Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

	Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

Lorsque des institutions gouvernementales ou des entreprises souhaitent stocker des informations confidentielles, elles utilisent le plus souvent un réseau en « air-wall », déconnecté d'internet, et isolé de toute connexion extérieure. Récemment pourtant, plusieurs chercheurs de l'université Ben-Gurion en Israël ont démontré qu'il était possible, une fois ce réseau contaminé par un virus spécifique, d'en récolter les données.

Les pirates informatiques peuvent voler les données de votre ordinateur même s'il est déconnecté et éteint.
Atlantico : Bien que les particuliers soient sans doute moins la cible de ce type d'attaque informatique, sont-ils tout aussi vulnérables ?
Michel Nesterenko : Tout ordinateur est potentiellement vulnérable. Mais les connaissances et la technologie nécessaire pour réussir un tel vol de données font que seules les ordinateurs dans lesquels sont stockés des données stratégiques ou des données commerciales de grande valeur sont vraiment à risque. Donc le consommateur normal n'a pas de grand souci à se faire.
Du temps de la Guerre Froide dans les années 60 les espions américains et russes pouvaient voler toutes les informations passant sur l'écran d'un ordinateur à partir du van stationné dans la rue.
C'est pour cela que certains ministères à Washington avaient blindés l'enveloppe extérieure des ordinateurs détenant des données sensibles de façon à empêcher toute émanation électromagnétique.

Jean-Paul Pinte : En tant que particulier, nous sommes encore plus vulnérables à ce type d'attaque ou d'infiltration qui, une fois installé sur une machine, permet d'y revenir et de se servir. Nous avons en effet moins pensé la sécurité de nos données par rapport à une entreprise par exemple, mais le risque demeure le même, il est même plus grand. Le ver installé sur un PC, il est en effet possible de faire ce que l'on veut, de s'installer confortablement et d'y revenir à sa guise. Une des seules façon de pirater un PC éteint serait d'être en rapport avec la C-MOS et nécessiterait donc un accès physique à la machine. Ce n'est donc à la portée du premier venu.
Comme pour votre Webcam éteinte, il est tout aussi possible d'en prendre la main à distance et certains vont même jusqu'à utiliser un cache ou collant qu'ils posent sur la Webcam pour s'en protéger. Un ordinateur quand il est éteint, c'est juste la boite d'alimentation qui est éteinte mais la carte mère continue à recevoir de l'énergie (un voyant lumineux au niveau de la carte mère est toujours présent). Il est donc toujours plus prudent de débrancher totalement son ordinateur et surtout de ne pas le laisser en mode veille ou veille prolongée. Il est également possible si l'on veut se protéger totalement de fermer son boîtier Wifi mais attention aux mises à jour qui se font parfois la nuit sur ces matériels.

Quelles données peuvent être récupérées ? Quelles sont les marges de manoeuvre des pirates informatiques avec pareil procédé ?
Michel Nesterenko : Potentiellement tout peut être récupéré à terme car le vol des données prends du temps, compte tenu des limitations de la bande passante. Ce type de procédé est fort utile dans un contexte militaire ou d'espionnage industriel. Les informations peuvent être revendues aux concurrents ou utilisées dans des manipulations boursières par exemple.

Jean-Paul Pinte : Une fois dans la machine, on peut tout faire avec quelques manipulations que connaissent bien ces hackers. A la base il y a quelques années, le but était simplement d'avoir pu infiltrer ou craquer une machine.
Aujourd'hui, ce sont tous vos contacts de messagerie, les fichiers stockés, les mots de passe qui peuvent être récupérés par exemple au même titre que tous les documents personnels. Il n'y a donc pas de limites.
Tous ces éléments pourraient se retrouver un jour sur la toile et servir par exemple dans le cas d'adresses de messagerie à des banques de données réutilisées par la suite pour faire des envois en masse comme cela se pratique dans le cas des mails nigérian.
Prendre la main sur votre machine revient à avoir la clé de votre domicile, le code de votre alarme et tout peut alors être envisagé en vue de vous voler des informations et des accès à des sites que vous utilisez et sur lesquels vous passez des actes d'achat par exemple.
Aujourd'hui, on parle même de vol de données qui pourraient vous faire chanter.

Comment savoir si notre ordinateur est infecté par ce type de virus ? Comment s'en apercevoir ?
Michel Nesterenko : Pour tout virus connu, il existe un antidote. Encore faut il que les anti-virus et parre-feu soient mis à jour constamment sur chacun des ordinateurs du réseau indépendamment.

Jean-Paul Pinte : Assurez-vous tout d'abord d'avoir la bonne dernière version officielle de vos logiciels et pensez à utiliser des solutions comme Anti Hacks qui détectera les problèmes de configuration et les logiciels obsolètes sur votre machine et qui, surtout, se chargera de configurer automatiquement les logiciels et vous aidera à les mettre à jour.
Ensuite un anti-virus que vous mettrez à jour tous les jours et pas à la petite semaine comme le font la plupart d'entre nous (beaucoup utilisent celui offert pour une période donnée par le fournisseur du PC mais oublient de le changer ou de l'actualiser dans le temps se retrouvant alors sans protection).

En attendant :
• surveillez vos barres d'outils et les liens que vous n'auriez pas ajouté personnellement ;
• contrôlez votre pointeur de souris qui à certains moments se déplacerait de façon inatendue ;
• regardez l'adresse URL du site que vous consultez car il pourrait changer lors d'une transaction financière par exemple ;
• veillez aux fenêtres intempestives qui s'affichent sur votre PC sans que vous n'interveniez et aux pages qui s'installent en arrière plan et que vous ne découvrez qu'une fois que vous fermez votre session Internet ou machine. Elles pourraient bien être la source d'un début d'installation d'une cyber-surveillance ;
• enfin si tout va plus lentement sur votre ordinateur; pensez à contrôler les fichiers qui se lancent au démarrage et surtout n'oubliez pas que le meilleur anti-virus est parfois de remettre à plat tous les six mois votre PC.

Quel est le niveau d'informatique nécessaire pour mettre en oeuvre correctement cette pratique ? Des solutions simples sont-elles mises à la disposition des amateurs ?
Michel Nesterenko : Le Hacking de haut niveau n'est pas une activité pour amateurs. Il faut des connaissances certaines pour mettre au point le virus adapté a une attaque particulière de même qu'il faut des informations précises obtenues par une opération de reconnaissance informatique et physique pour trouver l'ordinateur cible. Il s'agit d'un travail pour des spécialistes.

