Google monte une équipe de supers hackers pour traquer les failles informatiques

Une équipe de supers hackers pour traquer les failles informatiques

Google veut éradiquer les bugs qui peuvent être exploités par les pirates, mais aussi le gouvernement.

On croirait lire le scénario d'un film d'espionnage. Google a annoncé la création d'une équipe spéciale chargée de traquer les failles informatiques. Dénommée Project Zero, cette nouvelle équipe de sécurité sera composée des meilleurs hackers. Parmi eux, George Hortz, un Américain de 24 ans, surtout connu pour avoir piraté l'écran verrouillé de l'iPhone à l'âge de 17 ans et la Playstation 3, raconte le magazine spécialisé Wired. Quand il a découvert, au début de l'année, des failles dans le système d'exploitation de Google, Chrome OS, l'entreprise l'a payé 150.000 dollars pour les corriger. Outre Hortz, Project Zero accueille d'autres hackers célèbres, et Chris Evans , le recruteur du projet, continue de chercher des talents.

Project Zero sera chargée de trouver les failles dîtes «zero-day», c'est à dire des vulnérabilités qui n'ont pour l'instant jamais été découvertes et peuvent être dangereuses si elles sont exploitées par des pirates. L'équipe travaillera sur n'importe quel produit, et donc pas uniquement sur ceux de Google. «Nous ne posons pas de limite particulière à ce projet et travaillerons à l'amélioration de la sécurité de n'importe quel programme informatique utilisé par de nombreuses personnes. Nous porteront une grande attention aux techniques, aux cibles et aux motivations des attaquants», explique Chris Evans dans son communiqué.

Une réponse de Google à Heartbleed

Ce projet de Google arrive après Heartbleed, la faille de sécurité qui a secoué Internet il y a quelques mois. Fin avril déjà, l'entreprise s'associait à Facebook, Microsoft et d'autres pour lancer la Core Infrastructure Initiative. Un regroupement qui finance les projets Open Source en difficulté financière, et donc ceux qui seraient le plus exposés à une faille de sécurité passée inaperçue. Project Zero c'est aussi la réponse de Google à la NSA. La firme a mal encaissé les failles utilisées par l'agence américaine pour espionner ses utilisateurs. Google a déjà mis en place de nouveaux mécanismes de sécurité pour mieux protéger ses données.

Le mythe des hackers embauchés par les entreprises dont ils révèlent les failles n'est pas nouveau. En 2011, Apple embauchait Nicholas Allegra. À 19 ans, il était un membre éminent de la communauté du jailbreaking, c'est à dire du débridage d'iOS (le système d'exploitation des iPads et iPhones). Un an plus tard, la firme embauchait Kristin Paget dans son équipe de sécurité. Cette informaticienne avait longtemps fait partie d'un groupe de hackers éminents qui avait révélé des failles chez Microsoft.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.lefigaro.fr/secteur/high-tech/2014/07/16/01007-20140716ARTFIG00221-google-monte-une-equipe-de-supers-hackers-pour-traquer-les-failles-informatiques.php

---

1,2 milliard d'identifiants volés par des pirates russes

– Vol d’identifiants au dessus d’un nid de coucou

1,2 milliard d’identifiants volés par des pirates russes – Vol d’identifiants au dessus d’un nid de coucou

Le vol d’identifiants est passé à l’échelle supérieure avec la découverte que des cybercriminels russes avaient détourné 1,2 milliard de noms et mots de passe. A ce niveau, cela touche tout le monde, estime la firme de sécurité Hold Security qui a découvert ce groupe de pirates qu’il désigne sous le nom de CyberVor.
En Russie, des criminels ont constitué une énorme base constituée de 1,2 milliard de noms d’utilisateurs et de mots de passe volés, auxquels s’ajoutent 500 millions d’adresses e-mail, selon Hold Security, une société américaine spécialisée sur la sécurité Internet. Il s’agit probablement de la plus grosse base d’identifiants dérobés, récupérés d’attaques conduites dans tous les coins du web et qui ont touché environ 420 000 sites. « Jusqu’à présent, nous étions stupéfaits lorsque 10 000 mots de passe avaient été compromis, maintenant nous en sommes au stade du vol massif », a confié Alex Holden, fondateur de Hold Security, à nos confrères d’IDG News Service. Sa société n’a pas communiqué le nom des sites qui avaient été attaqués, invoquant des accords de confidentialité avec ses clients, mais elle a indiqué que cela incluait des familles et de petits sites web.

