Détection d’une grande famille de malware et découverte de son mode opératoire

	Détection d’une grande famille de malware et découverte de son mode opératoire

La nouvelle variante de ransomware TorrentLocker atteint en 2014 plus de 40 000 systèmes informatiques européens.

Quelles sont les caractéristiques de cette nouvelle variante ?

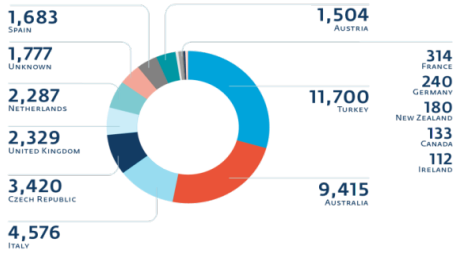
L'équipe de chercheurs canadienne ESET, spécialisée en menaces cybercriminelles, a découvert que depuis le début de l'année 2014, des attaques de ransomware du nom de TorrentLocker se propageaient partout en Europe. Cette variante identifiée par ESET comme Win32/Filecoder.Dl, appartient à la famille des ransomware. Il paraîtrait que les acteurs cachés derrière ce malware seraient de la même famille que le cheval de Troie bancaire : Hesperbot. Sa méthode change en revanche, puisque qu'il passe de la norme AES (Advanced Ecryption Standards) du chiffrement basé sur un compteur (CTR) au chiffrement d'enchaînement des blocs (Cipher Block Chaining, CBC)..

Le logiciel malveillant s'introduit malicieusement dans le système d'exploitation de sa victime, via des liens infiltrés eux-mêmes dans des e-mails frauduleux. Le logiciel crypte ensuite les données de l'ordinateur. Les documents, photographies et autres fichiers sont alors inutilisables pour le propriétaire. Le hacker peut aussitôt demander à la victime de payer une rançon si elle ne veut pas que ses données soient détruites. Les sommes demandées sont considérables, pouvant atteindre les 1200€. Pour déverrouiller ces données, la victime a besoin d'un code de déchiffrement que seul le pirate peut lui fournir et sans garantie.

Des techniques de persuasion toujours plus performantes

Les propriétaires de ces logiciels malveillants savent être de plus en plus convaincants en ciblant le message en fonction des pays qu'ils convoitent. Ils savent de mieux en mieux personnaliser et adapter leur message sur leurs cibles. Par conséquent, ils sont de plus en plus dangereux, car ces « faux » e-mails sont de plus en plus difficile à détecter pour les victimes.

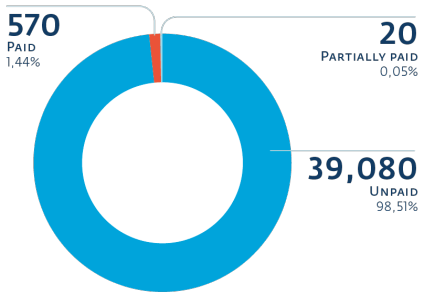
Les acteurs de ce logiciel malveillant utilisent de nombreuses ruses pour convaincre les internautes. Ils envoient des messages personnalisés, en mimant la provenance d'un organisme certifié. Ils en profitent ensuite pour réclamer le paiement d'une fausse facture. Ils arrivent même à troubler les internautes en allant jusqu'à insérer des images de CAPTCHA.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

Des conséquences irrémédiables, attention à ne pas les encourager !

La dernière vague de TorrentLocker a atteint 40 000 ordinateurs, représentant 280 millions de documents chiffrés en Europe, Canada, Australie et Nouvelle-Zélande. Près de 600 victimes ont payé la rançon, ce qui a fait gagner 481 578€ aux malfaiteurs en Bitcoins! En France, Torrentlocker a intercepté 2 170 247 fichiers avec une demande de rançon d'au minimum 830€.



Nombre de victimes ayant payé les cybercriminels pour le logiciel

L'équipe de chercheurs canadiens ESET a su démanteler TorrentLocker en localisant le malware grâce aux serveurs C&C qui généraient des URL pour les pages d'échanges d'argent avec les victimes.

La première règle à prendre en considération est qu'il faut d'une part protéger ses appareils que ce soit un PC, un Mac, un smartphone ou une tablette sous Android. Ensuite il faut veiller à ne pas ouvrir des e-mails inconnus ou paraissant suspects et surtout ne pas cliquer sur un lien trop rapidement ni ouvrir la pièce jointe. Le conseil à retenir est de ne pas payer les rançons demandées, ce qui encourage les pirates et les entraîne à développer leurs logiciels malveillants.

Les actualités sur Torrentlocker

Le logiciel malveillant est en constante évolution, l'équipe de sécurité ESET a mis en place un livre blanc, où elle publie régulièrement leurs analyses et informe sur les nouvelles apparences que prend le logiciel au fil du temps, disponible sur www.welivesecurity.com.

