Charlie Hebdo : les Anonymous sont déjà passés à l’attaque !

Charlie Hebdo : les Anonymous sont déjà passés à l’attaque !

Suite aux attentats survenus à la rédaction de Charlie Hebdo, le collectif de hackers connus du monde entier baptisés les Anonymous, ont promis d’attaquer les sites internet des djihadistes. Beaucoup se sont réjouis de cette nouvelle mais les autorités ont vivement critiqué les intentions des Anonymous craignant une surenchère de menaces.

Mais les Anonymous n’ont pas tenu compte de ces critiques et ont décidé de tout de même mettre en oeuvre leurs plans. Et ils n’ont pas attendu longtemps pour passer à l’attaque. On se demandait comment les hackers allaient s’y prendre pour mener à bien leur action.
48h après leurs déclarations nous en savons maintenant plus. Les Anonymous ont dévoilé une liste des comptes Twitter des djihadistes sur le site Pastebin. Ils ont par ailleurs encouragé les internautes à signaler ces comptes au célèbre réseau social. Mais même si leurs intentions sont louables, elles risquent de ralentir les autorités dans leurs enquêtes.
Par ailleurs, poursuit-il, en s’attaquant au serveur, les pirates d’Anonymous risquent de bloquer des données ou de faire disparaître les traces d’accès aux sites par les criminels. Traces qui pourraient être utilisées pour identifier d’autres terroristes – Olivier Bogaert, commissaire de la Computeur Crime Unit de la police fédérale belge –
Lire également : Premières arrestations d’internautes faisant l’apologie du terrorisme
En effet, en s’attaquant aux serveurs des sites djihadistes les Anonymous peuvent bloquer ou supprimer des données clés pour accéder aux sites des terroristes. Toujours est-il que les Anonymous n’ont pas tardé à passer à l’action. Comme certains de nos lecteurs ont pu le mentionner dans leurs commentaires, leur efficacité pourrait être utile aux autorités. Pourquoi ne pas travailler main dans la main ?

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

Source : http://www.phonandroid.com/charlie-hebdo-anonymous-passes-deja-attaque.html

Cyberattaques djihadistes : la France prête à « réagir », selon l’Anssi

Cyberattaques djihadistes : la France prête à « réagir », selon l’Anssi

L’Agence nationale de cyberdéfense se dit « très vigilante » après des attaques djihadistes de faible intensité contre quelques sites français.

L’Agence nationale de cyberdéfense (Anssi) est « très vigilante » afin « de réagir très rapidement » en cas de cyberattaque de grande ampleur contre la France, nous a confié son patron vendredi soir. Dès le début des opérations de traque des auteurs du massacre à Charlie Hebdo, quelques modestes cyberattaques ont touché la France et ont été revendiquées par des hackers se disant « djihadistes ».
Des messages soutenant les assassinats récents à Paris à Charlie Hebdo et près de Montrouge ont été affichés, à la place des pages d’accueil de quelques sites. La mort des assaillants lors des assauts des forces de l’ordre vendredi soir pourrait inciter les hackers djihadistes à réagir plus violemment.

Le site du Mémorial de Caen vendredi soir à 19 heures :
Jusqu’à présent, les attaques visent des « cibles faciles », selon l’Anssi. Le groupe AnonGhost a défiguré des sous-domaines universitaires, des mairies et au moins un site de personnalité politique (Patrick Devedjian), comme le relèvent Zataz.com et Ouest-France. Des pages affichaient le message « J’atteste qu’il n’y a de dieu qu’Allah. J’atteste que Muhammed est le messager de Allah », rapporte Ouest-France, qui pointe « le Fallaga Team, un groupuscule de hackers islamistes tunisiens ». « Je suis musulman et je suis pas Charlie », précisait un autre message.
D’autres sites, dont celui du Mémorial de Caen (Basse-Normandie) et une centaine d’autres en Bretagne, ont été défigurés ou mis hors ligne. « Au nom de Dieu, si ce hacking n’est pas suffisant pour vous faire parvenir le message. Nous vous connaissons faibles et tueurs d’innocents en Tunisie et aujourd’hui nous n’allons pas nous taire. Sauf le Prophète, chiens, nous ne serons pas cléments avec vous », précisait un message sur le site défiguré du Mémorial de Caen, traduit par France 3 Basse-Normandie, avant que le site ne soit mis hors ligne. Le site de la mairie de Sainte-Marie-aux-Chênes (Moselle) a lui aussi été touché par le même groupe Fallaga Team vendredi matin.

