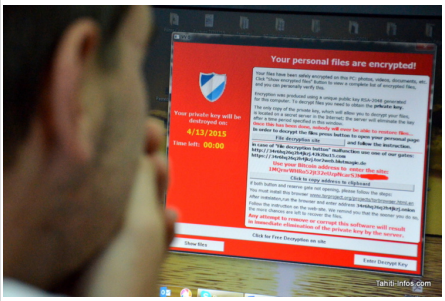
Attaque informatique importante contre les administrations et entreprises de Polynésie

Attaque informatique importante contre les administrations et entreprises de Polynésie

Depuis jeudi dernier, une attaque informatique de grande ampleur touche les services du Pays, de l'Etat et des entreprises de la Polynésie française. Le virus s'introduit sur les postes de travail par les mails, jeux flash et sites contaminés…



Les services informatiques du Territoire, de l'Etat et des entreprises sont en alerte rouge depuis bientôt une semaine : un virus s'est introduit sur de nombreux postes de travail et contamine même des serveurs au cœur de l'infrastructure des administrations et sociétés.

Un message de ce type peut accueillir les internautes imprudents

Ce virus est particulièrement vicieux, pour deux raisons. La première est qu'il est très évolué. Ce logiciel malveillant de dernière génération (une évolution de TeslaCrypt-2.0, détecté pour la première fois en juillet dernier) n'était pas encore identifié par les éditeurs d'anti-virus la semaine dernière. Kaspersky, la solution de sécurité du Pays et l'un des meilleurs du domaine, n'a mis à jour sa base de données virale contre cette nouvelle version qu'il y a deux jours.

La deuxième raison est le type d'attaques que commet ce virus : c'est un crypto-locker, aussi appelé « ransomware » pour « logiciel de rançon ». Une fois introduit sur les ordinateurs des victimes, il encrypte tous les fichiers du disque-dur puis demande une rançon pour rendre ses données à son propriétaire. Mais payer ne garantirait même pas le retour de toutes les données intactes…

NE PAS PAYER MAIS DEMANDER DE L'AIDE

Le conseil est de ne pas payer : « on ne peut pas décrypter les fichiers, mais des solutions existent pour récupérer les données. On peut essayer de revenir à des versions antérieures du fichier, sauvegardées automatiquement par Windows… Il y a aussi des façons de récupérer les fichiers originaux supprimés par le virus » nous explique un expert du CLUSIR (une association d'experts en informatique du Pays), qui assure qu'il ne faut pas céder à la panique. Il explique qu'en cas de contamination, il faut immédiatement éteindre le poste et le déconnecter du réseau, puis contacter son service informatique ou son prestataire informatique.

La situation semble désormais maitrisée dans les administrations après une sacrée frayeur. Nous avons ainsi appris que la direction de la Santé, l'Aviation civile, la direction des Ressources Marines et Minières, le palais de justice ou encore la clinique Paofai ont été attaqués. Certains serveurs auraient été contaminés et des bases de données rendues inaccessibles, par exemple celles de localisation des pêcheurs… Qui aurait été récupérée.

DES POSTES CONTAMINÉS VIA LES JEUX EN LIGNE

Les pirates utilisent des logiciels spéciaux pour infecter des sites web très populaires mais mal protégés. Ensuite, le « toolkit » essaiera de pénétrer les ordinateurs de tous les internautes qui visiteront ce site en testant les failles de sécurité connues. Pour vous protéger, gardez votre version de Windows, Flash, Javascript, votre navigateur etc. à jour.

On ne sait pas encore si c'est une attaque délibérée d'un groupe de pirates informatique – les mafias du monde entier se sont mises à ce nouveau modèle d'extorsion très juteux – ou s'il s'agit justes d'attaques aléatoires qui touchent particulièrement la Polynésie à cause de simples effets réseaux (un seul poste qui tombe et tout le réseau est contaminé ; un chef de service qui se fait avoir et tout son carnet d'adresses reçoit le virus par mail…). Les experts penchent pour la deuxième hypothèse, d'autant que le malware fait parler de lui dans le monde entier depuis quelques jours.

Les services informatiques qui luttent contre l'attaque en ce moment même nous confient que le principal point d'entrée du virus dans les réseaux était… Les sites de jeux en ligne contaminés par les pirates. Ensuite le virus a réussi à se répandre sur les réseaux des administrations puis des entreprises, jusqu'aux serveurs de fichiers du Pays par exemple, qui ont tous été passés en mode « lecture seule » ce mercredi pour essayer d'achever le virus.

L'autre mode de contamination : les fichiers attachés (particulièrement ceux ayant les extensions .js, .zip et .exe) et… les sites porno. Le meilleur conseil reste celui d'un informaticien contacté pour cet article : « Cette attaque c'est pour tout le monde, il est vraiment temps de faire vos sauvegarde. »

Les conseils de prudence du service informatique du Pays

Depuis le début de l'attaque contre les services du Pays, les informaticiens du Territoire sont sur le pied de guerre contre ce virus particulièrement sophistiqué. Plusieurs sources nous ont transmis les mails reçus dans toute l'administration territoriale, dont voici un extrait du dernier en date :

« Suite aux précédents courriels que nous vous avons envoyés, nous souhaitons vous tenir informés de l'évolution de l'infection virale. Elle touche aussi désormais d'autres sociétés de Polynésie française. La situation est inquiétante. (…)

Mise à jour de la définition virale

Nous vous demandons de vérifier que votre anti-virus Kaspersky est à jour. Pour cela, placer la souris sur l'icône « K » en bas à droite de votre bureau : la date d'édition des bases ne doit pas être antérieure à deux jours. Dans le cas contraire, merci de bien vouloir contacter le support du service informatique.