Pour plus d'informations sur TorrentLocker, vous pouvez consulter le livre blanc sur
http://presse.marketing-land.com/r/?F=23e5g9n2ctsdr5hy9tpgyh7gqgazh6hj3y38q6ds3xp5zm8q23sfj4q-5686679

Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a6329542c28f29

Une attaque informatique endommage une usine métallurgique allemande

Une attaque informatique endommage une usine métallurgique allemande

Un rapport allemand publié jeudi a révélé une attaque informatique inédite contre une usine métallurgique. Le piratage a provoqué d'importants dégâts matériels sur un haut fourneau.

Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.
Les pirates ont pris le contrôle du réseau de l'usine après avoir obtenu les informations nécessaires à l'aide de techniques sophistiquées d'ingénierie sociale.
L'attaque a provoqué la défaillance de plusieurs composants qui ont empêché l'arrêt contrôlé d'un haut fourneau, endommageant l'infrastructure.

« Techniques très avancées »
Selon le rapport – qui ne donne ni le nom de l'usine, ni la date de l'attaque – les hackers disposaient de capacités techniques « très avancées » et ont démontré maîtriser également les processus de production et de contrôle industriels.
ITworld souligne que des intrusions à l'origine de tels dégâts restent rares, citant le ver Stuxnet qui avait visé les capacités de recherches nucléaires iraniennes, détruisant près de 1000 centrifugeuses.

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

Source : http://www.rts.ch/info/sciences-tech/reperages-web/6399258-une-attaque-informatique-endommage-une-usine-metallurgique-allemande.html

Les 5 tendances du Big Data en 2015

Les 5 tendances du Big Data en 2015

L'analyse prédictive de Craig Zawada, Chief Visionnary Officer chez PROS, sur… l'analyse prédictive ! PROS est un groupe américain qui édite des technologies Big Data conçues pour répondre au problématiques d'aide à la vente (pricing, générer des devis, anticiper des fluctuations de prix, de devises…). La société est arrivée en France cette année à travers le rachat du français Cameleon Software.

1. Le Big Data est mort vive le Big Data! En 2015, le buzz autour du mot "Big Data" va considérablement faiblir. En revanche, nous constaterons un intérêt grandissant pour les analyses prédictives et prescriptrives basées sur les données pour en faire de véritables actifs pour l'entreprise. Ce sont ces analyses qui permettent aux entreprises d'améliorer leurs prises de décisions quant à la relation client et à l'optimisation de leurs revenus. Les dirigeants ne cherchent pas forcément à recueillir plus de données, mais plutôt à leur donner de la valeur et les analyser pour identifier de nouvelles segmentations et créer des ventes supplémentaires.

2. «La science des données » devient une science parmi d'autres. Au fils des ans, le terme de « science des données » a été associé aux outils et aux logiciels. En 2015, nous devrions observer un retour à ses racines scientifiques : écouter l'entreprise pour émettre des hypothèses, les tester grâce aux données, observer les résultats et recommander une solution. Nous verrons donc un retour aux principes fondamentaux de la méthode scientifique.

3. Les Chief Data Officers (CDO) ne sont pas légion en dehors de la Silicon Valley, mais la gouvernance des données l'est. Les sociétés de la Silicon Valley reposant sur des données, comme Yahoo, ainsi que la ville de San Francisco ont ouvert la voie à l'émergence des CDO. Au-delà de ses frontières, vous trouverez peu ce type de profil. En 2015, la nécessité d'organiser la gouvernance des données se fera ressentir car les données ne sont plus une simple opportunité pour l'entreprise mais un véritable actif de l'entreprise.

4. Aider les équipes commerciales grâce à l'analyse prédictive. Vendre n'a jamais été aussi complexe, et 2015 apportera son lot de nouveaux défis. Les entreprises qui investiront dans l'analyse prédictive et prescriptives seront armées pour mieux négocier et optimiser leur revenu. Selon l'enquête annuelle de PwC, les dirigeants ne sont pas confiants quant aux perspectives de croissance et investir dans leur base clients est la priorité n°1 pour l'année à venir.

5. Les industries dont les produits dépendent du pétrole et de dérivés de pétrole vont connaître une pression croissante des prix représentant de véritables opportunités pour certaines entreprises ou bien des challenges pour celles n'y prêtant pas attention. Beaucoup de sociétés dont les produits sont fabriqués à base de dérivés du pétrole ou des polymères profitent de la fluctuation des cours pour augmenter leur rentabilité. Mais dans de nombreux secteurs, comme la chimie ou le transport, la volatilité des prix représente un grand défi et peut entraîner des baisses de rentabilité spectaculaire. En 2015, les prix seront très variables. Les fournisseurs doivent s'attendre à des fortes pressions de leurs clients pour indexer les prix en fonction de la fluctuation du marché. Les fournisseurs doivent connaître la rentabilité de chaque client afin de savoir s'ils peuvent ou non baisser leurs tarifs, et non leurs marges. L'intelligence consistera à maintenir de manière sélective des prix élevés, tout en restant rentable et compétitif.

