Intel Security, et le centre de cybercriminalité européen d'Europol (EC3) révèle toute l'importance du facteur psychologique dans la réussite des attaques informatiques. « **Le facteur humain est toujours le point faible en matière de cybersécurité** », a expliqué Raj Samani, le directeur technique d'Intel Security.

« Les entreprises de tous les secteurs industriels, toutes les tailles et toutes les régions du monde sont en danger en raison du facteur social », résume Raj Samani. Il explique qu'« il est important de comprendre que les cybercriminels s'avèrent souvent être de bons psychologues et que le facteur humain est souvent utilisé comme un point d'entrée pour les cyberattaques » en précisant que les hackers savent parfaitement user de la séduction, du respect de l'autorité, du conformisme social et du besoin de retourner une faveur, sans oublier la loyauté ou la peur de rater une opportunité.

Cette étude révèle par exemple qu'en France, 92% des salariés sont incapables de détecter les tentatives de phishing les plus courantes et les plus fréquemment utilisées.

Ce résultat est d'autant plus inquiétant pour les entreprises françaises que le rapport révèle que 18% des utilisateurs visés par un courriel d'hameçonnage deviennent finalement des victimes après avoir cliqué sur un lien frauduleux.

C'est ainsi que Raj Samani conclut en déclarant qu'«il est crucial pour les entreprises d'éduquer leurs employés sur la cybersécurité en plus des mesures prises sur les niveaux opérationnels et techniques».

Expert Informatique et formateur spécialisé en sécurité Informatique, en cybercriminalité et en protection des données personnelles, Denis JACOPINI est en mesure de prendre en charge, en tant qu'intervenant de confiance, externe à l'entreprise, la sensibilisation de vos salariés au risque informatique et à la cybercriminalité afin de les informer des risques, des conséquences et des bonnes pratiques de l'informatique au quotidien.
Contactez-nous

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

Source : http://www.linformatique.org/cybercriminalite-92-des-salaries-francais-sont-incapables-de-detecter-du-phishing/
Par Emilie Dubois

Nous sommes tous des proies potentielles des pirates d'Internet

Nous sommes tous des proies potentielles des pirates d'Internet

3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Denis Jacopini est à Cavaillon ce soir. PHOTO DR

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes ?

Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité ?

Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver ?

Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

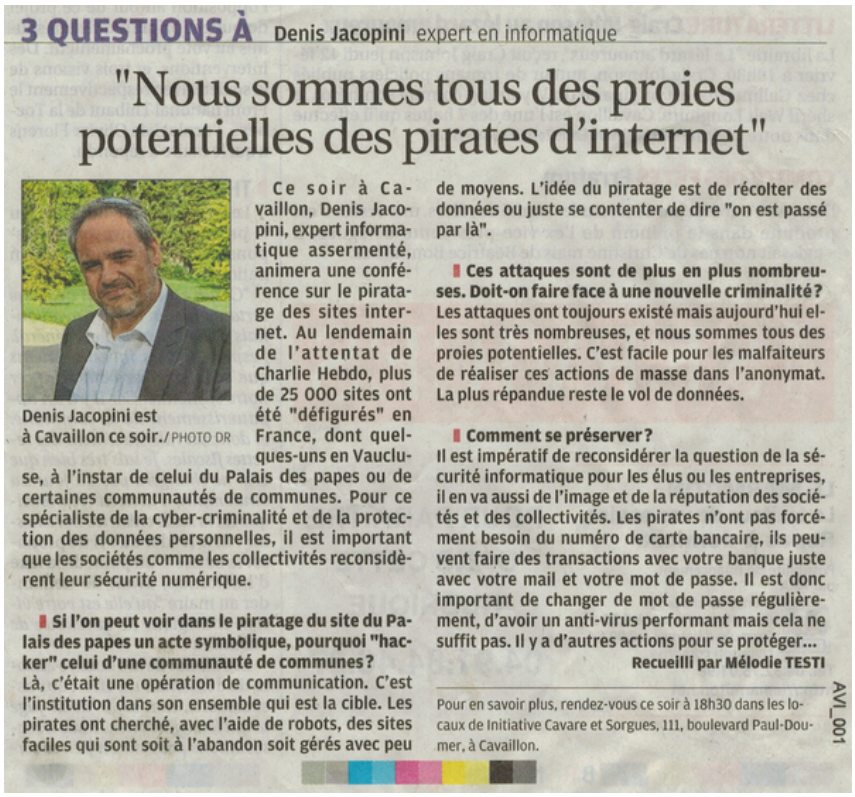
Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Cavaire et Sorgues, 111, boulevard Paul Doumer, à Cavaillon.

