Près de la moitié des Français confrontés à la cybercriminalité

Près de la moitié des Français confrontés à la cybercriminalité

Ransomware ou vol des données bancaires : près d'un Français sur deux (47%) a déjà été victime de cybercriminalité au cours de sa vie, selon l'étude annuelle Norton/Symantec révélée par Le Parisien / Aujourd'hui en France.

La cybercriminalité touche plus particulièrement les Français, puisque seulement quatre Européens sur dix sont confrontés à ce phénomène.
En détail, plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant qui permet au cybercriminel de demander de l'argent aux utilisateurs en échange de la décontamination de leur ordinateur, alors que 20% des Français confient avoir été victimes du vol de leurs données bancaires.
Ce rapport montre que les Français sont particulièrement méfiants vis-à-vis de la cybercriminalité. Plus de la moitié des sondés (55%) ont aujourd'hui plus peur de se faire voler leurs données bancaires en ligne que de se faire subtiliser leur portefeuille.
Plus de 17.000 consommateurs dans le monde ont été sondé cet automne pour les besoins de cette étude.

Réagissez à cet article
Source : http://www.lejdc.fr/france-monde/actualites/societe/techno/2015/11/30/pres-de-la-moitie-des-francais-confrontes-a-la-cybercriminalite_11685497.html

---

Le ransomware CryptoWall donne la migraine aux forces

de l’ordre

Le #ransomware CryptoWall donne la migraine aux forces de l’ordre

Bâti sur un labyrinthe de serveurs proxy, ce botnet est, pour l'instant, difficile à neutraliser. Pour se protéger, il faut faire des sauvegardes, mais pas n'importe comment.

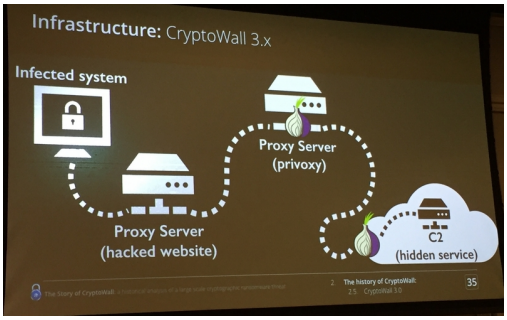
C'est l'un des plus importants « rançongiciels » du moment, et il le sera certainement encore pour un bout de temps. Car les pirates qui se cachent derrière ce néfaste malware ont mis en place un système pour l'instant assez inviolable et diaboliquement efficace. Bienvenue dans l'univers de CryptoWall.

Le chercheur en sécurité Yonathan Klijnsma de la société Fox IT est l'un de ceux qui essayent de pister ses auteurs. Il a profité de la conférence Botconf 2015, qui se déroule actuellement à Paris, pour présenter ses dernières analyses.

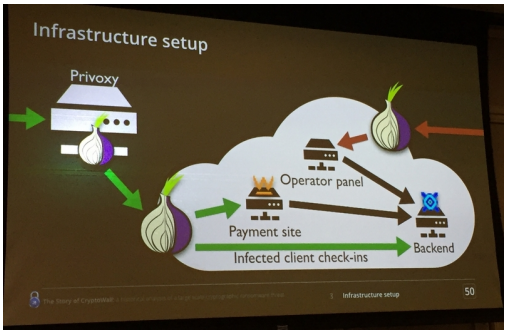
GK — Yonathan Klijnsma

Sur le principe, CryptoWall — qui existe actuellement dans sa version 4.0 — n'a rien d'original. Apparu pour la première fois en novembre 2013, ce code malveillant fonctionne un peu comme son aïeul Cryptolocker. Il infecte les ordinateurs et chiffre les fichiers qui s'y trouvent, ainsi que les noms de ces fichiers. Pour cela, il s'appuie sur les algorithmes AES 256bit et RSA 2048bit. Pour avoir une chance de récupérer ses données, il faut passer à la caisse. Plusieurs moyens de paiement sont acceptés : bitcoin, litecoin, UKash, moneypak, paysafecard, etc.
Ce qui rend ce malware si difficile à terrasser, c'est son infrastructure sous-jacente, composée d'une multitude de serveurs proxy en cascade, des intermédiaires qui servent essentiellement à brouiller les pistes. *« C'est un vrai labyrinthe. On ne sait jamais si la ressource que l'on a détectée est le véritable serveur de commande et contrôle, ou simplement un autre proxy »*, explique Yonathan Klijnsma.

Autre subtilité : le premier niveau de proxy est constitué de serveurs Web piratés. *« Ce sont de vrais sites totalement légitimes. Les propriétaires, évidemment, ne savent pas que leurs serveurs ont été détournés par des pirates. C'est assez malin de leur part, car cela complique le démantèlement du botnet. On ne peut pas simplement tirer le cordon. Il faut contacter chaque administrateur un par un »*, souligne le chercheur en sécurité.



© DR



© DR

Derrière le serveur Web piraté se trouve un autre proxy qui va faire le lien avec le réseau d'anonymisation Tor, dans lequel les pirates ont planqué toute leur infrastructure d'administration : les clés de chiffrement, le paiement, la diffusion de malware, etc. Tous ces « services » sont créés sous la forme de services Tor cachés (Tor Hidden Service). *« Pour les forces de l'ordre, c'est techniquement très difficile d'identifier les serveurs qui se cachent derrière »*, souligne Yonathan Klijnsma.
Pour avoir une chance de démanteler le réseau, il faut donc utiliser des méthodes d'investigation plus classiques, par exemple en infiltrant des forums de discussion. Mais cette méthode prend du temps et n'est pas forcément couronnée de succès.

Pour l'instant, ce cyberracket constitue donc quasiment le crime parfait. Les auteurs sont tellement insouciants qu'ils n'hésitent pas à se moquer ouvertement de leurs victimes, en les félicitant — sur l'un des écrans d'alerte — d'avoir rejoint *« la grande communauté CryptoWall »*.