Jean-Paul Pinte : Dès que ces cybercriminels ont réussi à installer un virus ou un cheval de Troie (souvent aussi nommé malware ou logiciel malveillant) votre ordinateur devient une source potentielle de revenus. Ils auront accès à toutes vos données personnelles (messages, mails, documents bancaires, mots de passe, photos, vidéos, …) stockées sur votre disque dur et pourront surveiller votre activité sur Internet et sur votre machine.
Aujourd'hui, pas besoin d'être un grand expert sur le sujet en dehors de quelques types d'infiltrations spécifiques sur des sites dits plus sécurisés. En effet, malheureusement, beaucoup d'aide est apportée aux cyberdélinquants par Internet.. Des solutions contenus dans certains forums permettent à des petites mains de se lancer tout d'abord dans le cadre d'arrêt d'une machine en réseau dans une entreprise. Petit à petit, pirates, hackers ou encore crackers découvrent les modes opératoires des plus grands pour se les approprier et pour aller plus loin comme s'il y avait un concours entre eux.
Comment s'en prémunir ? Doit-on se résigner à avoir un ordinateur vierge de toute connexion à internet, avec des protocoles de sécurité stricts, comme par exemple ne pas utiliser de clé usb étrangère ou ne pas prêter les siennes ?
Michel Nesterenko : Absolument. Éviter de connecter à internet un ordinateur détenant des données critiques et stratégiques est la première étape. Interdire l'utilisation de toute clé USB non cryptées avec des codes particuliers est une deuxième étape.
Ensuite, il faudra songer à installer un blindage autour de l'écran pour éviter toute émanation électromagnétique. Surtout, il ne faut jamais oublier de tenir à jour les anti-virus et parre-feu sur chaque ordinateur et crypter toutes les données résidant sur le disque dur.
Le nombre de situations où cela sera vraiment recommandé reste fort restreint. Pour l'écrasante majorité des utilisateurs, cela ne sera jamais nécessaire heureusement.
Jean-Paul Pinte : De plus en plus, il faudra apprendre à se protéger et à avoir une culture sécuritaire en ce qui concerne les materiels que nous utilisons et que nous connectons à notre PC car ils seront autant de sources et de moyens d'attaque pour ces délinquants.
Tout ce qui est installé, introduit et (télé)chargé sur nos machines doit faire l'objet d'une sorte de scan ou contrôle si l'on veut rester dans une protection plus sereine.
Nous en sommes loin aujourd'hui quand nous validons la mise à jour d'un logiciel sans être sûr que l'envoi émane de la société en question. Certains internautes ont découvert tardivement que des exécutables s'étaient installés sur leur PC mais n'ont pu en mesurer l'impact sur leurs données, logiciels, etc.
L'objectif premier du hacker va être d'installer un virus ou un cheval de Troie sur votre ordinateur. Il se présente simplement sous la forme d'un exécutable (par exemple .exe), soit installé suite à l'attaque d'un de vos logiciels mal configurés ou obsolètes (la version installée n'est pas la dernière et contient donc des failles de sécurité). Ces failles sont en général la conséquence d'un bug de programmation dans l'application qu'un hacker saura mettre à profit pour prendre le contrôle de votre ordinateur. Ces logiciels sont très nombreux en voici quelques uns à titre d'exemple :
– Microsoft Windows ;
– Les suites bureautiques (Microsoft Office, OpenOffice) ;
– Les navigateurs (Internet Explorer, Firefox, Chrome, Opera, Safari) ;
– Les logiciels multimedia (Acrobat Reader, Flash, Shockwave, Windows Media Player, Quicktime, RealPlayer, WinAmp, iTunes, VLC) ;
– Les messageries instantanées (Windows Messenger, Pidgin) ;
– Java.

On a pu ainsi découvrir des cas de figure où les PC des internautes sont devenus des serveurs à leur insu se voyant alors stocker à des jours et des heures des données de personnes malveillantes qu'ils ne pouvaient alors contrôler sur leur propre machine.
De même d'autres ont accepté avec trop de simplicité et de naïveté une clé USB offerte avant l'entrée dans un salon ou symposium. Le but étant de garder la clé mais pas son contenu, ils ont ouvert cette dernière sans penser à l'exécutable qui allait s'installer sur la machine et qui allait devenir un moyen d'infiltration sans limite pour l'offreur.
Certaines applications sur ces clés vont même pendant qu'un tiers tente de recopier un fichier à partir de votre machine scruter votre PC pour lui sous-tirer tous vos contacts et ce que vous pouvez imaginer avec sans vous garantir qu'il n'aura pas pris la main sur votre PC pour y revenir ultérieurement.

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

Source : http://www.atlantico.fr/rdv/minute-tech/pirates-capables-voler-donnees-meme-votre-ordinateur-est-pas-connecte-internet-michel-nesterenko-1893142.html

---

Cryptolocker : quand un virus prend vos données en otage

contre rançon

	**Cryptolocker : quand un virus prend vos données en otage contre rançon**

Depuis quelques jours, une campagne d'attaque utilisant CryptoLocker (logiciel malveillant de type cheval de Troie) semblerait être en cours. La société d'antivirus Trend Micro a été alertée par de nombreux appels et messages de la part de ses clients et partenaires. Loïc Guézo, évangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro et administrateur du Clusif, livre quelques pistes pour lutter contre ce ransomeware (logiciel malveillant prenant les données personnelles de l'utilisateur en otage) particulièrement nuisible.

Vous cliquez sur le lien d'un e-mail reçu. Le fond d'écran change. Une fenêtre s'ouvre. Un avis apparaît, vous informant que vos fichiers importants sont cryptés. Vous tentez de cliquer ailleurs. Impossible de quitter la fenêtre. L'écran est verrouillé. Un cauchemar nommé « Cryptolocker ».
Ce « ransomware » (ou rançongiciel) est un logiciel malveillant qui piège l'ordinateur de ses victimes et prend en otage leurs données personnelles. Il est précisé que le chiffrage des données du disque par le logiciel malveillant les rend inutilisables jusqu'au versement de la rançon demandée. Le pirate promet de fournir la clé capable de déchiffrer les données en échange d'une somme de quelques centaines d'euros, à régler en ligne via Paypal ou un virement en bitcoins. Le tout avec un compteur de temps bien visible, qui signifie que la décision doit être prise rapidement.
Bien sûr une clé unique est utilisée pour chaque machine piégée. Si la rançon demandée n'est pas versée dans le temps imparti, la clé de chiffrement ne sera pas communiquée et les données chiffrées définitivement perdues. Et si la rançon est payée, rien ne garantit pour autant la suite des opérations…
Ce scénario digne d'un thriller a fait son apparition fin 2013 et revient en force depuis quelques semaines. S'il est encore trop tôt pour connaître précisément le nombre de systèmes infectés par le programme malveillant, Le Monde Informatique du 6 janvier 2014 rapporte que Cryptolocker 2.0 aurait infecté 200 à 300 000 PC et qu'environ 0,4 % des victimes ont probablement payé la rançon réclamée, même si payer ne garantit absolument pas le déblocage du système.
Ce banditisme virtuel est basé sur un chantage avec comme otage les données de la victime. Il a été jugé suffisamment grave pour que des policiers, spécialement formés, enquêtent pour retrouver ces malfaiteurs du Net et les poursuivent. Des unités spéciales américaines et européennes ont, par exemple, travaillé ensemble et uni leurs efforts pour démanteler le 2 juin dernier le réseau criminel GameOver Zeus qui, entre autres, pouvait distribuer Cryptolocker.

