Coopération Internationale : Le Cap-Vert adhère à la Convention sur la Cybercriminalité

Coopération Internationale : Le Cap-Vert adhère à la Convention sur la Cybercriminalité

Praia, Cap-Vert – Le Cap-Vert vient d'adhérer à la **Convention sur la cybercriminalité**, créant ainsi les conditions de doter l'archipel de législation nécessaire pour punir ce type de délit, a appris la PANA de source officielle.
Cette Convention était réclamée par les Cap-verdiens, vu l'absence de législation qui permet de punir la cybercriminalité, ce qui a fait que plusieurs personnes ont été victimes de calomnie et de diffamation sur Internet, à travers des commentaires sur les sites d'informations et de blogs online.

La Convention sur la cybercriminalité, approuvée à Budapest (Hongrie) en 2001, réserve à chaque État adhérant la possibilité de produire une législation pour classer les infractions par dommages relatifs à la suppression des données informatiques, au sabotage, à l'utilisation indue de données, à la pornographie infantile, entre autres pratiques illégales.
Elle préconise aussi des infractions concernant la violation du droit d'auteur et aussi les responsabilités et sanctions proportionnelles et dissuasives, dont les peines privatives de liberté.

Toutefois, dans le cas du Cap-Vert, le pays devra aussi créer les conditions pour que les autorités compétentes puissent conserver les données informatiques, dont celles stockées, surtout quant il y a de sérieux risques de perte ou d'altération.
Il est aussi de la responsabilité de l'État du Cap-Vert d'adopter des mesures législatives nécessaires pour permettre aux autorités compétentes d'effectuer des recherches et des saisies de données informatiques stockées.
La Convention sur la cybercriminalité stipule aussi que: "chaque partie devra adopter des mesures législatives nécessaires pour obliger un prestataire du service à garder la confidentialité'.

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

Source : http://www.afriquejet.com/afrique-ouest/13826-informatique-et-cybercriminalite-le-cap-vert-adhere-a-la-convention.html

---

Un logiciel malveillant caché dans le chargeur d'une

cigarette électronique

Un logiciel malveillant caché dans le chargeur d'une cigarette électronique

Selon des experts interrogés par The Guardian, si le véhicule de l'attaque est inédit, l »anecdote » en elle-même n'a rien de surprenante : les différents supports USB sont fréquemment à l'origine de virus informatiques.

Décidément, on ne peut plus se fier à rien de nos jours ! The Guardian rapporte l'histoire d'un cadre d'une grande entreprise qui s'est fait piéger par un logiciel malveillant codé dans son chargeur de cigarette électronique. »L'ordinateur d'un des cadres était infecté par un logiciel malveillant dont la source ne pouvait être déterminée. Le système était à jour, avait un antivirus et disposait de tous les dispositifs anti-malwares. […] Au final, après avoir cherché du côté de tous les moyens d'infection traditionnels, le service informatique a cherché d'autres possibilités. Ils ont demandé au cadre: « Y a-t-il des changements dans votre vie récemment? » Et le cadre a répondu: « oui, j'ai arrêté de fumer il y a deux semaines et me suis mis à la cigarette électronique », témoigne un membre du personnel informatique de l'entreprise en question sur le site Reddit.

Selon des experts interrogés par The Guardian, si le véhicule de l'attaque est inédit, l »anecdote » en elle-même n'a rien de surprenante : les différents supports USB sont fréquemment à l'origine de virus informatiques. Les clefs USB sont d'ailleurs plus difficiles à pirater que les périphériques USB. Pour Pierre-Yves Bonnetain, consultant sécurité informatique interrogé par France Info, il faudrait remonter l'ensemble de la chaîne de production des cigarettes électroniques pour en savoir plus. »La chaîne de fabrication est relativement complexe. A un moment ou à un autre, quelque part dans la chaîne, il est parfaitement possible qu'un des ces soust-traitants approvisionnent des composants qui ont déjà été frabriqués en étant malveillants », explique-t-il.

En août, deux chercheurs allemands, Karsten Nohl et Jakob Lell, ont réalisé une expérience pour montrer comment il est possible de transformer le code qui permet de faire fonctionner le périphérique USB pour installer un virus sur l'ordinateur. La faille, nommée Bad USB, permettait de mémoriser n'importe quelle saisie sur votre clavier : mots de passe, numéros de carte bancaire… Et à l'heure actuelle, il existe malheureusement très peu de solutions pour se protéger de ce type de virus. Morale de l'histoire : évitez d'acheter des contrefaçons qui circulent sur le net !