Un malware d'origine russe ?

Certains éléments techniques semblent indiquer que les auteurs de CryptoWall — ou une partie d'entre eux — se trouvent en Russie. Un mécanisme dans le code évite, en effet, qu'il ne s'installe sur des ordinateurs qui se trouvent en Russie, en Biélorussie, en Ukraine ou au Kazakhstan. Ce type d'exception est typique pour des cybercriminels qui ne souhaitent pas avoir de problèmes avec les forces de l'ordre locales. *« En même temps, on ne peut jamais être sûr à 100 %. Cela pourrait être un faux indice »*, ajoute le chercheur.
En tant qu'utilisateur, pour se prémunir contre un fléau tel que CryptoWall ou consorts, le mieux c'est de faire des sauvegardes régulières de ses fichiers. Mais attention : pas n'importe comment. Il faut éviter les sauvegardes automatiques sur un disque en réseau sur lequel l'ordinateur est connecté en permanence. *« Dans ce cas, le malware ne va pas seulement chiffrer le contenu de l'ordinateur, mais aussi les sauvegardes »*, explique le chercheur. L'idéal, c'est donc de faire des sauvegardes régulières, mais à la main.

Réagissez à cet article
Source : http://www.01net.com/actualites/cryptowall-le-ransomware-qui-donne-la-migraine-aux-forces-de-l-ordre-934345.html
Gilbert KALLENBORN

La menace cyber-terroriste n’a jamais été aussi vaste

La menace cyber-terroriste n’a jamais été aussi vaste

Général d'Armée, Marc Watin-Augouard a cofondé en 2007 le Forum international de la cyber-sécurité. À l'heure des attentats, il revient sur les menaces de cyber-terrorisme qui pèsent sur les entreprises.

Le cyber-terrorisme est-il une réalité aujourd'hui ?

On le voit apparaître aujourd'hui autour de quatre phénomènes. Le premier, c'est l'atteinte aux contenus, comme l'effacement de sites. Suite aux attentats de janvier, 19.000 sites ont été effacés en France suite à des intrusions sur les serveurs, avec parfois la modification de données pour diffuser de la propagande ou de l'incitation au terrorisme. Le second phénomène, c'est l'utilisation du web par les terroristes à des fins d'organisation. Daesh n'aurait pas son visage actuel s'il n'existait pas un réseau mondial lui permettant de diffuser de l'information et des ordres. Le troisième aspect, c'est le recours des terroristes à la criminalité du cyber-espace pour se financer : vols de données bancaires, escroquerie, etc. Enfin, même si c'est une menace encore rare, il existe un danger d'attaque visant à bloquer ou saboter du matériel : en 2012, 30.000 ordinateurs de l'entreprise saoudienne Saudi Aramco ont été détruits à distance par des activistes. La menace cyber-terroriste n'a donc jamais été aussi vaste.

Toutes les entreprises peuvent-elles être concernées par ces menaces ?

Il ne faut jamais oublier que si une entreprise peut être une cible potentielle, elle peut être aussi un vecteur qu'on utilise pour mener une attaque en rebond. Regardez la chaîne américaine de magasins Target, qui a été victime en 2014 d'une cyber-attaque massive : elle a été touchée parce qu'on s'est d'abord infiltré chez un prestataire qui s'occupait de la climatisation des points de vente. Une entreprise peut donc être visée simplement parce qu'elle est sous-traitante de la « vraie » cible.

Quel est aujourd'hui le niveau de préparation des entreprises françaises face à ces cyber-menaces ?

Il y a une prise de conscience : nos entreprises sont en train de prendre très au sérieux ces dangers. C'est le cas tout d'abord des opérateurs d'importance vitale, qui travaillent dans les secteurs critiques, et qui doivent mettre en place des règles dans le cas de la loi de programmation militaire. Ces règles doivent d'ailleurs être aussi respectées par leurs sous-traitants, ce qui créé un effet de diffusion de l'hygiène informatique. Les entreprises ont également en face d'elles des assureurs qui s'intéressent de plus en plus à ces risques. Aujourd'hui, beaucoup d'entreprises s'organisent donc en commençant à faire remonter à l'échelon stratégique ce qui était considéré parfois comme un simple rouage technique. C'est positif.

Le problème, c'est que la cyber-sécurité coûte cher…

Oui, elle a un prix, mais les résultats d'une cyber-attaque aussi. Il y a des arbitrages à opérer. Mais si l'on se plonge dans le guide de l'hygiène informatique publié par l'Agence nationale de la sécurité des systèmes informatiques, on voit que nombre de ces prescriptions ne coûtent rien. Et qu'elles permettent d'annihiler 85 % des risques. Cela débute souvent avec la sensibilisation des personnels : une grande partie des cyberattaques est le fait de collaborateurs malveillants ou d'erreurs humaines dont les personnels sont les porteurs. L'arnaque de l'escroquerie au président commence par exemple par une interaction humaine. Le bon sens, l'organisation, la réflexion, cela n'a pas de coût.

Née dans la foulée des attentats de janvier, la loi sur le renseignement a brusqué les entreprises du numérique, notamment avec ces « mouchards » que sont les boîtes noires susceptibles d'aspirer des données. Comment réagissez-vous ?

Je comprends qu'on puisse dire que c'est une mauvaise loi, mais c'est de loin la meilleure. Et face aux problèmes qui sont aujourd'hui les nôtres, la question d'une éventuelle évasion à l'étranger de clients qui craindraient pour la confidentialité de leurs données me semble dépassée depuis quelques jours. On a trop souvent compris que cette loi reposait sur l'aspiration massive de données, ce n'est pas le cas : les boites noires ne transmettent pas de données nominatives et n'agissent que lorsque des algorithmes signalent des signaux faibles de comportement terroriste. Le point positif, c'est que cette loi amène opérateurs et hébergeurs à dialoguer avec l'État et que cela crée une co-responsabilité qui aidera à lutter contre les cyber-menaces.