Des attaques « de faible niveau technique », selon l’Anssi
« Nous observons un nombre de défacements de sites internet supérieur à la moyenne et très orientés sur l’affaire en cours, mais toujours de faible niveau technique », nous confie Guillaume Poupard, directeur général de l’Agence nationale de la sécurité des systèmes d’information (Anssi). « L’actualité motive certains à utiliser ce moyen pour porter des messages en s’attaquant à des cibles faciles », regrette-t-il. « L’Anssi et notamment son centre opérationnel restent très vigilants afin d’identifier ces attaques simples et surtout de réagir très rapidement si des opérations de plus grande ampleur venaient à être tentées », assure le patron de la cyberdéfense française.
« Il y a effectivement pas mal de choses qui remontent, des choses à la marge », nous a confié vendredi soir une source haut placée à la gendarmerie nationale, au sein de laquelle les cybergendarmes veillent sur l’Internet français. Mais il n’y a « rien de dramatique, quelques sites d’école et de mairie qui sont défacés », a précisé cet officier, qui a souhaité garder l’anonymat. « Il y a une surabondance de l’usage des réseaux, il vaut mieux les préserver », a-t-il ajouté, confirmant notre information selon laquelle des instructions ont été données aux policiers et aux gendarmes pour limiter leur usage des réseaux de télécommunications.

Rien à signaler chez SFR, OVH ou encore Telehouse
Contactés par nos soins, plusieurs acteurs du secteur télécom, dont le géant français de l’hébergement OVH, le gestionnaire de centres de données Telehouse ou encore l’opérateur SFR, nous ont affirmé vendredi soir qu’ils ne constataient pas d’activité inhabituelle sur leurs réseaux. Orange, qui dispose en Bretagne d’un centre de cyberdéfense, n’avait pas encore donné suite à nos demandes vendredi soir.
Dans le même temps, le groupe de hackers Anonymous, qui a affirmé sa volonté de venger les morts de Charlie Hebdo, a été très critiqué. Son opération, nommée #OpCharlieHebdo, a notamment pour but de neutraliser les moyens de communication des djihadistes. Mais elle met en péril le travail des services de renseignements : privés de leurs comptes habituels, les terroristes sont poussés à changer leurs habitudes de communication, à chiffrer leurs échanges, et ils disparaissent donc potentiellement des radars des enquêteurs.

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

Source : http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/cyberattaques-djihadistes-la-france-prete-a-reagir-selon-l-anssi-09-01-2015-1895301_506.php

l’Allemagne victime d’attaques DDoS

l’Allemagne victime d’attaques DDoS

Les sites du gouvernement allemand, ainsi que la page de la chancelière Angela Merkel, ont été piratés mercredi 7 janvier. L’attaque a été revendiquée par un groupe pro-russe qui demande à Berlin de cesser son soutien au gouvernement ukrainien. Le premier ministre ukrainien est actuellement en visite en Allemagne.

Un groupe de hackers pro-russes, connu sous le nom de CyberBercut, a revendiqué la cyberattaque de plusieurs sites du gouvernement allemand, dont la page d’Angela Merkel et le site du ministère des Affaires étrangères. Le groupe appelle l’Allemagne à cesser son soutien financier à Kiev. Selon les services de renseignements allemands, les sites du gouvernement font face à en moyenne 3 000 tentatives de piratage par jour, certaines venant de l’étranger. Le premier ministre ukrainien, Arseni Iatseniouk, actuellement en visite à Berlin, a attribué l’attaque aux services secrets de Moscou.
Selon Steffen Seibert, le porte-parole du gouvernement, les data-centers sont victimes d’une attaque sévère, perpétrée par des systèmes extérieurs, comme le relate Reuters. Le but des pirates est de saturer les serveurs pour les mettre hors service (attaque DDoS, attaque par déni de service).

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

Source : http://www.industrie-techno.com/cybersecurite-l-allemagne-victime-d-attaques-ddos.35488

L’Epita aide la Police à traquer les escrocs aux faux virements

L’Epita aide la Police à traquer les escrocs aux faux virements

L’École pour l’informatique et les techniques avancées a signé un partenariat avec l’Office Central de Police Judiciaire pour la répression de la grande délinquance financière pour lutter contre les escroqueries aux faux virements qui se sont multipliées depuis 2010. L’Epita travaillera notamment sur des outils de requêtage permettant d’améliorer le traitement et l’analyse des données.