Sauvegarde de vos données personnelles

Nous vous rappelons aussi que vous devez faire des sauvegardes de vos données professionnelles se trouvant sur votre poste de travail. Les serveurs de fichiers étant en lecture seule, sauvegardez vos données professionnelles sur un support externe (disque USB, clé USB), ne pas oublier de le déconnecter à la fin de la sauvegarde.

Rappels sur des règles de sécurité

Afin de vous protéger des virus qui sévissent actuellement, nous vous demandons de suivre scrupuleusement les consignes de sécurité suivantes :

– ne pas ouvrir des courriels suspects (expéditeur inconnu, objet du courriel rédigé en anglais…)

– ne pas ouvrir les pièces jointes à un courriel suspect, en particulier, ne surtout pas ouvrir les fichiers se terminant par l'extension .js. »

Réagissez à cet article

Source : http://www.tahiti-infos.com/Attaque-informatique-importante-contre-les-administrations-et-entreprises-de-Polynesie_a141657.html

---

Un malware qui reste lors d'une réinstallation du

système d’exploitation

Un malware qui reste lors d’une réinstallation du système d’exploitation

Conçu en particulier pour dérober des données bancaires, l’écosystème Nemesis comporte un logiciel malveillant qui s’installe à très bas niveau sur le disque dur.

Les équipes de Mandiant (FireEye) ont découvert, en septembre dernier, un logiciel malveillant employant des méthodes de persistance peu communes : il s’immisce dans le processus d’initialisation de l’ordinateur infecté, avant même le chargement du système d’exploitation, afin de pouvoir compromettre celui-ci à coup sûr et, surtout, résister à une tentative de nettoyage de la machine par réinstallation de son système d’exploitation – « un moyen largement considéré comme le plus efficace pour éradiquer un logiciel malveillant », soulignent les chercheurs de FireEye dans un billet de blog.

Analyse comportementale : la clé de la sécurité ?

E-handbook : L’analyse comportementale joue un rôle non négligeable dans la sécurité de votre entreprise.

Ce logiciel malveillant fait partie de Nemesis, un ensemble d’outils malicieux utilisé par le groupe FIN1, qui semble « localisé en Russie, ou un pays russophone », spécialisé dans le vol de données de cartes bancaires et, plus généralement, d’informations « aisément monétisables en provenance d’organisations telles que banques, organismes de crédit, opérations de DAB », etc.

Comme le rappellent les chercheurs de FireEye, le secteur d’amorçage des disques durs, le fameux MBR (Master Boot Record), ne contient pas que des données inertes relatives aux partitions définies : il recèle également quelques éléments de code utilisés durant le processus de démarrage ; « ce code cherche la partition active principale et passe ensuite le contrôle au VBR (Volume Boot Record) de cette partition ». Ce dernier contient également du code exécutable « spécifique au système d’exploitation présent sur cette partition », et lui permettant de lancer son démarrage.

Baptisé Bootrash, le logiciel malveillant découvert par les équipes de Mandiant, pirate ce processus en remplaçant le code d’amorçage du VBR par son propre code malicieux chargé d’appeler le bootkit Nemesis. Celui-ci « intercepte certaines fonctions du processus de démarrage et injecte les composants Nemesis dans le noyau de Windows ».

Les chercheurs de FireEye soulignent que ce n’est pas une première, mais que l’utilisation d’un bootkit MBR ou VBR n’est pas courant. Une chance, peut-être, car la détection peut s’avérer particulièrement difficile : ces logiciels malveillants peuvent « être installés et s’exécuter presque complètement en dehors du système d’exploitation Windows », passant au travers des mécanismes de vérification de son intégrité ou encore des anti-virus – à moins d’examiner méticuleusement la mémoire vive.

Réagissez à cet article

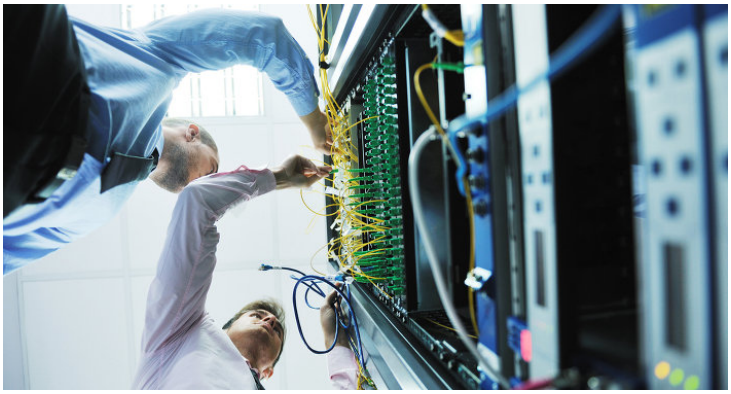
Source : http://www.lemagit.fr/actualites/4500260472/Un-malware-qui-reste-lors-dune-reinstallation-du-systeme-dexploitation

La fin des cartes bancaires est-elle proche?