Justement, n'y a t'il pas un problème de culture du web : né du militaire, il a aussi pris un virage libertaire. Comment concilier ces deux visages ?

Dans une pile électrique, il y'a deux pôles opposés, mais leur interaction crée la lumière. C'est la même chose dans le cyber-espace : il y a deux pôles, un sécuritaire et un libertaire. La peur est la fille de la sécurité, l'audace est la fille de la liberté. Il nous faut trouver la sagesse, l'équilibre. Aujourd'hui, nous avons besoin d'entendre les deux voix, et notamment celle des libertaires qui disent qu'il ne faut pas faire n'importe quoi au nom de la sécurité absolue. Le trop sécuritaire tuerait en effet le potentiel de croissance du web. Mais un cyber espace sans règles serait dominé par la loi du plus fort, avec des conceptions de la justice parfois très différentes. Dans le contexte actuel, il ne faut pas laisser les choses partir dans tous les sens : les actions contre Daesh menées par les Anonymous nous « arrangent » aujourd'hui, mais elles peuvent nous porter préjudice demain. Un des enjeux majeurs, c'est d'harmoniser la régulation mondiale du web. C'est une urgence. Il faut mettre fin au Far-West.

Réagissez à cet article

Source : http://www.lejournaldesentreprises.com/editions/44/chutier/la-menace-cyber-terroriste-n-a-jamais-ete-aussi-vaste-04-12-2015-275472.php

---

Le français Seolane détecte et neutralise les drones

malveillants

Le français Seolane détecte et neutralise les drones malveillants

L'entreprise a développé une station fixe au sol qui détecte la signature électromagnétique de ces engins volants. Sa solution intègre aussi un drone volant fourni par le groupe Eca qui se chargera d'identifier et de filmer le pilote avec une caméra embarquée.

Ce drone intervient dès lors que la station fixe a détecté un drone malveillant. © Seolane

Le survol illégal de drones au-dessus de bases militaires, centrales nucléaires et autres sites sensibles a mis à jour la nécessité d'identifier et de neutraliser les intrus. « *Ce marché devrait peser d'ici cinq ans entre 500 millions et un milliard d'euros* », estime Wilfrid Rouger, le fondateur et directeur général de Seolane une PME française créée en 2007 à Maisons-Laffitte (Yvelines).
Constituée d'une dizaine de personnes, l'entreprise est spécialisée dans l'intégration de systèmes de détection de signaux et de géolocalisation pour le transport et la sécurité. Le mois dernier, elle a remporté la première édition du concours Startup Challenge organisé le mois dernier par le salon Milipol, dédié à la sûreté des Etats.
Le prix récompense sa solution Dronelnt qui détecte, caractérise, traque et neutralise les drones malveillants avec une station fixe au sol. En cas de survol illégal d'un site, cette dernière va détecter la signature électromagnétique du drone et le localiser par radiogoniométrie. Une technique qui recourt à plusieurs capteurs pour localiser la position du drone par triangulation.

Drone fourni par Eca.

« *Nous avons lancé ce développement technologique il y a deux ans* », indique Wilfrid Rouger. Ce dernier a noué un partenariat avec le groupe Eca qui fournit un drone d'intervention. Fonctionnant de concert avec la station au sol, ce dernier dispose d'une autonomie allant jusqu'à 1h30 selon le modèle. Pour identifier le pilote et le filmer, l'engin volant embarque une caméra qui fonctionne de jour comme de nuit.
« *Plusieurs tests ont été réalisés avec succès avec la Gendarmerie nationale sur différents sites dont une centrale nucléaire* », fait valoir le directeur général de Seolane qui reçoit des demandes provenant de sites Seveso, aéroports et autres bases militaires qui s'inquiètent de l'explosion annoncée des vols illégaux de drones et des menaces terroristes.

Réagissez à cet article
Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article,I1602,Zoom-c1901a7c9c9d76e3b257db6e81734942.htm
Par Eliane Kan

Les 7 cyber menaces les plus exploitées chaque jour | Le

Net Expert Informatique

Les 7 cyber menaces les plus exploitées chaque jour

Les cyber-attaques qui frappent les États ou les grandes entreprises ont beau être celles qui font le plus régulièrement l'actualité, les cybercriminels usent tout autant de techniques d'escroqueries plus basiques mais tout aussi efficaces, ciblant les individus. La plupart des gens n'étant pas assez informés sur les cyber menaces ou ne suivant pas les mesures de cybersécurité classiques, restent la proie des hackers via des failles pourtant très connues, et exposent leur entreprise à des attaques beaucoup plus importantes.

Il vous qui se reconnaîtraient – ou l'un de leurs collègues ou amis – dans l'un des 7 profils décrit ci-dessous, il est encore temps de perfectionner vos compétences en matière de cybersécurité !

J'ai tendance à cliquer très (trop) rapidement
Un clic peut être suffisant pour être infecté par un virus ou pour être redirigé vers un site web malicieux. Les hackers sont très bons pour créer des contenus destinés à leurrer les utilisateurs et les inciter à cliquer. Ce contenu piégé peut être un message important – paraissant venir d'une personne ou d'une société que vous connaissez bien et en laquelle vous avez confiance – technique que l'on appelle le spear phishing. Il peut aussi simplement s'agir d'un spam, d'une publicité proposant une promotion trop belle pour être vraie ou encore d'une fausse enquête vous demandant de donner certaines informations personnelles.
Aussi, avant de cliquer, une bonne précaution à prendre est de survoler le lien hypertexte avec sa souris pour voir apparaître l'URL de destination et ainsi vérifier sa légitimité. Les liens de phishing contient toujours une petite erreur dans l'écriture du lien qui va donc mener vers un site factice ou infecter votre PC avec un malware. Deuxième précaution : portez plus d'attention aux comportements inhabituels. Une entreprise connue ne demande jamais des mots de passe et autres informations sensibles et n'envoie pas d'emails comportant des fautes d'orthographe ou des images de mauvaise qualité, etc. Bn d'autres termes, au moindre doute, ne cliquez pas !

