LETTRE D'INFORMATION : BON A SAVOIR (N°19)

Le Sniffing : Une forme d'attaque sur le réseau couramment utilisée par les pirates

Le Sniffing ou reniflement de trafics constitue l'une des méthodes couramment utilisée par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers ont généralement recours à ce procédé pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles. Les pirates informatiques utilisent des sniffers réseau ou renifleurs de réseau pour pouvoir surveiller le réseau et soustraire frauduleusement les différents types de données confidentielles susceptibles de les intéresser.

Mécanisme de fonctionnement d'un sniffer de réseau :

Un Sniffer est généralement utilisé pour intercepter les paquets qui circulent sur un réseau. Il offre, à cet effet, la possibilité pour un hacker d'examiner le contenu d'un certain nombre de paquets qui ne lui ont pas été initialement destinés. En tant que renifleur, cet outil peut donc intercepter tout type d'informations émises à travers le réseau et par conséquent afficher à la fois l'identité des utilisateurs au même titre que leurs mots de passe, surtout lorsque ces informations sont transférées par des
protocoles qui ne sont pas suffisamment sécurisés comme : le FTP (File Transfert Protocol), la DNS (Domain Name System) ou encore le HTTP (Protocole de transfert hypertexte). Lorsque les donnés ne sont donc pas cryptées et qu'elles doivent passer à travers une interface réseau de l'ordinateur par l'intermédiaire duquel s'exécute le renifleur réseau ou sniffer, les informations sont immédiatement interceptées par cette machine sans la moindre difficulté.

Afin de vous prémunir contre les risques de Sniffing, vous pouvez consulter l'agence Anti Cybercriminalité pour vous conseiller sur les différentes mesures à prendre en vue d'éviter les pièges tendus par les renifleurs.

Lien : http://www.anti-cybercriminalite.fr/article/le-sniffing-une-forme-dattaque-sur-le-r%C3%A9seau-couramment-utilis%C3%A9e-par-les-pirates

Prévention contre le sniffing réseau

Je me suis connecté dernièrement au réseau sans fil de la bibliothèque, et le soir même tous mes comptes avec lesquels je me suis connecté ont été piratés**,** pourtant je n'ai pas donné mon mot de passe à qui que ce soit et personne n'était à côté de moi ! … C'est une histoire qui n'est pas si rare qu'elle en a l'air, il s'agit d'une attaque par sniffing réseau aussi appelée reniflage réseau en français.

Reniflage réseau ?

Le reniflage réseau consiste à écouter les communications réseau afin de récupérer et d'analyser le contenu transmis. Ce contenu peut-être constitué d'informations très sensibles lorsqu'aucun chiffrement n'est utilisé. Parmi ces informations sensibles, on peut trouver le contenu d'une conversation par mail**,** les cookies ou encore les fameux mots de passe**.**

Comment se protéger contre le sniffing réseau ?

Vous comprenez maintenant déjà mieux pourquoi on dit souvent qu'il ne faut pas se connecter dans les cybercafés et autres réseaux publics.

Non seulement vous ne savez pas toujours quels programmes sont lancés sur l'ordinateur que vous utilisez, mais en plus vous pouvez être victime de reniflage réseau.

En fait, la meilleure protection contre ce type d'attaque est d'utiliser un protocole de communication sécurisé comme HTTPS.

Que faire si le site n'est pas en HTTPS ?

Me demanderiez-vous, et c'est une excellente question !

Eh bien vous pouvez également utiliser un service VPN qui chiffrera le trafic même pour les sites qui ne sont pas en HTTPS**.**

De quoi surfer sur les réseaux publics en paix.

Lien : http://www.leblogduhacker.fr/prevention-contre-sniffing-reseau/

Cybercriminalité : qu'est-ce que le "cuckoo smurfing" ?

Comment la « criminalité en col noir »* blanchit l'argent de la drogue

Le Code monétaire et financier français impose aux banques de communiquer à un organisme spécialisé dépendant du ministère des Finances, le Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) les opérations qui pourraient être en lien avec un certain nombre d'infractions listées. Cette obligation de diligence est édictée pour les opérations portant sur des sommes dont le montant unitaire ou total dépasse 150 000 euros (art. L 563-3). Ce montant est abaissé à 8 000 euros pour un client occasionnel.