La fin des cartes bancaires est-elle proche?

D'ici 5 ans, selon les prévisions, il n'y aura plus ni argent liquide, ni cartes bancaires. Ces changements marqueront un tournant dans notre quotidien. De même que dans la cybercriminalité.

En 2015, les pertes de la Russie liées à la cybercriminalité s'élèveront à un milliard de dollars, a déclaré le vice-président de la direction de la banque russe Sberbank Lev Khassis, ajoutant que dans 5-7 ans la carte bancaire, telle qu'on la connaît aujourd'hui, n'existerait plus. Pour payer, on utilisera alors différents appareils mobiles.



© FOTOLIA/ .SHOCK
La NSA disposerait d'un nouveau logiciel espion

Les pays scandinaves ont déjà l'intention de tenir un référendum pour arrêter l'usage de billets de banque. Leur réponse positive débouchera sur la disparition des distributeurs de billets.
« Les changements n'auront pas lieu dans tous les pays à la fois, estime Evgueni Kaspersky, directeur général de Kaspersky Lab. L'argent liquide se maintiendra au cours des cinq prochaines années. Tour à tour, les pays pourraient en outre interdire l'usage des bitcoins en tant que crypto-monnaie », remarque-t-il.
La monnaie virtuelle (bitcoin) et l'argent liquide auront la même popularité auprès des escrocs, estime Kaspersky. Par exemple, les rançons pour piratage des systèmes informatiques sont exigées en cybermonnaie. En Russie, le bitcoin est interdit, ce qui ne signifie pas le refus de la technologie elle-même. Les institutions financières adoptent à l'heure actuelle la technologie qui est actuellement utilisée par les créateurs de la crypto-monnaie.

« C'est une technologie géniale. On peut l'utiliser pour les transactions intra-bancaires. Elle peut aussi être utilisée pour l'identification des internautes », dit Kaspersky.

© FLICKR/ BTC KEYCHAIN
Une nouvelle monnaie va voir le jour en Europe

Le retrait de la circulation du papier monnaie marquera un vrai tournant dans la cybercriminalité: les escrocs s'installeront désormais sur Internet et le nombre de cyberattaques va augmenter. En 2015, on en enregistrait déjà 300 en moyenne chaque jour.
Une autre tendance de l'année 2015 qui perdurera en 2016 est l'essor du nombre des bandes des cybercriminels prêtes à attaquer différents systèmes opérationnels pour voler de l'argent ou espionner la personne en téléchargeant l'information. « La législation sur la cybercriminalité est insuffisante », estime M. Khassis.

Réagissez à cet article
Source : http://fr.sputniknews.com/economie/20151210/1020180651/carte-bancaire-bitcoin-cybercriminalite.html

CyberDélinquence ou CyberCriminalité ? Le terreau de l’argent facile et des créatures de rêve

	CyberDélinquence ou CyberCriminalité ? Le terreau de l’argent facile et des créatures de rêve

La cybercriminalité ou la Cyberdélinquence est devenue un fléau des temps modernes. Mais facile à comprendre. Cependant, qui s'y frotte s'y pique. Tous ceux qui aiment l'argent facile, les belles filles, les sensations fortes, les Bon chics bon genre sont les principales victimes.

Internet est devenu incontournable avec certes des avantages et des inconvénients. Mais en face, il y a des hommes et des femmes prêts à tout, pour détourner les objectifs.

Phénomène de ces dernières années, la cybercriminalité est devenue un fléau.

Les réseaux sociaux attirent toutes ces personnes, souvent aveugles. Au bout du compte, on perd toutes ses plumes, ses économies, son prestige. Les forces de police, de gendarmerie comptent ainsi jouer un grand rôle pour mettre fin à cela. Mais comme l'a dit le Président Macky Sall, il faut mutualiser et partager les informations. Les gouvernements, les forces de sécurité essaient tant bien que mal, à mettre fin à cette forme de délinquance. Un phénomène de société.

Dans une société en mal de repères, on veut tout et tout de suite.

De l'argent, de belles filles, des Don Juan qui vous couvrent de millions, des voyages, mais en … rêve. Tout est fiction dans ce phénomène. En effet, les internautes ou les victimes mordent souvent trop vite à l'hameçon. Qui dans ce Sénégal n'aimerait pas recevoir des millions sans bouger ? Si cela existait, cela ne sortirait pas du cercle d'amis. Une utopie.

Aujourd'hui, nombre de compatriotes sont étranglés par les banques et les problèmes familiaux. Rien que pour l'obtention d'un crédit bancaire, l'on vous demande des « tonnes de paperasse », authentifiés. Ce sont donc des heures et des heures de connexion jamais gratuites. On surfe à longueur de journée. Et à tous les niveaux de notre haute administration. On se connecte pour des banalités, des futilités. Des conversations à vous donner des insomnies, des dettes.

Ils sont hommes d'affaires, étudiants, chômeurs, commerçants, dans toutes les catégories sociales. On « tchatte » et on oublie tout. On est en retard sur tout. Parce que la tête dans les nuages. Vous voyez souvent des personnes, rire, sourire pour un rien, c'est toujours la bonne humeur sur les visages. Jusqu'à ce que tout vous tombe sur la tête. On vous déplume en un temps record, comme devant ces faiseurs de miracles multiplicateurs de billets.