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

Source : http://www.atlantico.fr/atlantico-light/cyber-piratage-logiciel-malveillant-cache-dans-chargeur-cigarette-electronique-1874188.html

---

Utilisation abusive de la

messagerie électronique : licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

	Utilisation abusive de la messagerie électronique : licenciement sans cause réelle et sérieuse en l’absence de déclaration préalable à la CNIL

Poursuivant sa construction jurisprudentielle extrêmement protectrice des droits personnels du salarié, la Cour de Cassation a rendu un nouvel Arrêt le 8 octobre 2014 (Cass. Soc 8 oct 2014 n° 13-14991) encadrant strictement le contrôle par l'employeur, de l'activité des salariés au travail.

En l'espèce, une salariée avait envoyé et reçu un peu plus de 1 200 mails personnels via sa messagerie professionnelle sur une période de deux mois.
L'employeur avait licenciée ladite salariée pour faute, au motif d'une utilisation excessive de sa messagerie professionnelle à des fins personnelles .

La jurisprudence bien établie de la Chambre Sociale de la Cour de Cassation considérait déjà qu'à défaut de déclaration à la CNIL d'un traitement automatisé d'information nominative en place dans l'entreprise, le licenciement fondé sur un tel grief est sans cause réelle et sérieuse.
Tel est le cas notamment du licenciement d'un salarié qui refuse d'utiliser le système de badge ou de pointeuse à l' entrée et sortie de l'entreprise: faute de déclaration préalable à la CNIL du système mis en place dans l'entreprise, l'employeur ne peut valablement sanctionner le salarié sur ce motif (Cass. Soc 6 avr. 2014 n° 01-45227)

Dans la présente espèce, l'employeur avait précisément réalisé cette déclaration à la CNIL.
Il avait toutefois déclaré le système de surveillance de la messagerie, non pas dès sa mise en service mais près de deux mois et demi après .
Or, ce dispositif avait servi, dès son installation, à mettre en lumière l'utilisation excessive par la salariée concernée de sa messagerie professionnelle à des fins professionnelles.
La Cour de Cassation a trouvé, dans cette espèce, l'occasion de durcir encore davantage sa jurisprudence en invalidant le licenciement de la salariée fondé sur une utilisation abusive de la messagerie électronique durant les deux mois ayant précédé la déclaration du dispositif de surveillance à la CNIL.
La Cour considérant que le système de surveillance étant antérieur à la déclaration à la CNIL, le moyen de preuve de l'employeur quant à la matérialité du motif de licenciement était donc illicite.

La Cour de Cassation indiquant précisément que :
« Constitue un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL ».

Cet arrêt ne fait qu'ajouter à l'arsenal existant de protection des droits des salariés dans l'entreprise à commencer par l'art L1222-4 du Code du travail qui dispose qu'aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance ou encore le fondamental art L1121-1 du Code du travail.

La Cour de Cassation s'estimant garante, en droit du travail, de la protection des droits fondamentaux des salariés poursuit sa jurisprudence protectrice des droits individuels du salarié qui ne s'arrêtent pas une fois la porte de l'entreprise franchie.
Par Me Sandrine PARIS-FEY
Avocat au Barreau de NANTES
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.juritravail.com/Actualite/motifs-personnels-de-licenciement/Id/172011

La protection des données personnelles largement ignorée par les professionnels européens de l’informatique

La protection des données personnelles largement ignorée par les professionnels européens de l’informatique

Vidéoprotection, contrôle d'accès…. la protection des données personnelles ne concerne pas que le eCommerce. Or selon un sondage récent, les acteurs européens ignorent l'arrivée imminente du Règlement général sur la protection des données dans le paysage réglementaire de 28 pays de l'Union d'ici à 2015. Malgré les fortes amendes que prévoit le dispositif envers les contrevenants…

Enquête en ligne menée par Ipswitch
sur un échantillon de 316 professionnels
de l'informatique. © Ipswitch

Selon une enquête d'Ipswitch, un éditeur américain de logiciels pour réseaux d'entreprise, une majorité de professionnels de l'informatique en Europe ne savent pas à quelle sauce ils vont être mangés en matière de gestion des données personnelles. En effet, les résultats semblent indiquer que les questions de réglementation et de conformité dans ce domaine sont largement méconnues. Un diagnostic qui s'applique tout particulièrement au Règlement général sur la protection des données (GDPR : General Data Protection Regulation), un texte qui devrait entrer en vigueur dans 28 pays de l'Union européenne entre la fin 2014 et le début de l'année 2015. Réalisée en ligne, en octobre 2014, l'enquête a recueilli la réponse de 316 internautes (104 du Royaume-Uni, 101 de France et 111 d'Allemagne).

