Detekt : l’outil Anti-Espions d’Amnesty International, Digitale Gesellschaft, l’Electronic Frontier Foundation et Privacy International…

Detekt : l’outil Anti-Espions d’Amnesty International…

Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, ont lancé un outil anti-espion : Detekt.

Ce billet a été rédigé par Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

Imaginez que vous n'êtes jamais seul
Quelqu'un regarde par-dessus votre épaule, enregistre toute activité sur votre ordinateur, lit et écoute vos conversations privées sur Skype, allume le microphone et la caméra de votre téléphone portable pour vous surveiller, vous et vos collègues, sans même que vous vous en rendiez compte.
Pour des milliers de défenseurs des droits humains et de journalistes qui, aux quatre coins de la planète, s'efforcent de dévoiler des atteintes aux droits humains et des injustices choquantes, nul besoin de l'imaginer.
Ils sont victimes d'une nouvelle forme sophistiquée de surveillance illégale. Certains gouvernements utilisent déjà des technologies de pointe pour installer des espions virtuels dans leurs bureaux et leurs salons.
La plupart des personnes ciblées ne savent même pas qu'elles sont espionnées, jusqu'à ce qu'on leur montre des copies de courriels et de vidéos où elles apparaissent, avec leurs collègues. Ces documents ont été extraits subrepticement de leurs propres ordinateurs portables. Ces « preuves » refont souvent surface lorsque les militants sont passés à tabac dans des cellules sordides, sanctionnés pour leur travail légitime ou contraints d' »avouer » des crimes qu'ils n'ont pas commis.

Le militant des droits humains et blogueur Ahmed Mansoor est l'un d'entre eux.
Ressortissant des Émirats arabes unis, il a été relâché en 2011. Il avait été incarcéré parce qu'il avait signé une pétition en faveur de la démocratie et animait un forum de discussion en ligne, que le gouvernement avait bloqué un an auparavant sous prétexte qu'il hébergeait des commentaires critiques envers les autorités. Après sa libération, Ahmed Mansoor a découvert que ses déplacements étaient parfois surveillés et a été agressé physiquement à deux reprises. Il s'est plus tard rendu compte que son ordinateur avait été infecté par des logiciels espions qui permettaient aux autorités de surveiller chacun de ses mouvements. Sa messagerie et son compte Twitter étaient également piratés.
Ce type de logiciels espions sophistiqués est l'arme idéale contre les défenseurs des droits humains. Ils sont de plus en plus utilisés dans le monde, même dans des États qui proclament défendre les libertés fondamentales.
Ces logiciels sont développés et produits dans des pays comme le Royaume-Uni, l'Allemagne et l'Italie, pour être ensuite vendus à des gouvernements du monde entier, sans qu'aucune réglementation ne garantisse qu'ils ne serviront pas à faciliter des atteintes aux droits humains.

« Cette nouvelle forme de surveillance semble tout droit sortie de 1984 de George Orwell, et elle rencontre un vif succès. Auparavant, les gouvernements interceptaient des communications ; aujourd'hui, ils peuvent entrer dans les systèmes et tout surveiller comme s'ils se trouvaient dans la pièce », a déclaré Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

Et même si l'Union européenne s'est récemment engagée à adopter des réglementations sur le commerce des équipements de surveillance, cette technologie dangereuse se développe à un rythme effréné.

Detekt
En réaction au nombre croissant de militants arrêtés arbitrairement et interrogés avec violence sur la base d'informations soutirées illégalement, des experts en technologie se sont mis à jouer « au chat et à la souris » pour combattre la surveillance ciblant des personnes qui exercent leur droit à la liberté d'expression et d'association. Certains de ces experts se sont associés avec Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, afin de lancer un nouvel outil.
Detekt est un logiciel simple qui permet d'effectuer une analyse sur un ordinateur fonctionnant avec le système d'exploitation Microsoft Windows pour y trouver la trace de logiciels espions et alerter ses utilisateurs afin qu'ils puissent agir.

Selon Claudio Guarnieri, l'un des cerveaux qui a développé cet outil, Detekt répond à une demande d'aide croissante de la part des militants depuis 2012.

« Nous avons commencé à faire des recherches sur les pays qui commercialisent des équipements de surveillance et avons découvert qu'une société allemande en vendait aux autorités de Bahreïn, qui les avaient utilisés contre les manifestants durant le soulèvement [depuis février 2011]. Tout est parti de là, et cela nous a emmenés vers des pays comme le Maroc, la Tunisie, l'Éthiopie et quelques autres, qui s'en sont eux aussi servis », a déclaré Claudio Guarnieri.

« Tant de pays utilisent désormais ces technologies, qu'il serait plus simple de se pencher sur les autres. Si vous prenez une carte et placez un point rouge sur chaque pays concerné, cela fait froid dans le dos: Bahreïn, le Maroc, les Émirats arabes unis, Oman, l'Éthiopie, le Soudan, l'Ouzbékistan, le Kazakhstan, l'Azerbaïdjan, l'Indonésie, la Malaisie, l'Australie, l'Inde, le Mexique, Panama, le Royaume-Uni et l'Allemagne, entre autres. »

La Coalition contre l'exportation illégale de technologies de surveillance, dont Amnesty International est membre, estime que le commerce mondial des technologies de surveillance représente 4 milliards d'euros par an, et qu'il est en expansion.

