La Cnil sanctionne « Attractive World » et « Meetic »

	La Cnil sanctionne « Attractive World » et « Meetic »

Meetic a indiqué qu'en s'inscrivant sur son site de rencontre, « les personnes ont conscience et sont informées que les données qu'elles fournissent sont nécessaires pour la fourniture du service auxquelles elles souscrivent « , une forme de consentement express en quelque sorte.

Après plusieurs mises en garde, réunions et rencontres avec la CNIL, les deux géants Meetic et Attractive World n'avaient pas fait mine de s'intéresser aux recommandations de l'autorité pour changer un aspect important relatif à la protection des données personnelles. La Commission nationale de l'informatique et des libertés a prononcé, fin décembre 2016, une sanction publique de 10 000 euros à l'encontre de la société Samadhi, propriétaire du site Attractive World et de 20 000 euros à l'encontre de Meetic SAS, en raison du traitement des données *sensibles* de leurs utilisateurs sans recueil de leur consentement exprès.

Il faut dire que ces sites sont de plus en plus thématisés, ciblés, en fonction de goûts ou de communautés. Un point que ne partage pas la CNIL qui déplore un manquement évident à la loi « *Informatique et Libertés* « .

Conséquence, en juillet dernier, 8 sites, et pas des moindres, ont été mis en demeure de rectifier le tir. Visiblement, deux d'entre eux n'ont pas joué le jeu. En effet, en cas d'attaque malveillante à l'encontre de ces sites, donc de piratage informatique, les données personnelles et *sensibles* peuvent se retrouver dans la nature ce qui pourrait être déplorable pour les utilisateurs qui n'ont pas donné leur consentement éclairé sur l'exploitation de leurs données privées, qui plus est, sur leurs affinités, leurs croyances, leurs avis politiques ou leurs origines ethniques.

« Les utilisateurs souhaitant s'inscrire aux sites devaient – en une seule fois – accepter les conditions générales d'utilisation, attester de leur majorité et consentir au traitement des données *sensibles*« , rappelle la Cnil. « La seule inscription au **site de rencontre** ne peut valoir accord exprès des personnes au traitement de telles données qui révèlent **des éléments de leur intimité**« .

Original de l'article : « Attractive World » et « Meetic » épinglés par la Cnil

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : « Attractive World » et « Meetic » épinglés par la Cnil

Des sites de piratage bientôt bannis du net par les USA ?

	Des sites de piratage bientôt bannis du net par les USA ?

Les États-Unis ont toujours pris très au sérieux les menaces de la cybercriminalité, que ce soit à l'égard de l'économie du pays ou bien à l'égard de la sécurité nationale.

L'Oncle Sam ne lésine pas sur les moyens pour traquer sans relâche les présumés pirates informatiques. Tout récemment, le gouvernement américain a rendu publique la liste regroupant des sites considérés comme ayant des liens à des affaires de piratage.
Au fil des années, de nouvelles méthodes de piratage, plus sophistiquées les unes que les autres, apparaissent. Alors, *aux grands maux les grands remèdes* ! Des trackers notoires sont depuis des années dans le collimateur des États-Unis. C'est le cas, parmi tant d'autres, de ***The Pirate Bay*** **ou** ***ExtraTorrent***. La Maison Blanche, selon des sources plausibles, inclut également dans sa liste de sites à abattre certains hébergeurs de fichiers. Parmi les noms cités figurent notamment *Rapidgator,* mais aussi *Uploaded*. Mais ces plateformes sont déjà connues, ou du moins, soupçonnées d'être mêlées à des activités d'espionnage. Ce qui est surprenant dans cette affaire, c'est surtout le fait que les États-Unis se penchent aussi sérieusement sur des sites de ripping tels que YouTube-MP3.