Concrètement, plus de la moitié des personnes interrogées (56 %) n'ont pas pu identifier la signification du terme »GDPR ». De plus, 52 % d'entre elles ont admis qu'elles n'étaient pas préparées. Par ailleurs, plus d'un tiers (35 %) des sondés ignorent si les stratégies et processus informatiques mis en place au sein de leurs entreprises sont conformes à la nouvelle réglementation. À l'inverse, 13 % des personnes interrogées placent le GDPR dans leur liste des priorités et 12% seulement seraient prêtes au changement. L'enjeu est pourtant de taille alors que le GDPR prévoit de fortes amendes (jusqu'à 100 millions d'euros ou 5 % du chiffre d'affaires mondial) pour les organisations qui enfreindront les règles !

La France en milieu de podium

Par rapport à leurs homologues allemands et britanniques, les Français se placent dans la moyenne. Ils ne sont ni particulièrement en retard ni particulièrement en avance. D'un coté, les Britanniques se révèlent être les plus préoccupés par la sécurité des « images de nature personnelle » (7% contre seulement 3 % des Français et 2 % des Allemands). De l'autre, nos voisins germaniques semblent les mieux au courant de la problématique GDPR. En effet, près de la moitié d'entre eux (49 %) ont été capables de préciser la signification de l'acronyme. À l'inverse, seul 36 % des professionnels français a su l'indiquer contre un quart (26 %) des professionnels britanniques.

Les résultats de cette enquête doivent pourtant être utilisés avec précaution. En effet, Ipswitch passe sous silence bon nombre d'informations. Par exemple, la nature exacte des métiers exercés par les sondés n'a pas été précisée. Rappelons-le, la problématique des données personnelles touche en priorité les Directeurs et les Responsables de la sécurité des systèmes d'information (DSI et RSSI) des entreprises. Mais également les Centres de supervision urbains (CSU) qui opèrent les caméras de vidéosurveillance déployées en ville. Citons encore les entreprises qui sécurisent des accès physiques avec, par exemple, des équipements biométriques. Ainsi que toute organisation qui doit gérer de près ou de loin des informations d'identification (voir encadré : »Qu'est-ce-qu'une donnée personnelle? »). Avec l'explosion de l'informatique dans le nuage (Cloud Computing), nul doute que cette liste non exhaustive se rallongera de manière exponentielle dans les années à venir.

Qu'est-ce-qu'une donnée personnelle ?

En France, « constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. » (Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).

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-e2460ddaaa1c99bf0e47ce05b66a4a7e.htm
par Guillaume Pierre

La reconnaissance juridique du vol de données

La reconnaissance juridique du vol de données

Pour assurer la protection des droits fondamentaux des citoyens, aussi bien les droits positifs que sa protection contre les abus, le Conseil d'Etat préconise 50 mesures à prendre d'urgence.

Le vol de données, une notion mal définie. On entend régulièrement parler dans la presse aussi bien de « vols de données personnelles » de clients, commis au détriment d'opérateurs ou de grandes entreprises, que de « vols de données confidentielles » qui s'apparentent plutôt à de l'espionnage industriel. Dans ces dossiers, le terme de « vol » est utilisé par commodité de langage, mais il n'est pas toujours la qualification retenue juridiquement. En effet, pour qu'il y ait vol, selon la définition du Code pénal (article 311-1), il faut constater la « soustraction frauduleuse de la chose d'autrui ». Or dans un vol de données, celles-ci ne sont pas « soustraites », mais recopiées ; elles demeurent à la disposition de leur légitime propriétaire qui ne peut donc pas déposer plainte pour « vol ».

Cette définition du vol par la « soustraction » date du Code Napoléon (1804). Remarquons que le droit romain était peut-être paradoxalement mieux adapté au vol de données, car les Institutes de l'empereur Justinien, publiées en 529, définissaient plus largement le vol (furtum) comme « contractatio rei fraudulosa » : la manipulation frauduleuse d'une chose (livre IV, titre I, 1). Et de préciser « furtum autem fit, non solum cum quis intercipiendi causa rem alienam amovet, sed generaliter cum quis alienam rem invito domino contractat » : il y a vol, non seulement quand on déplace la chose d'autrui pour la dérober, mais de manière générale quand on en dispose sans la volonté du propriétaire (IV, I, 6).

Mais notre Code pénal moderne lie le vol à la disparition matérielle. Ainsi en avait jugé récemment le tribunal de grande instance de Créteil (23 avril 2013), qui rappelait que « en l'absence de toute soustraction matérielle de documents (…), le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques (du légitime propriétaire) qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose ».