AVL001

A la suite des attentats de Paris à Charlie Hebdo le 7 janvier 2015, plus de 25000 sites Internet ont été « défigurés » en France. Dans le but de continuer à sensibiliser les chefs d'entreprises et Elus qui ne connaissent ou ne maîtrisent pas encore bien le sujet, le 10 février 2015, Denis JACOPINI a animé une conférence à Cavaillon.

Victime d'actes illicites, les cibles de la cybercriminalité se sentent démunies face à ce risque incoercible. Après un état des lieux, la conférence à dévoilé les principales raisons pour lesquelles la cybercriminalité sévit aussi facilement.

Enfin, des solutions de bon sens ont été présentées, concernant à la fois la mise en place de mesures de sécurité, mais aussi le respect de la loi informatique et libertés chargée d'encadrer l'usage et la protection des données personnelles, des données à caractère personnel.



3 QUESTIONS À Denis Jacopini expert en informatique

"Nous sommes tous des proies potentielles des pirates d'internet"

Denis Jacopini est à Cavaillon ce soir./PHOTO DR

Ce soir à Cavaillon, Denis Jacopini, expert informatique assermenté, animera une conférence sur le piratage des sites internet. Au lendemain de l'attentat de Charlie Hebdo, plus de 25 000 sites ont été "défigurés" en France, dont quelques-uns en Vaucluse, à l'instar de celui du Palais des papes ou de certaines communautés de communes. Pour ce spécialiste de la cyber-criminalité et de la protection des données personnelles, il est important que les sociétés comme les collectivités reconsidèrent leur sécurité numérique.

Si l'on peut voir dans le piratage du site du Palais des papes un acte symbolique, pourquoi "hacker" celui d'une communauté de communes?

Là, c'était une opération de communication. C'est l'institution dans son ensemble qui est la cible. Les pirates ont cherché, avec l'aide de robots, des sites faciles qui sont soit à l'abandon soit gérés avec peu de moyens. L'idée du piratage est de récolter des données ou juste se contenter de dire "on est passé par là".

Ces attaques sont de plus en plus nombreuses. Doit-on faire face à une nouvelle criminalité?

Les attaques ont toujours existé mais aujourd'hui elles sont très nombreuses, et nous sommes tous des proies potentielles. C'est facile pour les malfaiteurs de réaliser ces actions de masse dans l'anonymat. La plus répandue reste le vol de données.

Comment se préserver?

Il est impératif de reconsidérer la question de la sécurité informatique pour les élus ou les entreprises, il en va aussi de l'image et de la réputation des sociétés et des collectivités. Les pirates n'ont pas forcément besoin du numéro de carte bancaire, ils peuvent faire des transactions avec votre banque juste avec votre mail et votre mot de passe. Il est donc important de changer de mot de passe régulièrement, d'avoir un anti-virus performant mais cela ne suffit pas. Il y a d'autres actions pour se protéger...

Recueilli par Mélodie TESTI

Pour en savoir plus, rendez-vous ce soir à 18h30 dans les locaux de Initiative Cavare et Sorgues, 111, boulevard Paul-Doumer, à Cavaillon.