L'INGÉNIERIE SOCIALE, VECTEUR DE L'INFECTION
Les malfaiteurs s'appuient sur des techniques d'ingénierie sociale. Ils procèdent à l'envoi initial de leurres sous forme de vagues d'e-mails ciblés. D'où l'importance de vérifier la légitimité de chaque message. Il convient de toujours faire preuve d'une extrême prudence lorsque nous ouvrons la pièce jointe à un message électronique dont la source nous est inconnue.
Ce sont principalement aujourd'hui les utilisateurs de PC qui sont visés (des versions visant les mobiles apparaissent déjà). Mais le point de départ est bien le geste de l'utilisateur lui-même, piégé par un message avec pièce jointe. L'hameçon psychologique est celui de l'inquiétude naturelle, de la surprise ou de l'intérêt du destinataire du message. Il peut s'agir de faux courriers paraissant provenir d'un organisme social, d'une banque, d'une assurance, d'e-commerçants, de logisticiens ou de transporteurs, etc. La pièce jointe est censée être un document lié à un litige, une facture impayée, un avis de livraison en suspens, un remboursement sur trop-perçu…
L'éducation et la vigilance des utilisateurs isolés sont donc indispensables. Sur un réseau d'entreprise, l'information d'alerte doit être donnée et pourra plus facilement être souvent répétée : « n'ouvrez pas les mails de provenance inconnue sans vérification, ne cliquez jamais sur un lien si vous avez le moindre doute », etc.

COMMENT SE DÉFENDRE ET PRÉVENIR LE BLOCAGE ?
Il existe plusieurs moyens pour gérer cette menace, tant pour les particuliers que pour les entreprises. Il a été largement démontré que la sécurité basée sur les signatures a atteint ses limites, mais il existe cependant d'autres solutions avec des fonctions d'alerte plus évoluées. Ce sont par exemple des solutions basées sur les éléments environnementaux (comme la réputation d'adresses IP, les noms de domaine…). Un service de réputation va en particulier permettre de bloquer l'accès à certaines adresses IP correspondant à des C&C de botnets, empêchant tout simplement le Cryptolocker de s'initialiser et donc de chiffrer la cible !
Revoir la politique de sécurité des pièces jointes est urgent pour de nombreuses entreprises. L'adoption des bonnes pratiques permettra d'éviter une contamination très rapide.
Posons-nous les bonnes questions pour contrer Cryptolocker. Est-ce que l'entreprise dispose bien d'une politique de blocage des pièces jointes aux messages, empêchant par exemple le déclenchement d'un fichier exécutable ? Peut-on analyser « en amont » le comportement des pièces jointes ? Utilise-t-on un service avancé de réputation ? Surveille-t-on le comportement des pièces jointes sur la durée? A-t-on simplement le moyen de contrôler que la solution de sécurité reste activée ? Ces quelques premières précautions permettront d'éviter les catastrophes, en particulier pour les PME.
Il faut bien sûr toujours être sur ses gardes, ne pas négliger de mettre à jour les logiciels de sécurité installés et vérifier que le navigateur utilise la réputation de sites Web avant de cliquer sur un lien ou bien utiliser un service gratuit comme Trend Micro Site Safety Center.
Quant aux grandes entreprises, qu'elles se préparent à recevoir des attaques type Cryptolocker mais désormais ciblées. Et bien sûr, toujours communiquer en interne sur les risques, et communiquer, c'est répéter…

LES SYSTÈMES INFORMATIQUES DOIVENT ÊTRE PRÉPARÉS POUR RÉSISTER
On ne soulignera jamais assez que la formation des utilisateurs, la mise à jour régulière des logiciels et de bonnes pratiques d'utilisation de l'ordinateur individuel restent le socle de défense contre Cryptolocker ou toutes les nouvelles menaces similaires. Il est désormais nécessaire d'introduire des outils d'analyses plus complets (vision en temps réel de la menace ou exécution en environnement contrôlé – sandboxing – par exemple).
Si les cybercriminels perfectionnent chaque jour leurs logiciels malveillants qui deviennent ainsi de plus en plus sophistiqués, alors les systèmes informatiques doivent également être préparés pour résister mais surtout être cyber-résilients face à ces attaques. Cette lutte doit être globale pour non seulement réduire le taux de l'infection, mais également briser la chaîne de transmission des logiciels malveillants par une stratégie de défense en profondeur, y compris lors de son déroulement.
L'autre aspect fondamental reste la lutte policière et judiciaire contre ces nouvelles formes de criminalité dont les dernières semaines ont montré l'ampleur et le dynamisme.

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

Source : http://www.usine-digitale.fr/article/cryptolocker-quand-un-virus-prend-vos-donnees-en-otage-contre-rancon.N302748
par Loïc Guézo, Evangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro & Administrateur du Clusif

---

Fichiers pédopornographiques: un habitant de Peille arrêté

Fichiers pédopornographiques: un habitant de Peille arrêté

Un jeune homme de 21 ans, menuisier, inconnu de la justice, a été interpellé par le groupe « cybercriminalité », de la police judiciaire de Nice. Il est soupçonné d'avoir téléchargé pendant un an des centaines de fichiers (images et vidéos) de viols d'enfants.

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

Source : http://www.monacomatin.mc/nice/fichiers-pedopornographiques-un-habitant-de-peille-arrete.2023663.html

---

Une charte pour protéger les données personnelles

Une charte pour protéger les données personnelles

«l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Atlanta se positionne en protecteur des données personnelles. En effet, à l'occasion de la Journée mondiale des droits de l'Homme, la compagnie d'assurances a publié une charte régissant la protection des données personnelles de ses partenaires et ses clients. Ayant l'ambition d'être reconnu par ses clients, ses collaborateurs et ses partenaires comme «l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Un document qui matérialise les engagements de la compagnie envers ses clients et décrit les modalités suivant lesquelles la compagnie collecte et utilise les données personnelles de ses clients.
Affichée en interne, chez tous les agents et dans son site web, cette charte est en parfaite conformité avec la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

La publication de cette charte intervient suite à une large mise à niveau de l'ensemble des standards et procédures de la compagnie qui, par ailleurs, a reçu de la part de la Commission nationale de contrôle de protection des données à caractère personnel (CNDP) l'autorisation de traitement des données concernant les process opérationnels.