FinFisher compte parmi les entreprises qui développent ce type de logiciels espions. Cette société allemande qui a appartenu à l'entreprise britannique Gamma International a conçu le logiciel espion FinSpy, grâce auquel il est possible d'effectuer un suivi des conversations sur Skype, d'extraire des fichiers de disques durs, d'enregistrer toute utilisation du microphone ainsi que les courriels, et même de prendre des captures d'écran et des photos en utilisant la caméra de l'appareil.
Selon des recherches menées par Citizen Lab et des informations rendues publiques par Wikileaks, FinSpy a permis d'espionner des militants et des avocats défenseurs des droits humains à Bahreïn – dont certains vivaient au Royaume-Uni.
C'est le cas de Saeed Al Shehabi, militant politique bahreïnite actuellement installé au Royaume-Uni. En juillet 2014, Privacy International a publié des informations indiquant que Gamma International avait vendu des services de logiciels aux autorités bahreïnites.

« Nous savions que les autorités surveillaient les militants à Bahreïn, mais nous ne pensions pas qu'il leur était possible de le faire ici, au Royaume-Uni. J'ai peur, parce qu'on ne sait jamais quelles informations ils ont recueillis, ni comment ils vont les déformer et s'en servir. Je ne me sens pas du tout en sécurité. Detekt me semble un outil très utile, et inestimable pour des militants comme moi », a déclaré Saeed.

Sécurité et droits humains
Les organisations qui dénoncent la surveillance ciblée illégale sont fréquemment accusées de développer des outils susceptibles d'entraver l'action légitime du gouvernement contre le crime organisé.

Toutefois, les experts comme Claudio Guarnieri s'accordent à dire que le problème est l'absence quasi totale de contrôle, de cadres juridiques et de lignes directrices quant à l'utilisation de ces technologies intrusives.

« La transparence n'est pas de mise pour savoir qui s'en sert et dans quelles circonstances. La seule chose que nous savons, c'est que ces technologies servent souvent à entraver le travail des militants et des journalistes. Nous souhaitons lancer un débat pour tenter de comprendre comment cela fonctionne, car tout se déroule dans le plus grand secret. Il faut plus de transparence sur les implications légales, morales et politiques de l'emploi de ces technologies », a déclaré Claudio Guarnieri.

Nous espérons que Detekt apportera un sentiment de sécurité aux défenseurs des droits humains, aux journalistes, aux avocats et aux militants, et qu'il permettra d'ouvrir le débat sur la nécessité de réglementer le développement, la vente et l'utilisation des technologies de surveillance.

« Ce marché échappe à tout contrôle. Il faut des réglementations légales solides pour qu'il soit en phase avec les normes relatives aux droits humains. Les conséquences négatives et les dangers du recours non réglementé à ces technologies puissantes sont énormes et celles-ci doivent être contrôlées », a déclaré Marek Marczynski.

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

Source : http://www.huffingtonpost.fr/genevieve-garrigos/detekt-un-nouveau-logiciel-dans-le-jeu-du-chat-et-de-la-souris-contre-big-brother_b_6235750.html
par Geneviève Garrigos Présidente Amnesty International France

---

Des piratages informatiques facilités en raison d'un personnel trop peu qualifié

Des piratages informatiques facilités en raison d'un personnel trop peu qualifié

EY publie les résultats d'une étude mondiale sur le cybercrime qui fait état des menaces grandissantes auxquelles sont confrontées la plupart des entreprises. Les menaces principales sont notamment le phishing, les logiciels malveillants et la fraude.

Un état des lieux bien réel

La cybercriminalité apparaît aujourd'hui comme une menace globale dont les contours sont difficiles à appréhender. La prolifération de ce type d'agressions, souvent impunies par ailleurs, touche autant le secteur public que privé.

L'étude du cabinet EY intitulée Get Ahead of Cybercrime et menée auprès de 1.825 entreprises dans 60 pays montre que les entreprises ne sont pas suffisamment préparées à faire face aux inévitables attaques informatiques. Ainsi, plus d'un tiers (37%) des entreprises n'ont pas de perception en temps réel des risques cyber et ne disposent pas de la souplesse, du budget et des compétences nécessaires pour lutter contre la cybercriminalité en augmentation.

Dans le monde, 43% des sondés indiquent que leur budget total dédié à la sécurité de l'information restera globalement identique au cours des 12 prochains mois en dépit des menaces grandissantes. Au Luxembourg, 53% des sondés ont tout de même l'intention d'augmenter de plus de 5% leur budget en matière de sécurité de l'information.

Un personnel trop peu sensibilisé au risque informatique en cause

Mais c'est la négligence des employés, tout autant que leur prise de conscience insuffisante des risques, qui représente la plus importante vulnérabilité face à la cybercriminalité.

54% des sondés ont relevé un manque de ressources qualifiées

dont 6% disposent d’une équipe d’évaluation des menaces et 35% concèdent ne pas être dotés d’un programme d’évaluation des menaces.

Anticiper les attaques
Au Luxembourg, les menaces principales sont notamment le **phishing (25%)**, les **logiciels malveillants (20%)** et la **fraude (17%)**.

«Les entreprises doivent adopter une attitude proactive plutôt qu’une attitude uniquement réactive, les faisant dès lors évoluer de cibles faciles pour les cybercriminels vers de redoutables adversaires»

conseille Brice Lecoustey, à la tête du département Advisory pour le secteur commercial et public chez EY Luxembourg.

À travers plusieurs recommandations, le rapport encourage les entreprises à considérer la cybersécurité comme une capacité concurrentielle essentielle. Afin d’atteindre cet objectif,

l’entreprise est tenue de se maintenir dans un état permanent de préparation, d’anticiper de nouvelles menaces éventuelles et de perdre cet état d’esprit de «victime» devant conduire ses activités dans un état d’anxiété permanent.

«Au-delà des menaces internes, les entreprises doivent mener une réflexion plus large relative à leur ‘écosystème’ commercial et à l’incidence potentielle de leurs relations avec des tiers et des vendeurs en matière de sécurité», ajoute Olivier Maréchal, à la tête du département Advisory pour le secteur financier chez EY Luxembourg. Avant de conclure:

«C’est uniquement en atteignant un niveau avancé de préparation en matière de cybersécurité qu’une entreprise peut commencer à réellement bénéficier des investissements consentis dans ce domaine.»