AVI_001

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

Source : http://www.horizon2020.gouv.fr/pid29774/securite.html

---

Cybercriminalité : Une

stagiaire dérobe 1 million de FCFA à son patron

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Mardi 17 février 2015-Kadija Koné stagiaire dans une agence Rechercher agence de transfert d'argent a été épinglée par la Police de Lutte contre la Cybercriminalité (PLCC), pour escroquerie Rechercher escroquerie , faux et usage de faux Rechercher faux et usage de faux portant sur la somme d'un 1000 000 FCFA dérobé à son patron.

En effet, et pour subvenir aux soucis financiers de son ex compagnon, la stagiaire en question a frauduleusement retiré la somme de 1 581 550 FCFCA, sur le compte géré par son patron entre septembre 2014 et janvier 2015. Le patron ayant constaté les faits a avisé la PLCC Rechercher PLCC et porter plainte contre X.
Après enquêtes, la PLCC Rechercher PLCC a fini par mettre le grappin sur Kadija Koné, qui d'ailleurs ne mettra aucune difficulté pour reconnaitre les faits qui lui sont reprochés.
« Je voulais octroyer un prêt à usure à mon ex copain. J'ai retiré 1 000 000 FCFA sur le compte géré par mon patron. En retour et comme convenu j'ai reçu en récompense un acompte de 450 000 FCFA, ensuite mon ex devait me rembourser à hauteur de 1 200 000 FCFA », aurait-elle révélé dans les locaux de la PLCC. La stagiaire a été déférée devant le parquet pour escroquerie, faux et usage de faux.
Selon la nouvelle loi sur la cybercriminalité, cette dernière risquerait une peine allant jusqu'à 20 ans de prison ferme, et une amende de 40 millions de FCFA.

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

Source : http://koaci.com/cote-divoire-cybercriminalite-stagiaire-derobe-million-fcfa-patron-pour-aider-copain-elle-risque-prison-98895.html
Par Donatien Kautcha, Abidjan

Le ministre de la Poste et

des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Le ministre de la Poste et des TIC appelle à « une culture nationale » en matière de cyber-sécurité

Abidjan – Le ministre de la Poste et des Technologies de l'information et de la communication, Bruno Nabagné Koné, appelle au développement d' »une culture nationale » autour de la question de la sécurisation des réseaux et services numériques qui, estime-t-il, est essentielle pour lutter efficacement contre la cybercriminalité en Côte d'Ivoire.

Pour le ministre Nabagné Koné qui procédait lundi à l'ouverture d'un séminaire sur la cyber-sécurité organisé par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI) autour du thème principal « Développement d'une stratégie nationale en matière de cyber sécurité », il s'agit notamment d'élever la question au rang de celles relevant de la sécurité nationale.
Le séminaire qui s'étendra sur deux jours se veut, selon le DG de l'ARTCI, Bilé Diéméléou, une lucarne d'échanges et de partage d'expériences afin de présenter les actions entreprises par sa structure dans l'accomplissement de sa mission visant à développer la cyber-sécurité.
La rencontre sera également l'occasion d'établir les bases du développement d'un partenariat public/privé fort en matière de cyber-sécurité avec la centaine de structures conviées, a-t-il ajouté.
Le ministre Nabagné Koné déplorait, à l'occasion, le fait que le traitement de la question de la sécurisation des réseaux et services numériques, « considérée comme la 5ème roue du carrosse dont on peut se passer », n'a pas toujours suivi le niveau d'évolution enregistré ces dernières années en Côte d'Ivoire en matière de TIC et même dans le monde.
C'est pourquoi, il appelle à une culture nationale en la matière et qui, selon lui, permettra de faire du souci de la sécurisation du cyber espace ivoirien une question de sécurité nationale.
Le ministre des TIC rappelait auparavant le danger que laisse planer la cybercriminalité sur le développement global de la Côte d'Ivoire, un phénomène qui, a-t-il reprécisé, va au-delà de la perception commune l'assimilant abusivement aux petites escroqueries commises au moyen des outils de moderne de communication.
La cybercriminalité est plutôt le fait pour une personne de s'introduire de façon malveillante dans des systèmes d'information, a-t-il fait comprendre, relevant que c'est cet aspect des choses qui rend le phénomène si préoccupant.
« Que des personnes entrent dans nos systèmes, c'est de cela que nous avons peur et c'est face à cela que nous devons prendre des mesures », a fait remarquer M. Nabagné Koné.
Il a notamment relevé le fait que le phénomène, s'il n'est pas efficacement combattu, pourrait consacrer un recul de l'usage des TICS qui partirait d'une méfiance légitime des populations vis-à-vis des solutions offertes.
« Sans confiance, la réaction des utilisateurs sera le rejet et c'est notre société qui recule », a laissé entendre le ministre.
« Les personnes malveillantes dans le cyberespace ou en ligne sont nombreuses, organisées et leurs motivations sont très diverses: politiques, criminelles, terroristes ou activistes. La cyber-sécurité doit faire partie intégrante du progrès technologique », a-t-il, pour ce faire, appelé.