En effet, c'est la nouvelle version. Tout simplement. Comment se fait-il donc, que dans la clandestinité et dans l'illégalité, un inconnu vous détourne du système normal, sur un simple clic. Les victimes sont prises au piège après avoir été identifié. Sur le net, beaucoup de photos sont truquées. Des hommes se font passer pour des femmes, des femmes pour des hommes. Vous tombez toujours sur des personnages de rêve. Et dans votre subconscient, vous êtes prêts ou prêtes à tout. Pour oublier vos dettes, épouser cette perle rare, vous envoler sur une petite île, sans bruits ni tambours.

Loin de votre entourage, l'on vous propose toutes sortes de services jamais gratuits. Dès que l'argent commence à montrer son bout de nez, vous êtes pris comme une souris au piège. C'est d'abord les crédits téléphoniques, les virements, etc. Ce sont souvent des étrangers qui sont rois dans le phénomène. Mais de plus en plus, des Sénégalais y font légion.

Gagner de l'argent, épouser une belle fille, voyager, des dons… Ce qui est surprenant, c'est que beaucoup de victimes regrettent après avoir été dépouillé. Lors des mercredis de la police organisés cet été, le sujet sur la cybercriminalité avait été évoqué.

Devant les cadres, les hautes autorités de la police, la presse, entre autres, des panélistes avaient sonné l'alarme. Face à ce danger, des débats intéressants ont été organisé. Au Sénégal, il existe une entité qui s'occupe des données personnelles à « protéger » ? Et où il existe toujours selon les panélistes « un flou ». Dans un pays où il n'y a pas de textes juridiques spécifiques sur la cybercriminalité.

L'un des panélistes a évoqué un cas qui mérite attention. Celui d'une personne qui est tombée, par hasard sur un faux médecin. Ce dernier voulait à travers l'ordinateur, lui faire un check up. Imaginez un peu la suite. En lieu et place d'un toubib, ce fut un étranger qui après l'avoir photographié et non passé un « scanner », passe à l'acte deux. Le chantage. Mais la victime ne voulait pas que l'affaire s'ébruite. Déduire les frais et renvoyer la somme restante, une astuce payante

Autres faits importants.

Comment se fait-il que pour un « héritage », à recevoir, jamais dans un acte notarié, ou un « don » d'une personne anonyme, l'on puisse procéder à des virements d'argent… sans traces ? Les sociologues commencent à s'intéresser à l'affaire. Et souvent, leurs théories semblent incomprises de ces amateurs de sensations et de divertissements chèrement payés. Et le phénomène commence à devenir difficile à gérer. L'État du Sénégal a mis en place la brigade de lutte contre la cybercriminalité. Récemment, les gendarmeries africaines se sont rencontrées pour l'analyser. Surtout avec ces jeunes de plus en plus exposés. C'est pourquoi, le Président Macky Sall a demandé à toutes ces forces de défense : police, gendarmerie de mettre en place « des plateformes de partage ». Comme il l'a souligné lors cette rencontre, « les criminels ne connaissent pas les zones ». Souvent entre la gendarmerie et la police on parle « d'écoles ou de couleurs de tenue ».

Pour lui, ce qui importe « c'est le résultat ». Sinon, c'est « un éternel rattrapage ». En donnant comme exemple le ministère de l'Intérieur avec « Interpol ». Un phénomène selon lequel, il faut « une sensibilisation en direction de tous les citoyens.

Et pour ceux qui ont la responsabilité de gérer les systèmes informatiques ». Et le renforcement de la coopération internationale. La cybercriminalité n'a pas de frontières. Ou bien tout simplement être comme ce futé. Lorsqu'on lui a demandé une contrepartie, il a tout simplement demandé à son généreux donateur de lui envoyer l'argent, tout en y déduisant les soi-disant frais bancaires. Ce que le généreux « donateur » n'a pas voulu entendre.

Réagissez à cet article

Source : http://www.rewmi.com/cyberdelinquence-ou-cybercriminalite-le-terreau-de-largent-facile-et-de-creatures-de-reve.html

La face cachée du Web caché, le « dark Web »

	La face cachée du Web caché, le « dark Web »

Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaire.

«Sur Internet, on peut acheter une kalachnikov en deux clics.» Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge.

Depuis les attentats de janvier notamment, Internet (1) est au cœur des préoccupations. «Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles?», interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web… Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un navigateur personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une adresse IP, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

«Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre, explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet.»

Une fois sur TOR, pas de moteur de recherche. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches… C'est l'Internet «surfacique», une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur… C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden Wiki (le «wiki» caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 € ou un pistolet SIG Sauer de calibre 9 mm pour 790 €.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas… Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en bitcoins, une monnaie virtuelle et chiffrée, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire «confiance» à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un «facilitateur de la performance criminelle», selon Solange Ghernaouti: «Internet reflète notre réalité sociale, économique, politique et criminelle, poursuit-elle. Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation – on agit caché derrière un écran – à distance.»

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les «internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques», poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins.