Toutefois, la Cour d'appel de Paris a infirmé ce jugement (5 février 2014), et a considéré au contraire que le vol de données était bien caractérisé par le fait de réaliser « des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ». Suite à ces appréciations divergentes de l'applicabilité de l'incrimination de vol, ce dossier se retrouve désormais devant la Cour de cassation, dont la mission est justement de dire comment on doit appliquer le droit.
Il est à noter que la même Cour de cassation avait validé le 9 septembre 2003 une condamnation pour vol, basée sur le fait « d'avoir en sa possession, à son domicile, après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support du logiciel Self Card, sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire ». Elle a de nouveau validé le 4 mars 2008 une condamnation pour vol de données informatiques. Mais dans ces deux dossiers, la Cour n'a pas explicité comment l'incrimination de vol de données devait s'appliquer.

D'autres solutions juridiques
Lorsque l'on est victime d'un vol de données, d'autres solutions juridiques existent pour déposer plainte. Si les données copiées sont des données personnelles (relatives à des personnes identifiées ou identifiables), le recours à l'article 226-18 du code pénal (collecte frauduleuse de données personnelles) est possible.
Si le vol a été effectué via un accès frauduleux au système informatique (cas du hacking, du vol de mot de passe, du phishing…), l'article 323-1 du code pénal trouvera à s'appliquer.
Si c'est une base de données qui a été recopiée, son propriétaire peut réclamer la protection accordée par l'article L341-1 du code de la propriété intellectuelle, mais seulement si la constitution de la base a nécessité un investissement substantiel. La Cour de cassation a ainsi confirmé le 19 juin 2013 un arrêt refusant la protection d'une base de données en raison du caractère non substantiel des investissements réalisés.
Nouveaux éléments. L'arsenal juridique vient récemment de s'enrichir de deux nouveautés. Le 22 octobre 2014, dans une affaire de détournement de fichiers par un salarié, la Cour de cassation a validé la condamnation pour abus de confiance. Or l'article 314-1 du code pénal définit l'abus de confiance comme « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé ». N'étant pas des fonds ou des valeurs, on en déduit que pour la Cour de cassation les données sont des biens. Ce qui nous ramène à l'idée de vol : si les données sont des biens, la notion de vol de données devient plus naturelle.
Mais le législateur vient peut-être de rendre ces discussions inutiles. En effet, la loi antiterroriste du 13 novembre 2014 modifie l'article 323-3 du code pénal. Cet article, créé par la loi Godfrain de 1988, réprimait jusqu'ici l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression. Désormais, sont également interdits les faits « d'extraire, de détenir, de reproduire ou de transmettre » frauduleusement des données. La sanction encourue est de cinq ans de prison et 75.000 euros d'amende, et est portée à sept ans et 100.000 euros s'il s'agit de données personnelles volées dans un système d'information de l'Etat.
La nouvelle rédaction de l'article 323-3 permet donc de réprimer efficacement à l'avenir les vols de données. Elle rend inutile le recours à l'article 311-1 et les débats sur son applicabilité, d'autant plus que la sanction du vol « traditionnel » n'est que de trois ans de prison et 45.000 euros d'amende (article 311-3), soit moins que ce qui est prévu par le nouvel article 323-3 consacré aux données.

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

Source : http://pro.01net.com/editorial/633857/vers-la-reconnaissance-juridique-du-vol-de-donnees/
par Fabrice Mattatia

La collaboration transfrontalière, clé de la lutte contre la cybercriminalité

La collaboration transfrontalière, clé de la lutte contre la cybercriminalité

Europol vient d'annoncer l'interpellation d'une quinzaine d'individus, dont six français, suspectés d'avoir utilisé des chevaux de Troie pour perpétrer différents types de cyber-attaque. L'opération, pilotée par la France, a été réalisée en collaboration avec différents pays européens.

L'office de police intergouvernemental Europol, les forces de l'ordre françaises ainsi que six autres pays (Royaume-Uni, Estonie, Roumanie, Lettonie, Italie et Norvège) ont œuvré conjointement pour mettre la main sur quinze hackers. Jean-Pierre Carlin, directeur Europe du sud de LogRhythm, éditeur américain de logiciels de sécurité informatique basé dans le Colorado (Etats-Unis) et dont le siège social en France se trouve à Neuilly-sur-Seine (92), se félicite de cette collaboration transfrontalière. « Cette arrestation montre que nous sommes en train de rattraper notre retard sur les pirates informatiques, affirme-t-il. Nous disposons de davantage d'outils pour détecter l'origine des attaques et nous sommes capables de les tracer. Partager l'intelligence au-delà des frontières est la clé absolue. »