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

Source : http://news.abidjan.net/h/526302.html

Piratage Anthem : voici venu le temps du phishing

Piratage Anthem : voici venu le temps du phishing

Victime d'une importante cyber-attaque, l'assureur américain Anthem invite ses clients à ignorer les e-mails qui leur seraient envoyés en son nom.

Victime d'une attaque informatique qui a potentiellement exposé les données personnelles de 80 millions d'individus, Anthem est passé en mode gestion de crise.
La compagnie américaine d'assurances santé mène actuellement l'enquête avec les autorités sur place. Elle a également sollicité la firme Mandiant (filiale de FireEye) pour pratiquer un audit de son système d'information et adopter les solutions de protection ad hoc.
Depuis le lancement de l'alerte mercredi dernier, de nouveaux éléments ont été révélés… sans qu'Anthem en soit systématiquement à l'origine. On a ainsi appris, d'une source dite « proche du dossier » par la presse américaine, que les données subtilisées par les pirates n'étaient pas chiffrées.
Sur la liste figurent, selon les déclarations officielles de l'assureur, des noms, des dates de naissance, des numéros de téléphone et de Sécurité sociale, des adresses postales et électroniques, ainsi que des éléments relatifs à l'activité salariée de clients, comme leur niveau de revenus.
Il n'existe toujours pas de preuves que des informations bancaires et médicales aient été dérobées. Mais celles-ci pourraient l'être d'une façon détournée ; en l'occurrence, par des campagnes de hameçonnage (phishing). Les clients d'Anthem commencent effectivement à recevoir des e-mails d'apparence légitime qui les invitent à cliquer sur un lien pour bénéficier d'un suivi de leurs encours de crédit.
Problème : si l'entreprise a bel et bien annoncé son intention de fournir gratuitement ce service à toutes les victimes collatérales de la cyber-attaque, elle n'a pas encore adressé de communication officielle. Bilan : les e-mails reçus ces derniers jours ne sont qu'un scam visant à récupérer de précieuses données auprès des utilisateurs insuffisamment vigilants.
Voilà Anthem contraint d'user de pédagogie. La société cotée en Bourse – sur le NYSE – a ouvert une rubrique dédiée dans la foire aux questions du site AnthemFacts, créé pour centraliser les dernières nouvelles relatives à la cyber-attaque. Elle enjoint ses clients à ne cliquer sur aucun lien, à ne pas ouvrir les éventuelles pièces jointes, à ne renseigner aucune information sur le site Web qui s'ouvrirait éventuellement et à ne pas répondre au mail.
Pour l'heure, il reste difficile de déterminer s'il s'agit d'une campagne de phishing ciblée ou si ces envois de mails sont l'œuvre de pirates qui ont visé large en espérant toucher des souscripteurs aux assurances santé d'Anthem. Ce qui laisse supposer que les données volées sont bel et bien activement exploitées, ce sont plutôt ces appels téléphoniques invitant les clients à fournir leur numéro de carte bancaire et/ou de Sécurité sociale.
Le bilan pourrait être lourd : près de 40 millions de clients revendiqués à fin 2014… et autant d'anciens souscripteurs. Une affaire d'une telle envergure que le Département des services financiers de New York envisage aujourd'hui un audit global de toutes les compagnies d'assurance. L'agence fédérale compte intégrer ces contrôles « réguliers et ciblés » dans sa feuille de route. Elle projette aussi de durcir les obligations auxquelles les institutions sont soumises en matière de sécurité informatique.