———

LES MOTS POUR COMPRENDRE

Internet représente un réseau de télécommunication international reliant des ordinateurs à l'aide du protocole TCP/IP. Il sert de support à la transmission de données: pages Web, courriels, fichiers informatiques.

Une adresse IP (Internet Protocol) est un numéro d'identification attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Une adresse IP est un numéro unique permettant à un ordinateur de communiquer dans un réseau.

Un moteur de recherche est un site Internet régi par une application sur lequel, en entrant des mots-clés, on obtient une liste de sites correspondant à la demande. Exemple: Google.

Un réseau virtuel privé est un passage ou un lien qui permet d'ouvrir un réseau local vers l'extérieur et de le connecter à un autre réseau local, grâce à une connexion Internet et avec une sécurité optimisée.

Le wiki est une application Web participative dont les internautes peuvent modifier les contenus.

Le terme bitcoin (de l'anglais « bit », unité d'information binaire, et « coin », pièce de monnaie) désigne à la fois un système de paiement virtuel et l'unité de compte utilisée par ce système.

Le chiffrement est une technique d'écriture en langage crypté ou codé. C'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant de clés.

Réagissez à cet article

Source : http://www.la-croix.com/Ethique/Sciences-Ethique/Sciences/La-face-cachee-du-dark-Web-2015-12-08-1390141

Le créateur du bitcoin enfin démasqué ?

	Le créateur du bitcoin enfin démasqué ?

Une partie de la presse croit avoir mis la main sur le créateur du bitcoin. Connu sous le pseudonyme Satoshi Nakamoto, le père de la monnaie virtuelle, s'appellerait en réalité Craig Steven Wright.

L'identité du créateur du bitcoin passionne une partie de la presse américaine. Deux nouveaux sites affirment avoir découvert la personne qui se cache derrière la monnaie virtuelle. Il ne s'agirait pas d'un japonais mais d'un homme d'affaires australien, basé à Sydney.

On doit l'invention du bitcoin à un développeur connu sous le nom de Satoshi Nakamoto. Un pseudonyme qui lui a permis de demeurer loin de l'agitation et de toute caméra. Toutefois, sa véritable identité n'a jamais été exposée au grand jour. C'est pourquoi Gizmodo.com et Wired ont mené l'enquête afin de découvrir le nom du père du bitcoin.

Si les deux sites estiment savoir qui est le créateur de la monnaie, ils demeurent cependant prudents quant à leurs affirmations. Selon leurs informations, Craig Steven Wright aurait mis au point le bitcoin. Il aurait été épaulé d'un second collaborateur, en la personne de Dave Kleiman, un développeur américain dont le décès remonte à 2013.

La police australienne perquisitionne

Ces nouveaux éléments sont rapidement remontés aux oreilles des autorités australiennes. Suite à la publication de ces informations, la police du pays a procédé à la perquisition du domicile de Craig Steven Wright. Une célérité étonnante mais à laquelle la police a tenu à apporter un démenti. Cette visite impromptue ne serait pas due à ces révélations mais à une enquête liant l'homme d'affaires au fisc australien.

De leur côté, Gizmodo.com et Wired indiquent que leurs informations proviennent d'une série de courriers électroniques échangés entre Wright et son collaborateur mais également du cache de son blog personnel. Des publications, effacées depuis, font directement référence à la monnaie virtuelle.

Ainsi en janvier 2009, soit peu de temps après la sortie des premiers bitcoins, l'homme publiait un billet précisant que « la bêta de Bitcoin est en ligne aujourd'hui. C'est décentralisé… on essaye jusqu'à ce que ça marche ».

Plus tard, en 2011 Craig Wright évoquait le pseudonyme « Nakamoto » nommément dans un e-mail. « Je ne peux plus faire le Satoshi. Ils n'écoutent plus. Je suis mieux en tant que mythe. Retour à mes cours, mes gueulantes et au fait que tout le monde m'ignore. J'ai horreur de ça Dave, mon pseudonyme est plus populaire que je n'aurais jamais pu espérer », précisait-il.

Une chasse à l'homme et de grosses incertitudes

La recherche de Satoshi Nakamoto a déjà connu des ratés. En mars 2014, le magazine Newsweek avait cru tenir l'identité du père du bitcoin en la personne de Dorian Satoshi Nakamoto. Le japonais de 64 ans résidant aux Etats-Unis avait démenti être le créateur de la crypto-monnaie. L'homme était même allé plus loin en affirmant qu'il comptait attaquer le magazine américain devant les tribunaux suite à la publication de propos qu'il juge mensongers. L'ingénieur avait entrepris de lever des fonds pour soutenir sa cause. Pour éviter de telles nouvelles incertitudes, la presse américaine précise uniquement avoir obtenu des informations émanant d'une source anonyme.

Un hoax de haute volée ?

Face à la publication de ces nouvelles informations, les journalistes prennent des précautions nécessaires. Les documents mis en ligne par les auteurs de cette révélation ne peuvent, pour le moment, pas être clairement authentifiés et plusieurs incertitudes planent encore sur les implications réelles des deux individus dans la création de la monnaie virtuelle.

Les données présentées par Gizmodo.com et Wired doivent donc restées sujettes à caution. Une partie de la vérité pourrait être trouvée par les autorités britanniques. Craig Steven Wright aurait quitté l'Australie pour déménager à Londres. Si la police décide de poursuivre l'affaire, elle pourrait interroger l'homme d'affaires pour démêler une partie des informations.