Jusqu'à preuve du contraire, les sites européens ne sont pas dans le collimateur des États-Unis

C'est en tout cas ce que laissent entendre des pistes sérieuses qui se penchent sur la cybercriminalité. Ce serait vraiment sidérant de la part du gouvernement américain puisqu'il n'y a pas un seul pays européen où **les sites pirates ne pullulent pas.** En France, pour des raisons qu'on ne connaît pas, Zone-Téléchargement ne figure pas dans la liste noire des États-Unis. À noter tout de même que cette plateforme fait partie des plus gros acteurs du marché français.
Un grand nombre de sites de streaming sont **également dans le viseur de la Maison Blanche.** C'est le cas notamment de *Putlocker*, *Primewire* ou encore *123movies…* Comme pour la drogue, une grande partie des moyens financiers déployés par le gouvernement américain est destinée à la répression.
.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Les États-Unis révèlent les noms des sites de piratage qu'ils souhaitent bannir du net – MeilleurActu

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

Karspersky publie aujourd'hui sur son blog un compte rendu d'une enquête des autorités russes à laquelle ils ont collaboré. Celle-ci a permis l'arrestation en juin d'un groupe de 50 cybercriminels, baptisés Lurk, qui opéraient notamment l'Angler exploit kit.

L'Angler Exploit Kit connaissait ces dernières années une popularité redoublée. Ce couteau suisse du cybercriminel était une plateforme utilisée pour infecter les machines de victimes : en l'installant sur un serveur et en amenant la cible à se connecter à ce serveur via un navigateur par exemple, le cybercriminel pouvait avoir recours à tout un éventail d'exploits fournis par les créateurs du kit pour tenter d'infecter la machine de la victime.

Simple à utiliser, évolutif et souvent à jour avec les derniers exploits et dernières vulnérabilités découvertes, l'Angler Exploit Kit dominait naturellement le marché. Mais en juin 2016, l'utilisation de cet outil par les cybercriminels a soudainement chuté sans véritable explication.

De nombreux observateurs avaient néanmoins fait le lien entre l'arrestation d'un groupe de 50 cybercriminels par les autorités russes et la soudaine disparition de l'Angler Kit. Dans une longue note de blog, Ruslan Stoyanov, dirigeant de l'unité investigation chez Kaspersky confirme cette théorie et détaille les 5 années passées sur la piste de ce groupe de cybercriminels de haute volée qui avaient été baptisés « Lurk ».

Le nom du groupe Lurk vient du premier malware repéré par Kaspersky en 2011. Celui-ci se présentait sous la forme d'un malware bancaire sophistiqué, qui visait principalement les logiciels bancaires afin de procéder à des virements frauduleux en direction des cybercriminels. Swift a connu plusieurs versions et évolutions, allant parfois jusqu'à fonctionner entièrement in memory pour éviter la détection.

Le malware Lurk se présentait comme un logiciel modulaire, pouvant embarquer plusieurs modules capables de réaliser des actions différentes, mais toujours orientées vers le vol de données bancaires et l'émission de virements frauduleux depuis les machines infectées.

Une petite PME sans histoire

« Avec le temps, nous avons réalisé que nous étions face à un groupe d'au moins 15 personnes. (…) Cette équipe était en mesure de mettre en place le cycle complet de développement d'un malware : à la fois sa conception, mais aussi la diffusion et la monétisation, à l'instar d'une petite entreprise de développement logiciel » explique Ruslan Stoyanov. Et le groupe Lurk avait également un autre atout de taille dans sa poche : exploitant leur renommée parmi les cybercriminels russophones, ils avaient commencé à louer les services de leur plateforme d'exploit, baptisée Angler Kit.

Cet exploit kit était à l'origine utilisé pour diffuser le malware bancaire Lurk, mais face aux mesures de sécurisation mises en place par de nombreuses banques, les revenus déclinants du groupe les ont forcés à diversifier leur activité. Les premières détections d'Angler Kit remontent à 2013, mais ce kit vendu en Saas par les cybercriminels du groupe Lurk a rapidement gagné en popularité.