Le New York Times, qui fut le premier à rapporter ce vol, s’est adressé à un expert en sécurité indépendant pour vérifier que les données volées étaient authentiques. L’ampleur de la base constituée semble éclipser les précédentes découvertes de données compromises. Par comparaison, le vol subi par Target (révélé en janvier dernier) a affecté 40 millions de cartes de débit et 70 millions d’informations personnelles. C’est, en matière de détournement d’identifiants, l’un des faits de cybercriminalité les plus importants constatés jusqu’à présent et qui porte ce type de délit à un niveau supérieur. « Ces gens n’ont rien fait de nouveau ni d’innovant », constate Alex Holden. « Ils l’ont juste fait mieux et à un niveau de masse ce qui touche absolument tout le monde ».

Le gang CyberVor est constitué d’une douzaine de jeunes gens
Le groupe derrière l’attaque semble être basé dans le centre-sud de la Russie, a indiqué Alex Holden au New York Times. Selon les informations qu’il a communiquées au quotidien américain, il s’agit d’une douzaine de personnes d’une vingtaine d’années qui ne semblent pas avoir de liens avec le gouvernement. Avec des serveurs basés en Russie, le groupe a étendu ses activités cette année, probablement après avoir été en contact avec une organisation plus importante. Hold Security a dénommé le gang CyberVor d’après le mot russe « vor » (voleur). La société a indiqué qu’elle fournirait un service pour permettre aux utilisateurs de vérifier si leurs identifiants figurent parmi ceux qui ont été volés. L’information sera disponible dans deux mois environ. Le pré-enregistrement pour y accéder est possible dès maintenant.
Ce détournement massif de noms d’utilisateurs et de mots de passe met une fois de plus en lumière le peu de sécurité apportée par ces méthodes d’authentification, en particulier si les personnes se servent des mêmes noms et passwords pour plusieurs sites. Le recours à une méthode d’authentification à deux niveaux (avec envoi d’un code par SMS) renforce la sécurité mais ne constitue pas une garantie comme un utilisateur de PayPal vient tout juste de le démontrer. Après avoir, sans succès, alerté PayPal sur cette faille, il a expliqué comment cette fonction pouvait, en l’occurrence, être détournée via une connexion eBay.
Article de Martyn Williams / IDG News Service (adapté par Maryse Gros)

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemondeinformatique.fr/actualites/lire-des-pirates-russes-ont-amasse-1-2-milliard-d-identifiants-58272.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Les objets connectés ont de véritables problèmes en matière de sécurité

Les objets connectés ont de véritables problèmes en matière de sécurité

Connexions Bluetooth bavardes, chiffrement de piètre qualité, politiques de protection des données personnelles inexistantes… Les accessoires connectés ont tendance à vous mettre à nu.

Votre dernière course en forêt, vos déplacements à l'étranger, vos phases de sommeil, votre consommation en nicotine ou alcool, vos cycles de menstruations (si vous êtes une femme), votre pression artérielle, votre activité sexuelle… Pour toute activité personnelle, il y a désormais une application mobile et un accessoire connecté pour capter ces informations, comme par exemple le Nike Fuel Band. Et les utilisateurs en raffolent, si l'on croit les analystes. Selon Pew Research Center, plus de 60 % des Américains utilisent ces outils pour améliorer leur performances sportives ou préserver leur bonne santé. D'ici à 2018, le nombre de ces accessoires connectés devrait dépasser les 485 millions d'unités. Un marché en plein boom que tous les grands acteurs cherchent à accaparer, à commencer par Google et Apple.