Réagissez à cet article

Source :

http://pro.clubic.com/it-business/securite-et-donnees/monnaies-virtuelles/actualite-789108-bitcoin-vrai-createur-australie-nakamoto.html

L’agence météorologique australienne victime d’une cyber-attaque chinoise

L’agence météorologique australienne victime d’une cyber-attaque chinoise

L’équivalent australien de Météo France aurait été frappé par une cyber-attaque émanant de Chine. La faille serait très importante, impacterait jusqu’au ministère de la Défense australien, et coûterait plusieurs millions de dollars à réparer.

Le Bureau of Meteorology (BOM), l’agence nationale de météorologique australienne, a souffert d’une cyberattaque « massive »,rapporte la Australian Broadcasting Corporation le 2 décembre. D’une ampleur sans précédent en Australie, elle a été attribuée au gouvernement chinois par l’un des représentants gouvernementaux avec lequel la chaîne d’information s’est entretenue.

Le BOM héberge entre autres un centre de calcul à haute performance baptisé Solar, construit par Oracle sur la base d’une architecture Fujitsu. Outre le BOM, il est utilisé par de nombreuses agences gouvernementales australiennes, y compris le département de la Défense. D’après ce même représentant, sécuriser la faille de sécurité qui a permis cette attaque coûtera plusieurs millions de dollars.

Le gouvernement australien s’est refusé à confirmer l’information officiellement. La Chine de son côté nie toute responsabilité et juge les accusations sans fondement.

Réagissez à cet article

Source : http://www.usine-digitale.fr/article/l-agence-meteorologique-australienne-victime-d-une-cyber-attaque-chinoise.N368378

Donald Trump veut fermer Internet

	**Donald Trump veut fermer Internet**

Alors qu'il multiplie les prises de parole publiques, Donald Trump, candidat à la présidentielle des Etats-Unis pour 2016, a récemment tenu des propos assez radicaux vis-à-vis d'Internet.

Pour le milliardaire américain Donald Trump, tout est bon pour se faire remarquer. L'homme a l'ambition de remplacer Barack Obama à la tête des Etats-Unis et souhaite ainsi devenir le candidat du parti républicain. Si on n'abordera pas en détails les opinions conservatrices du milliardaire, ses propos sur Internet sont assez tranchés.

On a des enfants qui regardent Internet.(…) Et on se demande pourquoi on perd tous ces enfants qui partent la-bas (…) et qui veulent rejoindre l'Etat islamique (…) A cause d'Internet on a perdu beaucoup de gens.

On doit faire quelque chose. On doit aller voir Bill Gates et plusieurs autres personnes qui comprennent réellement ce qu'il se passe et leur demander de fermer Internet dans certains endroits. Les gens diront « liberté d'expression ! liberté d'expression ! ». Ces gens sont stupides. On a beaucoup de gens stupides. On doit faire quelque chose à propos d'Internet parce qu'ils recrutent des milliers de gens.

Donald Trump s'en est par ailleurs pris à Jeff Bezos, fondateur et PDG d'Amazon. Via trois messages publiés sur Twitter, l'homme estime que M. Bezos utilise le *Washington Post*, racheté en août 2013 et déficitaire, pour éviter de payer des taxes trop élevées. Face à ces agressions, Jeff Bezos a ironiquement répondu qu'il l'enverrait loin dans l'espace sur sa fusée Blue Origin.

Réagissez à cet article

Source : http://pro.clubic.com/technologie-et-politique/actualite-788798-donald-trump-gate.html##pid=22889469

Les tendances 2016 en cyber-sécurité

Les tendances 2016 en cyber-sécurité

Comme la plupart des professionnels de la sécurité informatique, je souhaite vraiment que mes prédictions ne se réalisent pas. Je préférerais que les entreprises ne soient ni piratées ni victimes de failles. Mais en prédisant la prochaine vague de menaces, nous espérons aider les entreprises à rester au fait de l'évolution des tactiques et des méthodes que les criminels vont utiliser pour les cibler. Voici dix menaces et tendances que nous devrions constater au cours de 2016 en matière de sécurité informatique.

Si une semaine peut sembler longue en politique, comme l'a observé l'ancien Premier ministre britannique Harold Wilson, une année dans le domaine de la cyber-sécurité peut ressembler à une éternité. Malgré les changements rapides, beaucoup de choses restent cependant constantes. Les trois principales menaces prévues par Check Point pour 2015 étaient la croissance rapide des logiciels malveillants inconnus, les menaces mobiles et les vulnérabilités critiques dans les plates-formes couramment utilisées (Android, iOS et autres). Ces prédictions se sont pleinement réalisées et ces menaces continueront certainement de poser nombreux problèmes. Le jeu du chat et de la souris qui a caractérisé la cyber-sécurité au cours des dernières années se poursuit. Les pirates tentent de trouver sans cesse de nouvelles manières d'attaquer les réseaux, comme le montrent les failles de cette année chez Anthem, Experian, Carphone Warehouse, Ashley Madison et TalkTalk.

