Top 5 des arnaques du moment en Côte d’Ivoire | Le Net Expert Informatique

	**Top 5 des arnaques du moment en Côte d’Ivoire**

A mi-parcours de son activité 2015, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) dans un souci de prévention, vous présente à travers cet article, les arnaques auxquels vous pourriez être confronté, parce que prisées par les cyberdélinquants. Voici le top 5 des arnaques du semestre écoulé, en nombre de dossiers traités, sur les 491 dossiers reçu par la PLCC, et leurs préjudices enregistrés, sur les 1 milliard 199 millions 319 milles 880 Fcfa de dommage subit par les victimes des 6 premiers mois de l'année 2015.

1- L'ACCÈS FRAUDULEUX À UN SYSTÈME D'INFORMATION

Cette arnaque concerne les détournements de transfert d'argent. C'est une escroquerie qui consiste pour le cyberdélinquant à faire à votre insu le retrait d'une somme d'argent qui vous est destinée via une institution de transfert d'argent. Elle occupe la première place de notre classement, avec 91 dossiers traités par la PLCC, pour un préjudice estimé à 68 millions 903 milles 772 F CFA. Ce sont les populations ivoiriennes qui sont surtout touchées par cette infraction »nouvelle ».

2- FRAUDE SUR LE PORTEFEUILLE ÉLECTRONIQUE

Elle s'est développée avec l'avènement des services Mobile Money proposés par les compagnies de téléphonie mobile dans nos pays africains. Les cyberdélinquants s'attaquent au portefeuille électronique des utilisateurs en vidant leur compte.
Avec 86 dossiers et un préjudice estimé à 37 millions 906 milles 300 F CFA, cette arnaque occupe la seconde marche du podium. Toujours avec les populations ivoiriennes qui prennent la place de victime numéro un des cyberdélinquants depuis un certain temps (voir article CYBERCRIMINALITÉ EN CÔTE D'IVOIRE: LESIVOIRIENS, PLUS TOUCHÉS PAR LES ARNAQUES).

3- L'ARNAQUE AUX FAUX SENTIMENTS

Considérée comme la »mère » des arnaques sur internet, l'arnaque aux faux sentiments, bien qu'elle soit la plus connue, continue de faire des victimes. C'est une escroquerie qui consiste pour le cyberdélinquant a utiliser les sentiments amoureux de leur proie pour leur soutirer de l'argent.
Si en nombre de dossier la baisse est significative par rapport aux semestres des années antérieurs (59 dossiers reçus), elle continue d'affoler les compteurs en terme de préjudice avec 448 millions 431 milles 586 F CFA seulement pour le premier semestre 2015 soit 37,39 % du préjudice totale, toute catégorie confondue, du premier semestre 2015, estimé à 1 milliard 199 millions 319 milles 880 Fcfa.

4- LE CHANTAGE À LA VIDÉO

Classé 4ième, le chantage à la vidéo peut être vue comme une résultante de l'arnaque aux faux sentiments. Le cyberdélinquant menace de divulguer des photos ou vidéo à caractère sexuelle de vous, prise dans l'intimité d'une relation.
Avec 54 dossiers, pour un préjudice de 66 millions 832 milles 324 F CFA, cette arnaque touche de plus en plus les Ivoiriens.

5- L'ARNAQUE AUX FAUX HÉRITAGES

La dernière place de ce top 5 revient à l'arnaque aux faux l'héritage. L'une des plus vielles ruses utilisée par les cyberdélinquants. Et pourtant, elle continue de faire des victimes. C'est une escroquerie ou tentative d'escroquerie, à la fois très ancienne et très commune encore aujourd'hui. Les escrocs vous envoient un mail vousinformant que vous avez été choisi pour toucher un fabuleux héritage providentiel.
Ce sont 37 dossiers qui ont été introduit à la PLCC, pour un préjudice qui s'élève à 407 millions 920 milles 762 F CFA.
Le nombre d'affaires et le montant des préjudices liés à ces infractions indiquent que le travail de sensibilisation contre la cybercriminalité doit se poursuivre. Car bien que la majorité de ces arnaques soit connue et expliquée à travers la toile, elles sont encore nombreuses ces personnes qui se laissent duper par les cyberdélinquants. Une fois de plus la PLCC vous invite à la prudence !!!

lu sur http://cybercrime.interieur.gouv.ci/

Source :
http://www.imatin.net/article/societe/broutages-cybercriminalite-en-cote-d-rsquo-ivoire-voici-le-top-5-des-arnaques-du-moment_30029_1440509278.html

---

Être immédiatement informé

lorsqu’on s’est fait voler ses données, c’est maintenant possible | Le Net Expert Informatique

	Être immédiatement informé lorsqu’on s’est fait voler ses données, c’est maintenant possible

Comme il est impossible de bâtir une protection à 100% efficace, une start-up de Baltimore propose de marquer les données pour les déceler immédiatement lorsqu'elles sont dérobées.