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

Source : http://www.itespresso.fr/piratage-anthem-temps-phishing-88038.html
Pat Clément BOHIC

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Des pirates se sont infiltrés dans les systèmes d'information d'une centaine de banques en 2013, ont dérobé au moins 300 millions de dollars, et agissent encore aujourd'hui, apprend Kaspersky.

C'est l'une des cyberattaques les plus sophistiquées jamais identifiées par Kaspersky. L'éditeur de solutions antivirus russe a dévoilé auprès du New York Times, lundi, les résultats d'une enquête menée depuis 2013 en partenariat avec Interpol et Europol. Conclusions : de 300 millions à 1 milliard de dollars ont été dérobés à une centaine de banques dans trente pays. Active depuis près de deux ans, la cyberattaque a toujours cours.

Pour ces raisons, l'éditeur reste volontairement imprécis sur les informations divulguées, ne fournissant pas, par exemple, le nom des établissements concernés. Les institutions sont basées principalement en Russie, au Japon, aux Etats-Unis et en Suisse. D'après le quotidien américain, JP Morgan Chase figure parmi les cibles.
Ce cybergang basé en Russie, Chine et Ukraine, « a franchi un nouveau cap » dans la méthode employée, souligne Kaspersky, en dérobant des fonds aux banques sans avoir à passer par les clients. L'attaque aurait débuté avec des infections classiques par hameçonnage, quand des employés de banque téléchargeaient malgré eux sur leur poste le malware nommé « Carbanak » – c'est également le nom de ce groupe de pirates.

Observer et imiter les transferts d'argent

Une fois bien installés sur les ordinateurs chargés des transferts de fonds ou de la compatibilité, il peuvent observer discrètement et patiemment les routines des employés et les processus des banques. Les pirates remontent ensuite sur les machines des responsables des transferts et des comptes, où ils installent un outil d'administration à distance (RAT) afin d'en prendre le contrôle et « d'imiter les activités normales ».
Ainsi, les assaillants peuvent créer de faux comptes pour y transférer de l'argent, a priori sans éveiller de soupçons. Si le hameçonnage n'a rien d'exceptionnel en soi, c'est l'aspect méthodique et la patience des pirates que Kaspersky pointe du doigt dans son rapport. De quoi leur avoir évité de s'être fait pincer à ce jour.
Ce qui a déclenché l'enquête remonte à la fin 2013 lorsqu'un distributeur s'est mis à émettre des billets en plein Kiev, en Ukraine. Alertée, la banque concernée a alors missionné Kaspersky. Lequel découvrira assez tôt que cette avarie allait en fait devenir, comparé à l'ampleur de la cyberattaque, le dernier souci de la banque.

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

S o u r c e :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-754433-kaspersky-cyber-attaque-banques.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_17/02/2015&partner=-&svc_position=865243299&svc_misc=-&crmID=639453874_865243299&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-754433-kaspersky-cyber-attaque-banques.html

Cybercrime : la fraude à un milliard de dollars

Cybercrime : la fraude à un milliard de dollars

La fraude est inédite par son ampleur : une centaine d'établissements financiers et de banques ont été victimes d'une cyberattaque encore jamais vue.(c) Shutterstock/EconomieMatin

La société de sécurité informatique Kaspersky Labs a mis au jour le pot aux roses, qui touche une trentaine de pays parmi lesquels la Russie, les États-Unis, l'Allemagne, la Chine, l'Ukraine ou encore le Canada. En tout et pour tout, c'est un milliard de dollars qui s'est évaporée des comptes de ces banques !

Interpol, sur le coup, reçoit l'aide des fins limiers de Kaspersky pour débusquer les pirates qui ont mis la main sur ce pactole. Il s'agirait, d'après les premiers renseignements, d'un groupe de hackers provenant de l'est de l'Europe (Russie et Ukraine), ainsi que de Chine.