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

Source : http://www.solutions-logiciels.com/actualites.php?titre=Les-5-tendances-du-Big-Data-en-2015&actu=15228

Protection de la vie privée : pas avant 2025, au mieux !

Protection de la vie privée : pas avant 2025, au mieux !

Une étude menée par Pew Research Center a posé la question a plus de 2500 experts et politiciens sur la création d'un cadre unique pour garantir la protection des données privées tout en facilitant l'innovation et le business des entreprises.

Le Pew Research Center a mené une enquête originale pour connaître l'opinion de plus de 2500 experts techniques et des politiciens sur l'avenir du respect de la vie privée. Concrètement, l'étude s'interrogeait sur la capacité des législateurs et développeurs à créer un cadre capable de garantir la vie privée d'ici 2025. Ce cadre devra à la fois simplifier l'innovation et la monétisation des applications, tout en offrant aux utilisateurs des options de sauvegarde de leurs données personnelles.
L'opinion des experts est divisée. 55% des répondants ne croient pas qu'un tel cadre puisse voir le jour dans la prochaine décennie. Mais 45% sont plus optimistes sur sa création et son acceptation. Par ailleurs, si les avis sont tranchés sur l'avenir de la confidentialité des données personnelles, il existe un consensus pour souligner que la vie en ligne est par nature publique. Il s'agirait donc bien d'un problème d'éducation de l'utilisateur, mais aussi du comportement des sites qui promettent plus de facilité contre des informations privées. L'étude qui cite Bob Briscoe, chercheur sur l'infrastructure et le réseau chez British Telecom, estime que cette facilité et ce confort sont à l'origine de l'absence de préoccupations des utilisateurs sur leurs données personnelles.

Un souci de définition, des outils de chiffrement nécessaires
Pour Joe Wilbanks, responsable de Sage Bionetworks revient sur le cadre général en constatant que 10 ans c'est trop court pour le législateur d'ajuster les règlements face à la rapidité des évolutions technologiques. D'autres comme Nick Arnett, expert en BI chez Buzzmetrics, confie que les définitions de « liberté » et de « vie privée » vont changer dans la société d'ici 2025 et il y aura souvent des désaccords sur ces transformations. Idem pour Homero Gil de Zuniga, directeur de recherche Digital Media à l'Université du Texas à Austin qui pense que « l'information sera encore plus omniprésente, plus fluide et portable. Les sphères publiques et privées numériques vont probablement se chevaucher ». Ce qui lui fait dire que ce qui est privé aujourd'hui ne le sera peut-être pas demain.
Peter Suber, directeur d'un projet d'accès illimité à la recherche (Open Access), prévient que pour créer un cadre unifié et acceptable, il y aura au préalable une course aux technologies qui favorisent la vie privée et la sécurité. Il ajoute que cette phase est en cours aujourd'hui avec le développement du chiffrement. Il reste des efforts à mener néanmoins sur la sécurité des données personnelles qui n'est pas du seul fait des entreprises.

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

Source : http://www.silicon.fr/donnees-personnelles-un-cadre-unique-en-2025-est-il-utopique-104490.html
Par Jacques Cheminat

Reprenez le contrôle de votre identité en ligne

Reprenez le contrôle de votre identité en ligne

Quand on s'inscrit avec un des géants du web comme Google ou Facebook. On souscrit à beaucoup plus qu'un seul service. On peut par exemple utiliser les mêmes identifiants pour s'enregistrer partout sur le web. C'est très pratique. Sauf que si votre compte se fait un jour pirater ou supprimer, vous perdez votre mail et tous les accès aux différents services que vous utilisez. IndieHosters veut vous aider à reprendre le contrôle de votre identité en ligne sans perdre le côté pratique.