Coopération inégale

Car, jusqu'à présent, les forces de l'ordre détectaient les malware et les chevaux de Troie sans remonter à la source. Les hackers bénéficiaient donc d'un anonymat total. « Puis, la collaboration entre les pays s'est peu à peu tissée, ajoute Jean-Pierre Carlin. Mais tous les Etats ne coopèrent pas de la même façon. Les pays européens adhérents d'Europol travaillent main dans la main, mais pour les Etats-Unis et les états asiatiques, la donne est différente. »

Cependant, des opérations comme celles-ci ne peuvent être un succès que si les bonnes informations sont mises à disposition. Les organisations ont un rôle à jouer, celui d'assurer leur propre protection. « Toutes les entreprises doivent garantir la surveillance de la moindre activité sur leur réseau en temps réel, précise le directeur Europe du sud de LogRhythm. Avec une visibilité accrue, les comportements anormaux sont identifiés immédiatement et les informations collectées sont partagées avec les autorités pour arrêter les criminels. C'est la fonction de notre produit d'analyse LogRhythm Security Analytics. »

Caroline Albenois

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

Source : http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-1e13ba8f63fad9bbf651b6e811431989.htm

---

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

Sony Pictures victime d'une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

Les employés de la filiale du groupe japonais Sony Pictures Entertainment basée à Los Angeles ont eu une surprise des plus désagréables ce lundi 24 novembre 2014. En allumant leurs ordinateurs, une image représentant un squelette avec comme titre en rouge « Hacked By #GOP » (Gardians of Peace) apparaissait sur leurs écrans. Par la suite, les pirates passaient leur message : « nous vous avons déjà prévenu, et ceci n'est que le commencement. Nous continuerons jusqu'à ce que nos exigences soient satisfaites .» En cas de refus d'obtempérer, les pirates menacent de dévoiler à la face du monde des documents obtenus.

Depuis l'expiration de ce délai le 24 novembre 2014 à 23h GMT, plusieurs archives ont été publiées sur divers sites. Même si la plupart des liens ne fonctionnent pas, il est toujours possible de récupérer, sur Thammasatpress, un fichier au format zip de 207 Mo qui contient trois fichiers intitulés LIST1, LIST2 et « Readme ». Ce dernier se présente sous le format texte et contient des adresses électroniques. Pour les deux autres, ils semblent regrouper des documents financiers ainsi que des codes sources et des bases de données. Une analyse avec la commande GREP, dont le rôle est de rechercher un mot dans un fichier et d'afficher les lignes dans lesquelles ce mot a été trouvé, permet d'identifier des clés de chiffrement, mais aussi ce qui ressemble à des documents d'identité relatifs à certaines stars hollywoodiennes à l'instar d'Angelina Jolie.

La société n'était pas joignable pour commenter ces informations, mais un communiqué adressé au Hollywood Reporter indique que « Sony Pictures Entertainment a connu une perturbation de son réseau, et nous travaillons d'arrache-pied pour la résoudre ». Une source a confirmé « qu'un seul serveur a été compromis et l'attaque s'est propagée à partir de là ». Les employés ont été invités à rentrer chez eux après l'attaque : « nous allons tous travailler de la maison. Nous ne pouvons même pas aller sur internet » a déclaré un employé sous le couvert de l'anonymat. Ce dernier a confirmé que le département informatique de l'entreprise a demandé aux employés d'éteindre leurs ordinateurs et de désactiver le WiFi de leurs appareils mobiles, mais également qu'un message adressé aux employés a précisé que la résolution de cet incident pourrait prendre jusqu'à trois semaines.

Outre le blocage des ordinateurs de Sony Pictures, ce sont de nombreux comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.

Cependant, le magazine spécialisé The Verge avance avoir reçu un courriel de la part des hackers responsables de cette attaque qui dit « nous voulons l'égalité [sic]. Sony ne le veut pas. C'est une bataille ascendante ». D'ailleurs un tweet cinglant de la part de GOP a été adressé à Michael Lynton, le PDG de Sony Entertainments, sur le compte de Starship Trooper's où lui et le reste du staff ont été traités de « criminels ».

Selon The Verge, les pirates ont affirmé avoir réussi à infiltrer la société en travaillant « avec d'autres employés ayant des intérêts similaires » parce que « Sony ne verrouille pas ses portes, physiquement, ». Pour The Verge, cela peut impliquer que les pirates ont réussi à pénétrer les serveurs de l'entreprise avec l'aide de personnes ayant accès aux serveurs internes de Sony.
Sony Pictures quant à lui a choisi de rester sobre dans sa communication en se contentant de dire que « nous enquêtons sur un incident informatique ».