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

Source : http://www.aujourdhui.ma/une/actualite/atlanta-une-charte-pour-proteger-les-donnees-personnelles-115014#.VIyAT9KG92o
Par ALM

Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

Kaspersky Lab prédit des attaques persistantes plus furtives et ultra ciblées

Les experts de l'éditeur de logiciels de sécurité informatique ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT (Advanced Persistent Threat ; Menaces persistantes avancées).

2015 sera l'année de la furtivité des cyber-menaces. © D.R.

Ces dernières années, Kaspersky Lab, un éditeur majeur de solutions de protection contre les cyber-attaques, a mis en lumière certaines des plus grosses campagnes d'attaques APT (Advanced Persistent Threats ; Menaces persistantes avancées), notamment RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/ The Mask et d'autres. Les experts de l'équipe de recherche du GReAT (Global Research et Analysis Team) de Kaspersky Lab ont surveillé plus de 60 acteurs responsables de cyber-attaques à travers le monde. En observant de près ces menaces, Kaspersky Lab a pu dégager une liste des menaces émergentes dans le monde des APT.

Fragmentation des plus gros groupes APT

En 2015 il faudra s'attendre à ce que les plus gros et les plus importants groupes d'attaques APT se divisent en plusieurs unités plus petites, opérant de manière indépendante. Cela entrainera une base d'attaque plus étendue et, donc, plus d'entreprises seront touchées du fait que chaque petit groupe diversifiera ses attaques. Dans le même temps, cela signifie que les plus grosses entreprises précédemment infectées par deux ou trois groupes APT majeurs (par ex. Comments Crew et Wekby) connaîtront plus d'attaques, provenant d'un panel de sources élargi.

La méthode APT sera utilisée pour un cyber-crime plus vaste

Pendant nombre d'années, les cybercriminels se sont focalisés exclusivement sur le vol d'argent de l'utilisateur final. Une explosion des taux de vols de cartes de crédit, de piratages des comptes de paiement électronique ou des connexions de banque en ligne ont causé aux consommateurs la perte de millions d'euros. Cependant les experts de Kaspersky Lab observent une tendance plus intéressante qui deviendra prééminente en 2015 : les attaques ciblant directement les banques et qui utiliseront des méthodes tout droit sorties des stratégies APT.

Les réseaux d'hôtels deviendront des cibles privilégiées.

Le Groupe Darkhotel est ainsi l'un des acteurs APT connus pour avoir ciblé des visiteurs particuliers durant leur séjour dans les hôtels de certains pays. Actuellement, les hôtels fournissent un excellent moyen de cibler une certaine catégorie de personnes, comme des dirigeants d'entreprise. Cibler les hôtels est également très lucratif car cela fournit des renseignements sur les mouvements d'individus importants dans le monde. En 2015, ce type d'attaques pourra se multiplier à plus grande échelle.

Evolution des techniques d'attaques.

Aujourd'hui, nous voyons déjà des groupes APT déployer constamment des malwares de plus en plus évolués pour des systèmes informatiques qui se complexifient constamment (comme Turla et Regin). En 2015, nous nous attendons à voir des implantations de malwares encore plus sophistiquées qui tenteront de déjouer encore plus efficacement les outils de détections des attaques.

Nouvelles méthodes d'exfiltration des données. Les jours où les attaquants activaient simplement une backdoor dans un réseau d'entreprise pour voler des téraoctets d'informations depuis les serveurs FTP dans le monde sont révolus. Aujourd'hui, des groupes plus sophistiqués ont recours aux SSL de manière régulière en plus des protocoles de communication personnalisés. En 2015, plus de groupes d'attaquants feront usage des services cloud afin de rendre l'exfiltration plus discrète et plus difficile à remarquer.

Utilisation de fausses bannières lors des attaques

Les attaquants commettent des erreurs. Dans la vaste majorité des cas analysés, nous observons des artefacts qui fournissent des indices sur le langage utilisé par les attaquants. Par exemple, dans le cas de RedOctober et d'Epic Turla, nous avons conclu que les attaquants parlaient probablement couramment le russe. Dans le cas de NetTraveler, nous avons abouti à la conclusion que les attaquants parlaient couramment chinois. Cependant les attaquants commencent à réagir à cette situation. En 2014, nous avons observé plusieurs opérations « fausses bannières» où les attaquants ont introduits des malwares inactifs communément utilisés par d'autres groupes APT. En 2015, avec la propension croissante des gouvernements à « nommer et pointer du doigt » les attaquants, les groupes APT vont prudemment ajuster leurs opérations et placer de fausses bannières dans la partie.

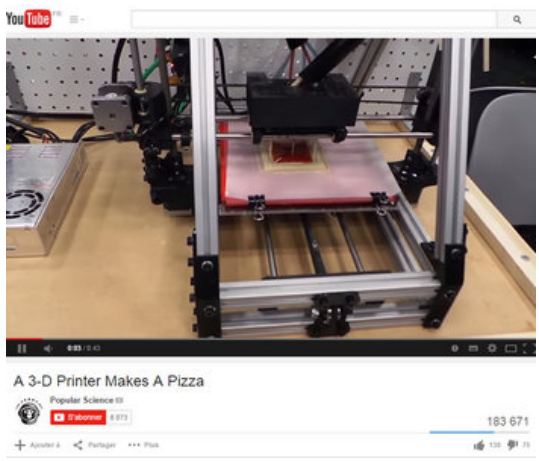
« Si nous pouvons qualifier l'année 2014 de 'sophistiquée', alors 2015 sera sous le signe de la 'furtivité'

Nous pensons que les groupes d'attaques APT évolueront pour devenir plus sournois et seront encore plus difficile à traquer. Cette année, nous avons déjà découvert des attaques APT utilisant les vulnérabilités dites « zéro day » ainsi que d'autres techniques plus persistantes et plus insidieuses encore. A partir de ces découvertes, nous avons développé et déployer de nouveaux outils de défense pour nos utilisateurs », explique Costin Raiu, directeur du GReAT de Kaspersky Lab.

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

Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-f344b63add3ab82ad1ae1f0fc9ae7dc8.htm par Erick Haehnsen

Une pizza fabriquée avec une imprimante 3D



Une pizza fabriquée avec une imprimante 3D

Alors qu'un voyage vers Mars prend au minimum six à neuf mois, la NASA a pensé aux pauvres astronautes américains privés de pizzas durant tout ce temps.

L'agence spatiale a octroyé 125 000 dollars (97 000 euros) à la compagnie SMRC pour développer une imprimante capable de fabriquer une pizza à partir de différentes « cartouches » d'ingrédients. Un prototype a été présenté en octobre 2013 sur le salon South by Southwest Eco à Austin au Texas.