J'ignore toujours les demandes de mises à jour
Les fournisseurs de solutions de sécurité investissent en permanence pour renforcer la sécurité de leurs produits face aux cyber-attaques et publient des patchs et mises à jour pour résoudre chaque problème rencontré. Toutefois, si ces mises à jours ne sont pas installées par les utilisateurs eux-mêmes, ceux-ci restèrent vulnérables aux attaques. Les navigateurs web sont le meilleur exemple d'outils utilisés au quotidien et pouvant facilement être exploités par les hackers. Lorsque l'on sait que seulement 18% des utilisateurs d'Internet Explorer utilisent la dernière version du navigateur, il est évident que les failles à exploiter pour les hackers sont nombreuses.

Je suis friand de free Wi-Fi
Les espaces de free Wi-Fi nous ont permis d'être plus connectés ou encore d'éviter les frais de connexion exorbitants lorsque nous sommes à l'étranger. Ces connexions étant ouvertes à tout le monde et ne contrôlé, il est très facile pour les hackers d'intercepter les données qui transitent via le Wi-Fi. Utiliser le Wi-Fi gratuit, c'est bien, mais il est clairement recommandé de ne pas consulter son compte en banque ou encore réaliser des achats en ligne avec sa carte d'identité lorsque l'on est connecté via un réseau Wi-Fi public. Dès lors que vous utilisez régulièrement un réseau de Wi-Fi public pour travailler, vous devez être en amure de vous connecter à un VPN pour renforcer la sécurité de votre connexion.

J'utilise des applications gratuites
Si vous êtes fan des dernières applications, jeux ou gadgets, vous devez savoir que certaines applications gratuites peuvent être infectées par des malwares. Celles-ci permettent aux hackers de collecter vos données à des fins malveillantes, sans que cela ne vous soit jamais notifié. Aussi, il est recommandé de télécharger des apps issues de sources connues.

J'utilise le même mot de passe pour tous mes comptes en ligne
Les hackers savent pertinemment que la plupart des gens réutilisent les mêmes mots de passe pour plusieurs sites. Ils vont ainsi dérober un mot de passe sur un site peu sécurisé et essayer d'utiliser ce même mot de passe sur des sites de vente très connus ou des réseaux sociaux sur lesquels vous pourriez avoir un compte, jusqu'à ce qu'ils trouvent des informations personnelles, financières ou même liées à votre entreprise. Le meilleur moyen de se prémunir de ce type de risques est d'utiliser des mots de passe compliqués et personnalisés pour chaque site web. Il existe de nombreux conseils en ligne pour savoir comment créer des mots de passe fort et facilement mémorisables.

Je ne verrouille jamais ma session
Le moyen le plus facile de dérober des données de valeur ou de pénétrer dans la vie privée d'une personne est d'accéder physiquement à son ordinateur non verrouillé puis de copier ses données ou de se connecter aux sites sur lesquels le mot de passe est enregistré et dont l'accès se fait automatiquement. Cela ne nécessite aucune compétence technique et, même si la personne est intentionnée est repérée par une caméra, cela ne permet absolument pas de la tenir pour responsable, en portant de la faille. Le conseil ici est évident, ne jamais laisser sa session ouverte sur son PC lorsque l'on s'absente.

Je partage énormément (trop) en ligne
Quel est le nom de jeune fille de votre mère ? Le nom de votre première école ? Le nom de votre première école ? Ce sont autant de questions de sécurité qui vous permettent de récupérer votre mot de passe oublié, et il serait bien dommage que quelqu'un puisse retrouver ces informations sur votre profil Facebook. Si vous êtes accro aux réseaux sociaux, mais que vous souhaitez vous protéger ainsi que votre entreprise des nombreuses menaces en ligne, vous pourriez commencer par restreindre l'accès à vos publications, à vos amis uniquement. Faites un nouveau tour sur votre profil et vérifiez les informations à quoi point cette ou cette information pourrait être utile si elle tombait entre de mauvaises mains.

De la même manière, informez-vous sur les termes et conditions des sites que vous fréquentez régulièrement dans la mesure ou certains d'entre eux pourraient déclarer collecter vos données et les utiliser pour de la publicité voire même les partager avec des sociétés tierces.

La cybersécurité commence avec vous ?
Aussi évoluée que soit la technologie, ce que l'utilisateur fait reste la plus grande partie de l'équation à résoudre. Les sites web que vous utilisez et l'entreprise pour laquelle vous travaillez peuvent faire le maximum pour assurer la protection de vos données, ils restent toutefois dépendants de vos actes. L'humain est le maillon faible de la sécurité, et pour changer cela nous devons tous prendre nos responsabilités et jouer notre rôle. Les bonnes pratiques de cybersécurité qui commencent à la maison, avec nos données et terminaux personnels, peuvent être facilement étendues à nos vies professionnelles.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Formateur n°93 84 03041 84

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

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

Source : http://www.globalsecuritymag.fr/Christophe-Jolly-Cisco-France-Les,20160728,64749.html
Par Christophe Jolly, Cisco France

Google For Education : un attrape-données personnelles ?

Google For Education : un attrape-données personnelles ?

Pour l'Electronic Frontier Foundation, Google profite de ses services Google For Education pour collecter et exploiter les données personnelles des élèves utilisateurs à son propre bénéfice et sans rapport avec l'enseignement. Google est pourtant signataire aux US d'un traité proscrivant ces pratiques.

Comme d'autres de ses concurrents, et notamment Microsoft, Google dispose d'une offre de services Cloud destinée spécialement aux acteurs de l'enseignement : Google For Education. Ce secteur est également un des principaux débouchés, aux Etats-Unis, pour le Chromebook.
Etudiants et enseignants sont depuis toujours des cibles de choix pour les fournisseurs de technologies. Mais Google pourrait aussi avoir un autre intérêt à être présent sur ce marché, un intérêt directement lié à son cœur de métier : la collecte et l'exploitation des données personnelles.