Cela paraît tellement évident que l'on se demande pourquoi personne n'y avait pensé avant. En effet, lorsqu'un vol de données se produit dans une entreprise, il se passe parfois des semaines voire des mois avant que le vol ne soit découvert. Et le plus fréquemment, c'est lorsque les données sont mises en vente sur les réseaux de l'Internet Underground, accessibles via des plates-formes comme Tor, que le cyber cambriolage est découvert.

Identifier en quelques secondes

Une start-up baptisée Terbium Labs vient de dévoiler un produit baptisé MatchLight avec lequel elle prétend être capable de tracer les données en quelques secondes, y compris sur ces réseaux underground accessibles via Tor.

Danny Rogers et Michael Moore, les deux fondateurs, affirment qu'ils auraient pu découvrir la faille sur les services du Trésor américain que nous avons relaté voici quelques jours.

Le constat des deux fondateurs est que la défense parfaite n'existe pas et qu'il existera toujours des trous. « Si vous ne pouvez pas tout stopper, que pouvez-vous faire d'autre ? c'est comme cela que nous nous sommes concentrés sur la détection immédiate des menaces », affirmait Danny Rogers à nos confrères de ZDNET.

Les empreintes Matchlight stockées dans le cloud

Le principe de fonctionnement de la solution MatchLight est le suivant. Lorsqu'un client héberge une base de données sensibles comme des numéros de cartes de crédit ou des mots de passe, l'appliance MatchLight génère des empreintes digitales pour ces données. Ces empreintes digitales sont envoyées vers le cloud MatchLight sans que les données sensibles auxquelles elles sont attachées y aillent. En combinaison avec un crawler web capable d'indexer également les sites de l'underground, l'entreprise peut être immédiatement informée lorsque l'une de ces empreintes digitales est trouvée dans la nature. Et ceci se produit de manière presque instantanée, indépendamment du type d'attaque qui a conduit au vol des données.

Terbium Labs a démarré en 2013 et a rapidement obtenu le soutien de grandes entreprises dont évidemment elle ne donne pas les noms, dans un programme bêta au long cours. Durant les tests de cette phase bêta, les deux fondateurs ont indiqué avoir identifié plus de 30000 cartes de crédit à vendre et 6000 adresses email en une seule journée, preuve selon eux, de l'efficacité de leur solution.

Source : http://www.mag-securs.com
/news/articletype/
articleview/articleid/34630/categoryid/58/
marquer-les-donnees-pour-constater-immediatement-les-vols.aspx

Boeing planche sur des drones capables de déployer des logiciels espions | Le Net Expert Informatique

Boeing planche sur des drones capables de déployer des logiciels espions

Le spécialiste de l'aéronautique Boeing travaille sur la production de drones capables d'infecter les ordinateurs et smartphones aux alentours.

En début de mois, nous apprenions que la société milanaise Hacking Team, qui propose des outils d'interception des communications entre internautes aux gouvernements ou aux pouvoirs publics, avait elle-même été hackée. Quelque 400 gigaoctets de données confidentielles ont été récupérés révélant la nature des relations entre Hacking Team et ses partenaires. Ces documents sont mis à disposition sur le site Wikileaks.
Parmi les informations révélées, la filiale Insitu de Boeing, spécialisée dans la production de drones, avait signé un partenariat avec Hacking Team afin de procéder à des hacks à distance. L'appareil serait ainsi en mesure de cibler un smartphone ou un ordinateur portable en particulier puis de l'infiltrer via un réseau Wi-Fi.
Selon le magazine The Intercept, qui rapporte l'information, le drone en question est prévu pour pouvoir accéder aux fichiers à distance, récupérer le journal des appels, l'historique des messageries instantanées ou encore les emails.
Au sein des emails aspirés sur les serveurs de Hacking team, nous trouvons notamment une feuille de route datant du mois de juin. Celle-ci fait mention d'un petit appareil pouvant être transporté par un drone et capable de récupérer les données transitant via les réseaux.
Le document explique que l'attaque devra prendre en charge Windows 10 ainsi que le navigateur Microsoft Edge et Skype Web. Sur OS X, Hacking Team a finalisé un dispositif scannant les sauvegardes locales d'iTunes et planchait sur la capture des certificats d'iCloud et des images de l'application Photos.
Retrouvez tous les détails de ce projet en italien sur cette page.