Mais ce marché est encore très balbutiant, et notamment en matière de protection de données personnelles. Symantec vient de publier, il y a quelques jours, un rapport d'analyse qui évalue le niveau de sécurité de tous ces engins. Résultat: la plupart des applications révèlent des failles flagrantes permettant à des tiers de récupérer des données à l'insu des utilisateurs. Une majorité des bracelets peuvent être localisés grâces à leurs puces Bluetooth. Activés en permanence, ils sont plutôt bavards et émettent une adresse physique de type MAC, ainsi que des identifiants divers et variés, qu'il est aisé de capter dans un rayon de 100 mètres.
C'est d'ailleurs ce que les analystes de Symantec ont fait: ils ont créé des sniffeurs Bluetooth basés sur une carte Raspberry Pi, qu'ils ont disséminés aux abords d'une compétition sportive, ou trimballés dans un sac à dos en plein milieu d'un centre commercial. Certes, ces données ne permettent pas d'identifier une personne, mais c'est un premier pas…

Des mots de passe transmis en clair
Autre problème: parmi les applications qui utilisent des services cloud pour stocker ou traiter les données captées, 20 % transmettent les identifiants en clair, sans aucun chiffrement. Parmi les 80 % restantes, certaines appliquent aux identifiants des fonctions de hachage de faible protection comme MD5, qui peut facilement être craqué par les cybercriminels.
Dans un certain nombre de cas, la gestion de sessions laisse également à désirer, permettant par exemple de deviner ou de calculer des identifiants et ainsi d'accéder à des comptes utilisateurs.
Enfin, plus de la moitié des applications (52 %) n'apportent aucune information sur la manière dont toutes ces données sont traitées et stockées, alors que c'est obligatoire dans bon nombre de pays. Et quand il existe un document d'information, celui-ci est souvent très vague. On peut donc douter du sérieux de ces fournisseurs en matière de protection des données personnelles.
En somme: si toutes ces nouveaux appareils et applications semblent bien pratiques, il est conseillé de regarder en détail leur fonctionnement, histoire de pas se faire avoir !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

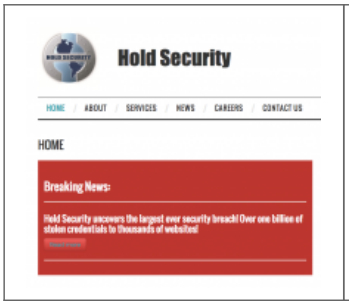
Références :
http://www.01net.com/editorial/624818/les-objets-connectes-sont-des-passoires-en-matiere-de-securite/#?xtor=EPR-1-NL-01net-Actus-20140806

Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en France ?

Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en France ?
Google a fait arrêter un Américain qui échangeait des photos pédopornographiques. Une pratique dont la légalité reste à prouver.

Il a alerté les autorités après avoir découvert des photos pédopornographiques dans les e-mails d'un habitant de Houston (Texas, Etats-Unis), rapporte la chaîne locale KHOU. Ce Texan, déjà coupable d'agression sexuelle sur un garçon de 8 ans en 1994, a été inculpé pour possession de pornographie infantile et promotion de pédopornographie.

Un milliards de mots de passe volés par un gang de pirates…



Un milliards de mots de passe volés par un gang de pirates…

Un petit groupe de cybercriminels a employé un botnet pour infiltrer des dizaines des milliers de sites web et récupérer une quantité gigantesque de données sensibles. Mais la firme qui a fait cette découverte en profite pour faire un formidable coup de com' et vendre un service derrière. Bizarre.La page d'accueil alarmiste de Hold Security, entreprise qui a révélé le piratage… Et qui propose une solution payante pour tenter d'y remédier.
Que vous soyez un expert en informatique ou un technophobe, à partir du moment où vous avez des données quelque part sur le web, vous pouvez être affecté par cette brèche. On ne vous a pas nécessairement volé directement. Vos données ont peut être été subtilisées à des services ou des fournisseurs auxquels vous avez confié des informations personnelles, à votre employeur, même à vos amis ou votre famille ». Voilà le discours flippant de Hold Security pour décrire la gigantesque collection de données personnelles volées que cette entreprise de sécurité a mis au jour.
Les chiffres présentés donnent en effet le tournis : d'après Hold Security, un gang d'une douzaine de hackers russes baptisé CyberVor aurait donc récupéré pas moins de 4,5 milliards de combinaisons de mots de passe et de noms d'utilisateurs. En omettant les doublons, CyberVor aurait accès à plus d'un milliard de comptes sur des milliers de sites différents, qui seraient rattachés à 500 millions d'adresses e-mail. Le hack du siècle, en somme.
Pour voler autant d'informations sensibles, CyberVor aurait usé de multiples sources et techniques, mais aurait surtout profité des services d'un botnet (un réseau de PC infectés par un logiciel malveillant) « qui a profité des ordinateurs des victimes pour identifier des vulnérabilités SQL sur les sites qu'ils visitaient. » Les membres de CyberVor auraient de cette manière identifié plus de 400 000 sites web vulnérables, qu'ils ont ensuite attaqué pour voler leur bases de données d'utilisateurs.