Références :

http://paperjam.lu/news/cybersecurite-les-entreprises-plutot-desarmees

par EY, Brice Lecoustey et Olivier MaréchalEY

cliquez ici pour consulter le rapport

CryptoPHP – Plus de 23 000 serveurs web infectés

CryptoPHP – Plus de 23 000 serveurs web infectés

La propagation du backdoor CryptoPHP se fait par les plug-ins et les thèmes piratés pour les CMS WordPress, Joomla et Drupal.

Plus de 23 000 serveurs web ont été infectés par un backdoor baptisé CryptoPHP qui est arrivé avec les thèmes et les plug-ins piratés pour des systèmes de gestion de contenu très populaires, à savoir WordPress, Joomla et Drupal. CryptoPHP est un script malveillant qui permet des attaques à distance avec la possibilité d'exécuter du code délictueux sur des serveurs web et d'injecter du contenu inapproprié sur des sites web.

Selon le cabinet de sécurité néerlandais Fox-IT, qui a publié un rapport sur cette menace la semaine dernière, la porte dérobée est principalement utilisée pour l'optimisation de BHSEO (Black hat search engine optimization), une opération qui consiste à injecter des mots-clés et des pages indélicates sur les sites compromis afin de détourner les recherches effectuées par les moteurs traditionnels et pousser du contenu malveillant le plus haut possible dans les résultats de recherche.

Un backdoor profitant de la culture pirate des webmasters

Contrairement à la plupart des backdoors s'attaquant aux sites web, CryptoPHP ne s'installe pas en exploitant les vulnérabilités. Les hackers distribuent simplement des versions piratées des plug-ins et thèmes commerciaux pour Joomla, WordPress et Drupal et attendent simplement que les webmasters les téléchargent et les installent sur leurs propres sites web. Ces plug-ins et thèmes piratés intègrent le backdoor CryptoPHP. Les serveurs web infectés par CryptoPHP agissent comme un réseau de zombies. Ils se connectent à des serveurs de commande et de contrôle exploités par les hackers en utilisant un canal de communication chiffré et attendent les instructions.

Avec l'aide du Centre national de la cybersécurité du gouvernement néerlandais et d'organisations de lutte contre la cybercriminalité (Fondation Shadowserver, Abuse.ch et Spamhaus), Fox-IT a pris le contrôle des domaines de commande et de contrôle de CryptoPHP envoyant des instructions aux serveurs infectés pour recueillir des statistiques. Une opération connue sous le terme « sinkholing ».

Plus de 1000 sites web infectés en France

« Au total, 23 693 adresses IP uniques étaient reliés aux centres de contrôle », ont indiqué dans un billet de blog les chercheurs de Fox-IT. Cependant, le nombre de sites concernés est probablement plus élevé, parce que certaines de ces adresses IP correspondent à des serveurs d'hébergement web partagé qui ont plus d'un site infecté. Les cinq premiers pays infectés par CryptoPHP étaient les États-Unis (8657 adresses IP), l'Allemagne (2877 adresses IP), la France (1 231 adresses IP), les Pays-Bas (1008 adresses IP) et la Turquie (749 adresses IP).

Depuis la publication du rapport de Fox-IT sur CryptoPHP la semaine dernière, les hackers ont fermé les sites qui ont poussé les plug-ins et thèmes piratés pour en créer de nouveaux. Ils ont également introduit une nouvelle version de leur backdoor, peut-être dans une tentative d'échapper à la détection.

Les chercheurs Fox-IT ont publié deux scripts Python sur GitHub que les webmasters peuvent utiliser pour scanner leurs serveurs et leurs sites web à la recherche de CryptoPHP. Ils ont également fourni des instructions pour le supprimer sur leur blog, tout en notant que finalement il est préférable de complètement réinstaller son CMS afin de repartir sur une base saine.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-plus-de-23-000-serveurs-web-infectes-par-cryptophp-59420.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Le rapport : https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf
Article de Peter Sayer, IDG NS (adaptation Serge Leblal)

Droit à l’oubli : les 13 critères dégagés par la CNIL

Droit à l’oubli : les 13 critères dégagés par la CNIL

Soucieuse de ne pas laisser Google et ses concurrents fixer eux-mêmes leurs propres conditions d'application du droit à l'oubli, la CNIL a publié une liste de 13 critères à prendre en compte dans la décision de donner ou non satisfaction à une demande de déréférencement.

Le 13 mai 2014, la Cour de Justice de l'Union Européenne (CJUE) a rendu son déjà célèbre arrêt Google Spain qui oblige Google à donner satisfaction aux internautes qui demandent la censure de résultats qui les concernent, consacrant ainsi l'existence d'un « droit à l'oubli » sur Internet. Toutefois la CJUE avait aussitôt nuancé cette obligation en prévenant Google qu'il fallait étudier les demandes au cas par cas, pour refuser les requêtes d'un individu lorsqu'il « il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations ».

La CJUE demandait que l'appréciation soit réalisée par Google lui-même, au regard de « la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à recevoir cette information ». La cour confiait ainsi à une entreprise privée le soin d'interpréter et appliquer le droit, à la place d'un juge dont c'est le métier et la fonction.
Or en signant cet arrêt inattendu qui contredisait l'avis de son avocat général, la cour de Luxembourg a fait naître un conflit inédit d'influence entre le secteur privé et des autorités publiques. D'un côté, Google a sauté sur l'occasion pour prendre un bout de souveraineté aux Etats et affirmer sa capacité autonome à déterminer ses propres critères jurisprudentiels, en mettant sur pieds un comité consultatif privé. De l'autre côté, les CNIL européennes qui se croyaient investies du pouvoir de faire respecter le droit à l'oubli avaient immédiatement annoncé leur intention de fixer elles-mêmes des critères, qu'elles appliqueraient en dernier recours si un internaute se plaint de ne pas avoir eu satisfaction. Elles ont ainsi boudé les réunions publiques de Google, n'acceptant pas d'être doublées.