En août dernier, les pirates ont affirmé être venus à bout de PlayStation Network via une attaque par déni de service qui a inondé le système de données réseau erronées. Toutefois, l'entreprise a tenu à rassurer les utilisateurs en affirmant qu'aucune des données personnelles des 53 millions d'utilisateurs de la plateforme PlayStation Network n'a été compromise suite à l'incident daté du 24 août. D'ailleurs, les ingénieurs ont pu à nouveau rendre l'accès disponible dès le lendemain. En 2011, une brèche dans la sécurité de la même plateforme exposait les identifiants (noms d'utilisateur et mots de passe) des utilisateurs.
Source : bloomberg, the verge

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

Source : http://www.developpez.com/actu/77586/Sony-Pictures-victime-d-une-attaque-informatique-les-pirates-ont-publie-certaines-donnees-sensibles-apres-un-chantage/

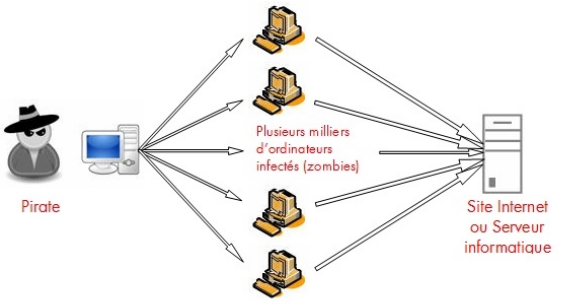
Dis papa, c'est quoi une attaque DDOS ?

Dis papa, c'est quoi une attaque DDOS ?

L'objectif d'une attaque DDOS, (en déni de service) vise à rendre inaccessible ou inopérant un site Internet. Parmi les attaques les plus fréquemment lancées, ce sont les attaques en déni de service distribué (DDoS : Distributed Denial of Service) qui sont les plus fréquentes.

Ce type d'attaque s'appuie sur un principe simple, celui du nombre qui fait la force : Il suffit de faire en sorte que plusieurs milliers machines sur Internet lancent de façon synchronisée de multiples requêtes vers leur cible.

Les machines lançant ces attaques peuvent le faire soit à l'insu de leur propriétaire (cas d'un « botnet » ou réseau de machines zombies) ou alors le font sur demande explicite et consciente d'une personne (cyber hacktivisme).



Le pirate active à distance tous les zombies (plusieurs milliers) préalablement infectés et leur donne l'ordre de contacter simultanément une cible. Au bout de quelques minutes, cette cible ne peut plus répondre à de nouvelles connexions, elle devient inaccessible.

Saturation des ressources

Dans le deux cas, le résultat est le même : les capacités de traitement du site sont dépassées, celui-ci est inaccessible. La saturation peut concerner tant la bande passante de l'accès réseau, des tables de session d'un firewall, la CPU des serveurs web, …

En fonction du point de saturation, on peut constater un effet boule de neige : Si c'est la bande passante réseau qui est totalement consommée inutilement alors, non seulement le site visée par l'attaque sera bloqué mais tous les autres serveurs de la plateforme seront aussi inaccessibles.

Le trou-noir (« blackholing ») à la rescousse

Le trou-noir est l'une des contre-mesures utilisée communément pour contrer une attaque en DDoS. Le fournisseur d'accès Internet va activer, au sein de son réseau, une règle de routage spécifique afin de détruire tous les flux à destination de l'adresse IP ciblée par l'attaque.

Cela aura pour effet immédiat de bloquer les flux d'attaques en amont de l'accès réseau et donc d'annuler tout effet de saturation. Activer un blackholing ne nécessite aucun équipement spécifique car tout est réalisé via les fonctions de routage de paquets nativement présentes dans les équipements réseau.

Pour se protéger d'une attaque de ce type, plusieurs solutions existent, le blackholing en est une, la plus simple à mettre en oeuvre, mais comme à chaque fois, quand le voleur s'est fait piéger en rentrant par la porte, la prochaine fois il rentrera par la fenêtre ou ailleurs…

Vous avez été victime d'une attaque DDOS ?
Vous souhaitez mettre en oeuvre une protection ?
Profitez de notre expertise et consultez-nous

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

Source : http://www.orange-business.com/fr/blogs/securite/series/les-5-minutes-du-professeur-audenard-episode-3-cleanpipe-bgp-et-gre

Les sites Internet de la Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

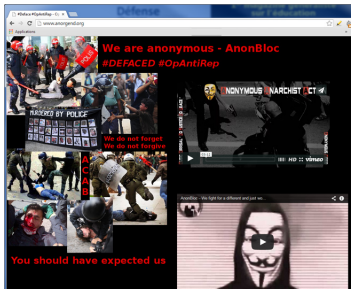
Les sites Internet de la Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

Aux manifestations organisées partout en France samedi dernier contre les violences policières se sont jointes des opérations menées en ligne par un collectif affilié à Anonymous. Des bases de données sur des Gendarmes ont été publiées, et des sites ont été piratés.