Des détails qui clochent
Sauf qu'il y a quelques petits détails qui clochent dans cette histoire. A commencer par le fait que Hold Security profite de cette annonce hallucinante pour tenter de s'enrichir immédiatement, en misant sur la peur du hacker qu'il a généré. En gros, la firme propose aux entreprises et aux particuliers de se préinscrire à un service –payant même s'il y a un essai gratuit- qui leur permettra notamment de savoir si oui ou non ils sont concernés par cette fuite de données. Et ce n'est pas donné : comptez 120 dollars par mois si vous êtes une entreprise.
D'autre part, Hold Security se refuse à donner le moindre nom de site dont la base a été piratée. Ce peut être compréhensible : son patron Alex Holden l'explique dans le New York Times, il ne souhaite pas révéler le nom des victimes pour des raisons de confidentialité. Il y aurait pourtant des entreprises du Fortune 500 selon lui dans le lot.
Mais comme le fait remarquer Forbes, il semble pour le moins étonnant (mais pas totalement impossible) que de si grandes entreprises se soient fait berner par une injection SQL, une technique très connue des hackers… et des experts en sécurité qui protègent les sites importants de telles attaques.

Des infos de piètre qualité ?
Il y a aussi de nombreuses informations qui manquent, dans la description de Hold Security. Quels botnets ont été utilisés ? Comment le malware a-t-il été inoculé dans la machine des victimes ? Et surtout pourquoi, comme l'indique le New York Times, le gang se contente-t-il d'utiliser pour l'instant leur fabuleuse base de données pour… envoyer du spam sur les réseaux sociaux, alors qu'ils pourraient à priori faire bien plus de mal ?
En réalité, il se peut que les milliards de mots de passe collectés par CyberVor étaient déjà disponibles sur le web underground depuis bien longtemps. Hold Security l'avoue sur son site : « Au départ, le gang a acquis des bases de données d'identifiants sur le marché noir ». Une pratique fort courante chez les cybercriminels, mais qui ne repose pas sur le moindre hack : il suffit de payer. Il est fort possible que ces « collectionneurs » aient au fil du temps accumulé un nombre de données incroyable, mais pas forcément « fraîches » et donc de piètre qualité. Il se peut aussi que la technique de l'audit d'un site par un botnet ait été fructueuse… Sur des sites de moindre envergure, voire des sites perso, mal sécurisés, qui n'ont pas fourni à Cybervor de quoi faire autre chose que du spam sur Twitter.
Quoiqu'il en soit, l'annonce de Hold Security vous donne une excellente excuse pour changer dès aujourd'hui vos mots de passe, ça ne fait jamais de mal !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/624854/comment-un-gang-de-pirates-a-t-il-pu-voler-plus-d-un-milliard-de-mots-de-passe/#?xtor=EPR-1-NL-01net-Actus-20140806

Objets connectés : HP s'inquiète des failles de sécurité

Le danger pourrait aussi bien venir des Objets connectés

Au total, 10 objets ont été passés au crible par les services de Fortify, la division d'HP dédiée à la cybersecurité.

Lesquels ? On ne sait pas exactement, l'entreprise se contente

de préciser qu'ils sont de tous types (webcam, domotique, hub etc…) et font partie des objets les plus vendus. Mais dans un souci diplomatique, le rapport semble préférer la discrétion, afin peut être de laisser le temps aux constructeurs de corriger ces vulnérabilités.

Le problème n'est pas anodin puisque comme le relève l'étude, 9 de ces 10 objets stockent ou utilisent des données personnelles de l'utilisateur. Parmi ceux la, 7 d'entre eux ne chiffrent pas les données qu'ils transfèrent vers le réseau, et 6 objets proposent des interfaces web vulnérables à des attaques de cross-site scripting ainsi qu'à d'autres types d'attaques plus simples basées sur le social engineering. Un exemple criant : 8 objets sur 10 ne posent aucune restriction sur le choix du mot de passe, permettant ainsi à l'utilisateur de choisir un mot de passe du type « 123456 »

L'internet des objets : un gruyère ?