S’il y a bien un type d’escroquerie qui a le vent en poupe en ce moment, c’est bien celle des faux virements. Apparu en 2010, le nombre de ce type d’entourloupes s’est multiplié au point d’atteindre les 700 faits recensés pour un préjudice estimé à 300 millions d’euros, d’après la direction centrale de la Police Judiciaire. Pour lutter contre ce fléau, l’Office Central pour la Répression de la Grande Délinquance Financière (OCRGDF) a mis en oeuvre plusieurs actions, dont un partenariat avec l’Epita afin d’améliorer ses outils, après deux précédents signés en 2011 et 2013, respectivement avec l’Office Central de lutte contre la criminalité liée aux technologies de l’information et de la communication et l’Office central pour la répression des violences aux personnes.
À travers son Institut d’innovation informatique (3IE), l’Epita va ainsi apporter son concours technique à l’OCRGDF pour améliorer le suivi des infractions à caractère économique, commercial et financier liées à la criminalité professionnelle ou organisée. 3IE travaillera, à partir d’une base école constituée de données anonymes agrémentée de quelques cas factices, sur la refonte de la base de données, la création d’applications web et l’implémentation de puissants outils de requêtage, permettant d’améliorer le traitement et l’analyse des données. Ces outils, annoncés comme ergonomiques et intuitifs, seront conçus afin que l’OCRGDF puisse les adapter facilement aux évolutions des comportements des délinquants.
« La lutte contre les nouvelles formes de la criminalité organisée nécessite une complémentarité entre les partenaires publics et privés. C’est dans cette optique que les compétences reconnues de l’Epita ont été une nouvelle fois sollicitées », explique Jean-Marc Souvira, chef de l’Office Central de Lutte contre la Grande Délinquance Financière de la direction centrale de la Police Judiciaire. « Ces partenariats avec la Police Judiciaire s’inscrivent dans la continuité de l’engagement citoyen de l’EPITA et participent au développement de l’éthique des jeunes ingénieurs », a quant à lui indiqué Joël Courtois, directeur général de l’Epita.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-l-epita-aide-la-police-a-traquer-les-escrocs-aux-faux-virements-59814.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

JE SUIS CHARLIE Hommage aux victimes et aux blessés au plus profond de….

En hommage à ce tragique événements, des messages émouvants

qui font vibrer notre solidarité nationale …

Télécharger notre affiche personnalisée en hommage à Charlie Hebdo

JE SUIS CHARLIE

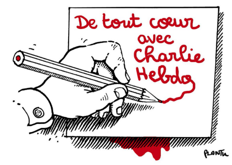
MORTS POUR LA LIBERTÉ

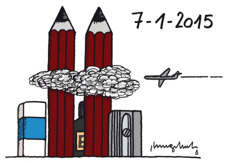
SOLIDAIRES

CHARLIE HEBDO

Face à l’horreur et la barbarie des actes terroristes qui sont survenus en fin de matinée contre le journal #CharlieHebdo, je pense aux familles des victimes, aux journalistes et aux forces de l’ordre.

Les plus beaux messages de la journée. »Ils voulaient mettre la France à genoux. Ils l’ont mise debout » »12 morts, 66 millions de blessés. »





Expéditeur: Direction Generale France <direction.generale.france.fr@sodexo.com>
Date: 7 janvier 2015 20:43:28 UTC+1
Destinataire: L'ensemble des collaborateurs <L'ensembledescollaborateurs@sodexo.com>
Objet: Attaque terroriste à Paris aujourd'hui

Cher tous,

Comme vous l'avez peut-être appris, l'hebdomadaire Français *Charlie Hebdo* a fait ce matin l'objet d'une attaque terroriste faisant douze morts et une dizaine de blessés dans les locaux du journal situés dans le centre de Paris.

C'est avec beaucoup d'émotion que je vous informe que Frédéric Boisseau, 42 ans, marié et père de deux enfants de 10 et 12 ans, collaborateur de Sodexo en France depuis 15 ans, figure parmi les victimes de cet attentat. Frédéric était responsable de l'équipe chargée d'assurer la maintenance du bâtiment pour le compte de la Régie Immobilière de la Mairie de Paris, un client de Sodexo en France.

Je vous invite à vous joindre à moi pour adresser nos pensées les plus émues à la famille et aux proches de Frédéric, ainsi qu'à ses collègues présents à ses côtés ce matin.

Tous ensemble, nous partageons le sentiment qu'il est intolérable qu'un de nos collègues ait ainsi pu perdre la vie dans des circonstances aussi tragiques et injustes, et pour une cause si contraire à nos valeurs.

Michel Landel
Directeur Général du Groupe

e-mail, attachments included, is confidential. It is intended solely for the addressees. If you are not an intended recipient, any use, copy or diffusion, even partial of this message is prohibited. Please delete it and

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

Source : https://www.facebook.com/pages/Je-suis-Charlie/759873537399013

Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

La CNIL a fait publier au Journal Officiel une délibération créant une norme simplifiée pour autoriser les entreprises et les administrations à enregistrer les conversations téléphoniques des employés sur le lieu de travail.