Chrome Sync par défaut sur Chromebook

Pour l'Electronic Frontier Foundation (EFF), Google a incontestablement dépassé les bornes en matière de données personnelles et surtout renié ses propres engagements. L'organisation vient à ce titre de saisir aux Etats-Unis le régulateur, la FTC.
En cause, les pratiques de la firme de Mountain View dans le cadre de son offre Google For Education. Selon l'EFF, Google piétine le « Student Privacy Pledge », un pacte signé par 200 entreprises, dont Google et qui encadre strictement les pratiques des fournisseurs en matière de confidentialité des données dans l'univers de l'enseignement.
Le « Student Privacy Pledge » proscrit ainsi la collecte, la conservation, l'utilisation et le partage des données personnelles des élèves hors des finalités touchant à l'enseignement. Google ne suivrait pas les règles en la matière, et ce de trois façons, juge l'EFF.
D'abord, lorsque les élèves se connectent avec leur compte Google for Education, la firme collecte les données personnelles des services non liés à l'enseignement et pour des finalités ne relevant pas non plus de l'enseignement.
Deuxième infraction : les ordinateurs Chromebooks disposent d'une fonctionnalité de synchronisation activée par défaut dans Chrome. Ce paramétrage permet ainsi à Google de collecter et d'exploiter intégralement l'historique de navigation, entre autres, des étudiants utilisant Google For Education. Et une fois encore sans que ces collectes de données relèvent des finalités admises.

Des pratiques trompeuses pour l'EFF

Enfin, Google a prévu dans les paramétrages d'administration de sa suite de services des paramètres autorisant sur les Chromebooks le partage des données des étudiants avec Google ainsi que des tiers. Or, le « Student Privacy Pledge » n'autorise pas un tel partage et une telle option n'aurait donc pas même dû être prévue à cet effet.
L'EFF demande donc au régulateur américain d'ouvrir une enquête sur les « agissements ou pratiques injustes et trompeurs » de Google, mais aussi d'exiger de la firme de détruire toutes les données des étudiants collectées jusqu'à présent en violation du « Student Privacy Pledge ».
Et cela pourrait faire beaucoup de données personnelles. Comme le rappelle ComputerWorld, Google revendiquait en octobre plus de 50 millions d'utilisateurs (élèves et enseignants) de Google For Education et 10 millions d'étudiants sur Chromebook.
Contacté par ComputerWorld, Google esquive les accusations formulées par l'EFF. La firme se déclare confiante dans le fait que ses outils respectent à la fois la loi et ses promesses, dont le Student Privacy Pledge.
Mais comme le signale l'EFF, Google a déjà reconnu au moins une mauvaise pratique et s'est engagé auprès de l'association à retirer l'activation par défaut de Chrome Sync sur les Chromebooks vendus aux établissements scolaires.

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/google-for-education-un-attrape-donnees-personnelles-39829148.htm

Nouvelle chaîne de Ponzi sur le bitcoin, Marchés Financiers

Nouvelle chaîne de Ponzi sur le bitcoin, Marchés Financiers

Aux Etats-Unis, le gendarme des marchés engage des poursuites contre deux sociétés du secteur du bitcoin. Il suspecte une nouvelle chaîne de Ponzi.

Le gendarme des marchés financiers américains, la Securities and Exchange Commission (SEC), annonce des poursuites contre deux sociétés – GAW Miners et ZenMiner – en charge de la création du bitcoin, la célèbre devise digitale. La création de cette devise et la validation des transactions sont assurées par des sociétés qui doivent résoudre de complexes calculs informatiques. Une activité coûteuse (électricité) et dont la rentabilité dépend du cours du bitcoin, ces sociétés étant rémunérées dans cette devise.
Deux d'entre elles ont promis à 10.000 investisseurs de s'associer à la création de bitcoins et d'en partager les bénéfices. Or la SEC estime que GAW et Zen ont en fait opéré une chaîne de Ponzi : l'argent collecté chez les uns a servi à attirer d'autres investisseurs pour les convaincre qu'ils participaient à un investissement sûr et rentable. La chaîne de Ponzi a opéré entre août 2014 et début 2015. Seulement, durant cette période, le bitcoin a perdu plus de la moitié de sa valeur, ce qui a commencé à éveiller des suspicions sur la réalité des rendements vantés.

Une série de tromperies
Le 11 septembre 2014, les présumés escrocs avaient assuré que l'intégralité des bénéfices seraient reversés aux victimes du 11 septembre 2001, pour le 13e anniversaire des attaques terroristes. Une nouvelle tromperie. Le 23 juillet 2013, le gendarme des marchés américains avait mis au jour une autre chaîne de Ponzi, organisée cette fois par un particulier texan. Ce dernier assurait pouvoir générer un rendement de 7 % par semaine. La SEC avait alors été très explicite : « Ce n'est pas parce les fraudeurs ont recours au bitcoin qu'ils peuvent échapper aux sanctions et se croire à l'abri des lois. Tout investissement financier sur le sol américain, en devises traditionnelles ou monnaies virtuelles, est du ressort de la juridiction de la SEC. »
Autour de 360 dollars, le bitcoin s'est habitué à ces vicissitudes, la devise connaissant des chaînes de Ponzi, le plus souvent de petite taille (quelques millions de dollars) et autres arnaques de manière récurrente. Dans le secteur, on a tendance à dédramatiser ce type « d'incidents », jugés inévitables pour une devise jeune et décentralisée. Faire le ménage dans ce secteur est le meilleur moyen d'assurer l'avenir du bitcoin.

Réagissez à cet article
Source : http://www.lesechos.fr/finance-marches/marches-financiers/021527837471-nouvelle-chaine-de-ponzi-sur-le-bitcoin-1180949.php

Contrefaçon : Interpol s’attaque à un millier de sites vendant des produits interdits

Contrefaçon : Interpol s’attaque à un millier de sites vendant des produits interdits

Les services des douanes ont mené conjointement avec Interpol plusieurs mesures pour identifier et stopper l'activité de sites de vente de produits contrefaits.