Logiciels malveillants « sniper »
Les plus grandes failles de 2016 seront le résultat de logiciels malveillants conçus sur mesure pour franchir les défenses d'entreprises spécifiques, telles que lors des attaques menées contre TV5 Monde. Les attaques génériques à champ large continueront de menacer les utilisateurs individuels et les petites entreprises, et les pirates amélioreront leurs méthodes d'attaque contre les grandes entreprises qui disposent de postures de sécurité plus sophistiquées. Ils utiliseront des méthodes de phishing plus approfondies et plus sophistiquées, et d'autres astuces d'ingénierie sociale pour accéder aux systèmes et aux données qu'ils souhaitent.

Les terminaux mobiles en 1ère ligne des attaques
Le nombre d'attaques mobiles continue d'augmenter à mesure que les appareils mobiles prennent place dans l'entreprise et offrent aux pirates un accès direct et potentiellement lucratif aux données personnelles et professionnelles. D'après une étude que nous avons menée en 2015, 42% des entreprises ont subi des incidents de sécurité mobile leur coûtant plus de 200 000 €, et 82% s'attendent à une augmentation du nombre d'incidents. Cette année a également été le témoin de l'émergence de plusieurs vulnérabilités mobiles critiques, notamment Certifigate impactant des centaines de millions d'appareils Android, et XcodeGhost – première infection malveillante à grande échelle ciblant des appareils Apple iOS non jailbreakés. Nous nous attendons à d'importantes vulnérabilités mobiles similaires l'année prochaine.

La bataille contre les menaces les plus dangereuses
Dans la bataille continue entre les pirates et les professionnels de la sécurité, les agresseurs déploient des variantes personnalisées de logiciels malveillants existants et d'attaques encore inconnues (« zero-day ») de plus en plus sophistiquées, capables de contourner la technologie de sécurité traditionnelle. Ces nouveaux vecteurs d'attaque exigent des solutions plus proactives et plus avancées pour stopper ces logiciels malveillants. Des innovations comme le sandboxing au niveau du CPU, capable d'identifier les menaces les plus dangereuses avant qu'elles ne parviennent à échapper à la détection des outils traditionnels et infecter les réseaux, seront plus que jamais nécessaires en 2016 pour faire face à ces nouvelles menaces.

Les infrastructures critiques plus que jamais en ligne de mire
En décembre 2014, une aciérie en Allemagne a été frappée par des pirates qui ont réussi à accéder au réseau de production de l'usine et causer des dommages « massifs ». Le département américain de la sécurité intérieure a découvert que le Trojan « Havex » était parvenu à compromettre les systèmes de contrôle industriel de plus de 1 000 entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Les cyber-attaques menées contre des services publics et des processus industriels clés se poursuivront, à l'aide de logiciels malveillants ciblant les systèmes SCADA qui contrôlent ces processus. Comme ces systèmes de contrôle sont de plus en plus connectés et offrent une surface d'attaque plus étendue, une meilleure protection sera nécessaire pour les défendre. Ces risques sur les infrastructures critiques sont particulièrement sensibles dans un contexte de menaces terroristes accrues.

Les objets connectés : futur terrain de jeu des hackers ?
L'Internet des objets en est encore à ses balbutiements, et il est peu probable qu'il ait un fort impact en 2016. Néanmoins, les entreprises doivent réfléchir à la manière dont elles peuvent protéger les appareils intelligents et se préparer à une plus vaste adoption de l'IoT. Les utilisateurs doivent se demander « où leurs données sont transmises » et « ce qui se passerait si quelqu'un mettait la main sur ces données ». L'année dernière, nous avons découvert une faille dans des routeurs équipant des TPE dans le monde entier, qui pourrait permettre à des pirates de les détourner pour lancer des attaques sur tous les appareils qui leur sont connectés. Nous nous attendons à plus de vulnérabilités similaires dans les appareils connectés.

Les wearables c'est beau … mais pas très sécurisé !
Les wearables tels que les montres intelligentes font leur entrée dans l'entreprise, présentant de nouveaux risques et défis pour la sécurité. Les données stockées dans les montres intelligentes et les autres appareils personnels intelligents sont vulnérables et pourraient même être utilisées par des pirates pour capturer de l'audio et de la vidéo via des Trojans d'accès à distance. Les entreprises qui autorisent l'utilisation de ces appareils doivent assurer leur protection via des mots de passe et des technologies de chiffrement renforcées.
Trains, avions et véhicules connectés… autant de portes d'entrée pour les hackers !

2015 est l'année de l'émergence du piratage de véhicules : leurs logiciels embarqués sont détournés afin de prendre le contrôle des véhicules. En juillet, Fiat Chrysler a rappelé 1,4 millions de véhicules Jeep Cherokee aux États-Unis après que des chercheurs aient découvert qu'ils pouvaient être piratés via le système de divertissement connecté. Avec plus de gadgets et de systèmes connectés que jamais dans les véhicules modernes, nous devons protéger ces systèmes. Il en va de même pour les systèmes complexes des avions de ligne, des trains et autres formes de transport public.

Véritable sécurité pour les environnements virtuels
La virtualisation a été rapidement adoptée par les entreprises au cours des dernières années, que ce soit via SDN, NFV ou le Cloud. Les environnements virtualisés sont complexes et créent de nouvelles couches réseau. C'est seulement maintenant que nous comprenons réellement comment protéger ces environnements. Lorsque les entreprises migrent vers des environnements virtualisés, la sécurité doit être conçue dès le départ pour offrir une protection efficace.