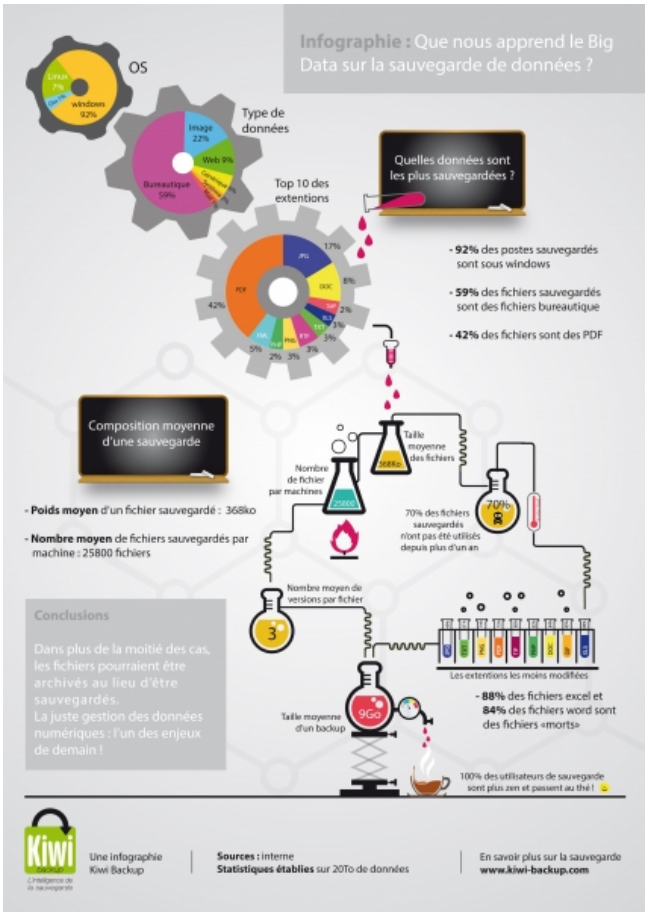
Il existe de nombreuses alternatives aux identifications de Facebook et Google. Elles s'appellent OpenID ou Mozilla Personna. Le problème avec ces outils, c'est qu'ils demandent d'être hébergés sur un serveur en ligne et qu'ils doivent être régulièrement mis à jour. Les compétences techniques demandées dépassent bien souvent les bases des internautes avertis et c'est une galère qui décourage même les utilisateurs les plus motivés.
Aujourd'hui, si vous allez chez un hébergeur connu comme OVH ou Gandi, vous aurez droit en un seul clic à une adresse mail, un hébergement pour un site web, une base de données et WordPress ou quelques logiciels libres.
IndieHosters veut aller encore plus loin en proposant tous les outils qui vous permettent de gérer votre identité en ligne. Et pour garantir la confidentialité des données, ils vous offrent en prime un certificat TSL (identique à celui utilisé pour les opérations bancaires en ligne par exemple). Vos données vous appartiennent et elles ne sont pas accessibles pour l'hébergeur. Et comme vous bénéficiez d'un serveur chez IndieHosters, vous pouvez également en profiter pour créer votre blog.

Lire la suite….

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

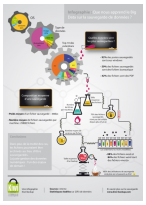
Source : http://www.gizmodo.fr/2014/12/18/reprenez-le-controle-de-votre-identite-en-ligne-avec-indiehosters.html

Sauvegarde des données et Big Data



Sauvegarde des données et Big Data

Infographie réalisée à partir de l'analyse de 20 To de données sauvegardées.
Que nous apprend le Big Data sur l'usage de la sauvegarde de données ?Des chiffres instructifs sont issus de cette analyse :
92 % des postes sauvegardés sont sous Windows,
Près de 60 % des fichiers sont des fichiers bureautiques (excel, word, PDF…),
42 % des fichiers sont des PDF,
70 % des fichiers sauvegardés n'ont pas été modifiés depuis plus de 1 an,
88 % des fichiers Excel et 84 % des fichiers Word n'ont pas été modifiés depuis plus de 1 an,
368 Ko : c'est le poids moyen d'un fichier sauvegardé,
9 Go : c'est le volume moyen d'un back-up.



Quelles conclusions peut-on tirer de cette infographie ?
Dans bien des cas, l'archivage serait plus approprié que la sauvegarde. Car pourquoi sauvegarder en incrémentiel un fichier qui ne bouge pas pendant des mois et peut être considéré comme un fichier « mort » ?
Le poids des PDF est extrêmement important et pourrait être réduit en sauvegardant les fichiers source uniquement et les PDF ayant une valeur juridique (contrats signés, devis,…)
Nous produisons beaucoup de fichiers bureautiques qui deviennent rapidement obsolètes et qui pourraient faire l'objet d'un « toilettage » plus régulier
La sauvegarde en ligne incrémentale est un outil puissant et complexe, permettant de sauvegarder plusieurs versions d'un même fichier sans augmenter l'espace de stockage nécessaire. Mais est-elle toujours utilisée à bon escient ? Une révision des critères de sauvegarde devrait être réalisée à intervalle régulier afin de ne pas engorger le cloud de fichiers qui ne seront jamais restaurés.

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

Source : http://www.journaldunet.com/solutions/expert/59471/sauvegarde-de-donnees-et-big-data.shtml

---

Denis JACOPINI et son équipe considère la sauvegarde comme la colonne vertébrale du système informatique. En ces temps quasiment 100% numériques, en cas de sérieux problème (panne, erreur de manipulation, acte malveillant, sinistre), la sauvegarde deviendra la source d'information la plus précieuse au monde.
Selon Denis JACOPINI, une sauvegarde de données doit être :
Automatisée : Pour ne plus oublier de sauvegarder, pour que la machine, bête comme une machine, y pense à notre place.