Les créateurs du Blackhole kit ont été arrêtés en 2013, ce qui a laissé au nouveau programme du groupe Lurk un boulevard pour devenir le nouvel exploit kit préféré des cybercriminels. Dès le mois de mai 2015, celui-ci dominait largement le marché. Angler Kit pouvait être loué par d'autre groupe de cybercriminels qui s'en servaient pour diffuser différents types de malwares allant du ransomware au traditionnel trojan bancaire.

Mais le 7 juin, les autorités russes sont parvenues à arrêter les cybercriminels cachés derrière ce système. Kaspersky explique avoir collaboré avec les autorités afin de mener cette investigation, notamment via de l'échange d'informations compilées par la société sur le groupe. Un processus qui semble avoir été long et difficile, mais qui aura finalement porté ses fruits : l'Angler Kit est hors service et peut maintenant laisser la place… au nouvel exploit kit à la mode.

Selon les données récentes compilées par la société Trend Micro, l'exploit kit Neutrino aurait maintenant le vent en poupe et profiterait le plus de la retraite anticipée de son concurrent. Un de coffré, dix de retrouvés ?

Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : L’un des outils préférés des cybercriminels mis à mal par un coup de filet ? – ZDNet

---

La cybercriminalité a de belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.

Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.

Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.

Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.

Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.

Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.

Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!

Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.

Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.

Article original de branchez-vous.com

Réagissez à cet article

Original de l’article mis en page : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Un vendeur d’armes du Black Market jugé

Un vendeur d’armes du Black Market jugé

Le vendeur d’armes Gun Runner arrêté et jugé. Il revendait dans le black market pistolets et armes de guerre.

Je vous ai souvent parlé de ce vendeur d’armes du black market baptisé GunRunner. Ce commerçant du dark web commercialisait Glocks, Uzi et pistolet Walthers, celui de James Bond, comme un boulanger vend des petits pains. Arrêté et jugé en juin dernier, Michael Andrew Ryan, a été traqué par l’ATF, l’agence en charge du contrôle des armes et explosifs sur le sol de l’Oncle Sam.

Gun Runner a oublié que l’ATF possédait un service de renseignement plutôt costaud et des bases de données qui feraient pâlir les amateurs de Big Data. Bilan, même si Michael Andrew Ryan limait les numéros de série, l’ATF a pu remonter au vendeur et à l’historique de ses produits vendues dans le black market. Il vendait son arsenal via son domicile du Kansas. Il revendait ses armes dans plusieurs boutiques, dont le shop Reloaded. Il a plaidé coupable. Il risque tout de même une peine maximale de 10 ans de prison et jusqu’à 250 000 $ d’amende.

Ryan connaitra son sort le 12 Septembre. Je doute qu’il passe Noël chez lui avec les matériels et les munitions qu’il a pu vendre : Beretta 9 mm, Taurus .38, Uzi, …

En novembre 2015, je vous parlais d’un autre vendeur de 48 ans qui a proposé 32 armes dans le dark web à des Suédois et Australiens. Selon une étude réalisée par un professeur de l’Université Carnegie Mellon, la vente illégale d’armes à feu représenterait moins de 3% des négociations dans les boutiques du Dark Web. Il faut dire aussi qu’avec les centaines de boutiques fourguant des milliers de drogues, le chiffre ne veut pas dire grand-chose.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Black market : un vendeur d’armes jugé – ZATAZ

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

---

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

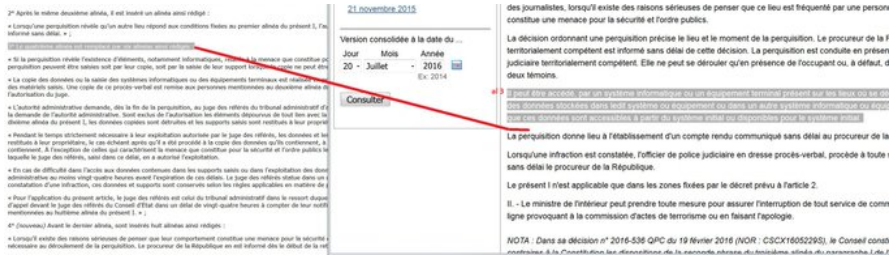
---

État d'urgence : la police pourra bien copier des données trouvées dans le Cloud

État d'urgence : la police pourra bien copier des données trouvées dans le Cloud

Contrairement à ce que nous écrivions mardi avec étonnement, il sera bien possible pour la police d'utiliser l'ordinateur ou le smartphone d'un suspect pour accéder à tous ses services en ligne, puis de copier les informations obtenues pour les exploiter si elles sont pertinentes.

Il faudrait toujours retourner son clavier sept fois sur le bureau avant de donner un satisfecit au gouvernement. Mardi, nous détaillions le cadre prévu dans le projet de loi de prorogation de l'état d'urgence, pour la copie des données informatiques dont Manuel Valls avait annoncé le retour. Il fallait vérifier si les exigences du Conseil constitutionnel en matière de respect de la vie privée étaient bien respectées.
À cette occasion, nous faisions remarquer à tort que le gouvernement n'avait pas prévu la possibilité de copier des données stockées dans les services en ligne des suspects, se limitant curieusement aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* ».
Pris dans un élan de naïveté, nous n'avions pas fait attention au fait que l'ensemble du dispositif n'était pas réécrit, et que le gouvernement avait laissé intacte une disposition non censurée par le Conseil constitutionnel, qui change toute l'analyse. Elle dit qu'en cas de perquisition administrative, « *il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Créé en novembre 2015, cet alinéa de l'article 11 de la loi du 3 avril 1955 relative à l'état d'urgence n'a pas été supprimé, comme le fait justement remarquer Marc Rees deNext Inpact :
Voir l'image sur Twitter



Suivre
marc rees @reesmarc
. @p_estienne j'ajoute que PJL #EtatdUrgence ne supprime pas accès au cloud cc @gchampeau (gauche PJL droite, L55)
11:03 – 20 Juil 2016
•
•
77 Retweets
•
1 j'aime
Il reste donc possible pour la police d'accéder sur place à toutes données disponibles sur le Cloud, en profitant des sessions ouvertes sur des services en ligne (ou dont le mot de passe est mémorisé). Dès lors, à partir du moment où ils sont affichés à l'écran ou téléchargés, ces messages Facebook, e-mails, documents Google Docs, historiques WhatsApp ou autres fichiers stockés à distance deviennent bien des « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », qui peuvent être copiées et analysées après autorisation du juge, dans le cadre désormais fixé.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : la police pourra bien copier des données trouvées dans le Cloud – Politique – Numerama

---

Des complices de cyberescrocs arrêtés en Côte d’Ivoire

Des complices de cyberescrocs arrêtés en Côte d’Ivoire

Utilisation frauduleuse d’éléments d’identification de personne physique, tentative d’escroquerie et complicité d’escroquerie sur internet. Accusés de tous ces crimes, Traoré Issouf, 28 ans, et Kouadio Konan Daniel, 27 ans, tous deux caissiers dans une agence de transfert d’argent nouvellement ouverte, séjournent à la Maison d’arrêt et de correction d’Abidjan (Maca), dans l’attente d’un procès.

Comme l’explique la Plateforme de lutte contre la cybercriminalité (PLCC), ces deux individus ont été arrêtés le 20 juin 2016 par ses agents. Ils sont suspectés d’avoir effectué des transferts frauduleux au profit de quelques cyberescrocs, qui recourent bien souvent à des employés de maisons de transfert d’argent pour encaisser leur butin.
Pour chaque transfert effectué, Kouadio Konan Daniel a avoué avoir perçu une commission de 10%. Mais pouvaient-ils vraiment nier les faits? Après analyse des éléments en leur possession, le Laboratoire de criminalistique numérique (LCN) de la Direction de l’informatique et des traces technologiques (DITT) a pu extraire de nombreux codes de transfert d’argent envoyés par téléphone portable.
Article original de Anselme Akéko – CIO-Mag Abidjan

Réagissez à cet article

Original de l’article mis en page : Transfert d’argent : des complices de cyberescrocs arrêtés en Côte d’Ivoire | CIO MAG

Prison ferme pour les auteurs de SpyEye botnet

	Prison ferme pour les auteurs de SpyEye botnet

Le code malveillant SpyEye botnet a fait de gros dégâts en son temps. Les deux auteurs, Russe et Algérien, de ce kit informatique dédié à l'espionnage viennent d'écoper de 24 ans de prison ferme.

Les deux pirates Russe et Algérien cachés derrière le code malveillant SpyEye ont été reconnus coupables par la justice américaine d'avoir fabriqué et vendu ce kit malveillant dont le but premier était d'infiltré les ordinateurs pour espionner et voler les données des machines infiltrées.

Le prix de SpyEye botnet

Les deux pirates ont été condamnés à 24 ans de prison ferme (les deux peines cumulées). Une condamnation forte pour un outil, aussi baptisé Zeus, qui a permis d'infecter des centaines de milliers d'ordinateurs de par le monde. Une peine de neuf ans et six mois pour Aleksandr Andreevich Panin (27 ans), connu sur la toile sous le pseudonyme de « Gribodemon » et « Harderman ». Le FBI avait lancé un « Wanted » sur la tête de Panin de 3 millions de dollars. En juin 2015, l'ensemble des interactions de Zeus / SpyEye avait été stoppé par le FBI, Europe et Eurojust. Plusieurs dizaines de personnes ont été arrêtés, de l'utilisateur de SpyEye aux blanchisseurs d'argent volé.

L'Algérien Hamza Bendelladj, alias Bx1 a écopé de 15 ans. Ce dernier, âgé de 27 ans, était le partenaire d'affaires de Panin. Ce ressortissant algérien avait plaidé coupable en Juin 2015. Il avait modifié SpyEye pour réaliser son propre outil malveillant qui lui a permis de voler 200.000 numéros de carte de crédit. Bendelladj, baptisé « Le pirate souriant » avait été arrêté à Bangkok, en janvier 2013. Extradé aux USA en mai 2013. Il vient de perdre définitivement son grand sourire !
Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.

Dans les outils proposés par les pirates, des ransomwares, comme Locker

Dans les outils proposés par les pirates, des ransomwares, comme Locker, qui se faisait passer pour le FBI.

SpyEye, comme j'avais pu vous le montrer à l'époque [1e capture écran de cet article], était commercialisé dans le black market, dans une boutique baptisée à l'époque DarkCode.
Article original

Réagissez à cet article

Original de l'article mis en page : Prison ferme pour les auteurs de SpyEye botnet

---

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Adepte du malware Lurk, un réseau de cybercrimels vient dêtre démantelé en Russie. Il est responsable du vol de plus de 22 millions deuros à des banques.

Une cinquantaine d'interpellations en Russie ont abouti au démantèlement d'un réseau de cybercriminels surnommé Lurk. Un nom qui découle de l'emploi d'un cheval de Troie identifié en 2012.
À l'époque, Kaspersky Lab avait évoqué le cas de Lurk dans des attaques drive-by. Conçu pour voler des données sensibles d'utilisateurs afin d'obtenir un accès à des services de banques en ligne russes, le malware n'était pas téléchargé sur le disque dur et opérait uniquement dans la mémoire RAM.
Threatpost (Kaspersky Lab) écrit que Lurk a commencé à attaquer des banques il y a un an et demi, et a rapatrié divers malwares de serveurs de commande et contrôle. Les attaquants ont utilisé un VPN compromis afin de rendre leur campagne plus difficile à détecter.
Grâce à Lurk, les cybercriminels ont dérobé plus de 1,7 milliard de roubles (près de 22 millions d'euros) à des comptes d'institutions financiers russes, a indiqué le FSB (l'ancien KGB) à l'agence de presse russe TASS.
Article original de Jérôme GARAY

Réagissez à cet article

Original de l'article mis en page : Piratage de banques : un gang russe démantelé