Nouveaux environnements, nouvelles menaces
2015 était également l'année du lancement de plusieurs nouveaux systèmes d'exploitation, tels que Windows 10 et iOS 9. La majeure partie des attaques menées contre les entreprises ces dernières années ciblaient Windows 7, en raison de la faible adoption de Windows 8. Mais avec Windows 10 et son offre de téléchargement gratuit, les cybercriminels vont donc tenter d'exploiter ce nouveau système d'exploitation. Ses mises à jour sont plus fréquentes et les utilisateurs maîtrisent moins son environnement.

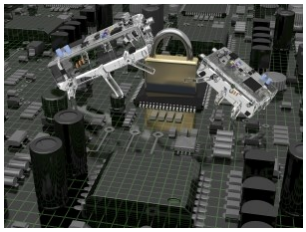
La consolidation de la sécurité pour la simplifier !
Pour se protéger contre les menaces multiformes, les professionnels de la sécurité sont susceptibles de se tourner vers des solutions d'administration centralisée de la sécurité. Les grandes entreprises qui possèdent pléthore de différents produits de sécurité sur leur réseau verront la consolidation comme un moyen de réduire à la fois coût et complexité. La multitude de solutions et de produits individuels devient rapidement ingérable et peut effectivement entraver la sécurité plutôt que l'améliorer. La consolidation de la sécurité fournit un moyen efficace de réduire la complexité afin que les nouvelles menaces ne s'égarent pas entre les mailles des différents systèmes.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-cyber-securite-en-2016-Check,20151204,58072.html

---

20% of cyber-attacks attributed to Conficker worm

Detected in everything from police body cameras to the business internet of things (IoT) landscape, now do you give a configuration fick?



The notorious Conficker worm has been gaining an ever-wider reputation for destruction. Last month SCMagazineUK.com reported on this comparatively old malware's presence as it started to appear pre-installed inside police body cameras.

Not content with infecting the security forces' use of Internet of Things devices, Conficker has continued to turn its venom towards the business landscape in general. October of this year saw Conficker ranked by security vendor Check Point as the most common malware used to attack British and international organisations.
Check Point suggests that as many as 20 percent of all attacks globally can be attributed to Conficker in the period identified.
Also known as by the name Downadup, Conficker was first identified as far back as 2008. It targets the Windows operating system and can form a botnet to infect a computer and spread itself to other machines across a network automatically, without human interaction.

Undead, still walking

As noted on The Register, networks belonging to the French Navy, the British House of Commons and Greater Manchester Police were all laid low by the malware. "Its recent resurgence hasn't caused anything like the same amounts of problems but still highlights the generally poor state of corporate security," wrote John Leyden.

How does the Conficker worm spread?

Microsoft's own advisory states that the Conficker worm spreads by copying itself to the Windows system folder. The firm notes, "It might also spread through file sharing and through removable drives, such as USB drives (also known as thumb drives), especially those with weak passwords."

What marks Conficker's resurgence now, in the dying days of 2015, is not only its brute-force attack ability on passwords but also its longer term ability to still cause impact. As botnets and remote control PC attacks now still grow, the prevalence of ransomware and data-stealing malware also continues to rank highly among the reported threats as measured by the security industry.

Common tools democratise hacking

Fraser Kyne, principal systems engineer at Bromium contacted SC to say that the use of common tools in this way democratises hacking, as it provides a framework for mounting similar attacks across a range of vectors.
"Re-purposing the tools of the past is a simple model for attackers, and one that is difficult to detect. We see some vendors claiming to be able to look for telltale signs of these models – but realistically they're playing a losing game where the attacker is always several steps ahead," said Kyne.
As a related note, Bromium Labs has recently blogged on the resurgence of malware that uses macros in Office documents, particularly Dridex. In this sense, malware is analogous to malaria. As vaccines become available, the disease morphs.
"The only practical (and sustainable) model for defending against malware is isolation. This needs to be done outside of the operating system. Modern hardware has the capability to do this securely, efficiently and invisibly for the user – and we're seeing proof of the success of this approach. In this model, the mosquito bites a crash test dummy, not the real user, and there's no impact to the business," he said.

Actually, you're failing miserably

Richard Cassidy, technical director EMEA, Alert Logic told SC that the proliferation of Conficker highlights organisations' continuing failure across the board to get it right when it comes to key security practices and policy enforcement.
"With the plethora of incredible security technologies today, from network access control to micro-visor security containers at the host process level, through to big data analytics platforms, all poised to detect advanced malware variants of C2C, botnet and remote control infection, it is a wonder therefore that organisations (including governments) are not only being successfully infected with malware, but also for inordinate periods of time before detection," said Cassidy.
He surmises that ultimately we have to assume that we will be infected, even if we manage to get all the required parts aligned.
"With this mindset, therefore, we will drive better protection of key data assets from being easily compromised and will work to ensure we are better poised to detect compromise activity, should a particular user not have adhered to a 'no-download' policy from untrusted sources," he said.
This article originally appeared on SC Magazine UK.

Réagissez à cet article
Source : http://www.scmagazine.com/20-of-cyber-attacks-attributed-to-conficker-worm/article/458392/