En moyenne, les objets étudiés par Fortify présentaient chacun 25 failles de sécurité, allant des plus obscures à d'autres beaucoup plus connues telles que des vulnérabilités ayant trait à Heartbleed. La générosité gratuite n'étant pas vraiment de ce monde, cette initiative n'est pas innocente de la part d'HP qui en profite pour faire la promotion de son activité de sécurité Fortify et redirige tout au long du rapport le lecteur vers son site Owasp, un site open source dédié à la sécurité des objets connectés.

Peu de chiffres, pas de noms, HP ne se mouille donc pas trop mais on peut rappeler que l'objet du rapport n'en reste pas moins pertinent : la sécurité des objets connectés est un enjeu de taille que les constructeurs ne peuvent se permettre de traiter à la légère.

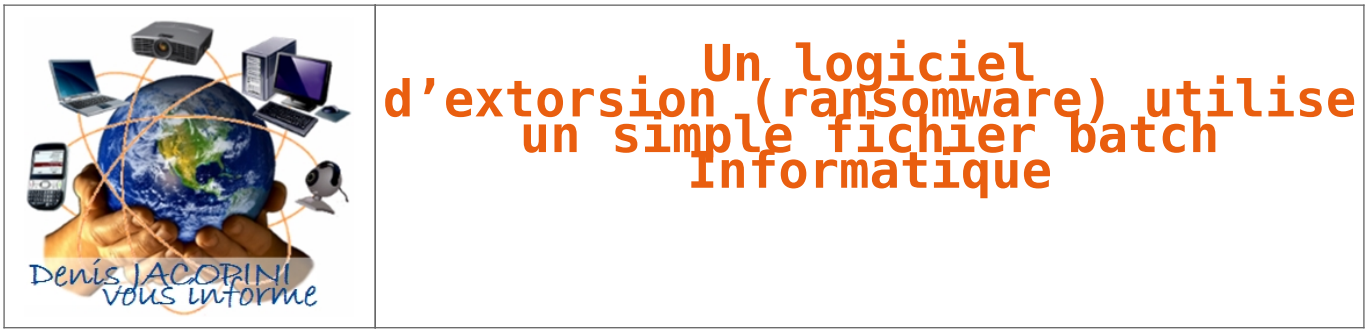
Cet article vous à plu ? Laissez-nous un commentaire (Source

de progrès)

Références :
http://www.zdnet.fr/actualites/objets-connectes-hp-s-inquiete-des-failles-de-securite-39804463.htm

---

Un logiciel d’extorsion (ransomware) utilise un simple fichier batch



Des chercheurs de Symantec ont récemment identifié une menace d’extorsion qui fonctionne avec un script et une ligne de commande en utilisant le programme de chiffrement Open Source GnuPG.

Pour extorquer de l’argent aux utilisateurs, des pirates ont mis au point un nouveau programme capable de chiffrer les fichiers sur l’ordinateur cible. Ce nouveau type de malware indique que les attaquants n’ont plus besoin de compétences pointues en programmation pour créer de dangereux programmes d’extorsion (ransomware) très efficaces, surtout quand les

technologies de chiffrement avancé sont accessibles gratuitement. Des chercheurs du fournisseur d'antivirus Symantec sont récemment tombés sur un logiciel malveillant de ce type, d'origine russe, dont le composant principal se limite à un simple fichier batch, c'est à dire un script avec une ligne de commande. Cette stratégie de développement permet à l'attaquant de contrôler et de mettre facilement à jour le malware, explique dans un billet le chercheur Kazumasa Itabashi.

Le fichier batch télécharge une clef publique RSA en 1024 bits depuis un serveur et l'importe dans GnuPG, un programme de chiffrement gratuit qui fonctionne également par ligne de commande. GnuPG est une implémentation Open Source de la norme de chiffrement OpenPGP. Il est utilisé pour chiffrer les fichiers de la victime avec la clé téléchargée. « Si l'utilisateur veut déchiffrer les fichiers concernés, ils a besoin de récupérer la clé privée de l'auteur du malware », indique le chercheur.