Comme l'y autorise l'article 24 de la loi du 6 janvier 1978, la CNIL a publié une « norme simplifiée » qui permet d'alléger les formalités administratives pour être autorisé à procéder à l'écoute et l'enregistrement des conversations téléphoniques du personnel sur le lieu de travail. La norme, qui vaut autorisation pour quiconque déclare s'y conformer, a été publiée ce mardi au Journal Officiel, en tant que délibération n° 2014-474 du 27 novembre 2014.
Elle autorise les entreprises et les administrations à écouter et enregistrer les conversations téléphoniques des agents et employés, avec toutefois un certain nombre de réserves. Notamment :
Les écoutes et enregistrements doivent être « ponctuels » et donc ne peuvent pas avoir de caractère « permanent ou systématique », y compris pour les salariés qui seraient en période d'essai. Toutefois la CNIL se garde de fixer un critère chiffré, que ce soit en quantité brute ou en proportion d'appels enregistrables ;

Il n'est pas autorisé de croiser les enregistrements avec des données provenant d'une capture d'écran du poste informatique de l'employé ;

Les enregistrements doivent uniquement servir à la formation des employés, leur évaluation ou « l'amélioration de la qualité du service » ;

L'enregistrement vidéo est proscrit dans le cadre de la norme simplifiée (c'est-à-dire il faut solliciter une autorisation complémentaire) ;

Les employés et leurs interlocuteurs doivent être informés de la possibilité d'enregistrement, et d'une série d'informations complémentaires (finalité, catégories de données traitées, destinataires, transfert hors UE le cas échéant, droit d'accès…).

Les enregistrements doivent être effacés au maximum 6 mois après leur collecte, et conservés avec « toutes précautions utiles pour préserver la sécurité des données », notamment d'identification des personnes autorisées à y avoir accès.

En outre, la CNIL précise que la norme simplifiée s'applique également aux « documents d'analyse, tels que les comptes-rendus ou les grilles d'analyse réalisés dans le cadre des écoutes et des enregistrements ». Elle précise que les données collectées dans ce cadre doivent être « adéquates, pertinentes et non excessives » au regard des finalités définies, et qu'elles ne peuvent porter que sur les données identifiant l'employé et l'évaluateur, les informations techniques de l'appel (date, heure, durée), et l'évaluation professionnelle correspondante.

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

Source : http://www.numerama.com/magazine/31780-la-cnil-simplifie-l-enregistrement-des-appels-telephoniques-au-travail.html
Par Guillaume Champeau

Le ministère de la Défense attaqué par des ‘Anonymous’

Le ministère de la Défense attaqué par des ‘Anonymous’

Le site Web du ministère de la Défense était inaccessible en raison d’une attaque en déni de service revendiquée par un groupe baptisé Anonymous OpGPII. Ils déclarent vouloir venger la mort du militant Rémi Fraisse.

Le site Internet du ministère de la Défense a fait l’objet hier 6 janvier d’une attaque informatique en déni de service, le rendant ainsi inaccessible aux internautes une bonne partie de la journée. « Le Centre d’analyse en lutte informatique défensive (Calid) est sur le coup » indiquait hier un porte-parole du ministère à 20Minutes.

Le DDoS a depuis été revendiqué sur Twitter par les membres d’un groupe se revendiquant d’Anonymous et baptisé « Anonymous OpGPII ». Ces derniers justifient cette attaque informatique par la mort du militant écologiste et opposant au barrage de Sivens, Rémi Fraisse, tué par une grenade des gendarmes le 25 octobre dernier. D’ailleurs pourquoi la Défense et non l’Intérieur dont dépend désormais la gendarmerie ?

« Aujourd’hui, nous commençons une opération pour le venger » déclarent des Anonymous dans un message mis en ligne sur le site Pastebin et repéré par le Figaro. « Pendant trop longtemps, Anonymous est resté à l’écart, nous n’avons pas pris de mesures. Mais maintenant, nous allons le faire » promettent-ils encore.

Un autre membre des Anonymous assurait cependant hier à 20 Minutes que le mouvement (jamais véritablement coordonné) n’était en rien responsable de l’attaque contre le ministère de la Défense. « Cela dit, cela fait des années qu’on leur a fait remarquer que leur site est truffé de failles » soulignait-il aussi.

De quoi permettre de futures attaques ? Une plainte pourrait en tout cas être déposée par le ministère, qui précise par ailleurs que deux adresses IP, liées au déni de service, ont été identifiées et signalées aux autorités.