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

Source : http://www.journaldunet.com/economie/magazine/creations-en-3d/pizza.shtml

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

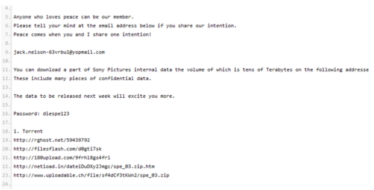
Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

Imaginez que toutes les données – ou presque – qui transitent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de térabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en plus probable.
Les documents internes de Sony Pictures publiés (fichiers Excel, Word, Powerpoint, PDF, etc.) se comptent déjà par centaines de milliers et en dizaine de gigaoctets, selon un décompte fiable établi par l'entreprise spécialisée en sécurité informatique Risk Based Security.
Le processus de diffusion est toujours le même. Des liens permettant de télécharger des fichiers RAR ou ZIP volumineux, par des sites de téléchargement direct ou grâce à des fichiers torrent, apparaissent sur l'éditeur de texte en ligne Pastebin, qui assure un certain anonymat à leurs auteurs. Les hackers envoient ensuite le lien du document Pastebin par e-mails à leurs contacts, soit n'importe qui ayant signifié son intérêt pour les documents Sony Pictures en écrivant aux adresses anonymes et temporaires que les membre de GOP diffusent régulièrement (journalistes, sympathisants des hackers, entreprises de sécurité informatique, enquêteurs, concurrents…).


Anyone who loves peace can be our member.
Please tell your mind at the email address below if you share our intention.
Peace comes when you and I share one intention!

jack.nelson-63vrbu1@yopmail.com

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresse
These include many pieces of confidential data.

The data to be released next week will excite you more.

Password: diespe123

1. Torrent
http://rghost.net/59439792
http://filesflash.com/d0gti7sk
http://180upload.com/9frhl8gs4frl
http://netload.in/dateiDuDXy2Jmgc/spe_03.zip.htm
http://www.uploadable.ch/file/sf4dCf3tKWn2/spe_03.zip

Extrait d'un message donnant accès aux fichiers volés à Sony Pictures Entertainment. | Pastebin

Les données sont ensuite accessibles pendant quelques heures, avant la désactivation des liens de téléchargement par les hébergeurs et la suppression du document Pastebin – vraisemblablement sur requête des autorités ou de représentants légaux de Sony. Entre le 24 novembre et le 10 décembre, six « livraisons » de ce type ont eu lieu. Les pirates, maniant le sens du teasing, en promettent à chaque fois davantage : « les données que nous publierons la semaine prochaine vous exciteront encore plus », annonçait par exemple un document Pastebin publié le 5 décembre.

Un chantage pécuniaire ?

Les textes diffusés par les hackers qui accompagnent la publication de ces fichiers n'en disent en revanche que peu sur les motivations réelles justifiant cette fuite massive et organisée. La piste de la Corée du Nord, qui agirait en représailles au film The Interview parodiant le régime de Kim Jong-un, est accréditée par des similarités constatées entre l'attaque du 24 novembre et celle subie par la Corée du Sud en 2013. Mais l'un des cadres du FBI, officiellement chargé de l'enquête, a confié le 9 décembre qu'il n'était pour l'instant pas possible d'en attribuer la responsabilité à Pyongyang.
Dans un document publié le même jour, les membres proclamés des GOP demandent bien à Sony d'« arrêter immédiatement de diffuser un film sur le terrorisme qui peut mettre fin à la paix régionale et causer une guerre », sans nommer le film en question, et reprenant une rhétorique déjà servie auparavant à The Verge. Mais ils signalent également avoir « formulé une demande claire à l'équipe dirigeante de Sony », encore une fois sans préciser laquelle :

« Ils ont refusé de l'accepter. On dirait que vous pensez que tout se passera bien, si vous trouvez les attaquants et ne réagissez pas à notre demande. Nous vous avertissons à nouveau. Répondez à ce que nous vous demandons si vous voulez nous échapper. »

De quoi donner du crédit à l'hypothèse d'une tentative d'extorsion de fonds de la part des hackers de « Guardian of Peace ». Ce motif a d'ailleurs été clairement exposé dans un e-mail envoyé aux dirigeants de Sony Pictures quelques jours avant l'attaque : « Nous avons de quoi causer beaucoup de tort à Sony Pictures. (…) Nous voulons une compensation monétaire. Payez, ou Sony Pictures sera frappé dans son ensemble. »

La diffusion au compte-gouttes des documents confidentiels constituerait, dans ce contexte, un moyen de pression supplémentaire pour obtenir cette « compensation », de nature à alimenter un feuilleton médiatique dévastateur pour Sony Pictures. Les médias du monde entier ont ainsi repris :

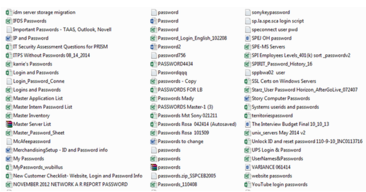
Les données privées de célébrités

Des adresses postales, des numéros de téléphone, des adresses électroniques, ou encore le numéro de sécurité sociale de Sylvester Stallone, contenus dans les documents liés aux films et séries de Sony Pictures ont été rendus publics. Parmi ces informations, on trouve les pseudonymes utilisés par Tom Hanks, Natalie Portman ou encore Ice Cube pour conserver un peu de tranquillité (lors d'une réservation d'hôtel par exemple).
Ont également été publiés une cote de popularité des acteurs pays par pays, ou encore les sommes d'argent perçues par Seth Rogen et James Franco pour le film The Interview. Le premier aurait reçu 8,4 millions de dollars pour avoir coréalisé et interprété l'un des rôles principaux, le second 6,5 millions : des divulgations auxquelles ils ont réagi avec humour.


L'affiche de « The Interview ». | Sony Pictures

Les données privées des salariés et partenaires de Sony Pictures

Numéros de téléphone, CV, photos d'identité, montants de salaires, demandes d'augmentation, e-mails, planning de vacances, factures médicales… Autant d'éléments propres à la vie interne d'une structure qui emploie près de 7 000 personnes aux Etats-Unis, et qui a collaboré avec de très nombreuses personnes ces dernières années – stagiaires, prestataires ou partenaires directs au sein d'entreprises rachetées par Sony, comme Columbia Pictures. Ces détails apparaissent notamment dans un dossier intitulé « Ressources humaines », et se trouvent aussi dans des documents de travail liés aux tournages de films et de séries Sony.
Encore plus grave, de très nombreux mots de passe utilisés par les employés pour se connecter à tous types de services (propres à Sony Pictures, mais aussi ailleurs sur Internet) font partie des publications. Comme le note cruellement Gizmodo, ils étaient stockés sur les disques durs de Sony Pictures dans des fichiers Word et Excel sans protection, et dans un dossier appelé « Mot de passe ».