Une rançon de 150 € pour déchiffrer ses propres données

Dans le chiffrement à clé publique sur lequel est basé OpenPGP, les utilisateurs génèrent une paire de clés associées, l'une rendue publique et l'autre qui reste privée. Le contenu chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. La nouvelle menace représentée par le ransomware que Symantec appelle Trojan.Ransomcrypt.L chiffre les fichiers avec les extensions suivantes: .xls, .xlsx, .doc, .docx, .pdf, .jpg, .cd, .jpeg, .1cd, .rar, .mdb et .zip. Les victimes sont invitées à payer une rançon de 150 € pour récupérer la clef privée.

Ce qui distingue le Trojan.Ransomcrypt.L des autres malwares ne tient pas à l'usage du chiffrement à clé publique – d'autres menaces adoptent la même technique – mais à sa simplicité et au fait que l'auteur a choisi d'utiliser un programme de chiffrement légal et Open Source, au lieu de

créer sa propre mise en oeuvre, ce que font souvent les auteurs de malwares.

Les chercheurs prévoient une augmentation des menaces
Il existe certains programmes d'extorsion complexes avec des fonctionnalités avancées, développés essentiellement pour être vendus à d'autres cybercriminels qui n'ont pas les compétences nécessaires. Mais Trojan.Ransomcrypt.L montre qu'il est devenu possible de développer ce type de logiciels malveillants à peu de frais et sans connaissance de programmation avancée. Si bien que les chercheurs de Symantec s'attendent à une augmentation du nombre de menaces de ce type dans l'avenir.

Article de Jean Elyan avec IDG News Service

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemondeinformatique.fr/actualites/lire-un-logiciel-d-extorsion-utilise-un-simple-fichier-batch-58248.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Les Objets connectés et leurs

failles de sécurité ont de quoi nous inquiéter

Les Objets connectés et leurs failles de sécurité ont de quoi nous inquiéter
Dans une étude, HP s'est penché sur les failles de sécurité au sein de 10 objets connectés parmi les plus populaires. L'entreprise relève que ces nouveaux objets présentent de nombreuses vulnérabilités et incite les constructeurs à en tenir compte.

Cybercriminalité : « la situation française, en terme de ressources humaines, est proche de l'artisanal »

Un rapport sur la cybercriminalité a été dévoilé le 30 juin 2014, visant à renforcer l'arsenal pénal contre les infractions commises sur internet. Par ailleurs, de prochaines

lois pourraient s'en inspirer, comme le projet de loi sur le terrorisme, qui en affiche un certain nombre de traits.

Le rapport de Marc Robert, « protéger les internautes », avait été remis dès le mois de février. L'objectif de cet épais volume : renforcer la lutte contre la cybercriminalité, dont les statistiques croissantes démontrent l'urgente nécessité pour la France de se doter d'un arsenal adapté.

Très rapidement, le rapport dresse un constat cruel : « comparé à ce dont disposent les États étrangers voisins, la situation française, en terme de ressources humaines, est proche de l'artisanal ». Il fait 54 propositions pour pallier ces lacunes.

Certaines d'entre elles tracent des axes de réflexions, mais beaucoup ont de concrètes implications. Pour preuve : le projet de loi relatif à la lutte contre le terrorisme, présenté le 9 juillet dernier à l'Assemblée nationale, s'en est directement inspiré. L'exposé des motifs de son article 12 reprend en substance la proposition n° 15, qui préconise une augmentation du quantum de la peine pour les atteintes aux systèmes de traitement automatisés de données (STAD) et la création d'une circonstance aggravante de commission en bande organisée. Globalement, l'ensemble des dispositions de la loi concernant le cyber-terrorisme, notamment les articles 10 à 16, découlent de ce rapport.

Comme base de toute action, le rapport recommande que des statistiques précises soient établies chaque année, sous l'égide de l'office national de la délinquance et des réponses pénales (ONDRP). En 2012, 84 774 infractions ont été recensées par la Police et la Gendarmerie sur internet en 2012, l'immense majorité (84 %) sont des escroqueries, des abus de confiance et des fraudes à la carte bancaire. Mais comme le relève le rapport, « les infractions constatées par les

services de Police et de Gendarmerie n'épuisent pas la réalité de la cybercriminalité ». Il faut donc appréhender la cybercriminalité à travers l'action des services de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), l'action des douanes ou encore de la commission nationale de l'informatique et des libertés (CNIL).