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

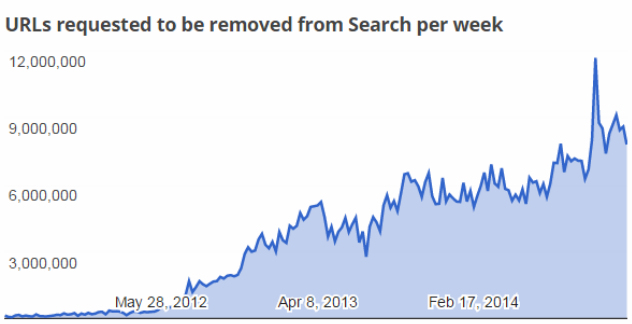
Source : http://www.zdnet.fr/actualites/le-ministere-de-la-defense-attaque-par-des-anonymous-39812391.htm

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

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

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

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



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

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

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

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

Attaquer des sites internet : Désormais un service comme un autre…

Attaquer des sites internet : Désormais un service comme un autre…

Les hackers de Lizard Squad vendent leurs services pour attaquer les sites

Faites-leur attaquer les sites concurrents
Vous aussi vous trouvez que GamAlive est un site qui mériterait d'être mis hors service ? Vous aussi vous estimez que nous dépassons trop souvent les bornes et que notre irréverence mérite un châtiment digne de ce nom ? Vous aussi vous pensez que nos moqueries répétées contre, au choix, les religions, les défenseurs des animaux, les végétariens, les porteurs de tongs, les racistes, les homophobes, les routiers et les fans de Sexion d'Assaut ne peuvent rester impunies, justement parce que vous êtes un pieux routier végétarien racite et homophobe qui défend les animaux et écoute Sexion d'Assaut dans son camion qu'il conduit avec des tongs ?

Ne cherchez plus et faites tomber le site GamAlive.
En effet, les Lizard Squad, ce groupe de hackers à l'origine des perturbations du PSN et du Xbox Live durant les fêtes de Noël, proposent désormais leurs services contre une modeste rétribution.
Ainsi, pour une somme allant de 6 à 500 dollars, vous pouvez vous offrir leurs services. Des attaques DDoS sont proposées contre les sites de votre choix. Des attaques d'une durée de 100 secondes à 30 000 secondes. Réparties sur plusieurs journées, elles peuvent aller jusqu'à bloquer un site pendant une vingtaine de jours, selon leurs dires.
Actuellement, seuls les bitcoins sont acceptés comme moyen de paiement, mais Paypal devrait prochainement être proposé aux clients intéressés par leurs services, même si on doute que le géant américain du paiement en ligne accepte de blanchir de l'argent issu de la cybercriminalité. Car on vous rappelle, au cas où vous seriez un peu con (comme un routier fan de Sexion d'Assaut qui conduit en tongs), que s'offrir leurs services est un acte illégal et répréhensible.

Et non, nous ne vous donnerons pas l'adresse du site, pour des raisons évidentes et, là aussi, légales.
Lire la suite….

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

Source : http://www.gamalive.com/actus/23252-hackers-lizard-squad-services-payants-attaques-ddos-sites-propose.htm
Par Cedric Gasperini

Vie privée, vie professionnelle, sommes-nous tous espionnés ? Reportage Zone Interdite

Vie privée, vie professionnelle, sommes-nous tous espionnés ? Reportage Zone Interdite

Avec le développement de la technologie, le monopole de la surveillance électronique n'est plus réservé à l'Etat : surveiller ses proches ou ses employés est devenu un jeu d'enfant.
Paul et Nicolas, deux maris, se livrent à l'espionnage conjugal. Ils ont installé des logiciels sur les téléphones portables de leurs épouses afin de suivre leurs conversations. Mais le danger vient aussi d'Internet, où les traces laissées sont très difficiles à contrôler. Des salariés ont ainsi été licenciés pour avoir critiqué leur patron sur Facebook. Cette tendance a parfois des conséquences tragiques. Aux Etats-Unis, Tyler Clementi, 18 ans, s'est donné la mort après avoir été filmé par ses colocataires. Au Royaume-Uni, des volontaires scrutent les images des caméras de surveillance pour dénoncer les infractions. Ils sont payés pour chaque alerte donnée.

Vie privée vie professionnelle sommes nous tous espionnés 1/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 2/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 3/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 4/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 5/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 6/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 7/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

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

Source : http://www.programme-tv.net/programme/culture-infos/r8841-zone-interdite/2703356-vie-privee-vie-professionnelle-sommes-nous-tous-espionnes/