Une des techniques utilisées par les blanchisseurs d'argent sale pour contourner cet obstacle consiste à fractionner les dépôts effectués auprès des banques afin de se maintenir constamment en deçà des seuils qui pourraient déclencher un contrôle de la part du banquier et une possible «déclaration de soupçon».

Vol au-dessus d'un nid de coucou

Ce fractionnement est appelé « *smurfing* » ou «schtroumphage», en référence aux Schtroumpfs, ces petits lutins bleus qui vivent cachés dans la forêt, personnages de bande-dessinée imaginés par le dessinateur Peyo connus dans le monde entier.

Le «saucissonnage» des dépôts peut être perfectionné par la multiplication de comptes au guichet d'une même banque ou dans différentes banques. Pour y parvenir, les «blanchisseurs» contactent *via* le net – on parle de cybercriminalité – les clients des banques

- soit en leur adressant des messages sur leur boîte e-mail leur demandant de se connecter au moyen d'un lien hypertexte à un site ressemblant à s'y méprendre à celui de la banque, ou de tout autre organisme financier, et de confirmer ses coordonnées bancaires, qu'ils pourront utiliser par la suite,
- soit en leur proposant des gains rapides et faciles en travaillant sur Internet sans bouger de chez eux.

Cette technique de «*fishing*» ou «hameçonnage» a été comparée au comportement du coucou qui dépose ses oeufs dans les nids des autres oiseaux, qui se chargeront de les couver.

Une vraie menace pour les démocraties

Le «*cuckoo smurfing*» désigne donc la technique de blanchiment d'argent sale qui consiste à disséminer les gains illicites sur différents comptes afin de se maintenir toujours en dessous des seuils qui pourraient déclencher les mesures de diligences exigées d'un banquier. Le cumul des opérations pourra dégager un total supérieur aux seuils fixés par le législateur, mais les blanchisseurs agissent de façon à ce que le professionnel ne puisse pas faire le rapprochement entre les différentes opérations.

Les liens entre délinquance économique et financière classique et les différentes formes de criminalité organisée, jusqu'au terrorisme, ne sont plus à démontrer. L'objectif des organisations criminelles est d'exercer, par la violence, la corruption et la fraude, des positions d'influence qui menacent à plus ou moins long terme les pouvoirs détenus jusque là par les États de droit.

* Le Conseil de l'Europe dans un rapport sur la criminalité organisée de 2005 fait une distinction au sein de la criminalité économique entre la criminalité en «col blanc» qui est le fait d'homme d'affaires, par ailleurs légitimes, tentés de prendre des raccourcis pour s'enrichir, et la criminalité en «col noir» qui est le fait de criminels opérant sur des marchés illicites.

Lien : https://scribium.com/anne-de-morel/a/cybercriminalite-quest-ce-que-le-cuckoo-smurfing/

Les hackers privilégient le «drive-by download»

CybercriminalitéLes criminels sont constamment à la recherche de possibilités d'infecter les appareils, selon un rapport paru jeudi.

MELANI a observé une augmentation des attaques contre des sites Web au deuxième semestre 2015. Les criminels sont constamment à la recherche de possibilités d'infecter commodément un maximum d'appareils de victimes potentielles.

Dans son rapport semestriel, la Centrale d«enregistrement et d'analyse pour la sûreté de l«information (MELANI) constate que si les hackers privilégiaient par le passé l'envoi de courriels, qui demande peu de connaissances techniques, c'est désormais le «drive-by download» qui a la cote: il consiste à propager des logiciels malveillants (maliciels) à grande échelle, à travers des sites web très fréquentés.

Les portails des journaux et les réseaux publicitaires sont les cibles préférées des escrocs, explique MELANI. Une infection chez un fournisseur de contenu publicitaire peut se révéler lourde de conséquences, en infectant plus loin de nombreux sites clients.

Familles de maliciels

Au deuxième semestre de l'année dernière, l'extorsion est restée une des méthodes favorites des cybercriminels afin d'obtenir des gains rapides. Les familles de maliciels de cryptages sont toujours plus nombreuses, avertit MELANI. Les attaques DDoS (déni de service distribué), qui visent à rendre des sites inaccessibles pour ensuite exiger une rançon, se sont multipliées en 2015.