Le constat est sans appel : ces infractions augmentent de manière exponentielle. En 2012, Le montant moyen d'une transaction frauduleuse est de 125 €, celles-ci constituant 0,08 % du total des transactions, et touchant 2,3 % des ménages. Le taux de poursuite, la « réponse pénale » est très faible, et seules 2 222 condamnations ont été prononcées pour des crimes et délits spécifiquement visés par la loi comme faisant partie de la cybercriminalité. Un tiers d'entre eux sont des atteintes aux personnes (délinquance sexuelle, et surtout, en hausse, la pédopornographie) ; un autre tiers est constitué d'infractions à la loi de 1881 (presse). Les si nombreuses infractions aux instruments de paiement ne représentent que 15 % du taux de répression.

Pour mieux lutter contre la cybercriminalité, le rapport s'appuie évidemment sur un volet préventif. La meilleure information du public, l'éducation dès le plus jeune âge à la pratique d'internet, la mise en place de numéros d'urgence sont préconisés. Mais c'est l'appareil judiciaire qui est complètement remodelé : il s'agit, est-il affirmé, de « former les acteurs pénaux, eu égard à la spécificité de la cybercriminalité ». Cette formation interviendrait dès la formation initiale, mais aussi en continu, du fait de la nature fortement évolutive de cette matière. Des magistrats référents verraient ainsi le jour, spécialistes de la cybercriminalité, pour traiter plus efficacement de ce contentieux. Le corpus pénal dont ils disposeraient ne doit

pas être « gonflé de lois inutiles » estime le rapport, qui note que l'arsenal répressif est déjà assez complet, et qu'il est indispensable de n'adopter que des dispositions utiles.

L'idée générale est que l'action globale soit coordonnée par une délégation interministérielle de lutte contre la cybercriminalité, la nature protéiforme de ces infractions nécessitant une organisation transversale. Au sein de la justice, c'est une mission de lutte contre la cybercriminalité qui serait créée, rattachée au directeur des affaires criminelles.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.dalloz-actualite.fr/flash/cybercriminalite-situation-francaise-en-terme-de-ressources-humaines-est-proche-de-l-artisanal

---

L'Union Européenne s'organise enfin pour lutter contre la

cybercriminalité

L'Union Européenne s'organise enfin pour lutter contre la cybercriminalité

L'Union Européenne prépare pour la rentrée la mise en place d'une force d'intervention commune dédiée à la cybersecurité. Cet organisme regroupera des experts venus de différents pays de l'UE et se penchera sur les cas dépassant la juridiction des enquêteurs nationaux.

Selon les informations du site britannique SCMagazine, cette force d'intervention commune répond au doux nom de Joint Cybercrime Action Taskforce et prendra ses fonctions en septembre 2014 pour une première période d'essai de 6 mois. Ce groupe aura pour objectif de lutter contre les réseaux de cybercriminalité étendus à l'international, à l'instar de certains botnets ou de plateforme de diffusion de malwares.

Ce groupe sera placé sous l'égide de l'European Cybercrime Task Force (EUCTF), un groupe constitué des différentes autorités nationales de lutte contre la cybercriminalité mis en place en 2010. L'EUCTF évaluera le travail de cette nouvelle force d'intervention. Cette dernière sera placée sous la direction d'Andy Archibald, le chef du département de lutte contre la cybercriminalité en Grande Bretagne.

Il aura sous ses ordres un ensemble d'expert en cybersecurité mandatés par différents pays mais SC magazine précise également que des participants externes aux pays de l'UE seront amenés à collaborer ponctuellement avec la JCAT.

Agir efficacement à l'international

Pour l'instant, les premiers pays à participer à ce projet sont la France, l'Angleterre, l'Autriche, le Royaume Uni, la Hollande, l'Allemagne mais aussi les Etats-Unis, qui disposeront tous d'une place permanente et d'experts au sein de cette force d'intervention. Si les résultats de cette première période d'essai s'avèrent concluants, la JCAT pourrait s'ouvrir à l'ensemble des pays européens.

Sa mise en place fait écho aux grandes opérations de démantèlement de réseaux botnets qui ont eu lieu récemment, avec notamment l'offensive contre le malware Gameover Zeus étendu à plusieurs états dans le monde. L'objectif de cette force d'intervention sera de permettre une plus grande coopération entre les différentes autorités nationales de lutte contre la cybercriminalité.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.zdnet.fr/actualites/une-force-d-intervention-cybersecurite-europeenne-sur-les-rails-39804343.htm