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

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spyware-logiciel-espion/actualite-774222-boeing-planche-drones-capables-deployer-spyware.html

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net Expert Informatique

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team

Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance | Le Net Expert Informatique

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance

De nouvelles informations émergent des centaines de milliers d'e-mails piratés au fabricant de logiciels espions Hacking Team. Des échanges ont montré que l'entreprise italienne a été contactée par Insitu, un fabricant de drones appartenant à Boeing, pour travailler sur un système qui permettrait aux engins de pirater des réseaux Wi-Fi à distance, a relevé le site The Intercept.

Un rapport daté du 1er juillet montre d'ailleurs qu'Hacking Team travaillait sur un système d'injection réseau utilisable par drone, c'est-à-dire « un équipement conçu pour insérer du code malicieux dans les communications d'un réseau Wi-Fi », explique le site spécialisé Ars Technica.

« Nous ne pouvons vendre nos produits qu'à des entités gouvernementales »

Selon un premier e-mail envoyé en avril, Insitu s'est montré intéressé par une présentation de Hacking Team à l'IDEX 2015, un salon de la défense qui s'est tenu aux Emirats arabes unis en février. « Nous aimerions potentiellement intégrer votre système de piratage de Wi-Fi à un système aérien et nous souhaiterions prendre contact avec un de vos ingénieurs qui pourrait nous expliquer, plus en détail, les capacités de l'outil, notamment la taille, le poids et les spécifications de votre système Galileo [un logiciel espion] », écrit alors Giuseppe Venneri, ingénieur mécanique en formation chez Insitu.

« Gardez à l'esprit que nous ne pouvons vendre nos produits qu'à des entités gouvernementales », répond un responsable de Hacking Team, sans fermer la porte à une collaboration. Selon un e-mail interne, le même responsable de Hacking Team indique qu'Insitu travaille avec des agences gouvernementales et demande quels produits seraient les plus adaptés à la demande du fabricant.

Aucun accord trouvé

La correspondance entre Insitu et Hacking Team s'est arrêtée en mai et a été fortement retardée par des discussions d'ordre légal, chaque entreprise souhaitant utiliser son propre accord de non-divulgation avant de démarrer les discussions commerciales. Les courriels les plus récents suggèrent que les négociations n'ont jamais commencé.

Le vendeur de logiciels espions italien Hacking Team est sous pression depuis un piratage qui a conduit à la publication de plus de 400 gigabits de données confidentielles début juillet. Certains documents indiquent notamment que l'entreprise pourrait avoir vendu des solutions de surveillance à des pays sous embargo comme le Soudan et la Russie.

Source : http://www.lemonde.fr/pixels/article/2015/07/20/hacking-team-a-travaille-sur-un-drone-capable-d-infecter-des-ordinateurs-a-distance_4691260_4408996.html
Par Florian Reynaud

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians | Le Net Expert Informatique

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians

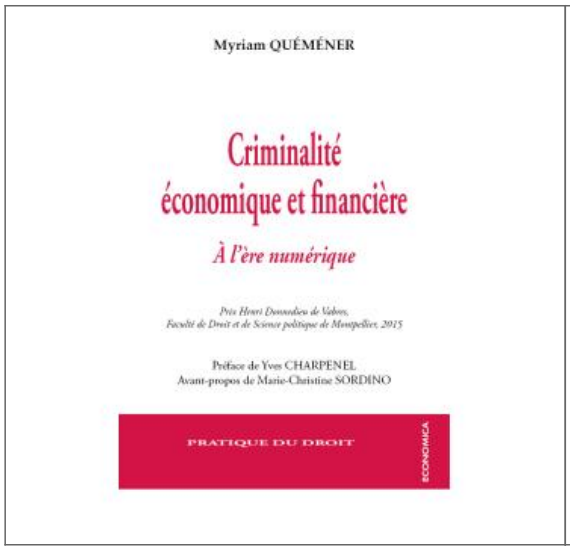
6 ressortissants nigérians ont été interpellés par les éléments de la Brigade de recherches du Commissariat de police de Golf Sud (Guédiawaye). Le matériel qui a été découvert chez eux a permis de conclure que ces derniers s'activaient dans la cybercriminalité, selon le journal Grand Place.