Contrôlée : J'ai rencontré trop de cas ou pendant des années des professionnels, avaient des systèmes de sauvegardes sur lesquels rien ne se sauvait, une panne avait interrompu le processus de sauvegarde depuis plusieurs mois ou pire, ne sauvegardaient que les raccourcis.
C'est la raison pour laquelle nous accordons beaucoup d'importance à notre audit des besoins, en communication rapprochée avec les éditeurs des différents logiciels créeant de la donnée dans l'entreprise, pour mettre en corrélation le « A sauver », le « Sauvé ».
Nous formons ensuite le client sur l'interprétation des rapports de sauvegarde qu'il va lui même contrôler (s'il ne souhaite pas souscrire à notre offre de contrôle des sauvegardes par nos services). l devient alors à même de savoir que ça fonctionne parfaitement.
Lorsqu'un dysfonctionnement apparait, il en est immédiatement informé. Cette rapidité d'alerte permet ensuite d'avoir du temps pour analyser le problème et le résoudre.

Externalisée : Un vol de l'ensemble de votre matériel informatique et du système de sauvegarde ne , vous met pas à l'abris d'une perte de vos données, de même qu'un sinistre…
Externaliser vos sauvegarde tout en y apportant la sécurité adaptée, vous permettra, même en cas de perte ou de destruction totale de votre système informatique, d'avoir accès à vos données à distance et de pouvoir recommencer à travailler en un temps record.

Historisée : En sauvegardant vos données sur plusieurs supports que vous faites tourner (le nombre de support dépendra du niveau de sécurité souhaité), vous pourrez, selon les paramètres choisis, retrouver un fichier effacé depuis plusieurs mois, qui ne se trouve évidemment plus sur les sauvegardes récentes. Cette fonction est très utile lorsque des données sont régulièrement effacées des systèmes informatiques. Il permet de retrouver le contenu d'une sauvegarde antérieure.

Parmi l'ensemble des logiciels gratuits et payants testés, nous avons à ce jour trouvé un produit qui non seulement regroupe l'ensemble des exigences répertoriées ci-dessus, mais également a été testé sur des nombreuses installations, plateformes et ne nous a toujours donné satisfaction.
Il peut sauver sur n'importe quel support, local réseau, ftp, cloud… et vous envoie le rapport de sauvegarde par e-mail. Des solutions existent même pour que vous soyez alerté des sauvegardes par SMS.
En plus, pour moins de 50 euros, je ne peux que vous conseiller ce produit : SyncBack

---

Espionnage Industriel par le Net : nouvelle victime

Espionnage Industriel par le Net : nouvelle victime

La fuite sur Internet d'emails sur la stratégie et les acquisitions de Snapchat a porté un coup sévère au moral de son patron et fondateur, Evan Spiegel.

Evan Spiegel, le PDG de Snapchat, est une victime collatérale du piratage de Sony Pictures et des fuites de données consécutives. Des emails du dirigeant du studio de cinéma ont été divulgués. Or, celui-ci, en tant qu'administrateur de Snapchat, avait accès à des données confidentielles, qui depuis ne le sont plus tellement.
Et Evan Spiegel a semble-t-il du mal à digérer. Le patron de l'application mobile s'est dit à la fois en colère et dévasté que des informations relatives à la stratégie et au plan de développement de la startup aient ainsi été dévoilées sur Internet.

Le secret indispensable à une startup
« J'ai eu le sentiment que j'allais pleurer toute la matinée, alors je suis sorti marcher et penser à certaines choses » écrit le dirigeant de Snapchat dans un mémo adressé aux salariés de l'entreprise américaine – puis mis en ligne ensuite sur Twitter.
Mais aux Etats-Unis, tout finit presque à ressembler à un scénario hollywoodien… « J'ai même rencontré un de mes professeurs de design du secondaire. Elle m'a serré très fort dans ses bras. J'en avais vraiment besoin » ajoute ainsi Evan Spiegel.
Les fuites sur Snapchat révélaient donc notamment que l'entreprise avait refusé une offre de rachat de trois milliards de dollars de Facebook, mais aussi qu'elle avait procédé à plusieurs acquisitions pour plusieurs millions de dollars, notamment dans le domaine des objets connectés.
« Nous gardons le secret car nous arrivons à faire notre travail libre de tout jugement – jusqu'à ce que nous soyons prêts à le partager. Nous avons des secrets car cela vous donne la possibilité de changer d'avis jusqu'à ce que vous soyez sûr d'avoir fait le bon choix » commente encore le PDG de Snapchat.

Keeping Secrets

I've been feeling a lot of things since our business plans were made public last night. Definitely angry. Definitely devastated.

I felt like I was going to cry all morning, so I went on a walk and thought through a couple of things. I even ran into one of my high school design teachers. She gave me a huge hug. I really needed it.

And I really need to tell you that I'm so proud of all of you. I want to give you all a huge hug because keeping secrets is exhausting.

Keeping secrets means coming home late, after working all day and night. Curling up with your loved ones, hanging out with your friends, and not being able to share all of the incredible things you're working on. It's painful. It's tiring.

Secrets also bring us together.

We keep secrets because we love surprising people. We keep secrets because it's the best way to keep showing the world that growth is not only possible, it's necessary. We keep secrets because it's the right thing to do, not because it's the easy thing to do.