Un millier d'entre eux ont été visés par les autorités.

Interpol annonce qu'un millier de sites proposant l'achat de produits contrefaits ou piratés ont été identifiés. Les autorités ont mené de nouvelles opérations conjointes des services policiers américains et européens.

« Les consommateurs du monde entier utilisent Internet pour acheter des biens de la vie de tous les jours et les criminels en profitent » pour vendre des produits « illégaux », estime le directeur de la branche crime organisé chez Interpol, Roraima Andriani.

Une vingtaine de pays ont pris part au 6e volet d'une opération baptisée « In our sites », dont la Belgique, la Bulgarie, la Colombie, la Croatie, le Danemark, la France, la Grèce, le Portugal, la Roumanie, l'Espagne ou le Royaume-Uni.

Ce type d'opération est désormais régulier. Chaque année, les autorités américaines et européennes dévoilent des listes de sites destinés à être fermés pour vente de produits contrefaits. Ces investigations surviennent lors de grandes occasions comme Noël, les soldes ou encore la Saint-Valentin.

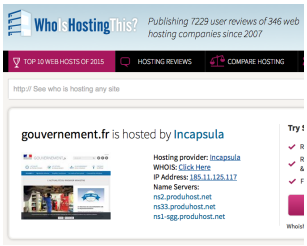
Réagissez à cet article

Source : http://pro.clubic.com/actualite-e-business/actualite-788224-contrefacon-internet.html

Le site web du gouvernement français utilise un CDN « made in USA »

Le site web du gouvernement français utilise un CDN « made in USA »

Le site web du gouvernement français est hébergé en France, mais utilise le CDN d'un opérateur états-unien. Étrange, car plusieurs opérateurs français ont des offres en la matière. Et savez-vous qui héberge le site web du Noël de la French Tech ?



Le site web du gouvernement français est en partie « made in USA » Vendredi dernier, le gouvernement subissait quelques sarcasmes pour avoir lancé, depuis son site web www.gouvernement.fr, un « concours de selfies tricolores » à l'occasion de l'hommage national aux victimes des attentats djihadistes du 13 novembre à Paris. Je suis allé sur le site web de notre exécutif pour voir ce qu'il en était de cet appel et il m'a semblé que les temps de réponse n'étaient pas excellents. J'ai alors utilisé la commande traceroute, qui m'a donné ce résultat :

```
> traceroute www.gouvernement.fr
traceroute: Warning: www.gouvernement.fr has multiple addresses; using 8.253.93.126
traceroute to cdn2.cdn-tech.com.c.footprint.net (8.253.93.126), 64 hops max, 52 byte packets
1  10.60.1.254 (10.60.1.254)  1.542 ms  0.814 ms  0.711 ms
2  reverse.completel.net (46.218.145.105)  2.448 ms  5.900 ms  3.290 ms
3  * * *
4  172.19.130.117 (172.19.130.117)  29.751 ms  30.536 ms  28.127 ms
5  te0-5-0-13.ccr21.par04.atlas.cogentco.com (149.6.164.101)  28.094 ms  26.642 ms  27.093 ms
6  level3.par04.atlas.cogentco.com (130.117.14.94)  27.026 ms  27.511 ms  20.037 ms
7  * * ae-3-80.ear2.paris1.level3.net (4.69.168.140)  21.277 ms
8  * * *
```

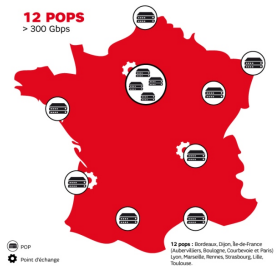
J'ai exécuté à nouveau cette commande, quelques minutes plus tard :

```
> traceroute www.gouvernement.fr
traceroute: Warning: www.gouvernement.fr has multiple addresses; using 204.160.107.126
traceroute to cdn2.cdn-tech.com.c.footprint.net (204.160.107.126), 64 hops max, 52 byte packets
1 10.60.1.254 (10.60.1.254) 1.431 ms 0.691 ms 0.694 ms
2 reverse.completel.net (46.218.145.105) 4.667 ms 2.219 ms 5.282 ms
3 * * *
4 172.19.130.113 (172.19.130.113) 16.804 ms 17.153 ms 15.894 ms
5 te0-0-0-3.rcr11.b015531-1.par05.atlas.cogentco.com (149.6.166.45) 26.342 ms 54.703 ms 30.250 ms
6 be2337.rcr21.par05.atlas.cogentco.com (130.117.1.1) 20.723 ms 29.652 ms 29.864 ms
7 be2424.ccr41.par01.atlas.cogentco.com (130.117.2.237) 30.037 ms
be2425.ccr42.par01.atlas.cogentco.com (130.117.3.205) 53.502 ms
be2424.ccr41.par01.atlas.cogentco.com (130.117.2.237) 33.899 ms
8 be12308.ccr21.par04.atlas.cogentco.com (130.117.49.42) 19.653 ms
be12309.ccr21.par04.atlas.cogentco.com (154.54.39.66) 22.496 ms
be12308.ccr21.par04.atlas.cogentco.com (130.117.49.42) 29.791 ms
9 level3.par04.atlas.cogentco.com (130.117.14.94) 28.197 ms 54.186 ms 30.102 ms
10 ae-32-80.car2.paris1.level3.net (4.69.168.131) 29.984 ms
11 ae-12-60.car2.paris1.level3.net (4.69.168.3) 16.255 ms 12 ae-42-90.car2.paris1.level3.net (4.69.168.195) 20.175 ms
13 * * *
```

Ces éléments techniques ne laissent aucun doute : le site officiel du gouvernement français est accessible via plusieurs IP différentes, il utilise très probablement un Content Delivery Network – ou CDN – et en l'occurrence il semble bien s'agir du CDN de l'opérateur états-unien Level3 Communications, un des plus importants opérateurs Internet au monde.
Surpris, j'effectue alors une autre recherche via le site WhoIsHostingThis : selon cette source d'information technique, le site serait « hébergé par » Incapsula.