Les criminels choisissent avant tout des entreprises qui dépendent de l'accès à leur site Internet, car elles sont plus faciles à faire chanter. Sous la menace d'une éventuelle perturbation de l'accès à leur site, certaines sont prêtes à mettre la main au porte-monnaie. «Mais en payant, elles donnent aux hackers les moyens financiers pour renforcer leur infrastructure d'attaque et intensifier leurs actions», souligne la centrale.

En 2015, MELANI a ouvert le site «antiphishing.ch», qui permet à chacun de signaler des sites de hameçonnage. Quelque 2500 sites ont été dénoncés la première année. A côté du phishing par usage abusif du logo de l'administration fédérale, constaté plusieurs fois, le

recours au phishing à l'aide de fichiers PDF est en recrudescence: au lieu d'un lien HTML, le courriel contient un fichier .pdf en annexe, qui lui-même incite à cliquer sur un lien malveillant.

Zurich et Valais

Comme au premier semestre 2015, Zurich et le Valais affichent au deuxième semestre un taux d«infection par habitant supérieur aux autres cantons. «Alors qu'à Zurich ce résultat tient à la forte densité d«ordinateurs, les raisons du taux d'infection élevé en Valais ne sont pas connues à l'heure actuelle», écrit MELANI dans son rapport.

http://www.24heures.ch/high-tech/hackers-privilegient-driveby-download/story/22106206

[Chiffrement] Après Apple, Whatsapp dans la ligne de mire ?

L'application de messagerie sécurisée Whatsapp serait la prochaine cible des autorités dans la guerre qu'elle mène contre la course au chiffrement des géants du web, révèle le ***New York Times***.

Il n'est pas question d'iPhone, d'Apple ou de terrorisme ici, néanmoins le problème reste le même : le chiffrement.

Dans le cadre d'une enquête en cours, un juge fédéral américain a donné son feu vert aux autorités pour procéder aux écoutes des communications passées depuis l'application de messagerie sécurisée Whatsapp. Problème, avec le chiffrement de bout en bout des communications proposées par la société depuis 2014 cela se révèle compliqué et l'enquête stagne.

Le Département de la Justice (DOJ) étudierait donc actuellement des solutions de contournement et des pourparlers seraient engagés entre Whatsapp et le DOJ, rapporte le *New York Times*.

Toutefois, alors que le contexte est déjà tendu et voit Apple et le FBI se livrer une guerre de tranchées autour de la sécurité des données et des communications, des sources proches du dossier assurent que le problème est autrement plus préoccupant dans cette affaire.

Pour le *NYT*, cela ouvrirait « *un nouveau front dans la contestation entre l'administration Obama et la Silicon Valley autour du chiffrement, de la sécurité et de la vie privée* ». Avec le chiffrement, l'avenir des écoutes électroniques serait en jeu. Écoutes que les agences de renseignement estiment être à la base de toute enquête criminelle.

La question étant désormais de savoir si le Département de la Justice doit forcer Whatsapp à aider le gouvernement afin qu'il obtienne ces informations, au risque de voir s'aggraver le conflit. De leur côté, les sénateurs seraient sur le point de légiférer concernant les sanctions civiles à imposer aux entreprises high-tech, qui refuseraient de répondre aux ordonnances du tribunal requérant leur coopération pour aider les autorités à accéder aux données chiffrées de leurs utilisateurs.

Un conflit juridique avec Whatsapp pourrait également inciter les législateurs à réviser la loi sur les écoutes (*wiretapping*) dont la dernière mise à jour remonte à une génération.

Pour l'Electronic Frontier Foundation (EFF), le FBI et le ministère de la Justice attendent juste le moment et le cas opportuns pour effectuer une demande qui apparaîtrait enfin raisonnable.

Whatsapp n'est pas la seule application chiffrée existante – Telegram serait d'ailleurs privilégiée par les djihadistes de l'organisation Etat islamique (OEI) pour communiquer – mais avec 1 milliard d'utilisateurs, elle est, de loin, la plus importante.

Le chiffrement n'est pas qu'une sécurité pour les clients des géants du web, c'est aussi un moyen pour le gouvernement de se protéger des cyberattaques dont il est régulièrement

victime. C'est pourquoi la Maison Blanche avait opéré un revirement sur le chiffrement en expliquant qu'il ne fallait en aucun cas l'affaiblir. Puis avait à nouveau changé d'avis peu après « *l'acte terroriste* » du 2 décembre perpétré à San Bernardino en Californie et revendiqué par l'organisation État islamique.