We keep secrets because we get to do our work free from judgment – until we're ready to share it. We keep secrets because keeping secrets gives you space to change your mind until you're really sure that you're right.

We care about taking the time to get things right. Secrets help us do that.

Secrets keep the space between our community and the public – space that we need to feel safe in our expression and creativity.

I am so sorry that our work has been violated and exposed.

A couple of people have asked me what we're going to do.
First we're going to be really mad and angry and upset. And that's ok.

It's not fair that the people who try to build us up and break us down get a glimpse of who we really are. It's not fair that people get to take away all the hard work we've done to surprise our community, family, and friends.

It's not okay that people steal our secrets and make public that which we desire to remain private.

When we're done being mad and angry and upset we're going to keep doing exactly what we are doing. And then we're going to do it ten times better.

We're going to change the world because this is not the one that we want to live in.

Evan Spiegel
December 17, 2014

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

Source : http://www.zdnet.fr/actualites/le-patron-de-snapchat-en-colere-et-devaste-39811579.htm

Vol de données : tous les coups sont permis pour piller l’économie française

Vol de données : tous les coups sont permis pour piller l’économie française

Vol d'ordinateur dans des chambres d'hôtel, disparition de brevets dans le Thalys entre Paris et Bruxelles, pénétration d'agents à l'occasion d'une visite, piratage de technologies… Alors qu'une crise endémique tenaille le pays et réveille les appétits les plus féroces, des fleurons de l'économie française font l'objet d'un pillage vertigineux. Animé par un cynique théâtre d'ombres que ne renierait guère John le Carré, il prendrait même depuis vingt ans une forme industrielle. Cet édifiant état des lieux émane d'un rapport choc de la délégation parlementaire au renseignement, composée de parlementaires tous habilités au «secret-défense» et emmenés par le président de la commission des lois à l'Assemblée, le député (PS) Jean-Jacques Urvoas, qui vient d'effectuer une plongée au cœur des services de renseignements et de la sécurité nationale. Ce document de 175 pages, porté à notre connaissance, pointe une «plurivoracité de la prédation économique» liée à une «technicisation de l'espionnage» mais aussi l'«utilisation croissante du vecteur Internet».

Ainsi, l'année dernière, la seule Direction générale de la sécurité intérieure (DGSI) a recensé des «cas d'ingérence», notamment dans le domaine de «la recherche fondamentale, où la culture de la protection est particulièrement faible, mais également dans l'aéronautique et la santé». Dès septembre 2011, les policiers spécialisés de la sous-direction de la protection du patrimoine économique, basée à Levallois-Perret, avaient révélé dans nos colonnes l'existence de près de 5 000 «cas» en quatre ans. Durant cette période, 3 189 entreprises ont été visées. À ce petit jeu, une cohorte de prédateurs occultes pilotée en sous-main par des agences étatiques ou des multinationales s'attaquait à la grande entreprise comme à la plus petite «pépite».

À ce titre, rappelle le rapport de la DPR, «nos principaux partenaires peuvent aussi être nos meilleurs adversaires dans le domaine économique». Sans les citer, les spectres de grandes puissances comme la Chine ou la Russie se profilent entre les lignes. En février dernier, le groupe Safran a été contraint d'épaissir sa cuirasse après des cyberattaques des sites d'une de ses filiales, le motoriste Snecma. «D'une ampleur limitée» et vite décelée, l'intrusion d'origine indéterminée avait conduit les services de sécurité à neutraliser puis retirer une dizaine d'ordinateurs du réseau de l'entreprise. L'Île-de-France, où 144 cas d'ingérence ont été mis au jour en 2013, concentre près de 20 % des attaques. Les secteurs les plus ciblés étant l'aéronautique, l'énergie nucléaire, les télécommunications, l'aérospatiale, la robotique et les machines-outils.

Le droit, un outil de prédation

«Au-delà de cet espionnage industriel dont l'existence est connue, mais dont les méthodes continuent malheureusement de surprendre des entreprises et des administrations insuffisamment armées, il serait naïf d'oublier que les principales ingérences empruntent aujourd'hui des voies légales», précise le rapport, qui brocarde sans détour les États-Unis, lesquels – ce ne sont pas les seuls – utilisent le «droit comme un puissant instrument de prédation». Ainsi, le rapport détaille la redoutable procédure Discovery, fondée sur le principe fondamental de la common law américaine permettant à un «plaignant d'adresser des demandes de pièces au défendeur afin de cibler son action en justice». Or, les demandes s'avèrent bien souvent extraordinairement vastes (d'où leur surnom de fishing expeditions, «parties de pêche») et peuvent procéder d'une volonté de profiter de cette procédure pour se livrer légalement à de l'espionnage économique. Il en est de même pour le deal of justice, qui permet au Department of Justice (DOJ) d'éperonner de grandes entreprises pour infraction aux lois états-uniennes en matière de corruption qui «s'appuie principalement sur le Foreign Corrupt Practices Act de 1977 et sur les lois de sanctions économiques contre des pays (Cuba, Iran, Libye, Soudan, Syrie…)».