En creusant un peu, il apparaît que Incapsula propose du CDN. Serait-il basé sur le réseau de Level3 ? On peut le penser puisque, selon cette page, « *Incapsula's CDN runs on top of major Tier 1 provider networks* »
Je pense que l'on peut légitimement se poser des questions sur les risques d'atteinte à l'intégrité du contenu diffusé à partir du site du gouvernement français. En effet, il est avéré que le gouvernement des USA ne se prive pas d'espionner tous les gouvernements étrangers, y compris en Europe, et même des entreprises privées. **Soyons un peu paranoïaques, et imaginons que des agences gouvernementales des USA souhaitent manipuler l'opinion publique française** : il ne serait pas très difficile de « faire mentir le CDN » et de lui faire remplacer des portions de contenu issus d'un site web par d'autres. Le CDN, situé entre le site web de notre gouvernement et les citoyens de notre République, pourrait substituer à dessein une photo truquée à une photo authentique, remplacer un texte, par exemple un discours officiel, par un autre, etc.

Vous imaginez le pouvoir d'influence sur l'opinion publique française que cela procurerait ?
J'ai contacté Romain Pigenel, directeur adjoint en charge du numérique au Service d'Information du Gouvernement. Il m'a assuré que le site web du gouvernement était bien hébergé en France, sur des serveurs situés à l'intérieur du territoire national. Et d'ailleurs la page de mentions légalesdu site indique explicitement « *Hébergement Alter Way Hosting*» .
Rappelons que cela fait plus de 3 ans que de grands opérateurs français ont lancé des offres de CDN : si l'offre CDN d'Orange a été construite en partenariat avec Akamai, encore un acteur venu des États-Unis, en revanche l'offre CDN de SFR a été conçue par des équipes françaises. Ce CDN repose sur des infrastructures de proximité, déployées en 12 points du territoire national et tirant profit des points de peering régionaux disponibles à Paris, Lyon et Bordeaux :

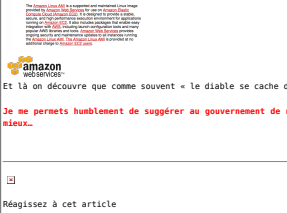


Le Noël de la French Tech hébergé… chez Amazon !

Autre épisode un peu malheureux, avec l'annonce hier matin par Axelle Lemaire de l'opération « **Noël de la French Tech** » :

Il s'agit d'une excellente initiative qui fait découvrir de nombreux produits, issus de startups françaises, susceptibles d'être offerts lors des fêtes de fin d'année. Je trouve tout à fait positif de mettre un coup de projecteur sur des entreprises françaises et de contribuer, fût-ce de façon marginale, à améliorer la balance de notre commerce extérieur, qui souffre du fait que les produits électroniques, informatiques et technologiques sont très majoritairement importés.
Mais malheureusement un afflux de connexions sur le site promu par la secrétaire d'État chargée du numérique a quelque peu perturbé son fonctionnement :

Du coup, en tapant www.noeldelafrenchtech.fr, je suis arrivé sur cette page :



Et là on découvre que comme souvent « le diable se cache dans les détails » : ce site web est hébergé dans le cloud d'Amazon… alors que les offres d'hébergement made in France ne manquent pas.

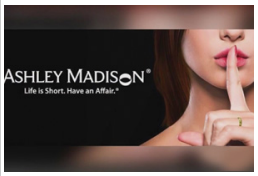
Je me permets humblement de suggérer au gouvernement de redoubler d'efforts pour mettre ses actes en accord avec sa communication : promouvoir les entreprises technologiques françaises c'est bien, utiliser leurs services en toute occasion où c'est possible c'est encore mieux…

Réagissez à cet article
Source : http://www.zdnet.fr/actualites/trange-le-site-web-du-gouvernement-francais-utilise-un-cdn-made-in-usa-39829142.htm
Par Pierre Col

L’individu cible des cyber attaques

L’individu cible des cyber attaques

Si les cyberattaques les plus marquantes ont visé des grands comptes ou des acteurs industriels majeurs, les PME se voient de plus en plus menacées. Reste à faire comprendre à un dirigeant, qu'au-delà de la taille de son entreprise, ce sont les individus – lui compris – qui sont visés.



En août 2015, les données (32 millions de comptes) du site de rencontres extraconjugales, Ashley Madison, ont été piratées.
Tavish Vaidya, doctorant de l'université de Georgetown à Washington, documente depuis quelques années le nombre et l'importance des cyberattaques du XXIe siècle. Il livrait récemment dans la MIT Technology Review, son top 20 où l'on retrouve l'assaut du ver Stuxnet sur des centrifugeuses iraniennes en 2010 ou l'infection en décembre 2013 par des hackers chinois des ordinateurs de membres européens du G20 lors de la réunion de l'organisation internationale à Saint-Pétersbourg.