C'est donc dans cet esprit que le G29, qui réunit la CNIL et tous ses homologues européens, a publié ce jeudi une première liste de critères généraux à prendre en compte dans l'acceptation ou le refus d'une demande de droit à l'oubli. Le document (.pdf) détaille chacun des critères à l'aune de l'arrêt de la CJUE. Les voici résumés (nos commentaires en italique) :

1. **Les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparaît-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?**
Seules les recherches du nom ou du pseudonyme d'un particulier entrent dans le champ de l'arrêt Google Spain.
2. **S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?**
Outre la détermination de ce qu'est un « rôle dans la vie publique », La CNIL ajoute un critère supplémentaire qui est de distinguer selon que l'information elle-même est une information pertinente au regard de cette vie publique, ou s'il s'agit d'une information d'ordre purement privé.
3. **Le plaignant est-il mineur ?**
Par principe si la réponse est oui le droit à l'oubli doit être respecté, au nom de 'l'intérêt supérieur de l'enfant » consacré par la Charte des droits fondamentaux de l'Union européenne.
4. **Les données sont-elles exactes ?**
En cas d'inexactitude, le droit à l'oubli joue le rôle d'un droit brutal de rectification. C'est toutefois à l'internaute d'apporter la preuve de l'inexactitude.
5. **Les données sont-elles pertinentes et/ou excessives ?**
Plusieurs sous critères sont ici ajoutés :

– Les données sont-elles relatives à la vie professionnelle du plaignant ?
une réponse positive joue en défaveur du droit à l'oubli, qui doit être utilisé pour la protection de la vie privée)
– L'information est-elle potentiellement constitutive de diffamation, d'injure, de calomnie ou d'infractions similaires à l'encontre du plaignant ?
la réponse positive doit reposer en priorité sur une décision judiciaire qualifiant les accusations, mais un critère de « contenu excessif » peut aussi s'appliquer par la CNIL
– L'information reflète-t-elle une opinion personnelle ou s'agit-il d'un fait vérifié ?
La CNIL vise ici le déréférencement de « campagnes de dénigrement » qui pourrait être accordé, ce qui semble flirter très dangereusement avec la ligne rouge de la censure pure et simple d'une opposition politique.
6. **L'information est-elle sensible au sens de l'article 8 de la Directive 95/46/CE ?**
Le fait que la page web dont la censure est demandée contient des informations sur l'origine raciale, la religion, les opinions politiques, l'orientation sexuelle, etc., doit jouer en faveur du droit à l'oubli.
7. **L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?**
La CNIL est ici favorable à ce qu'une information devenue obsolète puisse être supprimée, y compris (c'est un cas explicité) s'il s'agit par exemple d'une condamnation en première instance annulée en appel.
8. **Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?**
Il s'agit d'un critère de proportionnalité. La CNIL est par exemple favorable au déréférencement de pages qui relateraient une « infraction mineure » et qui posent problème pour la recherche d'un emploi, ou celui de photos intimes.
9. **Les informations issues du moteur de recherche créent-elles un risque pour le plaignant ?**
Sont visées ici les informations telles que des coordonnées bancaires, n° de passeport, adresse personnelle, etc., qui pourraient être utilisées par des tiers à mauvais escient.
10. **Dans quel contexte l'information a-t-elle été publiée ?**
A nouveau plusieurs sous-critères :
– Le contenu a-t-il volontairement été rendu public par le plaignant ?
Contrairement à ce que l'on pourrait croire, la CNIL estime que la réponse positive joue en faveur du droit à l'oubli, car il faut respecter le fait que la personne ne souhaite plus voir référencé un contenu qu'elle avait mis en ligne. Mais l'on doute que la réponse négative puisse jouer en sa défaveur. Dès lors, est-ce vraiment un critère ?
– Le contenu devait-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait rendu public ?
La mise en ligne à l'insu de la personne joue en faveur du déréférencement (ce qui rejoint notre point précédent)
11. **Le contenu a-t-il été rendu public à des fins journalistiques ?**
La CNIL refuse d'en faire véritablement un critère. Tout en reconnaissant qu'il faut « prendre en considération » le caractère journalistique de l'information dont la censure est demandée, la CNIL minimise au maximum sa portée par rapport aux autres critères.
12. **La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?**
Si oui, le droit à l'oubli sera en principe refusé, sauf si d'autres critères priment (tels que le préjudice subi)
13. **L'information est-elle relative à une infraction pénale ?**
Si la condamnation a été effacée par l'amnistie prévue par la loi, le droit doit être systématiquement accordé. Sinon, c'est la gravité et la date de l'infraction qui entrent en considération.

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

Source : http://www.numerama.com/magazine/31424-droit-a-l-oubli-les-13-criteres-degages-par-la-cnil.html
par Guillaume Champeau

Registre National du Commerce et des Sociétés gratuitement ouvert et partagé : ce que le projet de loi a visiblement

négligé

Registre National du Commerce et des Sociétés gratuitement ouvert et partagé : ce que le projet de loi a visiblement négligé

Le projet de loi du gouvernement: « pour la croissance et l'activité » ambitionne, et c'est louable, de renouer avec la croissance de moderniser l'économie en simplifiant les règles qui, aujourd'hui, constituent un frein à la création et à l'innovation.