Au sein même de l'administration Obama, les avis divergent sur la manière d'inciter les entreprises high-tech à coopérer et/ou répondre aux requêtes des forces de l'ordre. La Maison Blanche a refusé de légiférer en ce sens en imposant des *backdoors* aux firmes technologiques et fait depuis des pieds et des mains pour s'attacher la coopération active des géants du web… qui semblent freiner des quatre fers, pris en étau entre la sécurité des données de leurs clients et les impératifs de sécurité nationale qui semblent légitime dans le contexte actuel. Google, Facebook, Snapchat et Whatsapp s'apprêteraient même à accélérer sur le chiffrement en optant pour le *end-to-end* sur l'ensemble de leurs services.

Un juste équilibre est-il possible ? Une solution qui allierait un chiffrement fort, et la possibilité laissée aux autorités d'accéder aux données souhaitées. Le président Obama la appelé de ses voeux et ce, avant que le législateur ne vienne imposer une loi qu'il juge « *dangereuse* ».

La vie privée est une notion très importante chez Jan Koum, le fondateur de Whatsapp, ce dernier ayant grandi sous l'ère soviétique en Ukraine. Il fut l'un des premiers à manifester son soutien à Tim Cook lorsque le CEO d'Apple a publié sa lettre ouverte expliquant les raisons de son opposition au FBI.

« *Notre autonomie et notre liberté sont en jeu* », avait-il alors déclaré sur sa page Facebook.

15 mars 2016

Liens : http://www.journaldugeek.com/2016/03/15/chiffrement-whatsapp-ligne-mire/

Quand Facebook et WhatsApp servent à vendre drogues et animaux rare

Plusieurs organisations de défense de la nature sauvage ont déclaré hier que des trafiquants d'animaux publiaient activement leurs offres sur Facebook.

Ce cas est loin d'être isolé: depuis plusieurs années le Brésil lutte contre les trafiquants de drogue sur WhatsApp… Mais pourquoi les criminels optent pour ces applications populaires? Et comment les autorités locales combattent ce phénomène? dauphin © Flickr/ Ed Dunens Des pertes importantes de dauphins en Argentine L'organisation Traffic, créée par le Fonds mondial pour la nature (WWF) et l'Union internationale pour la conservation de la nature (UICN), a percé à jour un réseau de trafiquants d'animaux sur Facebook. D'après son dernier rapport en date, les criminels agiraient via des groupes fermés enregistrés en Malaisie occidentale. En se faisant passer pour des acheteurs, les protecteurs des animaux ont rejoint 14 de ces groupes et, en cinq mois, ont relevé plus de 300 annonces de vente d'animaux rares ou en voie d'extinction — des gibbons, des ours malaisiens, des pandas, des tortues et des oiseaux étaient activement achetés en tant qu'animaux domestiques ou pour être revendus. Au total, plus de 100 vendeurs ont été identifiés. un loris © Wikipedia/ Lionel Mauritson un loris Selon Traffic, ces groupes illégaux ont pu voir le jour en Malaisie car dans ce pays, les administrateurs de Facebook ne suivent pas rigoureusement les infractions au règlement du réseau social. En cinq mois d'observation, aucun des groupes n'a été fermé alors qu'ils comptaient presque 68 000 membres. SeaWorld © Flickr/ Josh Hallett SeaWorld reconnaît que ses employés ont infiltré des associations écologistes C'est seulement quand Traffic a fourni les résultats de son investigation à la direction du réseau social pour l'Asie du Sud-Est que l'accès à ces groupes a été immédiatement restreint, et que le personnel de Facebook a promis d'aider les activistes à mettre la main sur les criminels. Tous les documents ont été transmis aux autorités locales qui ont déjà annoncé l'interpellation de plusieurs dizaines de