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger.

«Dans 90 % des cas, il s'agit d'entreprises étrangères, dont certains grands groupes français, à l'image de la récente affaire impliquant BNP Paribas», souligne le rapport. La banque, accusée de transactions avec des pays sous embargo économique américain, avait accepté le 30 juin, devant un tribunal de New York, deux chefs d'accusation: «falsification de documents commerciaux» et «collusion» avant d'écoper de 6,5 milliards d'euros d'amende. «L'entreprise doit reconnaître sa culpabilité et négocier le montant de l'amende infligée. En contrepartie, le DOJ renonce aux poursuites pour une période de trois ans, période pendant laquelle l'entreprise doit faire preuve d'un comportement exemplaire, note le rapport. Pour prouver sa bonne foi, et là réside le principal problème, elle doit accepter la mise en place d'un moniteur en son sein, moniteur qu'elle choisit mais dont la désignation définitive est soumise à l'approbation des États-Unis. Le moniteur aura accès à l'intégralité des informations de l'entreprise afin de rédiger un rapport annuel extrêmement détaillé.»

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger. Ou encore, ce qui n'est pas la moindre affaire, dévoiler les démarches concurrentielles à l'étranger. Or, révèle la délégation parlementaire, les services secrets américains peuvent «solliciter toute information nécessaire, y compris les rapports de monitorat» en invoquant le Foreign Intelligence Surveillance Act. En clair, le droit sert de bélier pour forcer la protection et les espions passent derrière pour siphonner le savoir-faire français. Selon nos informations, un grand groupe énergétique français et un tycoon pétrochimique allemand ont récemment subi pareil traitement après avoir versé plusieurs milliards de dollars. Alors qu'aux États-Unis les services secrets et le business entretiennent des relations fusionnelles et souvent consanguines, au point que la CIA a créé et gère le fonds d'investissement In-Q-Tel permettant de capter de précieuses informations concurrentielles. Une source informée confie qu'une PME française développant un logiciel performant a été «tamponnée», sans succès, par cette structure qui lui proposait d'entrer dans son capital.

Proposition de loi sur le secret des affaires

Parmi les propositions très concrètes formulées pour défendre le système immunitaire des entreprises françaises, la Délégation parlementaire au renseignement suggère de jeter enfin les bases d'un dispositif national protégeant le secret des affaires. Évoquée de façon éparse et fragmentaire dans la charte des droits fondamentaux de l'Union européenne, le Code du commerce ou celui des postes et télécommunications, cette notion «n'a pas d'existence juridique stabilisée ni de définition uniforme», note le rapport. Ainsi, en droit, la définition du vol n'intègre pas les biens immatériels. Et, pour l'heure, le délit de révélation d'un secret de fabrique ne concerne que les seuls salariés de l'entreprise. Face à un arsenal répressif lacunaire, Jean-Jacques Urvoas a donc concocté une proposition de loi, déposée en juillet dernier et présentée mercredi devant le Medef, permettant d'inscrire dans le Code du commerce un titre en neuf articles sur le «secret des affaires». Protégeant le potentiel scientifique et technique, les positions stratégiques, les intérêts commerciaux et financiers ainsi que la capacité concurrentielle des entreprises, cette loi prévoit des sanctions pouvant aller jusqu'à sept ans d'emprisonnement et 750.000 euros d'amendes dès lors que la souveraineté nationale est en jeu.

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

Source : http://www.lefigaro.fr/conjoncture/2014/12/18/20002-20141218ARTFIG00005-espionnage-comment-on-pille-l-economie-francaise.php
par Christophe Cornevin

Confidentialité des donnés : 71 % des employés déclarent

avoir accès à des informations qu’ils ne devraient pas voir

	**Confidentialité des donnés : 71 % des employés déclarent avoir accès à des informations qu’ils ne devraient pas voir**

Une enquête de Ponemon Institute pour la société Varonis systems Inc révèle que les employés disposant d'accès excessifs aux données de l'entreprise représentent un risque de fuites. Cependant, moins d'un collaborateur sur quatre estime que leur entreprise accorde une priorité très élevée à la protection de ses données.

Une étude* commandée par Varonis Systems Inc, une société qui fournit des solutions logicielles pour les entreprises, et réalisée par le Ponemon Institute, un centre de recherche sur la confidentialité, la protection des données et les politiques de sécurité de l'information, révèle que la plupart des entreprises rencontrent des difficultés à trouver l'équilibre entre un besoin de sécurité renforcée et les exigences de productivité des salariés. L'étude précise que les employés qui disposent de privilèges excessifs d'accès aux données représentent un risque croissant pour les entreprises en raison de l'exposition accidentelle et intentionnelle d'informations sensibles ou critiques. 71 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient pas pouvoir consulter et 54 % de ces utilisateurs caractérisent ces accès comme fréquents ou très fréquents.