Pour ce faire le gouvernement fait l'exercice d'une attaque en règle des professions réglementées, qualifiées de tous les maux de la terre et qui méritent toutes la guillotine législative propre à les assainir!
Les greffiers des Tribunaux de Commerce, qualifiés notamment de rentiers ne sont pas épargnés!
L'une des propositions pour atteindre les objectifs envisagés s'inscrit dans la vague, très trendy, de l'open data. Dans cet esprit le gouvernement envisage de permettre l'ouverture et le partage gratuit des données du Registre National du Commerce et des Sociétés.
Pour les non initiés il est bon de rappeler le rôle de ce Registre tenu par l'Institut National de la Propriété Intellectuelle.

L'INPI est en charge de la centralisation au niveau national, sous forme de documents originaux, des informations et actes provenant des Registres du Commerce et des Sociétés (RCS) tenus localement par chacun des greffes de Tribunaux de commerce et des greffes des Tribunaux civils à compétence commerciale. L'ensemble de ces informations et actes forme le Registre National du Commerce et des Sociétés (RNCS).

A l'origine, un des objectifs de cette mission de centralisation par l'INPI du RNCS était la sécurisation de l'information légale sur les entreprises. La centralisation d'un second original de chaque acte et pièce déposés dans les différents RCS permettait de parer au risque de déperdition physique de cette information en cas par exemple d'incendie entraînant la destruction des archives papier d'un greffe.

14 millions d'euros versés à l'INPI
A l'heure de la dématérialisation et de la tenue électronique des registres légaux, la nécessité de cette sécurisation physique s'est significativement estompée. Aujourd'hui le rôle de l'INPI dans la tenue du RNCS se résume à archiver l'ensemble des actes et pièces transmis et à distribuer, de manière payante, 2 licences de données (IMR et bilans) pour les sociétés de renseignements commerciaux, ces licences étant constituées par le GIE Infogreffe pour le compte de l'INPI…

Pour être complet sur le sujet il convient de rappeler que les entreprises acquittent à chaque formalité une taxe de 5.90€ reversée à l'INPI par les greffiers. En 2013 le montant collecté s'est élevé à 14 M€ d'euros. Pour faire quoi? On peut encore s'interroger… Dans la mesure où la base de données de l'INPI et les licences ne sont autres que celles fournies par le GIE Infogreffe.

Il est important, alors que le texte du projet de loi est dans les mains de juristes éminents au Conseil d'Etat, de faire un peu de droit. Alors tentons d'expliquer, sans passion ni dogme, les difficultés auxquelles se heurtent le texte actuel.

La volonté de vouloir mettre en données ouvertes les données des entreprises afin de faciliter leur réutilisation dans le but de favoriser le développement économique ne ressort pas du simple postulat. Si aucun pays européen ne l'a encore mis en œuvre c'est que à cette liberté s'oppose des règles de droit dont l'essentiel ont pour but de protéger les individus.

Les données personnelles des dirigeants sont protégées
Ainsi le sujet de la propriété des données personnelles issues du RCS et du RNCS est le premier écueil qui doit être analysé pour déterminer les conditions de distribution de ces données.
L'article 2 de la loi informatique et libertés et la directive 95/46/CE définissent les données personnelles comme les données permettant d'identifier ou de rendre identifiable une personne physique. Cette définition concerne l'intégralité des informations des dirigeants des sociétés immatriculées au Registre du Commerce et des Sociétés. La nationalité, la date et lieu de naissance et bien sûr les noms, prénoms et adresses sont mentionnés.

La généralisation des transactions sur les données personnelles dont la collecte est la contre partie obligée de l'accès à un très grand nombre de services a répandu cette croyance infondée.

Ces données personnelles ne sont pas susceptibles d'appropriation, ce principe a été rappelé par le Conseil d'Etat dans son rapport: le numérique et les droits fondamentaux: « 50 propositions du Conseil d'Etat pour mettre le numérique au service des droits individuels et de l'intérêt général « .

Dans ce rapport le Conseil d'Etat promeut un droit à: « l'autodétermination informationnelle » décrit comme un « objectif » qui donne sens à tous les droits préexistants.

Les données personnelles peuvent être cédées après accord explicite
Mais le projet de loi gouvernemental soulève un autre problème de légalité. L'article 6 de la directive 95/46/CE dispose que « de telles informations ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ».
Or, les données personnelles des personnes physiques n'ont été collectées que pour une seule raison: celle de figurer au RCS et au RNCS et pour les seules finalités induites par ces mêmes registres. Ces données n'ont jamais été collectées pour qu'elles puissent ultérieurement figurer dans « une licence ouverte » à tous sur internet notamment pour être « googliser ». Les commerçants de base de données, les opérateurs de ces nouveaux marchés ne peuvent pas en principe réutiliser ces données personnelles.
L'article 7 de la Directive 95/46/CE dispose que « Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement ».

Le même principe est posé par l'article 7 de la loi dite Informatique et Libertés.
Si le RCS et le RNCS sont légalement « dispensés » du recueil de ce consentement, il n'en va nullement de même si les données sont ensuite sorties du RCS ou du RNCS pour être communiquées au public en vue de leur réutilisation.

Les données doivent être rendues anonymes
L'article 13 de la loi n°78-753 du 17 juillet 1978 dite CADA dispose que « Les informations publiques comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet ».
La CNIL exige également, au visa de la loi Informatique et Libertés, une anonymisation des données à caractère personnel figurant dans les documents administratifs.
En clair, chaque dirigeant, administrateur de société, chaque commerçant délivre son identité, son adresse et son âge. Ce sont autant de données personnelles. Si comme le prévoit le projet de loi gouvernemental, ces données devaient être exploitées à des fins commerciales, ce ne serait possible qu'avec l'accord de l'intéressé.
Gageons que le Conseil d'Etat relèvera ces obstacles qui, a priori, ont échappé au rédacteur du projet de loi et démontrent la non conformité des licences, aujourd'hui payantes, délivrées par l'INPi aux réutilisateurs professionnels.