La police de Guédiawaye (Sénégal) vient de démanteler un vaste réseau de cybercriminalité entretenu par des ressortissants nigérians. C'est suite à une information anonyme relative aux agissements répréhensibles de ces derniers que l'agent de police en chef de la commune de Golf Sud a mis sur pied un plan de neutralisation. Ainsi, ses hommes en civil se sont rendus sur les lieux dans la nuit du vendredis 10 juillet, aux environs de 23h, et ont pu arrêter 6 ressortissants nigérians.
Une perquisition de l'immeuble où ils ont été trouvés a permis de mettre la main sur 6 ordinateurs portables de marques différentes. L'exploitation des différents logiciels et autres systèmes des machines a permis la découverte d'installations et de fichiers de comptes bancaires de tiers ainsi que de faux documents étatiques et de réfugiés politiques.
Il y avait aussi plusieurs systèmes sur les ordinateurs portables avec des noms de code permettant à leurs propriétaires d'exercer, en toute discrétion, une activité criminelle.
– L'un permet d'effacer toutes les données après chaque redémarrage de l'outil informatique,
– alors que le deuxième est un système de navigation qui consiste à utiliser Internet sans pour autant être tracé ou repéré par les opérateurs de téléphonie.
– Et le troisième logiciel installé sur la machine ouvre la possibilité aux présumés cybercriminels de pirater les comptes bancaires d'autrui sans laisser des traces.

Source : http://www.leral.net/Cybercriminalite-a-Guediawaye-La-police-demantele-un-reseau-de-ressortissants-nigerians_a149877.html

---

La criminalité économique et financière à l'ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l'ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

Cyclisme et vol de données – la cyber-criminalité appliquée au sport | Le Net Expert Informatique

	Cyclisme et vol de données – la cyber-criminalité appliquée au sport

Le Tour de France 2015 va-t-il connaître son premier cyber scandale ? C'est en tout cas ce que l'on peut supposer après la divulgation de certaines données de performances du cycliste Crhis Froome qui ont été dérobées, estime Tanguy de Coatpont, directeur général France & Afrique du nord de Kaspersky Lab qui partage son analyse.

« Depuis plusieurs années, le sport connaît un engouement croissant auprès des publicitaires et des entreprises qui y investissent massivement, attirant par conséquent des cybercriminels poussés par l'appât du gain ou une volonté de nuire. Il n'est également pas difficile d'imaginer les conséquences psychologiques que peut avoir un vol de données sur un athlète dont le succès repose en partie sur sa concentration.
Les rumeurs concernant le possible piratage des données sportives de Chris Froome viennent nous rappeler que de nombreux aspects de la vie moderne, y compris le sport de haut niveau, sont de plus en plus connectés. Il y a quelques années, l'idée que les données d'un coureur du Tour de France soient dérobées aurait semblée anecdotique mais avec l'avancée des technologies et l'émergence des solutions d'analyse des performances qui sont aujourd'hui critiques à l'entraînement de nombreux sportifs, ce n'est plus surprenant. Ces sportifs doivent également faire face à une autre réalité : alors qu'ils sont maintenant élevés au rang de célébrités, les informations concernant leurs performances intéressent tout autant que celles qui concernent leur vie privée.
En sachant cela, tout individu ou entreprise doit prendre les mesures qui s'imposent pour protéger ses données informatiques. Même lors d'événements sportifs, où les données doivent être transmises et analysées quasiment en temps réel, il est impératif de prendre en compte les questions de sécurité informatique pour protéger les informations sensibles que sont les performances des athlètes mais également protéger les systèmes sur lesquels elles transitent.
Le partenariat entre Kaspersky Lab et l'écurie de Formule 1 de Ferrari nous a permis de mieux comprendre les défis auxquels ils sont confrontés pour sécuriser les données transmises lors des courses. Pour Ferrari, une solution de sécurité efficace est vitale afin de protéger les données qui sont une source d'information essentielle à l'équipe. Elles transitent très rapidement pour éviter d'être compromises et la solution de sécurité ne doit pas augmenter le temps de latence. Il n'est pas difficile d'imaginer que les contraintes de complexité et de performance sont similaires dans d'autres sports comme le cyclisme professionnel. »

Source : http://www.itrmanager.com/articles/157190/cyclisme-vol-donnees-cyber-criminalite-appliquee-sport.html

Les dessous de la société d’espionnage Hacking Team… | Le Net Expert Informatique

Les dessous de la société d’espionnage Hacking Team…

La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

Ennemie d'Internet
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

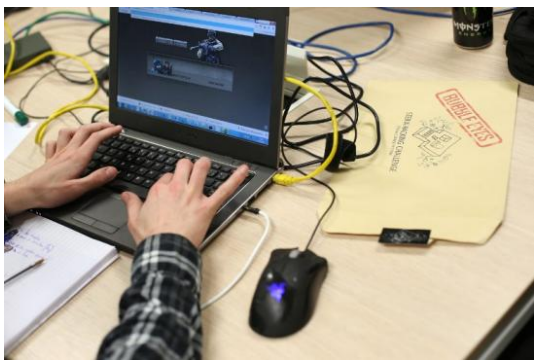
Des régimes autoritaires en clients
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« oficially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

La France, elle aussi intéressée par les services de l'entreprise
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

« Nous n'avons rien à cacher »
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN

Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique



Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

Source : http://www.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso