Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Université Lyon 3 : 88.000 contacts ont été dérobés par les pirates informatiques

Les services de l'université Lyon 3 avait d'abord parlé d'une fuite d'environ 5000 contacts pour la plupart étudiants, cependant depuis une plus récente information du site lepoint.fr, l'université aurait reconnu avoir fait fuité par erreur, 88 000 contacts. Un cas plus grave que le premier dont on vous avez fait écho au début du mois de février. Pour rappel, les fichiers dérobés contenaient les noms, prénoms, date de naissance, informations sur le cursus suivis, adresses personnelles postale et électronique, numéros d'étudiants fixe et mobile, mais aussi des conversations échangées par e-mail entre les étudiants et le personnel de l'université ou encore les coordonnées d'entreprises partenaires de l'université.

Des mesures contre les cyberattaques prises en décembre
Contactée par lepoint, l'université « a regretté un cafouillage de communication », avant qu'Yves Condemine, le directeur des systèmes d'informations (DSI), explique que « la base de données piratées concerne 88 000 contacts ». Bien qu'aujourd'hui « les problèmes sont réglés », il affirme néanmoins que « des mesures avaient été prises dès décembre », après des alertes envoyées par un des étudiants de l'université. Le directeur des services d'informations reste cependant « encore prudent » dans la surveillance du réseau même si « rien ne permet aujourd'hui de penser que (l')infrastructure soit compromise », affirme t-il.

L'agence de cyberdéfense n'analysera pas le réseau de l'université
Cependant, l'université n'a pas souhaité l'intervention de l'agence de cyberdéfense. Malgré l'urgence de la situation et la charge de travail nécessaire pour analyser la totalité du réseau, l'université a souhaité s'occuper seule de cette tâche. L'incident à néanmoins était signalé à son ministère de tutelle qui a contacté l'Anssi, l'agence nationale de cyberdéfense, sans pour autant la saisir. « Nous sommes restés en contact avec l'Anssi, via le ministère de l'Enseignement supérieur », affirme Yves Condemine à lepoint. Pas très rassurant si l'agence de cyberdéfense ne peut ni analyser, ni trouver d'éventuelles portes dérobées dans le réseau, ni même remonter jusqu'aux pirates pour comprendre leurs intentions en piratant la base de données d'une université.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.digischool.fr/a-la-une/universite-lyon-3-contacts-derobes-pirates-informatiques-26701.php

---

Fuites subies par Anthem : une attaque lente et silencieuse

Fuites subies par Anthem : une attaque lente et silencieuse

L'attaque menée contre Anthem, le second plus grand assureur aux États-Unis dans le domaine de la santé, qui a exposé les données personnelles identifiables de dizaines de millions d'assurés, n'était probablement pas un simple raid rapide mais plutôt un détournement continu et discret d'informations sur une période de plusieurs mois. L'attaque était conçue pour ne pas être détectée par les équipes informatiques et de sécurité de l'entreprise, et reposait sur un mécanisme d'infection par bot pour exfiltrer les données, explique Thierry Karsenti, Directeur Technique Europe de Check Point Software Technologies. Voici son analyse.

Selon les déclarations d'Anthem, les premiers signes de l'attaque sont apparus au milieu de la semaine dernière, lorsqu'un administrateur informatique a remarqué qu'une requête de base de données était exécutée à l'aide de son identifiant sans qu'il ne l'ait déclenchée. L'entreprise a déterminé qu'une attaque avait eu lieu, a informé le FBI et a engagé un consultant externe pour mener une enquête de sécurité.

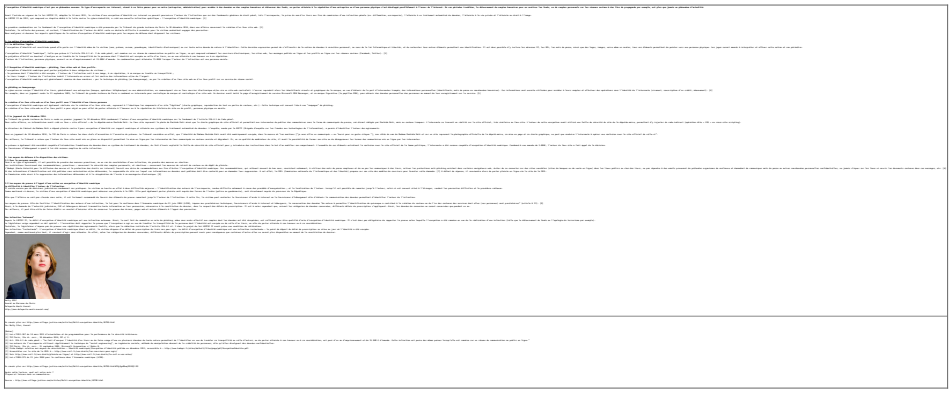
Les enquêteurs ont constaté qu'un logiciel malveillant personnalisé a été utilisé pour infiltrer les réseaux d'Anthem et dérober des données. Le type exact de logiciel malveillant n'a pas été communiqué, mais il semble être une variante d'une famille connue d'outils de piratage. Un rapport de sécurité indépendant signale que l'attaque a pu commencer trois mois auparavant. Le consultant a remarqué une « activité de type botnet » dans des entreprises affiliées à Anthem en novembre 2014.
Ce n'est pas surprenant car les activités de bot à long terme sont courantes dans les entreprises. Le Rapport Sécurité 2014 de Check Point, basé sur la surveillance d'événements dans plus de 10 000 entreprises dans le monde entier, a constaté qu'au moins un bot a été détecté dans 73% des entreprises, contre 63% l'année précédente. 77% des bots étaient actifs pendant plus de quatre semaines, et communiquaient généralement avec leur « centre de commande et de contrôle » toutes les trois minutes.
Les bots sont capables d'échapper à toute détection car leurs développeurs utilisent des outils d'offuscation pour leur permettre de contourner les solutions antimalwares traditionnelles reposant sur des signatures. En tant que tel, l'émulation des menaces, également appelée « émulation en bac à sable », devrait être utilisée comme couche de défense supplémentaire pour stopper les bots avant qu'ils n'infectent les réseaux. Des solutions antibots devraient également être déployées pour faciliter la découverte des bots, et empêcher d'autres fuites en bloquant leurs communications.
Il est également important que les entreprises segmentent leur réseau, en séparant chaque segment par des couches de sécurité pour empêcher les infections de bot largement répandues. La segmentation peut restreindre les infections à une zone particulière du réseau pour atténuer les risques et empêcher les infections d'accéder à des données confidentielles dans d'autres segments du réseau.
Avec ces trois approches préventives, les entreprises peuvent réduire considérablement leur exposition au type d'attaque lente et furtive qui semble avoir frappé Anthem, et éviter de devenir la victime de fuites à grande échelle.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

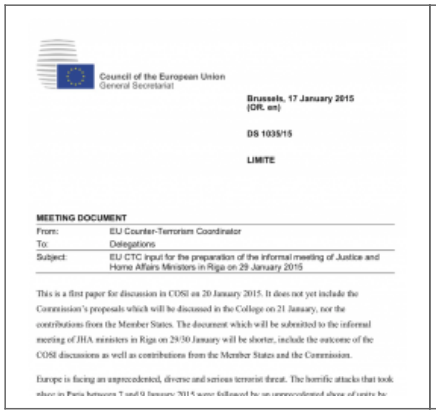
Source : http://www.itrmanager.com/articles/154049/fuites-subies-anthem-attaque-lente-silencieuse.html

Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

	Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.



L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?



Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From:	EU Counter-Terrorism Coordinator
To:	Delegations
Subject:	EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

La montée en puissance du terrorisme en Europe relance le débat sur le chiffrement des communications et la création de backdoors réservés aux forces de l'ordre européenne. Le coordinateur antiterrorisme de l'UE, Gilles de Kerchove, demande sans détour un accès aux clefs de chiffrement des géants de l'Internet.

Les géants de l'Internet vont-ils bientôt être obligés de partager leurs clés de chiffrement avec la police et les agences de renseignement européennes pour les aider à lutter contre le terrorisme ? C'est en tout cas une recommandation ferme de Gilles de Kerchove, le coordinateur antiterrorisme de l'Union Européenne. C'est une suggestion étonnante quand on se souvient que les entreprises comme Google ou Facebook ont commencé à chiffrer leurs communications pour lutter contre la curiosité des agences de renseignement chinoises mais aussi américaines, anglaises, allemandes, hollandaises et françaises comme l'ont indiqué les documents révélés par Edward Snowden.

L'association de protection des droits civils Statewatch
a divulgué un document rédigé par le coordinateur
antiterroriste Gilles de Kerchove.

Gilles de Kerchove suggère que la Commission européenne « devrait revoir ses règles pour obliger les entreprises de l'Internet et des télécommunications opérant dans l'UE à fournir … aux autorités nationales compétentes un accès à leurs communications [c'est à dire leurs clefs de chiffrement] », selon un document divulgué par l'association de protection des droits civils Statewatch. Dans ce document, M. de Kerchove expose ses vues sur les mesures anti-terrorisme à prendre dans l'UE en vue d'une réunion des ministres de la Justice et de l'Intérieur de l'UE à Riga, la semaine prochaine.

Des keyloggers pour suivre les échanges

Cette proposition est controversée parce que, comme le note le coordinateur, la généralisation du chiffrement pour les échanges sur Internet rend très difficile, voire impossible, les interceptions légales par les autorités nationales compétentes. Nous avons discuté de ces questions avec les cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N). Sans coopération des fournisseurs de services (Whatsapp, Skype ou encore iMessage), il est très difficile de lire les messages échangés. La solution la plus facile – pour les forces de l'ordre – est aujourd'hui l'installation d'un cheval de Troie ou keylogger (un enregistreur de frappes) sur les terminaux des suspects, smartphones, tablettes ou PC. Une opération toujours délicate puisqu'elle doit être effectuée à l'insu des utilisateurs.

« Whatsapp ou Viber commencent à être très utilisés par les criminels avec des mobiles jetables », nous avait confié le major Etienne Neff de la section de Paris. « Les criminels sont aujourd'hui plus sophistiqués et utilisent également des solutions payantes ». Les forces de l'ordre peuvent toujours accéder aux métadonnées fournies par les opérateurs mais il faut séparer le flux et le reconditionner pour le traiter.

Les entreprises également sous surveillance

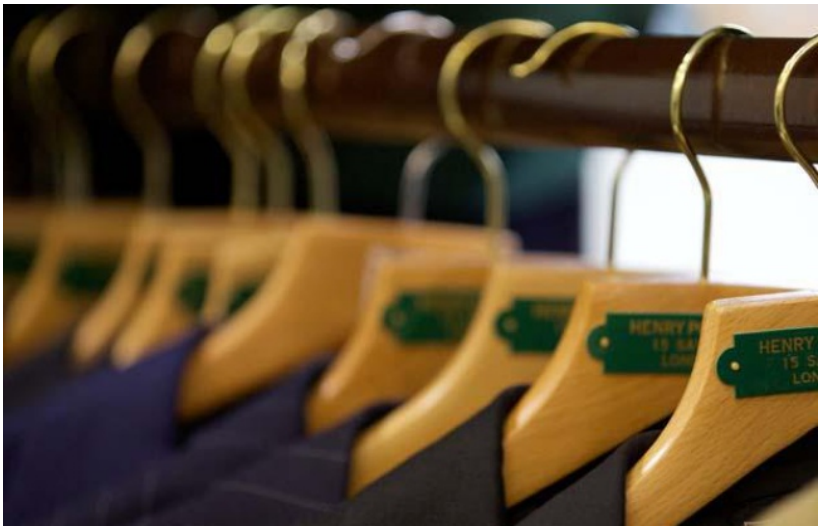
L'appel à plus de surveillance des échanges sur Internet est revenu sur le devant de la scène en Europe suite aux assassinats perpétués dans les bureaux du magazine satirique Charlie Hebdo et à l'épicerie HyperCacher à Paris. Après les deux attentats, les ministres de la Justice et de l'Intérieur de l'UE avaient publié une déclaration commune dans laquelle ils soulignaient qu'il est essentiel « d'entretenir une étroite collaboration avec les FAI pour endiguer la propagande terroriste en ligne ».

Si la Commission a refusé de commenter les plans anti-chiffrement de M. de Kerchove, le document fuité contient des détails supplémentaires comme le contrôle du « chiffrement décentralisé » des entreprises. Cela pourrait être une référence au chiffrement de bout-en-bout utilisé par certaines entreprises sensibles pour verrouiller leurs communications.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-l-ue-doit-elle-obliger-les-geants-de-l-internet-a-ceder-leurs-cles-de-chiffrement-59993.html
Par Serge Leblal

Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes – 20minutes.fr



Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes

Près de la moitié (49%) des entreprises de distribution et de biens de consommation au niveau mondial déclarent avoir été victimes de fraudes au cours des deux dernières années, selon une étude de PwC diffusée lundi.

«Ce chiffre ne cesse d'augmenter depuis 2009 (+12 points)», note le cabinet de conseil, qui a interrogé 5.128 dirigeants d'entreprises, dont 383 du secteur de la distribution et des biens de consommation, issus de 99 pays. La fraude la plus largement commise dans le secteur est le détournement d'actifs (76%), ce qui inclut «le vol, les décaissements frauduleux et l'appropriation illicite de matériel».

Risques liés à la cybercriminalité

La fraude aux achats arrive en deuxième position, beaucoup de répondants évoquant notamment des infractions liées à la sélection des fournisseurs (59%) ou bien aux contrats/accords de maintenance conclus avec ces derniers (39%).
Si la corruption n'est pas la fraude la plus constatée (25%), 56% des dirigeants interrogés la considèrent comme le risque le plus élevé pour une entreprise opérant à l'international.
Beaucoup de dirigeants évoquent également les risques grandissants liés à la cybercriminalité: un sur cinq déclare en avoir été déjà victime, et 27% pensent que leur entreprise y sera confrontée dans les deux années à venir.

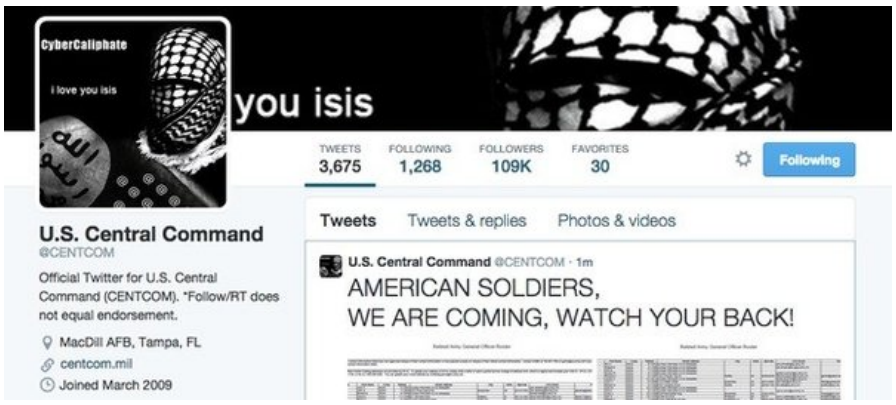
Risque de renvoi ou de poursuites judiciaires

La perte de propriété intellectuelle (contrefaçon, vols de données clients…) fait également partie de leurs préoccupations pour l'avenir: seuls 7% en ont déjà fait l'expérience, mais 21% estiment qu'ils y seront confrontés d'ici deux ans.
L'étude montre que dans plus de deux tiers des cas (67%), les auteurs de ces infractions sont des collaborateurs internes aux entreprises. Ce taux est supérieur dans les secteurs de la distribution/biens de consommation, aux taux constatés sur l'ensemble des secteurs (56%).
«Les auteurs de ces faits occupent, pour la plupart, des postes de cadres intermédiaires et sont sévèrement punis lorsqu'ils sont démasqués: les entreprises pratiquent majoritairement le renvoi; elles se lancent parfois dans des poursuites civiles ou recourent aux autorités judiciaires», indique PwC.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.20minutes.fr/societe/1515087-20150112-vols-cybercriminalite-contrefacons-pres-50-entreprises-victimes-fraudes

Les comptes Twitter et Youtube du commandement de l’armée US piratés



Les comptes Twitter et Youtube du commandement de l’armée US piratés

Le groupe de pirates informatiques Cyber Caliphate, qui se réclame de l’Etat islamique, s’est emparé, hier soir, des comptes Twitter et Youtube du commandement central de l’armée américaine (Centcom).

Un acte symbolique plus qu’une réelle cyberattaque

Dans un billet publié sur Pastebin, les pirates revendiquent le hack du réseau du Pentagone.

Rien de moins. Et de révéler ce qui est présenté comme des données confidentielles avant de menacer : *« Soldats américains, nous arrivons, surveillez vos arrières ! Nous sommes dans vos PC, dans vos bases militaires. »*

Un acte qui pourrait s’apparenter au début d’une cyberguerre, mais qui est plutôt considéré par le commandement de l’armée américaine comme du cybervandalisme.

Pourquoi minimiser ainsi les faits ?

Parce qu’à y regarder de plus près, les informations dévoilées sont au pire, non sensibles, ou mieux, carrément publiques. Seul un dossier contenant les données personnelles de plusieurs généraux (en activité ou à la retraite) pose problème, bien que ces informations ne soient pas classées.

Le commandement de l’armée a donc réagi avec mesure : « Nous pouvons confirmer que nos comptes Twitter et Youtube ont été compromis. Nous prenons les mesures appropriées pour adresser ce problème. » Et ont ajouté « Nous voyons cela comme un acte de cybervandalisme. Aucune information classée n’a été postée et aucune des données dévoilées ne proviennent des serveurs du Centcom. »

Le message posté par le groupe Cyber Caliphate semble indiquer que les pirates ont d’autres informations à partager. Nous verrons si elles se révèlent plus stratégiques que celles fournies jusque là. À moins qu’ils n’aient pas le temps d’agir : les Anonymous ont le groupe de hackers en ligne de mire.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

S o u r c e :

http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-749439-piratage-cyber-caliphate.html?estat_svc=s%3D223023201608%26crmID%3D639453874_822822691

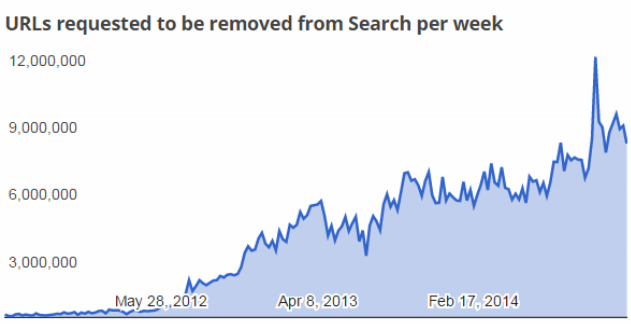
Google a retiré des millions de pages Web de son moteur en

2014

Piratage, Google a retiré des millions de pages Web de son moteur en 2014

En 2014, Google a reçu plus de 345 millions de demandes de retrait de pages Web de son moteur de recherche au nom du droit d'auteur. C'est 75% de plus qu'en 2012 et cela devrait encore s'accélérer en 2015.

Les grandes organisations d'ayants droit ont à plusieurs reprises reproché à Google de ne pas en faire suffisamment pour lutter contre le téléchargement illégal sur Internet. Le géant s'est pourtant, en matière de déréférencement, montré particulièrement actif en 2014.
Selon les données compilées par Torrent Freak et extraites des rapports de transparence de la firme, Google a reçu l'année passée environ 345 millions de demandes de retrait de pages Web de son moteur de recherche. Des requêtes DMCA dans la grande majorité des cas satisfaites par Google qui procède donc à leur déréférencement.



Moins de 100 millions de demandes en 2012
Et si le nombre de ces demandes est élevé, il est aussi en très forte croissance sur un an, de l'ordre de 75%. La tendance n'est pas nouvelle, même si l'inflation du nombre de demandes de retrait est plus forte ces dernières années.

En mai 2012, Google recevait moins d'un million de requêtes DMCA par semaine de la part des ayants droit. En 2014, ce rythme a atteint puis dépassé les 6 millions par semaine. Une inflation à laquelle participe largement l'industrie musicale britannique qui au travers de la BPI représente plus de 60 millions des demandes de retrait adressées à Google en 2014, soit 17% du total.
Quant aux domaines les plus ciblés par ces accusations de violation du droit d'auteur, il s'agit, d'après TorrentFreak, de 4shared.com, rapidgator.net et uploaded.net, visés chacun par 5 millions de requêtes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/piratage-google-a-retire-des-millions-de-pages-web-de-son-moteur-en-2014-39812271.htm

Des cybercriminels dérobent 25M$ à des banques russes

	Des cybercriminels dérobent 25M$ à des banques russes

Un groupe de cybercriminels baptisé Anunak a réussi à infiltrer les réseaux informatiques et à détourner les distributeurs automatiques d'institutions bancaires en Russie et dans des pays voisins. Il a également ciblé des terminaux point de vente de revendeurs américains et européens.

Un groupe de cybercriminels très aguerris a volé plus de 25 millions de dollars en piratant l'infrastructure de plusieurs institutions financières russes et de pays de l'ancien bloc soviétique, et en détournant des systèmes de points de vente appartenant à des revendeurs américains et européens. Des chercheurs de l'entreprise russe spécialisée dans la cybercriminalité Group-IB, et de l'entreprise de sécurité néerlandaise Fox-IT, ont baptisé le groupe Anunak, d'après le malware qui a servi de base au set d'outils utilisé par les pirates.
En général, les cybercriminels ciblent les clients des institutions financières, mais le groupe Anunak s'est attaqué directement aux institutions elles-mêmes, s'infiltrant dans leurs réseaux informatiques, jusqu'aux postes de travail et aux serveurs. Grâce à cet accès, le groupe a pu transférer des fonds sur des comptes dont ils avaient le contrôle, réussissant même dans certains cas, à détourner des distributeurs de billets automatiques sur lesquels ils ont pu ensuite retirer frauduleusement de l'argent. « Depuis 2013, ce groupe est parvenu à infiltrer les réseaux de plus de 50 banques russes et de 5 systèmes de paiement, et deux de ces institutions ont été privées de leur licence bancaire », a déclaré l'entreprise de sécurité russe Group-IB dans un rapport publié lundi. « À ce jour, le montant total du vol dépasse le milliard de roubles (environ 25 millions de dollars), la plus grande partie ayant été volée au cours du second semestre de 2014 ».

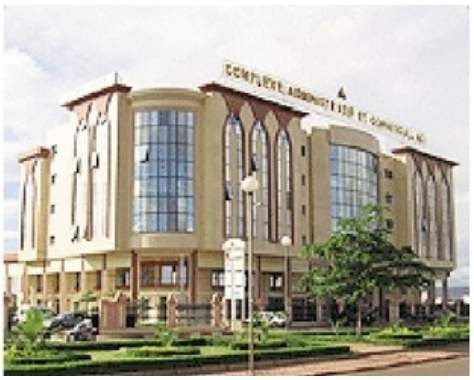
Un arsenal d'outils au service du piratage
Tout commence par l'infection des ordinateurs des salariés avec des logiciels malveillants, lesquels servent ensuite de point d'accès au réseau interne, aux serveurs et aux comptes de domaine actifs. Et le groupe Anunak ne lésine pas sur les outils : scanners de réseau, keyloggers, logiciels pour cracker les mots de passe, backdoors SSH, programmes de contrôle à distance, avec en plus, la plupart du temps, le framework Metasploit pour tester les failles et réaliser des exploits. Mais, leur principal outil est un cheval de Troie nommé Anunak. Celui-ci est basé sur le malware Carberp, conçu pour dérober des informations d'identification sur les sites de banque en ligne et dont le code source a été rendu public en juin 2013. Les chercheurs de Group-IB pensent que le groupe Anunak comprend sûrement des membres de l'ancien gang Carberp, éclaté en 2013 après des conflits internes.
Les attaquants utilisent plusieurs méthodes pour infecter les ordinateurs avec le Trojan Anunak. Par exemple, le téléchargement de logiciels malveillant quand les ordinateurs se connectent à certains sites (autrement appelé drive-by downloads) via des kits d'exploits (les chercheurs pensent que le groupe a injecté du code malveillant sur le site php.net en 2013 pour attaquer les visiteurs) ; des faux e-mails avec des pièces jointes malveillantes à en-tête de la Banque centrale de la Fédération de Russie ; l'installation d'autres programmes malveillants en utilisant les services de botnets. « Les cybercriminels sont de mèche avec plusieurs propriétaires de botnets pour diffuser massivement leurs programmes malveillants », ont expliqué les chercheurs de Group-IB. « Ils achètent aux propriétaires de botnets des informations sur les adresses IP des ordinateurs sur lesquels il y a déjà des logiciels malveillants contrôlés par le botnet et ils vérifient si les adresses IP appartiennent à des institutions financières ou gouvernementales. Si le malware du botnet se trouve dans les plages d'adresses que le groupe veut cibler, ils paient le propriétaire du réseau de zombies pour qu'il diffuse leur logiciel malveillant ».

Le vol de données de cartes de crédit confirmé
Depuis le début du second trimestre 2014, le groupe Anunak a également ciblé des revendeurs aux États-Unis, en Australie et en Europe, l'objectif étant d'infecter les terminaux points de vente avec leurs logiciels malveillants et de voler des données de cartes de paiement au moment des transactions. « Plus d'une quinzaine de violations potentielles ont été identifiées, dont une douzaine aux États-Unis, et le vol de données de cartes de crédit a été confirmé dans trois de ces cas », ont déclaré les chercheurs dans leur rapport. Le groupe a également compromis les ordinateurs de trois entreprises du secteur des relations publiques et des médias basées aux États-Unis. « Ils cherchaient peut-être des informations qu'ils pouvaient exploiter sur le marché boursier », ont déclaré les chercheurs. « Nous n'avons aucune preuve du piratage de banques en Europe occidentale ou aux États-Unis, mais les attaquants peuvent très bien utiliser les mêmes méthodes pour cibler des banques hors de Russie », ont mis en garde les chercheurs.

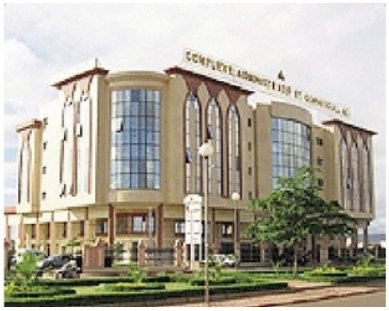
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cybercriminels-derobent-25m$-a-des-banques-russes-59699.html
Par Jean Elyan

Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

	Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

Ils sont de plus en plus jeunes et stupides puisque incapables d'évaluer les risques liés à l'objet de leurs forfaits. Avec la création de la cellule de lutte contre la cybercriminalité, nombre d'entre eux apprennent désormais à leurs dépens que certains actes ne restent jamais impunis.



Les faits remontent au lundi 15 septembre 2014 dans la zone ACI, une cité résidentielle censée pourtant être sous surveillance accrue au regard de ses occupants, pour la plupart, des ressortissants étrangers (missions diplomatiques, organisations internationales, etc.). Mais qu'importe pour les malfrats désormais regaillardis par les nombreuses failles du dispositif sécuritaire dans la capitale et surtout, par des décisions pour le moins controversées des plus hautes autorités de la République.
C'est donc en plein jour, aux environs de 14 heures dans la zone indiquée que trois individus armés ont envahi un magasin de vente de téléphones portables de grandes valeurs et autres accessoirs electroniques dont des clés USB, des chargeurs, des puces, cartes mémoires, etc.
Les deux premiers tinrent la gérante en joue pendant que le troisième dévalisait litteralement la boutique. Ils purent ainsi emporter des appareils d'une valeur marchande de plusieurs dizaines de milliers de nos francs ainsi que la somme de 35.000 F CFA en espèces. Et ils repartirent sans être inquietés. Mission accomplie? Loin s'en fallait !

La victime décida de porter plainte contre X au niveau de la Brigade d'Investigation judiciaire (BIJ) et, naturellement, la nature des objets volés aidant, l'affaire fut confiée à la Cellule de lutte contre la Cybercriminalité dirigée par l'Inspecteur divisionnaire Papa Mambi Keïta surnommé « l'Epervier du Mandé». Commença alors la cyber-traque !

Nous ne cesserons jamais de le dire: les objets électroniques sont de véritables traîtres. Ils sont susceptibles de tout révéler sur leurs propres utilisateurs. Et le saviez-vous ? Il est même possible d'ouvrir le micro de certains téléphones à distances. Quant aux puces, cartes mémoires ou clés USB, elles peuvent être également activées de loin. A ce stade, certains commentateurs comparent déjà notre époque à celle décrite par l'auteur de roman de science fiction, Georges Orwell dans «1984» avec le fameux « Big Brother » désormais présent dans la légende contemporainne*.
Naturellement, ces méthodes de surveillance necessitent des équipements adéquats, une collboration accrue des services techniques et surtout, une bonne dose d'intelligence; un aspect de la question qui ne fait nullement défaut au niveau de la cellule de lutte contre la cybercriminalité.

Mettant ainsi toutes ces aptitudes à contribtion, les enquêteurs parvinrent à identifier un nommé Souleymane Doumbia comme utilisateur d'un des objets volés. Il fut interpellé dans les heures qui suivront et sa victime l'identifia formellement comme étant un de ses agresseurs. Il était inutile de nier les faits. Mais comment diantre les enquêteurs sont-ils parvenus jusqu'à lui ? C'est bien la question qu'il se pose encore à l'heure actuelle. Difficile de trouver réponse à cette intérrogation. Et pour cause, « Big Brother » est passé par là. Ses complices, quant eux, attendent à leur tour d'être arrêtés. Une question de jours.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://maliactu.net/mali-arrestation-de-braqueurs-dans-la-zone-aci-big-brother-est-passe-par-la/

Copier les données de son entreprise pour son propre compte, c’est risqué !

Copier les données de son entreprise pour son propre compte, c’est risqué !

Fin octobre, la Cour de cassation a rejeté le pourvoi d’un salarié qui avait été condamné en appel pour avoir copié pour son propre compte plus de 300 documents confidentiels de l’entreprise qu’il quittait pour un concurrent.

Les documents étaient protégés par une charte de confidentialité signée par tous les salariés, dont le plaignant, onze ans plus tôt. Après 16 années passées dans la société, l’homme avait informé son employeur, un cabinet de courtage d’assurance, de son intention de démissionner de son emploi de chargé de clientèle en vue de rejoindre un autre cabinet de courtage. Un élément contextuel de nature qui permet également de mieux comprendre les décisions de première instance et d’appel.
Il avait ensuite extrait des données de son poste de travail à l’aide de « treize supports externes » et « en expédiant de son poste professionnel et à destination de sa messagerie électronique privée une multitude de fichiers numériques confidentiels ».

Fond documentaire personnel ?
Il avait admis suite à cela vouloir alimenter un fonds documentaire personnel, mentionnant qu’une partie des données copiées avaient été produites par lui même. Le plaignant également avait reproché à la Cour d’appel de ne pas avoir pris en compte le fait que les informations détournées n’avaient pas été diffusées auprès de tiers. Ces arguments ont été jugés irrecevables.
Dans son arrêt, la Cour de cassation a estimé que l’abus de confiance était caractérisé puisque « le prévenu a[vait], en connaissance de cause, détourné en les démultipliant, pour son usage personnel, au préjudice de son employeur des fichiers informatiques ».
Au terme des différentes procédures, le plaignant à été condamné à verser 12 500 euros à la partie adverse.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/justice-copier-des-donnees-du-si-pour-sa-pomme-c-est-risque-39810871.htm