Les mots de passes de Sony Pictures. | Risk Biaised Security

De quoi pousser d'anciens employés à réfléchir à une plainte collective, arguant du manque flagrant de sécurité du réseau de l'entreprise. « Il y a des raisons de penser qu'il y a eu une grosse négligence de la part de [Sony Pictures]. Nous nous inquiétons tous concernant notre vie privée, et nos familles », a déclaré l'un d'entre eux à Fox News, après avoir vu diffuser son passeport, son visa, son numéro de sécurité sociale et ses contrats passés avec l'entreprise.
Des avocats californiens incitent également les salariés actuels à se lancer dans de telles procédures. Particulièrement exposés, ils se sont vus en plus directement menacés dans un e-mail leur étant adressé. « Tout le monde panique, et personne ne sait quoi faire », a témoigné l'un d'eux sur le site Fusion, décrivant une hostilité grandissante au sein de Sony Pictures à l'encontre du service informatique. Le FBI, chargé de l'enquête, devrait faire le point devant les employés sur le comportement à adopter face à cette situation le 12 décembre.
Les dirigeants de Sony Pictures ne sont pas épargnés. L'un des premiers documents diffusés par le site d'information Fusion dresse le détail des rémunérations des 17 salariés les mieux payés, à commencer par le dirigeant Michael Lynton (3 millions de dollars par an) – une seule femme dans ce palmarès. Parmi les fichiers publiés figurent des sauvegardes de plusieurs mois de conversations par courriels (professionnels et personnels) issues des messageries Outlook de cadres de l'entreprise : Amy Pascal, vice-présidente de Sony Pictures, Steve Mosko, à la tête de Sony Television, ou encore Leah Weill, conseiller juridique en chef.

Des révélations sur les films et les séries Sony

Dans son ensemble, cette masse de données fourmille d'informations sur la manière dont Sony Pictures gère son catalogue, ses productions et ses projets. Finances de l'entreprise, projets marketing, bilans comptables liés aux séries diffusées à la télévision américaine, rétrospectives annuelles, bases de contacts, documents préparatoires pour des négociations… Ces milliers de fichiers bruts s'accompagnent de visées stratégiques, comme en témoignent les points de vue exprimés par des employés (s'énervant par exemple contre l'omniprésence d'Adam Sandler à l'écran).
Dans ces documents se nichent ainsi, fatalement, des informations propres aux films et aux séries télévisées estampillées Sony. On y apprend par exemple comment les dirigeants de Sony Pictures ont fait modifier la fin du film The Interview (attention spoiler !), et négocié avec Marvel, qui souhaitait que Spiderman apparaisse dans le prochain Captain America. Plus problématique, des scripts inédits d'épisodes de séries, et même de films devant sortir en 2015, ont été repérés.
Plusieurs médias, comme le Wall Street Journal, ont également extrait diverses phrases chocs des e-mails échangés ces dernières années par la vice-présidente Amy Pascal avec le tout-Hollywood (réalisateurs, agents, stars, etc.). On y trouve quelques commentaires désobligeants sur des acteurs : Angelina Jolie et son « ego devastateur » en prennent pour leur grade. Ou encore, une chronique détaillée des négociations et conversations, parfois brutes de décoffrage, entourant le biopic sur Steve Jobs sur lequel Sony travaille depuis trois ans (notamment sur les choix de casting du scénariste Aaron Sorkin, qui avait songé à Tom Cruise pour incarner le fondateur d'Apple).

En savoir plus sur http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html#Ox8W3PwS6l8JJu0T.99
Par Michaël Szadkowski journaliste à Pixels

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

Source : http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html
par Par Michaël Szadkowski

Droit à l’oubli pour les entreprises, plus qu’une idée…

	Droit à l’oubli pour les entreprises, plus qu’une idée…

Au nom du principe de la protection de la vie privée, une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles.

Dis-moi comment te référence Google, je te dirai qui tu es… ou pas. Car parfois, la révélation est rude, humiliante, voire dégradante, de celle que l'on voudrait effacer. Mais Internet possède malheureusement une très bonne mémoire, vive et éternelle. Pourtant, le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) a joué les hypnotiseurs : « Oubliez ! Je le veux », a-t-elle dit en substance aux moteurs de recherche. Une décision historique – ont estimé les commentateurs –, instaurant un « droit à l'oubli ». Mais est-ce vraiment sûr ? A y regarder de près la décision n'a qu'une portée limitée. Entre le moteur de recherche et l'internaute, désormais, c'est un peu « je t'oublie, moi non plus ». Parce que ce « droit à l'oubli » existe depuis… 1995.
C'est au nom du principe de la protection de la vie privée qu'une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles. La Cour de justice a souligné ce point au début de son arrêt, plaçant sa décision sous le signe de la sauvegarde des droits fondamentaux. « La CJUE a décidé que l'exploitant du moteur de recherche est tenu de supprimer, sur demande, les liens vers des pages Web, à condition que la démarche de l'internaute soit justifiée. L'arrêt n'instaure pas cependant un "droit à l'effacement des données", mais un "droit à la désindexation" : les liens perdurent, notamment à partir du site américain Google.com, accessible à un internaute européen », explique Olivier Cousi, avocat et associé du cabinet Gide, expert en droit de la propriété intellectuelle.

Zones grises
En outre, si la protection des données est encore imparfaite pour les particuliers, elle est inexistante pour l'entreprise. En effet, la protection comme l'entend l'arrêt de la CJUE ne concerne que les personnes physiques. Alors comment l'entreprise peut-elle gérer son e-réputation ? Quelle démarche pour contrer l'information fausse ou malveillante la concernant ? Autre sujet : cette absence d'intimité, renforcée en France par l'absence de secret des affaires, donne peu d'armes à l'entreprise pour contrer la diffusion de données confidentielles – procès-verbaux de conseil d'administration, chiffre d'affaires… C'est une des zones grises du droit à l'information qui protège également, c'est le bon côté de la médaille, d'une entreprise qui voudrait réécrire son histoire. Pour le reste, il faudra utiliser le bon vieux droit de la presse (diffamation) ou dénoncer la concurrence déloyale pour essayer de se défendre.
Un espoir quand même, un projet de règlement européen, qui doit être adopté « au plus tard en 2015 » par la France et l'Allemagne devrait venir réformer la directive de 1995. Il recommanderait un réel effacement des données et pourrait étendre la protection des données personnelles à certaines informations concernant les entreprises.

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

Source : http://www.lesechos.fr/enjeux/les-plus-denjeux/idees/0203967538313-pas-encore-de-droit-a-loubli-pour-lentreprise-1074046.php
par Valérie de Senneville

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

Quand la vidéosurveillance européenne contrarie la vidéoprotection française

L'arrêt rendu ce matin par la Cour de Justice de l'Union européenne en matière de vidéosurveillance risque d'avoir de douloureux effets en France. Il remet en effet en cause les efforts du ministère de l'Intérieur pour se passer de la CNIL dans l'installation des caméras de « vidéoprotection. »

Les faits examinés par la CJUE visait le cas d'un Tchèque ayant installé une caméra de surveillance chez lui, mais dont le champ de vision débordait sur la voie publique. Les flux étaient stockés sur disque dur, chez lui. Par ce biais, ce particulier avait finalement permis à la police d'identifier une personne suspectée d'avoir caillassé les fenêtres de sa maison. Cependant, la CNIL locale lui a infligé une amende, faute pour ce particulier d'avoir zappé le consentement préalable des personnes filmées. On pourra revoir notre actualité sur les solutions proposées par la Cour, mais l'important n'est peut-être pas là car l'arrêt est supposé provoquer un vent de panique en France, au ministère de l'Intérieur. Explication.

Vidéosurveillance, donnée personnelle, traitement automatisé

La Cour a en effet posé qu'en principe la vidéosurveillance relevait du champ d'application de la directive de 1995 sur les données personnelles, du moins « dans la mesure où elle constitue un traitement automatisé ». Cette analyse fait suite à un développement très logique :
La donnée personnelle embrasse « toute information concernant une personne physique identifiée ou identifiable. »
Est réputée identifiable « une personne qui peut être identifiée, directement ou indirectement, notamment par référence […] à un ou plusieurs éléments spécifiques, propres à son identité physique.»
Du coup, « l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel (…) dans la mesure où elle permet d'identifier la personne concernée ». En clair, une caméra de vidéoprotection capte donc des données à caractère personnelles quand les personnes filmées sont identifiées ou identifiables.
Mais y a t-il pour autant traitement automatisé de ces données ? La directive de 95 définit ce traitement par « toute opération ou [tout] ensemble d'opérations […] appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement […] la conservation ». La CJUE considère donc qu' « une surveillance effectuée par un enregistrement vidéo des personnes (…) stocké dans un dispositif d'enregistrement continu, à savoir le disque dur, constitue (…) un traitement de données à caractère personnel automatisé. »

Fort de ces enseignements, auscultons le régime français.

Les contrariété du régime français de la « vidéoprotection »
Une circulaire du 14 septembre 2011 décrit le cadre juridique applicable à l'installation de caméras de vidéoprotection, terme officiel pour repeindre de manière plus sympathique les outils de vidéosurveillance. Cette circulaire est importante puisqu'elle définit les (rares) cas où les autorités doivent effectuer une déclaration préalable auprès de la CNIL, et quand elles peuvent (très souvent) s'en passer.
Deux hypothèses sont envisagées par cette circulaire qui vient faciliter l'application du Code de la sécurité intérieure : des caméras installées sur la voie publique, des caméras installées sur des lieux non ouverts au public.

Les caméras installées sur la voie publique

Les caméras installées sur la voie publique (et dans des lieux ou établissements ouverts au public) nécessitent l'autorisation préalable du préfet après avis de la commission départementale de la vidéo protection. Donc sans passer par la CNIL.
Cependant, parfois, ce passage CNIL est nécessaire. Le ministère de l'Intérieur, épaulée par un avis du Conseil d'État (non public et concernant les caméras dans les prisons) l'estime inévitable seulement « si les traitements automatisés ou les fichiers dans lesquels les images sont utilisées sont organisés de manière à permettre, par eux-mêmes, l'identification des personnes physiques, du fait des fonctionnalités qu'ils comportent (reconnaissance faciale notamment). »
Décodons : en France, lorsque le flux permet l'identification via un système de reconnaissance faciale (ou de plaque d'immatriculation), il faut passer par la CNIL. L'Intérieur en déduit naturellement que « le seul fait que les images issues de la vidéoprotection puissent être rapprochées, de manière non automatisée, des données à caractère personnel contenues dans un fichier ou dans un traitement automatisé tiers (par exemple, la comparaison d'images enregistrées et de la photographie d'une personne figurant dans un fichier nominatif tiers) ne justifie pas que la CNIL soit saisie préalablement à l'installation du dispositif de vidéoprotection lui-même. »

On le voit, ce point est en exacte contradiction avec ce que vient de juger la CJUE : des personnes, une caméra, un flux, un stockage, nous voilà déjà plongé jusqu'au cou en Europe dans le règne du traitement automatisé de données personnelles. La France, pourtant un État membre, estime qu'il n'y a pas de traitement automatisé (donc pas de passage par la CNIL) faute de flux couplé à une reconnaissance faciale ou de plaque d'immatriculation. Un critère totalement surabondant !

Les caméras installées dans les lieux non ouverts au public

La circulaire précitée évoque aussi les caméras installées dans les lieux non ouverts au public (soit partout ailleurs que les voies publiques, la résidence privée ou la voiture). Ce régime n'est pas de la compétence de l'Intérieur, mais celui-ci donne malgré tout des pistes : il faut là encore l'avis de la CNIL « lorsque ces personnes sont identifiables ».

La Place Beauvau pose ici deux critères cumulatifs :
D'une part des images qui font l'objet d'un enregistrement et d'une conservation, et non d'un simple visionnage.
D'autre part, une identification possible parce que le lieu est fréquenté par des personnes « dont une partie significative est connue du responsable du système de vidéoprotection ou des personnes ayant vocation à visionner les images enregistrées. »

Cependant, ces deux critères ne se retrouvent pas dans les textes fondateurs :
Si la captation n'est pas un traitement selon l'Intérieur, la loi de 1978 tout comme la directive disposent que la collecte et la transmission le sont bien.
Le critère de la « connaissance » des personnes filmées par celui derrière la caméra est quelque peu restrictif : une reconnaissance indirecte est normalement suffisante, d'autant que même si personne ne peut identifier Mme Michu sur son écran de contrôle, elle aura son image et pourra le faire par la suite.

Enfin, le critère de la « partie significative » n'est pas intégré dans les textes socles.
Bref, l'arrêt rendu ce matin par la CJUE devrait naturellement amener la CNIL à se pencher plus en profondeur sur le régime français, et l'Intérieur à revoir le périmètre de ses yeux électroniques. D'autres actualités seront à suivre en fonction des retours obtenus auprès de ces deux acteurs.

Consultez l'arrêt de la Cour de Justice de l'Union Européenne de l'affaire C-212/13

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

Source : http://www.nextinpact.com/news/91367-quand-videosurveillance-europeenne-contrarie-videoprotection-francaise.htm#/page/1
par Marc Rees

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

Parallèlement aux grands dossiers à caractère géopolitique, la World Policy Conference, dont les travaux de sa septième édition viennent de s'achever à Séoul, a planché sur un problème lié à un autre genre d'actualité : l'émergence du Big Data et ses conséquences économiques et politiques.