Les manifestations en hommage à Rémi Fraisse et contre les violences policières qui se sont déroulées samedi dernier dans une vingtaine de villes françaises ont également connu un relais immatériel. Dans le cadre d'une action mondiale « contre les répressions policières » baptisée #OpAntiRep, un collectif de hackers anonymes utilisant la bannière Anonymous a réalisé samedi une série d'actions, en particulier contre les policiers et gendarmes italiens, mais également en France.

Outre d'habituelles attaques DDOS qui ont provoqué l'indisponibilité d'une vingtaine de sites internet, dont celui du syndicat de policiers Alliance http://anorgend.org, le collectif a surtout piraté le forum d'un site internet dédié aux réservistes de la Gendarmerie http://www.reserve-gendarmerie.org, destiné à « faire connaître la réserve et à mettre en relation les réservistes et candidats ». Ils affirment avoir réussi à pirater les noms, adresse e-mail, adresse IP et mot de passe (pour certains déchiffrés) de quelques 2 000 membres inscrits sur ce forum, et fournissent une capture d'écran de la base de données en guise de preuve :

Ce lundi, le site non officiel de la réserve de la Gendarmerie française était toujours fermé, un message expliquant aux visiteurs qu'il était « en maintenance ». Le forum est toutefois accessible, et affiche 1544 membres inscrits à l'heure où ces lignes ont été publiées sur le site source.
D'autres actions ont été menées, notamment contre le site de l'Association nationale des officiers de réserve de la Gendarmerie nationale (Anorgend), qui a été piraté pour en modifier la page d'accueil, désormais toute à la gloire d'Anonymous. Là aussi, une base de données de membres avec des mots de passe chiffrés a été diffusée :

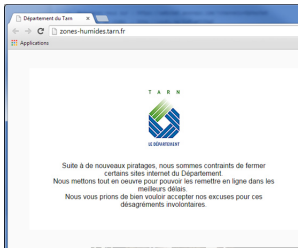


Dans un communiqué diffusé dans trois langues, le collectif #OpAntiRep explique que la journée du 22 novembre avait « pour origine des collectifs – occupants de différentes ZAD (Zones à défendre) – suite au décès par grenade offensive d'un étudiant en écologie lors d'un rassemblement », et affirme que « partout dans le monde, de nombreux camarades ont été tués ou blessés par leurs armes dans des manifestations contre l'oppression de ces gouvernements,sous la pression du monde capitaliste qui veut imposer ses projets de société ». L'appel à manifester partout dans le monde avait été relayé sur un site anarchiste.

« Nous devons informer le peuple par toutes les tactiques possibles », ajoutait le collectif Anonymous pour expliquer le sens de sa mobilisation en ligne. « Nous ne pouvons pas tolérer plus longtemps que le peuple soit mis à genoux par des robots sans âmes. Qui « servent et protègent » des machines, des institutions capitalistes et l'injustice. Nous protégeons le peuple. Nous ripostons ! ».
L'appel d'Anonymous France à agir en ligne le 22 novembre avait été lancé le 11 novembre dernier par une vidéo sur YouTube, vue près de 7000 fois :

D'autres documents ont été obtenus par les pirates, dont le plus sensible est le calendrier prévisionnel de positionnement et de relève des unités de CRS en France, dans le cadre des missions permanentes, jusqu'à la fin de l'année 2014. Le reste est plus anecdotique, avec la grille de rémunérations des CRS en fonction des grades, le règlement intérieur des compagnies, ou encore un manuel détaillé des véhicules de reconnaissance utilisés par les CRS.

Dès la fin octobre, Anonymous avait réagi à la mort de Rémi Fraisse en affirmant qu'il « ne restera pas les bras croisés », et en annonçant une « Opération Testet » (#OpTestet) pour s'opposer au barrage de Sivens sur la zone humide du Testet. S'en était suivie une série d'actions menées notamment contre le site officiel de la Région du Tarn ou celui de la FNSEA locale :



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

Source : http://www.numerama.com/magazine/31367-opantirep-anonymous-s-attaque-a-la-gendarmerie-francaise.html

---

Virus Regin : Conséquences informatiques ou clash diplomatique ?

Virus Regin : Conséquences informatiques ou clash diplomatique ?

REGIN – Il est déjà considéré comme l'un des malwares les plus sophistiqués de l'histoire de l'informatique. « Regin », le mystérieux logiciel malveillant dont le spécialiste de sécurité Symantec (éditeur de l'antivirus Norton) a révélé l'existence dimanche soir, pourrait bien continuer à faire parler de lui.