Et la propriété intellectuelle des fichiers?
Tout comme il pourra constater qu'il n'est pas juridiquement possible de demander aux greffiers et à leur GIE Infogreffe d'abandonner leur droit de propriété intellectuelle issu de leur qualité de producteur de bases de données (Directive 96/9/CE du 11 mars 1996 – Article L 341-1 du Code de la propriété intellectuelle – Article L 112-3 du Code de la propriété intellectuelle).
En clair, selon la loi, seuls les Greffiers sont en droit d'autoriser une extraction de leurs bases de données et une diffusion de leurs données. Le projet de loi, en ce qu'il ne recueille pas l'accord des Greffiers sur la réutilisation de leurs droits, constituerait une spoliation.
Au plan du droit, une telle situation de fait exige un dispositif indemnitaire. Or, la loi impose une protection des producteurs de bases de données pendant 15 ans à compter du dernier investissement. Ce point n'a pas échappé au Rapporteur, Richard Ferrand, qui l'a clairement évoqué dans son rapport sur le projet de loi. Enfin il serait cocasse de voir l'Etat contraint, par les règles de droit, de payer une indemnité pour assurer une diffusion gratuite des données du RNCS!

L'ensemble des obstacles relevés démontre, à l'évidence, que le projet ne peut être maintenu en l'état.
La raison voudrait qu'une solution viable pour tous soit envisagée. C'est pourquoi nous proposons de diffuser en licence ouverte les données par exemple sur le site d'ETALAB. Ce choix d'un projet phare du gouvernement éviterait le doublon que représente la solution INPI. Qui de mieux placé que les greffiers dont la mission est de recevoir, contrôler, saisir et valider les informations, actes et documents déposés par les entreprises lors de l'accomplissement de leurs formalités légales pour en assurer une diffusion en données ouvertes respectueuses du droit.
Nous y sommes prêts.

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

Source : http://www.huffingtonpost.fr/bernard-bailet/ouverture-et-partage-gratuit-des-donnees-du-registre-national-du-commerce-et-des-societes-ce-que-le-projet-de-loi-a-visiblement-neglige_b_6232202.html?utm_hp_ref=france
par Bernard Bailet Président du G.I.E. Infogreffe

La police judiciaire découvre

une escroquerie à la carte bancaire inédite

La police judiciaire découvre une escroquerie à la carte bancaire inédite

L'office anti cyber-criminalité de la police judiciaire a annoncé vendredi avoir démantelé un réseau d'une quinzaine d'escrocs à la carte bancaire utilisant une méthode nouvelle. Ils auraient fait plus d'une centaine de victimes.

Ils pensaient avoir trouvé un système imparable pour s'enrichir à distance. Mais malgré leur inventivité et après avoir fait des centaines de victimes en France, une quinzaine d'escrocs à la carte bancaire ont été interpellés par l'office anti cyber-criminalité de la direction centrale de la police judiciaire (DCPJ).

Des escrocs créatifs… et bricoleurs
Les cyber-escrocs qui comptaient dans leurs rangs des petits commerçants, n'avaient pourtant rien laissé au hasard mais surtout, ils avaient innové.
Leur méthode consistait à fabriquer eux-même des « TPE » (les terminaux de paiements électriques que l'on trouve dans la plupart des magasins) permettant d'enregistrer le code de la victime ainsi que les données associées à sa carte bancaire. Ces informations en main, les escrocs débitaient les cartes depuis l'étranger, échappant à tous les filtres habituels.
Les victimes elles, ne se doutaient de rien. Au terme de la transaction sur le « TPE » frauduleux elles recevaient même le reçu habituel leur garantissant que leur carte avait bien été débité du montant indiqué sur l'appareil.

« Eviter l'effet « boule de neige » »
« Nous avons enquêté pendant un an il fallait agir avant que cette méthode ne fasse « boule de neige » en France » a affirmé Valérie Maldonado, directrice de l'office anti cyber-criminalité de la PJ (**OCLCTIC**).
Reste maintenant à retrouver les victimes. Leur nombre pourrait dépasser la centaine. Quant au préjudice total il reste lui aussi à déterminer mais pourrait atteindre des centaines de milliers d'euros.

Des escroqueries qui se multiplient
La fraude à la carte bancaire n'a cessée de progresser ces dernières années en France, selon un rapport de l'Observatoire national de la délinquance et des réponses pénales (ONDRP). Entre 2010 et 2012, le volume de ces fraudes a augmenté de 44%. En 2012, on estimait le préjudice total à plus de 450 millions d'euros. Dans plus des deux tiers des cas, les victimes ne sont débitées qu'une seule fois pour un montant moyen de 900 euros. On estime que le nombre d'escroqueries à la carte bancaire augmente deux plus vite que le nombre de cartes mises en circulation.

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

Source : http://www.franceinfo.fr/actu/justice/article/la-police-judiciaire-decouvre-une-escroquerie-la-carte-bancaire-inedite-609719

Les CNIL européennes veulent imposer leur droit à l'oubli au monde entier

Les CNIL européennes veulent imposer leur droit à l'oubli au monde entier

Les établissements européens de protection des données personnelles ont publié un ensemble de règles encadrant le droit à l'oubli. Ils réclament notamment l'extension de la mesure à la version américaine de Google.

L'Europe milite pour un droit à l'oubli sans frontières. Le G29, le groupe européen des autorités de protection des données personnelles, a adopté mecredi un ensemble de recommandations pour encadrer cette mesure. Parmi leurs griefs, les CNIL européennes réclament l'extension du droit à l'oubli à tous les noms de domaine des moteurs de recherche, y compris en .com. Le premier site visé est Google, qui représente près de 90% du marché de la recherche en Europe.

135.000 demandes en quatre mois

Le droit à l'oubli est apparu en Europe en mai, à la suite d'une décision de la Cour de justice européenne. Cette dernière avait alors estimé que les moteurs de recherche, dont Google, étaient responsables du traitement des données à caractère personnel. En conséquence, les citoyens européens peuvent désormais obtenir, sous certaines conditions, le déréférencement de pages Internet qui contiennent des informations «inappropriées, hors de propos ou qui n'apparaissent plus pertinentes.»
Même si tous les moteurs de recherche en Europe sont touchés par la mesure, Google est le premier concerné. En quatre mois, le groupe américain a reçu plus de 135.000 demandes de droit à l'oubli, via un formulaire mis en ligne pour l'occasion. En cas de refus de la part de Google, les internautes peuvent s'adresser à leur CNIL nationale, qui pourra juger leur cas grâce aux critères adoptés mercredi. «Il s'agit d'avoir une mise en oeuvre harmonisée et une interprétation commune de l'arrêt de la Cour», explique Gwendal Le Grand, directeur des technologies et de l'innovation à la CNIL.

Pour le G29, Google n'en fait pas assez

Les règles proposées par le G29 risquent de relancer un débat que Google tente vainement d'apaiser. Actuellement, lorsqu'un internaute obtient le déréférencement d'un contenu en ligne portant sur sa vie privée, il est retiré des résultats de recherche de la version du moteur de son pays d'origine. Une protection jusqu'alors jugée adéquate par Google, qui géolocalise l'adresse IP de ses utilisateurs. Les internautes français sont par exemple automatiquement redirigés vers les résultats de Google.fr, même s'ils tapent Google.com sur leur barre de navigation. Il est tout de même possible d'accéder au résultats de recherche de Google.com, en cliquant sur un bouton prévu à cet effet sur l'écran d'accueil, ou en remplaçant simplement le «.fr» par «.com» dans la barre de navigation. Google est donc sommé d'étendre le droit à l'oubli «sur tous les noms de domaine en .com».

Les CNIL européennes ne sont pas tendres avec le groupe américain et considèrent qu'il n'en fait pas assez pour assurer le respect du droit des citoyens. «La loi européenne ne doit pas être contournée», prévient le groupe. «Les actions de Google sont sujettes aux décisions des autorités de protection des données personnelles et des juges», ajoute Gwendal Le Grand. Si Google n'adapte pas ses pratiques, les CNIL seront désormais en droit de lui réclamer le respect de ses nouvelles règles.
Contacté par le Figaro, Google a indiqué qu'il analyserait «attentivement» ces recommandations dès leur publication officielle.

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

Source : http://www.lefigaro.fr/secteur/high-tech/2014/11/27/01007-20141127ARTFIG00320-les-cnil-europeennes-veulent-imposer-leur-droit-a-l-oubli-au-monde-entier.php#xtor=AL-201
Par Lucie Ronfaut

Les e-commerçants ciblés par les attaques des cybercriminels

Les e-commerçants ciblés par les attaques des cybercriminels

Selon un rapport d'Imperva réalisé en octobre 2014, les e-commerçants sont les plus souvent ciblés par les cyber-attaques. Les attaques seraient plus nombreuses, mais également plus longues. 48 % des attaques cibleraient directement des applications web des e-commerçants, mais les institutions financières sont également concernées.

Les données des e-commerçants visées par les hackers

Les chiffres sont issus du rapport Web Application Attack Report (WAAR), réalisé par l'Application Defense Center (ADC) d'Imperva. Selon l'équipe du spécialiste de la sécurité informatique, près d'une attaque sur deux cible les e-commerçants, et notamment leurs applications web. 40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne.

D'après l'équipe ADC, le système de gestion de contenu WordPress est également souvent visé par les attaques. Pour Imperva, l'audience des sites est un critère de choix pour les hackers : « quand une application web ou une plateforme devient populaire, les hackers savent que le retour sur investissement d'une attaque sur ces supports sera intéressant pour eux, ils passent donc plus de temps à les explorer, soit pour voler des données soit pour utiliser les systèmes comme bots », estime le rapport WAAR.
Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013.
« Les e-commerçants doivent prendre ces menaces de cyber-attaque très au sérieux », soutient Amichai Schulman, directeur de la technologique pour Imperva, qui évoquent le verrouillage des bases de données et leur cryptage.
En France, la Fevad (Fédération du e-commerce et de la vente à distance) et Médiamétrie estiment que les consommateurs vont se tourner en masse vers les achats en ligne pour Noël 2014. 68% des internautes envisagent un achat sur internet d'ici la fin de l'année.

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

Source : http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels

Tom’s Guide victime d’une attaque de l’armée électronique syrienne

Tom’s Guide victime d’une attaque de l’armée électronique syrienne

En début d’après-midi, Tom’s Guide et de nombreux sites d’information ont été victimes d’une attaque informatique de la part de l’armée syrienne électronique. Des magazines tels que « The Independent » et « The Telegraph », en Grande Bretagne, le Chicago Tribune aux Etats-Unis ou encore le site de la ligue nationale de hockey (NHL.com) ont été simultanément touchés par cette attaque.

Sur ces sites, comme sur tomsguide.fr, le procédé de l’armée électronique syrienne est le même. Celle-ci aurait réussi à exploiter une faille du CDN de Gigya. Il s’agit d’un réseau de diffusion de contenus, notamment sociaux, qui est utilisé par plusieurs sites médias dans le monde, dont tomsguide.fr. Dès lors qu’elle a réussi à s’attaquer à Gigya, l’armée électronique syrienne a pu injecter une redirection dans le code distribué par ce service.

Des hackers proches de Bachar el-Assad
C’est la raison pour laquelle, une partie de des lecteurs de tomsguide.fr a vu s’afficher un message revendiquant le piratage du site et un lien affichant le drapeau du groupe de hackers. L’armée électronique syrienne est un groupe de pirates informatiques proche du régime de Bachar el-Assad. Né en 2011 en début de la guerre civile syrienne, il s’emploie à perturber le fonctionnement de médias occidentaux qu’il juge hostiles au régime syrien.

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

Source : http://www.tomsguide.fr/actualite/piratage-armee-syrienne,45695.html

CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online

	CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online

CyberArk annonce la publication d'un nouveau rapport qui détaille les tendances actuelles des cyberattaques ciblées avancées, lesquelles ont communément adopté comme signature clé l'exploitation malveillante des comptes à privilèges.

L'étude intitulée « Privileged Account Exploits Shift the Front Lines of Security » apporte une expertise sur les récentes tendances des attaques ciblées, à partir de l'expérience de terrain des analystes les plus réputés au monde en matière de menaces informatiques et de résolution des attaques de sécurité les plus dévastatrices. Les participants à cette analyse incluent :

· Groupe de renseignements de sécurité et de recherche Cisco Talos
· Service de consultance financière Deloitte LLP – Equipe de recherche informatique
· Deloitte & Touche LLP – Services en matière de risques informatiques
· Mandiant, une entreprise FireEye
· RSA, Division Sécurité d'EMC
· L'équipe RISK de Verizon

« Cette coalition rassemble certains des analystes des menaces informatiques les plus brillants, expérimentés et réputés au monde. C'est en comparant et en comprenant les points communs de nos recherches respectives que nous avons pu dresser un aperçu approfondi des modes de fonctionnement des attaques ciblées, explique Udi Mokady, PDG de CyberArk. Cette étude nous a permis de découvrir que presque chaque attaque avancée implique une exploitation de comptes à hauts pouvoirs, raison principale pour laquelle elles sont si difficiles à déceler et à stopper. Ces comptes permettent en effet aux assaillants d'accéder à des réseaux et bases de données sécurisés, d'effacer toute trace d'infraction, d'éviter toute détection et de créer des portes de sortie rendant leur éviction des réseaux quasi impossible. La sécurisation des comptes à privilèges est devenue la nouvelle priorité des systèmes de défense dans la bataille que les entreprises mènent actuellement face à la cybercriminalité. »

Les comptes à privilèges, qui se composent notamment des identifiants utilisés pour l'administration informatique des mots de passe par défaut et codés en dur ainsi que de backdoors d'applications, offrent aux pirates informatiques un véritable laissez-passer qui leur permet de se rendre où ils le souhaitent et de traverser le réseau sans le moindre obstacle. Ces comptes permettent également aux hackers d'effacer leurs traces et de soutirer des données en tous genres. Et dès que ceux-ci parviennent à obtenir un accès privilégié aux systèmes et applications critiques, il est extrêmement difficile de les arrêter et d'atténuer les risques de perte de données et de préjudice commercial.

Parmi les principales découvertes du rapport :
· Chaque secteur et chaque entreprise est aujourd'hui une cible : Les pirates informatiques ont élargi leur champ d'action et **ciblent aujourd'hui les entreprises de toutes tailles**, dans tous les secteurs confondus. Chaque attaque a souvent une cible bien déterminée, et les **pirates visent fréquemment leurs partenaires et fournisseurs**. Les analystes en sécurité ont étudié des attaques visant des cibles non-traditionnelles, telles que des **sociétés de transport par camion** et de nombreux autres prestataires de services professionnels (**conseillers en gestion, auditeurs, avocats spécialisés dans les contentieux, etc.**), lesquelles constituent une étape clé dans le processus d'attaque d'un partenaire commercial.
· La résistance de périmètre est futile : Les pirates parviendront tout de même à s'introduire dans le périmètre de sécurité, et les employés constitueront le point d'infection le plus probable. L'attaque par hameçonnage est la technique la plus répandue et ne fait que gagner en sophistication, ce qui a rendu les connexions des employés beaucoup plus simples à infiltrer que les réseaux ou autres logiciels.
· Les pirates restent cachés pendant plusieurs mois ou années : Lors de leur détection, la plupart des attaques étaient en cours depuis au moins 200 jours. Les attaques financières sont quant à elles décelables plus rapidement, en règle générale en moins de 30 jours. Les assaillants peuvent dissimuler leurs traces par le biais des comptes à privilèges, en supprimant l'historique des connexions ainsi que les autres preuves.
· Les pirates convoitent les accès à hauts pouvoirs : Dans presque chaque cyberattaque ciblée, des comptes à privilèges ont été piratés. D'après leurs recherches, les analystes de la sécurité déclarent qu'entre 80 et 100% des incidents de sécurité les plus graves avaient pour « signature » une exploitation malveillante de comptes à hauts pouvoirs au cours de leur processus d'attaque.

· Les menaces liées aux comptes à privilèges largement sous-estimées : Les risques et les failles de sécurité que présentent les comptes à privilèges sont bien plus importants que les entreprises ne le réalisent. Les sociétés sous-estiment grandement le nombre de comptes à hauts pouvoirs qu'elles possèdent et ignorent quels systèmes les hébergent. Les recherches de CyberArk ont démontré que les organisations comptent aujourd'hui au minimum trois à quatre fois plus de comptes à privilèges que d'employés.

· Les cyberattaques contre les comptes à privilèges sont de plus en plus sophistiquées : Les analystes de la sécurité ont recensé plusieurs types d'infractions au niveau des comptes à hauts pouvoirs, qui vont de l'attaque répétée des comptes de service à la violation des appareils embarqués de l' « Internet des objets », en passant par la création d'identités multiples dans Microsoft Active Directory afin d'assurer la redondance des points d'accès et des portes dérobées.

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

Source : http://www.globalsecuritymag.fr/CyberArk-publie-un-rapport-sur-les,20141120,48898.html
par CyberArk