La situation actuelle au Moyen-Orient ainsi que la place grandissante qu'occupe l'Asie dans le nouvel ordre mondial – dossiers liés à l'actualité internationale – ont été au centre de la 7e édition de la World Policy Conference (WPC) qui s'est tenue du 8 au 10 décembre à Séoul (voir L'Orient-Le Jour des 8, 9 et 10 décembre). Mais parallèlement, et dans le but d'élargir le débat et d'étendre les échanges de connaissances à un champ plus large que la sphère purement politique, les congressistes réunis dans la capitale coréenne ont planché dans le même temps sur des thèmes à caractère sociétal en rapport avec le changement climatique, l'énergie, l'environnement, les défis que pose le phénomène de Big Data, sans compter les rapports agroalimentaires entre l'Asie et l'Afrique. Autant de sujets liés aussi à l'actualité, mais une actualité d'un autre genre. Celle qui concerne les populations dans le détail de leur vie quotidienne et qui influe sur leur niveau de vie.

Le développement exponentiel de la révolution numérique est à n'en point douter l'un des principaux domaines qui touche de près le citoyen lambda. À l'ouverture de la session consacrée aux conséquences économiques et politiques du Big Data, le modérateur du débat, Nicolas Barré, directeur adjoint du quotidien Les Échos, indiquait, en guise d'entrée en matière, qu'en l'an 2000, un quart des données dans le monde étaient sous forme numérique. Aujourd'hui, cette proportion est quasiment de 100 pour cent. Et dans ce bouleversement vertigineux, l'Asie joue un rôle central. C'est du moins ce qu'affirme Chang Due Whan, président d'un géant médiatique en Corée du Sud, le Mackyung Media Group, qui possède, notamment, un quotidien, qui tire à un million d'exemplaires, ainsi que quinze de chaînes de télévision.

Évoquant les circonstances de cette révolution du XXIe siècle, Chang Due Whan souligne que la plupart des nouvelles inventions dans le domaine numérique viennent d'Asie. Il en déduit que cette zone sera la force motrice du secteur des appareils numériques, tels que les smartphones ou les phablets (combinaison du téléphone et de la tablette). Le développement dans ce domaine est tellement rapide que nombre d'utilisateurs estiment déjà que le PC est devenu obsolète et qu'il est de plus en plus évincé par la nouvelle génération de téléphones portables. Et dans ce cadre, souligne Chang Due Whan, la nouvelle technologie 5G va accroître considérablement le flux d'informations.

C'est précisément sur ce plan qu'intervient le problème du Big Data, en ce sens qu'il représente la capacité d'avoir accès, d'analyser et d'exploiter la quantité gigantesque de données disponibles, ce qui implique la création et l'utilisation efficace des outils permettant l'exploitation des données versées sur le marché un peu partout dans le monde. « Le Big Data est le nouveau pétrole », affirme à cet égard Chang Due Whan.
Le rythme de l'expansion de ce secteur d'activité a été mis en évidence par Luc-François Salvador, président exécutif pour l'Asie-Pacifique du groupe Capgemini, qui affirme que 90 pour cent des données actuelles ont été créées ces deux dernières années, et ce volume de données disponibles double chaque année. Conséquence prévisible : de nouveaux outils sont créés pour analyser et exploiter ces data. À titre d'exemple, Google a mis en place un système de gestion des maladies de manière à prévoir les dates, ou plus précisément les périodes, auxquelles apparaissent les grippes dans une région déterminée. Autre exemple dans ce domaine : au Japon, des chercheurs planchent sur l'analyse des données que l'on peut tirer de la façon de… s'asseoir ! La manière de s'asseoir devient ainsi une sorte de « signature » propre à la personne considérée.

La protection des données
Cette accumulation des données, notamment personnelles, à un rythme exponentiel, ainsi que la capacité grandissante d'analyser et d'exploiter de telles informations posent, à l'évidence, le problème de la protection des données personnelles et les craintes d'un fâcheux impact qui pourrait se manifester au niveau de la liberté de l'individu. Plusieurs intervenants ont évidemment soulevé ce point précis lors du débat. M. Salavador a ainsi relevé que le Big Data permet d'enregistrer des progrès énormes au niveau du traitement de certaines maladies ou aussi dans les projets d'urbanisme, mais dans le même temps, il pose le problème de la protection des données personnelles, ce qui implique la nécessité de concevoir les moyens dont devrait bénéficier le citoyen pour s'assurer une protection adéquate face au Big Data.

Cette question a été soulevée par un expert et consultant américain, Ben Scott, qui a affirmé qu'il se profile à l'horizon, du fait de ce problème, une perte de confiance de la population dans les gouvernements et les pratiques démocratiques, et, surtout, dans les outils informatiques, ce qui risque de pousser les individus à hésiter de trop s'engager dans l'utilisation des nouveaux outils ou applications numériques.

Un professeur universitaire américain, Joseph Nye, a relevé dans ce cadre que la capacité de traitement des données double chaque deux mois, de sorte que les citoyens vivant dans des pays démocratiques finissent par exprimer leurs appréhensions concernant l'exploitation des données personnelles. Certes, certaines personnes soulignent qu'au nom de la sécurité, face aux menaces terroristes, notamment, elles sont disposées à sacrifier de leur liberté ou de leur confidentialité. Cela pose, relève Joseph Nye, le problème de l'absence, au stade actuel, de contre-pouvoirs dans ce domaine.

Le Big Data risque-t-il ainsi de rendre quelque peu réel le danger de l'émergence d'un Big Brother ? Intervenant dans le débat, le député israélien de gauche Meir Sheetrit a apporté une nuance dans la nature du danger qui plane à cet égard, soulignant que le Big Data n'est pas exclusivement contrôlé par les gouvernements, mais il est aussi contrôlé et exploité surtout par les grandes entreprises, d'où la nécessité de protéger également les populations contre certaines grandes entreprises privées. Joseph Nye relèvera à ce propos que c'est dans la mesure où les données sont partagées entre plusieurs entreprises puissantes que le danger se fait plus grand au niveau de la confidentialité et de la liberté de l'individu.
Le débat sur ce plan est donc ouvert à l'échelle planétaire. Les experts et hauts responsables qui planchent sur la question feraient bien de proposer sans trop tarder des mesures concrètes en termes de protection des libertés individuelles avant que la situation dans ce domaine n'échappe à tout contrôle.

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

Source : http://www.lorientlejour.com/article/900564/la-wpc-participe-au-debat-le-big-data-debouchera-t-il-sur-un-big-brother-.html
par Michel TOUMA