Les méthodes employés, rapporte Interpol, marquent un tournant pour ce type d'infraction. Le processus mis en œuvre par les pirates relèvent d'une grande sophistication, qui leur permet de subtiliser l'argent « directement dans les banques », mais « sans avoir à viser ceux qui, au final, vont utiliser cet argent ».

Des méthodes redoutables donc, et transparentes, qui exploitent de nouvelles failles de sécurité et autres brèches dans les systèmes utilisés par les établissements bancaires. Et l'attaque se poursuit à l'heure actuelle.

Lire la suite….

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

Source : http://www.journaldeleconomie.fr/Cybercrime-la-fraude-a-un-milliard-de-dollars_a1994.html

---

Memex : Moteur de recherche

et nouvelle arme qui explore le Dark Web

	Memex : Moteur de recherche et nouvelle arme qui explore le Dark Web

Cette nouvelle arme a permis aux autorités américaines de démanteler un réseau de prostitution. Memex, le moteur de recherche développé et présenté en février par la Darpa, la branche de l'armée américaine spécialisée dans les réseaux, est utilisé depuis plus d'un an par les forces de l'ordre des Etats-Unis pour traquer toutes sortes de criminels. Ce moteur de recherche a la particularité d'explorer les tréfonds de la Toile.

Le Web invisible, terrain de jeu des criminels

«Certains estiment que Google, Microsoft et Yahoo ne nous donnent accès qu'à 5% du contenu du Web», explique Chris White, ingénieur de la Darpa, dans une interview accordée à la chaîne américaine CBS. Memex inspecte la partie invisible de la Toile, appelée le «Deep Web», plus vaste encore que ce que des moteurs comme Google explorent.

Ce Web «invisible» contient les pages non indexées par les moteurs, comme des pages éphémères, à faible trafic, ou des pages protégées par un logiciel spécifique, comme les réseaux anonymes Tor, connu notamment par les pirates. Ces pages sont un des principaux outils des différents réseaux criminels qui auraient ainsi publié pas moins 60 millions de pages ces deux dernières années, selon la Darpa.

Memex est capable d'indexer ce Web invisible pour aider les enquêtes dans les activités illégales trafic de drogue, de prostitution ou encore de pédophilie. Il peut aussi comprendre les liens entre les différentes pages et présenter les informations obtenues sous formes de graphiques, cartes, frises, etc.

«Il s'agit d'un bel exemple de la manière dont le Big Data peut aider à protéger les personnes vulnérables», estime Barack Obama dans le cadre de son rapport sur le Big Data, publié en janvier.

Et la protection des données personnelles?

Memex est actuellement au service de l'armée, mais ses applications pourraient également aider le secteur de la santé, en repérant par exemple précisément l'évolution géographique d'une épidémie. De belles perspectives, mais aussi de plus sombres.

La Darpa précise que ce nouveau moteur de recherche ultra-puissant n'a pas l'intention de collecter des données personnelles. Il en est cependant potentiellement capable. N'oublions pas le scandale du programme de surveillance Prism, révélé par Edward Snowden.

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

Source : http://www.20minutes.fr/web/1539339-20150212-memex-moteur-recherche-explore-dark-web

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

Dans le but d'encadrer le blocage de sites faisant l'apologie du terrorisme, la CNIL a nommé un magistrat en tant que conseiller honoraire à la Cour de cassation.