La faille est toujours humaine

Mais la nature de ces cyberattaques très médiatisées, qui ont touché de grandes organisations, ne joue pas forcément à l'avantage de ceux qui veulent provoquer une prise de conscience chez les dirigeants.
« Longtemps, la cybersécurité n'a concerné que les grands comptes. Et, chez la majorité de nos interlocuteurs en entreprise, la réponse reste encore : "ces sociétés sont très connues. Ce n'est pas comme nous, qui sommes beaucoup plus petits… Et ceci, même si la donne a changé" », explique Sergio Loureiro, président et cofondateur de SecludIT, une start-up créée en 2011 qui propose de réaliser en continu des scans automatiques de vulnérabilité sur les infrastructures des entreprises.
« Nous constatons que les grands groupes ont progressivement élevé leur niveau de sécurité, compliquant et rendant moins intéressant le fait d'attaquer directement leurs systèmes. Par contre, cela a encouragé les assaillants à s'en prendre aux PME… qui sont souvent leurs prestataires », détaille PierreYves Popihn, directeur technique de NTT Com Security (ex-Integralis), la filiale cybersécurité du groupe de télécommunications japonais.
Les entreprises, de plus en plus ouvertes sur leur écosystème, risquent alors de se compromettre les unes les autres… Malgré ses impacts résolument business, la cybersécurité traîne une étiquette trop « technique » auprès des directions générales, qui s'en défaussent sur le responsable de la sécurité des systèmes d'information (RSSI) ou le responsable informatique. Or, le message martelé par les experts est tout autre : dans la majorité des cas, la faille est humaine.
« 100 % des entreprises que nous testons ont au moins une faille critique dans leur système d'information, et nous sommes toujours arrivés à accéder à des informations confidentielles sur les collaborateurs ou les clients… Mais une fois qu'un attaquant a mis le pied dans l'entreprise, il va viser des individus en particulier, pour obtenir davantage, fait valoir Sergio Loureiro. Dans ces conditions, le PDG peut tout aussi bien être le maillon faible que la standardiste. »
Un exemple récent illustre justement le rôle important de « l'ingénierie sociale » pour exploiter les failles de sécurité.

Une lutte d'ego

La société BRM Mobilier, PME des Deux-Sèvres spécialisée dans l'aménagement de médiathèques et bibliothèques, a été placée en redressement judiciaire début septembre 2015, après que des malfaiteurs se sont fait passer tour à tour, par e-mail et téléphone, pour le président de cette entreprise de 44 salariés, et pour ses avocats. Les juges ont prononcé le redressement judiciaire avec poursuite des activités jusqu'au 11 mars 2016, le temps de retrouver un repreneur éventuel. Cette « arnaque au président » a permis de détourner 1,6 million d'euros par l'intermédiaire de la responsable administrative et financière de la société. *« Contrairement à une attaque à base de code malicieux, où un collaborateur ouvre une fausse pièce jointe d'e-mail, par exemple une facture, l'arnaque au président ne fait pas appel à un malware, il s'agit avant tout d'une escroquerie »*, note Charles Rami, expert cybersécurité chez Proofpoint, une entreprise américaine qui se spécialise notamment sur la protection des e-mails.
« Dans le cas de BRM, l'arnaque n'a sans doute pas été montée au hasard. Elle s'est déroulée juste après une importante entrée d'argent. Il est possible que l'entreprise ait été préalablement infectée par un cheval de Troie étudiant l'environnement financier et bancaire de l'entreprise. L'usurpation de l'identité en e-mail, elle, est très simple techniquement », décrit-il plus précisément. Un avis partagé par Pierre-Yves Popihn, qui estime que 15 % des cyberattaques en France servent avant tout à faire de la reconnaissance pour se voir ensuite presque littéralement « ouvrir la porte » de l'entreprise par un de ses salariés ou le dirigeant lui-même.

Cette usurpation d'identité peut-elle provoquer un déclic chez les dirigeants ?

« Tout le monde est concerné, mais deux populations sont très sensibles. Les personnes du service IT qui testent des usages et des technologies dans l'entreprise comme ils le feraient à leur domicile ; et les membres du top management, qui souhaitent connecter au SI leurs propres outils, leur smartphone personnel par exemple, même si cela peut entraîner des complications en termes de sécurité. Ces acteurs disposent souvent de comptes à privilège, c'est-à-dire des "clés" du système d'information, même quand cela n'est pas nécessaire au quotidien », témoigne Sandro Lancrin, architecte Sécurité SI et RSSI de Radio France.
Il souligne d'ailleurs, que cette problématique des individus revient trop régulièrement à une lutte d'ego, un directeur s'offusquant que l'un de ses subalternes dispose de droits informatiques et pas lui…

> **"Toutes les entreprises que nous testons ont au moins une faille critique dans leur SI"**
> Sergio Loureiro
> *président et cofondateur de SecludIT*

Malgré tout, la « conscience cyber » fait petit à petit son chemin en entreprise. Les affaires grand public, comme le vol de données du site d'adultère Ashley Madison l'été dernier, contribuent à attirer l'attention. *« C'est à double tranchant,* note Mounir Chaabane, conférencier Eucles pour l'Institut national des hautes études de la sécurité et de la justice, une émanation de la délégation interministérielle à l'Intelligence économique, *en donnant tant de visibilité à des affaires comme l'arnaque au président de BRM ou Ashley Madison, on se focalise sur des cas presque anecdotiques vu la diversité des formes que peut prendre une attaque. Ce vers quoi il faudrait tendre, c'est une culture qui mette les individus en face de leurs responsabilités, qu'ils soient PDG, trésorier, agent des ressources humaines ou administrateur système. »* Une culture bien plus présente dans d'autres pays, de la Finlande aux Etats-Unis, où des dirigeants ont déjà été tenus responsables des conséquences de cyberattaques menées contre leurs entreprises, et mis à la porte. Ainsi, le PDG et fondateur d'Ashley Madison n'a pas tardé à quitter son poste : l'an dernier, dans un entretien télévisé, il avait décrit les serveurs du site comme étant « impénétrables »…

A lire également

Suite à l'affaire BRM de Bressuire, la chambre de commerce et d'industrie des Deux-Sèvres a publié un guide « Spécial Arnaque », destiné aux chefs d'entreprise face aux nouvelles formes d'escroquerie, notamment la cybercriminalité. Pour le consulter : http://bit.ly/1ijoKRH.
Lire aussi les 22 fiches thématiques sur « La sécurité économique au quotidien », publiées par la Direction interministérielle à l'intelligence économique, http://bit.ly/1iOEGow

---

Réagissez à cet article
Source : http://www.alliancy.fr/a-laffiche/securite/2015/11/30/cybersecurite-lindividu-pour-cible