Productivité contre sécurité

Les informaticiens comme les utilisateurs finaux témoignent d'un manque de contrôle en ce qui concerne l'accès aux données et leur utilisation par les employés. Les deux groupes conviennent généralement du fait que leur entreprise préférerait négliger les risques de sécurité plutôt que sacrifier la productivité. Seulement 22 % des collaborateurs ayant participé à l'enquête estiment que leur entreprise accorde une priorité très élevée à la protection de ses données. Moins de la moitié des employés pensent que leur société applique des politiques de sécurité strictes en ce qui concerne l'utilisation et l'accès aux données.

Des fuites dues à la malveillance des collaborateurs

Les conclusions de l'enquête indiquent également que les informaticiens et les utilisateurs finaux s'accordent sur le fait que les comptes d'employés détournés pouvant conduire à des fuites de données sont très probablement le fait de collaborateurs internes disposant d'accès excessifs et souvent inconscients des risques que ceux-ci représentent. 50 % des utilisateurs finaux et 74 % des informaticiens estiment que les erreurs, les négligences ou la malveillance d'employés sont fréquemment ou très fréquemment à l'origine des fuites de données. Et seulement 47 % des informaticiens indiquent que les employés de leur entreprise prennent des mesures appropriées pour protéger les données auxquelles ils accèdent.

Dans le même temps, 76 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations de l'entreprise telles que des données relatives aux clients, des renseignements sur les collaborateurs, des rapports financiers et des documents commerciaux confidentiels. Et, 76 % des utilisateurs finaux jugent qu'il est parfois acceptable de transférer des documents de travail sur leurs périphériques personnels, alors que seulement 13 % des informaticiens en conviennent.

*Le rapport d'étude intitulé "Données : actifs protégés ou bombe à retardement ?" se fonde sur des entretiens menés en octobre 2014 auprès de 2 276 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne.

Source : http://www.courriercadres.com/carriere/internet-et-l-entreprise/securite-des-donnes-71-des-employes-declarent-avoir-acces-15122014

Par Audrey Pelé

Votre smartphone vous épie à

votre insu

Votre smartphone vous épie à votre insu

Une nouvelle étude de la Cnil publiée ce lundi souligne que deux tiers des applications pour smartphones collectent des informations personnelles auxquelles elles ne devraient pas avoir accès et sans que les utilisateurs en aient conscience. L'étude démontre que nos téléphones sont devenus de vrais petits espions domestiques.

Un nouveau rapport de la CNIL (Commission nationale de l'informatique et des libertés) publié ce lundi montre que les accès aux données personnelles des utilisateurs sont massifs et peu visibles par le citoyen mal informé. Deux applications sur trois captent des informations personnelles à l'insu des utilisateurs. Et l'augmentation du temps passé par les citoyens (de 2 à 4 heures par jour) sur leur portable augmente les risques de fuites de ce type de données.
La CNIL appelle de nouveau les éditeurs d'applications et leurs fournisseurs de services ou partenaires commerciaux à intensifier leur effort d'information des utilisateurs, sans s'abriter derrière des contraintes techniques. Apple, Google, Microsoft, Mozilla seraient les premiers visés.
La CNIL soulignait déjà en 2011 que la confidentialité des données personnelles des internautes n'est pas respectée par les géants du Web. Mais la tendance se renforce. La CNIL a conduit cette nouvelle étude avec l'aide de l'Inria, qui a installé l'outil d'analyse Mobilitics sur des Smartphones que des agents de la CNIL ont utilisé à la place de leurs téléphones personnels. L'étude, menée pendant trois mois, a passé au crible 121 applications Android (plus de 70% du marché des smartphones en France). Et les résultats sont édifiants.
L'étude a permis de dégager trois éléments majeurs. Les identifiants techniques, matériels ou logiciels sont utilisés à des fins publicitaires dans plus de 50% des cas. Les smartphones sont également de vrais « GPS de poche » et certaines applications ne se privent pas d'accéder à ces données qui dévoilent où nous nous trouvons, même lorsque l'abonné n'est pas en train d'utiliser l'application en question. La géolocalisation représente 30% des données collectées chez les utilisateurs. Parmi les 121 applications scrutées par la Commission, cinq ont même accédé au numéro de téléphone de l'utilisateur et deux ont pu récupérer la liste des identifiants des points d'accès WiFi à portée de l'utilisateur.
Si vous croyez encore que le maître à bord de votre smarthpone c'est vous, ce dernier élément va achever de vous convaincre. L'éditeur du système d'exploitation définit ce que les éditeurs d'applications sont autorisés à collecter ou non. Et si la CNIL condamne de nouveau les utilisations outrancières qui sont faites des données personnelles, elle a en réalité peu d'influence face au poids économique que représente pour les géants du Web la collecte de nos données personnelles.

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

Source : http://www.francesoir.fr/societe-science-tech/votre-smartphone-vous-epie-votre-insu
par la rédaction de FranceSoir.fr