Le blocage des sites internet faisant l'apologie du terrorisme est une mesure contestée par les défenseurs des libertés sur le net. C'est sa nature qui laisse penser à une censure du web, d'autant plus que ce dispositif administratif n'a pas besoin de l'intervention d'un juge, qui fait débat.
Pour replacer un représentant de la loi au centre de ce dispositif contesté, la Commission nationale de l'informatique et des libertés (CNIL) vient de nommer Alexandre Linden en tant que conseiller honoraire à la Cour de cassation. Le rôle de ce magistrat sera d'encadrer le blocage des sites internet faisant l'apologie du terrorisme, une manière détournée de placer un représentant de la loi pour juger de la pertinence de chaque mesure.
Alors qu'une première liste de 10 à 50 URL doit être soumise à l'Unité de coordination de la lutte antiterroriste, les décrets publiés le 6 février dernier précisent que l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est chargé de mettre en œuvre la loi. Les fournisseurs d'accès auront 24 heures pour bloquer l'accès à ces sites suite à la décision de l'office.
Alexandre Linden aura donc son mot à dire dans ces décisions, mais reste à savoir les moyens qu'il aura à disposition pour agir.

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

Source : http://www.linformatique.org/la-cnil-place-un-conseiller-pour-encadrer-le-blocage-de-sites-terroristes/

Fuites subies par Anthem : une attaque lente et silencieuse

L'attaque menée contre Anthem, le second plus grand assureur aux États-Unis dans le domaine de la santé, qui a exposé les données personnelles identifiables de dizaines de millions d'assurés, n'était probablement pas un simple raid rapide mais plutôt un détournement continu et discret d'informations sur une période de plusieurs mois. L'attaque était conçue pour ne pas être détectée par les équipes informatiques et de sécurité de l'entreprise, et reposait sur un mécanisme d'infection par bot pour exfiltrer les données, explique Thierry Karsenti, Directeur Technique Europe de Check Point Software Technologies. Voici son analyse.

Selon les déclarations d'Anthem, les premiers signes de l'attaque sont apparus au milieu de la semaine dernière, lorsqu'un administrateur informatique a remarqué qu'une requête de base de données était exécutée à l'aide de son identifiant sans qu'il ne l'ait déclenchée. L'entreprise a déterminé qu'une attaque avait eu lieu, a informé le FBI et a engagé un consultant externe pour mener une enquête de sécurité.

Les enquêteurs ont constaté qu'un logiciel malveillant personnalisé a été utilisé pour infiltrer les réseaux d'Anthem et dérober des données. Le type exact de logiciel malveillant n'a pas été communiqué, mais il semble être une variante d'une famille connue d'outils de piratage. Un rapport de sécurité indépendant signale que l'attaque a pu commencer trois mois auparavant. Le consultant a remarqué une « activité de type botnet » dans des entreprises affiliées à Anthem en novembre 2014.
Ce n'est pas surprenant car les activités de bot à long terme sont courantes dans les entreprises. Le Rapport Sécurité 2014 de Check Point, basé sur la surveillance d'événements dans plus de 10 000 entreprises dans le monde entier, a constaté qu'au moins un bot a été détecté dans 73% des entreprises, contre 63% l'année précédente. 77% des bots étaient actifs pendant plus de quatre semaines, et communiquaient généralement avec leur « centre de commande et de contrôle » toutes les trois minutes.
Les bots sont capables d'échapper à toute détection car leurs développeurs utilisent des outils d'offuscation pour leur permettre de contourner les solutions antimalwares traditionnelles reposant sur des signatures. En tant que tel, l'émulation des menaces, également appelée « émulation en bac à sable », devrait être utilisée comme couche de défense supplémentaire pour stopper les bots avant qu'ils n'infectent les réseaux. Des solutions antibots devraient également être déployées pour faciliter la découverte des bots, et empêcher d'autres fuites en bloquant leurs communications.
Il est également important que les entreprises segmentent leur réseau, en séparant chaque segment par des couches de sécurité pour empêcher les infections de bot largement répandues. La segmentation peut restreindre les infections à une zone particulière du réseau pour atténuer les risques et empêcher les infections d'accéder à des données confidentielles dans d'autres segments du réseau.
Avec ces trois approches préventives, les entreprises peuvent réduire considérablement leur exposition au type d'attaque lente et furtive qui semble avoir frappé Anthem, et éviter de devenir la victime de fuites à grande échelle.

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

Source : http://www.itrmanager.com/articles/154049/fuites-subies-anthem-attaque-lente-silencieuse.html