trafiquants. Néanmoins, les défenseurs des animaux craignent que les ventes d'animaux par le biais des réseaux sociaux soient d'une ampleur bien plus grande. Cependant, toutes ces interdictions ne concernent pas le service de messagerie WhatsApp appartenant à Facebook. Fin 2014, cette application s'est même dotée d'une fonction de cryptage: le message est codé au moment de l'envoi et il ne peut être décrypté que par le destinataire. Une telle approche de la protection des données a suscité l'inquiétude du FBI, dont le directeur a appelé en août 2015 à fournir aux services de renseignement une clé de décryptage — la réponse fut négative. Logo de Facebook © Sputnik. Natalya Seliverstova Le vice-président de Facebook arrêté au Brésil Les autorités brésiliennes sont encore plus révoltées par la politique de WhatsApp, utilisé aujourd'hui par plus de 70 millions d'habitants du pays pour contourner le coût élevé des appels et des SMS. WhatsApp est aussi massivement utilisé pour vendre des armes et des drogues — le Brésil compte officiellement plus d'un million de narcodépendants, dont beaucoup consomment des drogues dures comme le crack et la cocaïne. La police est pratiquement impuissante car WhatsApp refuse de lui fournir l'accès aux correspondances. Cela force le gouvernement brésilien à employer des méthodes peu traditionnelles pour faire pression sur WhatsApp: fin décembre, après un nouveau refus de fournir à la police des informations sur une affaire criminelle, la messagerie a été entièrement bloquée dans le pays pendant 48 heures. Toutefois, cette décision de justice a été levée le lendemain et plus de 1,5 million de Brésiliens ont commencé à utiliser le service protégé Telegram. https://fr.sputniknews.com/presse/201603041023121288-vents-drogues-animaux-rares-facebook-whatsapp/

Blanchiment d'argent sur eBay avec de faux scooters

Eric Vernier est docteur en sciences de gestion et maître de conférences. Il a écrit « Techniques de blanchiment et moyens de lutte », paru aux éditions Dunod. Entretien.

Quels types de trafics trouve-t-on sur les sites de vente d'occasion ?

Il y a quatre grands axes : l'escroquerie, la contrefaçon, le recel et le blanchiment d'argent. Il y a quelques années, le recel se pratiquait « au cul du camion », maintenant c'est « au cul » de ces sites. On y retrouve indifféremment de la petite escroquerie, des bandes organisées comme des organisations criminelles.

Comment se déroule le blanchiment d'argent ?

Le blanchiment peut se faire grâce à la vente de produits inexistants entre complices. Je me souviens de cette histoire de scooters de collection, vendus à des prix largement supérieurs au cours du marché.

C'est l'un de vos collègues, lui même collectionneur, qui m'avait alerté. Il s'étonnait du prix affiché dans certaines annonces diffusées sur eBay, supérieur de 30% à 50% à la cote officielle.

En y regardant de plus près, l'astuce, c'était de les vendre le plus cher possible, afin d'obtenir la trace de transactions et justifier des transferts d'argent. Vendeurs et acheteurs appartiennent en fait à la même organisation.

Les vérifications vont être difficiles à effectuer. Je me suis rendu compte de la manipulation lorsque j'ai téléphoné aux numéros affichés dans ces annonces. Soit ce numéro était erroné, soit le scooter en question était vendu. Ce devait être un réseau assez important, pour que ce soit aussi visible.

Mais le blanchiment peut s'effectuer grâce à l'achat de produits existants, payés avec de l'argent sale.

Dans les deux cas, ces ventes justifient des rentrées d'argent officielles en cas de contrôle par la police ou le fisc. Ce blanchiment est pratiqué par des amateurs, mais aussi par des organisations « professionnelles », en d'autres proportions.

Que peuvent faire les autorités face à ces trafics ?

On est dans le domaine du virtuel, donc le contrôle est difficile. Il y a une atomisation des échanges. Dans une boutique mondiale sur la Toile, la police comme la justice ne peuvent pas faire grand chose.

De temps en temps, ils arrêtent un réseau, mais c'est vraiment pour l'exemple. Les autorités forcent les sites à mettre en place des procédures de contrôle. Ces derniers s'exécutent, mais les outils qu'ils créent sont peu efficaces. Au final, tout le monde est content, et le blanchiment continue...

Je ne vois a priori aucune possibilité de contrôle sur ce type de délits. Comment voulez-vous évaluer la contrefaçon, puisque la photo de l'annonce est généralement authentique ?

http://rue89.nouvelobs.com/rue89-eco/2012/03/05/comment-blanchir-largent-ebay-faux-scooters-228777