Selon le site américain The Intercept, les services de renseignement américains et britanniques se cacheraient derrière. Pour mémoire, The Intercept a été créé par Glenn Greenwald, l'enquêteur ayant publié les révélations d'Edward Snowden sur les programmes de surveillance la NSA.
Citant des sources du secteur et une analyse technique du logiciel, The Intercept affirme que « Regin » est référencé dans des documents fournis par Edward Snowden lui-même, alors qu'il était encore consultant de l'agence américaine de renseignement. Interrogée sur ces informations, une porte-parole de la NSA a répondu par un lapidaire: « Nous n'allons pas commenter des rumeurs ».

L'affaire est néanmoins prise très au sérieux car « Regin » avait des objectifs très ambitieux
le malware aurait été utilisé contre des réseaux informatiques de gouvernements européens et Belgacom, le réseau public de télécommunications belge.
Dans le détail, « Regin » serait capable d'apporter une grande flexibilité aux attaquants. En effet, ces derniers seraient en mesure de charger des fonctions personnalisées adaptées à des objectifs individuels en cas de besoin. Le virus serait notamment capable de réaliser des captures d'écran, de prendre le contrôle d'une souris et de son curseur, de voler des mots de passe, de surveiller le trafic d'un réseau, et de récupérer des fichiers effacés.

Après l'abandon du dossier des « écoutes Merkel »
Si la nature des assaillants parvient à être authentifiée, les vieux démons pourraient se réveiller des deux côtés de l'Atlantique. L'affaire des écoutes de la NSA venait pourtant de refroidir avec l'abandon samedi de l'enquête concernant la mise sur écoute présumée d'un téléphone d'Angela Merkel. Selon le magazine allemand Focus, aucune preuve n'aurait été trouvée sur la responsabilité de la NSA. « Regin » pourrait donc raviver les tensions.
Interrogé par The Intercept, l'expert en sécurité qui a aidé à supprimer le logiciel espion des réseaux de Belgacom est formel. « Après avoir analysé ce malware et regardé les documents Snowden, je suis convaincu que Regin est utilisé par les services de renseignement américain et britannique », a affirmé Ronald Prins. C'est lui qui permet à l'équipe de Glenn Greenwald d'être si confiante dans ses affirmations.
D'autres sources abondent dans ce sens. « Nous sommes convaincus que ce produit est l'oeuvre des Etats-Unis ou de la Grande-Bretagne », a assuré à SC Magazine Erik de Jong, un expert en cyber-sécurité de la firme Fox-IT. « Nous avons examiné les documents de Snowden, les pièces s'imbriquent ». La société finlandaise F-Secure assure sur son blog que le virus, « pour une fois », ne vient pas de Russie ou Chine.

« Considéré comme révolutionnaire »
Symantec se dispense de donner des noms, mais plutôt des indices sur le niveau de sophistication. « Dans le monde des virus informatiques, rares sont les exemples qui peuvent être réellement considérés comme révolutionnaires. Ce que nous avons là en fait partie ». C'est par cette phrase que débute le rapport de la société publié dimanche.
La complexité de « Regin » implique une phase de conception ayant duré plusieurs mois, voire plusieurs années, et qui a nécessité un investissement financier important. « Le temps et les ressources employés indiquent qu'une nation est responsable », assure Candid Wueest, un chercheur travaillant pour le spécialiste américain de la sécurité informatique.

Encore difficile d'identifier formellement le(s) responsable(s)
Pas question néanmoins d'accuser formellement un Etat. « On ne fait pas d'attribution tant que l'on n'a pas de faits concrets, de preuves irréfutables », se justifie-t-il, « mais il est certain qu'on peut tirer des conclusions ». Chez Kaspersky Lab, le principal concurrent de Symantec en matière de sécurité informatique, on se refuse également à pointer du doigt un pays en particulier. La compagnie russe explique néanmoins que ce virus ne peut avoir été développé qu'avec le financement et les moyens techniques d'une agence nationale de renseignement.
Les experts détaillent ensuite le processus. « Les équipes de Symantec ont détecté des brèches de sécurité avérées dans 10 pays, en premier lieu la Russie puis l'Arabie saoudite, qui concentrent chacune environ un quart des infections », a indiqué Candid Wueest. Les autres pays touchés par ordre d'importance sont le Mexique et l'Irlande suivis par l'Inde, l'Afghanistan, l'Iran, la Belgique, l'Autriche et le Pakistan. Un travail d'orfèvre pour les spécialistes du genre.
Lire la suite….

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

Source : http://www.huffingtonpost.fr/2014/11/25/regin-virus-snowden-nsa-gchq-belgique-greenwald_n_6217356.html
Par Grégory Raymond